E-Health Data Security Using Hybrid Encryption Techniques

Ridwan Olayinka KOLAPO

LCU/PG/000145

Being a PhD Thesis Submitted to the Department of Computer Science, Faculty of Natural and Applied Sciences, Lead City University, Ibadan, Oyo State, Nigeria.

In Partial Fulfillment of the Requirements for the Award of Doctor of Philosophy Degree (PhD) in Computer Science

2022

Certification

This is to certify that Kolapo Ridwan Olayinka with matriculation number LCU/PG/000145 carried out this research work titled "E-Health Data Security Using Hybrid Encryption Techniques" in the Department of Computer Science, Faculty of Applied Sciences, Lead City University, Ibadan, Oyo state, for the award of Doctor of Philosophy Degree(PhD) and that this has not been previously submitted.

. . . .

Dr. Wilson Sakpere
Supervisor

Date

. . . .

Dr. Wilson Sakpere
Head of Department

Date

Dedication

This Thesis is dedicated to the Lord God Almighty for the gift of life and for His Mercies.

Acknowledgment

I want to thank the prestigious institution Lead City University for the Opportunity to learn ad complete my PhD program and to the University Library for the provision of adequate materials needed.

I am grateful to the Department of computer Science for giving me the privilege and opportunity to study and to learn, my appreciation goes to my supervisors, Dr. P. Achimugu, Dr. W. Sakapere and Prof. S. O. Akinola. I also like to acknowledge my lecturers, Dr. A. A. Waheed, Dr. A. M. Ayoade, Dr. W. Ajayi, Mrs K. Okesola for their supports and always ensuring that things are done rightly .

My appreciation goes to my family who has always supported me through this program.

“Even though the above-mentioned institutions and persons have assisted in the process of this research work, I alone stand responsible for the errors, if any, found in the work”

Abstract

The introduction of cryptography has brought plenty of improvement to health informatics, but not really employed in health institutes and this is often as a results of the protection issues that come together with the employment of e-Health systems. Security issues is taken into account a significant concern which is why health institutes still opt to follow the normal way of addressing health records. This study aim to ensure data security in health record using enhanced Ceasar Cipher, Affine Cipher and Red2 Cryptographic Techniques.

This method used is considered a double enhanced encryption algorithm with a steganography technique because it combines an enhanced Ceasar encryption method with Affine Cipher encryption technique to enhance security of medical health records along with Red2 algorithm, which helps encrypt cipher-text messages and hide them in images. The integration of the enhanced Caesar and affine ciphers is as follows: First, each field in the record is encrypted with the enhanced Caesar cipher encryption method, and the encrypted output is used as the input for the affine cipher encryption method after-which the output of the second encryption phase is fed into the steganography stage and the final output of the developed system is presented as an image.

The result of this study is presented as a software solution and also some metrics like accuracy, precision, recall and F1-score were measure to test the performance of the system and it shows that the enhanced ceasar cipher encryption technique used in this study has a larger computational time which compensate for the high level of security and also the image used for steganography resulted to having lesser image quality parameters as this also compensate for the addition security level.

In conclusion, the main aim of cryptographic system and steganographic system is to protect the confidentiality of data both at rest and in transit. With the mix of the enhanced Ceasar Cipher method and Affine cipher alongside Red2 Algorithm, these techniques has helped to enhance effectiveness.

Keywords: e-Health, cloud, encyrption algorithm, Ceasar Cipher, Affine Cipher, Red2 algorithm.

Word Count: 338

Table of Contents

Chapter Two: Literature Review

List of Tables

List of Figures

Chapter One

Introduction

1.1 Background to the Study

As the world of technology has progressed, it is also helped within the advancement of health-care sector. Technology has been a major tool within the improvement in fields like diagnosis, medicine, treatment and patient monitoring[1]. Securely collecting, maintaining and sharing patient records between hospital servers are often both arduous and costly[2]. In recent years, health personnel in countries round the world are investigating the likelihood of migrating a number of their medical systems to the cloud . Cloud computing is said to be the practice of having a network of resources to store, process and manage data on the web instead of a stationed physical infrastructure. Cloud computing offers the chance of offloading a number of the burden of maintaining this data by storing records in a very remote location while keeping it easily reachable and safely protected[3].

Information and communication technology (ICT) has brought about the thought of central business Model in electronic health. E-Health is defined as "the cost-effective and secure use of data and communications technologies in support of health and health-related fields, including healthcare services, health surveillance, health education, knowledge and research[4]. E-health record basically are stored on a physical devices which makes recovery have certain limitation and might be damaged but a cloud-based electronic health record cannot be damaged unless the cloud cease to exist. A good number of advantages of e-Health are reported, it can reduce time to diagnosis, improve equity of access for patients in remote areas, improve quality of life, and improve patient satisfaction[5]. Additionally, e-Health has the potential to create health care workers more efficient and produce system benefits and

technological spin-offs.

Cloud services are delivered through open network (internet), it are often accessed at any time anywhere within the world. These facilities may be accessed by various devices like mobile phones, laptops so many other devices.

Health-care is increasingly being supported by IT applications, like Cloud Computing. But sharing sensitive personal information in Cloud Computing will be risky, when an unauthorized user gets access to the present information and uses it aside from those intended by providers which make this thesis address the safety concerns of e-Health within the cloud. Many countries are keen to shift their traditional health care services to the new technology of Cloud Computing, so as to enhance the standard of care and reduce the price. However, these opportunities introduce new security risks which can not be ignored[5].

Most electronic health record system developed do not seem to be delivered through an open network because it is delivered to suit into just the workstation of a selected health institute and cannot be accessed outside that environment. A few are deployed which are mobile-based application but cloud lifts off this limitation of getting electronic health record system during a static platform as cloud-based electronic health system is delivered through the web which is able to make the health personnel work even from home and even giving the patient access to access their medical history/record using the proper generated key as authentication and authorization to the system, this can be enough reason to adopt cloud computing technology within the Health Sector[5].

Confidentiality of information in literature is expounded to data privacy, which make sure the safety of information and is formed available to only authorized users. This could be difficult because of the multi-tenancy properties of the cloud. Data

privacy may be done through encryption which may be symmetric or asymmetric encryption algorithm[6]. Confidentiality of knowledge raises questions when handling data in cloud and application hosting in cloud, because there are able to have two-sided confidentiality level which may be at the client-side or the cloud side,one amongst the questions is “Where is that the encryption and decryption taking place?”.

Many electronic health record system has been developed achieving the aim of automating the normal classification system but since the existence of cloud computing technology few works are done on Cloud-based health system[6] because health records/data is taken into account confidential records which should be kept secret and available to only the owner of the record and also the health professional treating the patient, this been a serious concern which has not allowed for much works to done and implemented on the cloud from the health sector because security of knowledge in cloud is that the most tedious add cloud computing.

According to a survey administered over 90% of chief technical officers believed that the first reason for not using cloud computing services is that of the information security and privacy concerns. Most health institute are not well convinced about the protection loopholes been filed which is even making it difficult for many of the hospitals to modify from the standard file system which consumes plenty of space and requires more human effort to the utilization of the automated system talk less of getting a Cloud-based health system. The few health institutes that have electronic health record system implemented and in use are watching closely the safety problems with cloud technology and don't seem to be able to shift to the cloud space. This can be the most reason for the shortage of maturity level in health informatics cloud computing technology[7].

Although providers get together on data sharing, interoperability remains a large challenge in several parts of the system, stakeholders have long better-known the crucial role of interoperability, it is still difficult to induce completely different information systems to exchange data with each other. Providers use systems with varied technical specifications, language, and semantics[8]. Some progress has been made through "meaningful use" necessities by the federal. Standards are set that have helped manufacturers and software designers build more compatible systems.

Cryptographic techniques play an important role within the field of cloud security. the simplest thanks to secure a message is cryptography[9]. Today, many methods of encryption are supported by public keys. Public-key cryptography is claimed to be the best method in the field of cryptography because it is used for both confidentiality and authentication[10]. In this work, the Caesar method was combined with a block cipher with a higher level of security than the traditional Ceaser method. However, this procedure applies only to type 1024 bits. In this study, the Ceaser and Affine Cipher are combined as a method alongside a steganography technique to improve the effectiveness and security level of the eHealth record system. The Ceasar method is one of the most effective ways to protect your messages and is still in use today, so use the Ceasar method. We also use the Affine Cipher method because it has the same properties as the Ceaser method.

1.2 Statement of the Problem

eHealth record is considered sensitive , several security measures implemented overtime using the ceasar technique has not really "beefed up" the security lapses to any high extent. The conventional Ceasar cipher technique is considered easy to hack and weak because of the computational complexity of the Caesar cipher is of order O(n) which is *a* linear and low complexity which implies little work to decipher and

reverse engineer. Also, the conventional Caesar cipher is limited to only ***n*** key possibilities, where ***n*** corresponds to the size of the English alphabets in Uppercase which is not a comprehensive representation of the English Language characters because it ignores the lowercase alphabet versions of the English alphabet used for encryption shifting which makes the number of key possibility equals to 25. These gap in literature is why this study considered enhancing the conventional Ceasar technique and increasing the range of key possibilities from from 26 to 256 and the key value range has been increased from 25 to 255 therefore more complexity and a double layer encryption techniques alongside a steganography technique to help enhace data security of eHealth records.

1.3 Justification of the Study

Considering the fact that e-Health has been in existence in different phases of medicine, tele-health and electronic medical records, there is a need to consider the security level of every records that are stored or categorized under e-health as a big umbrella. Several security implementation has been considered but the level of security implemented in this study uses both cryptographic and steganography

1.4 Aim and Objectives

The aim of this study is to ensure data security in health record using hybrid encryption techniques.

The objectives of this research are as follows to;

1. develop a model that will enhance data security in eHealth records.
2. encrypt text using two encryption techniques .
3. implement a stenography technique in objective 2 above.
4. Evaluate the performance of the developed technique.

1.5 Significance of the study

This study will help in the field of health informatics to help improve the security by introducing a 3-tier security phases This study if not carried out will leave the security gap in health informatics, though lots of works has been done to lift this security issues but this study will help left off this gap to a good height.

1.6 Scope of Study

The scope of this study is to deal with health record system and the cryptographic technique used in this study makes use of the same key for encryption and decryption in techniques one, three keys for encryption, shifting and decryption in technique two and the steganography technique used in this study has no need for the usage of keys for hiding and un-hiding images.

1.7 Limitation of the Study

This study is limited to the field of health-informatics as the cryptographic technique and the steganography technique used in this study is applied to just medical records. This study is tailored to textual data only as there are different variants of data such as Multimedia.

1.8 Operational Definition of Terms

Algorithm: An algorithm is a procedure used for solving a problem or performing a computation. Algorithms act as an exact list of instructions that conduct specified actions step by step in either hardware- or software-based routines.

E-Health: e-health is an emerging field in the intersection of medical informatics, public health and business, referring to health services and information delivered or enhanced through the Internet and related technologies.

Cryptography: In computer science, cryptography refers to secure information and communication techniques derived from mathematical concepts and a set of rule-

based calculations called algorithms, to transform messages in ways that are hard to decipher.

Steganography: Steganography is the technique of hiding secret data within an ordinary, non-secret, file or message in order to avoid detection; the secret data is then extracted at its destination

Encryption: Encryption is the method by which information is converted into secret code that hides the information's true meaning. The science of encrypting and decrypting information is called cryptography.

Decryption: Decryption is the process of transforming data that has been rendered unreadable through encryption back to its unencrypted form.

Plaintext: Plaintext is what encryption algorithms, or ciphers, transform an encrypted message into. It is any readable data including binary files in a form that can be seen or utilized without the need for a decryption key or decryption device.

Ciphertext: Ciphertext is encrypted text transformed from plaintext using an encryption algorithm. Ciphertext can't be read until it has been converted into plaintext (decrypted) with a key. The decryption cipher is an algorithm that transforms the ciphertext back into plaintext.

Endnotes

[1] Y. Alotaibi & F. Federico. *The Impactof Health Technology on Patient Safety*. **Saudi Med J**: 38(12), 2017, 1173-1180.

[2] I. Keshta & A. Odeh. *Security and Privacy of Electronic Health Records: Concern and Challenge*s. **Eyptian Informatics Journal**. 22(2), 2021, 177-183.

[3]P. A. Sanjay, S. Mani, & J. Zambrano. *A Survey of the State of Cloud Computing in Healthcare*. **Network & Communication Technologies**, 1(2), 2019, 12-19.

[4]Y. Hu & G. Bai. *A Systematic Literature Review of Cloud Computing in E-Health*. **Health informatics-An international journal (HIIJ)** Vol 3, No 4. 2019.

[5] R. L. Bashshur , G. Shannon , E. A. Krupinski, J. Grigsby. *Sustaining & realizing the promise of telemedicine.* AvailableOnline:http://europepmc.org/abstract/MED/23289907.

[6]B. Thimma Reddy, K. Bala Chowdappa, & S. Raghunath Reddy. *Cloud Security using Blowfish and Key Management Encryption Algorithm*. **International Journal of Engineering and Applied Sciences.** 2015 ISSN: 2394-3661, Volume-2, Issue-6.

[7]Gartener: *Seven Cloud-Computing Security Risks*. InfoWorld.2008-07. Available Online: http://www.infoworld.com/d/security-central/gartener-seven-cloud computingsecurity-risks-853.

[8]V. Joshua & L. D. Gamm. "*Health Information Exchange: Persistent Challenges and New Strategies*." **Journal of the American Medical Informatics Association** 17(3) 2014, 288–94.

[9] S. Bhawar & K. Joshi. "A *Review on Cloud Security Based Encryption and Decryption Techniques.* **International Journal of Engineering Research and Technology** 2021, Volume 10, Issue 02..

[10]T. Chuang Wang Zhi-xiang Zhu *Hybrid Encryption Algorithm Based on Wireless Sensor Networks* **IEEE International Conference on Mechatronics and Automation (ICMA)** 2019 ISBN: 978-1-7281-1699-0 DOI: 10.1109/IEEE Tianjin, China.

Chapter Two

Literature Review

2.1 Introduction

Cryptography is the science of using mathematics to encrypt and decrypt data. or it's the ability to send information between participants, in an obfuscated format, this prevents others from reading it. it allows you to store sensitive information or transmit it over unsecured networks (such as the Internet) so that no one other than the intended recipient can read it[1].

Today, our entire world depends on the Internet and its application to every aspect of their lives. This is required to secure our data through cryptography. Cryptography plays an important role in the science of secret texts[2]. It is the art of protecting information by transforming and applying technology. Perhaps the main reason to use email is the convenience and speed with which it can be transmitted, regardless of geographical distance. Today, one day, our entire planet depends on the Internet and its application to protect national security. Cryptography is used to ensure that the contents of a message are transmitted confidentially and will not be altered. Cryptography provides several security goals to ensure the confidentiality of data, data Modification, etc[3]. The idea of encryption and encryption algorithms by which we can encrypt our data into a secret code and cannot be read by hackers or unauthorized people even if it is attacked. The main reasons for not using encryption in email communications are current email encryption solutions and hardware key management. Various encryption techniques to promote information security. The evolution of coding is moving towards a future of endless possibilities. Because hacking can't be stopped, we're able to keep our sensitive data secure even if it's hacked by using encryption techniques and information security[4].

2.2 Concepts used in Cryptography

Authentication: Authentication mechanisms help establish proof of identity. This process ensures that the origin of the message is correctly identified.

Confidentiality: The principle of confidentiality specifies that only the sender and the intended recipient should be able to process the contents of a message[5].

Availability: The principle of availability states that resources should be available to authorized parties all the times.

Integrity: The integrity mechanism ensures that the contents of the message remain the same when it reaches the intended recipient as sent by the sender.

Access Control: Access Control specifies and controls who can access the process.

2.2.1 Types of Cryptography

Cryptography can be classifies into three categories:

- Symmetric Key Cryptography (Private/Secret Key Cryptography)
- Asymmetric Key Cryptography (Public Key Cryptography)
- Hash Function

2.2.1.1 Symmetric Key Cryptography

Symmetric key cryptography is a type of cryptography in which a single public key is used by both the sender and the receiver for the purpose of encrypting and decrypting a message[6]. This system is also known as private or secret key cryptography and AES (Advanced Encryption System) is the most widely used symmetric key cryptography[7].

The symmetric key system has the major disadvantage that both parties must somehow exchange keys securely, since there is only one key for encryption and decryption.

Types:

AES (Advanced Encryption Standard),

DES,

Triple DES,

RC2,

RC4,

RC5,

IDEA,

Blowfish,

Stream cipher,

Block cipher, etc. are the types of symmetric key cryptography[8].

2.2.1.2 Asymmetric Key Cryptography

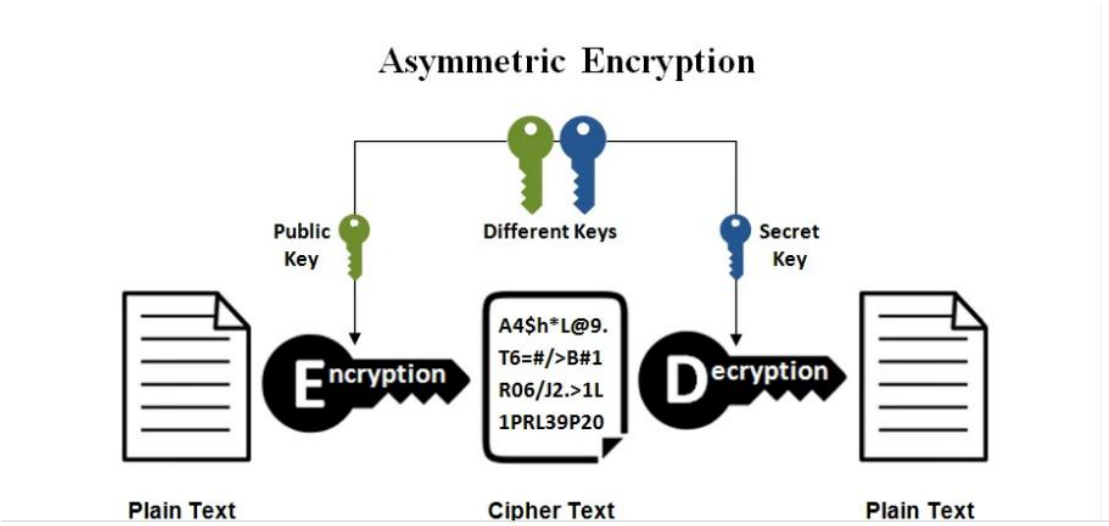


Figure 2.1 Asymmetric Encryption[8]

Asymmetric key cryptography is completely different and a more secure approach than symmetric key cryptography. In this system, each user uses two keys or a key pair (private key and public key) for encryption and decryption. The private key is kept secret from each user, and the public key is distributed over the network, so if anyone wants to send a message to any user, they can use those public keys[9].

One of the two keys can be used to encrypt the message and the other to be used for decryption purposes. Asymmetric key cryptography is also known as public key cryptography and is more secure than symmetric key cryptography. RSA is the most popular and widely used asymmetric algorithm[10].

Types of Assymetric key cryptography

RSA,

DSA,

PKCs,

Elliptic

Curve techniques, etc. are the common types of asymmetric key cryptography.

2.2.1.3 Hash Function

A hash function is a cryptographic algorithm that takes an input of arbitrary length and outputs a fixed length. A hash function is also considered as a mathematical equation that takes a seed (digital input) and produces an output known as a hash or message. This system works one way and does not require any keys. In addition, it is considered the foundation of Modern cryptography[11].

A hash function works by operating on two fixed-length blocks of binary data and then generating a hash code. There are different cycles of the hash functions, and each cycle takes a combination of the input of the most recent block and the output of the last

cycle.

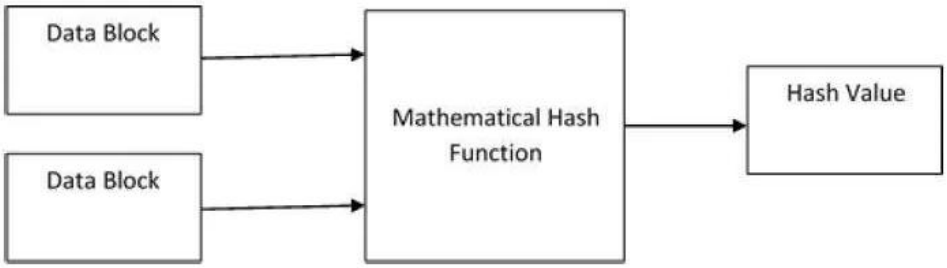


Figure 2.2 Hash Function[11]

Types of Hash Functions

Common hash functions include

Message Digest 5 (MD5),

SHA (Secure Hash Algorithm),

RIPEMD, and

Whirlpool.

MD5 is the most commonly used hash function to encrypt and protect passwords and private data[12].

Difference between Symmetric, Asymmetric and Hash Function Cryptography

Symmetric keys use a single key to encrypt and decrypt messages, and asymmetric keys use a key pair. One key is used for encryption and the other is used for decryption, but the hash function does not both decrypt and decrypt using the key necessary.

A symmetric key is relatively faster than a hash and asymmetric, but less reliable in terms of security.

Asymmetric keys were introduced to overcome the problem of key exchange in symmetric keys, and hash functions were introduced to provide more security than ever before[13].

If the key's compromised over the community then there'll lack of each sender and receiver in symmetric key, most effective lack of key proprietor in uneven key, and in hash function, there may be no key to compromise.

An asymmetric key has a higher complexity than a hash function, and a symmetric key has a much lower complexity.

How does cryptography work?

Cryptography algorithms, or cryptography, are mathematical functions used in the encryption and decryption process. Cryptographic algorithms work in combination with keys, words, numbers, or phrases to encrypt plain text. The same plaintext is encrypted with different keys for different ciphertexts. The security of encrypted data depends only on two things: the strength of the encryption algorithm and the confidentiality of the key. In addition to the cryptographic algorithm, all possible keys and all the protocols that make them work make up the cryptosystem[14].

2.3 Application Area of Cryptography

Cryptography has applications in many areas, from payment gateway security to secure messaging platforms like WhatsApp. Some of these applications are:

Figure 2.3 Application Area of cryptography[14]

1. **SSL/TLS Encryption:**

Browsing the web today is secure because you can encrypt the flow of data primarily through encryption. From browser identification to server authentication, encryption and encryption generally facilitated web browsing.

2. **Digital Signatures:**

As virtual contracts became more important, the arena became lacking a stable channel for skipping important files. Encryption provides a layer of authentication so you can verify the source, confidentiality, and integrity of your files.

3.**Safe Online Banking:**

Online banking services and payment applications will be considered later if they do not include data encryption. Encryption allows authentication systems to verify the identity of a particular individual before making a transaction, reducing credit card fraud in the process.

4. **Secure Chatting Services:**

Messaging apps such as WhatsApp, Telegram, and Signal employ end-to-end encryption protocols that ensure that no one but the sender and receiver can read the message. This is a big step from the era of text messages, where security has always been an issue. Thanks to encryption, there are many communication platforms available.

5. **Encrypted Emails:**

Since a large amount of personal information passes through the inbox, a secure communication method is absolutely necessary. Emails are now always encrypted, thanks to encryption algorithms such as PGP (Pretty Good Privacy).

6. **Crypto-Currency:**

With blockchain technology, cryptocurrencies have experienced astronomical rising interest rates and are still one of the most popular trading markets today. Thanks to encryption, fully decentralized, secure and tamper-proof systems have permeated the digital realm of today. The implementation is different in so many different ways that encryption has found its location. The next section on what encryption is, describes how to use encryption[15].

2.4 Historical Significance of Cryptography

The use of encryption may be traced to as a long way returned as approximately 3000 B.C., all through the Babylonian Era. Encryption technology developed as they had been utilized in navy and political settings, however because of the current extensive use of the Internet and the dramatic boom in the quantity of facts humans come into touch of their day by day lives, the settings wherein encryption technology are carried out and carried out have increased, and they're now used all round us in our day by day lives[16]. The records of encryption is the records of "the competition of wits" among encryption builders and encryption code breakers. Each time a brand new encryption set of rules is created, it's been decrypted, and that during flip has brought about the introduction of a brand new encryption set of rules, and cycles of set of rules introduction and decryption were repeated to this day. This white paper provides a short records of cryptography and the way encryption-associated technology have developed and could preserve to adapt in addition to the measures Internet customers ought to don't forget whilst enforcing current encryptions[17]. Hieroglyphics (pictograms utilized in historic Egypt) inscribed on a stele in approximately 3000 B.C. are taken into consideration the oldest surviving instance of encryption. Hieroglyphics had been lengthy taken into consideration not possible to ever study, however the discovery and observe of the Rosetta Stone within side the nineteenth century changed into the catalyst that made it viable to study hieroglyphics[18]. The "scytale cipher" changed into a shape of encryption used within side the metropolis kingdom of Sparta in historic Greece across the sixth century B.C. It concerned the usage of a cylinder of a positive diameter round which a parchment strip changed into wrapped, and the textual content changed into written at the parchment strip alongside the lengthy axis of the cylinder[19]. The approach of encryption changed into designed in order that the recipient might be capable of study it via way of means of wrapping the

parchment strip round a cylinder of the identical diameter. Encryption techniques like the “scytale cipher” that depend upon rearranging the series wherein characters are study are noted as “transposition ciphers”. The Caesar cipher, which regarded within side the 1st century B.C., changed into so named as it changed into regularly utilized by Julius Caesar, and it's miles a mainly distinguished approach of encryption a few of the terrific variety of encryption techniques that emerged all through the lengthy records of encryption[20]. The Caesar cipher approach of encryption entails changing every of the letters of the alphabet within side the unique textual content via way of means of a letter placed a fixed variety of locations similarly down the series of the letters within side the alphabet of the language. The sender and receiver agree earlier to update every letter of the alphabet within side the textual content via way of means of a letter that is, for instance, 3 letters similarly down of their alphabet.

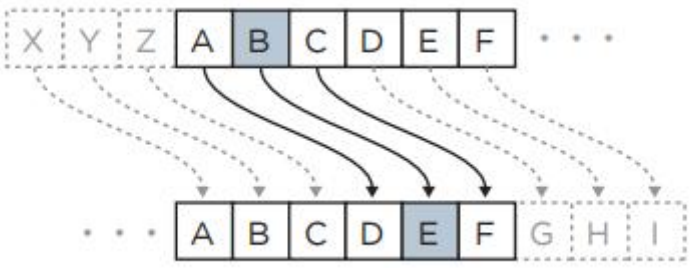


Figure 2.4 Ceasear Cipher Encryption[21]

Caesar ciphers are sometimes called "shift ciphers" because they involve character shifts. If the alphabet consists of 26 characters, the text encrypted with the Caesar cipher can be decrypted by trying 26 patterns. However, instead of shifting the letters by a fixed number of letters, you can freely change the order, which greatly increases the number of possible patterns (26-letter alphabet example: 26 x 25 x 24 x ... . = 400,000.0 00,000,000,000,000,000,000 patterns!) And dramatically makes decryption difficult[21].

Cryptography that rearranges strings according to specific rules as described above is called "surrogate encryption". Surrogate cryptography is a well-known encryption method and the most widely used encryption method in the history of encryption. A Modern cryptographic machine called the "Enigma" described below has made it possible to use the substitution cipher process at a higher level. An analytical method that decodes a "simple substitution cipher" that relies on character replacement rules, using the reverse method of taking advantage of the fact that each letter of the alphabet can be replaced by just one letter. B. Caesar cipher is known as "frequency analysis". Frequency analysis uses the frequency of letters (for example, the English alphabet has a frequency characteristic common to the letters listed below) to infer unencrypted letters and reprint the original text. To identify[22].

• The letter “e” is the most frequently used letter. (Figure 2)

• The letter “u” almost always follows the letter “q”.

• The words “any”, “and”, “the”, “are”, “of”, “if”, “is”, “it”, and “in” are very common.

All of the above cryptographic methods, including replacement and transposition ciphers, consist of an "encryption algorithm" and a "key". Cryptographic algorithms are the rules used to encrypt and decrypt text. Cryptographic algorithms refer to cryptographic rules, for example, by shifting characters with a substitution cipher, wrapping a strip of sheepskin in a cylinder, or writing a message with a transposition cipher. The key refers to the number of places where the character is shifted in the substitution cipher and the diameter of the cylinder used in the transpose cipher. Shifting a character by 5 digits in a Caesar cipher is different from shifting by 4 digits, which means that a different "key" is used[23].

2.4.1 **Classical Encryption**

Cryptography became popular in the Middle Ages as cryptography became more sophisticated based on the efforts to break classical cryptography and the knowledge gained from the invention of new cryptography[24]. The increase in diplomatic activity during this period led to an increase in the need to send sensitive information and led to the frequent use of encryption. The weakness of the "simple substitution cipher" represented by the Mary Queen of Scotts cipher Caesar cipher was that only one encrypted character could be assigned to each character in the alphabet. A well-known example of 16th-century cryptanalysis that took advantage of this weakness was the decryption of the code used by Queen Mary of Scotland to communicate with staff. The content of these messages convicted her and was executed in a plot to kill Elizabeth I of England[25]. The cipher used by Mary was known as the "nomencater cipher" and contained codes to replace phrases as well as letters in the alphabet. These "codes" can be found in the "codebook", which is the "key" of the ciphers owned by both the sender and the receiver, making it difficult to break the ciphers[26].

2.4.1.1 **Vigenère Ciphers**

A simple substitution cipher containing a pattern to replace each letter, such as that used by Queen Mary of Scotland, was finally deciphered. In addition, the "nomencater" used by Queen Mary of Scotland involved creating a huge codebook and providing each crypto user with a codebook, which was difficult. The issue of "getting and providing keys" was a problem for both Modulusern and medieval users of advanced cryptographic techniques[27]. At the beginning of the 15th century, Leon Battista Alberti developed the prototype of the "multi-table replacement" cipher. They have been widely used for decades, including the use of more than one set of scrambled alphabets. Such ciphers have been known as Vigenère ciphers since the

16th century since Blaze de Vigenère invented the powerful final form of multi-table substitution ciphers[28]. The Vigenère cipher involves the use of a diagram called the Vigenère square (Figure 2.5). For example, if you use the key "OLYMPIC" to encode "GOLD MEDALIST", the characters in the original text refer to the characters listed in the table above, and the characters in the key refer to the characters on the left side of the table. The encrypted message is at that intersection.

Plain text	GOLDMEDALIST
Key	OLYMPICOLYMP
Encrypted message	UZJPBMFOWGEI

Figure 2.5 Vignene Cipher[28]

Messages encrypted with Vigenère cipher are completely different depending on the key, so even if a third party obtains the conversion table, it is very difficult to decrypt the message without the key[29]. The point here is that there is no limit to the number of characters (frequency) that can be used as a key, so you can design an infinite number of keys. It took more than 100 years from the idea to the invention of the Vigenère cipher, but at that time simple substitution ciphers were used, so encryption and

decryption with the Vigenère cipher was more difficult than simple substitution ciphers. Therefore, it took time to compensate. Until Vigenère cipher is put into practical use[30].

2.4.1.2 **Uesugi Cipher**

During the 16th century, codes were created in Japan, including the use of Polybius squares. How to create an encrypted message is described in a book on the art of war written by Usami Sadayuki, a strategist of Kenshin Uesugi, a military commander during the Warring States period (civil war). This Uesugi cipher involves the use of a table consisting of 48 Japanese syllable phonetic characters engraved in a 7-by-7 grid, where each character is represented by a number at the top of each row and column[31]. (Figure 2.6)

七	六	五	四	三	二	一	
ゑ	あ	や	ら	よ	ち	い	一
ひ	さ	ま	む	た	り	ろ	二
も	き	け	う	れ	ぬ	は	三
せ	ゆ	ふ	ゐ	そ	る	に	四
す	め	こ	の	つ	を	ほ	五
ん	み	え	お	ね	わ	へ	六
	し	て	く	な	か	と	七

Figure 2.6 Uesugi Cipher[31]

2.4.2 **Modern Ciphers**

Ciphers during World War I and the Emergence of Encryption Machines

With the advancement of communication technology, encryption and decryption were actively carried out during World War I. German communications cable disconnected from Britain When Britain (UK) declared a war with Germany at the beginning of World War I (WW I), Britain disconnected Germany's underwater communications cable, and the German army After having to run the international communications cable, all over Britain or wireless communications, and the German army began to encrypt their communications to prevent enemy nations from reading them[32]. However, the UK forwarded all intercepted messages to an agency called the Admiralty Intelligence Department, nicknamed "Room 40," which was set up to decrypt encrypted German communications. One of his achievements was deciphering Zimmermann's Telegram[33].

2.4.2.1 **Zimmermann Telegram**

At the start of World War I, the involvement of the United States on the European front had an impact on the outcome of the war. Then German Foreign Minister Zimmermann devised a plan in which Mexico and Japan would launch attacks on the United States to prevent the United States from participating in the war in Europe[34]. Zimmermann ordered the German Ambassador to Mexico to carry out the attack, but the message was decrypted by Room 40. However, the UK decided not to reveal the contents of the message, partly because it wanted to prevent it. The Germans engineered an even stronger attack. code. after discovering that the UK had successfully decrypted their messages. In the end, Britain provided the US with a plain text telegram sent by the German Embassy in Mexico and stolen by a spy who

had infiltrated the Mexican telegraph office[35]. After receiving the telegram, the United States declared war on Germany and joined the European front.

The point here is that each time a cipher is broken, a stronger encryption method is developed. However, those who succeed in breaking the code usually do not reveal it immediately, but will continue to use this method for some time. As explained below, this is a Modulusern cycle of cryptographic creation and cracking[36].

2.4.2.2 **ADFGVX Cipher**

The ADFGX cipher devised was first put into practical use in 1918. You need to write 5 characters ADFGX in the columns and rows and replace 1 character with 2 characters. The encryption method is basically the same as Uesugi encryption so far. However, a special feature of ADFGVX cipher is that the resulting sequence of characters is now re-encrypted using transposed ciphers[37]. The ADFGX cipher was later improved by using the 6-character ADFGVX instead of the 5-character to make it easier to identify when sending a message over Morse code (Figure 2.7).

	A	D	F	G	V	X
A	d	h	x	m	u	4
D	p	3	j	6	a	o
F	i	b	z	v	9	w
G	1	n	7	0	q	k
V	f	s	l	y	c	8
X	t	r	5	e	2	g

Figure 2.7 ADFGVX Cipher[37]

Cryptography using such charts is virtually impossible to decrypt by discarding the key after only one use. However, this means sharing a huge number of keys with the front lines, so delivering and receiving these keys is a major obstacle to using them in combat[38].

2.4.3 **The Birth of Enigma**

The difficulty of decrypting ciphers, which were prepared by hand before the 20th century, dramatically increased with the emergence of encryption machines at the start of the 20th century. Enigma was the name of an encryption machine designed by the German inventor Arthur Scherbius in 1918, and it was marketed with portability and confidentiality as its sales features. Since the German forces had not yet learned that the cipher they were using in WW I had been decrypted when Enigma was first marketed, they were not aware of the need to improve their cipher, and because Enigma was very expensive, it was not adopted by the German forces. When Germany later discovered that they had lost WW I as a result of their cipher having been cracked by the British, a sense of crisis developed in Germany, because they felt the fate of the nation rested on ciphers, and it was then that they decided to adopt Enigma[39]. The ciphering method used by Enigma is known as a polyalphabetic substitution cipher, and the "key" consists of a combination of gear wheels (rotors), known as "a scrambler", on each of which 26 letters of the Modulusern alphabet are inscribed, and a mechanism known as the plugboard for performing single character substitutions[40]. Enigma is used by first setting the scrambler and then typing plain (unencrypted) text on the keyboard of the Enigma machine. The scrambled characters scrambled by the scrambler are displayed on the ramp panel. The scrambler rotates one dial each time a character is typed[41]. That is, different keys are used to scramble individual characters. Enigma decrypts encrypted messages when the same key used

to prepare the encrypted message is used to decrypt the message, facilitating both decryption and encryption. The Germans continued to improve after taking over the Enigma, choosing three out of five rotors for the scrambler and increasing the number of rotors accommodated from the original three to five[42]. The German army was completely confident in the Polish Enigma, but while Poland was under threat of German aggression, it was possible to decrypt the Enigma message, which is called the "bomb (cryptographic bomb)" in English. Invented the decryption system[43]. However, for economic reasons, Poland was unable to keep up with the increasing number of cryptographic schemes used in Germany when the Enigma was improved, and Poland was unable to continue its decryption efforts. Therefore, in 1939 Poland provided the UK with sufficient funding and personnel for research information and asked the UK to decipher it.Just two weeks later, Poland was invaded by Germany and World War II began[44]. The UK then began decrypting messages created by Germany on the Enigma machine using the information received from Poland. The discovery that the Germans repeat the same three letters twice at the beginning of an encrypted message to indicate a pattern (key) was a milestone in decrypting the Enigma message. The German information obtained by breaking the encrypted message of Enigma, called "Ultra" by Britain, was an important source of information for the Allies until the end of the war. Decoding the Enigma was kept secret, and the German army trusted and used the Enigma until the end of the war. (The decryption of the Enigma cipher was published in 1974, more than 20 years after it was achieved)[45].

2.4.3.1 **DES Cipher**

As the example of the Enigma cipher above shows, the decryption of the cipher was kept confidential by the country[46]. In 1973, the US Department of Commerce's

National Institute of Standards and Technology (NBS, later the National Institute of Standards and Technology (NIST)) publicly called for the US government to adopt encryption as a standard. Encryption algorithm. It is one of the two components that make up a cipher. H. The "encryption algorithm" and "key" have been revealed[47]. This was a historically important switch for encryption. NBS approved Data Encryption Standard (DES) encryption in 1976. This has become a global standard. Setting the encryption procedure for each personal use puts a heavy burden on the enterprise[48]. For example, when a bank sent a message to a major customer in the 1970s, the bank passed the key directly to the customer through a "key bearer." As the volume of banks increased and the number of keys delivered increased, key delivery became an administrative nightmare for banks[49]. Therefore, the disclosure of the encryption method was the trigger to solve this problem. Cryptography has reached a historically significant turning point with the disclosure of the algorithm, but the use of the "key" remains the same because the "same key" was used for both encryption and decryption (common key cryptography).). Same as Caesar cipher or DES cipher. The main problem with common key encryption was the supply of keys[50].

2.4.3.2 **Decrypting the DES Cipher**

When this technique is used in a public key cryptosystem, the number to the left of the equal sign is used as part of the public and private keys. For ridiculously large prime numbers, it is difficult to decipher the prime number to the right of the equal sign in a reasonable amount of time[51]. Of course, the details of the mathematical explanation are skipped here, but this property of prime factorization makes it difficult to decrypt the private key based on the public key. In fact, the British cryptographic research institute invented the public key cryptosystem before RSA, but the invention of the new cryptography was considered a top secret because it was

treated as a state secret, so its existence was made public until it was released. did not. 1997[52]. The public key cryptosystem is a very convenient system for exchanging the key for decrypting a cipher with only a specific party or multiple parties over the Internet. In other words, public keys are available to everyone on the Internet because it is difficult to decrypt the private key in a reasonable amount of time, but public key cryptosystems are all practical[53]. It can be considered that it is used for a specific purpose. A dramatic solution to the key distribution problem that has long been the cause of the problem. Here, simply think of SSL (Secure Socket Layer) as a method that makes it possible to easily encrypt information that can be used by anyone on the Internet by using this common key cryptography together with public key cryptography[54]. Let's look at. Cryptography (RSA cryptography) was used. SSL, proposed by Netscape Communications, is a protocol integrated into Netscape Navigator that enables secure communication between web servers and clients. Features of SSL include authenticating the identity of the server (web or mail server) and issuing a digital certificate used by the client for verification before initiating SSL communication. The correct server. It also encrypts subsequent communications to prevent data interception and leakage. The common key (actually, the random number that is the source of the common key) is securely distributed via the public key cryptosystem to establish encrypted data communication, and the key distribution problem is the public key[55]. Clearly resolved using. Key cryptosystem. Public key cryptosystems have significant advantages over shared key cryptosystems because they can expose their keys. However, the encryption process is time consuming and uses a combination of methods to perform message encryption using a common key securely provided by the public key cryptosystem.

2.5 Public-Key Cryptosystem

The solution to the key distribution problem, which has been a problem since the Caesar cipher era, was finally achieved with the advent of public key cryptosystems. Whitfield Diffie, Martin Hellman, and Ralph Merkle anticipate the era of network computing and work to solve the public key problem[56]. At the 1976 National Computer Conference, they presented the concept of "public key cryptosystem". It allows you to encrypt communications by using asymmetric keys (public and private keys) without first providing an encryption key. A private key known only to the recipient is used for decryption[57]. The key exchange concepts developed by Diffie, Hellman, and Merkle include Modular operations and one-way functions, or more precisely the function Y = AX (Modulus B). This function means that dividing A by a power of X by B leaves a remainder of Y. The shared key is obtained by performing the calculation using the procedure described below. This provides the same solution for both parties[58]

• The values of A and B are shared by sender and recipient before transmission of a ciphered message. (As an example, let us assume that A = 7 and B = 11).

• Then an X is specified that only the sender or receiver knows (in this example, we assume X = 3 and x = 6). • The values of X and x, and the corresponding Y and y, are calculated based on the common values of A and B. (The resulting values for Y and y in this example are Y = 2 and y = 4).

• Each party then supplies its own Y value to the other party.

• Each party then uses its own X value and the other's Y value to perform the Modular calculation again to get the solution. (Result Yx (Modulus 11) = 26 (Modulus 11) = 9, yX (Modulus 11) = 43 (Modulus 11) = 9) The concept of being able to publish a conversation while maintaining confidentiality is the exchange of secret keys. It led to

an innovative discovery that led to a major rewrite of the basic principle of having to. However, we have not yet been able to find a one-way function that achieves asymmetric encryption using different keys for encryption and decryption. This theory of public key cryptography was put into practice in the form of "RSA encryption"[59].

2.6 RSA Cipher

Three researchers at the Massachusetts Institute of Technology, Ronald L. Rivest, Adi Shamir, and Leonard M. Adolmen, have developed a mathematical method used to realize the concept of public key proposed by Diffie and Hermann[60]. This public key cryptography is called "RSA cryptography", which is the first letter of the names of the three researchers who developed the mathematical method. The RSA cryptosystem uses prime factorization. Prime factorization means factoring a number so that it is a prime number (a number that cannot be divided by 1 and any number other than itself), as shown in the following example.

$95 = 5 \times 19$

$851 = 23 \times 37$

$176653 = 241 \times 733$

$9831779 = 2011 \times 4889$

When this technique is used in a public key cryptosystem, the number to the left of the equal sign is used as part of the public and private keys. For ridiculously large prime numbers, it is difficult to decipher the prime number to the right of the equal sign in a reasonable amount of time. Of course, the details of the mathematical explanation are skipped here, but this property of prime factorization makes it difficult to decrypt the private key based on the public key[61]. In fact, the British

cryptographic research institute invented the public key cryptosystem before RSA, but the invention of the new cryptography was considered a top secret because it was treated as a state secret, so its existence was made public until it was released in. 1997[62]. The public key cryptosystem is a very convenient system for exchanging the key for decrypting a cipher with only a specific party or multiple parties over the Internet. In other words, public keys are available to everyone on the Internet because it is difficult to decrypt the private key in a reasonable amount of time, but public key cryptosystems are all practical. It can be considered that it is used for a specific purpose[63]. A dramatic solution to the key distribution problem that has long been the cause of the problem. Here, simply think of SSL (Secure Socket Layer) as a method that makes it possible to easily encrypt information that can be used by anyone on the Internet by using this common key cryptography together with public key cryptography[64]. Let's look at. Cryptography (RSA cryptography) was used. SSL, proposed by Netscape Communications, is a protocol integrated into Netscape Navigator that enables secure communication between web servers and clients. Features of SSL include authenticating the identity of the server (web or mail server) and issuing a digital certificate used by the client for verification before initiating SSL communication[65]. The correct server. It also encrypts subsequent communications to prevent data interception and leakage. The common key (actually, the random number that is the source of the common key) is securely distributed via the public key cryptosystem to establish encrypted data communication, and the key distribution problem is the public key. Clearly resolved using. Key cryptosystem. Public key cryptosystems have significant advantages over shared key cryptosystems because they can expose their keys. However, the encryption process is time consuming and

uses a combination of methods to perform message encryption using a common key securely provided by the public key cryptosystem[66].

2.7 Responsive Action of Cipher Enhancements for SSL

Efforts are being made to change the public key key length specification from 1024 bits to 2048 bits and to make the public key signing method conform to the SHA2 standard in order to respond to the increase in computer computing power. Timelines and guidelines for these issues are set by browser vendors and certification bodies based on recommendations from NIST, which develops cryptographic standards. In addition, SHA2 is receiving more attention from companies considering support for PCI DSS because the Payment Card Industry Data Security Standard (PCIDSS) complies with NIST recommendations. Users who use SSL encryption for communications can quickly upgrade client devices such as PC browsers, mobile phones, smartphones, and other devices, as well as web servers, to devices that can use the new hash functions for longer keys. It is important to process or respond and maintain the strength of encryption[67].

2.8 Crypto Techniques

Cryptography is defined as a technique to change meaningful data into a useless format using a key and restore the original format also using a key. Some techniques use multiple ways to encrypt and decrypt data, for example; asymmetric, symmetric, and attribute-based encryption. It facilitates data security, user and data authentication, user authorization and non-repudiation[68]. Although each of these methods has its own properties and uses a variety of techniques to ensure data security, these techniques and their use in the field of e-health research are presented below. First, symmetric or secret key encryption uses the same secret key for both encryption and decryption of the data. There are a number of specific benefits such as policy enforcement,

assigning roles and access privileges to each user, and key management where specially authorized people are granted keys and access rights, all of which this must be observed when using the secret key encryption algorithm[69]. In the field of electronic health, the most popular secret key algorithm is Advanced Encryption Standard (AES) . According to NIST, AES is considered a fast and secure symmetric algorithm for electronic health. The idea of using selective encryption using AES technique was brought up, where different keys are used to encrypt part of a file and each user, depending on their role, receives different keys. from the file owner[70]. It was also recommends using Selective AES which is an upgraded version and is better than original AES in terms of security and speed. Here it is suggested that before encryption with AES, the data is compressed and the key size is set according to the user choice, which ranges from 128 to 192 to 256. AES was recommended with big data in eHealth application by using custom AES in DaaS, one of the cloud services, making it faster and more efficient than ever when it is used with big data[71]. The use of secret key encryption is very effective for protecting eHealth data, however, meeting the requirements of eHealth role-based decryption will require customization to selective encryption or the use of a database engine. access control mechanism with it[72]. Then an asymmetric key encryption algorithm or public key encryption using a key pair where the key called the public key is used for encryption and the other key is used for decryption is called private key. The most common of these encryption techniques used in e-health are RSA and Elliptic Curve Cryptography (ECC)[73].

One of the security techniques using RSA includes users divided into different Modules such as administrators, patients, doctors and hospitals, then encrypt smooth beads, specific data Related to each user of this Module encrypted.

Using RSA in the medical database, encrypted files are stored in multi-level databases as well as private keys. In this concept, depending on the user level in the database, each user has access to his profile where he can get a private key and decode the files[74]. Another asymmetric encryption algorithm, CEC has a computer improvement that other linear algorithms due to CEC has been taken into account to protect the EHEALTH system[75]. The use of ECC techniques for related systems and comparing its performance with RSA and related research that CEC has faster performances because it uses smaller size keys RSA and maintains the level Proper security. ECC was used with an integrated unit dedicated to data encryption and decryption. This integrator includes a chip for user identification and a smart card reader, a USB (Universal Serial Bus) controller and a wireless transmitter where the USB is linked to the device wirelessly by USB protocol transmits using wireless transmitter architecture[76]. IBE was used for PHR access control, the use of this mechanism can reduce the complexity of key management and also make it resistant to outside attack, equation attack, reverse attack in computing context cloud[77]. An enhanced IBE program and an enhanced identity-based proxy re-encryption (IBPRE) program for use in electronic health systems was described and demonstrations on their security, analyzed their performance. Their yield, resulting in 'IBE is a secure INDsIDCPA (indistinguishable in an identity-choosing plaintext attack), IBPRE is INDIDCCA2 (indistinguishable as a plaintext-based identity-based attack) 2) safe. They also show that the IBPRE program performs better re-encryption, resulting in eHealth data protection and cost savings for users of the cloud-based eHealth service. The third technical crypto type is accumulated (ABE) in which the data is encrypted based on a specific attribute that must be adjusted to the user to decode the files[78]. ABE is a complement to the public key password with two methods; One is CIPHERTEXT

ABE policy (CPABE) in which each digitization is delimited according to the decoding strategy and others are an ABE (Kpabe) key in which the link between the lock and Cipher-text is reversed[79].

For these reasons, ABEs are used in eHealth systems to be able to provide role-based decryption and granular access control of publicly shared files, implying that even if a person with access to specific data, only an authorized user who meets the required set of key structural characteristics will be able to decrypt and read the files. These characteristics make it suitable for electronic health requirements[80]. CPABE was used as encryption mechanism and solved the problem of key rebuilding caused by any policy change by attaching a single-pin proxy (OTP) re-encryption method so that it is secure and easier to access. only by authorized personnel[81]. A software library containing both CPABE and KPABE and built a policy generator that was used to generate ABE policies using encryption keys that could be generated and data that could be encrypted chemical[82].

Multi-Authority ABE (MAABE) was used where the ABE is implemented with the division of users into domains, each with similar privileges, which reduces the difficulty with key management[83]. The refined and improved MAABE (eMAABE) was used to securely share PHR data. This Model ensures the security of the data and the user's retrieval as required. Finally, among the previously mentioned algorithms, combinations of different types can be used in a hybrid environment. These types of hybrid systems are equipped with more than one encryption technique, e.g. proxy re-encryption with asymmetric key encryption[84]. A type of unified cipher that includes RSA and AES. RSA is used to generate digital signatures that provide user authentication and AES is used to encrypt data to ensure data integrity and confidentiality[85].

An architecture called SAPPHIRE was introduced here to protect user privacy by providing anonymity and improved policy governance for key data owners. It is a combination of RSA and AES[86]. To provide a secure environment for DSE storage, a combination technique was proposed including symmetric block cipher, Blowfish for data encryption, and RSA for key encryption. This mechanism uses an enhanced version of RSA (eRSA) which is faster than native RSA. This combined method provides better security than any single encryption method[87]. Another use of the hybrid system is to use ABE in combination with image cryptography to insert a coded prescription and transmit it from doctor to pharmacist[88]. Another hybrid technique that uses AES and ABE together in eHealth, where AES is used to encrypt files and upload them to eHealth cloud, and ABE i.e. KPABE is used to give the user privileges access is associated with their attributes[89]. An hybrid Model was proposed that uses a combination of AES and MAABE to provide enhanced services for security, privacy, and access control to the existing eHealth system. It also improves system scalability and protects the system from attacks such as Man in the Middle Attack (MITM), Eavesdropping and Denial of Service (DOS) attacks[90]. The security mechanism used in [91] is ABE with the binary search tree method. Effective use of CPABE, this technique ensures that EHR privacy and security are appropriately maintained even during data sharing and fuzzy keyword searches. A proposed framework using a combined IBE and ABE mechanism was proposed which provides security through data secrecy, granular access control, and preventing inappropriate access to users' EHRs with multiple roles[92]. trick. The combination of IBE and ABE reduces administration costs as well as encoding and decoding times. This mechanism uses AES to encrypt data files and ABE to encrypt AES keys[93]. Using the IBE, ABE

and the signature of the Proposed Model provides authorized access control and audit controls[94].

An enhancement was provided to the existing Secure Index Search (SIS) algorithm to enhance control and information flow in the EHR cloud using a key management scheme[95]. mHealth application Models was proposed which uses ABE and IBE schemes, specifically IBBE and CPABPRE (proxy re-encoding based on ciphertext policy attribute). Patient data can be securely shared between patients and doctors, and patients can discover others with similar health conditions using private data matching and ensure the confidentiality and integrity of data is maintained. Patients can choose their doctor, encrypt and download the data, and authorized doctors will decrypt it. CPABPRE provides granular access control. Doctors simply generate a re-encryption key and re-encryption is performed by a proxy[96]. A mobile e-health solution was proposed that uses IBE to protect customer credentials, homomorphic encryption (HE) of medical records, and proxy re-encryption (PE) to protect privacy rights of each organization in the field of e-health[97].

Hybrid Maabe and KPABE hybrid systems, health records Safe and expandable hybrid systems (Hssehrs), are divided into two areas of security, called public domain names (PUD), where Health care professionals are accessible at EHR expected, HR sector (PSD) for people related to patients. Maabe used for many PUD attribute agencies can provide secret keys for PUD and Kpabe users used specifically to encrypt and manage PSD secret keys[98]. Other types of hybrid systems, hybrid mechanisms are proposed to solve the link, where is the situation that reliable cloud provider (CP) tries to access access from records The patient's health hinders the patient's data security and can track a patient and identify it, CP can do so because he is responsible for indexing the medical image and ' Download the downloads of the

Health Hospital Provider and Consumer Hospital. Therefore, this approach considers a third part of confidence as a safe and exact strategic communication that applies to strategic encryption data (PEP), which is then transferred to the image Blurred and encryption points (WEP), where it marks images, then encrypt and transfer images to random points (RP). RP is responsible for calculating the index of random images and the cache time makes it difficult for knowing CP to know the exact order of data received from the supplier hospital. When a consumer hospital wants data, it asks a third party to provide an index of medical images, then PEP secures the consumer's access to this data, sends the indexes and votes data access for CP. To gain access to accurate medical images, the consumer hospital performs an unconscious transfer process. [230] proposed a public cloud solution to prevent linking where, before sending a record to the public CP, the record is anonymized using a component known as translation. data pseudo-anonymization. This service includes PEP and a local cache that will randomize the order in which records are delivered to the CP[99]. In general, using a hybrid system is quite advantageous because it takes advantage of the features of more than one set of rules where those features can be extended securely, compute quickly, with less overhead. , using digital signatures, providing access[100].

2.9 Non-Crypto Techniques

As mentioned earlier, encryption has a significant impact on the security of eHealth systems. However, there are other methods that can provide security besides the encryption method. However, it is not widely used because it does not provide partial security to the eHealth cloud than the security provided by cryptography. Therefore, these systems are used in hybrid systems that use an cryptographic approach. Some of them are shown below. One such approach is the Authentication and Access Control Manager (AAM) prototype. In this prototype, users use tokens to access profiles

stored in the cloud to identify and access server users through the AAM server. This Model is cloud-based for complex calculations[101]. Another approach is to provide users with useful features such as file access, sharing, and management by establishing a central authority (CA) that divides individuals into layers of security. So; patients, doctors, nurses, families, insurance companies. Here, in order to gain user access and authentication, the security layer grants different access rights for each user, and this Model is responsible for the distribution of encryption keys[102]. A combination of Extensible Markup Language (XML), Attribute Based Access Control (ABAC), and Extensible Access Control Markup Language (XACML) were used for role-based access control (RBAC), policy enforcement, electronic medical record representation, and more[103]. Realized the benefits of. Record via XML. Due to the weak characteristics of RBAC, a two-tier access control mechanism consisting of a first-tier role-based access control and a second-tier extended RBAC was proposed the second level is time-centric and stores patient appointments individually[104]. Therefore, RBAC determines who can see the requested service, and enhanced RBAC shows the value of each service. A cloud-based, privacy-aware, role-based access control Model for controlling and tracking authorized access to data and resources was proposed[105]. Of the healthcare system. Another notable task is that which presented a new certificate-based encryption technique using Keyword Search (CBEKS). This technique is implemented using asymmetric encryption techniques. To set the correct permissions, the data recipient must send a keyword that describes the desired data file, followed by a certificate that represents the permissions that will be provided to that recipient. Keyword scope with Privacy Protection Equivalence Test (PET) and dynamically searchable encryption with Multi-Keyword Search (DSEKRSMS) were used to provide an effective approach. Searchable and privacy

protected for data exchange in cloud-based e-medical systems[106]. To reduce the time required for data validation, a hybrid blockchain Model of completely private blockchain (FPB) and federation blockchain (CB) has been proposed, here the FPB is used as the classical database for the medical institute and the CB is used to store the medical data of all the participating doctors. It provides tamper resistance and reliable storage[107]. The watermarking approach used in this study can mitigate internal threats to ehealth systems[108].

A patient-centric eHealth system Model was examined where an EHR system that is personally controlled using blockchain technology. You can use the blockchain to verify ownership of patient data, grant permissions, and ensure data integrity[109]. A protocol called Pseudonym-Based Encryption and Various Agencies (PBEDA) was proposed along with multi-layer blockchain technology for e-health systems to meet the standards of distribution architecture[110]. Blockchain was used to consolidate each outsourced EHR operation into a single transaction, protecting outsourced EHR from unauthorized changes[111]. A combination of blockchain and peer-to-peer interplanetary file system approaches was proposed IPFS', it provides a storage that provides secure distributed data storage and an efficient shared access control scheme[112]. EHEALTH Information System EHIS guarantee a framework consisting of entities for generating and managing marriage information to support. Patient (1P): Healthcare recipient, Provider (2P): Healthcare service, Payer (3P): Insurance company, National database (ND): Data storage cloud and certificate authority: Certified: Certified 3 person. The legitimacy of the 3PEHI framework[113]. The access control mechanism implemented in Mehealm Cloud, called risk-based control, provides access based on AIC (availability, integrity, confidentiality) principles. An approach that provides client platform security using trusted virtual domains (TVDs)[114]. This author used secret sharing to

maintain the privacy and high security of EHEALTH CLOUD[115]. A secure and simple frame is proposed here where EHEALTH data is divided into several segments, each of which is encrypted with a private key method and stored in an acceptable way. The order of the data and the decryption process are known to the user. This approach helps with all kinds of security measures, while the framework manages confidentiality and data security[116]. An Integrated Circuit Index (ICMetric) was propsed here, a framework for ensuring the security of wearable IoT healthcare devices. Here, the wearable sensor uses a MEMS (Micro Electro Mechanical Systems) bias to create an ICMetric device. This Model provides security services such as confidentiality, availability, user device reliability, data integrity, secure access control, and attack protection, device capture attack, brute force attack, dictionary attack, rainbow table attack, etc[117]. An architecture was shown using the Mandatory Access Control Security Model (MACSM) and the Access Control List Security Model (ACLSM). It is valued for providing high reliability, efficiency and reliability to protect patient information[118]. A security architecture for eHealth systems to avoid problems with major web-based systems was proposed which is Little or no link failure and fault tolerance[119]. Therefore, they presented a decentralized electronic medical system called iMedik D that facilitates both local and centralized access[120]

To protect the privacy of eHealth Public Cloud, a group-signed referral Model has been introduced to make health data unavailable to certain physicians. The authors also suggest that indexing patient records should not reveal their information, but should facilitate efficient searches[121]. A secure data sharing scheme that maintains data anonymity and confidentiality while sharing between public clouds using the provided bilinear matching mechanism was proposed here[122]. An e-health monitoring system using a geo-distributed cloud (GDC) and a traffic shaping algorithm (TSA)

was proposed, these help minimize service delays and protect the privacy of your health data[123].

2.10 Steganography Overview

With encryption, the message is Modified in a format encrypted using an encryption key known only to the sender and recipient. No one can access the message without using the encryption key. However, sending an encrypted message can easily raise suspicion of an attacker, so an encrypted message can be intercepted, attacked, or forcibly decrypted[124]. Steganography technology has been developed to overcome the shortcomings of cryptography. Steganography is the art and science of communicating in a way that hides the existence of communication. Thus, steganography hides the existence of data so that no one can detect its presence. In steganography the process of hiding information content inside any multimedia content like image, audio, video is referred as a "Embedding". For increasing the confidentiality of communicating data both the techniques may be combined. So, steganography (hiding information) and cryptography (protecting information) are totally different from one another[125]. Due to invisibility or hidden factor it is difficult to recover information without known procedure in steganography. Steganography recognition method, known as steganography analysis. Good imperceptibility and ample data capacity (hidden information efficiency) are two characteristics that all steganography techniques should have. The steganography algorithm uses a shared secret called a stegokey[126].

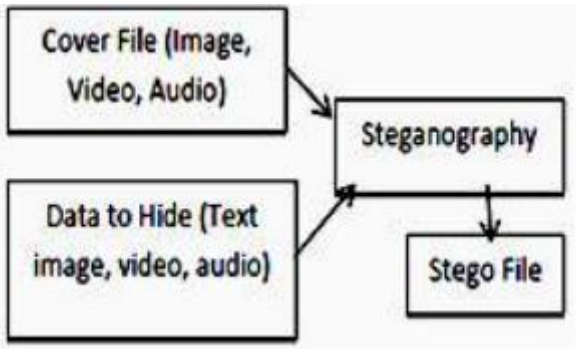


Figure 2.8 Block Diagram of Steganography[126]

Investigations include several cryptographic techniques and LSB, LSBM, LSBMR, SSHDT, RSTEG, OPA, GeneticX-Mean algorithm, VSS, SDSS, FDSS, BPCS, GLM algorithm, SDS, conversion domain technology, warping technology and more.

2.10.1 **Types of Steganography**

Different types of steganography exist depending on the nature of the cover object, there are many suitable steganography techniques for maintaining security[127]

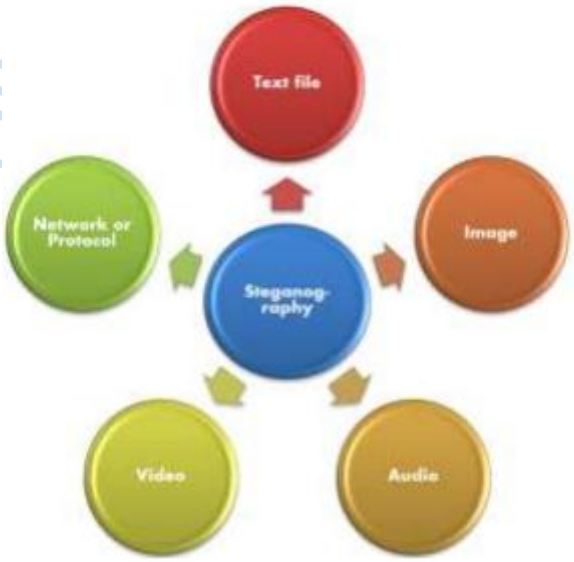


Figure 2.9 Phases of Steganography[127]

2.10.1.1 Text file Steganography

Secret data is hidden in a text file. In this way, secret data is hidden after every nth letter of every word in a text message. Text steganography requires less memory because it can only store text files. This allows for rapid communication or transfer of files from one computer to another. Text steganography is not commonly used for text files that contain large amounts of redundant data[128]. There are many ways to hide the data in a text file.

These methods

I)Format Based Method;

ii) Random and Statistical Method;

iii) Linguistics Method.

Image Steganography:

The process of hiding a secret message in an image file is called image steganography, and the process of using a cover object as an image to hide data is called image steganography. There are certain restrictions. For example, you may not be able to embed a large amount of data in an image because the image may be distorted, and you may suspect that the image may contain information. The traditional image steganography algorithm is the LSB embedding algorithm[129].

2.10.1.2 Audio Steganography

The method of hiding confidential information in audio is called audio steganography. It's also very robust in nature, but there is a limit to the amount of data that can be hidden. This method hides data in WAV, AU, and MP3 sound files. There are many different methods of audio steganography[129].

These methods are

i) Low Bit Encoding

ii) Phase Coding

iii) Spread Spectrum.

2.10.1.3 **Video Steganography**

There are two main types of steganography;

the spatial domain and the frequency domain.

Spatial Domain Based Method:

Transform Domain Based Method:

The method of hiding confidential information in a video is called video steganography. In this case, the video (combination of images) is used as a carrier to hide the data. In general, the Discrete Cosine Transform (DCT) changes the value used to hide the data in each frame of the video (for example, 8.667 to 9). This is imperceptible to the human eye. H.264, Mp4, MPEG and AVI are the formats used in video steganography[129].

2.10.1.4 **Network or Protocol Steganography:**

Network or Protocol Steganography is used to Modify a single network protocol. Hides information using network protocols such as TCP, PDU (Protocol Data Unit), UDP, ICMP, and IP as cover objects. Very safe and robust [129.]

2.11 Techniques Of Steganography

There are various steganography techniques used based on the information to hide. This Study gives a brief overview of some image steganography techniques as follows:

Figure 2.9 shows that different steganography techniques are broadly categorized into different categories.

Spatial Domain Technique: Spatial steganography directly Modifies some bits of a pixel value in an image to hide the data. The most commonly used method in this

category is the least significant bit. Spatial domain methods are categorized as follows [129]:

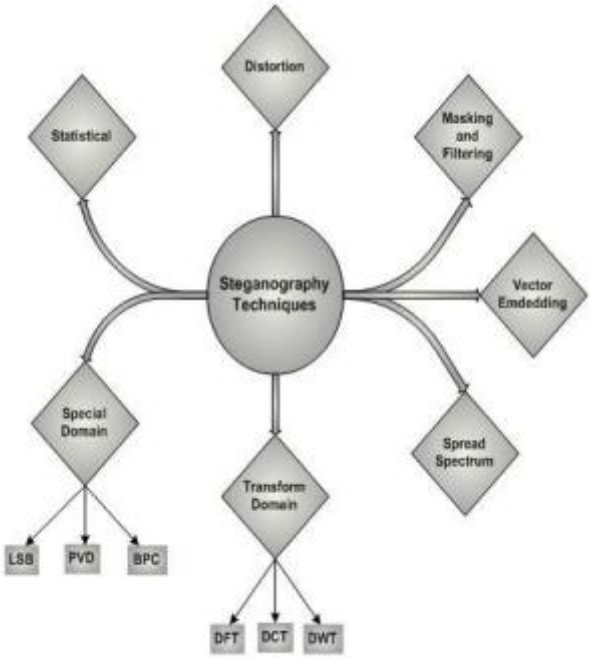


Figure 2.10 Steganography Technique[129]

a1. Least significant bit insertion (LSB): This technique takes a simple approach to embedding by replacing the least significant bit of the cover image pixel with a bit of secret data. Changing the LSB of the image pixel does not make a big difference in the image, so the image obtained after embedding is almost the same as the original image.

a2. Binary Pattern Complexity (BPC): This segmentation of the image measures its complexity. Complexity is used to determine the noisy block. This method replaces the noisy blocks in the bitplan with a binary pattern mapped from the secret data.

a3. Pixel Value Differencing (PVD): This technique selects two consecutive pixels to embed data. The payload is determined by examining the difference between two

consecutive pixels and is used as the basis for determining whether the two pixels belong to a border area or a smooth area[130].

B. Transformation domain-based techniques: These techniques try to encode the message bits with the transformation domain factor of the image. Data embedding performed in the transformation domain is often used for robust watermarking. Domain conversion techniques fall into various categories, including:

b1. **Discrete Fourier Transform (DFT)**: In this technique, the Discrete Fourier Transform is purely a discrete transform. A discrete-time signal is converted to a discrete frequency. These techniques convert a finite list of evenly spaced samples of a function into a list. Of the coefficients of a finite combination of complex sine waves ordered by their frequencies. It can be said that the sampled function is often converted from the time or line position of the original domain to the frequency domain[130].

b2. **Discrete Cosine Transform (DCT)**: This technique is similar to the Discrete Fourier Transform. The DCT converts a signal or image from a spatial domain to a frequency domain. Mathematical transformation transforms a pixel so that the position of the pixel value "spreads" into a portion of the image.

b3. **Discrete Wavelet Transform (DWT)**: This technique transforms an image from the spatial domain to the frequency domain. During the course of steganography, DWT identifies the high and low frequency information for each pixel in the image. This is a mathematical tool for hierarchically decomposing images. It is mainly used to process transient signals[130].

C. **Vector Embedding**: A vector embedding method that uses a robust algorithm with standard codecs (MPEG 1 and MPEG 2). This method embeds

the audio information in the pixels of the host video frame. It is based on the H.264 / AVC video coding standard. The algorithm designed the motion vector component function to control the embedding and as a secret bearer. The embedded information does not significantly affect the visual and statistical invisibility of the video sequence. This algorithm has high carrier utilization, high embedded capacity, and can be implemented quickly and effectively [130].

D. **Spread Spectrum**: This technique uses secret data that spreads over a wide frequency bandwidth. The signal-to-noise ratio for each frequency band should be small enough to make it difficult to detect the presence of data. Even if some of the data is deleted from multiple tapes, the other tapes have enough information to recover the data. Therefore, it is difficult to completely delete the data without completely destroying the cover. This is a very robust approach used in military communications [130].

E. **Statistical technique:** This technique embeds a message by manipulating some properties on the cover page. This involves splitting the coverage into blocks and then embedding message bits in each block. The cover block changes only if the message bit size is 1, otherwise it does not need to be changed [130].

F. **Distortion Technique**: This technique stores confidential data by distorting the signal. The encoder applies a series of changes to the cover image, and the decoding phase decodes the encrypted data using the private key into the original data along with the secret data [130].

G. **Masking and Filtering**: This technique highlights the image and hides the data. This approach is useful when the watermark becomes part of the image. The data is embedded in more important parts of the image rather than hidden in the noisy parts.

Watermark technology is further integrated into the image and can be applied without fear of destroying the image. This technique is used for 24-bit and grayscale images [130].

2.12 Review of Empirical Studies

Health information can be used for a variety of purposes, Clinical practice, decision making, operations, and workflow. The challenges of using the eHealth element to support superior healthcare meet the user interface, connectivity, authentication, patient data security, and user demands for healthcare services (patients and healthcare professionals). An effective dialogue with healthcare professionals. [131] explored various security Models in healthcare applications and sought to find ways to protect against information breaches. They evaluated various security requirements to ensure data protection and e-health security. They used an enhanced RBAC (Role Based Access Control) security Model to find solutions to the security challenges identified in the area of e-health. They are proposing a healthcare services integration platform that implements an extensible RBAC Model. This architecture is designed to provide four key functions: health information sharing, dietary recommendations, health information processing, and health information management on each smart device[132]. However, keep in mind that security issues have not yet been properly addressed. This Model is not suitable for distributed environments. Therefore, the proposed solution has limited use. The application also does not consider increasing the number of users.

A Secure Health architecture based on Secure Transport Layer / Secure Sockets Layer (TLS / SSL) using a lightweight framework to protect data exchanges with servers without the need for an additional layer of security shown was presented in this study[133]. Secure Health includes many security features such as authorization to

provide security services for data in transit and at rest. It has the advantage of preventing unauthorized persons from accessing the system containing medical information. In addition, it provides administrators with the possibility to detect language abuse based on the information provided[134]. Despite the advantages of this framework, the main challenge is that it is platform-dependent and inextensible. In a cloud-based environment, security policies and frameworks need to take into account future scalability and scalability. The watermarking approach used can mitigate internal threats to e-health systems[135]. A patient-centric eHealth system Model was examined here, an EHR system that is personally controlled using blockchain technology. You can use the blockchain to verify ownership of patient data, grant permissions, and ensure data integrity[136]. In this study, a protocol called pseudonym-based encryption and various agencies (PBEDA) was proposed along with the multi-layer blockchain technology for e-health systems to meet the standards of distribution architecture[137]. Blockchain technology was used to consolidate each outsourced EHR operation into a single transaction, protecting the outsourced EHR from unauthorized changes[138]. An approach that uses blockchain and peer-peer interplanetary file system (IPFS) storage which provides an efficient access control scheme for secure and decentralized data storage and sharing was proposed here to secure the ehealth information system (EHIS)[139]. A framework was proposed here which consists of the entities, to generate and manage the ehealth information are; patients (1P): the healthcare receivers, provider (2P): the health service providers, payer (3P): the insurance companies, national database (ND): cloud used to store data and certificate authority (CrA): a thirdparty who certifies the 3P`s legitimacy in the EHIS framework[140]. A dynamic access control mechanism was implemented with the ehealth cloud known as risk aware task-based control which ensures that the access is

granted based on the AIC (Availability, Integrity, Confidentiality) principle[141]. The author here proposed an approach which provides client platform security using trusted virtual domains (TVD)[142]. The author here used a secret sharing scheme to maintain privacy and high security in the ehealth cloud[143]. A safe and simple framework was proposed the framework divides e-health data into several segments, each of which is encrypted with a private key method and then sorted and stored. The order of the data and the decryption process are known to the user. This approach is suitable for all types of security measures, while the framework manages confidentiality and data security[144].

A brand new framework for digital nation was proposed at the Attribute-Based Encryption (ABE) encryption technique[145]. In this case, the consumer is split into primary domains: the personal area and the general public area. The secret is to control the complexity of key management[146]. In the personal area, every proprietor is handiest allowed to encrypt/get entry to statistics beneath his or her properties, even as the general public area lets in customers to use and use multi-authority EBAs to bolster their countermeasures. deputy security[146]. The predominant assignment with this method is scalability and flexibility, due to the fact integrating attribute-primarily based totally encryption right into a large-scale digital fitness document device poses a assignment. Serious and large key management. a hundred and ten proposed a steady and dependable framework the use of re-encryption and attribute-primarily based totally encryption (ABE) with proxy encryption enabled with the aid of using Rivest Shamir and Adleman (RSA). The motive of the use of proxies is to introduce a separation mechanism to make certain the validity of affected person statistics. In this case, handiest professionals get hold of write privileged locks even as examine privileged locks are given to patient[147]. The essence of that is to save you whole

delegation of the affected person. Thanks to this framework, the computational value has been significantly reduced. With this method, the clinical expert can without difficulty be avoided from acquiring the analyzing keys with out approval from each ends. However, the device nevertheless has room for a confined range of customers. Another safety version has been proposed with the aid of using [147]. A safety framework primarily based totally at the Advanced Encryption Standard (AES) set of rules became advanced to encrypt affected person facts consistent with the privateness policy[148]. The safety version lets in customers to preserve facts reliably and securely in a cloud-primarily based totally environment. The three-Model framework guarantees a excessive degree of safety and secrecy. The drawback of this framework is that it can not paintings with all sorts of working systems. It relies upon at the working device. It is likewise very complex to put into effect in a actual scenario. [149] has blended role-primarily based totally get entry to manipulate (RBAC) with a hierarchical identity-primarily based totally encryption scheme (HIBE) to offer encryption to steady affected person statistics earlier than it's miles outsourced. statistics storage[150]. RBAC facilitates to facilitate consumer privileges. The primary weak spot of this framework is that it does now no longer offer correct and dependable get entry to manipulate requirements. Patients can not get entry to the privileges in their personal facts with out following HIPAA regulations. From an entity perspective, a trust-primarily based totally evaluation safety version for e-fitness services[151, 152]. The version incorporates an in depth structure this is relevant to specific entities and serves as a unmarried reliability evaluation metric that may be used to assess a selected belongings of the safety device. secret. The effects acquired from the simulation display that the framework plays higher in phrases of calculating reliability than the diverse present reliability fashions for eHealth solutions. However,

this version is pretty heavy, it incorporates some of mathematical variables whose values have now no longer been sincerely evaluated.

We evaluated various security requirements related to data protection for e-health services. They proposed an improved role-based access control Model to design the Healthcare Services Integrated Platform (uHCSIP)[153]. However, this Model performs four key functions that are not available in a collaborative environment. As a result, privileged users cannot specify who has access to their medical data[154]. Models cannot be deployed in a cloud-based environment. The organization's new privacy and security Model is a major focus and the interaction of roles between native applications and eHealth services[155]. The framework is Modeled as a multi-agent system. Roles in the Model define access rights and initiate various requests to dynamically interact with agents that meet security requirements. To confirm the validity of the Model, we evaluated the performance using a simple case of an electronic medical system. The main drawback of this Model is the inability to summarize sensitive information. The need for data protection in eHealth systems is highlighted in this study[156]. They design and implement using the Single Point of Contact (SPoC), which guarantees request-based approvals and facilitates the integration and delivery of reliable eHealth services hosted in cloud-based domains.[157] . The results of the Model are very reliable, this application works only with a limited number of users. For so many users, flexibility and dynamics are not enough. Works are ongoing on an access control security Model that uses its own Hierarchical Similarity Analyzer (HSA). This Model evaluates the security level (SL) and assigns it to users who share data between different administrative domains. SL ensures that approved and approved percentages of data are shared with each agreed collaboration with different policies. This security Model allows for different

combinations of policies, recognizes potential policy inequality, and culminates in a set of rules defined for attribute conflicts. This Model was implemented using the XACML guidelines and compared to other similar security Models. One of the main challenges of this framework is the inability to integrate different types of political conflicts, such as time, semantic and syntactic constraints. In addition, federal agencies do not have an absolute guarantee of security and secrecy[159]. A new access control framework was developed to address the security and privacy challenges of Electronic Health Records (EHR). The framework includes hybrid cloud and access control policy migrations to ensure robust access control and data sharing that maintains approval between different healthcare providers. To make the Model more efficient, access control policy transformations have introduced multiple cryptographic building blocks targeting different EHR users with different privileges and access rights in different locations. Various cloud environments. The main limitation of this framework is that there is no room for user extension. Due to the limited number of users, there is no room for scalability[160].

In an attempt to locate answers to protection problems in EHR, there is an advanced granular get right of entry to manage for famous e-fitness applications. The framework complements the present conventional RBAC protection version for 2 purposes. It collects facts to distribute get right of entry to rules to one-of-a-kind sensor nodes and additionally shops very crucial statistics which include fitness, time and area statistics that is crucial for selection making. protection definition. The Modular nature of the framework makes it smooth and handy to set up rules throughout one-of-a-kind sensor networks. One of the principle demanding situations of the version is the dearth of an emergency and unlawful get right of entry to detection mechanism. one hundred thirty tries were made to offer a light-weight

protection version for eHealth[161]. To gain this, they take a look at one-of-a-kind units of protection protocols which include MiniSec, that is primarily based totally on RC4 in addition to one-of-a-kind encryption algorithms which include RC4 and Advanced Encryption Standard (AES). The researchers implemented cryptographic algorithms to a aggregate attack[162]. At the cease of the take a look at, they showed that the Skipjack and RC4 encryption algorithms are very powerful and dependable in making sure the confidentiality and integrity of digital fitness get right of entry to. However, the authors did now no longer look at powerful processes to the last protection requirements. Invariably, the conclusions drawn approximately the various algorithms studied can not aid the belief that they may be the high-satisfactory and maximum green. Since it's been set up that the conventional public key infrastructure (PKI) for enforcing cryptographic mechanisms is bulky and time consuming. There are defined numerous cryptographic strategies concerned to make certain fitness machine protection and digital privacy[162]. They analyzed the overall performance of those strategies, such as identity-primarily based totally encryption (IBE) and more recent identity-primarily based totally proxy re-encryption (IBPRE) schemes [163]. From the review, one located that the newly advanced IBPRE is higher and greater green for re-encryption, that can then be used to guard fitness statistics within side the cloud. The drawback of this approach is that the authors can not affirm the overall performance of different encryption strategies and consequently must now no longer be difficult at the effectiveness of the brand new IBPRE. In an attempt to steady scientific facts and different touchy scientific statistics, this was executed through combining scientific facts right into a unmarried document the use of facts hiding to cover the facts[164].

In their work, they proposed new processes to photograph hiding strategies that rely upon fuzzy good judgment and similarity. The motive is to permit choice of the

maximum huge bits (LSBs) out of series of the photograph pixels. They used comparable values of grey degrees produced withinside the message protecting pixels[165]. With this approach, messages are covered towards all kinds of assaults the use of symmetric encryption algorithms and lossless compression. The overall performance of cryptographic photograph nice and assessment is measured with the aid of root imply rectangular error (MSE), most signal-to-noise ratio (PSNR), structural similarity measure (SSIM), typical nice index (UQI) and correlation coefficient (CC). Based on the results obtained, the proposed new approach ensures the confidentiality and confidentiality of patient information while expanding the data warehouse[166]. The disadvantage of this approach is that it cannot handle and resolve noise reduction and data reduction. This can improve integration. Recognizing the vulnerability of cryptographic approaches to the security of health records. A technical review was conducted on several other security Models used to protect and protect electronic health information. In the end, they came up with two main approaches to ensuring security and privacy. This approach is a private approach and a safe approach on the one hand and a disaster recovery plan on the other. The old approach is a powerful mechanism for ensuring the confidentiality and integrity of medical information, but the following approach can only be used for trusted and trusted authentication mechanisms, release of electronic medical information[167]. The downside is the powerlessness of an effective mechanism if one of the approaches fails. The Model does not have enough interaction to store and run in a cloud environment. A rigorous investigation was carried out on role-based access control (RBAC) and found that there was no reason to request access to sensitive data. To address this weakness, they have developed a framework with a scenario-based access control Model (SitBAC). SitBAC is considered a conceptual framework that defines

situations in which a patient's access to electronic information is denied or granted. SitBAC uses a scenario schema consisting of Patient, Electronic Health Record (EHR), DataRequestor, and their relationships and attribute entities. This Model is considered common and can be used and adapted in areas other than medical information. One of the main weaknesses of this Model is the inability to take into account all possible stakeholders with different goals. In addition, the Model does not contain a formal representation of SitBAC as a knowledge base[168]. The security features of the Standard Communication Protocol (SCPECG) for calculating electrocardiograms to enable secure file storage was changed, a new approach to security allows users to properly access (permit or deny) SCPECG files for a variety of purposes, from education and clinical research to study interpretation and consultation[169]. The permissions supported by the cryptographic elements are decentralized and well implemented by the role-based configuration[170]. This app has proven to be extremely effective in authorizing and authenticating users and protecting the privacy of sensitive electronic health information[171]. Despite the effectiveness of the framework, it is difficult to use the Model in a distributed environment because the application cannot be deployed in a cloud-based environment. Modeling is technical and difficult to implement. There is no actual implementation that justifies its effectiveness and capabilities. Anonymity was seen as a way to protect eHealth information, they felt that using social security numbers was not enough for anonymity, as there was a tendency to reveal important patient information, in this context, they proposed Statistical Disclosure Control (SDC) approaches to protect and hide highly confidential properties while preserving the features and utility of the data. reasonably anonymous. These approaches focus only on numerical data that are continuously proportional to common nonnumerical

attributes whose application to EHR is less than optimal results[172]. The framework proposed here provides accurate and reliable results from SDC approaches to non-numerical clinical data, with particular attention to semantic preservation[174]. To achieve their goals, they used a structural knowledge base like SNOMEDCT. However, this framework can only be applied to non-numeric attributes. This framework also doesn't work for large datasets. The framework also causes significant delays during the anonymization process. Several anonymization approaches have been proposed by researchers. These approaches are primarily focused on applying existing security Models to the data and are therefore characterized by significant delays in the anonymization process. obtained from the data stream. On this note an anonymous feature has been developed without delay to preserve and ensure the confidentiality of medical information. This approach does not create any latency because the data streams are immediately anonymized with false [175]. In addition, late validation is also recommended to improve the usefulness of anonymous result data and also manage false positives. However, this method did not take into account statistical analysis and old data were taken into account to obtain the values, so it could not obtain more reliable anonymous results[176]. We also didn't consider when the confirmation would be delayed, so the results we got are unreliable. An efficient and secure security framework known as Patient Centered Access Control (ESPAC) was proposed that allows information requester on the eHealth platform to have role-based access[177]. Assigned roles and their respective attributes. ESPAC moves data to a central repository, reducing the overall maintenance cost of moving data from one repository to another[178]. Through this framework, you can access electronic health information anytime, anywhere. The system also ensures that user privacy and data integrity are taken into consideration. The weakness of this scheme was that it did not

take into account other forms of role-based access control (RBAC). It is intended to be a basic RBAC for addressing security and privacy concerns. It was commented that the confidentiality and security of medical information is important, to achieve this, they invert the encrypted and watermarked images so that the individual images processed with the watermarked and watermarked process are fully searchable due to their sensitive nature[179]. It was considered that of the information conveyed by medical images, they proposed a method for processing accessible encrypted and watermarked images for the security and privacy of medical images[180]. This system is used to protect and authenticate medical images. The framework is limited to images with text and audio data analysis. The need for electronic health information in a cloud-based environment to ensure interoperability and reduce operating costs was observed[181]. However, their main concern is how to ensure the security and confidentiality of the data stored in the cloud environment. To create a secure and reliable cloud environment where electronic medical records (EHRs) are stored, they have proposed a systematic access control framework that facilitates secure sharing. Complex and complex hybrid EHR choices from different healthcare providers in a cloud-based environment. However, this framework has not been tested with actual health datasets to truly confirm its relevance and reliability. In addition, the issue of configuring and processing the detailed approval mechanism for data sharing in cloud-based environments remains unresolved[182]. An attempt was made to eliminate e-health security-related situations using analysis of weaknesses detected using cryptography. This means that when access is given to fine-grained information, the computational load increases and information control problems occur. They solved these problems in a few steps. First, by implementing and defining access to regulations primarily based on information attributes. Second, authorization

information allows customers and owners to delegate most computing tasks, including Modularized information, to access unreliable cloud servers without disclosing the content of the data[183]. This process was performed using a combination of deferred re-encryption, proxy re-encryption, and attribute primary-based full encryption (ABE). However, this scheme has not proven to be completely scalable as it no longer provides environmentally friendly, reliable confidentiality and integrity of information. An access to develop protection and manage the structure was received to establish a trusted private domain name in fitness digital infrastructure resources[184]. The architectural Model provides a combination of customer and community protection, the framework has many open challenges[185]. There may be a problem with the data subject authenticating and obtaining the right to access the eHealth facts. This could be due to him not remembering the PIN to access the facts. When this happens, it can also raise issues of confidentiality of existence, anonymity of the buyer, and mission. Privacy and access rights to manage the structure of the HER was developed, this is especially annoying, but it allows you to encrypt patient information. The platform allows affected people to allow and grant access to scientific data from distances of several kilometers via mobile devices. Access rights are time independent and are no longer associated with a particular location. This framework is entirely based on today's cryptographic protection approach. The main drawback of this scheme is the time required to give up the key and then switch to an alternative for each encryption and decryption[186]. The complexity of key manipulate is a intense assignment of this approach. Adoption of diploma-key get proper of access to manipulate and zero-expertise protocol have become considered for e-Health machine[187]. In order to obtain a regular connection amongst several entities DUKPT and a -diploma aggregate of key encryption have become adopted. The framework

have become analyzed with apprehend to resistance to now no longer unusual place attacks and data confidentiality. The proposed scheme tolerates an extremely good extensive form of simultaneous authorization requests with splendid response time. The principal downside with this scheme is that it has restrained extensive form of entities: clients U, a cloud server CS, a issuer organization SP, and an authentication and get proper of access to manipulate manager AAM. This manner that it isn't continually scalable; this is not suitable for a cloud-based definitely environment because it will now not deliver room for collaborative sharing of resources. Another framework for controlling get entry to to non-public fitness records (PHRs) in a dispensed surroundings turned into proposed via way of means [188]. They took gain of the Attribute-Based Encryption (ABE) protection version to encrypt affected person facts to obtain and obtain scalable get entry to manipulate and granular get entry to for PHR. The machine has been divided into numerous protection domain names to lessen the complexity which can stand up from key distribution. In this case, every area best handles a small percent of customers. Users have absolute manipulate over their privacy. This scheme is dynamic in nature because it helps doing away with consumer get entry to privileges on demand. However, this system does now no longer aid greater specific owner-described get entry to manipulate policies. The new An affected person-focused plan with a great framework was proposed for controlling entry to digital fitness document facts. They diagnosed scalability and fine-tuned accessibility as a part of the challenges. So they optimized and leveraged Attribute-Based Encryption (ABE) fashions to stable and encrypt affected person PHR facts. They consciousness on conditions in which there are a couple of facts proprietors in addition to in which customers are divided into one-of-a-kind protection domain names. This is achieved to lessen the complexity of key control for proprietors and

customers. With multi-authority EBA operation, there may be higher overall performance in phrases of patience, secrecy and protection. Schema permits bendy amendment of diverse record attributes. Regardless of the authors' claims, the proposed framework has best been simulated and has now no longer been examined on actual instances to set up claims. The outcomes received can not assure the effectiveness of the framework whilst it's far examined in a actual situation. In addition, a few customers have additionally been taken into account. The authors did now no longer announce what should take place whilst an boom within side the variety of entities[190]. Fintech is frequently taken into consideration a completely unique innovation exceeded via way of means of one-of-a-kind monetary establishments across the world. This era development withinside the monetary region includes loads of improvements along with provider transport and facts protection. To create absolute cognizance and necessities of Fintech technologies, in particular for specialists and universities, a entire FinTech survey via way of means of reviewing and amassing latest traits and development The diploma is recorded. In their work; Relevant and widely recognized are the five areas of technology considered Saintosanct: data technology, applications and management, service Models, equipment and muscle infrastructure, and safety and security. It is grouped. They have completed research to develop an excellent dynamic solution for Fintech labeling "Data driven Framework (DF2)" to ensure that Fintech [190] delivers the FinTech process. With the current expansion in the development of network solutions, there are various challenges that are currently hindering the efficient and wonderful use of this amazing innovation. Security and data protection are seen as major challenges[167]. Basically, the encryption process has a problem handling data that doesn't really apply to the ciphertext. Recognizing this great challenge, [191] proposed a technique for

mixing arithmetic operations and processes on a fully homomorphic sensor-based cipher (FHE) emphasizing the computation of encrypted real numbers. . The main technique of their work is to use DaC to augment a math operation based on a polynomial and divide it into binomials. Their findings show that the efficiency and reliability of the encryption and decryption techniques can obtain good results from decoding encoding results[192]. Due to the ubiquitous nature of mobile devices mobile devices, especially iOS and Android devices as well as other Internet-based devices (connected) devices, needs and urgency to ensure and ensure the complete and effective security of data data at rest and data in transit without incurring performance costs is critical. After identifying security and privacy as one of the key challenges in maximizing the significant benefits of using these devices effectively, a proposal on security and privacy Models will be configured. Architecture and design to enhance security in general through dynamic programming. A problem has been detected. NPhard attempts to use the full protection weight value defined and described by the security classifier[193]. A final demonstration on the effectiveness of this Model by demonstrating its usefulness using a prototype Android app . The rapid development of Internet-based methods and techniques has certainly facilitated the spread of network-based applications. Successful connectivity environments have been found to bring a combination of technologies and strategies, such as the Internet of Things (IoT) and cloud computing. From existing literature, security and privacy issues are the biggest challenge of data transmission related to inadequate privacy and protected communication protocols[194]. To find a permanent solution to this challenge, [195] proposed a solution that primarily focused on a single strategy for achieving secure transmission through the introduction of multi-channel communication. They

evaluated the performance of the proposed method through implementation and testing and confirmed that it could provide an effective and reliable level of security.

It is apparent that the high-quality and useful consequences and programs of scientific selection guide structures can not be overstated with the software of records mining techniques. In addition to decreasing session and prognosis hours, it may additionally assist enhance diagnostic accuracy and precision. Naïve Bayes has been used for a while to find out beneficial statistics to enhance scientific and scientific guide structures. Given a number of the cumulative blessings of this innovation, its large adoption and use has been hampered and prone because of safety and privateness concerns. Recognizing this extensive challenge, a hundred seventy five has evolved a safe, affected person-targeted scientific selection answer that facilitates physicians correctly and rather reliably diagnose affected person risks. In their paintings, the sufferers` legacy statistics are conserved withinside the cloud which may be used to educate the algorithm (Naïve Bayes classifier) with out revealing any essential statistics approximately affected person. To sooner or later acquire their objective, they designed an additive homomorphic proxy aggregation scheme that's a brand new cryptographic tool. Not handiest that, they delivered a privacy preserving top sickness names retrieval protocol to leverage the outflow of the Bayesian classifier. The method does, however, now no longer think about a few different records mining techniques[196]. Because of diverse advances in Information and Communication Technologies (ICT), it's been located that scientific selection guide structures is gaining floor and turning into rather impactful within side the international fitness sector. Despite the massive and identified blessings of this top notch innovation, sufferers end up very prone because of the shortage of good enough safety and privateness measures to make certain statistics safety. Against this backdrop, it was

proposed that a brand new shielding scientific selection guide initiative referred to as Peneus. This framework may be carried out to reveal fitness reputation in addition to expect sickness. To enhance this framework, they took it a step in addition with the aid of using designing a method for computing a not unusualplace integer over ciphertext withinside the SIMD (Single Instruction, Multiple Data) style[197]. The paintings grew to become out to be very efficient, even though that didn`t consist of constructing dependable bootstrap techniques in addition to a platform helping the high-extent plaintext domain[198]. a hundred and eighty proposes an digital fitness machine primarily based totally on a community of semantic sensors, the reason of this machine is to put into effect a machine associated with sensors, mobile-primarily based totally programs and marriage to offer fitness care services. In the study, tool interoperability and records normalization become taken into consideration a tough task, an digital scientific machine with semantic sensor community become evolved (prototype) to remedy those problems. tool interoperability issues. In the proposed machine, IETF YANG is used to version eHealth semantic records to symbolize eHealth sensor statistics.

The several characteristics of information hiding discussed has been suggested in Steganography as the art of passing information in a manner that the very existence of the message is unknown. The goal of steganography is to avoid drawing suspicion to the transmission of a hidden message[199]. The recent growth in computational power and technology has propelled it to the forefront of today`s security techniques of contemporary steganography techniques for image in spatial and transform domains and steganalysis techniques for the detection of secret message in the image, authors explore the steganography, its history, features, tools and various techniques like LSB, masking, filtering and other transformations used for hiding messages in an image.

The paper also describes various methods to hide the secret or confidential message in an original file so that it is unintelligible to an interceptor[200] , addressed the concept of embedding the secret message into an image using LSB technique and then applied AES algorithm to provide better security. A reverse procedure was proposed which described in paper by using an alteration component method[201]. As addressed user enters username, password and a key. A key is taken from automatic key generator device which generates a unique key after some specific time. After this the secret message and key is encrypted and encrypted message is embedded into cover image and stego image is produced[202]. In a study, the secret message is first compressed then the message is hashed and encrypted using encryption key. This method results in robust Model and achieves two important principles of security i.e. privacy and authenticity[203]. An overview used to hide secret messages or images in space and transform domains was presented in [204]. A method was introduced in which the secret message was first compressed using the wavelet transform technique and then embedded in the cover image using the LSB. Bits of the secret message are inserted into the image using a random number generator[205]. The basic terms of cryptography and steganography was introduced in this study, ensuring that the combination of both provides multiple layers of security and meets requirements such as capacity, security, and robustness[206]. In another study, the study introduced a method based on image ranking. First, the secret data is encrypted using the RSA encryption algorithm, and then the user selects the appropriate image to hide the specific data. This makes it more difficult for an attacker to successfully launch an attack[207]. In [208], this article demonstrates that these techniques can be used to make data more secure and robust. [209] Introduced a method of embedding a secret image in a cover image using LSB technology, encrypting it using the DES algorithm, and using a key image. In [2\10], the

author first uses LSB technology to embed confidential data in the cover image and then applies DES encryption to encrypt the data this improves security. The author in this literature first encrypts the data using the RC4 encryption algorithm and then embeds it in the BMP cover image using three different steganography techniques[211]. At [212], secret images are embedded in 24-bit or 8-bit images using LSBs, and the results are evaluated for 2, 4, and 6 LSBs in .png and .bmp files. In [213], the author encrypts the secret image, uses the key to convert it to an encrypted image, converts this encrypted image to intermediate text, embeds it in the cover image, and finally converts it again, metamorphic encryption. I proposed a new method called. The image will be converted. In the [214] article, basic steganography terminology, steganography techniques, classifications, and reviews of previous studies by researchers were proposed. The [215] publication discussed how to hide information on billboards. This method can be used to announce a secret message in a public place. In paper [216], the user selects a secret image in BMP format and encrypts it using the BLOWFISH encryption algorithm. This is because BLOWFISH is faster, more powerful and has better performance than DES, 3DES, AES, RC6 and RC4. Approach to hide images [217], i. H. The Hide Behind Corners (HBC) algorithm is used to place keys in the corners of an image. All corner keys are encrypted by generating a pseudo-random number. Then the hidden image will be sent. The recipient needs to know all the keys used in the corners when encrypting the image. Reverse data hiding (RDH) is used to keep the original image, when the original image is unlocked in all corners with the correct private key used to hide the image will be generated. In [218], the user enters the username and password to log in to the system. After a successful login, the user can use the key to embed a secret message in the image and create a Stay Gold image. The same key is used on the receiving side to retrieve the hidden

data. Here, the secret message is first transferred to the text file. The text file is then compressed into a ZIP file and converted to binary code using the ZIP text file. Text file compression is more secure and difficult to detect. In [219], the author presents a new technique for information hiding based on Huffman coding. Grayscale images of sizes m * n and p * q are used as cover and secret images, respectively. Huffman coding is performed on the secret image, and each bit of the Huffman code in the secret image or message is embedded in the cover image using the LSB. In the paper [220], confidential data is encrypted using the RSA encryption algorithm, and the user selects an image suitable for hiding specific data, and this confidential data uses LSB. Similar to embedding in a cover image. Finally, a Stay Gold image was created, the article shows how to encrypt and decrypt a secret file embedded in an image file using a random LSB insertion method in which the bits of the secret message are randomly distributed to the image bits. These random numbers are generated using the key[221].

Endnote

[1]P. Mell & T. Grance. *The NIST Definition of Cloud Computing*. **NIST Special Publication** 2011, 800-145.

[2]N. Khan & A. Al-Yasiri. *Identifying Cloud Security Threats to Strengthen Cloud Computing Adoption Framework*, **The 2nd International Workshop on Internet of Thing: Networking Applications and Technologies** IoTNAT' 2016.

[3]S. A. DeChaves, C. B. Westphall, C. M. Westphall, G. A. Gerônimo. *Customer Security Concerns in Cloud Computing*. **IARIA.** 2011, 978-1-61208-113-7.

[4]M. F. Umer, M. Sher, I. Khan. *Towards Multi-Stage Intrusion Detection using IP Flow Records*. **(IJACSA) International Journal of Advanced Computer Science and Applications.**, Vol. 7, No. 10, 2016.

[5]*cloud computing roadmap.* https:// www.summitbiz.net. (Available Online)

[6]Vmare: *Your Cloud in health care* http//Vmare.com/files/pdf/vmare-your-cloudin-healthcare-industry-brief.pdf (Available Online).

[7]Sullivan, T. "The ways cloud computing will disrupt IT, 2009. " http://www. cio.com.au/article/296892/nick_carr_ways_cloud_computing_will_disrupt_it.

[8]A.M Chandrashekhar, Shashikumar. *Cloud Computing Service And Deployment Models.* **International journal for research in applied science and engineering technology**, 2017**,** Vol 5, Issue VI.

[9]CommVault.: *Your Top 5 Cloud Data Protection Challenges.Solved*. commvault.com/cloud. (Available Online)

[10]F. Yahya, V. Chang, J. Walters, and B. Wills, *"Security Challenges in Cloud Storage*, 2014, pp. 1–6.

[11]R. Masa'deh, R. Shannak, M. Maqablach & A. Tarhini. "*The Impact Of Knowledge Management On Job Performance In Higher Education: The case of the university of jordan*. **Journal of enterprise information management**, 29(6), 2016, 120-137.

[12]*Cloud Computing: Clear Benefits: The Emerging Role of Cloud Computing in Healthcare Information Systems.* Available online: http://www.techrepublic.com/whitepapers/cloud-computing-clear-benefits-the-emerging-role-of-cloud-computing-in-healthcare-information-systems/2384337

[13]X. Wang, J. Ma, F. Xhafa, M. Zhang, X. Luo. *Cost-Effective Secure E-Health Cloudsystem Using Identity Based Cryptographic Techniques*. **Future Gener ComputSyst**;67,2017, 242–54.

[14]Q. Kester, L. Nana, A. Pascu, S. Gire, J. Eghan, N. Quaynor. *A Security Technique For Authentication And Security Of Medical Images In Health Information Systems.* **15th International Conference on Computational Science and Its Applications, Banff, AB, Canada**, 2015, pp. 8–13.

[15]N. Kahani, K. Elgazzar, K. Cordy. *Authentication And Access Control In E-Health Systems In The Cloud.* **In: IEEE International Conference on High Performance and Smart Computing (HPSC), Big Data Security on Cloud (BigDataSecurity), New York, NY, USA,** 2016, pp. 13–23.

[16]A. Omotosho, O. Adegbola, O. Mikail & J. Emuoyibofarhe. *A Secure Electronic Prescription System Using Steganography With Encryption Key Implementation*. **arXiv preprint arXiv**, 2015, 1502.01264.

[17]A. Omotosho & J. Emuoyibofarhe. *A Criticism Of The Current Security, Privacy And Accountability Issues In Electronic Health Records*. **arXiv preprint arXiv**, 2015, 1501.07865.

[18]M. A. Kamoona, M. A & A. M. Altamimi. *Cloud E-Health Systems: A Survay On Security Challenges And Solutions*. **In proceedings of 2018 8th International Conference on Computer Science and Information Technology (CSIT), (IEEE)**, 2018 :pp. 189-194.

[19]S. N. Dhanabagyam & G. R. Karpagam. *Secure Communications For E-Health In Mobile Cloud Computing Using Provable Security*. **International Journal of Pure and Applied Mathematics**, 2017, 114(7): 325-335.

[20]X. A Wang, J. Ma, F. Xhafa, M. Zhang & X. Luo. *Cost-Effective Secure E-Health Cloud System Using Identity Based Cryptographic Techniques.* **Future Generation Computer Systems**,, 2017, 67: 242-254.

[21]R. Charanya, S. Nithya & N. Manikandan. *Attribute Based Encryption For Secure Sharing Of E-Health Data*. **In Materials Science and Engineering Conference Series** 2017, 263(4): 042030.

[22]L. Selvam & R. J. Arokia.. *Secure Data Sharing Of Personal Health Records In Cloud Using Fine-Grained And Enhanced Attribute-Based Encryption*. **In proceedings of 2018 International Conference on Current Trends towards Converging Technologies** 2018, (ICCTCT) (IEEE), pp. 1-6.

[23]P. Chinnasamy & P. Deepalakshmi. *Design Of Secure Storage For Health-Care Cloud Using Hybrid Cryptography*. **In proceedings of 2018 Second International Conference on Inventive Communication and Computational Technologies**, 2018, (ICICCT) (IEEE), pp. 1717-1720.

[24]A. Omotosho, O. Adegbola, O. Mikail & J. Emuoyibofarhe. *A Secure Electronic Prescription System Using Steganography With Encryption Key Implementation*. **arXiv preprint arXiv**, 2015, 1502.01264.

[25]P.K. Maganti & P. M. Chouragade. *Secure Health Record Sharing For Mobile Healthcare In Privacy Preserving Cloud Environment*. **In proceedings of 2019 IEEE International Conference on Electrical, Computer and Communication Technologies**, 2019 (ICECCT) (IEEE), pp. 1-4.

[26]P. K. Maganti & P. M. Chouragade. *Secure Application For Sharing Health Records Using Identity And Attribute Based Cryptosystems In Cloud Environment*. **In proceedings of 2019 3rd International Conference on Trends in Electronics and Informatics**, 2019, (ICOEI)(IEEE), pp. 220-223.

[27]R. Manoj, A. Alsadoon,, P. Prasad, N. Costadopoulos, & S. Ali. *Hybrid Secure And Scalable Electronic Health Record Sharing In Hybrid Cloud*. **In proceedings of 2017 5th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering,** 2017,(MobileCloud) (IEEE), pp. 185- 190.

[28]M. A. Kamoona & A. M. Al*tamimi. Cloud E-Health Systems: A Survey On Security Challenges And Solutions*. **In proceedings of 2018 8th International Conference on Computer Science and Information Technology**, 2018, (CSIT), (IEEE) :pp. 189-194.

[29]C. H. Liu, T. L. Chen, H. Y. Lin, F. Q Lin, C. M. Liu, E. P. Wu & T. S. Chen. *Secure Phr Access Control Scheme In Cloud Computing*. **International Journal of Information and ElectronicsEngineering**, 2013, 3(3):329.

[30]M. Drozdowicz, M. Ganzha,& M. Paprzycki. *Semantically Enriched Data Access Policies In Ehealth*. **Journal of medical systems**, 2016, 40(11): 238.

[31]C. Xu, N. Wang, L. Zhu, K. Sharif & C. Zhang. *Achieving Searchable And Privacy-Preserving Data Sharing For Cloudassisted E-Healthcare System*. **IEEE Internet of Things Journal**, 2019, 6(5): 8345-8356.

[32]H. Han, M. Huang, Y. Zhang, & U. A. Bhatti. *An Architecture Of Secure Health Information Storage System Based On Blockchain Technology*. **In proceedings of International Conference on Cloud Computing and Security**, 2018, (Springer, Cham), pp. 578-588.

[33]S. Chenthara, K. Ahmed, H. Wang & F. Whittaker. *Security And Privacy Preserving Challenges Of E-Health Solutions In Cloud Computing*. **IEEE Access** ,2019, 7: 74361- 74382.

[34]S. Badr, I. Gomaa & E. Abd-Elrahman. *Multi-Tier Blockchain Framework For Iot-Ehrs Systems*. **Procedia Computer Science**,2018, 141: 159-166.

[35]S. Cao, G. Zhang, P. Liu, X. Zhang, & F. Neri. *Cloud-assisted Secure ehealth Systems For Tamper-proofing EHR Via Blockchain*. **Information Sciences**,2019, 485: 427- 440.

[36]D. C. Nguyen, P. N. Pathirana, M. Ding, & A. Seneviratne. *Blockchain For Secure Ehrs Sharing Of Mobile Cloud Based E-Health Systems*. **IEEE Access**,2019, 7: 66792-66806.

[37]D. H. Kim & J. Kwak. *The Framework of 3P-Based Secure eHealth Information System*. **In proceedings of 2018 International Conference on Platform Technology and Service (PlatCon) (IEEE)**, 2019, pp. 1-6.

[38]A. Sakr, E. Yaacoub, H. Noura, M. Al-Husseini, K. Abualsaud, T. Khattab, M. Guizani. *A secure Client-side Framework For Protecting The Privacy of Health Data Stored on The Cloud*. **In proceedings of 2018 IEEE Middle East and North Africa Communications Conference (MENACOMM) (IEEE)**, 2018, pp. 1-6.

[39]R. Tahir, H. Tahir, A. Sajjad, & K. McDonaldMaier. *A Secure Cloud Framework For Icmetric Based iot Health Devices*. **In Proceedings of the Second International Conference on Internet of thing**, 2017.

[40]N. A. Azeez, & C. Van der Vyver. *Security And Privacy Issues In E-Health Cloud-Based System: A Comprehensive Content Analysis*. **Egyptian Informatics Journal**,2019, 20(2): 97-108.

[41]D. Patra, S. Ray, J. Mukhopadhyay,B. Majumdar, &A. K. Majumdar. *Achieving E-Health Care In A Distributed Ehr System*. **In proceedings of 2009 11th International Conference on eHealth Networking, Applications and Services** , 2009 (IEEE), pp. 101-107.

[42]R. Zhang & L. Liu. *Security Models And Requirements For Healthcare Application Clouds*. **In proceedings of 2010 IEEE 3rd International Conference on cloud Computing (IEEE)**, 2010, pp. 268-275.

[43]H. Wang. *Anonymous Data Sharing Scheme In Public Cloud And Its Application In E-Health Record*. **IEEE Access**,2018, 6: 27818- 27826.

[44]K. Abouelmehdi, A. Beni-Hessane, H. Khaloufi. *Big Healthcare Data: Preserving Security And Privacy*. **Journal of Big Data**,2018. 5 (1), 1.

[45]A. Alrawais. *An Attribute-based Encryption Scheme to Secure Fog Communications*. **IEEE access**,2017, 5, 9131-9138.

[46]N. A. Azeez, Ayofe & C. V. der Vyver. *Security And Privacy Issues In E-Health Cloud-Based System: A Comprehensive Content Analysis*. E**gyptian Informatics Journa**l,2019, 20 (2), 97-108.

[47]R. S. Balapure & P. Khodke, P. *Privacy Preservation Of E-Health Care System In Cloud*, **Exchange**,2017, 4 (3).

[48]M. Chen. *Privacy Protection And Intrusion Avoidance For Cloudlet-Based Medical Data Sharing*. **IEEE transactions on Cloud computing**,2018, 113, 48-52.

[49]M. Elhoseny. *Secure Medical Data Transmission Model For Iot-Based Healthcare Systems.* **Ieee Access**,2018, 6, 20596-20608.

[50]S. Sharma, K. Chen, A. Sheth. *Toward Practical Privacy Preserving Analytics For Iot And Cloud-Based Healthcare Systems*. **IEEE Internet Computing**,2018, 22 (2), 42-51.

[51]Wencheng S. *Security And Privacy In The Medical Internet Of Things: A Review*. **Security and Communication Networks**. 2018.

[52]D. Rachmawati, A. S. Jaysilen & M. A. Budiman. *Hybrid Cryptosystem Using A Tiny Encryption Algorithm And Luc Algorithm*. **Paper presented at the IOP Conference Series: Materials Science and Engineering**, 2018.

[53]K. R. Sajay, S. S. Babu & Y. Vijayalakshmi. *Enhancing The Security Of Cloud Data Using A Hybrid Encryption Algorithm*. **Journal of Ambient Intelligence and Humanized Computing** , 2019, 1–10.

[54]A. Vishwanath, R. Peruri & J. He. *Security In Fog Computing Through Encryption*. **DigitalCommons@ Kennesaw State University**, 2016.

[55]L. Yang, Z. Han, Z. Huang & J. Ma. *A Remotely Keyed File Encryption Scheme Under Mobile Cloud Computing*. **Journal of Network and Computer Applications***, 2018,* 106:90–99.

[56]L. Zou, M. Ni, Y. Huang, W. Shi & X. Li. *Hybrid Encryption Algorithm Based On Aes And Rsa In File Encryption*. **Paper presented at the International Conference on Frontier Computing**, 2020.

[57]X. Liu, G. Yang, Y. Mu & R. H. Deng. *Multi-User Verifiable Searchable Symmetric Encryption For Cloud Storage*. **IEEE Transactions on Dependable and Secure Computing** , 2020, 17 (6):1322–32.

[58]H. Mahmoud, A. Hegazy & M. H. Khafagy. *An Approach For Ample Data Security Based On Hadoop Distributed File System*. **Paper presented at the 2018 International Conference on Innovative Trends in Computer Engineering (ITCE)**, 2018.

[59]P. Dixit, A. K. Gupta, M. C. Trivedi, V. K. Yadav. *Traditional And Hybrid Encryption Techniques: A Survey.* **in Networking communication and data knowledge engineering, Springer**,2018, pp. 239-248.

[60]C. L. Chowdhary, P. V. Patel, K. J. Kathrotia, M. Attique, K. Perumal, M. F. Ijaz. *Analytical Study of Hybrid Techniques for Image Encryption And Decryption,* **Sensors**, 2020, vol. 20, no. 18, pp. 5162, doi: 10.3390/s20185162.

[61]S. Mishra & A. Dastidar. *Hybrid Image Encryption And Decryption using Cryptography And Watermarking Technique for High Security Applications*. **2018 International Conference on Current Trends towards Converging Technologies** (ICCTCT), 2018, pp. 1-5, doi: 10.1109/ICCTCT.2018.8551103.

[62]A. Abdullah, *Advanced Encryption StAndard (Aes) Algorithm To Encrypt And Decrypt Data*. **Cryptography and Network Security**, 2017, vol. 16, pp. 1-11.

[63]S. R. Zeebaree. *Des Encryption And Decryption Algorithm Implementation Based On Fpga.* **Indonesian Journal of Electrical Engineering and Computer Science,** 2020 vol. 18, no. 2, pp.774-781, doi: 10.11591/ijeecs.v18.i2.pp774-781.

[64]T. Hidayat & R. Mahardiko. *A Systematic Literature Review Method On Aes Algorithm For Data Sharing Encryption On Cloud Computing.* **International Journal of Artificial Intelligence Research**, 2020, vol. 4, no.1, pp. 49-57.

[65]P. Semwal & M. K. Sharma. *Comparative Study Of Different Cryptographic Algorithms For Data Security In Cloud Computing.* **2017 3rd International Conference**

on Advances in Computing, Communication & Automation (ICACCA) (Fall), 2017, pp. 1-7, doi: 10.1109/ICACCAF.2017.8344738.

[66]N. A. Al-gohany & S. Almotairi. *Comparative Study Of Database Security In Cloud Computing Using Aes And Des Encryption Algorithms.* **Journal of Information Security and Cybercrimes Research**, 2019 vol. 2, no. 1, pp. 102-109.

[67]M. B. Yassein, S. Aljawarneh, E. Qawasmeh, W. Mardini, &Y. Khamayseh. *Comprehensive Study Of Symmetric Key And Asymmetric Key Encryption Algorithms.* **2017 International Conference on Engineering and Technology (ICET)**, 2017, pp. 1-7, doi: 10.1109/ICEngTechnol.2017.8308215.

[68]P. Chinnasamy, S. Padmavathi, R. Swathy, & S. Rakesh. *Efficient Data Security Using Hybrid Cryptography on Cloud Computing.* **In Inventive Communication and Computational Technologies, Springer**,2021, pp. 537-547.

[69]S. K. Tallapally & B. Manjula. *Competent Multi-Level Encryption Methods For Implementing Cloud Security.* **InIOP Conference Series: Materials Science and Engineering**, 2020, vol. 981, no. 2, p. 022039.

[70]E. M. Alsaadi, S. M. Fayadh, & A. Alabaichi. *A Review On Security Challenges And Approaches In The Cloud Computing.* **InAIP Conference Proceedings**,2020, vol. 2290, no. 1, p. 040022.

[71]N. Mohammed &N. Ibrahim. *Implementation Of New Secure Encryption Technique For Cloud Computing.* **2019 International Conference on Computing and Information Science and Technology and Their Applications (ICCISTA)**, 2019, pp. 1-5, doi: 10.1109/ICCISTA.2019.8830668.

[72]S. Zhang, Z. Yang, J. Yang, Y. Huang. *Provably Secure Generative Linguistic Steganography*. **arXiv** 2021, arXiv:2106.02011.

[73]Z. L.Yang, S. Y. Zhang, Y. T. Hu, Y. F Huang. *Vae-Stega: Linguistic Steganography Based On Variational Auto-Encoder*. **IEEE Trans. Inf. Forensics Secur**. 2020, 16, 880–895.

[74]H. Kang, H. Wu, H, X.Zhang. *Generative Text Steganography Based On Lstm Network And Attention Mechanism With Keywords.* **Electron. Imaging** 2020, 2020, 291.

[75]X. L. Yang, X. Guo, Z. M. Chen,Y. F. Huang,Y. J. Zhang. *RNN-Stega: Linguistic Steganography Based On Recurrent Neural Networks*. **IEEE Trans. Inf. Forensics Secur**. 2018, 14, 1280–1295.

[76]S. Mahato, D. A Khan, D. K. Yadav. *A Modified Approach To Data Hiding in Microsoft Word Documents By Change-tracking Technique*. **J. King Saud Univ.-Comput. Inf. Sci**. 2020, 32, 216–224.

[77]R. Yang, Z. H. Ling. *Linguistic Steganography by Sampling-based Language Generation*. **In Proceedings of the 2019 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference** (APSIPA ASC), Lanzhou, China, 18–21 November 2019; pp. 1014–1019.

[78]A. A. Chaw. *Text Steganography In Letter Of Credit (Lc) Using Synonym Substitution Based Algorithm*. **Int. J. Adv. Res. Dev**.2019, 4, 59–63.

[79]A. A. Hamzah, S. Khattab, H. Bayomi. *A Linguistic Steganography Framework Using Arabic Calligraphy*. **J. King Saud Univ.-Comput.Inf. Sci**. 2021, 33, 865–877.

[80]A. Majumder, S. Changder. *A Generalized Model Of Text Steganography By Summary Generation Using Frequency Analysis*. **InProceedings of the 7th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)**, Noida, India, 29–31 August 2018; pp. 599–605.

[81]L. Xiang, L, W. Wu, X. Li, C. Yang. *A Linguistic Steganography Based On Word Indexing Compression And CAndidate Selection.Multimed*. **Tools Appl**. 2018, 77, 28969–28989.

[82]N. Naqvi, A. T. Abbasi, R. Hussain, M. A. Khan, B. Ahmad. *Multilayer Partially Homomorphic Encryption Text Steganography(Mlphe-Ts)*: *A Zero-Steganography Approach*. **Wirel. Pers. Commun**. 2018, 103, 1563–1585.

[83]Y. Liu, J. Wu, G. Xin. *Multi-Keywords Carrier-Free Text Steganography Based On Part Of Speech Tagging*. **In Proceedings of the 13th International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery (ICNC-FSKD), Guilin, China**, 29–31 July 2017; pp. 2102–2107.

[84]N. Wu, Z.Yang, Y. Yang, L. Li, P. Shang, W. Ma, Z. Liu. *Stbs-Stega: Coverless Text Steganography Based On State Transition-Binary Sequence*. **Int. J. Distrib. Sens. Netw.** 2020, 16.

[85]N. Alghamdi, L. Berriche. *Capacity Investigation Of Markov Chain-Based Statistical Text Steganography: Arabic Language Case.* I**n Proceedings of the 2019 Asia Pacific Information Technology Conference, Jeju Island, Korea**, 25–27 January 2019; pp. 37–43.

[86]N. Wu, P. Shang, J. Fan, Z. Yang, W. Ma, Z. Liu. *Coverless Text Steganography Based On Maximum Variable Bit Embedding Rules*. **J. Phys. Conf. Se**r. 2019, 1237, 022078.

[87]N. Wu, P. Shang, J. Fan, Z. Yang, W. Ma, Z. Liu. *Research On Coverless Text Steganography Based On Single Bit Rules*. **J. Physics Conf. Ser**. 2019, 1237.

[88]Z. Yang, S. Jin, Y. Huang, Y. Zhang, H. Li. *Automatically Generate Steganographic Text Based On Markov Model And Huffman Coding*. **arXiv** 2018, arXiv:1811.04720.

[89]H. Huanhuan, Z. Xin, Z. Weiming, Y. Nenghai. *Adaptive Text Steganography By Exploring Statistical And Linguistical Distortion*. **In Proceedings of the 2017 IEEE Second International Conference on Data Science in Cyberspace (DSC), Shenzhen, China**, 26–29 June 2017; pp. 145–150.

[90]J. R. Jayapandiyan, C. Kavitha, K. Sakthivel. *Enhanced Least Significant Bit Replacement Algorithm in Spatial Domain of Steganography Using Character Sequence Optimization*. **IEEE Access** 2020, 8, 136537–136545.

[91]K. Wang & Q. Gao. *A Coverless Plain Text Steganography Based On Character Features*. **IEEE Access** 2019, 7, 95665–95676.

[92]N. Wu, W. Ma, Z. Ziu, P. Shang, Z. Yang, J. Fan. *Coverless Text Steganography Based on Half Frequency Crossover Rule*. **In Proceedings of the 2019 4th International Conference on Mechanical, Control and Computer Engineering (ICMCCE), Hohhot, China,** 5–27 October 2019; pp. 726–7263.

[93]N. Wu, Z. Liu, W. Ma, P. Shang, Z .Yang, J. Fan. *Research On Coverless Text Steganography Based On Multi-Rule Language Models Alternation*. **In Proceedings of the 2019 4th International Conference on Mechanical, Control and Computer Engineering (ICMCCE), Hohhot, China**, 5–27 October 2019; pp. 803–8033.

[94]G. Maji &S. Mandal. *A Forward Email Based High Capacity Text Steganography Technique Using A RAndomized And Indexed Word Dictionary*. **Multimedia Tools Appl**. 2020, 79, 26549–26569.

[95]M. Fateh & M. Rezvani. *An Email-Based High Capacity Text Steganography Using Repeating Characters*. **Int. J. Comput. Appl**. 2021, 43, 226–232.

[96]N. Alanazi, E. Khan, A. Gutub. *Efficient Security And Capacity Techniques for Arabic Text Steganography Via Engaging Unicode StAndard Encoding. Multimed*. **Tools Appl**. 2020, 80, 1403–1431.

[97]D. Bhat, V. Krithi, K.N. Manjunath, S. Prabhu, A. Renuka. *Information Hiding Through Dynamic Text Steganography And Cryptography*. **Comput. Inform**. 2017, 1826–1831.

[98]R. Kumar, A. Malik, S. Singh, S. Chand. *A High Capacity Email Based Text Steganography Scheme Using Huffman Compression*. **In Proceedings of the 2016 3rd International Conference on Signal Processing and Integrated Networks (SPIN), Noida, India**, 11–12 February 2016; pp. 53–56.

[99]A. Taha, A. S. Hammad, M. M. Selim. *A High Capacity Algorithm For Information Hiding In Arabic Text.* **J. King saud univ. Comput.Inf. Sci**. 2018, 32, 658–665.

[100]N. Alanazi, E. Khan, A. Gutub. *Inclusion of unicode stAndard seamless characters to expAnd arabic text steganography for secure individual uses*. **J. King Saud Univ. Comput. Inf. Sci.** 2020.

[101]S. Al-Nofaie, A. Gutub, M. Al-Ghamdi. *Enhancing Arabic Text Steganography For Personal Usage Utilizing Pseudo-Spaces*. **J.King Saud Univ.-Comput. Inf. Sci**. 2019, 33, 963–974.

[102]A. A Gutub & K.A. Alaseri. *Refining Arabic Text Stego-techniques for Shares Memorization Of Counting-based Secret Sharing*. **J.King Saud Univ.-Comput. Inf. Sci**. 2019.

[103]A. Ditta, C. Yongquan, M. Azeem, K. G. Rana, H. Yu, M. Q. Memon. *Information Hiding: Arabic Text Steganography By Usingunicode Characters To Hide Secret Data*. **Int. J. Electron. Secur. Digit. Forensics** 2018, 10, 61–78.

[104]M. T. Ahvanooey, Q. Li, Q, J. Hou, H. D. Mazraeh, J. Zhang. *AITSteg: An Innovative Text Steganography Technique For Hidden Transmission Of Text Message Via Social Media*. **IEEE Access** 2018, 6, 65981–65995.

[105]S. Chaudhary, M. Dave, A. Sanghi. *AggrAndize Text Security And Hiding Data Through Text Steganography*. **In Proceedings of the 2016 IEEE 7th Power India International Conference (PIICON), Bikaner, India**, 25–27 November 2016; pp. 1–5.

[106]B. Khosravi, B. Khosravi, K. Nazarkardeh. *A New Method For PDF Steganography In Justified Texts*. **J. Inf. Secur.Appl.** 2019, 45, 61–70.

[107]R. Kumar, A. Malik, A, S. Singh, B. Kumar, S. Chand. *A Space Based Reversible High Capacity Text Steganography Scheme Using Font Type And Style*. **In Proceedings of the 2016 International Conference on Computing, Communication and Automation (ICCCA), Greater Noida, India**, 29–30 April 2016; pp. 1090–1094.

[108]S. G. R. Ekodeck, R. Ndoundam. *Steganography Based On Chinese Remainder Theorem*. **J. Inf. Secur. Appl**. 2016, 29, 1–15.

[109]Y. Li, J. Zhang, Z. Yang, R. Zhang. *Topic-Aware Neural Linguistic Steganography Based On Knowledge Graphs.* **ACM/IMS Trans.Data Sci**. 2021, 2, 1–13.

[110]Z. Yang, L. Xiang, S. Zhang, X. Sun, Y. Huang. *Linguistic Generative Steganography With Enhanced Cognitive-Imperceptibility*. **IEEE Signal. Process. Lett**. 2021, 28, 409–413.

[111]X. Zhou, W. Peng, B. Yang, J. Wen, Y. Xue, P. Zhong. *Linguistic Steganography Based On Adaptive Probability Distribution*. **IEEE Trans. Dependable Secur. Comput**. 2021.

[112]A. Naharuddin, A. D. Wibawa, S. Sumpeno. *A High Capacity And Imperceptible Text Steganography Using Binary Digit Mapping On Ascii Characters*. **In Proceedings of the 2018 International Seminar on Intelligent Technology and Its Applications (ISITIA), Bali, Indonesia**, 30–31 August 2018; pp. 287–292.

[113]A. Malik, G. Sikka, H. K.Verma. *A High Capacity Text Steganography Scheme Based On Lzw Compression And Color Coding*. **Eng.Sci. Technol. Int. J**. 2017, 20, 72–79.

[114]J. K. Sadié, L. M. Metcheka, R. Ndoundam. *A High Capacity Text Steganography Scheme Based On Permutation And Color Coding*. **arXiv** 2020, arXiv:2004.00948.

[115]A. F. Al-Azzawi. *A Multi-layer Arabic Text Steganographic Method Based On Letter Shaping*. **Int. J. Netw. Secur. Its Appl. (IJNSA)** 2019,11. Available online: https://ssrn.com/abstract=3759471.

[116]O. W. Liang & V. Iranmanesh. *Information Hiding Using Whitespace Technique In Microsoft Word*. **In Proceedings of the 2016 22nd International Conference on Virtual System & Multimedia (VSMM), Kuala Lumpur, Malaysia**, 17–21 October 2016; pp. 1–5.

[117]S. S. Baawi &D. A. Nasrawi. *Improvement Of "Text Steganography Based On Unicode Of Characters In Multi-lingual" By Custom Font With Special Properties*. **In Proceedings of the IOP Conference Series: Materials Science and Engineering, Jonkoping, Sweden**, 22–23 June 2020; Volume 870, p. 012125.

[118]S. T. A. Shah, A. Khan, A. Hussain. *Text Steganography Using Character Spacing After Normalization*. **Int. J. Sci. Eng. Res**.2020, 11, 949–957.

[119]M. Shin, H. Jeon, Y. Ju, B. Lee, S. Jeong. *Constructing Rbac Based Security Model In U-Healthcare Service Platform*. **Sci World J** 2014;1–13.

[120]W. Li, D. Hoang. *A New Security Scheme For E-Health System*. **In: International Symposium on Collaborative Technologies and Systems**, 2009. CTS '09., Baltimore, MD, USA, 2009, pp. 361–366.

[121]L. Fan, O. Lo, W. Buchanan, E. Ekonomou, T. Sharif, C.Sheridan. *Protecting Patient Privacy For e-Health Services In the Cloud*. **SPoC**:, 2014, pp. 1–6.

[122]S. Bhartiya, D. Mehrotra, A. Girdhar. Proposing hierarchy-similarity based access control framework: *A multilevel Electronic Health Record Data Sharing Approach for Interoperable Environment.* **Journal of King Saud University – Computer and Information Sciences**,2019, 1-15.

[123]F. Rezaeibagha & Y. Mu. D*istributed Clinical Data Sharing Via Dynamic Access Control Policy Transformation*. **Int J Med Inf** 2016:25–31.

[124]O. Garcia-Morchon & K. Wehrle. *Efficient And Context-Aware Access Control For Pervasive Medical Sensor Networks*. **In: 2010 8th IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops), Mannheim, Germany,** 2010, pp. 322–327.

[125]S. Amini, R. Verhoeven, J. Lukkien & S. Chen. *Toward A Security Model For A Body Sensor Platform.* **In: 2011 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA**, 2011, pp. 143–144.

[126]X. Wang, J. Ma, F. Xhafa, M. Zhang, X. Luo. *Cost-Effective Secure E-Health Cloudsystem Using Identity Based Cryptographic Techniques*. **Future Gener ComputSyst** 2017;67:242–54.

[127]R. Karakıs, I. Güler, I. Çapraz, E. Bilir. *A Novel Fuzzy Logic-Based Image Steganography Method To Ensure Medical Data Security*. **Comput Biol Med** 2015;172–183.

[128]N. A. Azeez, T. Iyamu, I. M. Venter. *Grid Security Loopholes With Proposed Countermeasures*. **26th International Symposium on Computer and Information Sciences. London: Springer**; 2011. p. 411–8.

[129]A. Sahi, D. Lai, Y. Li. *Security And Privacy Preserving Approaches In The Ehealth Clouds With Disaster Recovery Plan*. **Comput Biol Med** 2016;78:1–8.

[130]M. Peleg, D. Beimel, D. Dori, Y. Denekamp. *Situation-Based Access Control: Privacy Management Via Modeling Of Patient Data Access Scenarios*. **J Biomed Inform** 2008;41:1028–40.

[131]O. Rubio, A. Alesanco, J. García. *A Robust And Simple Security Extension For The Medical StAndard SCP-ECG*. **J Biomed Inf** 2013;142–151.

[132]N. A. Azeez, A. B. Babatope. *An Alternative Approach to Network Intrusion Detection*. **J Comput Sci Appl Int J Nigeria Comput Soc** 2016:129–43.

[133]S. Martínez, D. Sánchez, A. Valls. *A Semantic Framework To Protect The Privacy Of Electronic Health Records With Non-Numerical Attributes*. **J Biomed Inf** 2013:294–303.

[134]S. Kim, M. Sung, Y. Chung. *A Framework To Preserve The Privacy Of Electronic Health Data Streams*. **J Biomed Inf** 2014,95–106.

[135]M. Barua, X. Liang, R. Lu, X. Shen. *ESPAC: Enabling Security And Patient-Centric Access Control For E-Health In Cloud Computing*. **Int J Security Netw** 2011,67–76.

[136]N. A. Azeez,H. D. Iliyas. *Implementation Of A 4-Tier Cloud-Based Architecture For Collaborative Health Care Delivery*. **Nigerian J Technol Dev** 2016;13(1):17–25.

[137]Q. Kester, L. Nana, A. Pascu, S. Gire, J. Eghan, N. Quaynor. *A Security Technique for Authentication And Security of Medical Images in Health Information Systems.* **In: 2015 15th International Conference on Computational Science and Its Applications, Banff, AB, Canada,** 2015, pp. 8–13.

[138]Q. Kester, L. Nana, A. Pascu, S. Gire, J. Eghan, Quaynor, N. *A Security Technique for Authentication And Security of Medical Images in Health Information Systems.* **In: 2015 15th International Conference on Computational Science and Its Applications, Banff, AB, Canada**, 2015, pp. 8–13.

[139]R. Wu, G. Ahn, H. Hu. *Secure Sharing of Electronic Health Records in Clouds*. **In: 8th International Conference Conference on Collaborative Computing: Networking, Applications and Worksharing, Collaboratecom 2012 Pittsburgh, PA, United States**, October 14-17, 2012, Pittsburgh, PA, United States, 2012, pp.711–718.

[140]S. Yu, C. Wang, K. Ren, W. Lou. *Achieving Secure, Scalable, And Fine-grained Data Access Control in Cloud Computing.* **In: 2010 Proceedings IEEE, INFOCOM, San Diego, CA, USA**, 2010 pp. 1–9.

[141]H. Löhr, A. Sadeghi, M. Winandy. *Securing the E-Health Cloud***. In: 1st ACM International Health Informatics Symposium (IHI 2010)., Arlington, Virginia, USA**, 2010, pp. 1–10.

[142]T. Hupperich, H. Löhr, A. Sadeghi, M. Winandy. *Flexible Patient-Controlled Security for Electronic Health Records*. **In: 2nd ACM SIGHIT International Health Informatics Symposium (IHI 2012)., Miami, Florida, USA, 2012**, pp. 1–5.

[143]N. Kahani, K. Elgazzar, K. Cordy. *Authentication And Access Control in e-Health Systems in the Cloud.* **In: IEEE International Conference on High Performance and Smart Computing (HPSC), Big Data Security on Cloud (BigDataSecurity), New York, NY, USA**, 2016, pp. 13–23.

[144]Li, M, Yu, S, Ren, K, Lou, W. *Securing Personal Health Records in Cloud Computing: Patient-Centric And Fine-Grained Data Access Control in Multiowner Settings.* **In: International Conference on Security and Privacy in Communication Systems, Singapore, Singapore**, 2010, pp. 89–106.

[145]K. Gai, M. Qiu, X. Sun. *A survey on FinTech.* **J Netw Comput Appl** 2018, 103 :262–73.

[146]N. Azeez & I. Venter. *Towards Ensuring Scalability, Interoperability And Efficient Access Control In A Multi-Domain Grid-Based Environment.* **SAIEE Afr Res J** 2013:54–68.

[147]K. Gai & M. Qiu. *Blend Arithmetic Operations On Tensor-Based Fully Homomorphic Encryption Over Real Numbers*. **IEEE Trans Ind Inf** 2018;14(8):3590–8.

[148]X. Liu, R. Lu, J. Ma, L. Chen, B. Qin. *Privacy-Preserving Patient-Centric Clinical Decision Support System on Naive Bayesian Classification*. **IEEE J Biomed Health Inf** 2016;20(2).

[149]E. Alasaarela, R. Nemana, S. DeMello. *Drivers And Challenges of Wireless Solutions in Future Healthcare.* **Proceedings of the 2009 International Conference on eHealth, Telemedicine, and Social Medicine; Cancun, Mexico**. 1–7 February 2009.

[150]E. AbuKhousa, N. Mohamed & J. Al-Jaroodi. *E-health cloud: opportunities And challenges*. ***Future internet****, 2012,* **4**(3): 621-645.

[151]R. Asija & R. Nallusamy. A Survey on Security and Privacy of Healthcare Data, 2014.

[152]R. Sumathi & E. Kirubakaran. *SCEHSS: Secured Cloud Based Electronic Health Record Storage System with Re-Encryption at Cloud Service Provider.* **International Journal of Computer and Communication Engineering***, 2013,* **2**(2): 162.

[153]E. AbuKhousa, N. Mohamed & J. Al-Jaroodi. *E-Health Cloud: Opportunities And Challenges*. **Future internet***, 2012,* **4**(3): 621-645.

[154]Asija, R., & Nallusamy, R. A Survey on Security and Privacy of Healthcare Data, 2014.

[155]H. Löhr, A. R. Sadeghi & M. Winandy. *Securing The E-Health Cloud*. **In *Proceedings of the 1st acm international health informatics symposium* (ACM)**,2020 pp. 220-229.

[156]N. Kahani, K. Elgazzar & J. R. Cordy. *Authentication And Access Control In E-Health Systems In The Cloud*. **In proceedings of 2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS) (IEEE)**,2016, pp. 13-23.

[157]T. Sahama, L. Simpson & B. Lane. *Security And Privacy in eHealth: Is it possible?*. **In *proceedings of 2013 IEEE 15th International Conference on e-Health Networking, Applications And Services (Healthcom 2013)* (IEEE)**, 2013, pp. 249-253.

[158]J. L. Fernández-Alemán, I. C.Señor, P. A. O. Lozoya & A. Toval. *Security And Privacy In Electronic Health Records: A Systematic Literature Review.* **Journal of biomedical informatics***, 2013,* 46(3): 541-562.

[159]A. Abbas & S. U. Khan. *A Review On The State-Of-The-Art Privacy-Preserving Approaches In The E-Health Clouds*. **IEEE Journal of Biomedical and Health Informatics**,2014, *18*(4), 1431-1441.

[160]Rezaeibagha, F., Win, K. T., & Susilo, W. *A Systematic Literature Review on Security And Privacy Of Electronic Health Record Systems: Technical Perspectives*. ***Health Information Management Journal*** *, 2015*,44(3): 23-38.

[161]R. Sumathi & E. Kirubakaran. *SCEHSS: Secured Cloud Based Electronic Health Record Storage System with ReEncryption at Cloud Service Provider*. ***International Journal of Computer And Communication Engineering****, 2013,* **2**(2): 162

[162]Omotosho, A., Adegbola, O., Mikail, O. O., & Emuoyibofarhe, J. (2015). *A Secure Electronic Prescription System Using Steganography With Encryption Key Implementation*. *arXiv preprint arXiv:1502.01264*.

[163]A. Omotosho & J. Emuoyibofarhe. *A Criticism Of The Current Security, Privacy And Accountability Issues In Electronic Health Records*. ***arXiv preprint arXiv****:2015,1501.07865*.

[164]B. S. Varsha & P.S. Suryateja. *Using Advanced Encryption StAndard for Secure And Scalable Sharing of Personal Health Records in Cloud*. **International Journal of Computer Science and Information Technologies (IJCSIT)** *,2014,***5**(6): 7745-7747.

[165]Oh, J. Y., Yang, D. I., & Chon, K. H. (2010). *A Selective Encryption Algorithm Based On Aes For Medical Information*. **Healthcare informatics research 16**(1): 22-29.

[166]D. Shin, T. Sahama & R. Gajanayake. *Secured E-Health Data Retrieval In Daas And Big Data*. **In proceedings of 2013 IEEE 15th International Conference on e-Health Networking, Applications and Services** (IEEE)2013, pp. 255- 259.

[167]M. A. Kamoona & A. M. Altamimi. Cloud E-health Systems: *A Survay on Security Challenges And Solutions*. **In proceedings of 2018 8th International Conference on Computer Science and Information Technology (CSIT), (IEEE)**, 2018, pp. 189-194.

[168]A. Abbass & S. U. Khan. *A Review on the State-of-the-art Privacy-Preserving Approaches in the e-health Clouds*. *I**EEE Journal of Biomedical And Health Informatics,*** 2014,*18*(4), 1431-1441.

[169]N. Ramakrishnan & B. Sreerekha. *Enhancing Security of Personal Health Records in Cloud Computing by Encryption.* **In *International Journal of Science And Research (IJSR),* 2013.**

[170]B. N. Pooja. *Secure Mechanism for Medical Database Using RSA*. **International Journal of Application or Innovation in Engineering & Management***, 2014,* **3**(7): 320-327.

[171]S. N. Dhanabagyam & G. R. Karpagam. *Secure Communications for e-Health in Mobile Cloud Computing Using Provable Security*. ***International Journal of Pure And Applied Mathematics****,* 2017*,* **114**(7): 325-335.

[172]R. Sridevi & C. Nithiya. *E-Health Security using ECC algorithm.* ***International Journal of Advanced Research in Basic Engineering Sciences And Technology*** *(IJARBEST)*,2016, **2**(19): 114-117.

[173]K. L. Tsai, F. Y. Leu, T. H. Wu, S. S. Chiou, Y. W. Liu & H. Y. A. Liu. *Secure ECC-based Electronic Medical Record System*. ***J. Internet Serv. Inf. Secur****. 2014,* ***4***(1): 47-57.

[174]C. H. Liu, F. Q. Lin, D. L. Chiang, T. L. Chen, C. S. Chen, H. Y. Lin, Y. F. Chung, and T. S. Chen. *Secure Phr Access Control Scheme For Healthcare Application Clouds*. **In *proceedings of 2013 42nd International Conference on Parallel Processing*, (IEEE)** ,2013, pp. 1067-1076.

[175]X. A. Wang, J. Ma, F. Xhafa, M. Zhang, & X. Luo. *Cost-Effective Secure E-Health Cloud System Using Identity Based Cryptographic Techniques*. ***Future Generation Computer Systems****, 2017,* **67**: 242-254.

[176]Y. Zheng. *Privacy-Preserving Personal Health Record System Using Attribute-Based Encryption,* 2011,***Masters Thesis*, (Publisher: Worcester Polytechnic Institute). Available Online: *https://digitalcommons.wpi.edu/etd-theses/902***

[177]*A systematic literature review on security And privacy of electronic health record systems: technical perspectives*. ***Health Information Management Journal****, 2015,* **44**(3): 23- 38.

[178]R. Charanya, S. Nithya, & N. Manikandan. *Attribute Based Encryption for Secure Sharing of e-health Data*. **In *Materials Science And Engineering Conference Series****, 2017,* **263**(4): 042030.

[179]J. A. Akinyele, M. W. Pagano, M. D. Green, C. U. Lehmann, Z. N. Peterson & A. D. Rubin. *Securing Electronic Medical Records Using Attribute-Based Encryption On Mobile Devices*. **In *Proceedings of the 1st ACM workshop on Security And privacy in smartphones And mobile devices* (ACM)**,2011, pp. 75-86.

[180]K. Kulkarni & A. M. Dixit. Privacy Preserving System Using Attribute Based Encryption for e-health Cloud, 2014.

[181]L. Selvam & R. J. Arokia. *Secure Data Sharing of Personal Health Records in Cloud Using Fine-Grained And Enhanced Attribute-Based Encryption*. **In *proceedings of 2018 International Conference on Current Trends towards Converging Technologies (ICCTCT)* (IEEE)**,2018, pp. 1-6.

[182]M. A. Sadikin & R. W. Wardhani. I*mplementation Of Rsa 2048-Bit And Aes 256-Bit With Digital Signature For Secure Electronic Health Record Application*. **In *proceedings of 2016International Seminar on Intelligent Technology And Its Applications (ISITIA)* (IEEE)**,2016, pp. 387-392.

[183]J. Pecarina, S. Pu, & J.C. Liu. *Anonymity For Enhanced Control And Private Collaboration In Healthcare Clouds*. **In *proceedings of 4th IEEE International Conference on Cloud Computing Technology And Science Proceedings* (IEEE)**, 2012, pp. 99-106.

[184]P. Chinnasamy, & P. Deepalakshmi. *Design of Secure Storage for Health-care Cloud using Hybrid Cryptography*. **In *proceedings of 2018 Second International Conference on Inventive Communication And Computational Technologies (ICICCT)*** (IEEE),2018, pp. 1717-1720.

[185]A. Omotosho, O. Adegbola, O. Mikail & J. Emuoyibofarhe. *A Secure Electronic Prescription System Using Steganography With Encryption Key Implementation.* ***arXiv preprint arXiv****, 2015,1502.01264*.

[186]Li, M., Yu, S., Zheng, Y., Ren, K., & Lou, W. (2012). *Scalable And Secure Sharing Of Personal Health Records In Cloud Computing Using Attribute-Based Encryption*. **IEEE transactions on parallel and distributed systems 24**(1): 131-143.

[187]N. M. Shrestha, A. Alsadoon, P. W. C. Prasad, L. Hourany & A. Elchouemi. *Enhanced E-Health Framework For Security And Privacy In Healthcare System*. **In *proceedings of 2016 Sixth International Conference on Digital Information Processing And Communications (ICDIPC)* (IEEE)**,2016, pp. 75-79.

[188]Z. Liu, J. Weng, J. Li, J. Yang, C. Fu & C. Jia. *Cloud-Based Electronic Health Record System Supporting Fuzzy Keyword Search.* ***Soft Computing****, 2016,* **20**(8): 3243-3255.

[189]J. Huang, M. Sharaf, T. S. Huang. *A Hierarchical Framework for Secure And Scalable ehr Sharing And Access Control in Multi-cloud*. **In *proceedings of 2012 41st International Conference on Parallel Processing Workshops****,*2012 (IEEE), pp. 279- 287.

[190]X. Yang, G. Lin, Y. Liu, F. Nie, & L. Lin. *Fast Spectral Embedded Clustering Based On Structured Graph Learning For Large-Scale Hyperspectral Image.* ***IEEE Geoscience And Remote Sensing Letters***,2020, vol. 99, pp. 1–5.

[191]S. Dong, P. Wang, & K. Abbas. *A Survey On Deep Learning And Its Applications.* ***Computer Science Review***, 2021, vol. 40, no. 1, Article ID 100379.

[192]J. Fridrich, M. Goljan, & D. Rui Du. *Detecting Lsb Steganography In Color, And Gray-Scale Images.* ***IEEE Multimedia***, 2021, vol. 8, no. 4, pp. 22–28.

[193]A. A. Tamimi, A. M. Abdalla, & O. Alallaf, *Hiding An Image Inside Another Image Using Variable-Rate Steganography.* ***International Journal of Advanced Computer Science And Applications***, 2013, vol. 4, no. 10, pp. 1–4, 2013.

[194]L. A. Gatys, A. S. Ecker, & M. Bethge. *Image Style Transfer Using Convolutional Neural Networks.* **In *Proceedings of the IEEE Conference on Computer Vision And Pattern Recognition,*** *2016,* pp. 2414–2423, Las Vegas, NV, USA.

[195]J. Johnson, A. Alahi & L. Fei-Fei. *Perceptual Losses For Real-Time Style Transfer And Super-Resolution.* **In *Proceedings of the European Conference on Computer Vision*, pp. 694–711, Computer Vision - ECCV 2016, Amsterdam, The Netherlands**,2016.

[196]L. A. Gatys, A. S. Ecker, M. Bethge, A. Hertzmann, & E. Shechtman, *Controlling Perceptual Factors In Neural Style Transfer*. **In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition**,2017, pp. 3730–3738, Honolulu, HI, USA.

[197]A. Sanakoyeu, D. Kotovenko, S. Lang, & B. Ommer. *A Style-aware Content Loss For Real-time Hd Style Transfer.* **In *Proceedings of the European Conference on Computer Vision***, pp. 715–731, Computer Vision - ECCV 2018, Germany, September 8-14, 2018.

[198]X. Liu, M. Cheng, Y. Lai & P. Rosin. *Depth-Aware Neural Style Transfer.* **In Proceedings of the Symposium on Non-Photorealistic Animation and Rendering**, pp. 1–10, Los Angeles California, July 2017.

[199]F. Luan, S. Paris, E. Shechtman & K. Bala. *Deep photo style transfer.* **In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition**, pp. 1–9, Honolulu, HI, USA, July 2017.

[200]Y. Liu, Z. Xu, W. Ye. *Image Neural Style Transfer With Preserving The Salient Regions*. **IEEE Access**, vol. 7, Article ID 40037, 2019.

[201]V. Dumoulin, J. Shlens & M. Kudlur, "*A Learned Representation For Artistic Style.* **In Proceedings of the Conference on ICLR**, pp. 1–26, Toulon, France, April 2017

[202]D. Chen, L. Yuan, J. Liao, N. Yu, & H. G. StyleBank. *An Explicit Representation For Neural Image Style Transfer.* **In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition**, 2017, pp. 1–10, CVPR), Honolulu, HI, USA.

[203]Q. Tian & M. Schmidt. *Fast Patch-Based Style Transfer Of Arbitrary Style.* **In Proceedings of the Conference on Neural Information Processing Systems Barcelona, Spain**,2016, pp. 1–5.

[204]X. Huang & S. Belongie. *Arbitrary Style Transfer In Real-Time With Adaptive Instance Normalization.* ***In Proceedings of the IEEE International Conference on Computer Vision***, Barcelona, Spain, 2017, pp. 1510–1519.

[205]Y. Li, C. Fang, J. Yang, Z. Wang, X. Lu & M. Yang. *Universal Style Transfer Via Feature Transforms.* **In Proceedings of the Conference on Neural Information Processing Systems**, Long Beach, United States,2017, pp. 1–11.

[206]J. Qin, Y. Luo, X. Xiang, Y. Tan, & H. Huang. *Coverless Image Steganography: A Survey.* **IEEE Access**, vol. 7, no. 99, Article ID 171372, 171394 pages, 2019.

[207]M. Dalal & M. Juneja. *A Secure Video Steganography Scheme Using Dwt Based On Object Tracking.* **Information Security Journal: A Global Perspective**, no. 1, pp. 1–18, 2021.

[208]Y. Qian, D. Jing, W. Wei & T. Tan. *Deep Learning For Steganalysis Via Convolutional Neural Networks.* **In *Proceedings of the SPIE-International Society for Optical Engineering*, San Francisco, CA, United State**s, March 2015.

[209]G. Xu, H.-Z. Wu, & Y.-Q. Shi. *Structural Design Of Convolutional Neural Networks For Steganalysis.* ***IEEE Signal Processing Letter***s,2016, vol. 23, no. 5, pp. 708–712.

[210]Y. Jian, J. Ni, & Y. Yang. *Deep Learning Hierarchical Representations For Image Steganalysis.* **IEEE Transactions on Information Forensics and Security**, 2017, vol. 12, no. 11, pp. 2545–2557.

[211]S. Baluja. *Hiding Images In Plain Sight: Deep Steganography.* **Advances in Neural Information Processing Systems**, 2017, vol. 30, pp. 2069–2079.

[212]D. Volkhonskiy, I. Nazarov, & E. Burnaev. *Steganographic Generative Adversarial Networks.* **In Proceedings of the Conference on Neural Information Processing Systems**,Long Beach, United States, 2017, pp. 1–8.

[213]J. Zhu, R. Kaplan, J. Johnson, & L. Fei-Fei. *Hidden: Hiding Data With Deep Networks.* **In Proceedings of the European Conference on Computer Vision**, 2018, Munich, Germany, pp. 682–697.

[214]M. Tancik, B. Mildenhall, & R. Ng. *Stegastamp: Invisible Hyperlinks In Physical Photographs.* **In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition**, Seattle, Washington, USA, 2020, pp. 1–13.

[215]I. J. Kadhim, P. Premaratne, P. J. Vial, & B. Halloran. *Comprehensive Survey Of Image Steganography: Techniques, Evaluations And Trends In Future Research.* **Neurocomputing**, 2019, vol. 335, pp. 299–326.

[216]H. Y. Chen, I. S. Fang, & W. C. Chiu. S*elf-Contained Stylization Via Steganography For Reverse And Serial Style Transfer*. **In Proceedings of the IEEE Winter Conference on Applications of Computer Vision**, 2018 pp. 1–15, WACV), Lake Tahoe, NV, USA.

[217]N. Zhong, Z. Qian, Z. Wang, & X. Zhang. *Steganography In Stylized Images.* **Journal of Electronic Imaging**, vol. 28, no. 3, pp. 1–12, 2019.

[218]Q. Li, X. Wang, B. Ma. *Image Steganography Based On Style Transfer And Quaternion Exponent Moments.* A**pplied Soft Computing**, vol. 110, no. 3, Article ID 107618, 2021.

[219]S. Zhang, S. Su, J. Lu, Q. Zhou, & C. Chang. *Csst-net: An Arbitrary Image Style Transfer Network Of Coverless Steganography.* **The Visual Computer**, pp. 1–13, 2021.

[220]R. Zhang, S. Dong & J. Liu. *Invisible Steganography Via Generative Adversarial Networks.* **Multimedia Tools and Applications.** vol. 78, no. 7, pp. 8559–8575, 2019.

[221]T.-Y. Lin, M. Maire, S. Belongie. *Microsoft coco: Common Objects in Context.* **In Proceedings of the European Conference on Computer Vision**, pp. 740–755, Computer Vision - ECCV 2014, Zurich, Switzerland, September, 2014.

Chapter Three

Methodology

3.1 Introduction

This chapter discusses the research methodology used in the development of the cryptographic system and the procedures involved in achieving this confidentiality. Starting with the data collection approach to obtain the data used as a case study in this study to support the testing of the cryptographiic system. Two fact-finding mathematical setup was used for the development of the system alongside an algorithmic set up for the steganography stage of the design.

3.2 System Development Phases

The approach used in systems development is the waterfall system development Model as this Model ensures that all processes are completed successfully before moving on to another stage and this article presents A system with a robust design without completing one stage to move on to the next can be difficult. The systems development life cycle (SDLC) follows the critical phases required for developers, such as planning, analysis, design, and implementation. There are several systems development lifecycle Models. The waterfall Model is the oldest Model that was originally called the "system development life cycle". A waterfall Model is a sequence of steps where the output of each step becomes the input of the next step. These steps often follow the same basic steps, but many different waterfall methods provide different names. Different projects can focus on different parts of SDLC, but all projects have factors in these four stages[2].

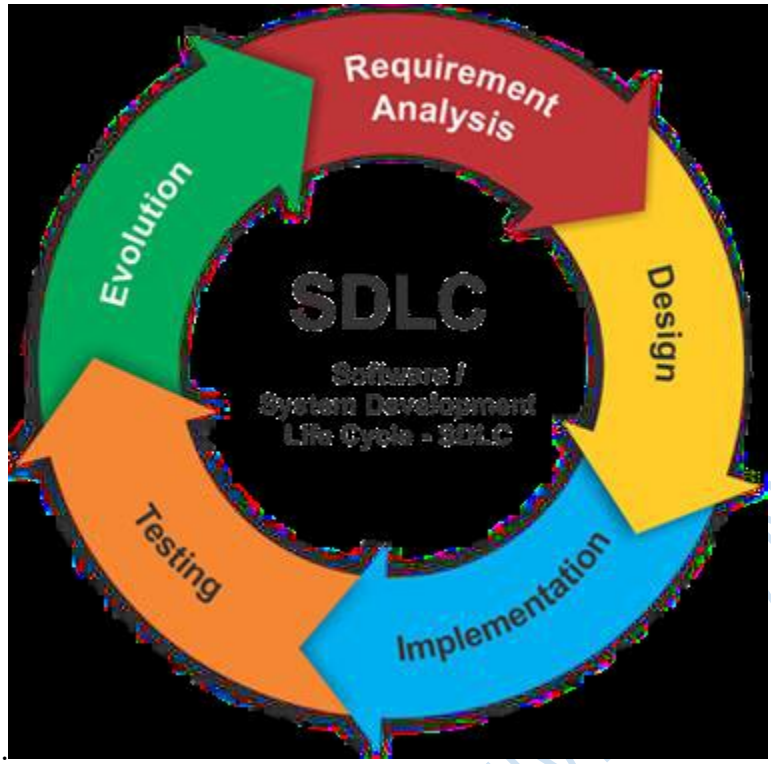


Figure 3.1 SDLC Phases[2]

3.3 Research Framework

The scheme below illustrates the conceptual framework which has the following cryptographic operations performed;

1. After the key has been determined, the medical health records are encrypted using the first crypto technique which is Ceasar Cipher Technique (Ciphertext 1).
2. The cipher text obtained from the first encryption is used as input to the second encryption phase which is the Affine Technique (Ciphertext 2).
3. The Ciphertext 2 is then uploaded into a selected image (this phase is the steganography stage)
4. Ones the upload is successful, the result of this is presented as an Image.

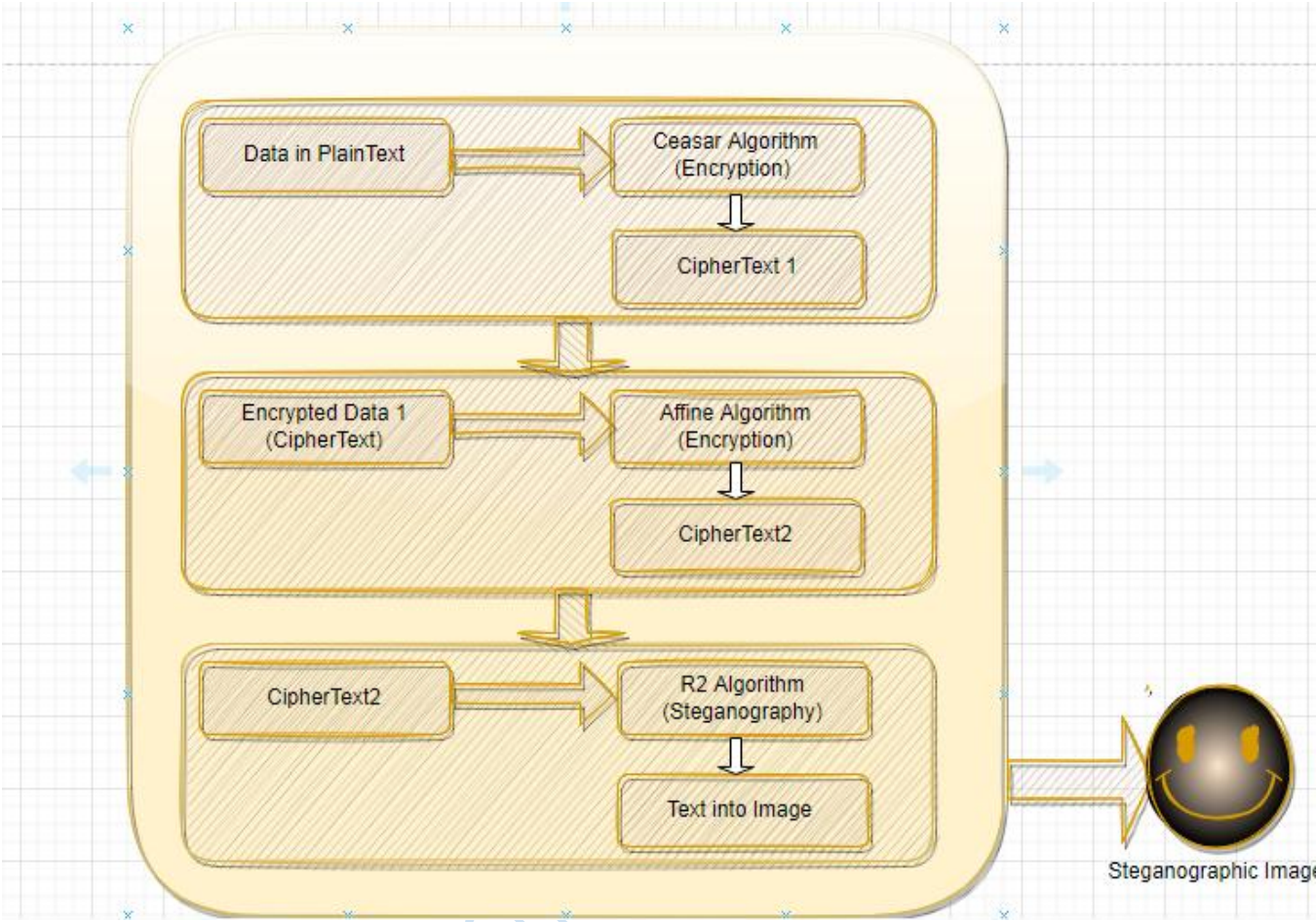


Figure 3.2 Conceptual Diagram for the Encryption Phase

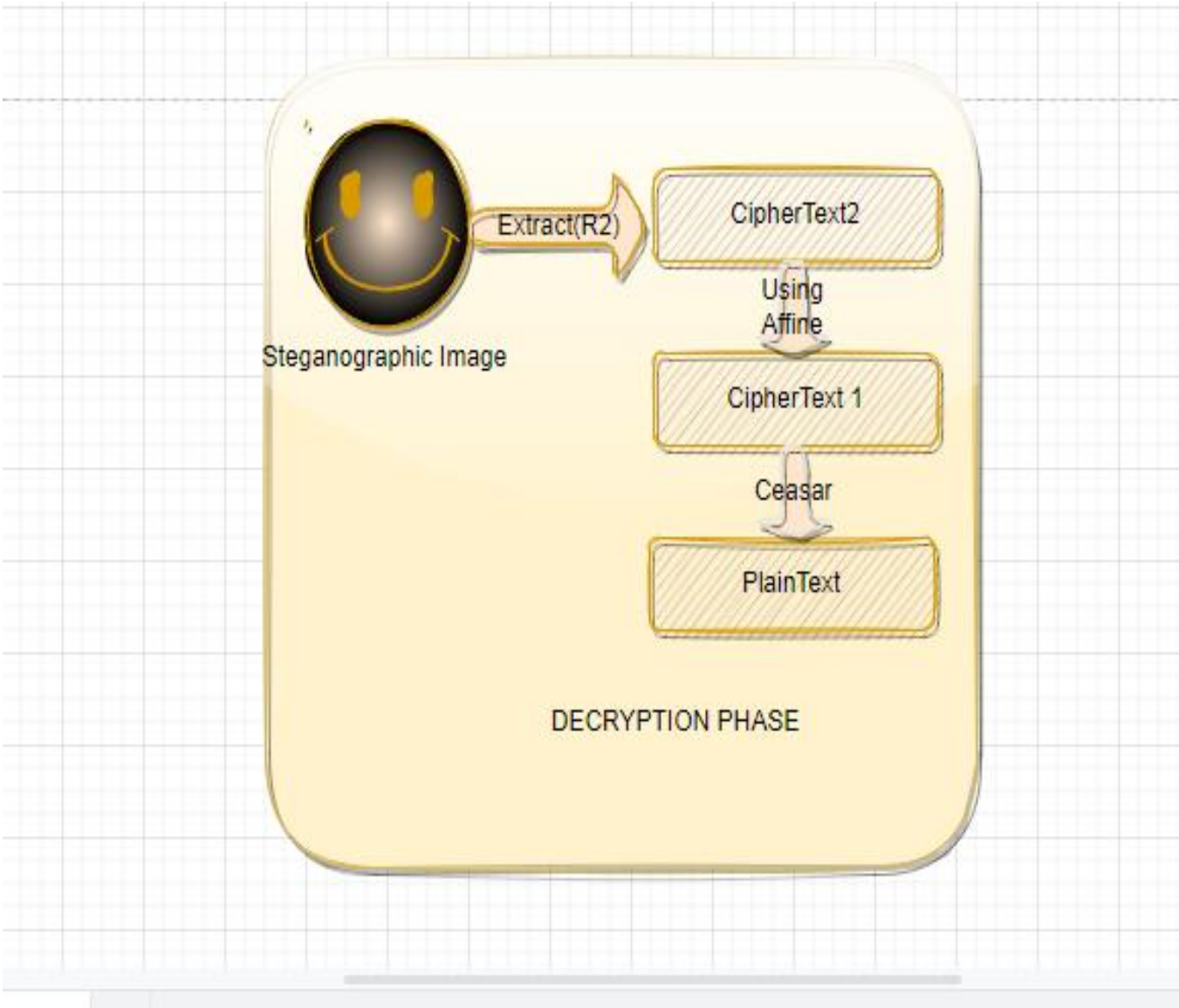


Figure 3.3 Conceptual Diagram for the Decryption Phase

The conceptual diagram presented in figure 3.3 above shows the demonstration of how the decryption process is been carried out, as the decrption process starts from extracting the text embedded into the image which is referred to as the steganographic image, after this text has been extracted from the image, the result of this extraction is the ciphertext 2, and considering the fact that ciphertext 2 was achieved using the

Affine ciphertext, then this same technique, Affine, is used to decrypt the ciphertext 2 to get Ciphertext 1.

The decryption of Ciphertext 1 back to having the original text which is referred to as the plaintext from the conceptual diagram above is done implementing the Ceasar ciphertext technique because the Ceasar technique was used to encypt the plaintext to get the ciphertext 1. These stages of decryption employs the steganographic phase and the cryptographic phase.

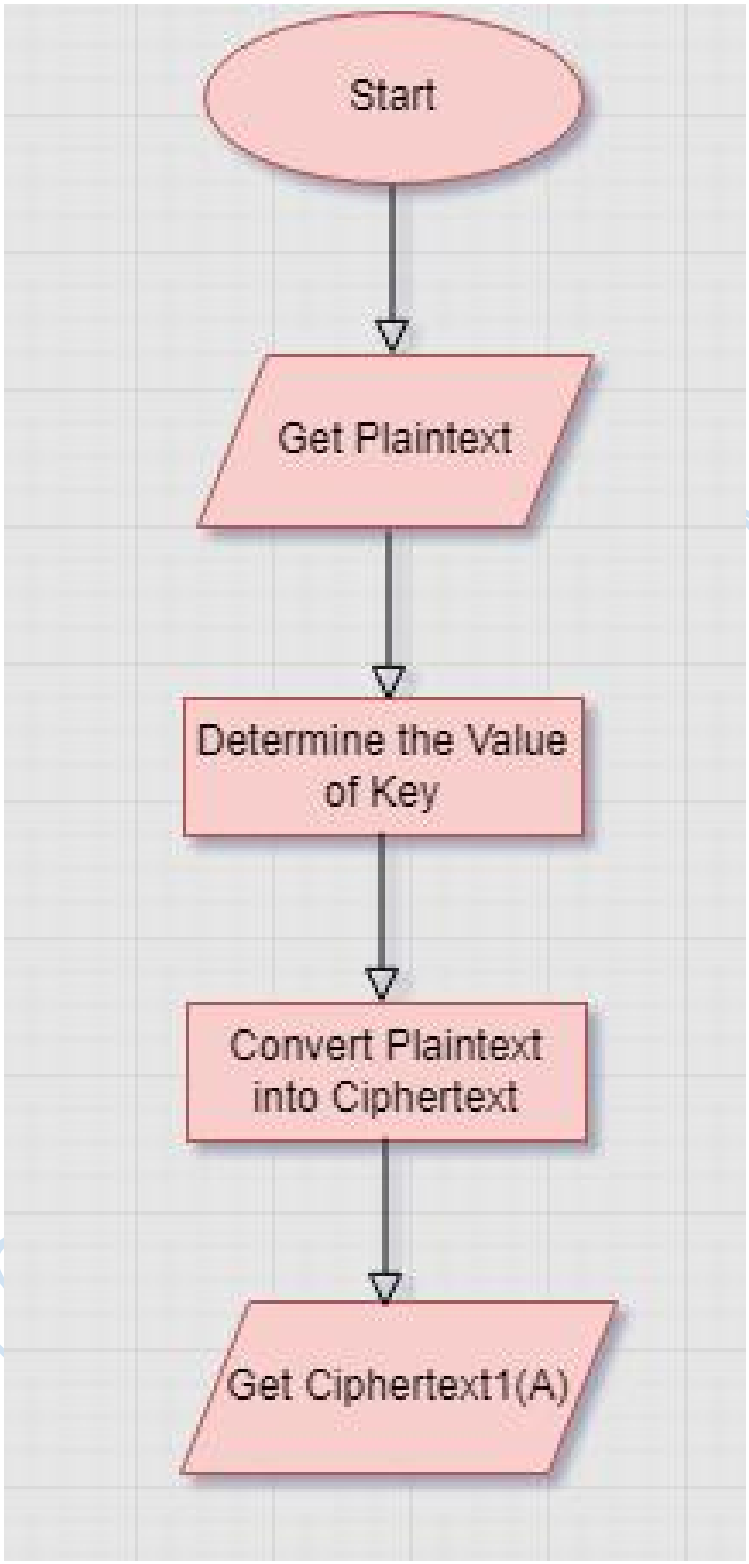


Figure 3.4 Flowchart for encryption (Researcher, Kolapo R. 2022)

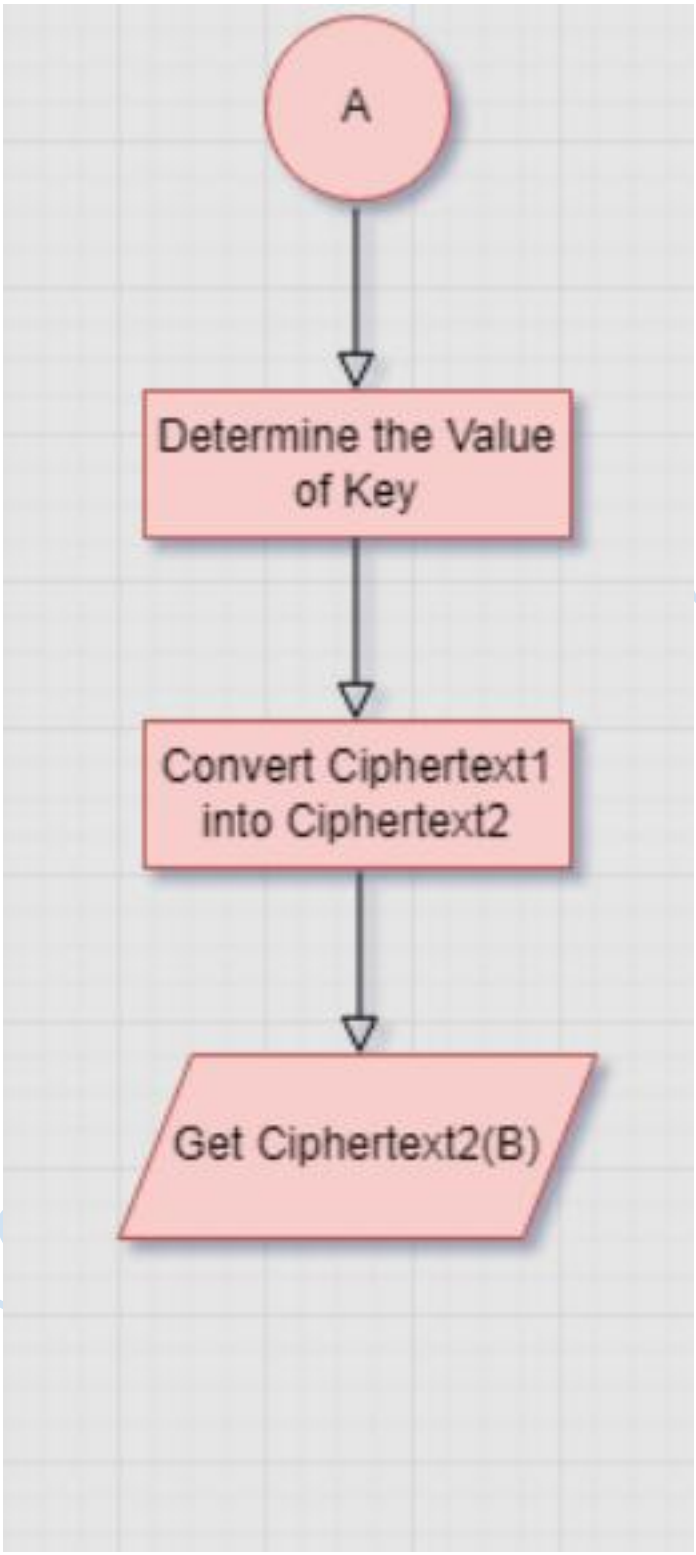


Figure 3.5 Flowchart for decryption (Researcher, Kolapo R. 2022)

The flowcharts presented above breaks down each encryption stages to show that there are values determined for keys used in each stages of the encryption process which are expected to be communicated between the sender and the receiver in a secure channel or way. While decryption is done to convert the ciphertext to plain text and this can be achieved using a private key which at this stage has been communicated securely.

3.4 Caesar and Affine Cipher

Caesarean section of message concealment and affine cipher begin by translating the message into ASCII code. The conventional Caesar and Affine used the 26 letter alphabets and this give rooms for 25 possible shifts as these techniques are mono-aplhabetic i.e there is an integal value attached to the positioning of every letter in tl 26 English alphabets.

The figure 3.7 below shows a snippet of the ASCII table which is employed in th study as this study considers using the 256 character of the ASCII table, the characters consist of Uppercase alphabet, Lowercase alphabets, special characte printable characters and even symbols. With the use of the ASCII table for tl implementation of our cryptographic stage as against the 26 alphabets of the engli letter, we have 255 possible combinations which means there are 255 possible keys against the 25 possible keys in the conventional Ceasar and Affine techniques.

The screenshots below shows a snippet of the ASCII code and the categories in whi these codes falls into.

ASCII control characters (character code 0-31)

The first 32 characters in the ASCII-table are unprintable control codes and are used to control peripherals such as printers.

DEC	OCT	HEX	BIN	Symbol	HTML Number	HTML Name	Description
0	000	00	00000000	NUL	&#000;		Null char
1	001	01	00000001	SOH	&#001;		Start of Heading
2	002	02	00000010	STX	&#002;		Start of Text
3	003	03	00000011	ETX	&#003;		End of Text
4	004	04	00000100	EOT	&#004;		End of Transmission
5	005	05	00000101	ENQ	&#005;		Enquiry
6	006	06	00000110	ACK	&#006;		Acknowledgment
7	007	07	00000111	BEL	&#007;		Bell
8	010	08	00001000	BS	&#008;		Back Space
9	011	09	00001001	HT			Horizontal Tab
10	012	0A	00001010	LF
	Line Feed
11	013	0B	00001011	VT	&#011;		Vertical Tab
12	014	0C	00001100	FF			Form Feed
13	015	0D	00001101	CR
	Carriage Return
14	016	0E	00001110	SO	&#014;		Shift Out / X-On
15	017	0F	00001111	SI	&#015;		Shift In / X-Off
16	020	10	00010000	DLE	&#016;		Data Line Escape
17	021	11	00010001	DC1	&#017;		Device Control 1 (oft. XON)
18	022	12	00010010	DC2	&#018;		Device Control 2
19	023	13	00010011	DC3	&#019;		Device Control 3 (oft. XOFF)
20	024	14	00010100	DC4	&#020;		Device Control 4
21	025	15	00010101	NAK	&#021;		Negative Acknowledgement
22	026	16	00010110	SYN	&#022;		Synchronous Idle
23	027	17	00010111	ETB	&#023;		End of Transmit Block
24	030	18	00011000	CAN	&#024;		Cancel

ASCII printable characters (character code 32-127)

Codes 32-127 are common for all the different variations of the ASCII table, they are called printable characters, represent letters, digits, punctuation marks, and a few miscellaneous symbols. You will find almost every character on your keyboard. Character 127 represents the command DEL.

DEC	OCT	HEX	BIN	Symbol	HTML Number	HTML Name	Description
32	040	20	00100000				Space
33	041	21	00100001	!	!		Exclamation mark
34	042	22	00100010	"	"	"	Double quotes (or speech marks)
35	043	23	00100011	#	#		Number
36	044	24	00100100	$	$		Dollar
37	045	25	00100101	%	%		Procenttecken
38	046	26	00100110	&	&	&	Ampersand
39	047	27	00100111	'	'		Single quote
40	050	28	00101000	(	(		Open parenthesis (or open bracket)
41	051	29	00101001	)	)		Close parenthesis (or close bracket)
42	052	2A	00101010	*	*		Asterisk
43	053	2B	00101011	+	+		Plus
44	054	2C	00101100	,	,		Comma
45	055	2D	00101101	-	-		Hyphen
46	056	2E	00101110	.	.		Period, dot or full stop
47	057	2F	00101111	/	/		Slash or divide
48	060	30	00110000	0	0		Zero
49	061	31	00110001	1	1		One
50	062	32	00110010	2	2		Two
51	063	33	00110011	3	3		Three
52	064	34	00110100	4	4		Four
53	065	35	00110101	5	5		Five
54	066	36	00110110	6	6		Six

The extended ASCII codes (character code 128-255)

There are several different variations of the 8-bit ASCII table. The table below is according to ISO 8859-1, also called ISO Latin-1. Codes 128-159 contain the Microsoft® Windows Latin-1 extended characters.

DEC	OCT	HEX	BIN	Symbol	HTML Number	HTML Name	Description
128	200	80	10000000	€	€	€	Euro sign
129	201	81	10000001				
130	202	82	10000010	‚	‚	‚	Single low-9 quotation mark
131	203	83	10000011	ƒ	ƒ	ƒ	Latin small letter f with hook
132	204	84	10000100	„	„	„	Double low-9 quotation mark
133	205	85	10000101	…	…	…	Horizontal ellipsis
134	206	86	10000110	†	†	†	Dagger
135	207	87	10000111	‡	‡	‡	Double dagger
136	210	88	10001000	ˆ	ˆ	ˆ	Modifier letter circumflex accent
137	211	89	10001001	‰	‰	‰	Per mille sign
138	212	8A	10001010	Š	Š	Š	Latin capital letter S with caron
139	213	8B	10001011	‹	‹	‹	Single left-pointing angle quotation
140	214	8C	10001100	Œ	Œ	Œ	Latin capital ligature OE
141	215	8D	10001101				
142	216	8E	10001110	Ž	Ž		Latin captial letter Z with caron
143	217	8F	10001111				
144	220	90	10010000				
145	221	91	10010001	‘	‘	‘	Left single quotation mark
146	222	92	10010010	’	’	’	Right single quotation mark
147	223	93	10010011	“	“	“	Left double quotation mark
148	224	94	10010100	”	”	”	Right double quotation mark
149	225	95	10010101	•	•	•	Bullet
150	226	96	10010110	–	–	–	En dash
151	227	97	10010111	—	—	—	Em dash

Figure 3.7 ACSII Table[4]

The operation of the affine cipher is performed by sequential encryption and decryption using both ciphers. Therefore, plaintext encrypted with the generator cipher produces ciphertext 1. Cipher 1 is placed as plaintext and encrypted with an affine cipher to generate ciphertext 2. The decoding process then decodes and clarifies CipherTEXT 2. Adventure tokens are decoded into ciphertext 1 and cleared. Caesar ciphers are part of the so-called change conversion changes. In Ceasar coding, generating a cipher with a complaint (P) and generating a Ciplext (C) can be represented by the following appropriate function: Where K is a change of purpose for the ASCII code. A ciphertext (C) to plaintext (P) conversion is performed for decryption in some caesarean sections. This can be represented by a similar function

$$CX \equiv V + K \text{ Modulus } 256,\ 0 \leq P \leq 255$$

k is the number of ASCII code shifts required to decrypt with the Caesar cipher. This is done by converting the ciphertext (CX) to the plaintext (T). This can be expressed by the following function.

$$T \equiv CX - K \text{ Modulus } 256,\ 0 \leq P \leq 255$$

To encrypt the Caesar cipher:

1. Convert the message character in the plain-text into ASCII code

2. Determine the value of k, then employ the use of transformation

$$CX \equiv V + K \text{ Modulus } 256,\ 0 \leq P \leq 255$$

3. Convert the code obtained in step 2 into message character

4. The result in step 3 is the cipher-text message

To decrypt the Caesar cipher:

1. Convert the message character in the cipher-text into ASCII code

2. Determine the value of k, then employ the use of transformation

$$P \equiv CX - K \text{ Modulus } 256,\ 0 \leq P \leq 255$$

3. Convert the number obtained in step 2 to the message character

4. The results in step 3 are plain-text messages

Affine cipher is an extension of Caesar cipher. The affine cipher for generating the encryption that converts plaintext (P) to ciphertext (C) can be expressed by the following congruent function.

$CX \equiv ((a*p) + b)$ Modulus 256, $0 \leq P \leq 255$

Where a and b are integers. b is the number of alphabet shifts required. a must be disjoint so that congruence can be expressed in 256 or vice versa. Plaintext (P) based on the description of the relationship between ciphertext (CX) and plaintext (P) is obtained. The plaintext (P) can be expressed by the following congruence function as the opposite of the ciphertext (CX).

$P \equiv (\bar{a} (c - b))$ Modulus 256, $0 \leq c \leq 255$

Where $\bar{a}$ is the inverse of a(Modulus 26) .$\bar{a}$ can be searched using congruence $\bar{a} \equiv a^{\emptyset(256)-1}$(Modulus 256). Or you can use the definition that "given an integer a with (a,m) = 1, an integer solution x of $ax \equiv 1$(Modulus M) is called an inverse of a Modulusulo m." .

To encrypt the affine cipher:

1. Convert the message character into ASCII code

2. Determine the values of a and k, then employ the use of transformation

$C \equiv ((a*p) + b)$ Modulus 256, $0 \leq P \leq 255$

3. Convert the code obtained in step b into the message character

4. The results in step c are the chipher-text message

To decrypt the affine cipher:

1. Convert the message character into ASCII code

2. Determine the values of $\bar{a}$ and k , then employ the use of transformation

$PX \equiv (\bar{a}(c - k))$ Modulus 256, $0 \leq C \leq 255$

3. Convert the code obtained in step b into the message character

4. The results in step c are plain-text messages

3.7 Hididng Text in Image Using Red2 Algorithm

Any image is a number that represents the brightness of different dots or pixels. Images have different sizes depending on their width and height. Pixels are the points of the matrix of the width and height of the image. Each pixel has 24 bits or three bytes of information to represent the image and can be used to mask information. In the Modular proposal, a new masking method is used based on algorithms. Since each pixel is a combination of three components (R, G and B), the red component is used to hide information. Any red pixel value with a decimal value of Sixteen is used to mask the message. The entire message is split into equal 2-bit values and embedded in the red pixel value of the image. This is passed until the end of the image. The message length is also embedded in the image by the software. The same software must be used to receive, decode the image, and extract the message.

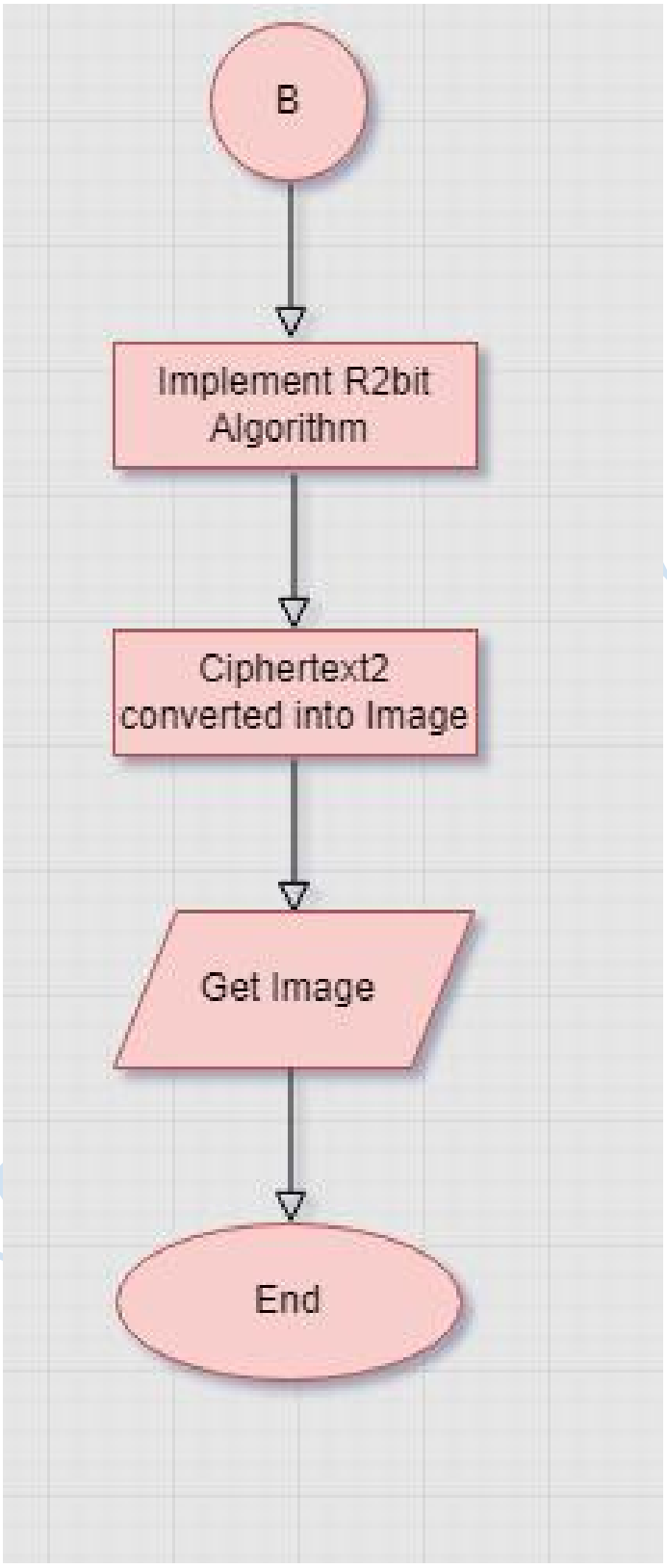


Figure 3.6 Flowchart for the Steganography Phase (Researcher, Kolapo R. 2022)

Algorithm for Hidding the Ciphertext into a selected image;

Step 1: Extract the pixels of the image and store it in an array. Step 2: Convert text box text into binary bits and store them in an array.

Step 3: Loop through all the pixels of the image to check if the Red value <= 16.

Step 4: If the value of Red in RGB is <=16 create a new value of R as “01”+Two bits of the Message Array + Old Red Value and rewrite the pixel value.

Step 5: Repeat step 3 till all the bits of the character array have been embedded.

Step 6: Write the new Image

Algorthim for Extracting the Text from the image;

Step 1: Extract the pixels of the stego image and store it in an array.

Step 2: Loop through all the pixels of the image to check if the first two bits of Red value = “01”.

Step 3: If step 2 is true then extract the 3rd and 4th bit of the red and store it in a bit character array and rewrite the Red pixel value with the last four bits.

Step 4: Repeat step 2 till all the bits of the character array have been retrieved.

Step 5: Write the new Image

Step 6: Combine 8 bits of the character bit array retrieved and extract the text.

Endnotes

[1] Y. Zhang "*Book Review: Data Collection Research Methods in Applied Linguistics.* **Sec.education. Front Psychol**. 2021.

[2] M. A. Adeagbo, J.E.T. Akinsola, A. A. Awoseyi & F. Kasali. *Project Implementation Decision Using Software Development Life Cycle Models: A Comparative Approach*. **Journal of Computer Science and its Application**. Vol 28.2021.

[3] K. Kyeremeh. *Overview of system development life cycle models*. **Journal of Management and Science**. 11(1), 2021,12-22.

[4] T. Tommy, R. Rosyida, I. Lubis & A. Marwan. "*A Simple Compression Scheme based on ASCII Value Differencing* . **Journal of Physics Conferencing Series**. 1007(1)2018: 012022.

Chapter Four

Results and Discussion of Findings

4.1 Introduction

A combination of cesarean section and affine cryptography is done to make the cipher harder to crack. In fact, the Caesar cipher is easy to solve using brute force and the most common character frequency representations. An example application of the Caesar and affine cipher combination is to use it to encrypt keywords in medical records.

4.2 **Implementation of the encryption Algorithm**

If the keyword to be encrypted is the name of a prescription say for instance;

PARACETAMOL.

Encryption is done on this particular keyword using the combination of Ceaser and Affine Cipher.

Given that the keys are 8 and 9

K = 8 and a = 9

$\bar{a} \equiv a^{\emptyset(256)-1}$(Modulus 256)

$\bar{A} = 9 \equiv 9^{\emptyset(256)-1}$(Modulus 256) =

57(Modulus 256) or 9x ≡ 1(Modulus 256)

9 x 57 ≡ 1 (Modulus 256)

Then x = 57 = $\bar{a}$

Encryption 1 will be done using Ceasar Cipher

4.2.1 **Implementation of Ceasar Cipher algorithm**

Plain Text: PARACETAMOL

The first step is to change the plaintext into ASCII code

	P	A	R	A	C	E	T	A	M	O	L
ASCII	80	65	82	65	67	69	84	65	77	79	76
CX	88	73	90	73	75	77	92	73	85	87	84
Ciphertext1	X	I	Z	I	K	M	\	I	U	W	T

Table 4.1: Implementation of Plaintext using Ceasar Technique (Researcher, Kolapo R. 2022)

To get the value of CX we use the mathematical formula;

Where V is the ASCII;

$C \equiv V + 8$ Modulus 256;

$C \equiv 80 + 8$ Modulus 256

$C \equiv 88$Modulus 256

$C \equiv 88$

C = CX.

The above mathematical steps shows are CX is derived for one of the letters in the plaintext.

The output Value which is labeled as CX in the above table is matched to decimal in the ASCII table, so, ciphertext 1 is gotten by having the symbol matched to the decimal numbers of CX in the ASCII table.

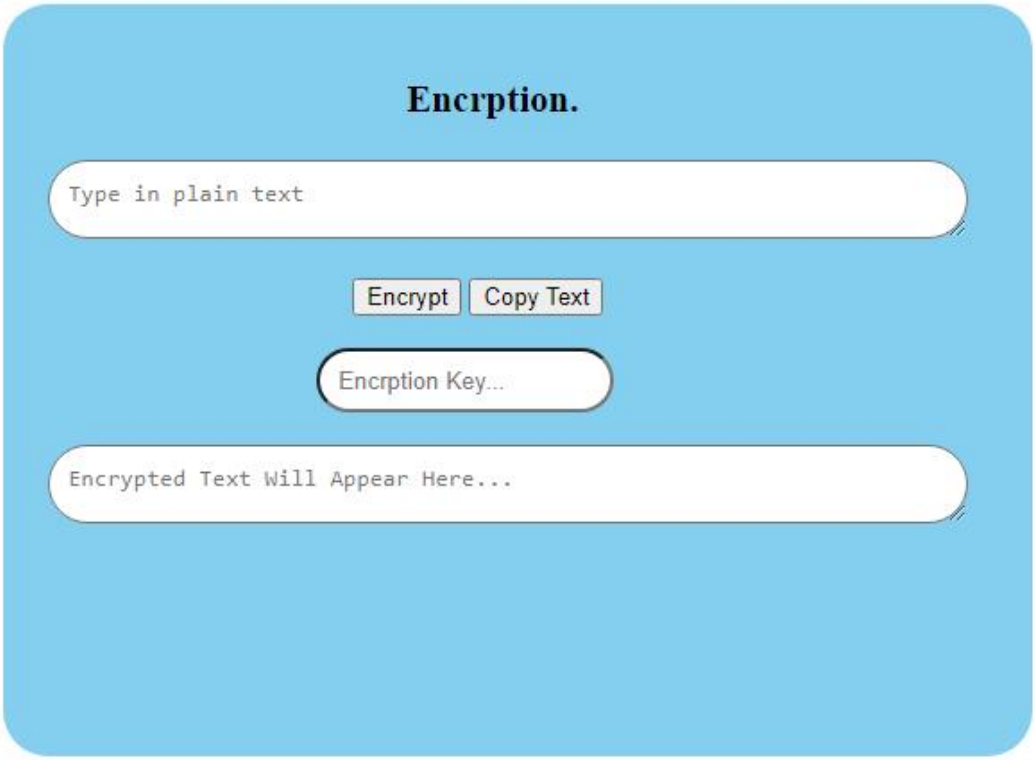


Figure 4.1 Interface showing the Encryption phase for Ceasar Technique (Researcher, Kolapo R. 2022)

Figure 4.1 shows the interface for the encryption process of Ceasar encryption, the figure above is the home phase for the encryption process as this GUI provides the tab for inputting the original text to be scrambled and also a tab to provide the key to be used as for encryption of the plaintetxt.

Figure 4.2 Interface of the Encryption phase showing the Plaintext Input (Researcher, Kolapo R. 2022)

Figure 4.2 showcase the graphical Interface after the plaintext has been inputted and the key has been inserted to be '8'. The encryption key is not pre-determined as it can be any integal number and this same key is used for decryption the scrambled word. This key is communicated by the sender to the receiver through any secure channel as a leak of this key makes the system very vulnerable.

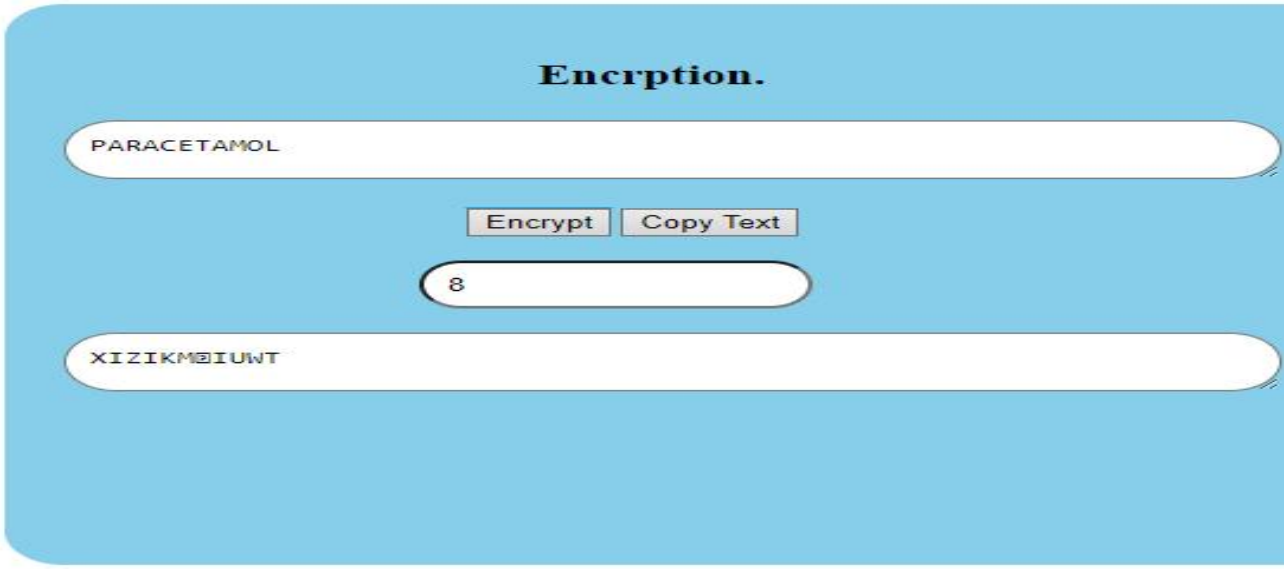


Figure 4.3 Interface of the Encryption phase showing the Plaintext Input and the CipherText Output. (Researcher, Kolapo R. 2022).

The figure above shows the GUI that shows the result of the plaintext after encrypting, the encrypted text is considered the ciphertext 1 and this Ciphertext 1 is used as an input into the next phase of encryption which is the Affine Cipher. The Ciphertext 1 gotten as a result in this user interface is the same as the result calculated manually using the ASCII standard.

4.2.2 **Implementation of Affine Cipher**

Since Ciphertext 1 is obtained from the Ceasar encryption, the Ciphertext 1 serves an a Plaintext for Affine Cipher which means the Plaintext to be encrypted using Affine Cipher is the Ciphertext obtained from the encyrption using Ceasar cipher.

The first step is to change the plaintext (Ciphertext1) into ASCII code

	X	I	Z	A	K	M	\	I	U	W	T
ASCII	88	73	90	73	75	77	92	73	85	87	84
CX	32	153	50	153	171	189	68	153	5	23	252
Ciphertext2	SP	™	2	™	<<	1/2	D	™	ENQ	ETB	ü

Table 4.2 Implementation of Ciphertext 1into Ciphertext 2 (Researcher, Kolapo R. 2022)

To obtain the values for CX for Affine Cipher we use the mathematical expression;

Where V is the ASCII;

CX ≡ ((9 * V) + 8)) Modulus 256, 0≤V≤255

CX ≡ ((9 * 88) + 8)) Modulus 256 = 32

CX ≡ ((9 * 73) + 8)) Modulus 256 = 153

CX ≡ ((9 * 90) + 8)) Modulus 256 = 50

CX ≡ ((9 * 73) + 8)) Modulus 256 = 153

CX ≡ ((9 * 75) + 8)) Modulus 256 = 171

CX ≡ ((9 * 77) + 8)) Modulus 256 = 189

CX ≡ ((9 * 92) + 8)) Modulus 256 = 68

CX ≡ ((9 * 73) + 8)) Modulus 256 = 153

CX ≡ ((9 * 85) + 8)) Modulus 256 = 5

CX ≡ ((9 * 87) + 8)) Modulus 256 = 23

CX ≡ ((9 * 84) + 8)) Modulus 256 = 252

4.3 Implementation of the decryption Algorithm (Affine Decryption)

To have the Ciphertext decrypted, we decrypt the ciphertext 2 first by converting the ciphertext 2 into ASCII code, then using the mathematical expression;

T ≡ (57(CX - 8) Modulus 256, 0≤CX≤255

4.3.1 Implementation of the Affine Decryption

Ciphertext2		™	2	™	<<	1/2	-	™	ENQ	ETB	ü
ASCII	32	153	50	153	171	189	68	153	05	23	252
	88	73	90	73	75	77	92	73	171	87	84
Plaintext 1	X	I	Z	I	K	M	\	I	<<	W	T

Table 4.3 Implementation of Ciphertext 2 into Plaintext 1(Researcher, Kolapo R. 2022)

Using the mathematical expression; T ≡ (57(C - 8)Modulus 256, 0≤C≤255

Where C is the ASCII;

T ≡ (57 (32 - 8) Modulus 256 = 88

T ≡ (57 (153 - 8) Modulus 256 = 73

T ≡ (57 (50 - 8) Modulus 256 = 90

T ≡ (57 (153 - 8) Modulus 256 = 73

T ≡ (57 (171 - 8) Modulus 256 = 75

T ≡ (57 (189 - 8) Modulus 256 = 77

T ≡ (57 (68 - 8) Modulus 256 = 92

T ≡ (57 (153 - 8) Modulus 256 = 73

T ≡ (57 (05 - 8) Modulus 256 = -171

T ≡ (57 (23 - 8) Modulus 256 = 87

T ≡ (57 (252 - 8) Modulus 256 = 84

From the result obtained above, the digits are now converted using the ASCII table to obtained the text for Plaintext .

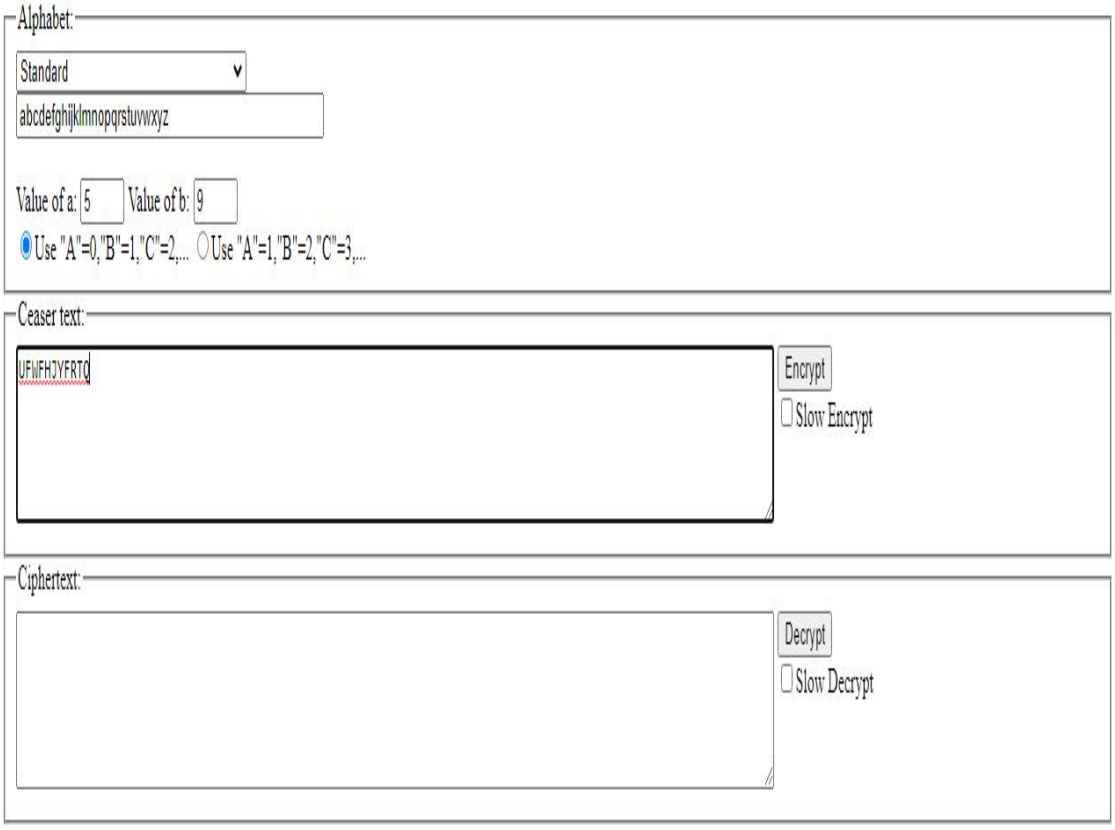


Figure 4.5 Interface showing Affine Ciphertext with ciphertext from Ceasar being its input (Researcher, Kolapo R. 2022)

The figure above is the user interface showing the Affine encryption phase, where the output from the previous encryption which is Ceasar encryption is the input for this phase, and key used in this encryption phase are also determined by the user and this keys are not pre-determined also.

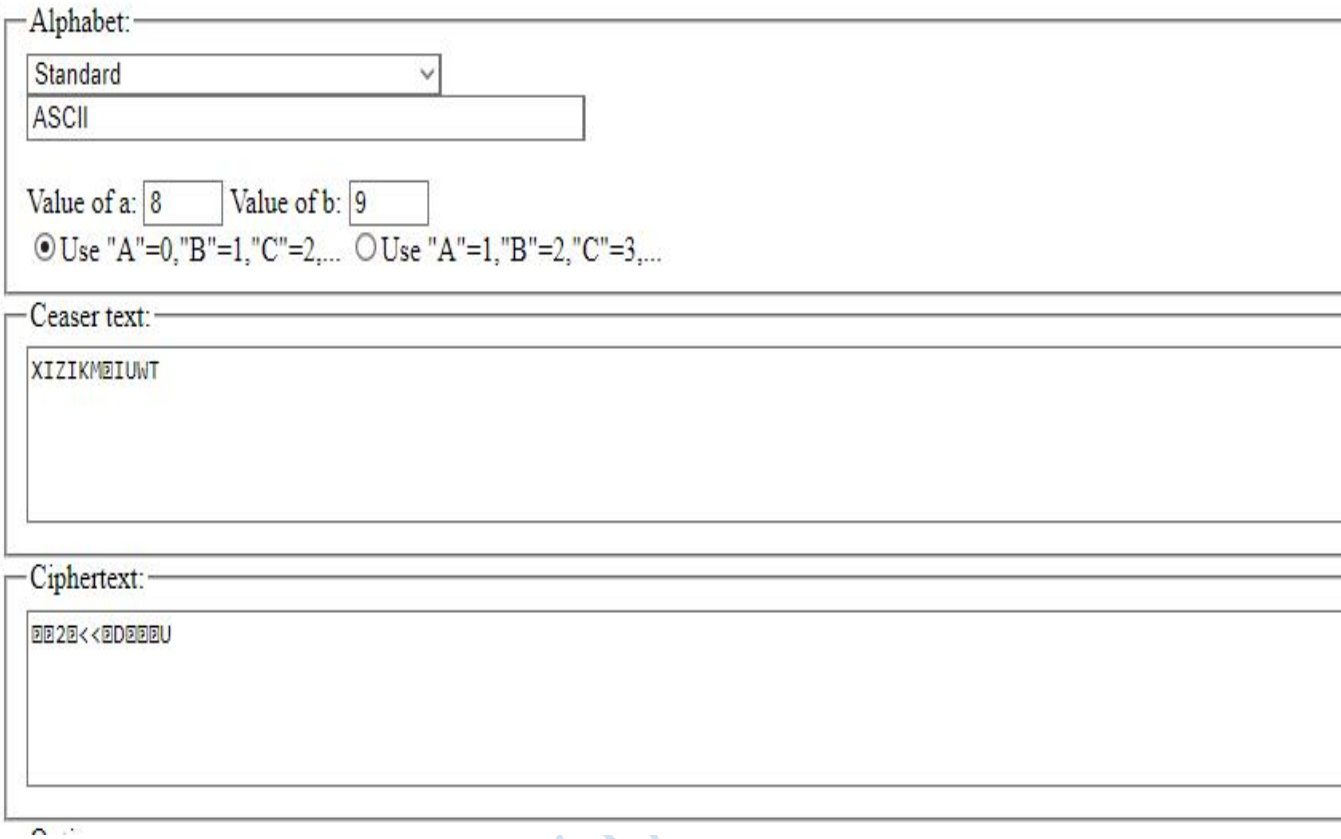


Figure 4.6 Interface showing Affine Implementation showing the Input text and the output text. (Researcher, Kolapo R. 2022).

The figure above showcase the second layer of the encryption stage which is the Affine cipher encryption, this phase uses two keys for encryption and decryption as shown above the output from the first cipertext is fed in as an input into this phase to be encrypted and the ciphertext is provided as the result of the encryption. The result provided from the figure above is the ciphertext 2.

4.3.1 **Decryption using Ceasar Cipher**

The plaintext Obtained from the decryption process using Affine cipher is seen as a ciphertext and is decrypted using Ceasar Cipher.

Fisrtly, this ciphertext is changed into numbers and then this mathematical expression is applied;

$P \equiv (V - k)$ Modulus 256, $0 \leq C \leq 255$

Where V is the ASCII

And we know k to be 8;

Plaintext1	X	I	Z	I	K	M	\	I	<<	W	T
ASCII	88	73	90	73	75	77	92	73	85	87	84
Px	80	65	82	65	67	69	84	65	77	79	76
Plaintext2	P	A	R	A	C	E	T	A	M	O	L

Table 4.4 Implementation of Ciphertext 2 into Plaintext Using Ceasar Technique (Researcher, Kolapo R. 2022)

The Obtained Plaintext is accurate after been passed through the Ceasar encryption and Affine Cipher encryption.

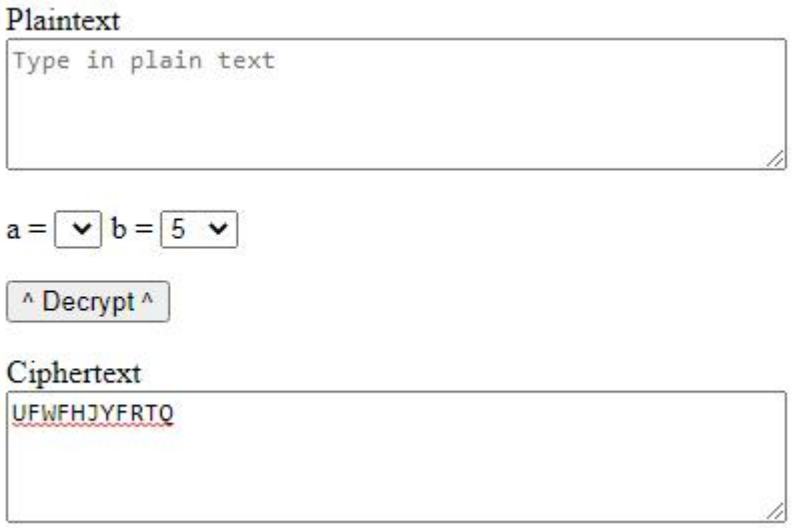


Figure 4.7 Interface showing the implementation of Ciphertext 2 into the Orignal plaintext (Researcher, Kolapo R. 2022)

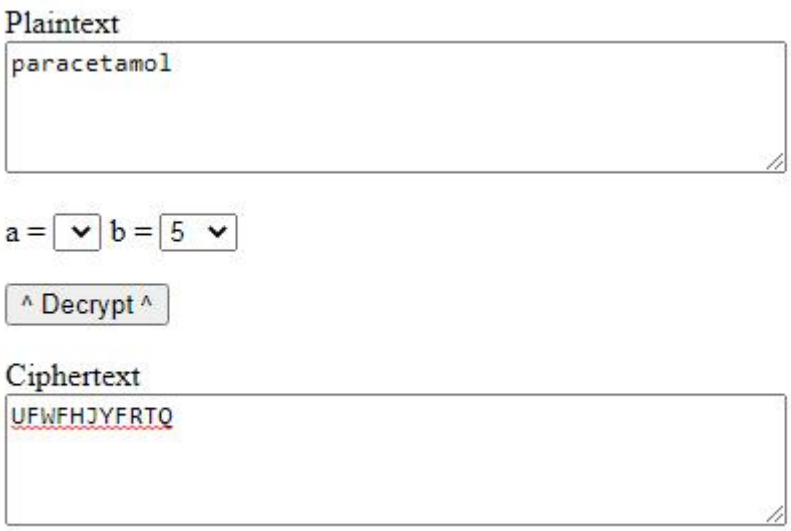


Figure 4.8 Interface showing the implementation of Ciphertext 2 into the Orignal plaintext (Researcher, Kolapo R. 2022)

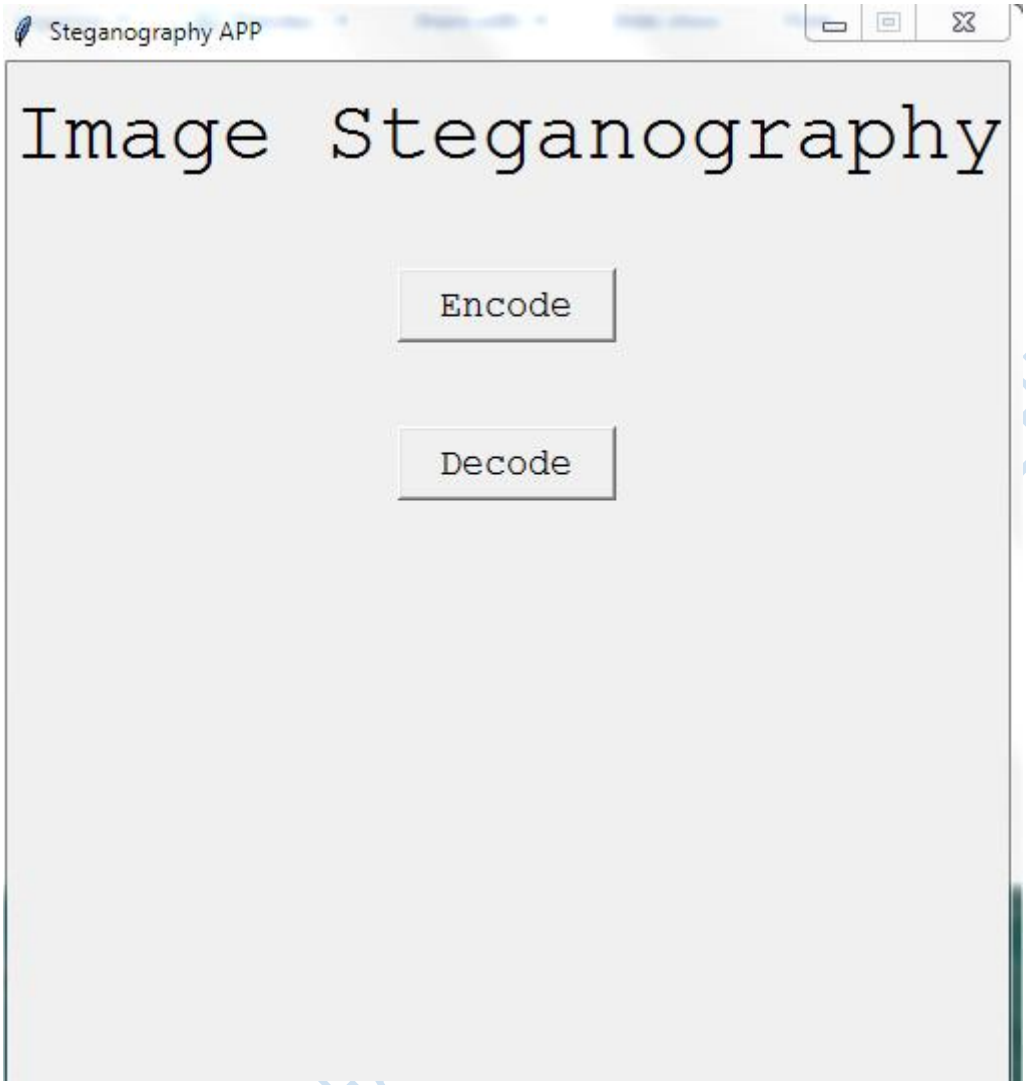


Figure 4.9 Interface showing the steganography Technique page (Researcher, Kolapo R. 2022)

The figure above is the interface for the steganography phase of this study. This interface provides the user with the flexibility to either encode certain text into an image or the extract the text out of the image using the encode button as shown in the figure above.

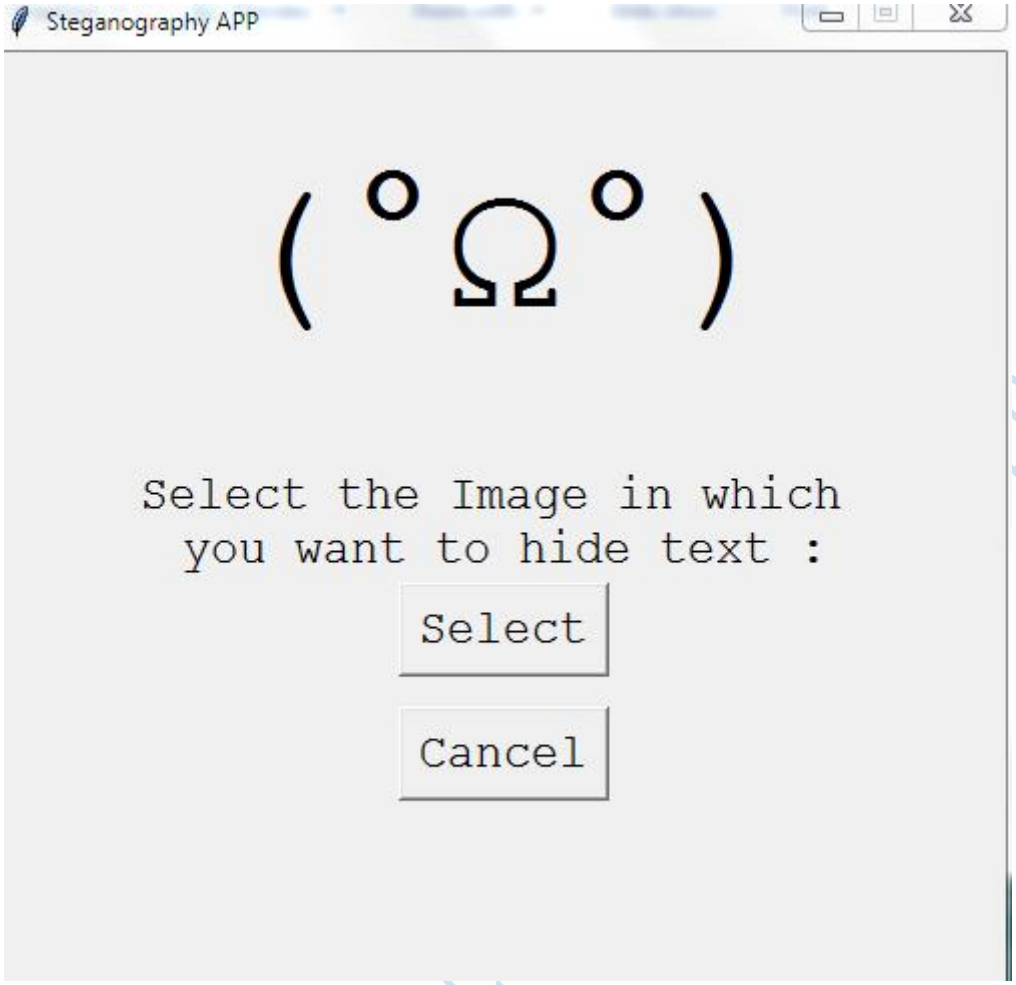


Figure 4.10 Interface showing the "SELECT IMAGE" phase for the steganography Technique (Researcher, Kolapo R. 2022)

The interface above allows the user to select image to be used for the hiding of the text, one of the most interesting and flexible part of this phase is that it allows user to select any image from the users computing device as this design does not limit the user to just certain image to be used for hiding text into the image.

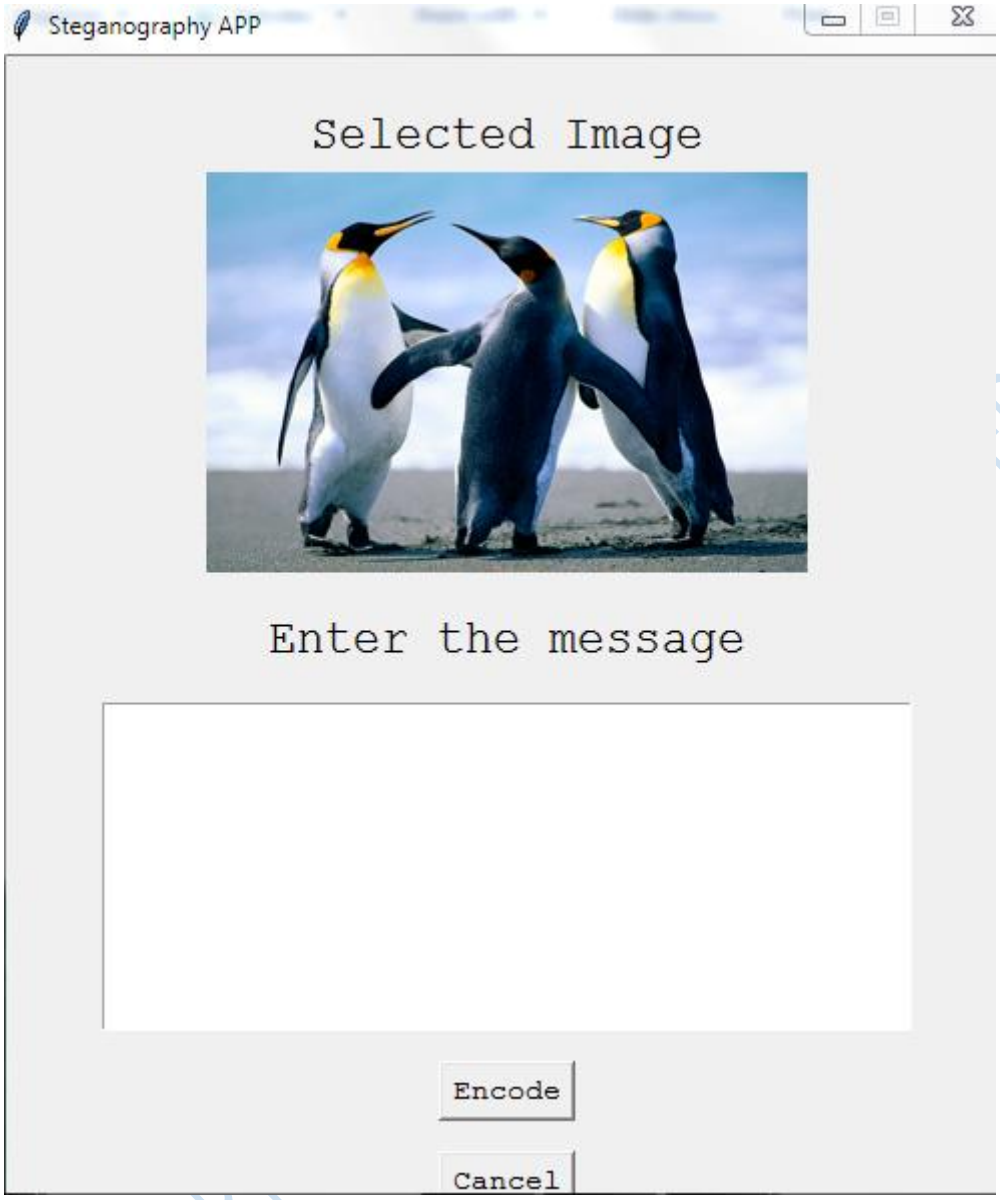


Figure 4.11 Interface Showing the "SELECTED IMAGE" where text is to hidden (Researcher, Kolapo R. 2022)

The figure above shows how the interface looks like after an image has been selected from the list of mages on the users device. The image presented above is the image that will house or hide the text in this study.

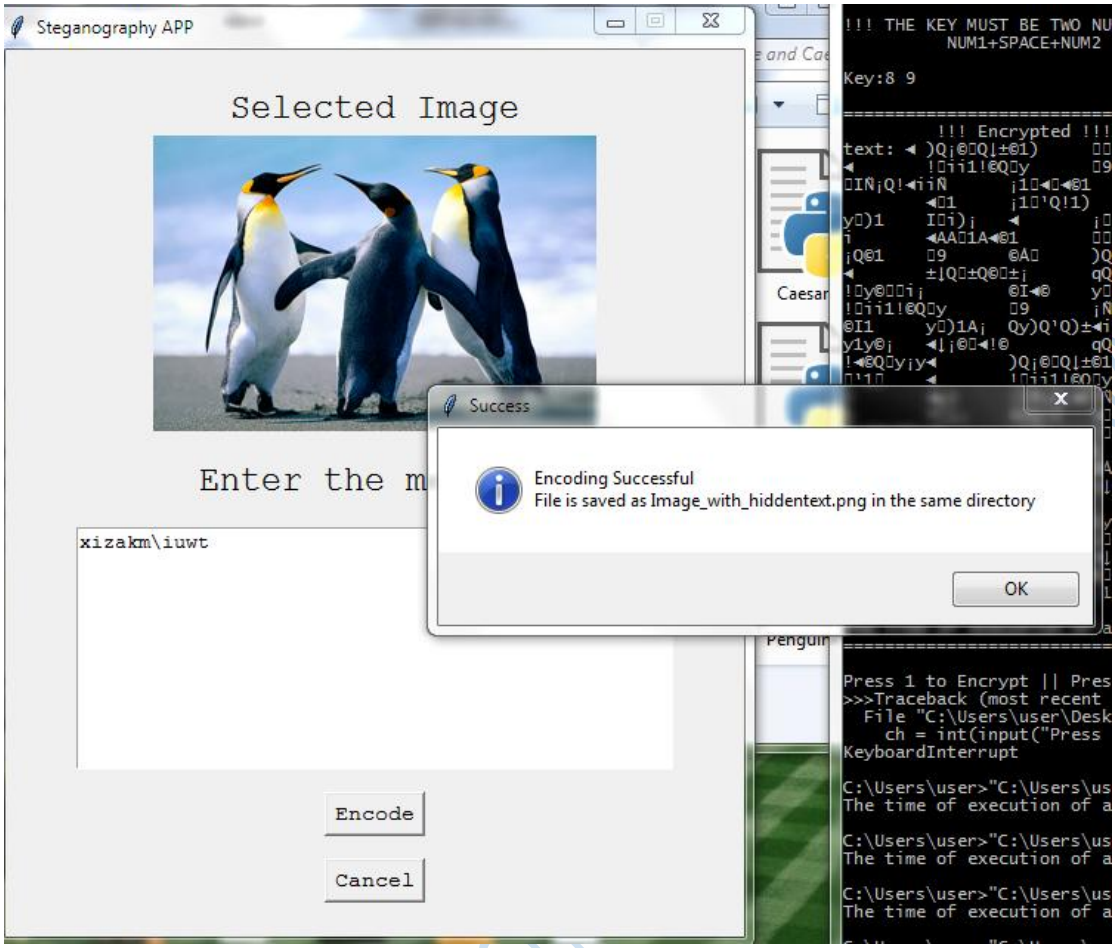


Figure 4.12 Interface showing the Encoding Phase with the Success message (Researcher, Kolapo R. 2022)

The figure above shows two things, the first activity shown in the above figure is the ciphertext to be hidden in the image, which is the ciphertext 2 from the resultant of the cryptographic technique used in this study. The second activity is the success message showed to indicate that the text has been successfully encoded into the image. Without the success message been presented there is no way the user can confirm the operation of hiding the text into an image was successfully carried out.

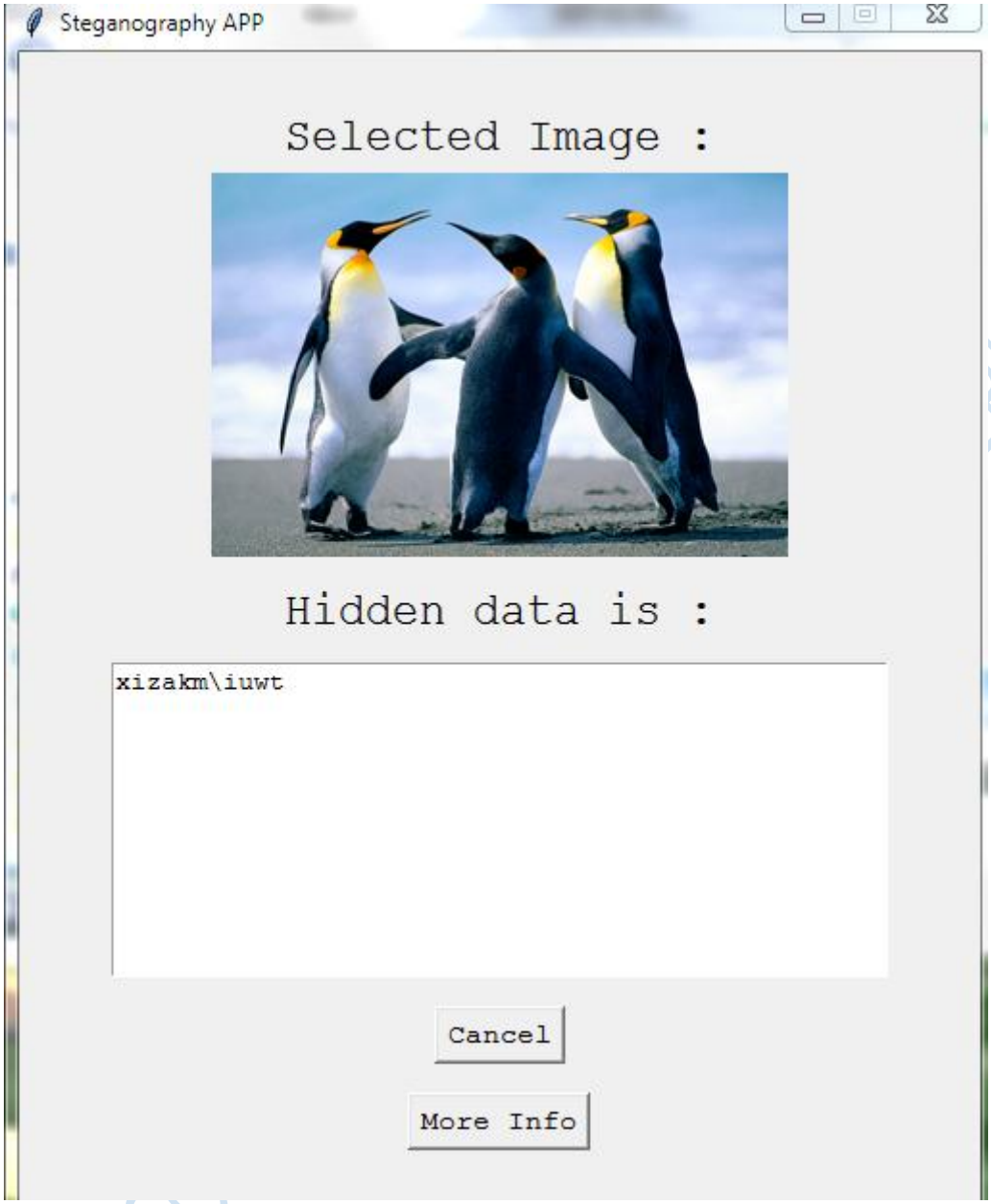


Figure 4.13 Interface showing the retrieved message from the Selected Image (Researcher, Kolapo R. 2022)

Word Length	Encoding Time (ms)	Decoding Time (ms)	Accuracy %
11	28.41	26.02	100
687	27.72	27.53	100
1374	32.51	31.05	100

Table 4.5 Table showing the Encryption and Decryption Time analysis for Ceasar Cipher (Researcher, Kolapo R. 2022)

The above table shows the size of the word length used (which is the number of characters in the plaintext used for the encryption process),the encryption and decryption time analysis for the enhanced Ceasar Cipher technique and the accuracy of Ceasar Cipher.

This accuracy was calculate using the mathematical setup below;

$$\frac{\text{WordLenght of Plain text}}{\text{Word Length of Cipher text}} * 100$$

Word Length	Encoding Time (ms)	Decoding Time (ms)	Accuracy %
11	19.17	19.10	100
687	11.46	11.01	100
1374	35.23	36.44	100

Table 4.6 Table showing Encryption and Decryption time analysis for Affine Cipher (Researcher, Kolapo R. 2022)

The above table shows the size of the word length used (which is the number of characters in the plaintext used for the encryption process),the encryption and decryption time analysis for Affine Cipher technique and the accuracy of Affine Cipher. This accuracy was calculate using the mathematical setup below;

$$\frac{\text{WordLenght of Plain text}}{\text{Word Length of Cipher text}} * 100$$

Word Length	Encoding Time (ms)	Decoding Time (ms)	Image Dimension Before encoding	Image Size Before encoding(kb)
11	30.15	16.62	1024*768	760
687	52.95	19.19	1024*768	760
1374	46.42	14.36	1024*768	760

4.7 Table showing Word Length, Encoding Time, Decoding Time and Dimension of the Steganography Image (Researcher, Kolapo R. 2022)

The table above shows the Word Length which is the number of characters of the Ciphertext embedded in the image, the time analysis taken to hide this text into the image which is captured as the encoding time, the time it takes to extract this text back from the image, which is recorded as the decoding time, the Dimension of the image before hiding the text into the image and the size of the image on disk before hiding the text into the image.

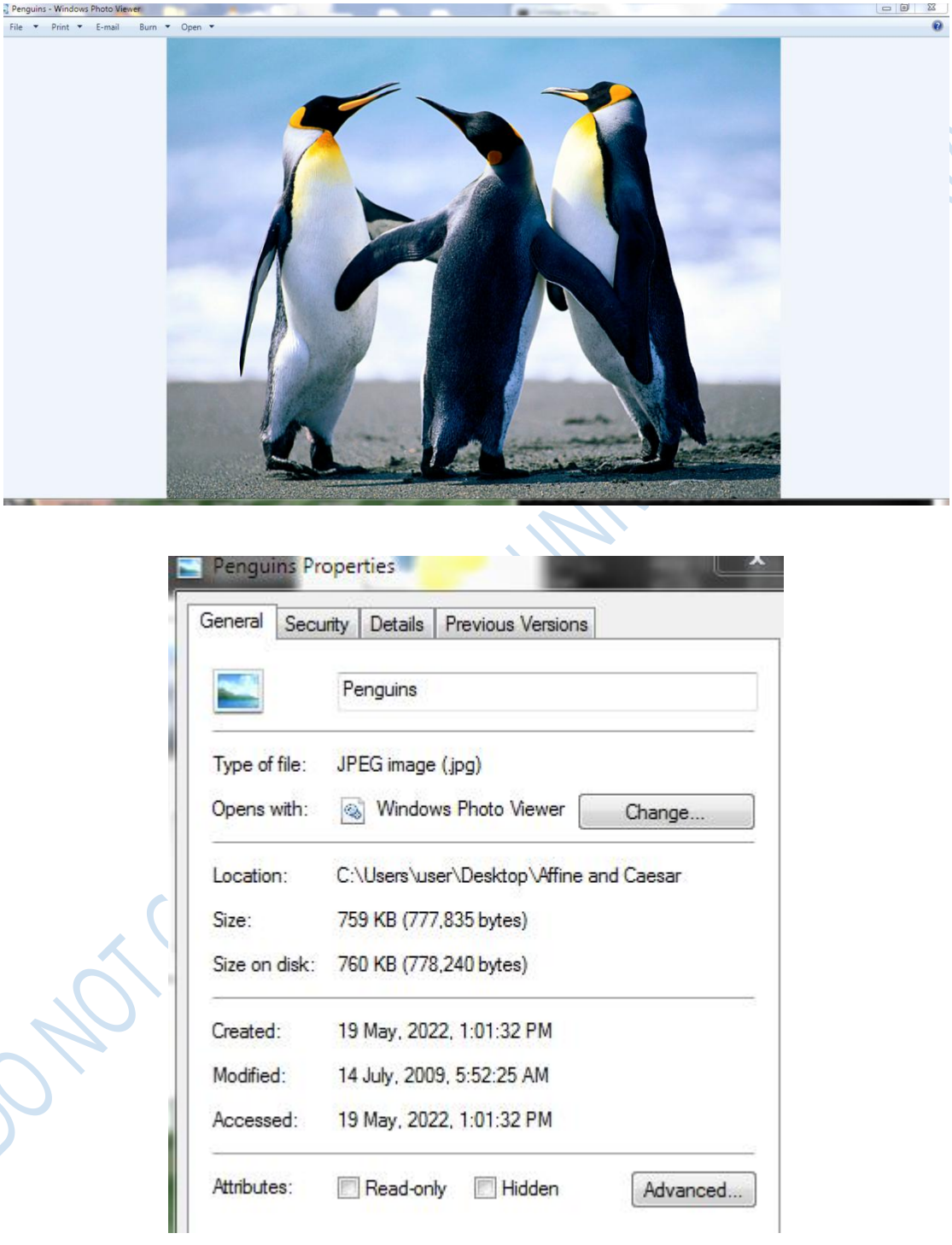
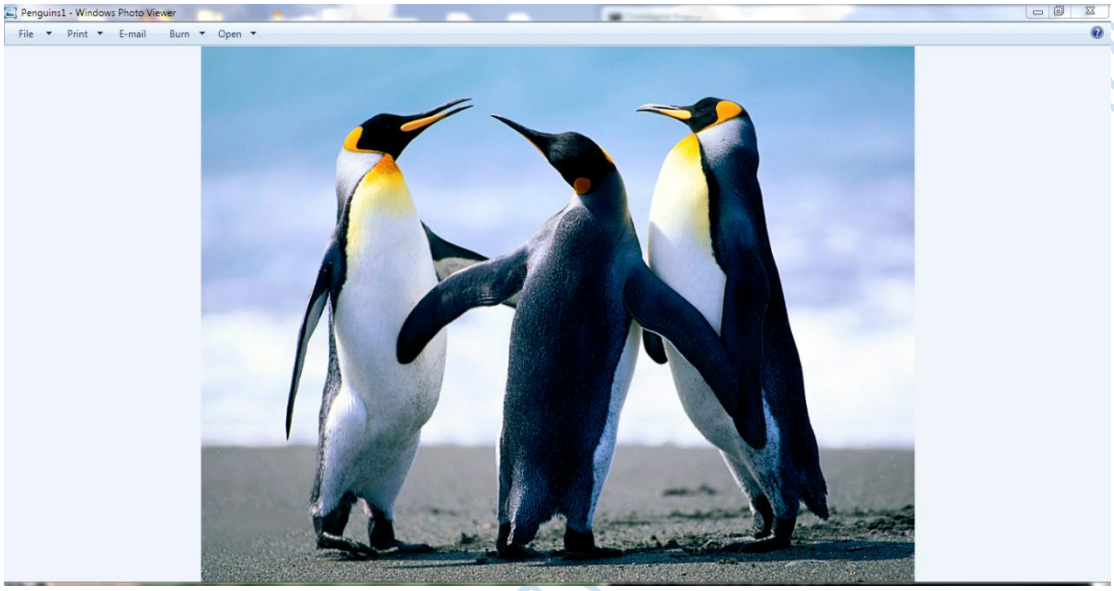


Figure 4.14 Image showing Properties of the SELECTED IMAGE before image hiding (Researcher, Kolapo R. 2022)

The figure above shows the properties of the image used for encoding before the encryption process was carried out. The size of the image used on disk is of priority in this study as this size allows us to know if the image is actually holding something or not .



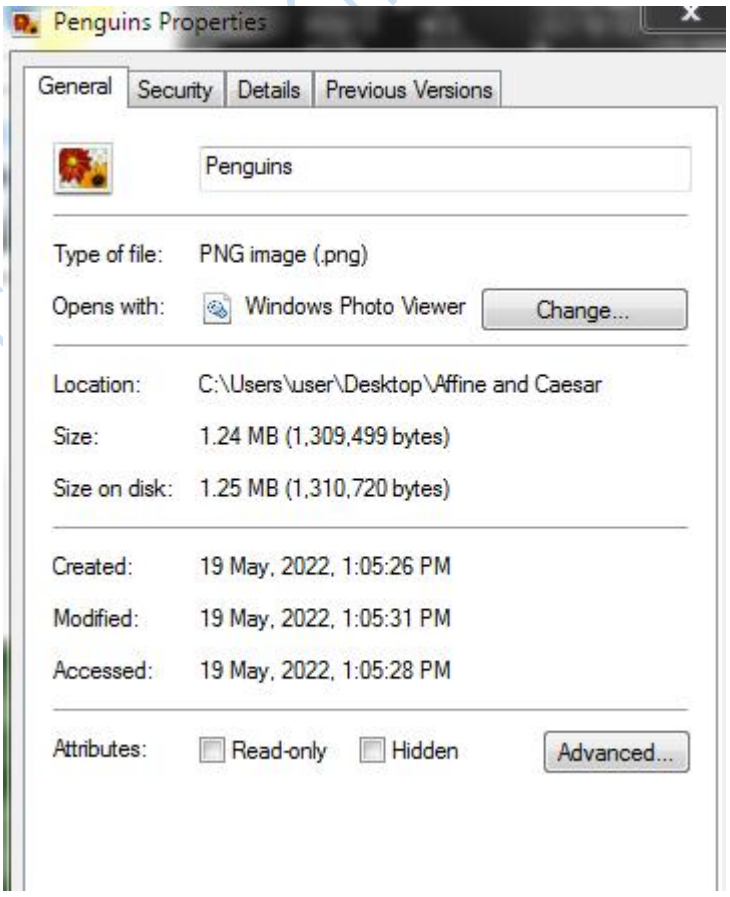
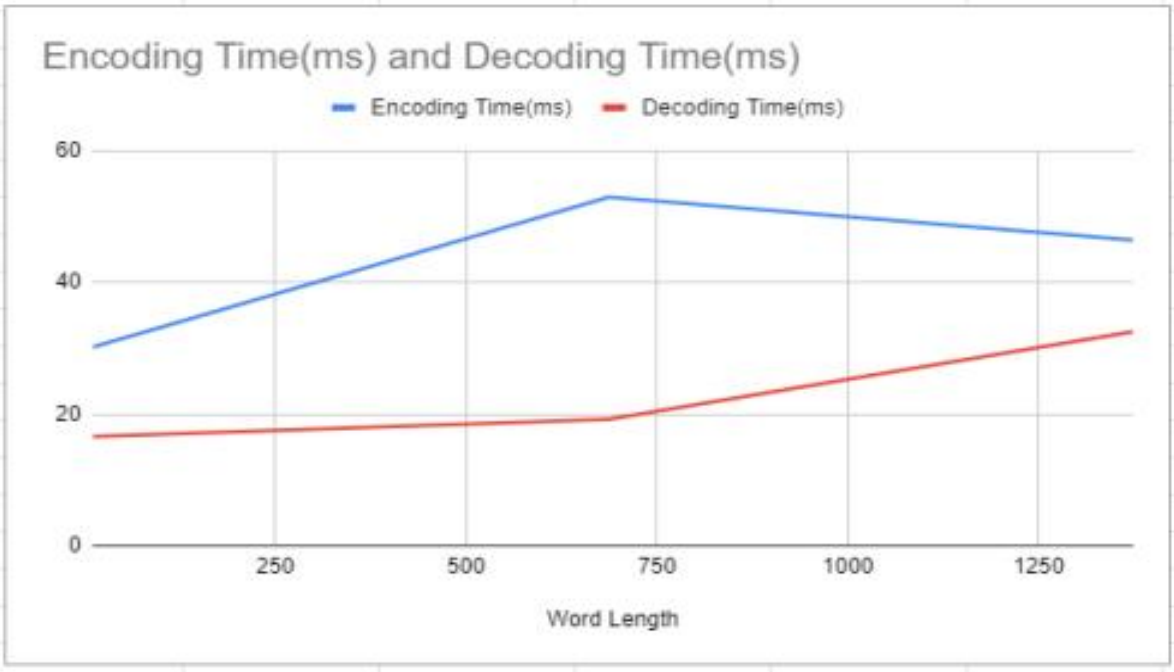


Figure 4.15 Image showing Properties of the SELECTED IMAGE after image hiding (Researcher, Kolapo R. 2022)

The interface above shows the properties of the image after the encryption process has been carried out, this properties shows what the image dimension and size is after text has been hidden into it.

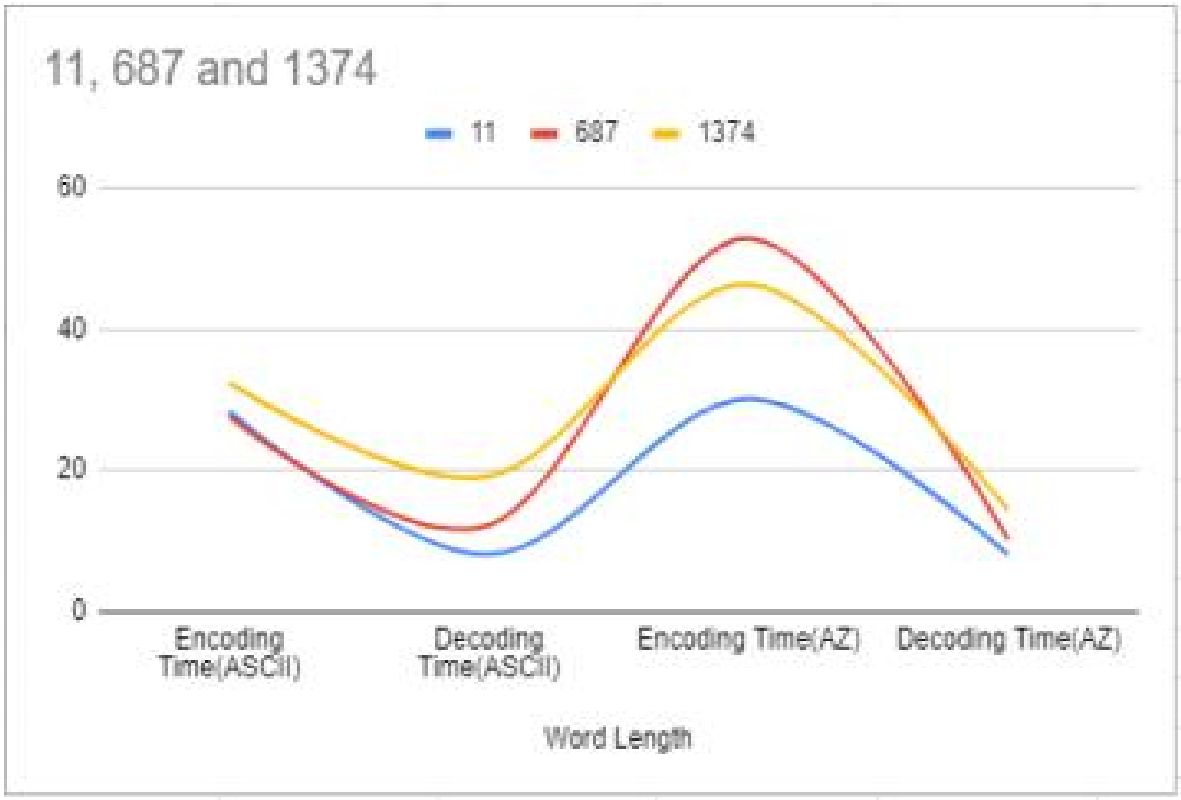
Word Length	Encoding Time (ms)	Decoding Time (ms)	Image Dimension Before encoding	Image Size Before encoding(mb)
11	30.15	16.62	1024*768	1.24
687	52.95	19.19	1024*768	1.24
1374	46.42	14.36	1024*768	1.24

4.8 Table showing Word Length, Encoding Time, Decoding Time and Dimension of the Steganography Image after encoding. (Researcher, Kolapo R. 2022)



The table above shows the Word Length which is the number of characters of the Ciphertext embedded in the image, the time it takes to hide this text into the image

which is captured as the encoding time, the time it takes to extract this text back from the image, which is recorded as the decoding time, the Dimension of the image after hiding the text into the image and the size of the image on disk after hiding the text into the image.



The graph above is a representation of the encoding time and the decoding of the enhanced Ceasar Cipher used in this study. The Ceasar cipher used in this study uses ASCII standard for its alphabet shift as Ceasar shift is considered mono-alphabetic. The graph shows the trend of the Ceasar cipher used in this study as against the conventional Ceasar cipher that uses just 25 letter alphabets which allows for just 25 possible shifts. The above visualization helps shows the comparison.

4.4 Parameters of Evaluation

The parameters used for evaluating the Steganography technique which encompasses the original image and the encoded image are accuracy, precision, recall, and F1-score.

Accuracy

Accuracy = (TP + TN)/ (TP + TN + FP + FN)

The number of correctly classified data instances divided by the total number of data instances is known as accuracy.

Precision

Precision is the amount of information provided by a number in terms of its digits; it indicates how near two or more measurements are to each other. It is unaffected by accuracy.

Precision=TP/(TP + FP)

Recall

The fraction of relevant instances that were retrieved is known as recall (also known as sensitivity).

Recall = TP/ (TP + FN)

F1-Score

The harmonic mean of precision and recall is used to get the

F1 score.

F1=(2*precision*recall)/(precision + recall)

The table below shows the evaluation of the steganographic technique as against another technique was is referred to as pixel based algorithm.

Evaluation Parameters	Red2 Steganography	Pixel Based Steganography
Accuracy	98.9921	99.5387
Precision	98.0902	99.0218
Recall	99.9288	99.9292
F1- Score	98.000	99.4734

Table 4.9 Table showing the performance evaluation of the developed system

From Table 4.9 above, it is observed that the image quality parameter values of the developed system is lesser than that of the pixel based algorithm steganography technique. This is due to the fact that the developed system using Red2 steaganographic technique encrypts the secret message by replacing the characters with other characters that are often outside the English Alphabet domain. The added security compensates for the reduced image quality.

Chapter Five

Conclusion

5.1 Conclusion

The combination of Ceasar Cipher encryption technique alongside Affine cipher encryption technique used as a cryptographic technique in this study makes it difficult to solve sensitive medical data that are encoded using this two technique. If solving Caesar cipher comes within a short time using any of the bruteforce attacks, combining the ceasar cipher encryption technique with Affine cipher makes it more difficult to break and even if there will be any successful attack on this two encryption techniques then the computational time to attack both technique will be higher or greater than the time it will take to attack just one of these technique, and if we have attacks taking longer time then before the success the admin of the system might have been aware that there is any intruder breaking the layers of encryption. This study did not stop at combining Ceasar and Affine Cipher but also employ the use of a watermarking technique to help strengthen the security of the medical data that is been stored using this technique. If we keep having techniques that can be combined to protect our medical data then we should not be scared to share our medical data over the internet with whom we are pleased to shared it with so far the necessary technologies are in place and necessary precautions are taken. Ceasar cipher can be integrated with other encryption algorithm with the likes of AES, RSA and co. The combination of Caesar ciphers and other algorithms is secure, and given that other algorithms combined with other algorithms cover the rest of the Caesar ciphers, there is not much need to combine Caesar ciphers with other cryptographic techniques. maybe.

Based on the obvious narrations, it can be deducted that;

1. Combination of ceasr cipher, Affine Cipher and Red2 Algorithm is done to cover for the backlogs of Ceasar cipher technique so that the algorithm created can be more rigorous to solve. The benefit is that affine cipher has three different keys in doing encoding, decoding and shifting and after this is done, Red2 algorithm helps conceal the text/messages in an image.

2. The combination of these 3 techniques can be used to secure sensitive data just like the medical data that is been used as a case scenerio in this study. This was seen from the manual calculation and the implementation of red2 algorithm shown in this study.

3. Ceasar Cipher can be applied with any other algorithm so far it makes the encoding difficult to solve.

5.2 Recommendation

This thesis implements 2 layer encryption technique alongside steganography for exchanging messages and further emphasizes data hiding in images.

The steganograpgy technique used in this thesis can be applied in watermarking, fingerprinting, detection of unauthorized or illegally copied material. The strength of security level achieved in Red2 is very high and third parties will not be able to get back the original hidden information without the software or how it works. Since this steganography technique is considered very high in strength and hidden messages can not been retrieved back to his original form, future works can be done in embedding the text in other media formats such as Audio and Videos as Image was used in this thesis.

5.3 Contribution to Knowledge

This study has contributed to the field of computing and medical health records in the aspect of security and privacy. This study has helped integrate the field of computer security into the record section in the medical field and this will help tackle the breach of security which the medical health record sector has suffered over time. This study has also help contributed greatly to the field of computing by showcasing how good cryptographic techniques can be combined with steganography techniques.

5.4 Area of Further Research

As recommended the steganography technique used in this thesis can be applied in watermarking, fingerprinting, detection of unauthorized or illegally copied material as studies for further works. Also more cryptographic techniques can be combined with the cryptographic techniques used in this thesis to see and evaluate its performances.

Biblography

Journals

Abbas A. & Khan S. U. *A review on the state-of-the-art privacy-preserving approaches in the e-health clouds*. **IEEE Journal of Biomedical and Health Informatics**,2014, *18*(4), 1431-1441.

Abdullah A. *Advanced encryption stAndard (aes) algorithm to encrypt And decrypt data*. **Cryptography and Network Security**, 2017, vol. 16, pp. 1-11.

Abouelmehdi K, Beni-Hessane A, Khaloufi H. *Big healthcare data: preserving security And privacy*. **Journal of Big Data**,2018. 5 (1), 1.

AbuKhousa E., Mohamed N. & Al-Jaroodi J. *e-Health cloud: opportunities And challenges*. ***Future internet**, 2012,* **4**(3): 621-645.

Adeagbo M. A., Akinsola J.E.T., Awoseyi A. A & Kasali F. *Project Implementation Decision Using Software Development Life Cycle Models: A Comparative Approach*. **Journal of Computer Science and its Application**. Vol 28.2021.

Ahvanooey M. T, Li Q, Hou Q, Mazraeh H. D, Zhang J. *AITSteg: An innovative text steganography technique for hidden transmission of text message via social media*. **IEEE Access** 2018, 6, 65981–65995.

Alanazi N & Khan E. Gutub A. *Inclusion of unicode stAndard seamless characters to expAnd arabic text steganography for secure individual uses*. **J. King Saud Univ. Comput. Inf. Sci.** 2020.

Alanazi N, Khan E, Gutub A. *Efficient security And capacity techniques for Arabic text steganography via engaging Unicode stAndard encoding. Multimed*. **Tools Appl**. 2020, 80, 1403–1431.

Al-Azzawi A. F. *A multi-layer arabic text steganographic method based on letter shaping*. **Int. J. Netw. Secur. Its Appl. (IJNSA)** 2019,11.

Al-gohany N. A. & Almotairi S. *Comparative Study of Database Security in Cloud Computing Using AES And DES Encryption Algorithms.* **Journal of Information Security and Cybercrimes Research**, 2019 vol. 2, no. 1, pp. 102-109.

Al-Nofaie S, Gutub A, Al-Ghamdi M. *Enhancing Arabic text steganography for personal usage utilizing pseudo-spaces*. **J.King Saud Univ.-Comput. Inf. Sci**. 2019, 33, 963–974.

Alotaibi Y. & Federico F. *The impactof health technology on patient safety*. **Saudi Med J**: 38(12), 2017, 1173-1180.

Asija R. & Nallusamy R. A Survey on Security and Privacy of Healthcare Data, 2014.

Azeez N. & Venter I. *Towards ensuring scalability, interoperability And efficient access control in a multi-domain grid-based environment.* **SAIEE Afr Res J** 2013:54–68.

Azeez N. A & Babatope A. B. *An alternative approach to network intrusion detection*. **J Comput Sci Appl Int J Nigeria Comput Soc** 2016:129–43.

Azeez N. A, & Van der Vyver C. *Security And privacy issues in e-health cloud-based system: A comprehensive content analysis*. **Egyptian Informatics Journal**,2019, 20(2): 97-108.

Azeez N. A., Iliyas H. D. *Implementation of a 4-tier cloud-based architecture for collaborative health care delivery*. **Nigerian J Technol Dev** 2016;13(1):17–25.

Badr S, Gomaa I. & Abd-Elrahman E. *Multi-tier blockchain framework for IoT-EHRs systems*. **Procedia Computer Science**, 2018, 141: 159-166.

Balapure R. S. & Khodke P. *Privacy Preservation Of E-Health Care System In Cloud*, **Exchange**,2017, 4 (3).

Baluja S. *Hiding images in plain sight: deep steganography*. **Advances in Neural Information Processing Systems**, vol. 30, 2017, pp. 2069–2079.

Barua M., Liang X., Lu R., Shen X. *ESPAC: enabling security And patient-centric access control for e-Health in cloud computing*. **Int J Security Netw** 2011,67–76.

Bhartiya S, Mehrotra D, Girdhar A. Proposing hierarchy-similarity based access control framework: *A multilevel Electronic Health Record data sharing approach for interoperable environment.* **Journal of King Saud University – Computer and Information Sciences**, 2019, 1-15.

Bhat D, Krithi V, Manjunath K.N, Prabhu S, Renuka A. *Information hiding through dynamic text steganography And cryptography*. **Comput. Inform**. 2017, 1826–1831.

Bhawar S. & Joshi K.. "*A review on cloud security based encryption And decryption techniques.* **International Journal of Engineering Research and Technology** 2021, Volume 10, Issue 02.

Cao S, Zhang G, Liu P, Zhang X, & Neri F. *Cloud-assisted secure eHealth systems for tamper-proofing EHR via blockchain*. **Information Sciences**,2019, 485: 427- 440.

Chandrashekhar A.M & Shashikumar. *Cloud computing service And deployment Models.* **International journal for research in applied science and engineering technology**, 2017**,** Vol 5, Issue VI.

Chaw A. A. *Text steganography in Letter of Credit (LC) using synonym substitution based algorithm*. **Int. J. Adv. Res. Dev**.2019, 4, 59–63.

Chen M. *Privacy protection And intrusion avoidance for cloudlet-based medical data sharing*. **IEEE transactions on Cloud computing**,2018, 113, 48-52.

Chinnasamy P, Padmavathi S, Swathy R & Rakesh S. *Efficient Data Security Using Hybrid Cryptography on Cloud Computing.* **In Inventive Communication and Computational Technologies, Springer**,2021, pp. 537-547.

Dalal M. & Juneja M. "*A secure video steganography scheme using DWT based on object tracking*. ***Information Security Journal: A Global Perspective***, no. 1, 2021,pp. 1–18.

DeChaves S. A, Westphall C. B, Westphall C. M, Gerônimo G. A.. *Customer Security Concerns in Cloud Computing*. **IARIA.** 2011, 978-1-61208-113-7.

Dhanabagyam S. N. & Karpagam G. R. *Secure Communications for e-Health in Mobile Cloud Computing Using Provable Security*. ***International Journal of Pure And Applied Mathematics****,* 2017*,* **114**(7): 325-335.

Ditta A., Yongquan C., Azeem M., Rana K. G., Yu H., Memon M. Q. *Information hiding: Arabic text steganography by usingUnicode characters to hide secret data*. **Int. J. Electron. Secur. Digit. Forensics** 2018, 10, 61–78.

Dixit P., Gupta A. K., Trivedi M. C., Yadav V. K. *Traditional And hybrid encryption techniques: a survey.* **in Networking communication and data knowledge engineering, Springer**,2018, pp. 239-248.

Dong S., Wang P & Abbas K., *A survey on deep learning and its applications*, **Computer Science Review**, vol. 40, no. 1, Article ID 100379, 2021.

Drozdowicz M, Ganzha M, & Paprzycki M. *Semantically enriched data access policies in eHealth*. **Journal of medical systems**, 2016, 40(11): 238.

Ekodeck S. G. R & Ndoundam R. *Steganography based on Chinese Remainder Theorem*. **J. Inf. Secur. Appl**. 2016, 29, 1–15.

Fan L., Lo O, Buchanan W, Ekonomou E, Sharif T, Sheridan C. *Protecting Patient Privacy for e-Health Services in the Cloud*. **SPoC**:, 2014, pp. 1–6.

Fateh M. & Rezvani M. *An email-based high capacity text steganography using repeating characters*. **Int. J. Comput. Appl**. 2021, 43, 226–232.

Fernández-Alemán J. L., Señor I. C., Lozoya P. A. O. & Toval A. *Security And privacy in electronic health records: A systematic literature review.* **Journal of biomedical informatics***, 2013,* 46(3): 541-562.

Fridrich J., Goljan M & Rui Du D. *Detecting LSB steganography in color, and gray-scale images*. **IEEE Multimedia**, vol. 8, no. 4, 2001, pp. 22–28.

Gai K. & Qiu M. *Blend arithmetic operations on tensor-based fully homomorphic encryption over real numbers*. **IEEE Trans Ind Inf** 2018;14(8):3590–8.

Gai K., Qiu M., Sun X. *A survey on FinTech.* **J Netw Comput Appl** 2018, 103 :262–73.

Gutub A. A & Alaseri K.A. *Refining Arabic text stego-techniques for shares memorization of counting-based secret sharing*. **J.King Saud Univ.-Comput. Inf. Sci**. 2019.

Hamzah A. A, Khattab S & Bayomi H. *A linguistic steganography framework using Arabic calligraphy*. **J. King Saud Univ.-Comput.Inf. Sci**. 2021, 33, 865–877.

Hidayat T. & Mahardiko R. *A Systematic literature review method on aes algorithm for data sharing encryption on cloud computing.* **International Journal of Artificial Intelligence Research**, 2020, vol. 4, no.1, pp. 49-57.

Hu Y. & Bai G.. *A systematic literature review of cloud computing in e-Health*", **Health informatics-An international journal (HIIJ)** Vol 3, No 4. 2019.

Jayapandiyan J. R, Kavitha C, Sakthivel K. *Enhanced least significant bit replacement algorithm in spatial domain of steganography using character sequence optimization*. **IEEE Access** 2020, 8, 136537–136545.

Jian Y., Ni J., & Yang Y. *Deep learning hierarchical representations for image steganalysis*. **IEEE Transactions on Information Forensics And Security**, vol. 12, no. 11, 2017, pp. 2545–2557.

Joshua V. & Gamm L. D. "*Health Information Exchange: Persistent Challenges And New Strategies*." **Journal of the American Medical Informatics Association** 17(3) 2014, 288–94.

Kadhim I. J., Premaratne P., Vial P. J & Halloran B. *Comprehensive survey of image steganography: techniques, Evaluations, and trends in future research*," ***Neurocomputing***, vol. 335, 2019,pp. 299–326.

Kang H, Wu H, Zhang X. *Generative text steganography based on LSTM network And attention mechanism with keywords.* **Electron. Imaging** 2020, 2020, 291.

Karakıs R., Güler I., Çapraz I., Bilir E. *A novel fuzzy logic-based image steganography method to ensure medical data security*. **Comput Biol Med** 2015;172–183.

Keshta I. & A. Odeh. *Security And Privacy of electronic health records: Concern And Challenge*s. **Eyptian Informatics Journal**. 22(2), 2021,177-183.

Khosravi B, Khosravi B, Nazarkardeh K. *A new method for pdf steganography in justified texts*. **J. Inf. Secur.Appl.** 2019, 45, 61–70.

Kim S., Sung M., Chung Y. *A framework to preserve the privacy of electronic health data streams*. **J Biomed Inf** 2014,95–106.

Kyeremeh K. *Overview of system development life cycle models*. **Journal of Management and Science**. 11(1), 2021,12-22.

Li Q., Wang X., & Ma B. *Image steganography based on style transfer and quaternion exponent moments*. ***Applied Soft Computing***, vol. 110, no. 3, Article ID 107618, 2021.

Li Y., Zhang J., Yang Z., Zhang R. *Topic-aware neural linguistic steganography based on knowledge graphs.* **ACM/IMS Trans.Data Sci**. 2021, 2, 1–13.

Liu C. H, Chen T. L, Lin H. Y, Lin F. Q, Liu C. M, Wu E. P. & Chen T. S. *Secure PHR Access Control Scheme in Cloud Computing*. **International Journal of Information and Electronics Engineering**, 2013, 3(3):329.

Liu X, Lu R, Ma J, Chen L, Qin B. *Privacy-Preserving Patient-Centric Clinical Decision Support System on Naive Bayesian Classification*. **IEEE J Biomed Health Inf** 2016;20(2).

Liu X., Yang G., Mu Y. & Deng R. H. *Multi-user verifiable searchable symmetric encryption for cloud storage*. **IEEE Transactions on Dependable and Secure Computing** , 2020, 17 (6):1322–32.

Liu Y, Xu Z., Ye W. *Image neural style transfer with preserving the salient regions*. ***IEEE Access***, vol. 7, Article ID 40037, 2019

Liu Z., Weng J. , Li J., Yang J., Fu C. & Jia C. *Cloud-based electronic health record system supporting fuzzy keyword search.* ***Soft Computing****, 2016,* **20**(8): 3243-3255.

Mahato S, Khan D. A, Yadav D. K. *A modified approach to data hiding in Microsoft Word documents by change-tracking technique*. **J. King Saud Univ.-Comput. Inf. Sci**. 2020, 32, 216–224.

Maji G. & Mandal S. *A forward email based high capacity text steganography technique using a rAndomized And indexed word dictionary*. **Multimedia Tools Appl**. 2020, 79, 26549–26569.

Malik A, Sikka G, Verma H. K. *A high capacity text steganography scheme based on LZW compression And color coding*. **Eng.Sci. Technol. Int. J**. 2017, 20, 72–79.

Martínez S, Sánchez D, Valls A. *A semantic framework to protect the privacy of electronic health records with non-numerical attributes*. **J Biomed Inf** 2013:294–303.

Masa'deh R, Shannak R, Maqablach M. & Tarhini A.. "*The impact of knowledge management on job performance in higher education: The case of the University of jordan*. **Journal of enterprise information management**, 2016, 29(6), 120-137.

Naqvi N, Abbasi A. T, Hussain R, Khan M. A, Ahmad B. *Multilayer partially homomorphic encryption text steganography(Mlphe-ts)*: *A zero-steganography approach*. **Wirel. Pers. Commun**. 2018, 103, 1563–1585.

Peleg M, Beimel D, Dori D, Denekamp Y. *Situation-based access control: privacy management via modeling of patient data access scenarios*. **J Biomed Inform** 2008;41:1028–40.

Pooja B. N.. *Secure Mechanism for Medical Database Using RSA*. **International Journal of Application or Innovation in Engineering & Management**, *2014,* **3**(7): 320-327.

Qin J., Luo Y., Xiang X., Tan Y., & Huang H. *Coverless image steganography: A survey*. ***IEEE Access***, vol. 7, no. 99, Article ID 171372, 171394 pages, 2019.

Ramakrishnan N. & Sreerekha B. *Enhancing Security of Personal Health Records in Cloud Computing by Encryption.* **In International Journal of Science And Research (IJSR*), 2013.***

Rezaeibagha F. & Mu Y. D*istributed clinical data sharing via dynamic accesscontrol policy transformation*. **Int J Med Inf** 2016:25–31.

Rezaeibagha F., Win K. T., & Susilo, W. *A systematic literature review on security And privacy of electronic health record systems: technical perspectives*. ***Health Information Management Journal*** *, 2015***,**44(3): 23-38.

Rubio O, Alesanco A, García J. *A robust And simple security extension for the medical stAndard SCP-ECG*. **J Biomed Inf** 2013;142–151.

Sahi A., Lai D., Li Y. *Security And privacy preserving approaches in the eHealth clouds with disaster recovery plan*. **Comput Biol Med** 2016;78:1–8.

Sajay K. R, Babu S. S & Vijayalakshmi Y . *Enhancing the security of cloud data using a hybrid encryption algorithm*. **Journal of Ambient Intelligence and Humanized Computing** , 2019, 1–10.

Shah S. T. A., Khan A., Hussain A. **Text steganography using character spacing after normalization**. **Int. J. Sci. Eng. Res**.2020, 11, 949–957.

Sharma S, Chen K, Sheth A. *Toward practical privacy preserving analytics for IoT And cloud-based healthcare systems*. **IEEE Internet Computing**,2018, 22 (2), 42-51.

Shin M, Jeon H, Ju Y, Lee B, Jeong S. *Constructing RBAC based security model in u-healthcare service platform*. **Sci World J** 2014; 1–13.

Sridevi R. & Nithiya C. *E-Health Security using ECC algorithm.* ***International Journal of Advanced Research in Basic Engineering Sciences And Technology*** *(IJARBEST)*,2016, **2**(19): 114-117.

Sumathi R. & Kirubakaran E. *SCEHSS: Secured Cloud Based Electronic Health Record Storage System with ReEncryption at Cloud Service Provider*. ***International Journal of Computer And Communication Engineering****, 2013,* **2**(2): 162

Taha A, Hammad A. S, Selim M. M. *A high capacity algorithm for information hiding in Arabic text. J. King Saud Univ*. **Comput.Inf. Sci**. 2018, 32, 658–665.

Tamimi A. A., Abdalla A. M & Alallaf O. *Hiding an image inside another image using variable-rate steganography*. **International Journal of Advanced Computer Science And Application***s*, vol. 4, no. 10, 2013, pp. 1–4.

Thimma Reddy B, Bala Chowdappa K., & Raghunath Reddy S. *Cloud Security using Blowfish And Key Management Encryption Algorithm*. **International Journal of Engineering and Applied Sciences.** 2015 ISSN: 2394-3661, Volume-2, Issue-6.

Tommy T., Rosyida R., Lubis I. & Marwan A. "*A Simple Compression Scheme based on ASCII Value Differencing*. **Journal of Physics Conferencing Series**. 1007(1): 012022,2018.

Tsai K. L., Leu F. Y., Wu T. H., Chiou S. S., Liu Y. W. & Liu H. Y. A.. *Secure ECC-based Electronic Medical Record System*. ***J. Internet Serv. Inf. Secur****. 2014,* ***4***(1): 47-57.

Umer M. F, Sher M, Khan I. *Towards Multi-Stage Intrusion Detection using IP Flow Records*. **(IJACSA) International Journal of Advanced Computer Science and Applications.** 2016, Vol. 7, No. 10

Varsha B. S. & Suryateja P.S.. *Using Advanced Encryption StAndard for Secure And Scalable Sharing of Personal Health Records in Cloud*. **International Journal of Computer Science and Information Technologies (IJCSIT)** *,2014,***5**(6): 7745-7747.

Vishwanath A, Peruri R & He J. *Security in fog computing through encryption*. **DigitalCommons@ Kennesaw State University**, 2016.

Wang K & Gao Q. *A Coverless plain text steganography based on character features*. **IEEE Access** 2019, 7, 95665–95676.

Wang X. Ma A., Xhafa J., F., Zhang M., & Luo X. *Cost-effective secure E-health cloud system using identity based cryptographic techniques*. ***Future Generation Computer Systems****, 2017,* **67**: 242-254.

Wencheng S. *Security And privacy in the medical internet of things: a review*. **Security and Communication Networks**. 2018.

Wu N, Yang Z, Yang Y, Li L, Shang P, Ma W, Liu Z. *STBS-Stega: Coverless text steganography based on state transition-binary sequence*. **Int. J. Distrib. Sens. Netw.** 2020. 16.

Xiang L, Wu L, W, Li X., & Yang C. *A linguistic steganography based on word indexing compression And cAndidate selection.Multimed*. **Tools Appl**. 2018, 77, 28969–28989.

Xu C, N, Wang Zhu L, Sharif K. & Zhang C. *Achieving Searchable And Privacy-Preserving Data Sharing for CloudAssisted E-healthcare System*. **IEEE Internet of Things Journal**, 2019, 6(5): 8345-8356.

Xu G., Wu H.-Z & Shi Y.-Q. *Structural design of convolutional neural networks for steganalysis*. **IEEE Signal Processing Letters**, vol. 23, no. 5,2016, pp. 708–712.

Yahya F, Chang V, Walters J, & Wills B, *"Security Challenges in Cloud Storage*, 2014, pp. 1–6.

Yang L, Han Z, Huang Z & Ma J. A remotely keyed file encryption scheme under mobile cloud computing. **Journal of Network and Computer Applications**, *2018,* 106:90–99.

Yang X. L., Guo X, Z, Chen M, Huang,Y, Zhang J. *RNN-Stega: Linguistic steganography based on recurrent neural networks*. **IEEE Trans. Inf. Forensics Secur**. 2018, 14, 1280–1295.

Yang X., Lin G., Liu Y., Nie F & Lin L. *Fast spectral embedded clustering based on structured graph learning for large-scale hyperspectral image*, **IEEE Geoscience And Remote Sensing Letters**, vol. 99, 2020, pp. 1–5,.

Yang Z, Xiang L, Zhang S, Sun X, Huang Y. *Linguistic generative steganography with enhanced cognitive-imperceptibility*. **IEEE Signal. Process. Lett**. 2021, 28, 409–413.

Yang Z. L, Zhang S. Y, Hu Y. T, Huang Y. F. *VAE-Stega: Linguistic steganography based on variational auto-encoder*. **IEEE Trans. Inf. Forensics Secur**. 2020, 16, 880–895.

Zeebaree S. R. *DES encryption And decryption algorithm implementation based on FPGA.* **Indonesian Journal of Electrical Engineering and Computer Science,** 2020 vol. 18, no. 2, pp.774-781, doi: 10.11591/ijeecs.v18.i2.pp774-781.

Zhang R., Dong S., & Liu J. *Invisible steganography via generative adversarial networks*. ***Multimedia Tools And Applications***, vol. 78, no. 7,2019, pp. 8559–8575.

Zhang S., Su S., Lu J., Zhou Q & Chang C. *CSST-Net: an arbitrary image style transfer network of coverless steganography*. **The Visual Computer**, 2021, pp. 1–13,

Zhang Y. "*Book Review: Data Collection Research Methods in Applied Linguistics.* **Sec.education. Front Psychol**. 2021.

Zhong N., Z., Qian Z., & Wang X. Zhang. *Steganography in stylized images*. **Journal of Electronic Imaging**, vol. 28, no. 3, 2019, pp. 1–12.

Zhou X., Peng W., Yang B., Wen J., Xue Y., Zhong P. *Linguistic steganography based on adaptive probability distribution*. **IEEE Trans. Dependable Secur. Comput**. 2021.

Conference Proceedings

Akinyele J. A., Pagano M. W., Green M. D., Lehmann C. U., Peterson Z. N. & Rubin A. D.. *Securing electronic medical records using attribute-based encryption on mobile devices*. **In *Proceedings of the 1st ACM workshop on Security And privacy in smartphones And mobile devices* (ACM)**,2011, pp. 75-86.

Alasaarela E., Nemana R., DeMello S. *Drivers And Challenges of Wireless Solutions in Future Healthcare.* **Proceedings of the 2009 International Conference on eHealth, Telemedicine, and Social Medicine; Cancun, Mexico**. 1–7 February 2009.

Alghamdi N & Berriche L. *Capacity investigation of Markov chain-based statistical text steganography: Arabic language case.* I**n Proceedings of the 2019 Asia Pacific Information Technology Conference, Jeju Island, Korea**, 25–27 January 2019; pp. 37–43.

Alrawais A. *An attribute-based encryption scheme to secure fog communications*. **IEEE access**,2017, 5, 9131-9138.

Alsaadi E. M, Fayadh S. M & Alabaichi A. *A review on security challenges And approaches in the cloud computing.* **InAIP Conference Proceedings**,2020, vol. 2290, no. 1, p. 040022.

Amini S, Verhoeven R, Lukkien J. & Chen S. *Toward a security model for a body sensor platform.* **In: 2011 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA**, 2011, pp. 143–144.

Azeez N. A., Iyamu T., Venter I. M. *Grid security loopholes with proposed countermeasures*. **26th International Symposium on Computer and Information Sciences. London: Springer**; 2011. p. 411–8.

Baawi S. S. & Nasrawi D. A. *Improvement of "text steganography based on unicode of characters in multi-lingual" by custom font with special properties*. **In**

Proceedings of the IOP Conference Series: Materials Science and Engineering, Jonkoping, Sweden, 22–23 June 2020; Volume 870, p. 012125.

Charanya R, Nithya S. & Manikandan N. *Attribute based encryption for secure sharing of E-health data*. **In Materials Science and Engineering Conference Series** 2017, 263(4): 042030.

Charanya R., Nithya S., & Manikandan N. *Attribute based encryption for secure sharing of E-health data*. **In *Materials Science And Engineering Conference Series**, 2017,* 263**(4): 042030.

Chaudhary S, Dave M, Sanghi A. *AggrAndize text security And hiding data through text steganography*. **In Proceedings of the 2016 IEEE 7th Power India International Conference (PIICON), Bikaner, India**, 25–27 November 2016; pp. 1–5.

Chen D., Yuan L., Liao J., Yu N & StyleBank H. G. *An explicit representation for neural image style transfer*. **In Proceedings of the IEEE Conference on Computer Vision And Pattern Recognition, , CVPR), Honolulu, HI, USA**, July 2017, pp. 1–10.

Chen H. Y., Fang I. S. & Chiu W. C., *Self-contained stylization via steganography for reverse and serial style transfer*. ***In Proceedings of the IEEE Winter Conference on Applications of Computer Vision, WACV), Lake Tahoe, NV, USA***, March 2018, pp. 1–15.

Chenthara S, Ahmed K, Wang H. & Whittaker F. *Security And Privacy preserving Challenges of e-Health Solutions in Cloud Computing*. **IEEE Access**,2019, 7: 74361- 74382.

Chinnasamy P. & Deepalakshmi P. *Design of Secure Storage for Health-care Cloud using Hybrid Cryptography*. **In proceedings of 2018 Second International Conference on Inventive Communication and Computational Technologies**, 2018, (ICICCT) (IEEE), pp. 1717-1720.

Chinnasamy P., & Deepalakshmi P. *Design of Secure Storage for Health-care Cloud using Hybrid Cryptography*. **In *proceedings of 2018 Second International Conference on Inventive Communication And Computational Technologies (ICICCT)*** (IEEE),2018, pp. 1717-1720.

Chuang T, Zhi-xiang-Zhu W. *Hybrid Encryption Algorithm Based on Wireless Sensor Networks* **IEEE International Conference on Mechatronics and Automation (ICMA)** 2019 ISBN: 978-1-7281-1699-0 DOI: 10.1109/IEEE Tianjin, China.

Dumoulin V., Shlens J & Kudlur M. *A learned representation for artistic style*. **In *Proceedings of the Conference on ICLR*, Toulon, France**, April 2017, pp. 1–26.

Elhoseny M. *Secure medical data transmission model for IoT-based healthcare systems.* **Ieee Access**,2018, 6, 20596-20608.

Garcia-Morchon O. & Wehrle K. *Efficient And context-aware access control for pervasive medical sensor networks*. **In: 2010 8th IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops), Mannheim, Germany,** 2010, pp. 322–327.

Gatys L. A., Ecker A. S & Bethge M. *Image style transfer using convolutional neural networks*. ***In Proceedings of the IEEE Conference on Computer Vision And Pattern Recognition***, June 2016 , pp. 2414–2423.

Gatys L. A., Ecker A. S., Bethge M., Hertzmann A & Shechtman E. *Controlling perceptual factors in neural style transfer***. In Proceedings of the IEEE Conference on Computer Vision And Pattern Recognition, July 2017**, pp. 3730–3738.

Han H, Huang M, Zhang Y, & Bhatti U. A. *An architecture of secure health information storage system based on blockchain technology*. **In proceedings of International Conference on Cloud Computing and Security**, 2018, (Springer, Cham), pp. 578-588.

Huang J., Sharaf M., Huang T. S. *A hierarchical framework for secure And scalable ehr sharing And access control in multi-cloud*. **In *proceedings of 2012 41st International Conference on Parallel Processing Workshop****s,*2012 (IEEE), pp. 279- 287.

Huang X. & Belongie S., *Arbitrary style transfer in real-time with adaptive instance normalization*, **In *Proceedings of the IEEE International Conference on Computer Vision*, Venice, Italy**, October 2017, pp. 1510–1519.

Huanhuan H, Xin Z, Weiming Z, Nenghai Y. *Adaptive text steganography by exploring statistical And linguistical distortion*. **In Proceedings of the 2017 IEEE Second International Conference on Data Science in Cyberspace (DSC), Shenzhen, China**, 26–29 June 2017; pp. 145–150.

Hupperich T., Löhr H., Sadeghi A., Winandy M. *Flexible Patient-Controlled Security for Electronic Health Records*. **In: 2nd ACM SIGHIT International Health Informatics Symposium (IHI 2012)., Miami, Florida, USA, 2012**, pp. 1–5.

Johnson J., Alahi A & Fei-Fei L. *Perceptual losses for real-time style transfer and super-resolution*," **In Proceedings of the European Conference on Computer Vision, Computer Vision - ECCV 2016, Amsterdam, The Netherlands**, October, 2016, pp. 694–711,

Kahani N., Elgazzar K., Cordy K. *Authentication And Access Control in e-Health Systems in the Cloud.* **In: IEEE International Conference on High Performance and Smart Computing (HPSC), Big Data Security on Cloud (BigDataSecurity), New York, NY, USA**, 2016, pp. 13–23.

Kamoona M. A, & Altamimi A. M.. *Cloud E-health Systems: A Survay on Security Challenges And Solutions*. **In proceedings of 2018 8th International Conference on Computer Science and Information Technology (CSIT), (IEEE)**, 2018 :pp. 189-194.

Kester Q, Nana L, Pascu A, Gire S, Eghan J, Quaynor N. *A Security Technique for Authentication And Security of Medical Images in Health Information Systems.* **15th International Conference on Computational Science and Its Applications, Banff, AB, Canada**, 2015, pp. 8–13.

Kim D. H. & Kwak J. *The Framework of 3P-Based Secure eHealth Information System*. **In proceedings of 2018 International Conference on Platform Technology and Service (PlatCon) (IEEE)**, 2019, pp. 1-6.

Kumar R, Malik A, Singh S, Chand S. *A high capacity email based text steganography scheme using huffman compression*. **In Proceedings of the 2016 3rd International Conference on Signal Processing and Integrated Networks (SPIN), Noida, India**, 11–12 February 2016; pp. 53–56.

Kumar R., Malik A., Singh A, S., Kumar B., Chand S. *A space based reversible high capacity text steganography scheme using font type And style*. **In Proceedings of the 2016 International Conference on Computing, Communication and Automation (ICCCA), Greater Noida, India**, 29–30 April 2016; pp. 1090–1094.

Li M, Yu S, Ren K, Lou W. *Securing Personal Health Records in Cloud Computing: Patient-Centric And Fine-Grained Data Access Control in Multiowner Settings.* **In: International Conference on Security and Privacy in Communication Systems, Singapore, Singapore**, 2010, pp. 89–106.

Li W & Hoang D. *A new security scheme for e-health system*. **In: International Symposium on Collaborative Technologies and Systems**, 2009. CTS '09., Baltimore, MD, USA, 2009, pp. 361–366.

Li Y., Fang C., Yang J., Wang Z., Lu X & Yang M. *Universal style transfer via feature transforms*. **In *Proceedings of the Conference on Neural Information Processing Systems*, , Long Beach, United States**, December 2017, pp. 1–11.

Liang O. W & Iranmanesh V. *Information hiding using whitespace technique in Microsoft word*. **In Proceedings of the 2016 22nd International Conference on Virtual System & Multimedia (VSMM), Kuala Lumpur, Malaysia**, 17–21 October 2016; pp. 1–5.

Lin T.-Y., Maire M., Belongie S. *Microsoft COCO: common objects in context*. **In *Proceedings of the European Conference on Computer Vision*, Computer Vision - ECCV 2014, Zurich, Switzerland**, September, 2014. pp. 740–755.

Liu C. H., Lin F. Chiang Q. D. L., Chen T. L., Chen C. S., Lin H. Y., Chung Y. F., and Chen T. S. *Secure PHR access control scheme for healthcare application clouds*. **In *proceedings of 2013 42nd International Conference on Parallel Processing*, (IEEE)** ,2013, pp. 1067-1076.

Liu X., Cheng M., Lai Y & Rosin P. *Depth-aware neural style transfer*. ***In Proceedings of the Symposium on Non-Photorealistic Animation And Rendering, Los Angeles California***. July 2017,pp. 1–10.

Liu Y, Wu J, Xin G. *Multi-keywords carrier-free text steganography based on part of speech tagging*. **In Proceedings of the 13th International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery (ICNC-FSKD), Guilin, China**, 29–31 July 2017; pp. 2102–2107.

Löhr H., Sadeghi A. R. & Winandy M. *Securing the e-health cloud*. **In *Proceedings of the 1st acm international health informatics symposium* (ACM)**,2020 pp. 220-229.

Löhr H., Sadeghi A., Winandy M. **Securing the E-Health Cloud. In: 1st ACM International Health Informatics Symposium (IHI 2010)., Arlington, Virginia, USA**, 2010, pp. 1–10.

Luan F., Paris S., Shechtman E & Bala K.,**Deep photo style transfer**. **In Proceedings of the IEEE Conference on Computer Vision And Pattern Recognition, Honolulu, HI, USA**, July 2017, pp. 1–9.

Maganti P. K. & Chouragade P. M. *Secure Application for Sharing Health Records using Identity And Attribute based Cryptosystems in Cloud Environment*. **In proceedings of 2019 3rd International Conference on Trends in Electronics and Informatics**, 2019, (ICOEI)(IEEE), pp. 220-223.

Maganti P.K. & Chouragade P. M.. *Secure Health Record Sharing for Mobile Healthcare in Privacy Preserving Cloud Environment*. **In proceedings of 2019 IEEE International Conference on Electrical, Computer and Communication Technologies**, 2019 (ICECCT) (IEEE), pp. 1-4.

Mahmoud H, Hegazy A & Khafagy M. H. . *An approach for ample data security based on Hadoop distributed file system*. **Paper presented at the 2018 International Conference on Innovative Trends in Computer Engineering (ITCE)**, 2018.

Majumder A & Changder S. *A generalized model of text steganography by summary generation using frequency analysis*. **InProceedings of the 7th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)**, Noida, India, 29–31 August 2018; pp. 599–605.

Manoj R, Alsadoon A, Prasad P, Costadopoulos N, & Ali S. *Hybrid secure And scalable electronic health record sharing in hybrid cloud*. **In proceedings of 2017 5th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering,** 2017,(MobileCloud) (IEEE), pp. 185- 190.

Mishra S. & Dastidar A. *Hybrid Image Encryption And Decryption using Cryptography And Watermarking Technique for High Security Applications*.

2018 International Conference on Current Trends towards Converging Technologies (ICCTCT), 2018, pp. 1-5, doi: 10.1109/ICCTCT.2018.8551103.

Mohammed N. & Ibrahim N. *Implementation of New Secure Encryption Technique for Cloud Computing.* **2019 International Conference on Computing and Information Science and Technology and Their Applications (ICCISTA)**, 2019, pp. 1-5, doi: 10.1109/ICCISTA.2019.8830668.

N. Khan & A. Al-Yasiri. *Identifying Cloud Security Threats to Strengthen Cloud Computing Adoption Framework*, **The 2nd International Workshop on Internet of Thing: Networking Applications and Technologies** IoTNAT' 2016.

Naharuddin A., Wibawa A. D., Sumpeno S. *A high capacity And imperceptible text steganography using binary digit mapping on ASCII characters*. **In Proceedings of the 2018 International Seminar on Intelligent Technology and Its Applications (ISITIA), Bali, Indonesia**, 30–31 August 2018; pp. 287–292.

Nguyen D. C, Pathirana P. N, Ding M, & Seneviratne A. *Blockchain for Secure EHRs Sharing of Mobile Cloud based E-health Systems*. **IEEE Access**,2019, 7: 66792-66806.

Patra D, Ray S, Mukhopadhyay J, Majumdar B, & Majumdar A. K. *Achieving e-health care in a distributed EHR system*. **In proceedings of 2009 11th International Conference on eHealth Networking, Applications and Services** , 2009 (IEEE), pp. 101-107.

Pecarina J., Pu S., & Liu J.C. *Anonymity for enhanced control And private collaboration in healthcare clouds*. **In *proceedings of 4th IEEE International Conference on Cloud Computing Technology And Science Proceedings* (IEEE)**, 2012, pp. 99-106.

Qian Y., Jing D., Wei W & Tan T. *Deep learning for steganalysis via convolutional neural networks*. **In *Proceedings of the SPIE-International Society for Optical Engineering*, San Francisco, CA, United States**, March 2015.

Rachmawati D, Jaysilen A. S. & Budiman M. A. *Hybrid cryptosystem using a tiny encryption algorithm And Luc algorithm*. **Paper presented at the IOP Conference Series: Materials Science and Engineering**, 2018.

Sadikin M. A. & Wardhani R. W.. I*mplementation of RSA 2048-bit And AES 256-bit with digital signature for secure electronic health record application*. **In *proceedings of 2016International Seminar on Intelligent Technology And Its Applications (ISITIA)* (IEEE)**,2016, pp. 387-392.

Sahama T., Simpson L. & Lane B. *Security And Privacy in eHealth: Is it possible?*. **In *proceedings of 2013 IEEE 15th International Conference on e-Health Networking, Applications And Services (Healthcom 2013)* (IEEE)**, 2013, pp. 249-253.

Sakr A, Yaacoub E, Noura H, Al-Husseini M, Abualsaud K, Khattab T, Guizani M. *A secure client-side framework for protecting the privacy of health data stored on the cloud*. **In proceedings of 2018 IEEE Middle East and North Africa Communications Conference (MENACOMM) (IEEE)**, 2018, pp. 1-6.

Sanakoyeu A., Kotovenko D., Lang S & Ommer B. **A style-aware content loss for real-time HD style transfer**. **in Proceedings of the European Conference on Computer Vision, Computer Vision - ECCV 2018, Germany**, September 8-14, 2018 ,pp. 715–731.

Selvam L. & Arokia R. J. *Secure Data Sharing of Personal Health Records in Cloud Using Fine-Grained And Enhanced Attribute-Based Encryption*. **In proceedings of 2018 International Conference on Current Trends towards Converging Technologies** 2018, (ICCTCT) (IEEE), pp. 1-6.

Selvam L. & Arokia R. J. *Secure Data Sharing of Personal Health Records in Cloud Using Fine-Grained And Enhanced Attribute-Based Encryption*. **In *proceedings of 2018 International Conference on Current Trends towards Converging Technologies (ICCTCT)* (IEEE)**,2018, pp. 1-6.

Semwal P. & Sharma M. K. *Comparative study of different cryptographic algorithms for data security in cloud computing.* **2017 3rd International Conference on Advances in Computing, Communication & Automation (ICACCA) (Fall)**, 2017, pp. 1-7, doi: 10.1109/ICACCAF.2017.8344738.

Shin D., Sahama T. & Gajanayake R. *Secured e-health data retrieval in DaaS And Big Data*. **In proceedings of 2013 IEEE 15th International Conference on e-Health Networking, Applications and Services** (IEEE)2013, pp. 255- 259.

Shrestha N. M., Alsadoon A., Prasad P. W. C., Hourany L. & Elchouemi A. *Enhanced e-health framework for security And privacy in healthcare system*. **In *proceedings of 2016 Sixth International Conference on Digital Information Processing And Communications (ICDIPC)* (IEEE)**,2016, pp. 75-79.

Sumathi R. & Kirubakaran E. *SCEHSS: Secured Cloud Based Electronic Health Record Storage System with ReEncryption at Cloud Service Provider.* **International Journal of Computer and Communication Engineering**, *2013,* **2**(2): 162.

Tahir R, Tahir H, Sajjad A, & McDonaldMaier K. *A secure cloud framework for ICMetric based IoT health devices*. **In Proceedings of the Second International Conference on Internet of thing**, 2017.

Tallapally S. K. & Manjula B. *Competent multi-level encryption methods for implementing cloud security.* **InIOP Conference Series: Materials Science and Engineering**, 2020, vol. 981, no. 2, p. 022039.

Tancik M, Mildenhall B & Ng R. StegaStamp: *invisible hyperlinks in physical photographs*. **In *Proceedings of the IEEE Conference on Computer Vision And Pattern Recognition*, CVPR), Seattle, Washington, USA**, June 2020.pp. 1–13.

Tian Q & Schmidt M. *Fast patch-based style transfer of arbitrary style*. **In *Proceedings of the Conference on Neural Information Processing Systems*, Barcelona, Spain**, December 2016,pp. 1–5.

Volkhonskiy D., Nazarov I & Burnaev E. *Steganographic generative adversarial networks*. **In Proceedings of the Conference on Neural Information Processing Systems, Long Beach, United States**, December 2017, pp. 1–8.

Wang H. *Anonymous Data Sharing Scheme in Public Cloud And Its Application in E-Health Record*. **IEEE Access**, 2018, 6: 27818- 27826.

Wu N, Liu Z, Ma W, Shang P, Yang Z , Fan J. *Research on coverless text steganography based on multi-rule language models alternation*. **In Proceedings of the 2019 4th International Conference on Mechanical, Control and Computer Engineering (ICMCCE), Hohhot, China**, 5–27 October 2019; pp. 803–8033.

Wu N, Ma W, Ziu Z, Shang P, Yang Z, Fan J. *Coverless Text Steganography Based on Half Frequency Crossover Rule*. **In Proceedings of the 2019 4th International Conference on Mechanical, Control and Computer Engineering (ICMCCE), Hohhot, China,** 5–27 October 2019; pp. 726–7263.

Wu N, Shang P, Fan J, Yang Z, Ma W, Liu Z. *Research on coverless text steganography based on single bit rules*. **J. Physics Conf. Ser**. 2019, 1237.

Wu N., Shang P, Fan J, Yang Z, Ma W, Liu Z. *Coverless Text Steganography Based on Maximum Variable Bit Embedding Rules*. **J. Phys. Conf. Se**r. 2019, 1237, 022078.

Wu R., Ahn G., Hu H. *Secure Sharing of Electronic Health Records in Clouds*. **In: 8th International Conference Conference on Collaborative Computing: Networking, Applications and Worksharing, Collaboratecom 2012 Pittsburgh, PA, United States**, October 14-17, 2012, Pittsburgh, PA, United States, 2012, pp.711–718.

Yang R & Ling Z. H. *Linguistic Steganography by Sampling-based Language Generation*. **In Proceedings of the 2019 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference** (APSIPA ASC), Lanzhou, China, 18–21 November 2019; pp. 1014–1019.

Yassein M. B, Aljawarneh S, Qawasmeh E, Mardini W, & Khamayseh Y. *Comprehensive study of symmetric key And asymmetric key encryption algorithms.* **2017 International Conference on Engineering and Technology (ICET)**, 2017, pp. 1-7, doi: 10.1109/ICEngTechnol.2017.8308215.

Yu S., Wang C., Ren K., Lou W. *Achieving Secure, Scalable, And Fine-grained Data Access Control in Cloud Computing.* **In: 2010 Proceedings IEEE, INFOCOM, San Diego, CA, USA**, 2010 pp. 1–9.

Zhang R. & Liu L. *Security Models And requirements for healthcare application clouds*. **In proceedings of 2010 IEEE 3rd International Conference on cloud Computing (IEEE)**, 2010, pp. 268-275.

Zhu J., Kaplan R., Johnson J & Fei-Fei L. *HiDDeN: hiding data with deep networks*. **In Proceedings of the European Conference on Computer Vision, Computer Vision - ECCV 2018, Munich, Germany**, September 2018. pp. 682–697.

Zou L, Ni M, Huang Y, Shi W & Li X. *Hybrid encryption algorithm based on AES And RSA in file encryption*. **Paper presented at the International Conference on Frontier Computing**, 2020.

Theses

Zheng Y. *Privacy-preserving personal health record system using attribute-based encryption,* 2011, ***Masters Thesis*, (Publisher: Worcester Polytechnic Institute). Available Online: *https://digitalcommons.wpi.edu/etd-theses/902***

Online source

Bashshur R. L , Shannon G, E. Krupinski A, Grigsby J.. *Sustaining & realizing the promise of telemedicine.* Available Online: http://europepmc.org/abstract/MED/23289907.

CommVault.: *Your Top 5 Cloud Data Protection Challenges.Solved*. commvault.com/cloud. (Available Online)

Cloud Computing: Clear Benefits: The Emerging Role of Cloud Computing in Healthcare Information Systems. Available online: http://www.techrepublic.com/whitepapers/cloud-computing-clear-benefits-the-emerging-role-of-cloud-computing-in-healthcare-information-systems/2384337

Gartener: *Seven cloud-computing security risks*. InfoWorld.2008-07. Available Online: http://www.infoworld.com/d/security-central/gartener-seven-cloud computingsecurity-risks-853.

Appendix

Programming Code for the Encryption, Decryption and the Steganography Technique

```
<!DOCTYPE html>
<html>
<head>
    <title>Encryption</title>
</head>
<body>

    <div style="margin-left: 30%;margin-top: 10%; background-color: skyblue; width: 550px; height: 400px; padding-top: 20px; padding-left: 25px; border-radius: 25px;">
        <h3 style="margin-left: 200px; font-size: 21px;">Encrption.</h3>
        <label><textarea type='text' id="plainInput" placeholder="Type in plain text" style="width: 500px; border-radius: 25px; padding-left: 10px; padding-top: 10px;"></textarea></label><br><br>
        <div style="margin-left: 170px;">
            <button id="encryp-btn">Encrypt</button>
            <button id="copyToClipBoard">Copy Text</button><br><br>
        </div>
        <input type="number" name="" id="shiftInput" min="0" placeholder="Encrption Key..." max="25" style="width: 150px; margin-left: 150px; border-radius: 25px; padding-left: 10px; height: 30px;"><br><br>
        <label>
            <textarea type='text' id="encrytedInput-1" placeholder="Encrypted Text Will Appear Here..." style="width: 500px; border-radius: 25px; padding-left: 10px; padding-top: 10px;"></textarea>
        </label>

    </div>
```

```
<script type="text/javascript">
        document.getElementById("encryp-btn").onclick = function()
{myFunction()};

        function myFunction() {
          console.time('Execution Time');

            // task starts
            for (var i = 0; i < 100000000;i++);
            // task ends

            console.timeEnd('Execution Time');
        }
        let encrypBtn = document.getElementById('encryp-btn');
        let eInput = document.getElementById('encrytedInput-1');
        let pInput = document.getElementById('plainInput');
        let inputs = [eInput,pInput]
        let copyBtn = document.getElementById('copyToClipBoard');

        inputs.forEach( input => {
            input.oninput = () => {
                input.value = input.value.toUpperCase()
            }
        })

        function encrypt() {
            let pInput = document.getElementById('plainInput').value;
            let solved = ''
```

```
                let shiftInput =
parseInt(document.getElementById('shiftInput').value)


                for (var i = 0; i< pInput.length; i++){
                        let ascii_num = pInput[i].charCodeAt()
                        let sum = ascii_num + shiftInput
                        sum >= 65 && sum <= 90 ? solved +=
String.fromCharCode(sum) : sum > 90 ? solved += String.fromCharCode(65 + (sum
& 91)) : solved += pInput[i]
                }
                eInput.value = solved
        }


        function copyText() {
                eInput.select()
                eInput.setSelectionRange(0,99999)
                document.execCommand('copy')
                alert('Copied to clipboard!')
        }


        copyBtn.addEventListener('click',copyText)
        encrypBtn.addEventListener('click',encrypt)


    </script>


</body>
</html>


<!doctype html>
<html>
<head>
```

```
<meta charset="utf-8">
<title>Untitled Document</title>

<script type="text/javascript">
        document.getElementById("btnDe").onclick = function() {myFunction()};

                function myFunction() {
                  console.time('Execution Time');

                        // task starts
                        for (var i = 0; i < 100000000;i++);
                        // task ends

                        console.timeEnd('Execution Time');
                }
function Encrypt(f) {
        var word, newword, code, newcode, newletter
        var addkey, multkey
        word = f.p.value
        word = word.toLowerCase()
        word = word.replace(/\W/g, "")
        addkey = 0

        for (i=0; i < f.add.options.length; i++) {
                addkey = addkey + (f.add.options[i].text)*(f.add.options[i].selected)
        }

        multkey = 0
```

```
        for (i=0; i < f.mult.options.length; i++) {
                multkey = multkey + (f.mult.options[i].text)*(f.mult.options[i].selected)
        }

        newword = ""

        for (i = 0; i < word.length; i++) {
                code = word.charCodeAt(i) - 97
                newcode = ( (multkey*code + addkey) % 26 ) + 97
                newletter = String.fromCharCode(newcode)
                newword = newword + newletter
        }

        f.c.value = newword + " "
}

function Decrypt(f) {
        var word, newword, code, newcode, newletter
        var addkey, multkey, multinverse

        word = f.c.value
        word = word.toLowerCase()
        word = word.replace(/\W/g, "")
        addkey = 0

        for (i=0; i < f.add.options.length; i++) {
                addkey = addkey + (f.add.options[i].text)*(f.add.options[i].selected)
        }
```

```
        multkey = 0

        for (i=0; i < f.mult.options.length; i++) {
                multkey = multkey + (f.mult.options[i].text)*(f.mult.options[i].selected)
                //if (i==3) alert(multkey +" + "+f.mult.options[i].text + " * " +
f.mult.options[i].selected+" = "+(f.mult.options[i].text) * ( f.mult.options[i].selected));
        }

        multinverse = 1

        for (i=1; i <= 25; i = i + 2) {
                if ( (multkey*i) % 26 == 1 ) { multinverse = i }
        }

        newword = ""

        for (i = 0; i < word.length; i++) {
                code = word.charCodeAt(i) - 97
                newcode = ( (multinverse*(code + 26 - addkey)) % 26 ) + 97
                newletter = String.fromCharCode(newcode)
                newword = newword + newletter
        }

        f.p.value = newword.toLowerCase()
}

</script>
</head>

<body><form>Plaintext<br>
```

```
  <textarea name="p" rows="4" cols="50" wrap="soft" placeholder="Type in plain
text"></textarea>

  <p>a =

  <select name="mult" size="1">

  </select>

b =

  <select name="add" size="1">

  <option>0</option>

  <option>1</option>

  <option>2</option>

  <option>3</option>

  <option>4</option>

  <option>5</option>

  <option>6</option>

  <option>7</option>

  <option>8</option>

  <option>9</option>

  <option>10</option>

  <option>11</option>

  <option>12</option>

  <option>13</option>

  <option>14</option>

  <option>15</option>

  <option>16</option>

  <option>17</option>

  <option>18</option>

  <option>19</option>

  <option>20</option>

  <option>21</option>

  <option>22</option>
```

```
 <option>23</option>
 <option>24</option>
 <option>25</option>
 </select>
 </p>
 <input id="btnDe" name="btnDe" value="^ Decrypt ^"
onclick="Decrypt(this.form)" type="button"></p>
 <p>Ciphertext<br>
 <textarea name="c" rows="4" cols="50" wrap="soft" placeholder="Encrypted Text
Will Appear Here..."></textarea> </p>
</form>
</body>
</html>


<script type="text/javascript">
        encryptcount = 0;
   decryptcount = 0;


function chooseAlphabet()
{
   var alpha = document.getElementById("alpha-choice");
        var alphaChoice = alpha.options[alpha.selectedIndex].value;
        document.getElementById("alphabet").value = alphaChoice;
        document.getElementById("wrapper").innerHTML = "";
}


function keyChange()
{
   document.getElementById("wrapper").innerHTML = "";
}
```

```
function blocksBtn()
{
   if (document.getElementById("blocks").checked == true)
   {
      document.getElementById("removeChar").checked = true;
      document.getElementById("removeChar").disabled = true;
   }
   else if (document.getElementById("blocks").checked == false)
   {
      document.getElementById("removeChar").disabled = false;
   }
}

function resetEncryptCount()
{
        encryptcount = 0;
        document.getElementById("ciphertext").value = "";
}
function resetDecryptCount()
{
        decryptcount = 0;
        document.getElementById("plaintext").value = "";
}

function belongsTo(character, checkstring)
{
        p = 0;
        for (k=0;k<checkstring.length;k++)
```

```
        {
                if (character == checkstring.substr(k,character.length))
                {
                        p = p + 1;
                }
        }
        if (p > 0)
        {
                return "true";
        }
        else
        {
                return "false";
        }
}

function HCF(one, two)
{
        a=Math.abs(one);
        b=Math.abs(two);
        while (b != 0)
   {
      tmp = b;
      b = a % b;
      a = tmp;
   }
        return a;
}
```

```
function randomNumber(min, max)
{
	return Math.floor(Math.random() * (1 + max - min) + min);
}

function affine(palphabet, keya, keyb)
{
	palph = palphabet;
	calph = "";
	if (document.getElementById("A=0").checked == true)
	{
		for (w = 0; w < palph.length; w++)
		{
			cnum = (parseInt(keya) * w + parseInt(keyb)) % palph.length;
			calph = calph + palph.substr(cnum,1);
		}
	}
	else if (document.getElementById("A=1").checked == true)
	{
		for (w = 0; w < palph.length; w++)
		{
			cnum = (parseInt(keya) * (w + 1) + parseInt(keyb)) %
palph.length;
			calph = calph + palph.substr(cnum - 1,1);
		}

	}

	return calph;
}
```

```
function reverseString(stringUsed)
{
	reversed = "";
	for(l = stringUsed.length -1; l >= 0; l--)
	{
		reversed += stringUsed.substr(l,1);
	}
	return reversed;
}

function subs(palphabet, calphabet, ptext)
{
	ctext = "";
	for (i = 0; i < ptext.length; i++)
	{
		a = ptext.substr(i,1);
		if (belongsTo(a,palphabet) == "true")
		{
			for (j = 0; j < palphabet.length; j++)
			{
				b = palphabet.substr(j,1);
				c = calphabet.substr(j,1);
				if (a == b)
				{
					ctext = ctext + c;
				}
			}
		}
```

```
                else
                {
                        ctext = ctext + a;
                }
        }

        return ctext;
}

function remove(stringUsed, alphabetUsed)
{
        m = 0;
        newstring = stringUsed;
        while (m<newstring.length)
        {
                if (belongsTo(newstring.substr(m,1),alphabetUsed) == "false")
                {
                        newstring = newstring.substring(0,m) +
newstring.substring(m+1,newstring.length);
                }
                else
                {
                        m++;
                }
        }
        return newstring;
}

function blocks(string)
{
```

```
        newstring = string;
        strlength = newstring.length;
        d = 5;
        while (d < strlength)
        {
                newstring = newstring.substring(0,d) + " " +
newstring.substring(d,strlength);
                strlength = newstring.length;
                d = d + 6;
        }
        return newstring;
}



function encrypt()
{
   if (document.getElementById("alphabet").value == "")
        {
                alert("Choose an alphabet, or type your own.");
        }
        else if
(HCF(document.getElementById("keyA").value,document.getElementById("alphabet
").value.length) != 1)
        {
                alert("This function has no inverse, so you will not be able to decrypt it.
Choose another value for a.");
        }
        else
        {
                key1 = document.getElementById("keyA").value;
```

```
        key2 = document.getElementById("keyB").value;
        alphabet1 =
document.getElementById("alphabet").value.toLowerCase();
        alphabet2 = affine(alphabet1.toUpperCase(),key1,key2);
        plain = document.getElementById("plaintext").value.toLowerCase();

        if (document.getElementById("removeChar").checked == true)
        {
            plain1 = remove(plain,alphabet1);
        }
        else
        {
            plain1 = plain;
        }

        if (document.getElementById("blocks").checked == true)
        {
            plain1 = remove(plain,alphabet1);
            plain2 = blocks(plain1);
        }
        else
        {
            plain2 = plain1;
        }

        if (document.getElementById("slow-encrypt").checked == false)
        {
            document.getElementById("ciphertext").value =
subs(alphabet1,alphabet2,plain2);
```

```
                }
                if (document.getElementById("slow-encrypt").checked == true)
                {
                        if(encryptcount >= plain2.length)
                        {
                                alert("You have finished the message. Press Reset or
deselect Slow Encrypt");
                        }
                        else
                        {
                                document.getElementById("ciphertext").value =
document.getElementById("ciphertext").value +
subs(alphabet1,alphabet2,plain2.substr(encryptcount,1));
                                encryptcount = encryptcount + 1;
                        }
                }

        }
}

function decrypt()
{
   if (document.getElementById("alphabet").value == "")
        {
                alert("Choose an alphabet, or type your own.");
        }
        else if
(HCF(document.getElementById("keyA").value,document.getElementById("alphabet
").value.length) != 1)
        {
                alert("This function has no inverse, so you will not be able to decrypt it.
Choose another value for a.");
```

```
        }
        else
        {
                key1 = document.getElementById("keyA").value;
                key2 = document.getElementById("keyB").value;
                alphabet1 =
document.getElementById("alphabet").value.toLowerCase();
                alphabet2 = affine(alphabet1.toUpperCase(),key1,key2);
                cipher = document.getElementById("ciphertext").value.toUpperCase();

                if (document.getElementById("slow-decrypt").checked == false)
                {
                        document.getElementById("plaintext").value = subs(alphabet2,
alphabet1, cipher);
                }
                if (document.getElementById("slow-decrypt").checked == true)
                {
                        if (decryptcount >= cipher.length)
                        {
                                alert("You have finished the message. Press Reset or
deselect Slow Decrypt");
                        }
                        else
                        {
                                document.getElementById("plaintext").value =
document.getElementById("plaintext").value + subs(alphabet2, alphabet1,
cipher.substr(decryptcount, 1));
                                decryptcount = decryptcount + 1;
                        }
                }
```

```
        }
}

function showCiphertextAlphabet()
{
   key1 = document.getElementById("keyA").value;
        key2 = document.getElementById("keyB").value;
        alphabet1 = document.getElementById("alphabet").value.toLowerCase();
        alphabet2 = affine(alphabet1.toUpperCase(),key1,key2);

        cipherAlphabet = "<table style=\"color:black;background-color:lightgray\"
border=\"1\"><tr><td>Plaintext Alphabet</td>";
        for (i=0; i<alphabet1.length; i++)
        {
        cipherAlphabet += "<td width=\"20px\" style=\"text-align:center\">";
        cipherAlphabet += alphabet1.substr(i,1);
        cipherAlphabet += "</td>";
        }
        cipherAlphabet += "</tr><tr><td>Ciphertext Alphabet</td>";
        for (i=0; i<alphabet2.length; i++)
        {
        cipherAlphabet += "<td width=\"50px\" style=\"text-align:center\">";
        cipherAlphabet += alphabet2.substr(i,1);
        cipherAlphabet += "</td>";
        }
        cipherAlphabet += "</tr></table>";

        document.getElementById("wrapper").innerHTML = cipherAlphabet;
}
```

```
function resetFunction()
{
   document.getElementById("alphabet").value = "abcdefghijklmnopqrstuvwxyz";
   document.getElementById("alpha-choice").selectedIndex = "0";
   document.getElementById("plaintext").value = "";
   document.getElementById("slow-encrypt").checked = false;
   document.getElementById("ciphertext").value = "";
   document.getElementById("keyA").value = 1;
   document.getElementById("keyB").value = 0;
   document.getElementById("slow-decrypt").checked = false;
   document.getElementById("removeChar").checked = false;
   document.getElementById("blocks").checked = false;
   document.getElementById("removeChar").disabled = false;
   encryptcount = 0;
   decryptcount = 0;
   document.getElementById("wrapper").innerHTML = "";
}
</script>

<!DOCTYPE html>
<html>
<head>
        <title></title>
</head>
<body>

        <form>
    <fieldset data-role="controlgroup" style="min-width:200px">
      <legend style="color:black">Alphabet:</legend>
```

```
        <select name = "alpha-choice" id = "alpha-choice"
onchange="chooseAlphabet()">

            <option selected id = "alpha-standard" value =
"abcdefghijklmnopqrstuvwxyz">Standard</option>

            <option id = "alpha-punctuation" value =
" .,?!abcdefghijklmnopqrstuvwxyz">Include Basic Punctuation</option>

            <option id = "alpha-numbers" value =
"abcdefghijklmnopqrstuvwxyz0123456789">Include Numbers</option>

            <option id = "alpha-all" value =
" .,?!abcdefghijklmnopqrstuvwxyz0123456789">Include Basic Punctuation and
Numbers</option>

            <option id = "alpha-own" value = "">Use you own alphabet</option>

        </select>

        <br>

        <input id="alphabet" value="abcdefghijklmnopqrstuvwxyz"
style="width:350px;max-width:100%"></input><br><br>

        <div style="display:inline-block">

        <label style="color:black">Value of a:</label>

        <input id="keyA" type="number" value="1" min="-50" max="50"
oninput="keyChange()" style="width:50px;max-width:100%"></input>

        </div>

        <div style="display:inline-block">

        <label style="color:black">Value of b:</label>

        <input id="keyB" type="number" value="0" min="-50" max="50"
oninput="keyChange()" style="width:50px;max-width:100%"></input>

        </div><br>

        <div style="display:inline-block">

        <label style="color:black"><input type="radio" name="sub-type" id="A=0"
checked value="A=0">Use "A"=0,"B"=1,"C"=2,...</input></label>

        </div>

        <div style="display:inline-block">

        <label style="color:black"><input type="radio" name="sub-type" id="A=1"
value="A=1">Use "A"=1,"B"=2,"C"=3,...</input></label>

        </div>
```

```
    </fieldset>
    <fieldset data-role="controlgroup">
     <legend style="color:black">Ceaser text:</legend>
     <div style="display:inline-block;width:70%;min-width:200px">
        <textarea id="plaintext" style="width:100%" rows="5"></textarea>
     </div>
     <div style="display:inline-block;vertical-align:top">
        <input type="button" id="encryptBtn" value="Encrypt" onclick="encrypt()"
class="button button1"><br>
        <label style="color:black"><input type="checkbox" id = "slow-encrypt"
onchange="resetEncryptCount()">Slow Encrypt</label>
     </div>
    </fieldset>
    <fieldset data-role="controlgroup">
     <legend style="color:black">Ciphertext:</legend>
     <div style="display:inline-block;width:70%;min-width:200px">
        <textarea id="ciphertext" style="width:100%" rows="5"></textarea>
     </div>
     <div style="display:inline-block;vertical-align:top">
        <input type="button" id="decryptBtn" value="Decrypt" onclick="decrypt()"
class="button button3"><br>
        <label style="color:black"><input type="checkbox" id = "slow-decrypt"
onchange="resetDecryptCount()">Slow Decrypt</label>
     </div>
    </fieldset>
    <fieldset data-role="controlgroup">
     <legend style="color:black">Options:</legend>
     <div style="display:inline-block">
        <input type="button" id="showCipherAlpha" value="Show Ciphertext
Alphabet" onclick="showCiphertextAlphabet()" class="button button2">
     </div>
```

```
  </fieldset>
    <fieldset data-role="controlgroup">
      <legend style="color:black">Ceaser text:</legend>
      <div style="display:inline-block;width:70%;min-width:200px">
        <textarea id="plaintext" style="width:100%" rows="5"></textarea>
      </div>
      <div style="display:inline-block;vertical-align:top">
        <input type="button" id="encryptBtn" value="Encrypt" onclick="encrypt()"
class="button button1"><br>
        <label style="color:black"><input type="checkbox" id = "slow-encrypt"
onchange="resetEncryptCount()">Slow Encrypt</label>
      </div>
    </fieldset>
    <fieldset data-role="controlgroup">
      <legend style="color:black">Ciphertext:</legend>
      <div style="display:inline-block;width:70%;min-width:200px">
        <textarea id="ciphertext" style="width:100%" rows="5"></textarea>
      </div>
      <div style="display:inline-block;vertical-align:top">
        <input type="button" id="decryptBtn" value="Decrypt" onclick="decrypt()"
class="button button3"><br>
        <label style="color:black"><input type="checkbox" id = "slow-decrypt"
onchange="resetDecryptCount()">Slow Decrypt</label>
      </div>
    </fieldset>
    <fieldset data-role="controlgroup">
      <legend style="color:black">Options:</legend>
      <div style="display:inline-block">
        <input type="button" id="showCipherAlpha" value="Show Ciphertext
Alphabet" onclick="showCiphertextAlphabet()" class="button button2">
      </div>
```

```
  </fieldset>
    <fieldset data-role="controlgroup">
      <legend style="color:black">Ceaser text:</legend>
      <div style="display:inline-block;width:70%;min-width:200px">
        <textarea id="plaintext" style="width:100%" rows="5"></textarea>
      </div>
      <div style="display:inline-block;vertical-align:top">
        <input type="button" id="encryptBtn" value="Encrypt" onclick="encrypt()"
class="button button1"><br>
        <label style="color:black"><input type="checkbox" id = "slow-encrypt"
onchange="resetEncryptCount()">Slow Encrypt</label>
      </div>
    </fieldset>
    <fieldset data-role="controlgroup">
      <legend style="color:black">Ciphertext:</legend>
      <div style="display:inline-block;width:70%;min-width:200px">
        <textarea id="ciphertext" style="width:100%" rows="5"></textarea>
      </div>
      <div style="display:inline-block;vertical-align:top">
        <input type="button" id="decryptBtn" value="Decrypt" onclick="decrypt()"
class="button button3"><br>
        <label style="color:black"><input type="checkbox" id = "slow-decrypt"
onchange="resetDecryptCount()">Slow Decrypt</label>
      </div>
    </fieldset>
    <fieldset data-role="controlgroup">
      <legend style="color:black">Options:</legend>
      <div style="display:inline-block">
        <input type="button" id="showCipherAlpha" value="Show Ciphertext
Alphabet" onclick="showCiphertextAlphabet()" class="button button2">
      </div>
```

```
  </fieldset>
    <fieldset data-role="controlgroup">
      <legend style="color:black">Ceaser text:</legend>
      <div style="display:inline-block;width:70%;min-width:200px">
        <textarea id="plaintext" style="width:100%" rows="5"></textarea>
      </div>
      <div style="display:inline-block;vertical-align:top">
        <input type="button" id="encryptBtn" value="Encrypt" onclick="encrypt()"
class="button button1"><br>
        <label style="color:black"><input type="checkbox" id = "slow-encrypt"
onchange="resetEncryptCount()">Slow Encrypt</label>
      </div>
    </fieldset>
    <fieldset data-role="controlgroup">
      <legend style="color:black">Ciphertext:</legend>
      <div style="display:inline-block;width:70%;min-width:200px">
        <textarea id="ciphertext" style="width:100%" rows="5"></textarea>
      </div>
      <div style="display:inline-block;vertical-align:top">
        <input type="button" id="decryptBtn" value="Decrypt" onclick="decrypt()"
class="button button3"><br>
        <label style="color:black"><input type="checkbox" id = "slow-decrypt"
onchange="resetDecryptCount()">Slow Decrypt</label>
      </div>
    </fieldset>
    <fieldset data-role="controlgroup">
      <legend style="color:black">Options:</legend>
      <div style="display:inline-block">
        <input type="button" id="showCipherAlpha" value="Show Ciphertext
Alphabet" onclick="showCiphertextAlphabet()" class="button button2">
      </div>
```

```
        <div style="display:inline-block">
            <input type="button" id="resetBtn" value="Reset" onclick="resetFunction()"
class="button button2">
        </div>
        <div style="display:inline-block">
            <label style="color:black"><input type="checkbox" id =
"removeChar">Remove all Characters not in alphabet</label><br>
            <label style="color:black"><input type="checkbox" id = "blocks"
onclick="blocksBtn()">Put ciphertext in blocks of 5</label>
        </div>
      </fieldset>
    </form>


</body>
</html>
```

Biodata

A. Personal Data

Full Name: Ridwan Olayinka Kolapo

Address: Block D Plot 1 Lead Garden Estate Off Arapaja Road Odo-Ona Kekere, Ibadan.

Email address: ashiwaju93@gmail.com

Phone number: +234(0)8132393870

Date and Place of Birth: 1st April, 1993; Ibadan, Oyo State.

Nationality: Nigerian

Marital status: Married

Name of Next of Kin: Mr. T.O Kolapo

B. Educational Background

Primary Education

i) Ini-Oluwa Nursery and Primary School, Ibadan, Oyo state

Primary School Leaving Certificate. 1995-2003

Secondary Education

i) Oladipo Alayande School of Science Ibadan, Oyo State.

West African School Certificate. 2006-2009

Higher Education

i) Lead City University, Ibadan, Oyo State

PhD in Computer Science 2018 - Present

ii) University of Ibadan, Ibadan, Oyo State, Nigeria.

M.Sc. in Computer Science. 2015-2017

iii) Lead City University, Ibadan, Oyo State

B.Sc. in Computer with Electronics. 2009-2013

C. 1. Work Experience

i) Onicha Local Government Council, Ebonyi State.

IT Officer (NYSC) 2013 – 2014.

ii) Cobol Consulting Firm Adamasigba, Ibadan.

Customer Service Officer 2012- 2013.

iii) Lead City University, Ibadan, Oyo State

Lecturer II 2018 - Present.

2. Courses Taught Within The Current Academic Sessions

GST 103 End User Computing.

GST 203 Application of Computer.

CSC 101 Introduction to Computer Science.

SEN 101 Introduction to Computer Science.

CMP 311 Application of Computer to Art.

HIM 311 Database Construction in Health Informatics.

SEN 212 Computer Architecture and Organization.

ACC 502 Introduction to Spreadsheet Packages.

BED 403 Fundamentals of Data Processing.

EHS 305 Environmental information systems.

CSC 608 Information Storage and Retrieval.

IFT 202 Fundamentals of Information Technology.

IFT 203 Information Technology in Business.

CYB 201 Fundamentals of Cybersecurity

CYB 202 Cybersecurity in Business

OIM 304 Internet Technologies and Corel Draw

D. Publications

Thesis/Dissertation

i) Construction of a programmable digital timer for electric cookers (BSc project)

ii) Fuzzy Inference system for the diagnosis of upper respiratory tract infection (MSc Dissertation)

iii) An improved privacy technique in a Cloud-based e-Health System. (PhD in View research work)

Published Papers

i. "Addressing medical diagnosis errors in the upper respiratory tract infection using fuzzy inference system". Adeyemo A. B. and Kolapo R. O. [Computing,

Information Systems, Development Informatics & Allied Research Journal Vol. 8 No. 3, September, 2017].

ii. "Ontology Development for Human Resources in Nigerian Universities". Ridwan Kolapo, Philip Achimugu, Oluwatolani Achimugu, Temilola John-Dewole. [2nd International Faculty Of Basic Medical and Applied Sciences Conference Lead City University, Ibadan. October 2018].

iii. 'Information System Security in the Institution of higher education (A case study of American University)". Odegbesan O. and Kolapo R. O. [Invention Journal of Research Technology in Engineering and Management Volume 3 Issue 2, February 2019].

iv. "A secured, Efficient and Simplified Symmetric Application for Encryption and Decryption of Text Files Using a One-Time Key". Vivian Nwufoh, Ridwan Kolapo, Olajide Ogunsanwo and Temilola John-Dewole. [2nd International Conference on Applied ICT Lead City University, Ibadan. October, 2019]. ISBN: 978-978-977-446-3.

v. "An Improved Privacy Technique in a Cloud based e-Health System". Ridwan Kolapo and Oluwatolani Achimugu. [2nd International Conference on Applied ICT Lead City University, Ibadan] October, 2019. ISBN: 978-978-977-446-3.

vi. "Development of a Microcontroller Based Home Automation System Using Bluetooth and Android Application". Temilola John-Dewole, Ridwan Kolapo, Oluwatobi Johnson and Immaculata Ojo. [2nd International Conference on Applied ICT Lead City University, Ibadan]. October, 2019. ISBN: 978-978-977-446-3.

vii. "An Improved Approach for Generating Test Cases during Model-Based Testing Using Tree Traversa Algorithm ". Oluwatolani Achimigu, Philip

Achimigu, Chinonyelum Nwufoh, Sseggujja Husssein, Ridwan Kolapo and Tolulope Olufemi. [Journal of Software Engineering and Application] 2021. ISSN online: 1945-3124. ISSN Print: 1945-3116.

viii. "Expert System For Diagnosing Typhoid Fever Using Fuzzy Logic Technique". V.B Gaji, O. Achimugu, A.K Ademuwagun, P.O Achimugu, A. Akinkitan and R.O Kolapo. [Air Force Institute Of Technology Kaduna First International Conference On Data Science And Engineering]. December, 2021.

ix. "Fingerprint-Based Identity Verification for University of Ilorin".J.K Ayeni, M.J. Abdullahi, O. Achimugu, R.O. Kolapo and A.A Akinkitan. [Air Force Institute Of Technology Kaduna First International Conference On Data Science And Engineering]. December, 2021.

E. Major Conferences/Workshop Attended

i) 60 hours of professional development in Database Design and Programming with SQL (Oracle Academy. March, 2020).

ii) 2nd International Conference on Applied ICT (ICAICT 2019).

iii) 2nd International Faculty of Basic Medical and Applied Sciences Conference (FASCON 2018).

iv) Ethical Conduct in Higher Institution Organized by Liprorich Consulting Limited.

v) One-Day Oracle Academy Workshop.

F. Others

i) Certifications

i. Certification in Poise Skills and Customer Relations.

ii. Certificate of completion Cisco Certified Network Associates.

iii. Executive Diploma in Ethical Conduct in Higher Institutions (Liprorich Consulting Limited, Ibadan).

iv. Certificate of completion in Database Design and Programming with SQL (Oracle Academy).

G. Referees

Dr. P.O. Achimugu
Faculty of Computing
Air Force Institute of Technology, Kaduna
check4philo@gmail.com
+234(0)8093482286

Dr. Babatunde Adebo
Physics Department
Lead City University
Adebo.babatunde@lcu.edu.ng
+234(0)8035022462

Dr.(Mrs) Oluwatolani Achimugu
Faculty of Computing
Air Force Institute of Technology, Kaduna.
+234(0)8181451719
tolapeace@gmail.com

Mr. Adeniyi Adebiyi
Premises Manager
The Metropolitan Club
Neyoromah25k@gmail.com
+234(0)8059135174

_____ _____

Signature Date

University Compliance Form

This is to certify that this thesis by Kolapo Ridwan Olayinka with Matriculation Number LCU/PG/000145 in the Department of Computer Science, Faculty of Natural and Applied Sciences, Lead City University, Ibadan is in full compliance with the approval of the University's format and style.

…… ……

Signature Date