The International Journal of Computational Science, Information Technology and Control Engineering (IJCSITCE) Vol.10, No.1/2/3, July 2023

DATA SECURITY THROUGH CRYPTO-STEGANO SYSTEMS

Dinaeli Paul Sabaya, Adam Aloyce Semlambo and Joel Kazoba Simon

Institute of Accountancy Arusha (IAA), Informatics Department, Tanzania

ABSTRACT

Unauthorized access and hacking are major issues for internet users, and numerous articles have been published on various approaches to solving this issue. This study proposes a novel method for encoding a hidden message within the text by combining text steganography and substitution cryptography. While steganography and cryptography can be used to protect data, neither is sufficient to provide better security as they can be broken by steganalysis and cryptoanalysis. Therefore, the terms "cryptography-stegano" should be combined for improved security. In this method, data is first encrypted using a substitution cryptography technique to produce the cypher text, which is then encrypted using text steganography to produce a more secure cypher text sent to the recipient. Contrary to popular belief, using image steganography and cryptographic methods is unnecessary for effective data encryption. The study shows that combining text steganography with cryptographic techniques is an excellent data security method. Additionally, other combinations, such as audio and video steganography, should also be considered for better security

KEYWORDS

Steganography, cryptography, cryptography-stegano, security, Data, cypher, encryption, decryption.

1. INTRODUCTION

Both stenography and cryptography have the same objective: to secure data or information being transferred from one person or system to another. The only distinction between them is that while Steganography conceals the secret message or information so that the sent message is unnoticed and undetected by the third party, cryptography uses a mathematical algorithm to scramble up a message so that only the sender and the intended recipient can read it (Saleh et al., 2016).

Since the words "cryptography" and "graphia" in Greek imply "writing" and "hidden," respectively, the correct definition of cryptography is "the concealment of writing." The science of employing mathematics to encrypt and decrypt data was created in an Egyptian town 4000 years ago. Steganography's correct definition is "covered writing" since it derives from the Greek terms "steganos," which means "covered/protected," and "graphia," which means "writing." Steganography is the practice of encoding one piece of data as another, such as text, image, audio, or video. Around 440 B.C., the first steganographic method was discovered in ancient Greece. Herodotus used it for the first time during the war when he picked his most dependable slave, shaved his head, tattooed a warning message to Greece about Persian invasion intentions, and then waited for the message to be covered by the growing hair. Then he dispatched his slave to carry the message. The slave answered similarly when the receiver shaved his head to understand the message (Shaik et al., 2012).

Nowadays, most people use the internet as a quick, easy, accurate, and simple way to convey information because of the improved science and technology. However, this medium of transition has one major issue, which is that private or secret information can be discovered or stolen in various ways (Saleh et al., 2016).

Some websites occasionally request delicate personal data, such as your phone number, address, and credit card information. Before sending information, it is crucial to safeguard it. Users are always reminded to protect their information from third parties when sending it through an open source. Because of this, the study aims to comprehend and integrate Steganography and cryptography into a single system for increased security and confidentiality. Thus, the main objective of this study is to study the crypto-stegano system for security data

2. BACKGROUND OF THE STUDY

Using steganography and cryptography together to secure data has received much attention, particularly with picture steganography. However, this project aims to integrate substitution cryptography and text steganography. This section provides a variety of linked papers on the use of Steganography and cryptography together.

Steganography and cryptography are two well-liked methods of transferring various data from one system to another, according to Abdelmged A. A. (2016). A new method for concealing data in an image was enhanced using Huffman coding. However, as they can both be broken with some effort by the intended receiver, neither cryptography nor Steganography alone can ensure greater security. Therefore, combining the two approaches could be a solution for enhanced data security, giving rise to the phrase "crypto- stegano."

Cryptography is not a sufficient method for protecting data from a cryptanalyst because it simply retains the secret of the data by changing it into a different form. On the other side, Steganography conceals the data's substance so that the intended recipient cannot discover its existence. It becomes simple for unintended users to get the data if they successfully discover its presence. The data was concealed using the image steganography technique known as the Least Significant Bit (LSB). Neither Steganography nor Cryptography is a reliable method of data security. However, when these two methods—Steganography and cryptography—are merged into a single system, internet users benefit from increased security and confidentiality. Steganography conceals the data's existence in a non-secret file, such as an image, video, text, or audio file. To combine these two techniques, the data must first be encrypted before using one of the steganographic procedures to create a new cypher text (AbikoyeOluwakemi et al., 2012).

As more people became familiar with the internet, network users grew. They encountered numerous difficulties transmitting and storing personal data like passwords and account numbers. When steganographic techniques are coupled with cryptography to encrypt data, it is more difficult to identify the presence of the delivered data than when the two techniques are used separately (Goudar et al., 2012).

Given how far technology has come, most people now prefer to use the Internet as their primary method of international data transfer. Data can be transferred in various ways, including through e-mail, chats, and other channels. This method of transferring data is straightforward and quick. It has become crucial to pay close attention when transferring data using steganographic and cryptographic methods to ensure data security (Swanson et al., 1998).

According to Dunbar (2002), steganography and cryptography are both intended techniques that are used to secure information from hackers in the digital age. Although neither technique is flawless, they are both very good; thus, most experts advise combining them.

Internet users have reported that security concerns have emerged as a major issue while transferring data. Everyone wish their data to be safe and confidential. Combining cryptography and steganography methods is suggested as the best way to safeguard the information in 4 Section 2.1. Related Works. A significant amount of digital data is being shared via various networks, particularly via the steganographic image approach, due to the rapid expansion of computer networks and the rise in digital technology. Different steganographic approaches, including image, text, audio, and video, can be employed; however, due to the internet's explosive increase in popularity today, picture steganography has received more research attention than other steganographic techniques (Atown, 2014).

Before the advent of modern science and technology, humans employed covert tattoos or invisible ink to transport data securely while avoiding suspicion. Due to science and technology advances, steganography and cryptography techniques are now considered crucial data security solutions (AbikoyeOluwakemi et al., 2012).

Steganography and cryptography are two methods for protecting data; the only distinction between them is that cryptography focuses on protecting the presence of a secret message, while Steganography focuses on protecting the content of a message. It is much better to combine both methods into a single system to secure data (Kumar and Murti, 2011).

3. CRYPTOGRAPHIC TECHNIQUES IN SECURING DATA

Cryptography usually starts with encrypting the plain text to the cypher text. The cypher text is transferred to the intended recipient, who describes the received cypher text to get the original message from the sender (plain text). Encryption and descriptions depending on the cryptography type (Kessler., 2017). This section will include types, techniques used, functions and limitations of cryptography.

3.1. Types of Cryptography

The cryptography key is divided into three types (A et al. l, 2016), which are;

- Symmetric key
- Asymmetric key
- Hash value

3.1.1. Symmetric Key

The symmetric key is sometimes known as single or secret key cryptography, where both the receiver and the sender share the same key to encrypt and decrypt the data. It is easily perceived that both the sender and receiver must know the key, but it is a secret between them.

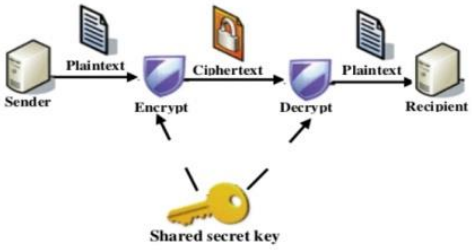


Figure 1: The Symmetric Key
Source; (Researchers, 2023)

Figure 1 shows that the sender and the receiver share the same key to encrypt and decrypt the data.

Mathematically, the example below shows that the receiver and the sender have the same cypher matrix as a key.

Example:

The sender wants to encrypt this data,

'AIMS BROUGHT ME THIS FAR'

With the key,

$$\begin{pmatrix} 334 \\ 011 \\ 434 \end{pmatrix}$$

Note

To encrypt the message above, all alphabets should be assigned to numbers as follows;

Table 1. Alphabet with natural numbers

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
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Source; (Researchers, 2023)

Table 1 shows the assigned alphabet from A to Z . This depends on the sender and user agreement. They may agree to start from 0 instead of 1.

Therefore, the data above can be encrypted as follows;

The sender is supposed to assign a number to each letter and break the enumerated message in a sequence of 3 by 1 vector since the cypher matrix of 3 by 3. After that, the sender multiplies the cypher matrix with the obtained vectors (encoding matrix) to get the cypher text. Here each word is separated by 27.

Thus, AIMS BROUGHT ME THIS FAR becomes;

Matching letters of the phrase AIMS BROUGHT ME THIS FAR with natural numbers

Table 2. Matching letters of the phrase AIMS BROUGHT ME THIS FAR with natural numbers

A	I	M	S		B	R	O	U	G	H	T		M	E		T	H	I	S		F	A	R	
1	9	13	19	27	2	18	15	21	7	8	20	27	13	5	27	20	8	9	19	27	6	1	18	27

Source; (Researchers, 2023)

The sender can let C be the cypher matrix and E the encoding matrix, so
Encrypted Message (EM)=C x E

$$EM=\begin{pmatrix}334\\011\\434\end{pmatrix}\begin{pmatrix}1191881320191\\9271520582718\\132727279627\end{pmatrix}$$

The encrypted message will be;

$$\begin{pmatrix}82146127192162120162165\\2229224732173345\\83165145200175140181166\end{pmatrix}$$

Therefore the sender sends the encrypted message above with the cypher matrix (key). After the receiver receives it, they are supposed to find the inverse of the cypher matrix (key), and multiply it with the received message. The answer will be in vector form, so they would need to arrange it appropriately and then assign the letters to each number to obtain the plain text back.

$$\text{Inverse cypher matrix} =\begin{pmatrix}-101\\-443\\4-3-3\end{pmatrix}$$

Decrypted Message

$$(DM)=\begin{pmatrix}-101\\-443\\4-3-3\end{pmatrix}\begin{pmatrix}82146127192162120162165\\2229224732173345\\83165145200175140181166\end{pmatrix}$$

$$DM=\begin{pmatrix}1191881320191\\9271520582718\\132727279627\end{pmatrix}$$

By arranging and assigning letters to each number, we obtain Table 3.2, which gives the original message after decryption as ‘’AIMS BROUGHT ME THIS FAR’’.

3.1.2. Asymmetric Key

The Asymmetric Key, sometimes known as public key cryptography, refers to the type of cryptography where the key the sender uses to encrypt the plain text differs from the key the receiver uses to decrypt the cypher text. Consider the figure below;

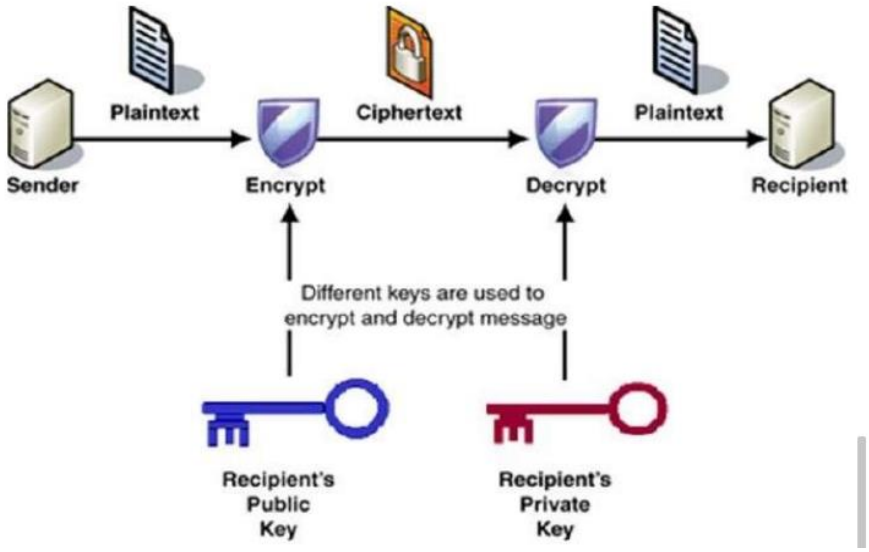


Figure 2: The Asymmetric key
Source; (Researchers, 2023)

Figure 2 shows that the key the sender uses to encrypt the data differs from the one the intended receiver uses.

3.1.3. Hash Values Key

This type of cryptography uses a mathematical transformation to encrypt information. It does not use a key since the plain text is not recoverable from the cypher text.

3.2. Techniques used in Cryptography

The following content is per (Kuo, Accessed April 2017)

In Cryptography, a plain text message can be converted into a cypher text message using two techniques. That are transpositions and substitution techniques.

3.2.1. Transposition Technique

This is the cryptographic technique where characters are -arranged or shifted in some regular pattern to form the cypher text. Characters retain their identity, but they change their position. The transposition technique includes the rail fence technique and simple column transposition.

a. Rail Fence Technique

This is the transposition technique in which the plain text is written down as a sequence of diagonals and then read off as a sequence of rows.

For example;

- We code the message *HIDE IT BEHIND MY OFFICE* in a depth-2 rail fence as follows:

H D I B H N M O F C

I E T E I D Y F I E

Therefore the cypher text the sender will send is 'HDIBHNMOFC IETEIDDYFIE.'

- We code the message DON'T GIVE HIM MONEY in a depth -3 rail fence as follows

D G H O X
O T I E I M N Y
N V M E

Therefore the coded text that the sender will send is 'DGHOX OTIEIMNY NVME' where X means the gap is filled when the diagonal cannot be completed.

b. Simple Column Transposition

This transposition technique follows the rule of mixing up characters in plain text to form cypher text.

This method is called column transposition because the cypher text is obtained column-wise. The length of rows must be the same as the length of the keyword. Simple column transposition is divided into **regular and irregular**.

Example

The plain text 'HIDE IT BEHIND MY OFFICE' with the keyword 'MISA' can be decrypted as follows;

For irregular column transposition, the keyword is ordered alphabetically

Table 3. Irregular column transposition

A	I	M	S
H	I	D	E
I	T	B	E
H	I	N	D
M	Y	O	F
F	I	C	E

Source; (Researchers, 2023)

Therefore the coded text is 'HIHMFITIYIDDNOCEEDFE'
For regular column transposition

Table 3. Regular column transposition

M	I	S	A
D	I	E	H
B	T	E	I
N	I	D	H
O	I	F	M
C	I	E	F

Source; (Researchers, 2023)

Therefore the cypher text becomes ‘DBNOCITYIEEDFEH

3.2.2. Substitution Technique

This cryptographic technique replaces the character in the plain text with another letter, number, or symbol. It is divided into

i. Caeser cypher
ii. Kamasutra Cipher
iii. Monoalphabetic substitution

a. Caeser Cipher

This refers to the substitution technique which Julius Caesar proposed. Each letter in the plain text is replaced by a letter corresponding to another letter or number in the alphabet (Kuo, Accessed, April 2017). For example

Table 4. Caesar Table

Plain text	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
Cipher text	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

Source; (Researchers, 2023)

In Table 5, letters are assigned to letters so that ‘A’ is assigned to X, ‘B’ is assigned to Y and so on.

Note: It is not always three places down the alphabet that can be used rather, it depends on the sender's wish.

For example

The plain text like ‘HIDE IT BEHIND MY OFFICE’

It can be encrypted to a cypher text as ‘EFAB FQ YBEFKA JV LCCFB’.

Mathematically, if each letter is assigned to a number from 0 to 25 (A to Z) Caesar cipher can be represented as follows;

Table 6. Caesar Cipher text

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Source (Researchers, 2023)

For Encryption

Cipher text = (Plain Text + Key) Mod 26

C = (P + K) Mod 26

- So 'HIDE IT BEHIND MY OFFICE' is encrypted as follows;

Table 7. Encryption of HIDE IT BEHIND MY OFFICE in Caesar cypher.

Plain	H	I	D	E	I	T	B	E	H	I
Position	7	8	3	4	8	19	1	4	7	8
Key	17	17	17	17	17	17	17	17	17	17
+	24	25	20	21	25	36	18	21	25	25
Mod 26	24	25	20	21	25	10	18	21	24	25
Ciphertext	Y	Z	U	V	Z	K	S	V	Y	Z
Plain	N	D	M	Y	O	F	F	I	C	E
Position	13	3	12	24	14	5	5	8	2	4
Key	17	17	17	17	17	17	17	17	17	17
+	30	20	29	41	31	22	22	25	19	21
Mod26	4	20	3	15	5	22	22	25	19	21
Ciphertext	E	U	D	P	F	W	W	Z	T	V

Source; Researchers (2023)

Thus the cypher text is 'YZUV ZK SVYZE UD PFWWZTV' as shown in Table 7.

➢ **For Decryption**

After the message is received, the receiver decrypts it by using the formula below;

Plain text = (Cipher Text -Key) *Mod 26*

➢ P=(C-K) *Mod 26*

- 'YZUV ZK SVYZE UD PFWWZTV' becomes,

Table 8. Decryption of YZUV ZK SVYZE UD PFWWZTV in Caesar cypher.

Cypher	Y	Z	U	V	Z	K	S	V	Y	Z
Position	24	25	20	21	25	10	18	21	24	25
Key	17	17	17	17	17	17	17	17	17	17
-	7	8	3	4	8	-7	1	4	7	8
Mod 26	7	8	3	4	8	19	1	4	7	8
Cypher	E	U	D	P	F	W	W	Z	T	V
Position	4	20	3	15	5	22	22	25	19	21
-	-13	3	-14	-2	-12	5	5	8	2	4
Mod 26	13	3	12	24	14	5	5	8	2	4
Plain	H	I	D	E	I	T	B	E	H	I
Plain	N	D	M	Y	O	F	F	I	C	E

Source; (Researchers, 2023)

Therefore the original message after decryption by the receiver is 'HIDE IT BEHIND MY OFFICE 'as shown in Table 8 above.

b. Kamasutra Cipher

This is the substitution technique with the main goal of teaching women to hide their secret message from prying eyes. The key is the permutation of the alphabet, and the plain text must be equal to the cypher text. The alphabet should be divided into two halves to pair the letters as follows;

Table 9: Kamasutra cipher.

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

Source; (Researchers, 2023)

In Table 9, the Kamasutra technique works as follows; the letter "K" becomes "T", the letter "G" becomes "F", and so on. So if the sender is to encrypt 'HIDE IT BEHIND MY OFFICE,' the cypher text will be ' XNLT JK QOWIYA HR PGECUB'.

c. Monoalphabetic substitution

This is the simple substitution technique where the substitution is fixed for each alphabet; thus, if B is encrypted to S, then S. will replace B every time. The technique is simple, and it is easy to break. Consider the example below, where each letter is encrypted as the next.

Table 10: Monoalphabetic substitution

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

Source; (Researchers, 2023)

So 'HIDE IT BEHIND MY OFFICE' is encrypted to 'IJEF JU CFIJOE NZ PGGJDF' as shown in Table 3.7.

3.3. Function of Cryptography

According to Ajit Singh Singh (2013), Cryptograph functions are discussed below. Cryptography is important when transferring data over any untrusted medium, like the internet. It protects data from thieves and hackers and can be used for authentication. The functions of cryptography are as follows;

1. **Confidentiality:** Cryptography ensures that no one apart from the data's receiver and sender can obtain the data's content.
2. **Authentication**: It provides the identity between the receiver and sender; that is, it ensures that whoever receives or sends data is an authoritative party.
3. **Non-repudiation**: Cryptography ensures that the intended recipient receives the data from the right sender and not otherwise.

4. **Integrity:** This is another role of cryptography where it ensures the quality of the content to the sender.

3.4. Limitation of Cryptography

Apart from the functions of cryptography discussed above, cryptography has certain limitations:

1. Most algorithms are known.
2. When the data are passing, they are known; thus, they attract hackers.
3. It uses common technology.
4. Its security depends on the computational difficulty of mathematical problems.
5. It is costly in terms of time.
6. In symmetric algorithms, authenticity and non-repudiation are not supported.

4. STEGANOGRAPHIC TECHNIQUES IN SECURING DATA

In Steganography, we cover the writing so that no one apart from the intended recipient knows its presence. In this section, we look at Steganography's types, techniques, and functions.The chapter also includes limitations, models and characteristics of the steganographic technique.

4.1. Types of Steganography

There are three types of steganography Dunbar(2002). Namely

- Pure Steganography
- Secret Steganography
- Public key Steganography

a. Pure Steganography

This type of Steganography does not require exchanging secret information before sending a message. There is no need to exchange the cypher (stegano key). This implies that the sender and the receiver should assume that no one except them is aware of the message. Pure Steganography is called pure because it does not combine its technique with any other technique (A et al.,2016.)

b. Secret key Steganography

Dunbar(2002), This type of Steganography requires exchanging the secret key (stegano-key). The secret key takes the cover message and embeds it secretly by using a secret key. It also makes sure that only the sender and the receiver of the data suspect the presence of the data and read the secret message. Secret key combines the cryptography technique with the steganography approach by encrypting the data and hiding it within a cover carrier (A et al.,2016.)Since it requires the exchange of the stegano-key, sometimes it is easy to suspect the presence of the data. However, even if the third party suspects the presence of the data, they cannot extract the message.

c. Public key Steganography

This is another type of Steganography that uses public key cryptography. It uses public and private keys to secure data. The sender uses the public key to encrypt the plain text, while the receiver uses the private key to decrypt the cypher text. It uses a mathematical algorithm which

makes this type more secure since, even if non-intended recipients suspect the presence of the data, they can crack the algorithm (Rani and Chaudhary,2013)

4.2. Techniques Used in Steganography

According to Nitesh and Pamulaparty(2016), steganography can be categorized depending on the media used to hide the data.

1. Text steganography
2. Image steganography
3. Audio steganography
4. Video steganography

4.2.1. Text Steganography

Rani and Chaudhary (2013) define text steganography as a steganographic technique which hides the message behind other text files; the technique is achieved by changing the text formatting. It is the toughest type of Steganography since there are very limited places in a text carrier that are possible to hide the text message in;

Examples

Example 1: If the sender wants to use a text steganographic technique to send a message like 'DO NOT GO', they may write it like this;

First: Distribute ordinary notebooks or take good ones.

The receiver will understand that they will take every first letter of every single word, that is

Distribute **O**rdinary **N**otebook **O**r **T**ake **G**ood Ones – 'DO NOT GO'

Note: The sender must ensure that the message will not attract suspicion.

Example 2: If the sender needs to hide the message 'HE IS NOT DONE ANY' inside the information below:

'Aims's flagship programme is a 10-month Structured masters programme in the Mathematical sciences. The programme was
upgraded in 2012 from a postgraduate
Diploma. The master's degree is conferred
by the three South African universities in the
partnership. African students can apply
for full scholarships, including travel, board and
lodging, tuition and stipend. Aims are
committed to greater participation by women
in science and a geographically representative
student body from the African continent.
In the Aims research centre, students, often
Aims alumni, study towards an MSC or PhD.'

The sender may send the information above with these numbers **32 09 15 24 28 12 16 25 02 38 06 19 02 15**

Where by the receivers understand that the number sent with the information is the key, so from each given number, they take the letter at that position at the respective line. This implies that 32 is the position of the letter or number in the first line. 09 is the position of the letter or number in the second line, and so on, as shown below.

‘Aims’s flagship programme is a 10-mont**H**
Structur**E**dmasters programme in the
Mathematical sc**I**ences. The programme was
upgraded in 2012 from a po**S**tgraduate
Diploma. The master's degree is co**N**ferred
by the three S**O**uth African universities in the
partnership. Studen**T** from Africa can apply
for full scholarships, inclu**D**ing travel, board and
l**O**dging, tuition and stipend. Aims is
commited to greater participation by women
in sci**E**nce and a geographically representative
student body from the **A**frican continent.
I**N** the Aims research centre students, often
Aims alumni, stud**Y** towards a MSC or PhD.’

Therefore ‘HE IS NOT DONE ANY’ is hidden, as shown above.

Text steganography is divided into the following techniques:

- Selective hiding
- Abbreviation
- Semantic method
- Word shifting
- Syntactic Method

a) Selective Hiding

This text steganography technique hides the characters in the words' first or any specific location. Joining those characters helps to get stegotext. Its main weakness is that it requires a considerable amount of plain text.

b) Abbreviations

This refers to the type of steganographic technique which shortens the words to hide the data. A single word can replace the number of data, creating different meanings that help generate the cover text. In this technique, both the sender and the receiver should know the abbreviations. This technique is secure. However, it is only useful for short-length data and not otherwise.

c) Semantic Method

This refers to the text steganographic technique, which considers synonyms of a word. It takes the data exactly or nearly the same as other words in the same language. This technique is more secure for implementing Steganography in open areas.

d) Word Shifting

Word shifting is the text steganographic technique where the secret data is hidden by shifting the words horizontally, left or right. It is a good technique, but if someone knows the algorithm, they can compare the hidden content with the algorithm and extract the data.

e) Syntactic Method

This text steganographic technique uses punctuation marks such as commas, question marks and full stops to hide bits 0 and 1. This technique is better than others since the chance of someone hacking the hidden data is minimal. Using the syntactical method properly will never attract the hacker to extract the hidden data.

f) Line Shift Coding

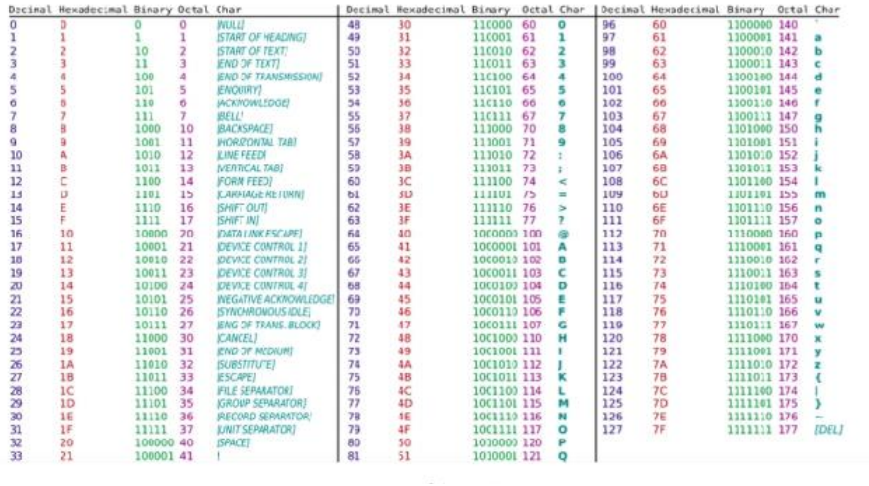
This is the text steganographic technique where text lines are vertically shifted to encode the document.

4.2.2. Image Steganography

This is the most common steganographic technique, which hides data inside images. It is the most frequently used approach because of the limitation of the human eye. The technique does not attract the hacker to suspect the hidden data. The original and embedded images with data are identical (Dhanani et al.,2016). Image steganography uses various techniques. Some are known as American standard codes for information Interchanging code (ASCII) and list significant Bits (LSB).

- American standard code for information Interchanging code (ASCII)

This is the code which is used to interchange the information. It assigns letters, numbers and other characters, like a punctuation mark, into a form that can be sent to and understood by other computing devices such as modems and printers. The computer does not understand English, French, Maasai or any other language, it only understands binary numbers like 0 and 1. If 5 is pressed on the keyboard, the keyboard sends the value 101(value equivalent to 5) to the main memory, which further evaluates in secondary memory. Then, the output is 5 on the monitor's screen. Similarly if "M" is pressed on the keyboard, the value is 077, equivalent to 1001101, and so on. A complete ASCII Table involves decimal, hexadecimal, binary, octal and characters, as shown in the figure below (Bairagi, 2011)



Decimal	Hexadecimal	Binary	Octal	Char	Decimal	Hexadecimal	Binary	Octal	Char	Decimal	Hexadecimal	Binary	Octal	Char
0	0	0	0	[NULL]	48	30	110000	60	0	96	60	1100000	140	`
1	1	1	1	[START OF HEADING]	49	31	110001	61	1	97	61	1100001	141	a
2	2	10	2	[START OF TEXT]	50	32	110010	62	2	98	62	1100010	142	b
3	3	11	3	[END OF TEXT]	51	33	110011	63	3	99	63	1100011	143	c
4	4	100	4	[END OF TRANSMISSION]	52	34	110100	64	4	100	64	1100100	144	d
5	5	101	5	[ENQUIRY]	53	35	110101	65	5	101	65	1100101	145	e
6	6	110	6	[ACKNOWLEDGE]	54	36	110110	66	6	102	66	1100110	146	f
7	7	111	7	[BELL]	55	37	110111	67	7	103	67	1100111	147	g
8	8	1000	10	[BACKSPACE]	56	38	111000	70	8	104	68	1101000	150	h
9	9	1001	11	[HORIZONTAL TAB]	57	39	111001	71	9	105	69	1101001	151	i
10	A	1010	12	[LINE FEED]	58	3A	111010	72	:	106	6A	1101010	152	j
11	B	1011	13	[VERTICAL TAB]	59	3B	111011	73	;	107	6B	1101011	153	k
12	C	1100	14	[FORM FEED]	60	3C	111100	74	<	108	6C	1101100	154	l
13	D	1101	15	[CARRIAGE RETURN]	61	3D	111101	75	=	109	6D	1101101	155	m
14	E	1110	16	[SHIFT OUT]	62	3E	111110	76	>	110	6E	1101110	156	n
15	F	1111	17	[SHIFT IN]	63	3F	111111	77	?	111	6F	1101111	157	o
16	10	10000	20	[DATA LINK ESCAPE]	64	40	1000000	100	@	112	70	1110000	160	p
17	11	10001	21	[DEVICE CONTROL 1]	65	41	1000001	101	A	113	71	1110001	161	q
18	12	10010	22	[DEVICE CONTROL 2]	66	42	1000010	102	B	114	72	1110010	162	r
19	13	10011	23	[DEVICE CONTROL 3]	67	43	1000011	103	C	115	73	1110011	163	s
20	14	10100	24	[DEVICE CONTROL 4]	68	44	1000100	104	D	116	74	1110100	164	t
21	15	10101	25	[NEGATIVE ACKNOWLEDGE]	69	45	1000101	105	E	117	75	1110101	165	u
22	16	10110	26	[SYNCHRONOUS IDLE]	70	46	1000110	106	F	118	76	1110110	166	v
23	17	10111	27	[ENG OF TRANS. BLOCK]	71	47	1000111	107	G	119	77	1110111	167	w
24	18	11000	30	[CANCEL]	72	48	1001000	110	H	120	78	1111000	170	x
25	19	11001	31	[END OF MEDIUM]	73	49	1001001	111	I	121	79	1111001	171	y
26	1A	11010	32	[SUBSTITUTE]	74	4A	1001010	112	J	122	7A	1111010	172	z
27	1B	11011	33	[ESCAPE]	75	4B	1001011	113	K	123	7B	1111011	173	{
28	1C	11100	34	[FILE SEPARATOR]	76	4C	1001100	114	L	124	7C	1111100	174	|
29	1D	11101	35	[GROUP SEPARATOR]	77	4D	1001101	115	M	125	7D	1111101	175	}
30	1E	11110	36	[RECORD SEPARATOR]	78	4E	1001110	116	N	126	7E	1111110	176	~
31	1F	11111	37	[UNIT SEPARATOR]	79	4F	1001111	117	O	127	7F	1111111	177	[DEL]
32	20	100000	40	[SPACE]	80	50	1010000	120	P					
33	21	100001	41	!	81	51	1010001	121	Q					

Figure 3: An ASCII TABLE
Source; (Wikimedia Commons)

In figure 3 above, each letter, number and other character are assigned so that any computer and other devices can understand it.It uses ‘A’ as 65,’B’ as 67 and so on. “a” as 97,”b” as 98 and so on, “0” as 48 while “1” as 49 and so on. Each alphabet, number and character is represented with a 7-bit binary number (a string of seven 0s and 1s)

- **Least Significant Bit(LSB)**

The least significant bit refers to the rightmost bit, which replaces the byte of the secret message. For example, in binary number 10111001, the least significant bit is 1nthat is 10111001**.** LSB is a good technique for hiding data because it is undetectable in plain sight. If secret data is hidden, say 1 in 1011010, it becomes 1011011. These two pixels are very close to each other in such a way that it is not easy to be noticed by anyone. In LSB, the cover image must be greater than 8 times the size of the hidden message (Shaik et al.,2014).

I. Audio Steganography

This refers to the science of hiding data by adjusting it to the sound of a sign in an undetectable way. It is the most difficult technique of Steganography because an attacker can easily detect the change in sound within a minute.

II. Video Steganography

This is the steganographic technique where the data is hidden inside the video in such a way that it is none detectable by the non-intended recipient. It also takes advantage of the limitation of human eyes as in image steganography.

4.3. Characteristics of Steganographic Techniques

According to Olguin(2016), steganographic techniques have the following features.

- Hiding capacity: This is an important feature of any steganographic technique that deals with the size of the information hidden inside the cover file. That is, the stegosystem successfully recovers the total number of bits hidden.

- Robustness refers to the hidden data's ability to retain its safety. The stego-media transforms scaling, the addition of the random noise, rotation and other changes
- Tamper-resistance: This is an important feature of the steganographic even if the hacker successfully extracts the hidden data, this tamper-resistance will make it difficult for the hacker to change anything in the original data.
- Perceptual transparency: This is another important feature of the steganographic technique where each cover media has a certain information-hiding capacity.
- Security: The data transmitted must be secured from being attacked by the hacker
- Undetectable: This feature will ensure that the embedded algorithm is undetected by a third party.

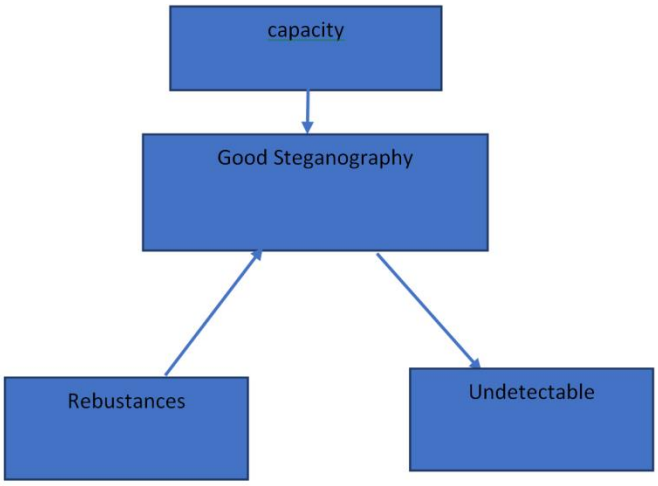


Figure 4; Common features of Steganography.
Source; (Researchers, 2023)

Figure 4 shows common characteristics that every stenographic technique must possess

Steganographic Model

According to Olguin (2016), the steganographic model contains three parameters:

- Cover file(C)
- Message (M)
- Stego-key (K)

Message; refers to the secret data the sender wants to encrypt/hide. Cover file: This refers to the file used to hide the information Stego-key; This is the specific key used to hide and recover the data M and X.

Now, let's apply the steganographic method *f(X,M,K)*, Which leads us to the stego-lifeas An output denoted by *Z*.

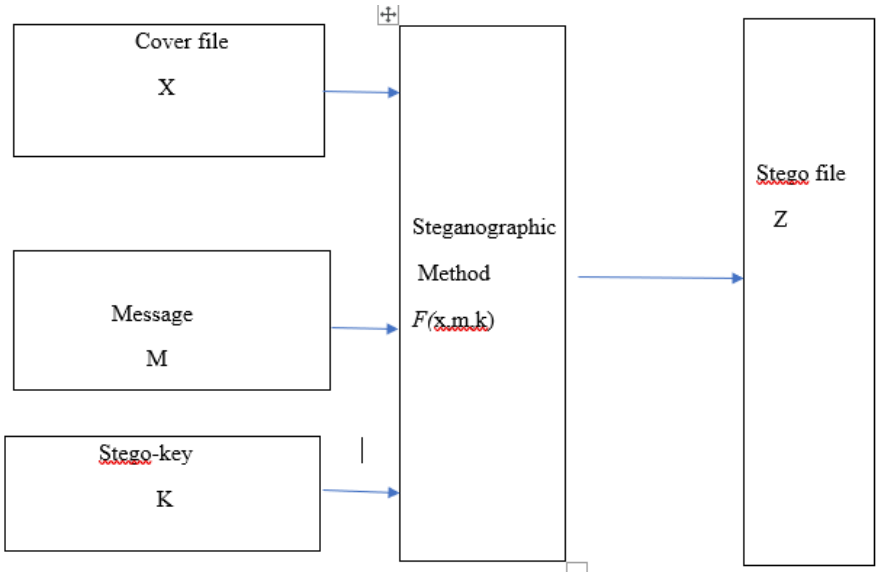


Figure 5 Steganographic model
Source; (Researchers, 2023)

From the model above in Figure 5 receiver recovers the message by applying the inverse process using the same key used during the hiding of information (Olgium,2016)

4.4. The Function of Steganography

The following are the functions agencies of Steganography.

- Intelligence agencies use it for sending secret information.
- Used for safeguarding data.
- Protection of data alteration.
- Makes it default to detect hidden data.
- It provides us with the strengthening of the secrecy of the encrypted data.
- Used for confidential communication and secret data storing.
- It provides the potential capacity to hide the existence of confidentiality.

4.5. L. imitation of Steganography

- It is less secure since it is already known once the data is detected.

5. CRYPTO- STEGANO IN SECURING DATA

Any combination of cryptography can be used for better data security, but the combination is not perfect. This section presents a combination of substitution cryptographic techniques and text steganographic.

5.1. Crypto-Steganography

Steganography and cryptography are cousins in the spy craft family (Olguim,2016). However, as we have seen in previous chapters, cryptographic and steganographic techniques differ. Cryptographic techniques change the data's original structure, making it meaningless to third

parties. Steganographic techniques hide the presence of the data by hiding them inside the multimedia file. Due to the different limitations of each technique, researchers recommend, 'none of these techniques is perfect unless they are combined'. The combination of Steganography and cryptography is called 'Cryptography or 'Crypto-stegano.'' Consider the figure below for the combination process between cryptography and stenography

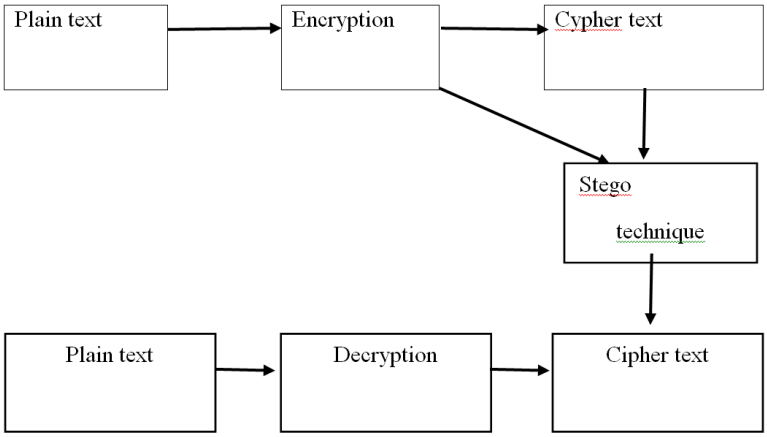


Figure 6; The combination of cryptography and Steganography.
Source; (Researchers, 2023)

In Figure 6, it is shown that the sender must encrypt the data to get the cypher text undergoes a steganographic process depending on the sender's interest in steganographic techniques.

This is where the sender obtains another cypher text which is more secure and ready to be transmitted to the receiver. Cryptography and Steganography combine in different ways depending on the sender's interest. The sender can combine asymmetric with video techniques and symmetric with text techniques.

Since many authors have already discussed combining cryptographic techniques with image stenographic techniques, this chapter shows the combination of cryptographic techniques with text steganographic techniques.
For the combination in the following examples, the sender encrypts the data using a substitution technique in cryptography to get the cypher text and the Steganography to obtain another cypher text sent to the receiver.

5.2. Example 1

The sender from AIMS-TZ wants to send this data 'THE TIME FOR THIS RESEARCH WAS TOO LIMITED 'to the chairperson of AIMS-TZ. However, the sender does not want anybody, especially tutors and Dr Isambi, the Director of AIMS-TZ, to be aware of this issue. So the sender uses strong encryption to ensure that even if the data passes to those non-intended recipients, they cannot extract it.

5.2.1. Encryption Part

Encrypt using the cryptographic technique,

This is the key that the sender and the chairperson of AIMS are aware of.

Cipher matrix = $\begin{pmatrix} 1001 \\ 0112 \\ 2101 \\ 2014 \end{pmatrix}$

Following the same procedures as in the previous chapter on encrypting the data

Table 11; Encrption of time for this research was too limited

T	H	E		T	I	M	E		F	O	R		T	H	I	S		R	E	S	E
20	8	5	27	20	9	13	5	27	6	15	18	27	20	8	9	19	27	18	5	19	5
A	R	C	H		W	A	S		T	O	O		L	I	M	I	T	E	D		
1	18	3	8	27	23	1	19	27	23	15	15	27	12	9	13	9	20	5	4	27	27

Source; (Researchers, 2023)

Plain matrix= $\begin{pmatrix} 2020272719311595 \\ 8962027581915134 \\ 513158181272727927 \\ 275189518232312122027 \end{pmatrix}$

Cypher text= $\begin{pmatrix} 1001 \\ 0112 \\ 2101 \\ 2014 \end{pmatrix} \begin{pmatrix} 2020272719311595 \\ 8962027581915134 \\ 513158181272727927 \\ 2751895182323122027 \end{pmatrix}$

The cypher text becomes ;

$$\begin{pmatrix} 4725453624372621272932 \\ 632574655428186666285 \\ 7554788370613741575141 \\ 153731419876111125109105107145 \end{pmatrix}$$

Encrypt using a steganographic technique

After this first cypher cypher text, applying text steganography, the sender decides to use classmates' names. This implies that the non-intended recipient may think that those are just names. Even if he concentrates, he will not understand what it means. Only the chairperson will understand that the first group with few words is the key, and the one with many names is the data.

Table 12; Cipher Matrix

1.Abdulazeez	Abigail	Adugna	1.Agatha
Ahmed	1.Annclet	1.Anna	1.Arnold
2.Bob	1.Bright	Charles	1.Chepkoeck
2.Cloudine	Collins	Desdery	4.Diana

Source; (Researchers, 2023)

In table 12, The receiver understands that it is key and can arrange the cypher text depending on the rows of the cypher matrix.

Table 13 Cipher Text

47.Dinaeli	25.Eddy	45.Edrisa	36.Emmanuel	24.Eugine
37.Eunice	26.Francis	21.Gideon	27.Gilbert	29.Gloria
85.Maria	67.Idris	32.Jane	57.Jarome	46.John
55.Joseph	42.Joshua	81. Juma	86.Kalifa	66.Kettie
62,Kudra	32.Henry	75.Martha	54.Marwa	78.Mawazo
83.Miracle	70.Nattie	61.Nicholaus	37.Njambi	41.Olufemi
57.Peter	51.Prince	41.Privatus	153.Saida	73.Samson
141.Sibeso	98.Taiwo	76.Yannick	111.Joyati	125.Tanjona
109.Manon	105.Sollazo	107.Lilian	145.Selwin	

Source; (Researchers, 2023)

The chairperson takes the numbers beyond the names, and for names without numbers, he will consider them as (0); then, he creates the matrix and decrypts it as follows;

In the first group, he obtains a matrix, which is a cypher matrix

$$\text{Cypher text}= \begin{pmatrix} 1001 \\ 0112 \\ 2101 \\ 2014 \end{pmatrix}$$

And in the group, he obtains another matrix, the cypher text. And the second group, he obtains another matrix: the cypher text.

$$\text{Cipher text} = \begin{pmatrix} 4725453624372621272932 \\ 6732574655428186666285 \\ 7554788370613741575141 \\ 153731419876111125109105145 \end{pmatrix}$$

So the chairperson follows the same procedure shown in the previous chapter to decrypt the message; he finds the inverse of the cypher matrix and then multiplies it with the cypher text.

$$= \begin{pmatrix} -3-111 \\ 210-1 \\ -10-223 \\ 41-1-1 \end{pmatrix} \begin{pmatrix} 4725453624372621272932 \\ 6732574655428186666285 \\ 7554788370613741575141 \\ 153731419876111125109105145 \end{pmatrix}$$

$$\text{Plain text} = \begin{pmatrix} 202027271919311595 \\ 8962027581915134 \\ 513158181272727927 \\ 2751895182323122027 \end{pmatrix}$$

Then the chairperson arranges and assigns the letters to those numbers he gets the original message which was ‘THE TIME FOR THIS RESEARCH WAS TOO LIMITED’ as shown in Table 14

Table 14. Assigned plain text

T	H	E		T	I	M	E		F	O	R		T	H	I	S		R	E	S	E
20	8	5	27	20	9	13	5	27	6	15	18	27	20	8	9	19	27	18	5	19	5
A	R	C	H		W	A	S		T	O	O		L	I	M	I	T	E	D		
1	18	3	8	27	23	1	19	27	23	15	15	27	12	9	13	9	20	5	4	27	27

Source; (Researchers, 2023)

5.3. Example 2

The sender wants to send this message ‘THIS IS AIMS TANZANIA’, and the sender does not want people to know

5.3.1. Encryption part

By using Caesar cypher in cryptography, the sender encrypts the data as follows:

Table15. Encryption Part

Plain	T	H	I	S	I	S	A	I	M
Position	19	7	8	18	8	18	0	12	18
Key	21	21	21	21	21	21	21	21	21
+	40	28	29	39	29	39	21	33	39
Mod 26	14	2	3	13	3	13	21	7	13
Cipher	O	C	D	N	D	N	V	D	H
Plain	S	T	A	N	Z	A	N	I	A
Position	18	19	0	13	25	0	13	8	0
Key	21	21	21	21	21	21	21	21	21
+	39	40	21	34	46	21	34	29	21
Mod 13	13	14	21	8	20	21	8	3	21
Cipher	N	O	V	I	U	V	I	D	V

Source; (Researchers, 2023)

Therefore in Table 15, the first cypher text is

‘ O C D N D N V DH O V I U V I D V’

After the sender encrypts this information using by Caesar cypher technique in cryptography, then encrypts it again using text stenographic technique to obtain another cypher text as follows;
‘ O C D N D N V DH O V I U V I D V’ becomes

‘**O**ur **C**ommittee **D**oes **N**ot **D**emand **N**or **V**alue **D**ocuments **H**ardly **N**oted **O**pportune. **V**arious **I**nmates **U**se **V**iolence **I**n **D**emanding **V**agary’

Where the sender will send this information like this;

Our committee does not demand, nor value documents hardly noted opportune. Various inmates use violence to demand vagaries [1, 21].

This means that anybody can see this text, and the non-intended recipient understands that this is as usual information. While the intended- recipient understands to use the first letter from each word of that information and then decrypt it by using the key '21'.

5.3.2. Decryption Part

So the sender decrypts the information as follows;

After taking the first letter of each word, the sender will get ' O C D N D N V DH O V I U V I D V' and then use the Caesar cypher technique in cryptography with 21 as a key for decryption is as follow:

Table 16. Decryption part

Cipher	O	C	D	N	D	N	V	D	H
Position	14	2	3	13	3	13	21	3	7
Key	21	21	21	21	21	21	21	21	21
-	-7	-19	-18	-8	-18	-8	0	-18	-14
Mod 26	19	7	8	18	8	18	0	8	12
Plain	T	H	I	S	I	S	A	I	M
Cipher	N	O	V	I	U	V	I	D	V
Position	13	14	21	8	20	21	8	3	21
Key	21	21	21	21	21	21	21	21	21
-	-8	-7	0	-13	-1	0	-13	-18	0
Mod 26	18	19	0	13	25	0	13	8	0
Plain	S	T	A	N	Z	A	N	I	A

Source; (Researchers, 2023)

So the receiver obtains the original data, 'THIS IS AIMS TANZANIA' as shown in Table 5.6

6. CONCLUSION AND RECOMMENDATION

The study has shown that cryptography and Steganography are well-known techniques for providing security, especially when combined. This study presents a new approach for combining cryptography and Steganography using substitution technique in cryptography and text technique in Steganography. It has been observed that most authors combine the cryptography technique with the image steganography technique, believing it is the strongest combination. As presented in this study combining the substitution technique with the text steganography technique is also a secure combination for securing data. When encrypting the data, it depends on the sender's effort and critical thinking.

This study recommends that the combination of text steganographic technique and cryptographic technique is also one of the strongest for securing data. Video, audio steganographic techniques with cryptographic techniques securing data should also be combined in securing data, and they are also strong combinations

REFERENCES

[1] K. Bairangi. "Ascii based even-odd cryptography with grey code and image steganography. A dimension in data security". 1, 2011.

[2] M. Ajitsinh, Madhu Pahal. "study of cryptography and its techniques"." international Journal of Advanced Research in Computer Science and Software Engineering, 3, 2013.

[3] A.A, A.-H. S. Saad and N. Hussien. 'a combined approach of steganography and cryptography technique based on parity checker and Huffman encoding'. 'International Journal of Computer Applications (0975-8887)', 148, 2016.

[4] A.Siper, R. Farley, and C. Lombardo. 'the rise of steganography' 2005.

[5] Dunbar." A detailed look at steganographic techniques and their use in an open-systems environment". "SANS Institute 2002", 2002

[6] AbikoyeOluwakemi, S.AdewoleKayonde, and J.OladipupoAyatunde. Efficient data hiding system using cryptography and Steganography. IJAIS, 11(4): 1-6, 2012.

[7] Dhani, K. Panchal, M. Scholar and lecturer. Steganography using web documents as a carrier: a survey. INTERNATIONAL JOURNAL OF ENGINEERING DEVELOPMENT AND RESEARCH, 6(4), 2016.

[8] G.C Kessler. An overview of cryptography. 86(6), 2017.

[9] H. Y. Atown. "hide and encryption fingerprint image by using lsb and transposition pixel by spiral method". "International Journal of Computer Science and Mobile Computing".3:624 – 632, 2014.

[10] J. Olguin. Steganography. Available from www. Trustwave.com, 2016.

[11] M. D. Swanson, M. Kobayashi, and A.H Tewfik. Multimedia data-embedding and watermarking technologies. Proceedings of the IEEE, 86(6):1064 – 1087, 1998.

[12] N. Rani and J. Chaudhary. Text steganography techniques: A review. International Journal of Engineering Trend and Technology (IJETT), 4(7), 2013.

[13] R. Gouder, P. N. Patil, and A.G. Meshram. Secure data transmission by using Steganography. Information and knowledge management. 2(1), 2012.

[14] R. M. Kumar and P.R Murti. Data security and authentification using sts protocol(IJCSIT) International Journal of Computer Science and Information Technologies; 2, 2011.

[15] R. M. Nitesh and L. Pamulaparty. Text steganography: review. International Journal of computer Science Information & Technology & Security (IJCSITS), 6(4), 2016.

[16] R. Shaik, R.Job and R. massai. "image steganography using lsb + Huffman cod".International Journal of Computer Applications(0975- 8887), 99(5),2014.

[17] R.Shaik, R.Job and R. Massai. "data security and authentification using steganography and sts protocol". International Journal of Advanced Research in Computer Science and Electronic Engineering (IJARCSEE), 1(5):PP-114. 2012.

AUTHOR

Adam AloyceSemlambo is a researcher, book author and currently working as Lecturer informatics department at the Institute of Accountancy Arusha (IAA)

Dinaeli Paul Sabaya,is a researcher and currently working as Lecturer informatics department at the Institute of Accountancy Arusha (IAA)

Joel Kazobais a researcher and currently working as lecturer informatics department at the Institute of Accountancy Arusha (IAA)