Enhancing Messaging Security Using Image Steganography Technique

Kayode Mathias MADEWA
LCU/PG/002718

Being a MSc Postfield Presentation Submitted to the Department of Computer Science, Faculty of Natural & Applied Sciences, Lead City University, Ibadan, Oyo State, Nigeria

In Partial Fulfillment of the Requirements for the Award of Master of Science Degree (MSc) in Computer Science

2023

Certification

This is to certify that Kayode Mathias MADEWA with matriculation number LCU/PG/002718 carried out this research work titled "Enhancing End To End Messaging Security Using Image Steganography Technique" in the Department of Computer Science, Faculty of Applied Sciences, Lead City University, Ibadan, Oyo state, for the award of Masters Degree (MSc) and that this has not been previously submitted.

. . . .

Dr. Waheed
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 and complete my Msc 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 supervisor, Dr. A. A. Waheed. I also like to acknowledge my lecturers, Dr. W. Sakpere, Dr. W. Ajayi, Dr. A. M. Ayoade, Dr. R. O Kolapo, Mrs K. Okesola and Mrs Afe for their supports and always ensuring that things are done rightly .

My appreciation goes to Kofo, Tobi and Tayo for their understanding and support. I also thank my colleagues and friends who 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 steganography has brought plenty of improvement to information security, but not really employed in Information banks and this is often as a results of the protection issues that come together with the employment of Information security. Security issues is taken into account a significant concern which is why every individual still opt to follow the normal way of addressing sensitive information. The aim of this study is to enhance end to end messaging security using image steganography technique. End to End SMS has always been dealing with security issues as there are no security measures being put in place to improve the Confidentiality of the context of the SMS. The Methodology used in this study implore the use of mathematical expression as the first step is to convert the secret message into binary and thus obtain a bitstream as the result of this step. then divide the obtained bitstream into a set of groups with three bits in each group. To this end, from the least significant bit, grouping is then done to every three continuous bits in a group. The result of this study is presented as a software solution, as it is implemented and tested for use. This study uses evaluation parameters like Mean square error and Peak Signal to Noise Ratio to measure the performance of the images that are used in the cause of this study, the images that are evaluated is the stego-image with text of different word-lengths embedded in it.

Keywords: Encryption , Algorithm, Red2 algorithm.

Word Count: 249

Table of Contents

List of Tables

List of Figures

Chapter One

Introduction

1.1 Background to the Study

Cryptography is the study and implementation of techniques to hide information from being read. Data that can be read and understood without any special measures is called plain-text. The method of representing plain-text in such a way as to hide its substance is called encryption. Encrypting plain-text results in unreadable form is called cipher-text. The process of reverting cipher-text to its original plain-text is called decryption[1].

Steganography is a part of the cryptographic techniques which refers to the art of covert communications. The message is embedded among another object referred to as a cover Work, by tweaking its properties. It become additional necessary as additional folks be part of the computer network revolution. Steganography is the art of concealing information in ways in which prevents the detection of hidden message. A completely unique methodology is projected to produce additional security for the key information with the mixture of compression and encoding methodology. It needs less memory house and quick transmission rate as a result of compression technique is applied[2].

It's been propelled to the forefront of current security techniques by the exceptional growth in process power, the rise in security awareness by, e.g., people, groups, agencies, government and through intellectual pursuit. With procedure on the opposite hand, different, distinctive marks square measure embedded in distinct copies of the carrier object that square measure equipped to totally different customers. This allows the belongings of owner to spot customers who break their licensing agreement by supplying the property to third parties. This project describes the LSB algorithmic

program used for image steganography to parenthetically the safety potential of steganography for end to end SMS Security[3].

1.2 Statement of the Problem

End to End SMS has always been dealing with security issues as there are no security measures being put in place to improve the Confidentiality of the context of the SMS. This poses a security threat to the telecommunication industry as SMS being sent over different channels can be cloned or diverted to another user and this has a major effect in the telecommunication industries. Lots of research work has been done on steganography as it is been applied to the medical field, forensics but this study lift the security challenges faced by the telecommunication sector on end to end SMS communication.

1.3 Aim and Objective of Study

The aim of this study is to enhance end to end messaging security using image steganography technique.

The objectives of the study are as follows to:

i. Review existing steganography framework for end to end Image security
ii. Develop a framework for the steganography technique
iii. Evaluate the developed system.

1.4 Significance of Study

Steganography surpasses every other mechanisms used for securing data in information security. The modern digital arena calls for a more robust information hiding technique and thus, this as always been a major flashpoint for researchers which this study has addressed as this threat in information security is a big gap that if left un-attended to will eventually make the field of information technology an unsafe world.

1.5 Scope of Study

The scope of this study is that it will focus mainly on text and not multimedia like Voice notes or MMS and can be implemented over any network.

1.6 Limitation of Study

This Study is only considers the use of Text and in the implemenation of this study Audio was not considered as it can be considered for further studies.

1.7 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.

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 un-encrypted form.

Plain-text: Plain-text 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.

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

Endnotes

[1]D. Abbas, M. AlyanNezhadi, & M. Forghani. "*A New Steganography Method for Embedding Message in JPEG Images*." 2019 5th Conference on Knowledge Based Engineering and Innovation (KBEI). IEEE**,** 2019.

[2]K. Jawwad, K. Gunjan, G. Sonali & K. Atiya "*A Novel Approach to Steganography Using Pixel-based Algorithm in Image Hiding.*" 2020 International Conference on Computer Communication and Informatics (ICCCI). IEEE, 2020.

[3]C. Ghule Isha, H. Sonawane Dhanasahjri, S. Sakhala Siddhi, T. Khade & R. Dahake "*Data Hiding Using Audio Steganographic Techniques*". **International Journal of Scientific Development and Research (Ijsdr)**.Volume 8 Issue 5, 2023, Pg 2257-2262

Chapter Two

Literature Review

2.1 Overview

Steganography 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

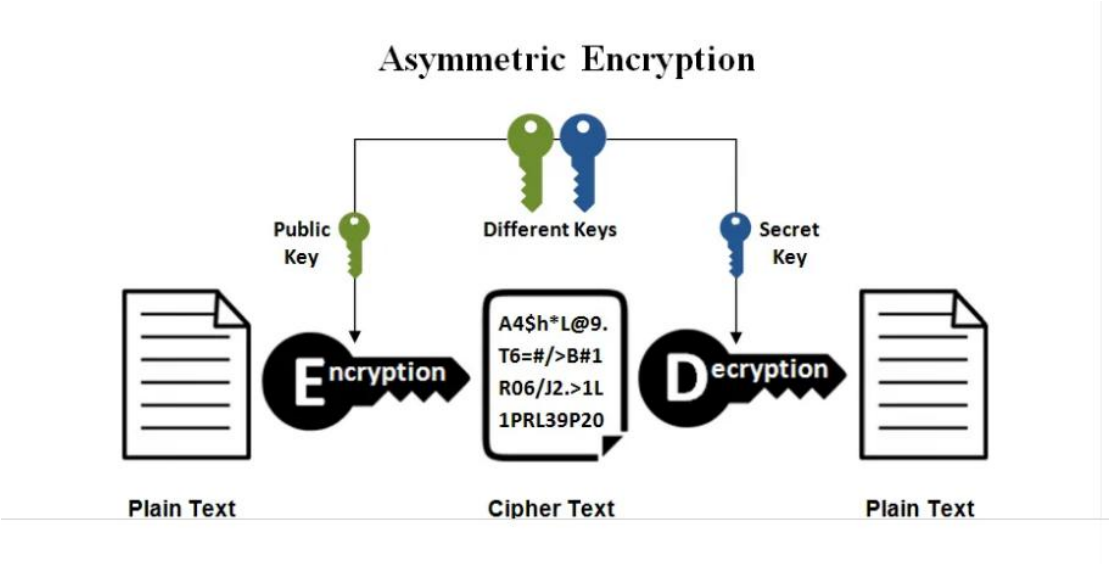

Figure 2.1 Asymmetric Encryption[8]

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.

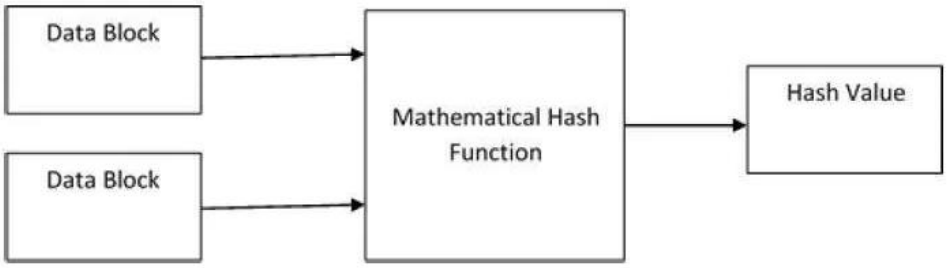

Figure 2.2 Hash Function[11]

Types of Hash Functions

- 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 Cipher-texts. 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.

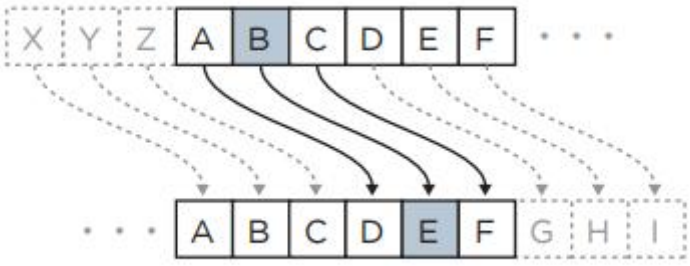

Figure 2.4 Ceasear Cipher Encryption[21]

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 Modern 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

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

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 Modern 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 e-Health 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 e-Health data, however, meeting the requirements of e-Health 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 plain-text attack), IBPRE is INDIDCCA2 (indistinguishable as a plain-text-based identity-based attack) 2) safe. They also show that the IBPRE program performs better re-encryption, resulting in e-Health data protection and cost savings for users of the cloud-based e-Health 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 Cipher-text 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 e-Health 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 Cipher-text

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 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].

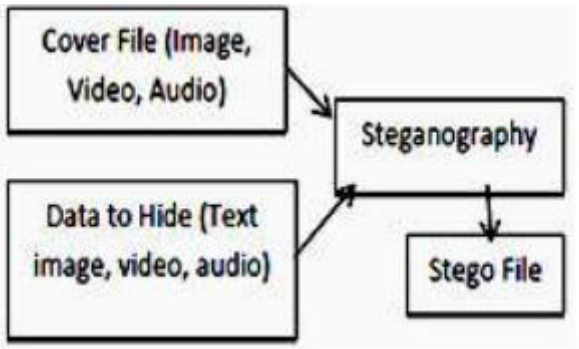

Figure 2.8 Block Diagram of Steganography[126]

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.

2.9.1 **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]

2.9.1.1 **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].

2.9.1.2 **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.

2.9.1.3 **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].

2.9.1.4 **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].

2.10 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]:

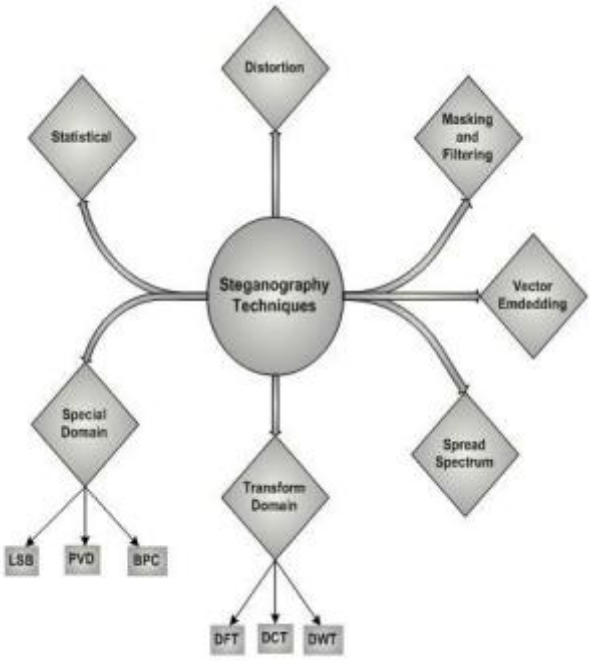

Figure 2.10 Steganography Technique[129]

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].

2.11 Review of Empirical Studies

System studies was proposed on image steganography. Steganography is the method whereby data is hidden inside other data so only the recipient can reveal hidden information after recovering the item. An Adaptive Image Steganography Method Based on Histogram of Oriented Gradient and PVD-LSB Techniques. This algorithm is effective on the security factor of secret image since the embedded checksum will validate for any unauthorized user or intruders attempt to corrupt the picture in any aspect[4].

In a work done by a researcher, system, large-scale JPEG image steganalysis using hybrid deep learning framework[5]. Its was proposed that a generic hybrid deep-learning framework for JPEG steganalysis incorporating the domain knowledge

behind rich steganalytic models. Digital image steganography using modified LSB & AES crptography. The cryptographic algorithms are AES, RSA, DES, 3DES and blowfish algorithms, & the steganography technique in LSB.

In a research conducted, systems results improving selection-channel-aware steganalysis features. The best detectors of contentadaptive steganography are built as classifiers trained on examples of cover and stego images represented with rich media models (features) formed by histograms f - quantized noise residuals. LSB based Steganography using Bit masking method on RGB planes. Steganography hides the existence of information that needs to be exchanged or transferred through some public media like the internet[6].

In a research conducted recently, it was proposed that a system with new LSB-S image steganography method blend with cryptography for secret communication. A method of image coding is proposed that hides the information along a selected pixel and on the next value of the selected pixel, that is, pixel + 1. International journal of advanced research in computer science & software engineering. MATLAB provides more security for secret communication[7].

A brand new framework for digital nation was proposed at the Attribute-Based Encryption (ABE) encryption technique. 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[131]. 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[132]. 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[133]. 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.

Evaluation of various security requirements related to data protection for record services was considered in a study. The Study proposed an improved role-based access control Model to design the Healthcare Services Integrated Platform (uHCSIP)[134]. 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. 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[135]. 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, evaluation of the performance was done using a simple case of an electronic medical system. The main drawback of this Model is the inability to summarize sensitive information.

In an attempt to locate answers to protection problems in Record System, 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[136]. 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. 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[137]. 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 [137]. 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[138].

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[139]. 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 , addressed the concept of embedding the secret message into an image using LSB technique and then applied AES algorithm to provide better security[140]. A reverse procedure was proposed which described in paper by using an alteration component method[141]. 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[142]. 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[143]. An overview used to hide secret messages or images in space and transform domains was presented in [144]. 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[145]. 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[146]. 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[147]. In an article it was demonstrated that these techniques can be used to make data more secure and robust[148]. In a research studied, 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[149].

Endnotes

[1]J. Pelzl & B. Preneel. *Understanding Cryptography: A Textbook for Students and Practitioners*. **Springer**, 2020.

[2]M. Akram W.C. Barker. *Securing Web Transactions TLS Server Certificate Management.* **Nist Special Publication** 2020,1800-16.

[3]V. Gamido, M. V. Gamido, & A. M. Sison, "*Developing a Secured Image File Management System Using Modified AES,*" **Bulletin of Electrical Engineering and Informatics, (ISSBN)**, vol. 8, no. 4, 2019, pp. 1461-1467.

[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]S. Niharika & K. Avinash. *Secure PDF Text Steganography Turning Secrecy Into Inconspicuous Encoding*. 4th International Conference of Intelligent Circuit and Systems . IOP Publishing. 2022

[6]K. Ridwan. *Hiding Random Text Using Steganography*. **International Journal of Multidisciplinary Research and Studies**. Vol 06, Issue 09, 2023, pp. 1 -13.

[7]T. Sullivan, "*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,** Vol 5, Issue VI, 2017.

[9]CommVault.: *Your Top 5 Cloud Data Protection Challenges. Solved*. 2014, Available at https://top-5-cloud-data-protection-challenges-solved.pdf (kapost-files-prod.s3.amazonaws.com)

[10]I. Giroti & M. Malhotra. Quantum Cryptography: *A Pathway to Secure Communication.* 6th International Conference on Computation System and Information Technology for Sustainable Solutions (CSITSS) 2022.

[11]G. D.Reddy, Yaddanapudi VSSRR Udai Kiran, Prabhdeep Singh, Shubhranshu Vikram Singh, Sanchita Shaw & Jitendra Singh. *A Proficient and secure way of Transmission using Cryptography and Steganography,* 2nd International Conference on Technological Advancements in Computational Sciences (ICTACS) 2022.

[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]H. Fernando, T. Hewavitharana ,A. Perera. *Evaluation of Electronic Document Management (EDM) Systems for construction organizations.* Moratuwa Engineering Research Conference (MERCon) 2019.

[14]P.Verma, V. Bittal, & N. Dongre. A*n Effective Technique for EDMS Using Smart Data Hub System*. International Conference on Smart Systems and Inventive Technology (ICSSIT) 2019.

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

[17]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**, 114(7), 2017, 325-335.

[18]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**, 67: 2017, 242-254.

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

[20]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.

[21]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.

[22]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, (ICECCT) (IEEE), 2019, pp. 1-4.

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

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

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

[26]A. Ikuomola, E.A. Oyekan & O.M. Orogbemi. *A Secured Cloud-Based Electronic Document Management System*. **International Journal of Innovative Research and Development,** 2022, DOI:10.24940/ijird/2022/v11/i12/DEC22010

[27]I. Nedoshytko & O. Patriak. *Electronic Document Management and its Value for Business.* **Digital Platform Information Technologies in Sociocultural Sphere,** 2022, DOI:10.31866/2617-796X.5.2.2022.270142.

[28]A. Ikuomola, E.A. Oyekan & O.M. Orogbemi. *A Secured Cloud-Based Electronic Document Management System*. **International Journal of Innovative Research and Development,** 2022, DOI:10.24940/ijird/2022/v11/i12/DEC22010.

[29]S. Fu, B. Thorsteinsdottir, Xin Zhang & G. S. Lopes. *A Hybrid Model to Identify Fall Occurrence from Electronic Health Records.* **International Journal of Medical Informatics**. 162(3): 2022 104736|DOI:10.1016/j.ijmedinf.2022.104736

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

[31]C. Xu, N. Wang, L. Zhu, K. Sharif & C. Zhang. *Achieving Searchable and Privacy-Preserving Data Sharing for Cloud-assisted E-Healthcare System*. **IEEE Internet of Things Journal**, 6(5), 2019, 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, (Springer, Cham), 2018, 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,** 7: 2019, 74361- 74382.

[34]S. Badr, I. Gomaa & E. Abd-Elrahman. *Multi-Tier Blockchain Framework for Iot-Ehrs Systems*. **Procedia Computer Science**,141: 2018, 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**, 485: 2019, 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**,7: 2019, 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, pp 1-10.

[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**, 20(2): 2019, 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, (IEEE), 2009, 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**,6: 2018, 27818- 27826.

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

[45]A. Alrawais,C. Hu, X. Xing & X. Cheng. *An Attribute-based Encryption Scheme to Secure Fog Communications*. **IEEE access**,Vol 5, 2017, pp. 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, 20(2), 2019, 97-108.

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

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

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

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

[51]Wencheng S, Z. Cai, Y. Li, F. Liu, S. Fang & G. Wang. *Security and Privacy in the Medical Internet of Things: A Review*. **Security and Communication Networks**. 2018, doi.org/10.1155/2018/5978636.

[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, pp. 1–10.

[54]A. Vishwanath, R. Peruri & J. He. *Security in Fog Computing Through Encryption*. **International Journal of Information Technology and Computer Science**, Vol 8, Issue 5, 2016, pp.28-36.

[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**, 106: *2018,* 90–99.

[56]L. Zou, M. Ni, Y. Huang, W. Shi & X. Li. *Hybrid Encryption Algorithm Based on Aes and Rsa in File Encryption*. International Conference on Frontier Computing, 2020. pp 541-551.

[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**, 17 (6), 2020,1322–32.

[58]H. Mahmoud, A. Hegazy & M. H. Khafagy. *An Approach for Big Data Security Based on Hadoop Distributed File System*. 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**, vol. 20, no. 18, 2020, 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**, vol. 16, 2017, pp. 1-11.

[63]S. R. Zeebaree. *Des Encryption and Decryption Algorithm Implementation Based on Fpga.* **Indonesian Journal of Electrical Engineering and Computer Science,** vol. 18, no. 2, 2020, 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**, vol. 4, no.1, 2020, pp. 49-57.

[65]P. Semwal & M. K. Sharma. *Comparative Study of Different Cryptographic Algorithms for Data Security in Cloud Computing.* 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**, vol. 2, no. 1, 2019, 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.* 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, vol. 981, no. 2, 2020, 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, vol. 2290, no. 1, 2020, p. 040022.

[71]N. Mohammed & N. Ibrahim. *Implementation of New Secure Encryption Technique for Cloud Computing.* 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*. **Association for Computational Linguistics,** 2021, pp. 3046–3055

[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**. 16, 2020, 880–895.

[74]H. Kang, H. Wu & H, X.Zhang. *Generative Text Steganography Based on Lstm Network and Attention Mechanism with Keywords.* **Electron. Imaging,** Vol 32, 2020, Article ID: art00021.

[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,** 14, 2018, 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**, 32, 2020, 216–224.

[77]R. Yang, & Z. H. Ling. *Linguistic Steganography by Sampling-based Language Generation*. In Proceedings of the Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC), Lanzhou, China, 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,** 4, 2019, 59–63.

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

[80]A. Majumder & S. Changder. *A Generalized Model of Text Steganography by Summary Generation Using Frequency Analysis*. In Proceedings of the 7th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), Noida, India, 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**. 77, 2018, 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,** 103(2), 2018, 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, 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.** Vol 16, Issue 3, 2020.

[85]N. Alghamdi & L. Berriche. *Capacity Investigation of Markov Chain-Based Statistical Text Steganography: Arabic Language Case.* In Proceedings of the Asia Pacific Information Technology Conference, Jeju Island, Korea, 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. Vol 1237, Issue 2, 2019, pp. 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 IEEE Second International Conference on Data Science in Cyberspace (DSC), Shenzhen, China,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** 8, 2020, 136537–136545.

[91]K. Wang & Q. Gao. *A Coverless Plain Text Steganography Based on Character Features*. **IEEE Access** 7, 2019, 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, 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, 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,** 79, 2020, 26549–26569.

[95]M. Fateh & M. Rezvani. *An Email-Based High Capacity Text Steganography Using Repeating Characters*. **Int. J. Comput. Appl,** 43, 2021, 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,** 80, 2020, 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, 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.** 32, 2018, 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.** Vol 34, Issue 4, 2022. pp. 1343 - 1356.

[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**. 33(8), 2019, pp. 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**. 33(9), 2019.

[103]A. Ditta, C. Yongquan, M. Azeem, K. G. Rana, H. Yu & M. Q. Memon. *Information Hiding: Arabic Text Steganography by Using Unicode Characters to Hide Secret Data*. **Int. J. Electron. Secur. Digit. Forensics** 10, 2018, pp. 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,** 6, 2018, 65981–65995.

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

[106]B. Khosravi, B. Khosravi & K. Nazarkardeh. *A New Method for PDF Steganography in Justified Texts*. **J. Inf. Secur.Appl.** 45, 2019, 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, 2016, pp. 1090–1094.

[108]S. G. R. Ekodeck & R. Ndoundam. *Steganography Based on Chinese Remainder Theorem*. **J. Inf. Secur. Appl**. 29, 2016, 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**. 2, 2021, 1–13.

[110]Z. Yang, L. Xiang, S. Zhang, X. Sun & Y. Huang. *Linguistic Generative Steganography with Enhanced Cognitive-Imperceptibility*. **IEEE Signal. Process. Lett**. 28, 2021, 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, 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**. 20, 2017, 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, Article ID: 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),** Vol 11, 2019.

[116]O. W. Liang & V. Iranmanesh. *Information Hiding Using Whitespace Technique in Microsoft Word*. In Proceedings of the 22nd International Conference on Virtual System & Multimedia (VSMM), Kuala Lumpur, Malaysia, 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,Volume 870, 2020, p. 012125.

[118]S. T. A. Shah, A. Khan & A. Hussain. *Text Steganography Using Character Spacing After Normalization*. **Int. J. Sci. Eng. Res,** 11, 2020, 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, pp. 1–13.

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

[121]L. Fan, O. Lo, W. Buchanan, E. Ekonomou, T. Sharif & C.Sheridan. SPoC: *Protecting Patient Privacy for e-Health Services in the Cloud.* The Fourth International Conference on eHealth, Telemedicine, and Social Medicine, 2012, pp. 98-104.

[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 Vol 89,** 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,** 67, 2017, 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** 78, 2016, 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, Vol** 41, Issue 6, 2008, 1028–1040.

[131]O. Rubio, A. Alesanco, & J. García. *A Robust and Simple Security Extension for the Medical Standard SCP-ECG*. **J Biomed Inf (46)1,** 2013, 142–151.

[132]N. A. Azeez, & A. B. Babatope. *An Alternative Approach to Network Intrusion Detection*. **Journal of Computer Science and its Application Vol 23, No 1** 2016.

[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,** Vol 50, 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** 13(1), 2016,17–25.

[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]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.

[139]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.

[140]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***, vol. 99, 2020, pp. 1–5.

[141]S. Dong, P. Wang, & K. Abbas. *A Survey on Deep Learning and its Applications.* ***Computer Science Review***, vol. 40, no. 1, 2021, Article ID 100379.

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

[143]Y. Liu, Z. Xu & W. Ye. *Image Neural Style Transfer with Preserving the Salient Regions*. **IEEE Access**, vol. 7, 2019, Article ID 40037.

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

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

[146]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.

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

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

[149]S. Zhang, S. Su, J. Lu, Q. Zhou, & C. Chang. *Csst-net: An Arbitrary Image Style Transfer Network of Coverless Steganography.* **The Visual Computer: International Journal of Computer Graphics, Vol 38, Issue 6,** 2022, pp. 2125–2137.

Chapter Three

Methodology

3.1 Classical LSB Framework

After the platform is designed or determined, then the output which is the secret message is then fed into the steganography stage, and for this study, Improved LSB technique will be implemented for the steganography stage.

The classical LSB bit uses different words, the 8th bit of some or all of the bytes within an image will be modified to a bit of the key message. Once employing a 24-bit image, a bit of each of the red, green and blue colour components are often used, since they're each represented by a computer memory unit(byte). In different words, one will store 3 bits in each pixel.

An 800 × 600 pixel image, will so store total quality of 1,440,000 bits or 180,000 bytes of embedded information. Within the LSB technique of Message concealing, the least significant bit will be replaced by the message bit of the key message. We tend to evaluated the technique victimization gray scale images of size 64*64 within which each pixel value will portrayed with 8 bit illustration.

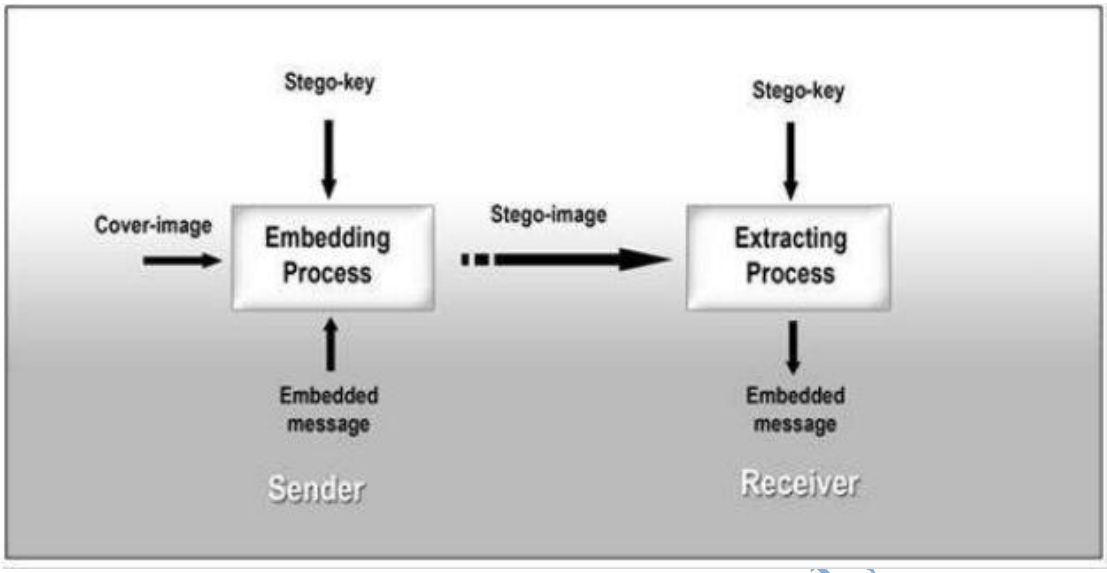

Figure 3.1 Classical Framework for Steganography[1].

After reviewing the current products on the market for steganography, it was determined that there was not a practical implementation for 8-bit images. Although network speed is increasing, and bandwidth problems are decreasing, file size is still of utmost importance and smaller file sizes are optimal in network communication. Thus, the current steganographic use of 24-bit images leads to slower communication and thus development of an 8-bit image format would be beneficial. A 24-bit bitmap image would be converted to an 8-bit bitmap image while simultaneously encoding the desired hidden information. An algorithm would be created to select representative colors out of the 24-bit image to create the palette for the 8-bit image. This palette would then be optimized to an 8-bit colormap that could be applied with minimal changes to the quality of the original image. This process of compressing the image from a 24-bit bitmap to an 8-bit bitmap resulted in minor variations in the image, which are barely noticeable to the human eye. However, these slight variations aid in hiding the data. Since there would not be an original 8-bit image to compare

with the stego-image, it would be impossible to discern that the slight variations caused by hiding the data are different from the slight variations caused by compression.

A practical steganographic implementation for 8-bit images enabled smaller file sizes to be utilized in steganographic communications. While also limiting the size of the hidden file, this implementation addressed issues that have been passed by in other applications, and provided a more compact vehicle for those secret communications that do not require a large cover-file.

3.2 Classical LSB Algorithm

In this system, the secret message is used to hide in a cover bmp image. Firstly each character of secret message and each pixel of cover bmp image are converted into binary values. The user has to input stego-key as the password (stego-key is used to embed the secret message in a cover file).

After inserting secret message into cover image file, the resulting stego-image is sent to the receiver through the desired communication channel. While defining the starting point of embedding LSB, the stego-key is firstly collected from the user. The summation of the ASCII value of each character of stego-key is calculated and then the average of those characters value is computed. While substituting the secret message into LSB of cover image, the first LSB position is chosen according to the calculated average value of input stego-key characters. Then the substitution processing will continue until the end of secret message.

A. The embedding algorithm at the sender side

Step (1) : Get the input cover image and secret message.

Step (2) : Accept the stego-key from the user and calculate average value of them.

Step (3) : Convert each character of secret message and each LSB bit of cover image (R channel) from the position of average of stego-key.

Step (4) : Substitute the LSB bit of cover image (R channel) with binary values of secret message with respect to the starting point until the end of secret message.

Step (5) : Insert the end character value at the end of secret message.

Step (6) : Calculate the PSNR, SNR of original and resulting images.

Step (7) : Send a stego-image to the receiver.

3.3 Enhanced LSB Framework

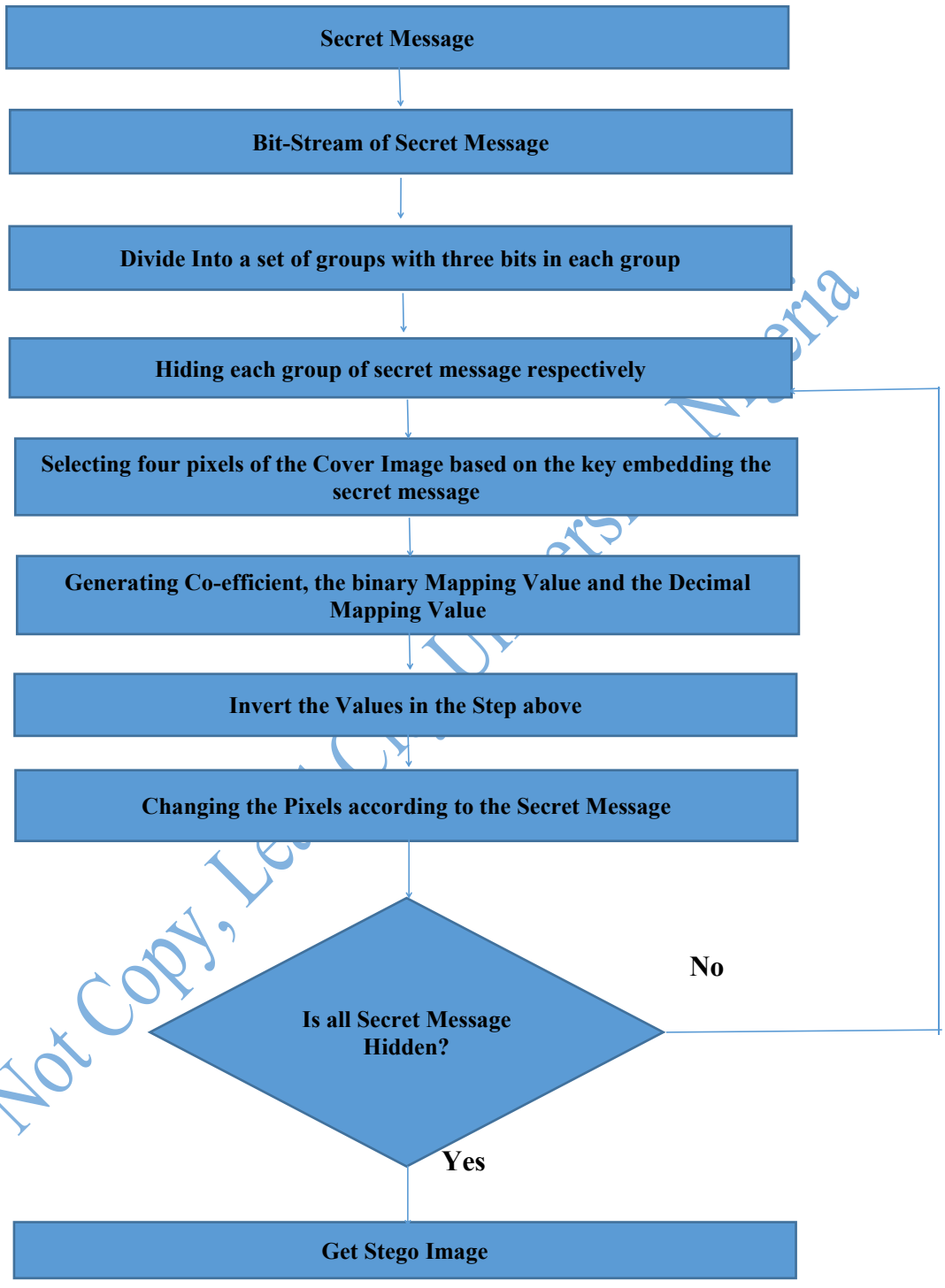

Figure 3.2 The Embedding Phase (Source: Researcher's Fieldwork, 2023)

B. The extracting algorithm at the receiver side

Step (1) : Get the input stego calculate average value

Step (2) : Load the stego-image that is sent from the sender.

Step (3) : Extract each of LSB bit from the stego image until to find out the end bit.

Step (4) : Reconstruct the collecting LSB bits from the stego-image.

Step (5) : Transform the LSB bits to correspondent characters.

In the embedding phase, we perform the following steps:

(i) We first convert the secret message into binary and thus we obtain a bitstream as the result of this step.

(ii) We divide the obtained bitstream into a set of groups with three bits in each group. To this end, from the least significant bit, we group every three continuous bits in a group.

(iii) In this step, a set of pixels from the cover image is selected based on the key to embedding the secret message. It is to be noted that the number of pixels

selected in this step is X length of the secret message. This is because every three bits in the secret message are hidden into four pixels of the cover image.

(iv) Now we generate every four coefficient. Note that by only one change in each coefficient we have a number in the range of [0, 7].

(v) Based on the bits in the secret message, we choose the operations needed to generate such a message.

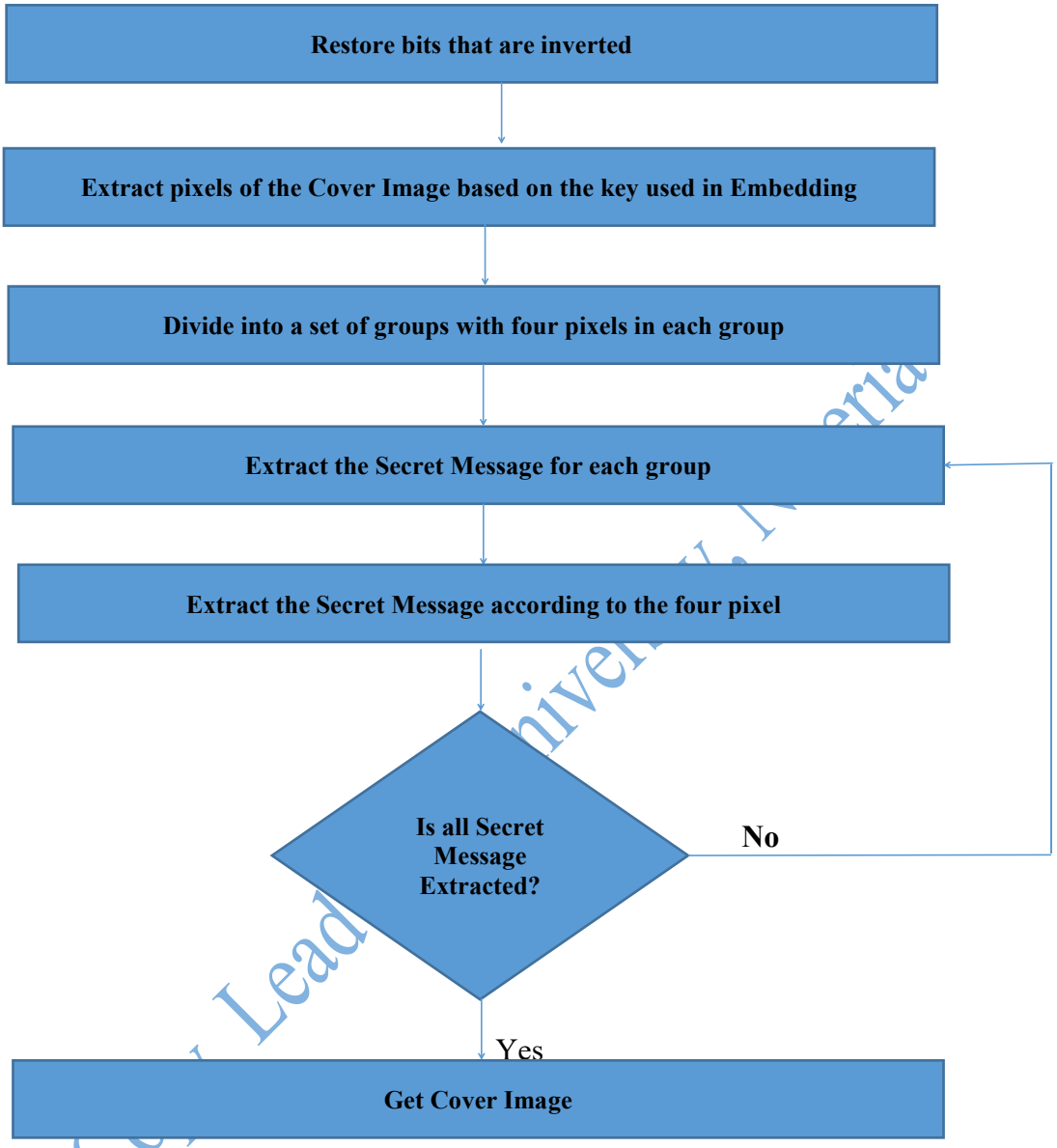

Figure 3.3 The Extracting Phase (Source: Researcher's Fieldwork, 2023)

The main steps in the extracting phase of our steganography approach are shown in Figure 3. 3 above

In the extracting phase, we only need to perform the mapping function over each group of four coefficient from the received image. In the extracting phase, we perform the following steps:

i. Restore bits that are inverted from the embedding

ii. We first extract pixels of the cover image based on the key in the embedding phase

iii. We divide the pixels into a set of groups with four pixels in each group

iv. We extract a secret message according to the four pixels and equation (9) for each group.

v. We add the secret messages to each other and thus we obtain a bit-stream of secret messages as the result of this step

Endnotes

[1]A. Kumar Sahu & M. Sahu. *Digital image steganography and steganalysis: A journey of the past three decades.* **Open Comput. Sci**. 10, 2020, 296–342

Chapter Four

Results and Discussion

4.1 Discussion

Steganography been implemented in this study uses 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.

For the sake of the Peculiarity of this study to Information Security, as much emphasis is laid on the Steganography phase. Figure 4.1 shows the interface that allows for the Users, to input there preferred text, this interface is not limited to any users as it can be used by any user that has access to the software solution being developed.

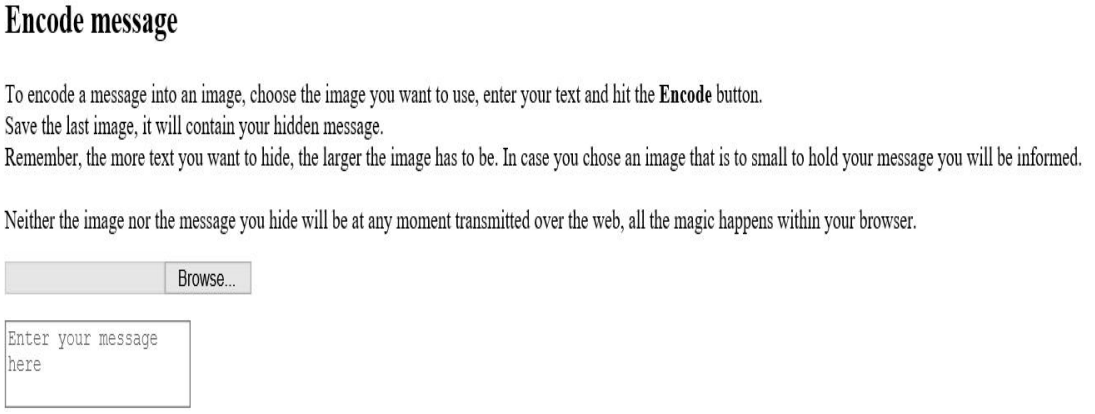

Figure 4.1 Interface showing the Encoding page (Source: Researcher's Fieldwork, 2023)

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.

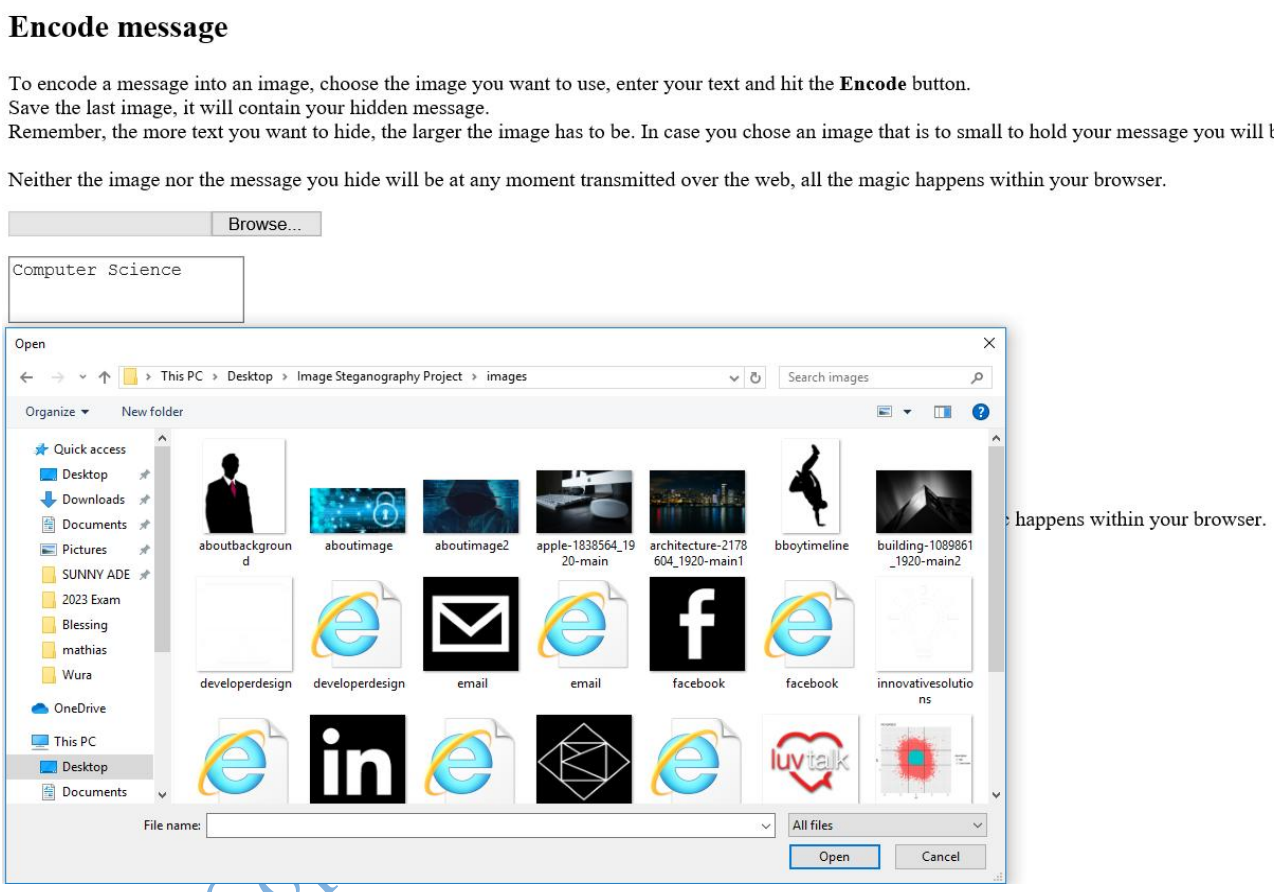

Figure 4.2 Interface showing the "SELECT IMAGE" phase for the steganography Technique (Source: Researcher's Fieldwork, 2023)

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.

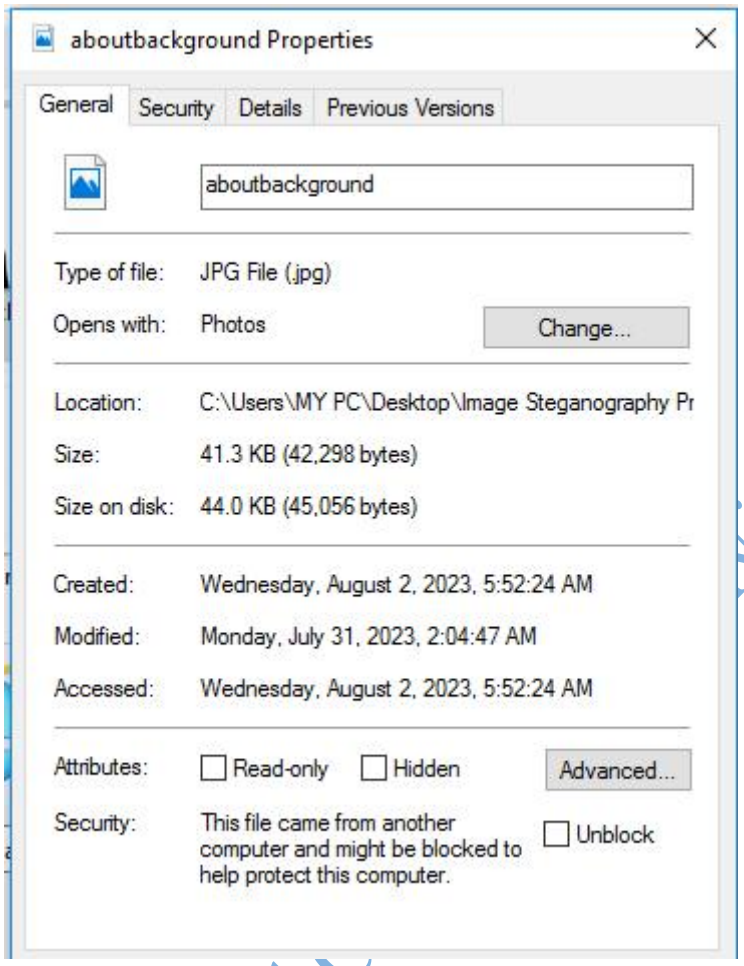

Figure 4.3 Interface Showing the Properties of the selected Image where text is to be hidden (Source: Researcher's Fieldwork, 2023)

The figure in 4.3 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.

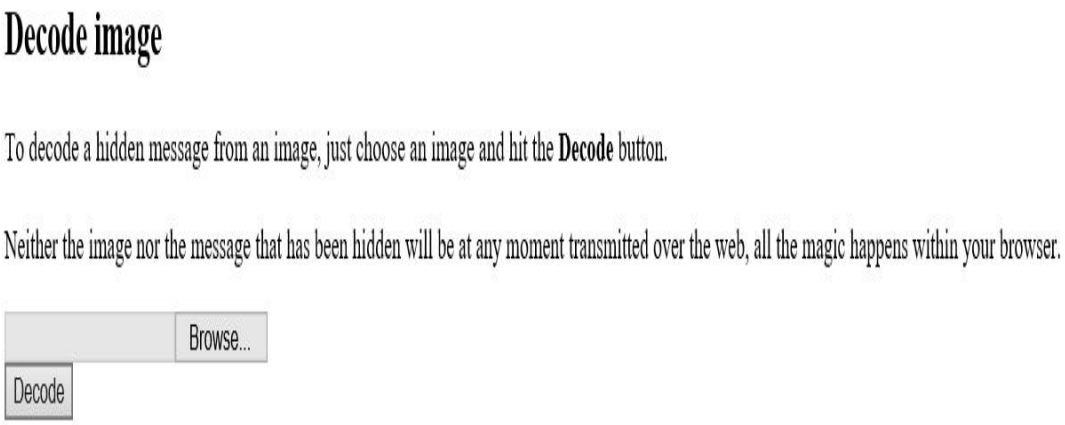

Figure 4.4 Interface showing the Decoding Phase (Source: Researcher's Fieldwork, 2023)

The figure above shows two things, the first activity shown in the above figure is the Cipher-text to be hidden in the image, which is the Cipher-text 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.

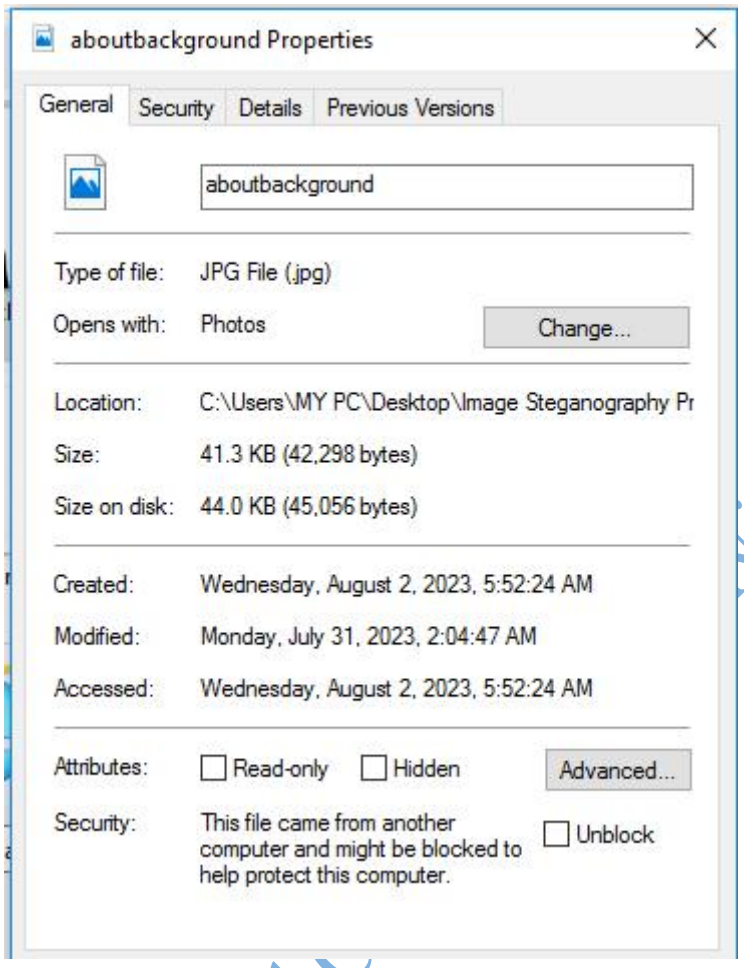

Figure 4.5 Interface Showing the Properties of the Stego. Image when text is hidden (Source: Researcher's Fieldwork, 2023)

4.2 Parameters of Evaluation

The parameters used for evaluating the Steganography technique which encompasses the original image and the encoded image are Mean Square Error and Peak Signal to Noise Ratio. The table below shows the evaluation of the steganographic technique as against another technique was is referred to as pixel based algorithm.

To calculate PSNR

PSNR (peak signal to noise ratio) - PSNR Peak signal-to-noise ratio often abbreviated PSNR, is an engineering name, for the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity. The peak error between the compressed image and original image is measured in terms of PSNR .

The higher value of PSNR indicates higher quality of image. To calculate PSNR, MSE is first computed. Cumulative difference between the compressed image and original image is MSE. Small value of MSE improves image quality and reduces the error.

PSNR = 10 log10 (R2/ MSE)

R is either specified by the user or taken from the range of the image data type. For example, for an image of data type uint8, the value for R is 255.

To calculate the MSE

Mean square error (MSE) -Mean Squared Error (MSE) is defined as the square of differences in the pixel values between the corresponding pixels of the two images. The mean square error (MSE) of N * M size image is given by,

MSE= ΣM, N [I1 (m, n) – I2 (m, n)] 2 / (M*N)

M &N -number of rows and columns in the input images

Cover Image	Word Length	Dimension	MSE	PSNR
20230802_103016.jpg	200	981*1150	3.331	42.987
20230802_103016.jpg	500	981*1150	3.156	41.763
20230802_103016.jpg	1374	981*1150	3.186	41.234
20230804_150118.jpg	200	620*300	6.611	37.436
20230804_150118.jpg	500	620*300	3.321	37.873
20230804_150118.jpg	1374	620*300	4.889	36.437
20230805_091010.jpg	200	800*450	6.669	40.345
20230805_091010.jpg	500	800*450	7.985	41.123
20230805_091010.jpg	1374	800*450	6.523	39.878

Table 4.1 Performance Evaluation of the Cover Image (Source: Researcher's Fieldwork, 2023)

Cover Image	Size (kb)	Word Length	Dimension	I.MSE	I.PSNR	**Stego Image**	**PSNR**	**MSE**	**Size (kb)**
20230802_103016.jpg	258	200	981*1150	3.331	42.987	Lenna 512 * 580	63.3454	0.0301	110
20230802_103016.jpg	258	500	981*1150	3.156	41.763	Lenna 512 * 585	62.3319	0.038	234
20230802_103016.jpg	258	1374	981*1150	3.186	41.234	Lenna 555 * 580	62.3132	0.0382	500
20230804_150118.jpg	564	200	620*300	6.611	37.436	Peppers 384 * 512	63.2896	0.0305	134
20230804_150118.jpg	564	500	620*300	3.321	37.873	Peppers 384 * 550	62.3275	0.038	178
20230804_150118.jpg	564	1374	620*300	4.889	36.437	Peppers 384 * 567	62.3876	0.0375	432
20230805_091010.jpg	674	200	800*450	6.669	40.345	Kids 318 * 400	59.5063	0.0729	149
20230805_091010.jpg	674	500	800*450	7.985	41.123	Kids 318 * 405	58.5506	0.0908	274
20230805_091010.jpg	674	1374	800*450	6.523	39.878	Kids 318 * 411	58.5638	0.0905	556

Table 4.2 Comparison of the Image with a traditional LSB image(Source: Researcher's Fieldwork, 2023)

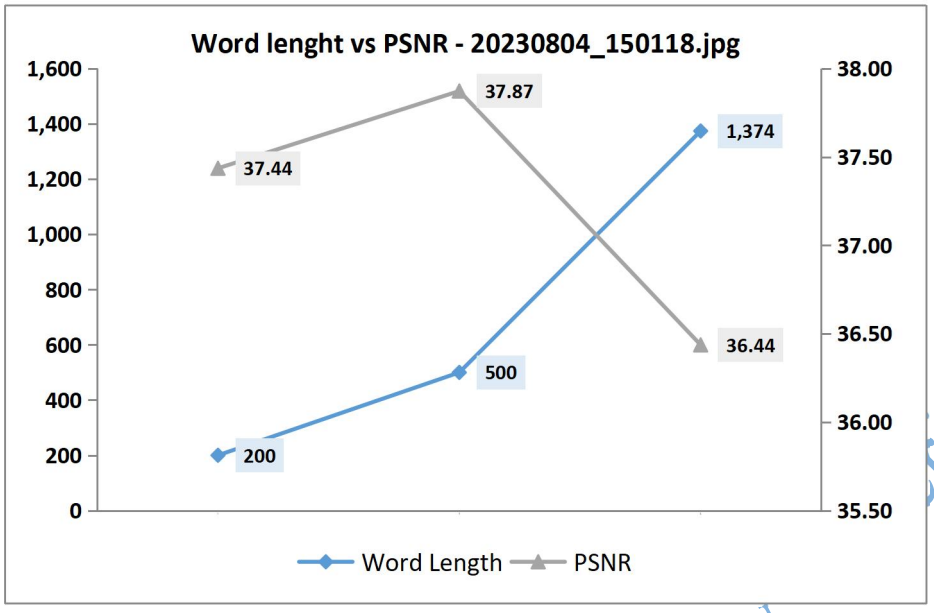

Figure 4.6 Graphical Representation for the PSNR for Image 20230804_150118.jpg

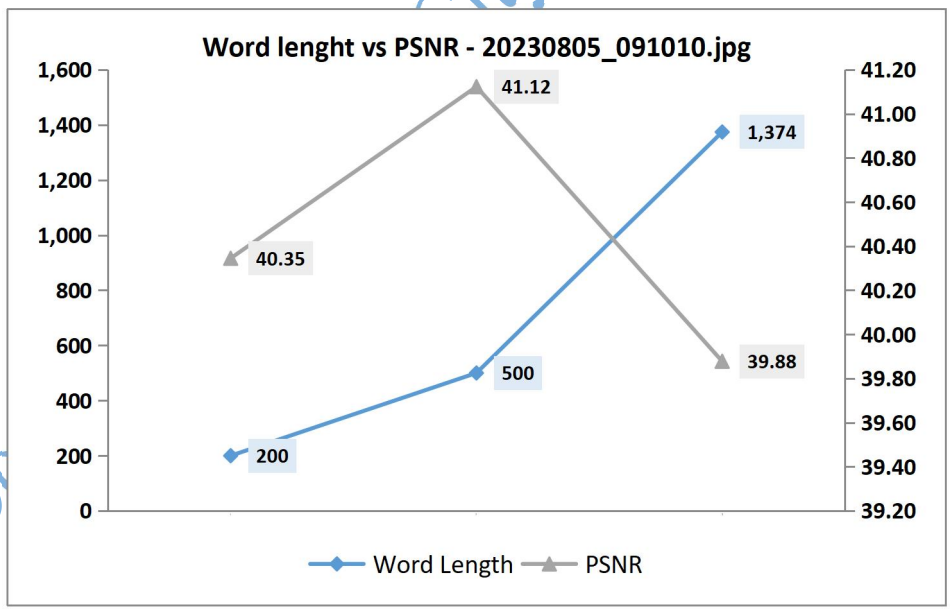

Figure 4.7 Graphical Representation for the PSNR for Image 20230805_091010.jpg

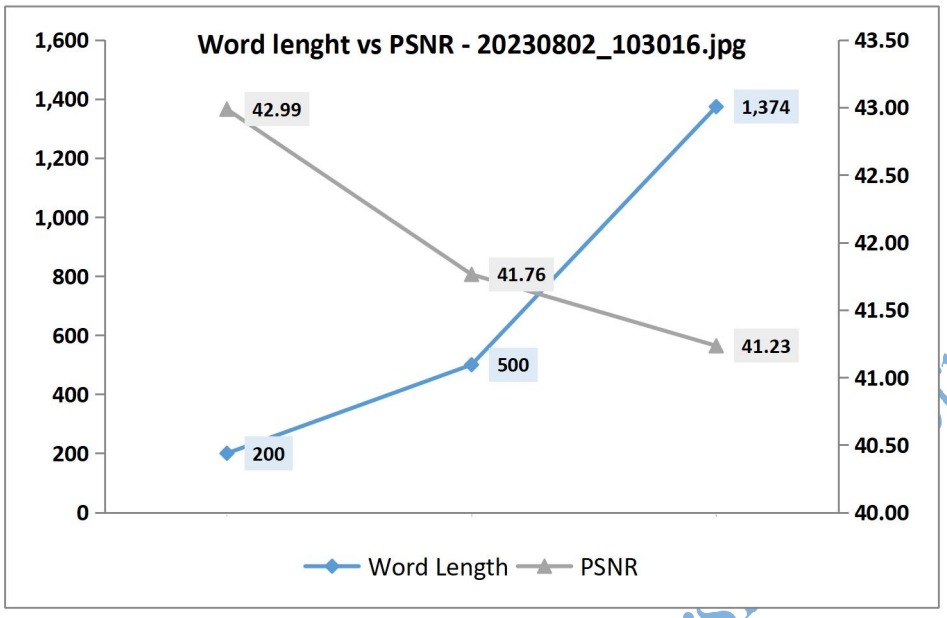

Figure 4.8 Graphical Representation for the PSNR for Image 20230802_103016.jpg

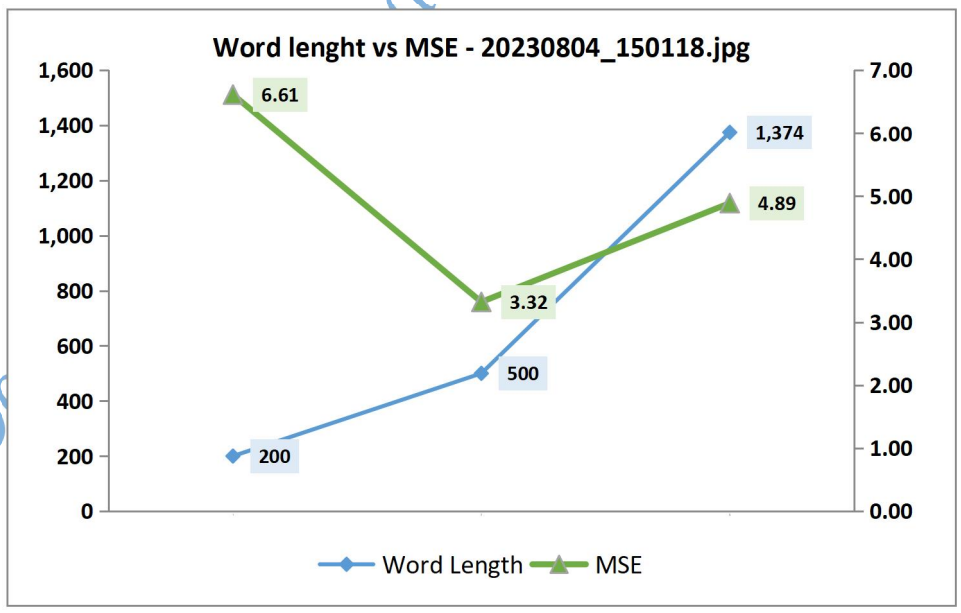

Figure 4.9 Graphical Representation for the MSE for Image 20230804_150118.jpg

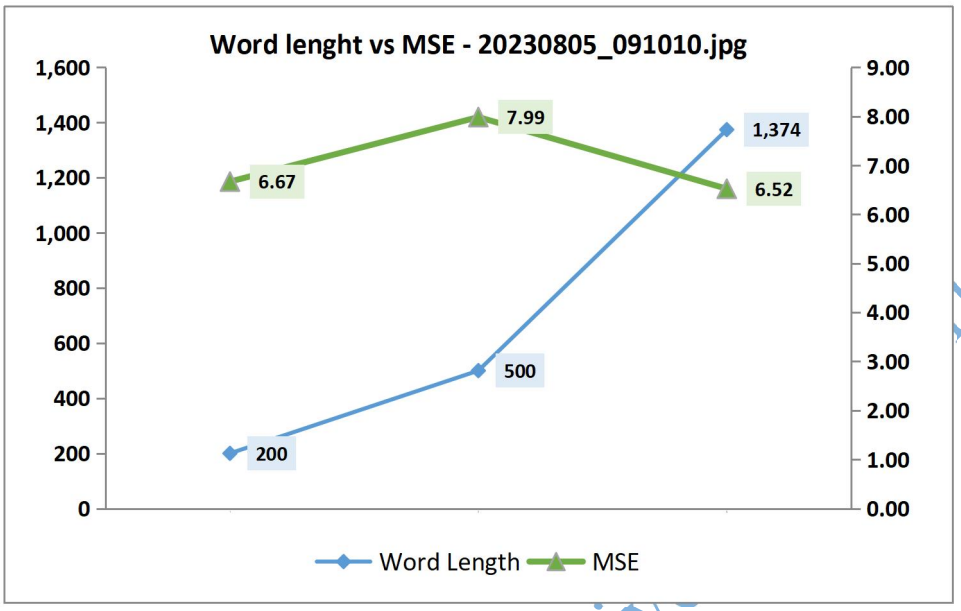

Figure 4.10 Graphical Representation for the MSE for Image 20230805_091010.jpg

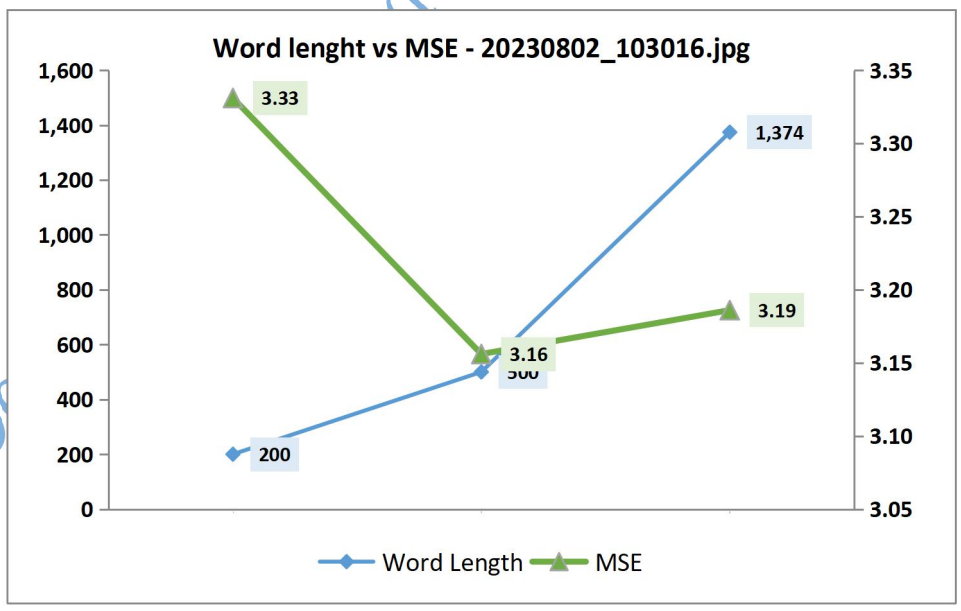

Figure 4.11 Graphical Representation for the MSE for Image 20230802_103016.jpg

The PSNR gets better with the increase in compressed image bit rate as shown in the table above. The results show increasing trend in PSNR values on the other hand MSE decreases gradually with the improvement in compressed image bit rate. Hence greater the compressed image bit rate, better the quality of the image as well as errors on lower side.

Chapter Five

Conclusion

5.1 Summary of Results

The steganography technique in this study makes it difficult to solve sensitive medical data that are encoded using this two technique. If solving any cryptographic technique comes within a short time using any of the attacks, combining the cryptography encryption technique Steganography technique 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 steganography but also employ the use of a watermarking technique to help strengthen the security of sensitive information that is been stored using this technique. If we keep having techniques that can protect our sensitive data then we should not be scared to share our 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.

5.2 Recommendation

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

The steganography 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 this study 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 information security in the aspect of the following;

i. Confidentiality

ii. Integrity and,

iii. Availability.

This study has also help contributed greatly to the field of computing by showcasing how good steganography techniques.

5.4 Suggested Area of Further Research

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. And also aside the use of Image Steganography, other techniques using other forms of multimedia formats such as Audio and Video formats can be employed in further studies to implement cases in Information Security.

Bibliography

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.* In 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.** 5, 2017, 9131-9138.

Alsaadi E. M, Fayadh S. M & Alabaichi A. *A Review on Security Challenges and Approaches in the Cloud Computing.* InAIP Conference Proceedings**.**vol. 2290, no. 1, 2020, 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, Volume 870, June 2020, 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.

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.

Tongxu Yue, 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.

Dumoulin V., Shlens J & Kudlur M. *A Learned Representation for Artistic Style*. In *Proceedings of the Conference on ICLR*, Toulon, France, 2016, 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.

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 Workshops,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 Survey 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), 2018, 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.

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 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),2010 pp. 220-229.

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, 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*. In Proceedings 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.

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.

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 2016 International Seminar on Intelligent Technology and Its Applications (ISITIA) (IEEE),2016, pp. 387-392.

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.

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.

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: I*nvisible 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.

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.

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.

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.

Journals

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.

Sahu A. K & Sahu M. *Digital image steganography and steganalysis: A journey of the past three decades.* **Open Comput. Sci**. 10, 2020, 296–342

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.** 2022.

Alanazi N, Khan E, & Gutub A. *Efficient Security and Capacity Techniques for Arabic Text Steganography via Engaging Unicode Standard Encoding.* ***Multimed*** **Tools and Application** 80(2), 2020.

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**, vol. 2, no. 1, 2019, 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**. 33, 2019, 963–974.

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

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**, 20(2): 2019, 97-108.

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

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

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

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**, Vol 29, Issues 4, 2017, 505 - 519.

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

Cao S, Zhang G, Liu P, Zhang X, & Neri F. *Cloud-assisted Secure eHealth Systems for Tamper-proofing EHR via Blockchain*. **Information Sciences**, 485, 2019 427- 440.

Chandrashekhar A.M & Shashikumar. *Cloud Computing Service and Deployment Models.* **International Journal for Research in Applied Science and Engineering technology**, Vol 5, Issue VI, 2017.

Chaw A. A. *Text steganography in Letter of Credit (LC) Using Synonym Substitution Based Algorithm*. **Int. J. Adv. Res. Dev,** 4, 2019, 59–63.

Chinnasamy P, Padmavathi S, Swathy R & Rakesh S. *Efficient Data Security Using Hybrid Cryptography on Cloud Computing.* **In Inventive Communication and Computational Technologies, Springer**,2020, pp. 537-547.

Dalal M. & Juneja M. "*A Secure Video Steganography Scheme Using DWT Based on Object Tracking*. **Information Security Journal: A Global Perspective**, 31(4). 2021, pp. 1–18.

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

Ditta A., Yongquan C., Azeem M., Rana K. G., Yu H & Memon M. Q. *Information Hiding: Arabic Text Steganography by Using Unicode Characters to Hide Secret Data*. **Int. J. Electron. Secur. Digit. Forensics** 10, 2018, 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, , 2021, Article ID 100379.

Drozdowicz M, Ganzha M, & Paprzycki M. *Semantically Enriched Data Access Policies in eHealth*. **Journal of Medical Systems**, 40(11): 2016, 238.

Ekodeck S. G. R & Ndoundam R. *Steganography Based on Chinese Remainder Theorem*. **J. Inf. Secur. Appl**. 29, 2015, 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 Seganography Using Repeating Characters*. **Int. J. Comput. Appl**. 43(3), 2018, 1–7.

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.

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**. 33, 2021, 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.** vol. 4, no.1, 2020, 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. 2014.

Jayapandiyan J. R, Kavitha C & Sakthivel K. *Enhanced Least Significant bit Replacement Algorithm in Spatial Domain of Steganography Using Character Sequence Optimization*. **IEEE Access.** 8, 2020, 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.

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** ,291, 2020.

Keshta I. & A. Odeh. *Security and Privacy of Electronic Health Records: Concern and Challenges*. **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.** 45, 2019, 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, 2021, Article ID 107618.

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

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.** 17 (6): 2020, 1322–32.

Liu Y, Xu Z., Ye W. *Image Neural Style Transfer with Preserving the Salient Regions*. ***IEEE Access***, vol. 7, 2019, Article ID 40037.

Liu Z., Weng J. , Li J., Yang J., Fu C. & Jia C. *Cloud-Based Electronic Health Record System Supporting Fuzzy Keyword Search. **Soft Computing.** **20**(8): 2015,* 3243- 3255.

Maji G. & Mandal S. *A Forward Email Based High Capacity Text Steganography Technique Using a Randomized and Indexed Word Dictionary*. **Multimedia Tools Appl**. 79, 2020, 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**. 20,2017, 72–79.

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**. 103, 2018, 1563–1585.

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

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. *Distributed Clinical Data Sharing via Dynamic Access Control 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.*** 44(3), *2015,* 23-38.

Sahi A., Lai D & Li Y. *Security and Privacy Preserving Approaches in the eHealth Clouds with Disaster Recovery Plan*. **Comput Biol Med.** 78, 2016, 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**., 11, 2020, 949–957.

Sharma S, Chen K & Sheth A. *Toward Practical Privacy Preserving Analytics for IoT and Cloud-based Healthcare Systems*. **IEEE Internet Computin.** 22 (2), 2018, 42-51.

Sridevi R. & Nithiya C. *E-Health Security Using ECC Algorithm.* **International Journal of Advanced Research in Basic Engineering Sciences and Technology** *(IJARBEST).* **2**(19):2016, 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. 2**(2): *2013,*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**. 32, 2018, 658–665.

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***. ***4***(**1**): *2014,* 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**, Vol. 7, No. 10, 2016.

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). 5**(6): *2014,* 7745-7747.

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

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.

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

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,** 14, 2018, 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**. 28, 2021, 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**. 16, 2020, 880–895.

Zeebaree S. R. *DES Encryption and Decryption Algorithm Implementation Based on FPGA.* **Indonesian Journal of Electrical Engineering and Computer Science,** vol. 18, no. 2, 2020, pp.774-781, doi: 10.11591/ijeecs.v18.i2.pp774- 781.

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.

Online Sources

CommVault.: Your Top 5 Cloud Data Protection Challenges. Solved. 2014, Available at https://top-5-cloud-data-protection-challenges-solved.pdf (kapost-files-prod.s3.amazonaws.com)

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

Appendix

Programming Code for the Encryption, Decryption and the Steganography Technique

Appendix I

```
import pandas as pd
import numpy as np
import matplotlib.pyplot as plt
import seaborn as sns
# %matplotlib inline

df = pd.read_csv('RTA Dataset.csv')
df.head()
df.shape
# print the dataset information
df.info()

df.isnull().sum()/100

df['Accident_severity'].value_counts().plot(kind='bar')

import matplotlib.pyplot as plt

# Plot the bar chart
ax = df['Accident_severity'].value_counts().plot(kind='bar', color=['#FF6347', '#4169E1', '#32CD32'])

# Customize the plot
```

```
ax.set_xlabel('Accident Severity')
ax.set_ylabel('Count')
ax.set_title('Distribution of Accident Severity')
ax.legend(['Minor', 'Moderate', 'Severe'])
ax.grid(axis='y', linestyle='--')

# Save the plot
plt.savefig('accident_severity_plot.png')
plt.show()

"""This shows imbalance multiclass label on the dataset"""

# plot the bar plot of road_surface_type and accident severity feature
plt.figure(figsize=(6,5))
sns.countplot(x='Road_surface_type', hue='Accident_severity', data=df)
plt.xlabel('Rode surafce type')
plt.xticks(rotation=60)
plt.savefig('accident_severity_plot.png')
plt.show()

# convert object type column into datetime datatype column
df['Time'] = pd.to_datetime(df['Time'])

# Extrating 'Hour_of_Day' feature from the Time column
new_df = df.copy()
new_df['Hour_of_Day'] = new_df['Time'].dt.hour
df_new = new_df.drop('Time', axis=1)
df_new.head()

def fill_missing_values(df):
    # Loop over each column in the dataframe
    for col in df.columns:
        if df[col].dtype == 'float64' or df[col].dtype == 'int64': # Check if column is
numeric
```

```
                # Fill missing values with mean
                df[col].fillna(df[col].mean(), inplace=True)
            else:
                # Fill missing values with mode
                df[col].fillna(df[col].mode()[0], inplace=True)
    return df

# Fill missing values using the function
df_new = fill_missing_values(df_new)

df_new.isnull().sum()

from sklearn.preprocessing import LabelEncoder

def label_encode_features(df):
    le = LabelEncoder() # create a label encoder object

    for col in df.columns:
        if df[col].dtype == 'object': # check if column is of type 'object'
            df[col] = le.fit_transform(df[col].astype(str)) # label encode the column

    return df

# Label encode the object-type features using the function
new_df = label_encode_features(new_df)

new_df.head()

df_new.columns

#handling imbalance multiclass
X = new_df.drop(['Accident_severity', 'Time'], axis=1)
y = new_df['Accident_severity']
```

```
X

!pip install imblearn

from sklearn.model_selection import train_test_split, cross_val_score
from sklearn.preprocessing import LabelEncoder, StandardScaler
from sklearn.pipeline import Pipeline
from imblearn.pipeline import make_pipeline
from imblearn.over_sampling import SMOTE
from sklearn.ensemble import RandomForestClassifier, GradientBoostingClassifier,VotingClassifier
from sklearn.metrics import classification_report, confusion_matrix, accuracy_score

le = LabelEncoder()
y = le.fit_transform(y)
sc = StandardScaler()
X = sc.fit_transform(X)
X_train, X_test, y_train, y_test = train_test_split(X, y, test_size=0.3, random_state=42)
smote = SMOTE(random_state=42)
X_train_res, y_train_res = smote.fit_resample(X_train, y_train)

# modelling using random forest baseline
rf = RandomForestClassifier(n_estimators=800, max_depth=20, random_state=42)

rf.fit(X_train_res, y_train_res)

# predicting on test data
predics = rf.predict(X_test)

cm = confusion_matrix(y_test, predics)
ConfusionMatrixDisplay(cm).plot()
```

```
# classification report on test dataset
classif_re = classification_report(y_test,predics)
print(classif_re)

from sklearn import tree
from sklearn.tree import DecisionTreeClassifier
from sklearn import metrics
from sklearn.metrics import confusion_matrix
from sklearn.metrics import classification_report
from sklearn.metrics import ConfusionMatrixDisplay

decisionTree = DecisionTreeClassifier(criterion='entropy')
print(decisionTree)

dtc_model = decisionTree.fit(X_train_res, y_train_res)

from matplotlib import pyplot

# feature importance

importance = dtc_model.feature_importances_
for i,v in enumerate(importance):
  print('Feature: %0d, Score: %.5f' % (i,v))

# Barchat for feature importance

pyplot.bar([x for x in range(len(importance))], importance)
pyplot.show()

prediction = dtc_model.predict(X_test)

cm = confusion_matrix(y_test, prediction)
ConfusionMatrixDisplay(cm).plot()
print(classification_report(y_test, prediction))
```

```
import pandas as pd
from sklearn.model_selection import train_test_split
from sklearn.ensemble import RandomForestClassifier
from sklearn.metrics import accuracy_score, classification_report, confusion_matrix

# Load the dataset (replace 'your_dataset.csv' with your actual dataset file)
data = pd.read_csv('your_dataset.csv')

# Feature columns (replace 'feature1', 'feature2', etc. with the actual feature column
names)
features = data[['feature1', 'feature2', 'feature3', ...]]

# Target column (replace 'target' with the actual column containing the severity codes)
target = data['target']

# Split the data into training and testing sets (adjust the test_size as needed)
X_train, X_test, y_train, y_test = train_test_split(features, target, test_size=0.25,
random_state=42)

# Initialize the Random Forest Classifier
rf_classifier = RandomForestClassifier()

# Train the model
rf_classifier.fit(X_train, y_train)

# Make predictions on the test set
y_pred = rf_classifier.predict(X_test)

# Calculate accuracy
accuracy = accuracy_score(y_test, y_pred)
print(f"Accuracy: {accuracy}")
# Generate classification report and confusion matrix
print("\nClassification Report:")
print(classification_report(y_test, y_pred))
```

```
print("\nConfusion Matrix:")
print(confusion_matrix(y_test, y_pred))

import pandas as pd
import numpy as np
import matplotlib.pyplot as plt
import seaborn as sns
# %matplotlib inline

df = pd.read_csv('RTA Dataset.csv')
df.head()
df.shape
# print the dataset information
df.info()

df.isnull().sum()/100

df['Accident_severity'].value_counts().plot(kind='bar')

import matplotlib.pyplot as plt

# Plot the bar chart
ax = df['Accident_severity'].value_counts().plot(kind='bar', color=['#FF6347',
'#4169E1', '#32CD32'])

# Customize the plot
ax.set_xlabel('Accident Severity')
ax.set_ylabel('Count')
ax.set_title('Distribution of Accident Severity')
ax.legend(['Minor', 'Moderate', 'Severe'])
ax.grid(axis='y', linestyle='--')

# Save the plot
plt.savefig('accident_severity_plot.png')
```

```
plt.show()

"""This shows imbalance multiclass label on the dataset"""

# plot the bar plot of road_surface_type and accident severity feature
plt.figure(figsize=(6,5))
sns.countplot(x='Road_surface_type', hue='Accident_severity', data=df)
plt.xlabel('Rode surafce type')
plt.xticks(rotation=60)
plt.savefig('accident_severity_plot.png')
plt.show()

# convert object type column into datetime datatype column
df['Time'] = pd.to_datetime(df['Time'])

# Extrating 'Hour_of_Day' feature from the Time column
new_df = df.copy()
new_df['Hour_of_Day'] = new_df['Time'].dt.hour
df_new = new_df.drop('Time', axis=1)
df_new.head()

def fill_missing_values(df):
    # Loop over each column in the dataframe
    for col in df.columns:
        if df[col].dtype == 'float64' or df[col].dtype == 'int64': # Check if column is
numeric
            # Fill missing values with mean
            df[col].fillna(df[col].mean(), inplace=True)
        else:
            # Fill missing values with mode
            df[col].fillna(df[col].mode()[0], inplace=True)
    return df

# Fill missing values using the function
```

```
df_new = fill_missing_values(df_new)

df_new.isnull().sum()

from sklearn.preprocessing import LabelEncoder

def label_encode_features(df):
    le = LabelEncoder() # create a label encoder object

    for col in df.columns:
        if df[col].dtype == 'object': # check if column is of type 'object'
            df[col] = le.fit_transform(df[col].astype(str)) # label encode the column

    return df

# Label encode the object-type features using the function
new_df = label_encode_features(new_df)

new_df.head()

df_new.columns

#handling imbalance multiclass
X = new_df.drop(['Accident_severity', 'Time'], axis=1)
y = new_df['Accident_severity']

X

!pip install imblearn

from sklearn.model_selection import train_test_split, cross_val_score
from sklearn.preprocessing import LabelEncoder, StandardScaler
from sklearn.pipeline import Pipeline
```

```
from imblearn.pipeline import make_pipeline
from imblearn.over_sampling import SMOTE
from sklearn.ensemble import RandomForestClassifier, GradientBoostingClassifier,VotingClassifier
from sklearn.metrics import classification_report, confusion_matrix, accuracy_score

le = LabelEncoder()
y = le.fit_transform(y)
sc = StandardScaler()
X = sc.fit_transform(X)
X_train, X_test, y_train, y_test = train_test_split(X, y, test_size=0.3, random_state=42)
smote = SMOTE(random_state=42)
X_train_res, y_train_res = smote.fit_resample(X_train, y_train)

# modelling using random forest baseline
rf = RandomForestClassifier(n_estimators=800, max_depth=20, random_state=42)

rf.fit(X_train_res, y_train_res)

# predicting on test data
predics = rf.predict(X_test)

cm = confusion_matrix(y_test, predics)
ConfusionMatrixDisplay(cm).plot()

# classification report on test dataset
classif_re = classification_report(y_test,predics)
print(classif_re)

from sklearn import tree
from sklearn.tree import DecisionTreeClassifier
from sklearn import metrics
from sklearn.metrics import confusion_matrix
```

```
from sklearn.metrics import classification_report
from sklearn.metrics import ConfusionMatrixDisplay

decisionTree = DecisionTreeClassifier(criterion='entropy')
print(decisionTree)

dtc_model = decisionTree.fit(X_train_res, y_train_res)

from matplotlib import pyplot

# feature importance

importance = dtc_model.feature_importances_
for i,v in enumerate(importance):
  print('Feature: %0d, Score: %.5f' % (i,v))

# Barchat for feature importance

pyplot.bar([x for x in range(len(importance))], importance)
pyplot.show()

prediction = dtc_model.predict(X_test)

cm = confusion_matrix(y_test, prediction)
ConfusionMatrixDisplay(cm).plot()
print(classification_report(y_test, prediction))
import pandas as pd
from sklearn.model_selection import train_test_split
from sklearn.ensemble import RandomForestClassifier
from sklearn.metrics import accuracy_score, classification_report, confusion_matrix

import pandas as pd
import numpy as np
import matplotlib.pyplot as plt
```

```
import seaborn as sns
# %matplotlib inline

df = pd.read_csv('RTA Dataset.csv')
df.head()
df.shape
# print the dataset information
df.info()

df.isnull().sum()/100

df['Accident_severity'].value_counts().plot(kind='bar')

import matplotlib.pyplot as plt

# Plot the bar chart
ax = df['Accident_severity'].value_counts().plot(kind='bar', color=['#FF6347',
'#4169E1', '#32CD32'])

# Customize the plot
ax.set_xlabel('Accident Severity')
ax.set_ylabel('Count')
ax.set_title('Distribution of Accident Severity')
ax.legend(['Minor', 'Moderate', 'Severe'])
ax.grid(axis='y', linestyle='--')

# Save the plot
plt.savefig('accident_severity_plot.png')
plt.show()

"""This shows imbalance multiclass label on the dataset"""

# plot the bar plot of road_surface_type and accident severity feature
plt.figure(figsize=(6,5))
```

```
sns.countplot(x='Road_surface_type', hue='Accident_severity', data=df)
plt.xlabel('Rode surafce type')
plt.xticks(rotation=60)
plt.savefig('accident_severity_plot.png')
plt.show()

# convert object type column into datetime datatype column
df['Time'] = pd.to_datetime(df['Time'])

# Extrating 'Hour_of_Day' feature from the Time column
new_df = df.copy()
new_df['Hour_of_Day'] = new_df['Time'].dt.hour
df_new = new_df.drop('Time', axis=1)
df_new.head()

def fill_missing_values(df):
    # Loop over each column in the dataframe
    for col in df.columns:
        if df[col].dtype == 'float64' or df[col].dtype == 'int64': # Check if column is
numeric
            # Fill missing values with mean
            df[col].fillna(df[col].mean(), inplace=True)
        else:
            # Fill missing values with mode
            df[col].fillna(df[col].mode()[0], inplace=True)
    return df

# Fill missing values using the function
df_new = fill_missing_values(df_new)

df_new.isnull().sum()

from sklearn.preprocessing import LabelEncoder
```

```
def label_encode_features(df):
    le = LabelEncoder() # create a label encoder object

    for col in df.columns:
        if df[col].dtype == 'object': # check if column is of type 'object'
            df[col] = le.fit_transform(df[col].astype(str)) # label encode the column

    return df

# Label encode the object-type features using the function
new_df = label_encode_features(new_df)

new_df.head()

df_new.columns

#handling imbalance multiclass
X = new_df.drop(['Accident_severity', 'Time'], axis=1)
y = new_df['Accident_severity']

X

!pip install imblearn

from sklearn.model_selection import train_test_split, cross_val_score
from sklearn.preprocessing import LabelEncoder, StandardScaler
from sklearn.pipeline import Pipeline
from imblearn.pipeline import make_pipeline
from imblearn.over_sampling import SMOTE
from sklearn.ensemble import RandomForestClassifier, GradientBoostingClassifier,VotingClassifier
from sklearn.metrics import classification_report, confusion_matrix, accuracy_score
```

```
le = LabelEncoder()
y = le.fit_transform(y)
sc = StandardScaler()
X = sc.fit_transform(X)
X_train, X_test, y_train, y_test = train_test_split(X, y, test_size=0.3, random_state=42)
smote = SMOTE(random_state=42)
X_train_res, y_train_res = smote.fit_resample(X_train, y_train)

# modelling using random forest baseline
rf = RandomForestClassifier(n_estimators=800, max_depth=20, random_state=42)

rf.fit(X_train_res, y_train_res)

# predicting on test data
predics = rf.predict(X_test)

cm = confusion_matrix(y_test, predics)
ConfusionMatrixDisplay(cm).plot()

# classification report on test dataset
classif_re = classification_report(y_test,predics)
print(classif_re)

from sklearn import tree
from sklearn.tree import DecisionTreeClassifier
from sklearn import metrics
from sklearn.metrics import confusion_matrix
from sklearn.metrics import classification_report
from sklearn.metrics import ConfusionMatrixDisplay

decisionTree = DecisionTreeClassifier(criterion='entropy')
print(decisionTree)
```

```
dtc_model = decisionTree.fit(X_train_res, y_train_res)

from matplotlib import pyplot

# feature importance

importance = dtc_model.feature_importances_
for i,v in enumerate(importance):
  print('Feature: %0d, Score: %.5f' % (i,v))

# Barchat for feature importance

pyplot.bar([x for x in range(len(importance))], importance)
pyplot.show()

prediction = dtc_model.predict(X_test)

cm = confusion_matrix(y_test, prediction)
ConfusionMatrixDisplay(cm).plot()
print(classification_report(y_test, prediction))
import pandas as pd
from sklearn.model_selection import train_test_split
from sklearn.ensemble import RandomForestClassifier
from sklearn.metrics import accuracy_score, classification_report, confusion_matrix

# Load the dataset (replace 'your_dataset.csv' with your actual dataset file)
data = pd.read_csv('your_dataset.csv')

# Feature columns (replace 'feature1', 'feature2', etc. with the actual feature column
names)
features = data[['feature1', 'feature2', 'feature3', ...]]

# Target column (replace 'target' with the actual column containing the severity codes)
target = data['target']
```

```
# Split the data into training and testing sets (adjust the test_size as needed)
X_train, X_test, y_train, y_test = train_test_split(features, target, test_size=0.25,
random_state=42)

# Initialize the Random Forest Classifier
rf_classifier = RandomForestClassifier()

# Train the model
rf_classifier.fit(X_train, y_train)

# Make predictions on the test set
y_pred = rf_classifier.predict(X_test)

# Calculate accuracy
accuracy = accuracy_score(y_test, y_pred)
print(f"Accuracy: {accuracy}")
# Generate classification report and confusion matrix
print("\nClassification Report:")
print(classification_report(y_test, y_pred))
print("\nConfusion Matrix:")
print(confusion_matrix(y_test, y_pred))

import pandas as pd
import numpy as np
import matplotlib.pyplot as plt
import seaborn as sns
# %matplotlib inline

df = pd.read_csv('RTA Dataset.csv')
df.head()
df.shape
# print the dataset information
df.info()
```

```
df.isnull().sum()/100

df['Accident_severity'].value_counts().plot(kind='bar')

import matplotlib.pyplot as plt

# Plot the bar chart
ax = df['Accident_severity'].value_counts().plot(kind='bar', color=['#FF6347',
'#4169E1', '#32CD32'])

# Customize the plot
ax.set_xlabel('Accident Severity')
ax.set_ylabel('Count')
ax.set_title('Distribution of Accident Severity')
ax.legend(['Minor', 'Moderate', 'Severe'])
ax.grid(axis='y', linestyle='--')

# Save the plot
plt.savefig('accident_severity_plot.png')
plt.show()

"""This shows imbalance multiclass label on the dataset"""

# plot the bar plot of road_surface_type and accident severity feature
plt.figure(figsize=(6,5))
sns.countplot(x='Road_surface_type', hue='Accident_severity', data=df)
plt.xlabel('Rode surafce type')
plt.xticks(rotation=60)
plt.savefig('accident_severity_plot.png')
plt.show()

# convert object type column into datetime datatype column
df['Time'] = pd.to_datetime(df['Time'])
```

```
# Extrating 'Hour_of_Day' feature from the Time column
new_df = df.copy()
new_df['Hour_of_Day'] = new_df['Time'].dt.hour
df_new = new_df.drop('Time', axis=1)
df_new.head()

def fill_missing_values(df):
    # Loop over each column in the dataframe
    for col in df.columns:
        if df[col].dtype == 'float64' or df[col].dtype == 'int64': # Check if column is
numeric
            # Fill missing values with mean
            df[col].fillna(df[col].mean(), inplace=True)
        else:
            # Fill missing values with mode
            df[col].fillna(df[col].mode()[0], inplace=True)
    return df

# Fill missing values using the function
df_new = fill_missing_values(df_new)

df_new.isnull().sum()

from sklearn.preprocessing import LabelEncoder

def label_encode_features(df):
    le = LabelEncoder() # create a label encoder object

    for col in df.columns:
        if df[col].dtype == 'object': # check if column is of type 'object'
            df[col] = le.fit_transform(df[col].astype(str)) # label encode the
column
```

```
    return df

# Label encode the object-type features using the function
new_df = label_encode_features(new_df)

new_df.head()

df_new.columns

#handling imbalance multiclass
X = new_df.drop(['Accident_severity', 'Time'], axis=1)
y = new_df['Accident_severity']

X

!pip install imblearn

from sklearn.model_selection import train_test_split, cross_val_score
from sklearn.preprocessing import LabelEncoder, StandardScaler
from sklearn.pipeline import Pipeline
from imblearn.pipeline import make_pipeline
from imblearn.over_sampling import SMOTE
from sklearn.ensemble import RandomForestClassifier,
GradientBoostingClassifier,VotingClassifier
from sklearn.metrics import classification_report, confusion_matrix, accuracy_score

le = LabelEncoder()
y = le.fit_transform(y)
sc = StandardScaler()
X = sc.fit_transform(X)
X_train, X_test, y_train, y_test = train_test_split(X, y, test_size=0.3,
random_state=42)
smote = SMOTE(random_state=42)
X_train_res, y_train_res = smote.fit_resample(X_train, y_train)
```

```
# modelling using random forest baseline
rf = RandomForestClassifier(n_estimators=800, max_depth=20, random_state=42)

rf.fit(X_train_res, y_train_res)

# predicting on test data
predics = rf.predict(X_test)

cm = confusion_matrix(y_test, predics)
ConfusionMatrixDisplay(cm).plot()

# classification report on test dataset
classif_re = classification_report(y_test,predics)
print(classif_re)

from sklearn import tree
from sklearn.tree import DecisionTreeClassifier
from sklearn import metrics
from sklearn.metrics import confusion_matrix
from sklearn.metrics import classification_report
from sklearn.metrics import ConfusionMatrixDisplay

decisionTree = DecisionTreeClassifier(criterion='entropy')
print(decisionTree)

dtc_model = decisionTree.fit(X_train_res, y_train_res)

from matplotlib import pyplot

# feature importance

importance = dtc_model.feature_importances_
for i,v in enumerate(importance):
```

```
  print('Feature: %0d, Score: %.5f' % (i,v))

# Barchat for feature importance

pyplot.bar([x for x in range(len(importance))], importance)
pyplot.show()

prediction = dtc_model.predict(X_test)

cm = confusion_matrix(y_test, prediction)
ConfusionMatrixDisplay(cm).plot()
print(classification_report(y_test, prediction))
import pandas as pd
from sklearn.model_selection import train_test_split
from sklearn.ensemble import RandomForestClassifier
from sklearn.metrics import accuracy_score, classification_report, confusion_matrix

# Extrating 'Hour_of_Day' feature from the Time column
new_df = df.copy()
new_df['Hour_of_Day'] = new_df['Time'].dt.hour
df_new = new_df.drop('Time', axis=1)
df_new.head()

def fill_missing_values(df):
    # Loop over each column in the dataframe
    for col in df.columns:
        if df[col].dtype == 'float64' or df[col].dtype == 'int64': # Check if column is
numeric
            # Fill missing values with mean
            df[col].fillna(df[col].mean(), inplace=True)
        else:
            # Fill missing values with mode
            df[col].fillna(df[col].mode()[0], inplace=True)
    return df
```

```
# Fill missing values using the function
df_new = fill_missing_values(df_new)

df_new.isnull().sum()

from sklearn.preprocessing import LabelEncoder

def label_encode_features(df):
    le = LabelEncoder() # create a label encoder object

    for col in df.columns:
        if df[col].dtype == 'object': # check if column is of type 'object'
            df[col] = le.fit_transform(df[col].astype(str)) # label encode the column

    return df

# Label encode the object-type features using the function
new_df = label_encode_features(new_df)

new_df.head()

df_new.columns

#handling imbalance multiclass
X = new_df.drop(['Accident_severity', 'Time'], axis=1)
y = new_df['Accident_severity']

X

!pip install imblearn

from sklearn.model_selection import train_test_split, cross_val_score
```

```
from sklearn.preprocessing import LabelEncoder, StandardScaler
from sklearn.pipeline import Pipeline
from imblearn.pipeline import make_pipeline
from imblearn.over_sampling import SMOTE
from sklearn.ensemble import RandomForestClassifier,
GradientBoostingClassifier,VotingClassifier
from sklearn.metrics import classification_report, confusion_matrix, accuracy_score

le = LabelEncoder()
y = le.fit_transform(y)
sc = StandardScaler()
X = sc.fit_transform(X)
X_train, X_test, y_train, y_test = train_test_split(X, y, test_size=0.3,
random_state=42)
smote = SMOTE(random_state=42)
X_train_res, y_train_res = smote.fit_resample(X_train, y_train)

# modelling using random forest baseline
rf = RandomForestClassifier(n_estimators=800, max_depth=20, random_state=42)

rf.fit(X_train_res, y_train_res)

# predicting on test data
predics = rf.predict(X_test)

cm = confusion_matrix(y_test, predics)
ConfusionMatrixDisplay(cm).plot()

# classification report on test dataset
classif_re = classification_report(y_test,predics)
print(classif_re)

from sklearn import tree
from sklearn.tree import DecisionTreeClassifier
```

```
from sklearn import metrics
from sklearn.metrics import confusion_matrix
from sklearn.metrics import classification_report
from sklearn.metrics import ConfusionMatrixDisplay

decisionTree = DecisionTreeClassifier(criterion='entropy')
print(decisionTree)

dtc_model = decisionTree.fit(X_train_res, y_train_res)

from matplotlib import pyplot

# feature importance

importance = dtc_model.feature_importances_
for i,v in enumerate(importance):
  print('Feature: %0d, Score: %.5f' % (i,v))

# Barchat for feature importance

pyplot.bar([x for x in range(len(importance))], importance)
pyplot.show()

prediction = dtc_model.predict(X_test)

cm = confusion_matrix(y_test, prediction)
ConfusionMatrixDisplay(cm).plot()
print(classification_report(y_test, prediction))
import pandas as pd
from sklearn.model_selection import train_test_split
from sklearn.ensemble import RandomForestClassifier
from sklearn.metrics import accuracy_score, classification_report, confusion_matrix

import pandas as pd
```

```
import numpy as np
import matplotlib.pyplot as plt
import seaborn as sns
# %matplotlib inline

df = pd.read_csv('RTA Dataset.csv')
df.head()
df.shape
# print the dataset information
df.info()

df.isnull().sum()/100

df['Accident_severity'].value_counts().plot(kind='bar')

import matplotlib.pyplot as plt

# Plot the bar chart
ax = df['Accident_severity'].value_counts().plot(kind='bar', color=['#FF6347',
'#4169E1', '#32CD32'])


<!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>

<input id="btnDe" name="btnDe" value="^ Decrypt ^"
onclick="Decrypt(this.form)" type="button">

Cipher-text

<textarea name="c" rows="4" cols="50" wrap="soft" placeholder="Encrypted Text
Will Appear Here..."></textarea>

</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("Cipher-text").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("Cipher-text").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("Cipher-text").value =
document.getElementById("Cipher-text").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("Cipher-text").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 showCipher-textAlphabet()
{
     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>Cipher-text 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("Cipher-text").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">Cipher-text:</legend>

                <div style="display:inline-block;width:70%;min-width:200px">

                    <textarea id="Cipher-text" 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
Cipher-text Alphabet" onclick="showCipher-textAlphabet()" 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">Cipher-text:</legend>
                <div style="display:inline-block;width:70%;min-width:200px">
                    <textarea id="Cipher-text" 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
Cipher-text Alphabet" onclick="showCipher-textAlphabet()" 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">Cipher-text:</legend>
            <div style="display:inline-block;width:70%;min-width:200px">
                <textarea id="Cipher-text" 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
Cipher-text Alphabet" onclick="showCipher-textAlphabet()" 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">Cipher-text:</legend>
            <div style="display:inline-block;width:70%;min-width:200px">
                <textarea id="Cipher-text" 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
Cipher-text Alphabet" onclick="showCipher-textAlphabet()" class="button button2">
            </div>
        </fieldset>
            <fieldset data-role="controlgroup">
            <legend style="color:black">Ceaser text:</legend>
<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">Cipher-text:</legend>
            <div style="display:inline-block;width:70%;min-width:200px">
                <textarea id="Cipher-text" 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
Cipher-text Alphabet" onclick="showCipher-textAlphabet()" 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">Cipher-text:</legend>
            <div style="display:inline-block;width:70%;min-width:200px">
                <textarea id="Cipher-text" 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
Cipher-text Alphabet" onclick="showCipher-textAlphabet()" class="button button2">
            </div>
        </fieldset>
            <fieldset data-role="controlgroup">
            <legend style="color:black">Ceaser text:</legend>
<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">Cipher-text:</legend>
            <div style="display:inline-block;width:70%;min-width:200px">
                <textarea id="Cipher-text" 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
Cipher-text Alphabet" onclick="showCipher-textAlphabet()" 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">Cipher-text:</legend>
            <div style="display:inline-block;width:70%;min-width:200px">
                <textarea id="Cipher-text" 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
Cipher-text Alphabet" onclick="showCipher-textAlphabet()" 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">Cipher-text:</legend>
            <div style="display:inline-block;width:70%;min-width:200px">
                <textarea id="Cipher-text" 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
Cipher-text Alphabet" onclick="showCipher-textAlphabet()" 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 Cipher-text in blocks of 5</label>

            </div>

        </fieldset>

    </form>


</body>

</html>
```

Bio-Data

A. Personal Data

Full Name: Kayode Mathias MADEWA

Address: 18, Ademola Saka Str, Peace Estate, Isolo, Lagos.

Email Address: madewamk@yahoo.com

Phone Number: 08023281125

Date and Place of Birth: 20/05

Nationality: Nigerian

Marital Status: Married

No. of Children & their ages: 2

Name and Address of Spouse: Mrs. Kofoworola Madewa

Email Address of Next of Kin: Kofo.madewa@gmail.com

Name and Address of Next of Kin: Same as Above

Date of Assumption of Duty in Current Establishment: 08/03/2006

Status on First Appointment in Current Establishment: Fleet Data Mgr.

Present Position: Customer Logistics Mgr

B. Educational Background

Primary Education	**Year**
St James Pry School, Okeigbo	1979 – 1984

Secondary Education

St Peter Unity Secondary School, Akure	1985 – 1991

Higher Educational Institutions Attended With Dates & Qualification

The Polytechnic Ibadan,	HND Computer Science,	1998
University of Ibadan,	Master of Managerial Psychology	2004
Lead City University, Ibadan.	Bsc Computer Science	2021

C. Work Experience with Date

i. Fleet Data Manager	2010 – 2011
ii. Business System Expert, Planning & Logistics – SAP	2012 – 2014
iii. Customer Service Operations Manager	2015 – 2016
iv. National Transportation Manager	2017 – 2019
v. National Warehouse Manager	2019 – 2020
vi. Customer Logistics Manager	2021 - Till Date

D. Published Refereed Conference Proceedings:

i. Impact Of Blockchain Technology On Financial Technology In Nigeria

ii. Analysis of modern Cybersecurity Threat Techniques and available Mitigating Methods.

E. EXTRA CURRICULAR ACTIVITIES

- Reading
- Travelling
- Surfing the Internet

F. REFEREES

Prof. Philip Achimugu
Faculty of Computing
Air Force Institute of Technology, Kaduna

check4philo@gmail.com
+234(0)8093482286

Dr. Kolapo Ridwan Olayinka
Department of Computer Science
Lead City University, Ibadan
Kolapo.ridwan@lcu.edu.ng
+234(0)8132393870

Dr. Wilson Sakpere
Computer Science Department
Lead City University, Ibadan,
sakpere.wilson@lcu.edu.ng
+234(0)8159582869

…….. ……..

Signature Date

The University Compliance Certification

This is to certify that this thesis by Kayode Mathias MADEWA with Matriculation Number LCU/PG/002718 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