Received: February 27, 2023. Revised: June 12, 2023.

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

High PSNR Using Fibonacci Sequences in Classical Cryptography and Steganography Using LSB

Christy Atika Sari[1]* Muhammad Hafizh Dzaki[2] Eko Hari Rachmawanto[2]
Rabea Raad Ali[2] Mohamed Doheir[3]

[1]Dian Nuswantoro University, Indonesia
[2]National University of Science and Technology, Nasiriyah, Iraq
[3]Geomatika Malaysia University, Malaysia
*Corresponding author's Email: christy.atika.sari@dsn.dinus.ac.id

Abstract: The exchange of confidential information should be done in a secure environment. Therefore, security is needed if the exchange of information is carried out using Internet media. The way to secure the information can be done using cryptography and steganography techniques. and vigenere cipher had been applied as cryptography techniques and the LSB method as steganography techniques. This research has also compared the effect of the Fibonacci sequence in the encryption process. In this study, six images were used, each with a different extension, size, and type of images. All these images will be inserted with the secret message resulting from the encryption that applies the Fibonacci sequence or without applying the Fibonacci sequence. Fibonacci series is used to generate a random key, which is used for encrypting the message in playfair encryption algorithm. The level of effectiveness of the Fibonacci sequence has been determined and measured using MSE, PSNR, Entropy, UACI, and NPCR. The highest PSNR was in a 512x512 pixel grayscale image with a result of 7.9632, the best PSNR obtained was more than 85 dB, while the best UACI obtained was more than 49% using Fibonacci and 34% without implementing Fibonacci. The NPCR obtained is both above 99%, it is just that the image that has been implemented by Fibonacci produces a slightly higher UACI.

Keywords: Steganography, Color image, Fibonacci, Least significant bit, Vigenere.

1. Introduction

Based on review, of all the forms of information that can be circulated, such as text, images, sound, and video, text, and images are the most commonly used forms of information exchange via the internet [1–7]. Given the risks on the internet that can occur, to prevent the theft or alteration of information sent via the internet, several ways can be done to improve security aspects [8, 9]. Several techniques have been implemented to secure data such as cryptography and steganography. Cryptography and Steganography [1, 6, 7, 9–11] are the techniques for securing data and information by using different keys and visual results. These two techniques are one of the solutions to improve the security aspects of conducting information transactions via the internet. In both cryptography and Steganography, in general, the principle that they must fulfill is to protect data security with five main rules, namely the confidentiality, integrity, availability, authenticity, and non-repudiation factors. Cryptography [8, 11] is the art and science of keeping messages secure. Cryptography itself comes from the Greek language and consists of 2 words. Cryptos which means 'hidden' and Graphein which means 'writing'. In the science of cryptography, information in a message that can initially be understood by humans will be scrambled with a 'key'. The result is a secret message that is no longer comprehensible to humans. technically, cryptography will convert plain text into cipher text using a 'key'. To restore the real meaning of the message, we also need a 'key' to convert the cipher texts into plain texts again. Based on the 'key',

Cryptography is divided into two. Symmetric cryptography is a type of cryptography where the 'key' for encryption is the same as the 'key' used for decryption. Old and simple algorithms such as and vigenere cipher are examples of symmetric cryptography algorithms [12–14]. Meanwhile, asymmetric cryptography is a type of cryptography where the 'key' used to encrypt is not the same as the 'key' used to decrypt. In asymmetric cryptography, new terms appear as the public key and private key. Modern algorithms such as RSA and AES are examples of asymmetric cryptography algorithms. Steganography [4, 5, 15, 16] is the science and art of hiding secret messages in such a way that the existence of the message is undetectable by the human senses. Steganography also comes from the Greek language and consists of 2 words. Steganos which means 'veiled' and Graphein which means 'writing'. In general, the application of Steganography can be done to insert a message in another digital file in the form of an image, video, or sound. This digital file is used as a cover to cover the message that you want to insert [10, 12, 17, 18]. Thus, the result of Steganography is a digital file that is different from the initial file and has been inserted with a message. The inserted digital file visually does not look different. However, human senses are unable to see the difference. This can happen because the manipulation that occurs in the Steganography process occurs at the binary level [13, 19, 20]. The lowest level in the computer data hierarchy. The basic requirement for Steganography is that the size of the hidden message should not be more than the size of the cover file. Some algorithms used in applying Steganography include least significant bit and Ezstego. The two message security techniques mentioned can complement each other. Cryptography will hide the original meaning of a message and convert it into a random message, then the randomized message will be inserted into a cover file, such as an image [11]. So, even if an unauthorized person gets this secret message, he or she will still have difficulty getting the information contained in the image because of Steganography. Even if he gets the information in the image, he still does not get the real meaning because there is still cryptographic security. To apply the cryptography techniques mentioned, the algorithms that are easy to perform are algorithm and Vigenere cipher algorithm. The algorithm is the oldest and simplest asymmetric algorithm [5, 7]. The basic concept of is to shift the alphabetical sequence according to many 'n' values, where this 'n' value will be the 'key' to encrypt or decrypt. Meanwhile, the Vigenere cipher Algorithm is a further modified algorithm of the Algorithm. Vigenere cipher is formed from many variations of 's shifting alphabet which results in a new table known as the Vigenere table. In general, both and Vigenere cipher only provide encryption and decryption for 26 alphabets. So, if someone wants to add certain numbers or symbols, they need a custom sequence for and a custom Vigenere Tabula Recta for Vigenere cipher so that the encryption and decryption process can run. To implement the mentioned Steganography techniques, an easy-to-do algorithm applies the concept of the least significant bit [14, 17]. As the name implies, this algorithm will occur at the binary level. The computer sees a digital message or cover file that will be used as essentially binary. By using the LSB concept, the binary bits of the message will be inserted into the binary bits of the cover whose significant value is the lowest. Thus, the inserted message can be recovered by taking all the binary bit values of the cover file that have the lowest significant value. Steganography manipulates the cover file to make it appear as if it contains the inserted message. What happens is just changing the smallest significant value of the cover file according to the binary value of the message you want to insert. Steganography requires it to work. The size of the message to be inserted cannot be more than the size of the cover file. The steganography result file is called the Stego File. From the research that has been studied by previous researchers, many of them have examined cryptography techniques using classical cryptography algorithms, such as and Vigenere cipher, or using modern cryptography algorithms such as RSA and DES. As for steganography techniques, the LSB method for inserting messages into cover media, such as photos, has been widely researched. However, research related to the use of the Fibonacci sequence in the data encryption process in cryptography techniques still have opportunities to develop [21–23].

Thus, this research aims to compare cryptography which is applies the Fibonacci sequence with those that do and do not. The comparison that has been carried out in this research uses the help of image media which is the message inserted with a cryptographic process that has been done beforehand. For the cryptography technique, this research uses algorithm and Vigenere cipher algorithm. Meanwhile, for the steganography technique, this research uses the LSB method. The Fibonacci sequence that has been used in this research uses the same concept as the Fibonacci sequence in general, but this research slightly modifies it to make it seem more varied.

The outline of this paper present ten section where section 1 is the introduction of the paper. Section 2 covers related research on classical

cryptography. Section 3 covers and section 4 covers Vigenere cipher. Section 5 covers least significant bit (LSB). Section 6 covers Fibonacci. Meanwhile section 7 covers our proposed method. Section 8 covers quality measurement. Section 9 covers testing of experiment result. Finally, section 10 covers conclusion.

2. Related research

Some related research that has been studied by previous researchers is useful as a basic reference in terms of comparison, analysis, and enriching the discussion. Research conducted by Raksha Verma in 2022 [24] recalled the basic concept of cryptography from one of the oldest algorithms. Verma's research discusses the complete steps of how to encrypt and decrypt the Algorithm along with mathematical calculations. The discussion is also presented in the form of a flowchart so that the explanation is easy to understand. The conclusion that can be obtained is that is the easiest cryptography algorithm to do. This is because only provides encryption for 26 capital and non-capital alphabet characters by shifting the cipher alphabet according to the 'key' value used. Therefore, Caesar's cipher can be easily broken using the Brute force method. It is better, in encrypting a message using Caesar's cipher, the encrypted cipher text is re-encrypted using Caesar's algorithm once again or can be combined using other encryption algorithms. Research researched by Deepanshu Gautam in 2018 [25] recalls a modified Cryptography algorithm from with the name Vigenere cipher. Vigenere cipher itself is considered more secure in securing data than because the 'key' used is not limited to an integer value between 1 to 25. The 'key' used in the encryption and decryption process can be a word. Thus, an attempt to perform the Brute force method to break the encrypted message in Vigenere cipher is more difficult to break than. A distinctive feature of the Vigenere cipher is the Vigenere table which is a guideline for encryption and decryption. In the research discussed by Gautam, it is also included how to encrypt messages using Vigenere cipher mathematically. Gautam also wrote an example of a Vigenere table that is commonly used as a guideline for encryption and decryption. It can be concluded that the Vigenere cipher is a further modified encryption algorithm. With innovations and modifications from, Vigenere cipher is considered to have more security than. Research researched by Indra Gunawan in 2019 [26], discusses research related to the idea of combining two different encryption algorithms to produce cipher text that is more difficult to crack. The research Indra has done is to combine the algorithm and the RSA Algorithm. The algorithm used in Indra's research is the algorithm in general. Meanwhile, Rivest Shamir Adleman or abbreviated RSA is one of the modern cryptographic algorithms used to encrypt a message. Unlike Caesar or Vigenere, RSA is asymmetric cryptography. This means that the 'key' for encryption is different from the 'key' for decryption. Indra's research shows the steps to be able to combine two types of encryption algorithms to create a cipher text that is more difficult to crack. What can be obtained from this research is that it is possible to combine two cryptographic algorithms. The encryption result of the combination of two algorithms will produce a cipher text that is more difficult to crack.

However, because insertion and manipulation occur at the binary level, human senses will have difficulty realizing the difference. Both parts of the encrypted data are put back together and Steganography is performed to be inserted into the cover image. So, the purpose of this combination is to increase the security aspect as implemented in our proposed method.

In this research, Fibonacci is used to randomize the Vigenere cipher key. The original cipher is encrypted with the and produces ciphertext1, this ciphertext is then encrypted with the Vigenere cipher using a Fibonacci-based random key. Next is embedding with LSB.

3. Caesar cipher

The algorithm is the oldest and most popular symmetric cryptography technique. It is called symmetric because the 'key' used for encryption is the same as the 'key' used for decryption. The name Caesar itself is taken from a Roman emperor named Julius Caesar. Historically, Julius Caesar used this encryption to protect the important messages he sent and prevent information from being leaked by intruders. Reportedly, Caesar's cipher is the origin of cryptography. This algorithm is said to be the simplest and easiest cryptographic algorithm. This can happen because the basic Caesar algorithm only accepts 26 alphabets from 'A' to 'Z', both capital and non-capital. Then, each alphabet of the message is replaced with another alphabet whose value depends on how big the shift value is. Therefore, the actual shift value can only be between 1 and 25 shifts. Due to this limitation, the is relatively easy to crack using the Brute Force method by criminals [12]. However, with the development of the human mindset, itself has been subjected to several more complex

Table 1. Sample bits in LSB

Bits	Information
1001 1000	The lowest significant value is 0
0011 0111	The lowest significant value is 1
0001 1101	The lowest significant value is 1
0101 1011	The lowest significant value is 1
1100 1010	The lowest significant value is 0
0011 1111	The lowest significant value is 1
0001 0010	The lowest significant value is 0
1110 0110	The lowest significant value is 0

variations to obtain more security aspects [25–29]. High. In addition to shifting the alphabet, the shift value of the can be manipulated by multiplying, dividing, and reversing the order of the alphabet. Thus, the security aspect of can be increased [12], [29]. In general, the encryption and decryption of the algorithm can be represented in Eq. (1), and equation (2), where $E(P)$ is Character P encryption, $D(P)$ is Character P decryption, P is P value in ASCII table, n is shift value.

$$E(P) = (P + n)\ mod\ 26 \quad (1)$$

$$D(C) = (C - n)\ mod\ 26 \quad (2)$$

4. Vigenere cipher

The Vigenere cipher algorithm is a symmetric cryptography technique and is a further modification of the Algorithm. This algorithm was introduced in the ^{16}th century by Blaise de Vigenere. The reason why Vigenere cipher can be said to be a further modification of is that Vigenere cipher consists of various lines with different shift values [12, 14, 29]. The number of lines with different values forms a table called the Vigenere table.

Unlike where the 'key' value is limited to 25 shifts, the 'key' used in Vigenere cipher can be a random word. If the length of the 'key' is less than the message length, then the characters that make up the 'key' will be repeated until it meets the message length. Meanwhile, if the length of the 'key' is more than the message length, the 'key' will be cut according to the required message length as shown in Eqs. (3) until Eq. (6). Changes in the human mind make further modifications to Vigenere by including numbers and symbols such as '!', '@', '#', and others. Thus, producing a custom Vigenere Table that certainly affects the variety of 'keys' and the variety of message contents that can be created.

$$E(P) = (P + K)\ mod\ 26 \quad (3)$$

$$E(P) = (P + K) - 26,$$
if the sum of P and K is more than 26 (4)

$$D(P) = (C - K)\ mod\ 26 \quad (5)$$

$$(P) = (C - K) + 26,$$
if the sum of P and K is minus (6)

5. Least significant bit

Least significant bit (LSB) is one of the commonly methods in Steganography. As the name implies, LSB designates the lowest significant bit value in an 8-bit binary format. For example, there are 8 image pixels with an 8-bit binary format as shown in Table 1. In computer memory, each value in the matrix that makes up a digital image is in binary form. On the other hand, a digital text message is also stored in binary form on the computer. Since the basic form of all the things mentioned is binary, the idea of inserting a message into another medium as a container becomes possible. This concept is the basis of LSB. The result of inserting a message into an image using the LSB method will result in an image that is different from the original image [3, 8], 12, 17]. However, the difference only occurs at the binary level. Thus, the human senses will find it very difficult to realize the difference. A basic requirement that must be met in performing LSB Stegongraphy is that the length of the message bits multiplied by eight cannot be more than the length of the cover bits [14], [30]. If this condition is not met, the message will be truncated.

6. Fibonacci

The Fibonacci sequence in mathematics that many people are familiar with is a recursive sequence of 2 previous numbers with 0 and 1 as the base [21–23]. Thus, if the base number is assumed to be $a = 0$ and $b = 1$ the Fibonacci form as in the example above can be made into a mathematical model as shown in Eq. (7) where $Fab(n)$ is n-th Fibonacci number, a is a first base number, n is second base number.

$$F_{ab}(n) = \begin{cases} a, for\ n = 1 \\ b, for\ n = 2 \\ F(n-1) + F(n-2), else \end{cases}$$
$$where\ a \neq b \neq 0 \quad (7)$$

$$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, ...,$$
$$89, 144, 233, 377, 610, 987$$

$$Q_\lambda = \begin{bmatrix} 1 & 1 & \dots & 1 & 1 \\ 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 \end{bmatrix}_{\lambda x \lambda} = \begin{bmatrix} f_\lambda & f_{\lambda-1} + \cdots + f_1 & f_{\lambda-1} + \cdots + f_2 & \dots & f_{\lambda-1} \\ f_{\lambda-1} & f_{\lambda-2} + \cdots + f_0 & f_{\lambda-2} + \cdots + f_1 & \dots & f_{\lambda-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ f_2 & f_1 + \cdots + f_{1-(\lambda-2)} & f_1 + \cdots + f_{1-(\lambda-3)} & \vdots & f_1 \\ f_1 & f_0 + \cdots + f_{0-(\lambda-2)} & f_0 + \cdots + f_{0-(\lambda-3)} & \dots & f_0 \end{bmatrix} \quad (9)$$

$$Q_\lambda^k = \begin{bmatrix} f_{k+\lambda-1} & f_{k+\lambda-2} + \cdots + f_k & f_{k+\lambda-2} + \cdots + f_{k+1} & \dots & f_{k+\lambda-2} \\ f_{k+\lambda-2} & f_{k+\lambda-3} + \cdots + f_{k-1} & f_{k+\lambda-3} + \cdots + f_k & \dots & f_{k+\lambda-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ f_{k+1} & f_k + \cdots + f_{k-(\lambda-2)} & f_k + \cdots + f_{k-(\lambda-3)} & \vdots & f_k \\ f_k & f_{k-1} + \cdots + f_{k-\lambda+1} & f_{k-1} + \cdots + f_{k-\lambda+2} & \dots & f_{k-1} \end{bmatrix} \quad (10)$$

7. Proposed method

The research that has been done is divided into two main techniques. Cryptography technique that converts the secret message into cipher text and steganography technique that inserts the secret message into a prepared image. Each technique will also be divided into two, message encryption and secret message decryption. For the cryptographic techniques, as the objective of this research is to compare the effect of the Fibonacci sequence, the flowchart will still be divided into two, cryptographic techniques that apply the Fibonacci sequence and cryptographic techniques that do not apply the Fibonacci sequence as shown in Fig. 1 until Fig. 4. Fig. 1 is a scheme for encrypting a message without applying the Fibonacci sequence. Meanwhile, Fig. 2 is a scheme for encrypting a message by applying the Fibonacci sequence. Both Fig. 1 and Fig. 2 use the same secret message input. However, because Fig. 2 the Fibonacci sequence is involved, and the 'key' treatment that will be used in Fig. 1 and Fig. 2 will be different. The result of the cryptographic encryption produces a cipher text that is certainly different between Fig. 1 and Fig. 2. The steganography process is done using the same image in both diagrams and had been compared. We adopted proposed method by Kalika Prasad [31]. The generalized Fibonacci sequence is given by λ^{th} as in Eq. (8), with initial values $f_0 = f_1 = f_2 = \cdots = f_{\lambda-2} = 0, f_{\lambda-1} = 1$.

$$f_{\lambda+k} = f_k + f_{k+1} + \cdots + f_{\lambda+k-1} \quad k \geq 0, \lambda \in \mathbb{Z}^+ \quad (8)$$

The corresponding multinacci Q_λ-matix of order λ as shown in Eq. (9).

By mathematical induction, it can be easily verified that Eq. (10)

Further, for generalized negative multinacci sequence the recurrence Eq. (8) can be re-write as in Eq. (11).

$$f_k = f_{k+\lambda} - (f_{k+1} + \cdots + f_{k+\lambda-1}) \quad for\ k \leq -1 \quad (11)$$

or, equivalently

$$f_{-k} = f_{-k+\lambda} - (f_{-k+1} + \cdots + f_{-k+\lambda-1}) \quad for\ k \geq 1 \quad (12)$$

Encryption algorithm:

1. Sender chooses Caesar key
2. Secret key
3. Encryption: $E(P) = (P + n)\ mod\ 26$
4. Secret key Vigenere cipher using secret number e, such that $1 < e < \emptyset(p)$
5. Key matrix: $k \leftarrow Q_\lambda^k$, where Q_λ^k is multinacci matrix order as shown in Eq. (10)
6. Encryption: $E(P) = (P + K)\ mod\ 26$
7. Do least significant bit
8. Transmit to receiver

Decryption algorithm:

1. Do invert Least Significant Bit
2. Secret key vigenere cipher: $\lambda \leftarrow k^D$, where where D is receiver secret key
3. Key matrix vigener cipher: $k \leftarrow Q_\lambda^k$
4. Decryption Vigenre cipher: $D(P) = (C - K)\ mod\ 26$
5. Decryption : Encryption: $E(P) = (P + n)\ mod\ 26$
6. Get Plaintext

Based on Fig. 1, the scheme has been done in several stages:

1. Enter the secret message.
2. Select a shifting 'key' n and perform the encryption algorithm.
3. Select the word 'key' for Vigenere cipher and perform the Vigenere cipher encryption algorithm.

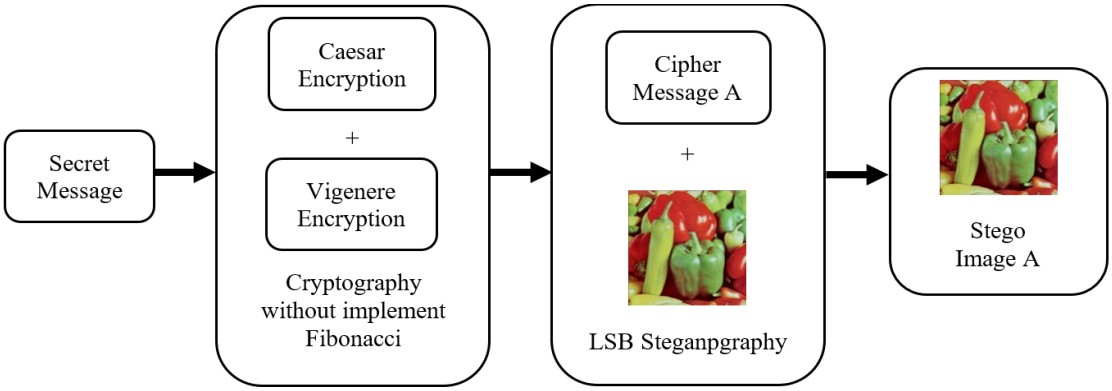


Figure. 1 Image encryption without Fibonacci

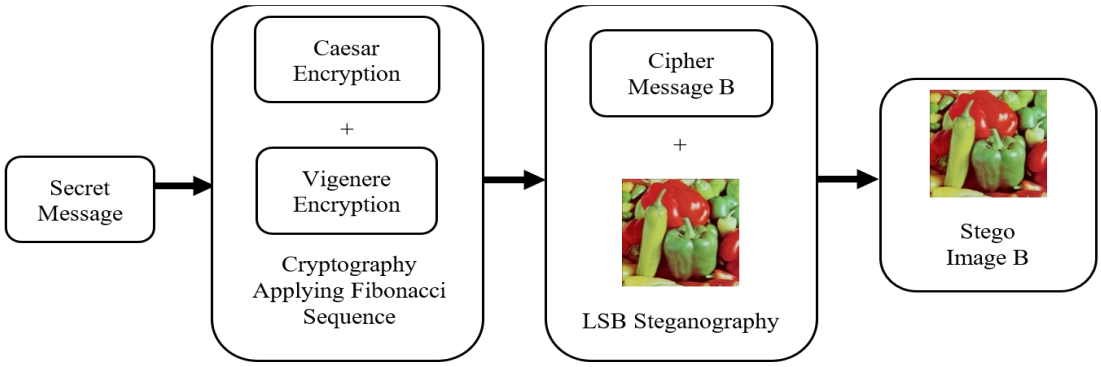


Figure. 2 Image encryption using Fibonacci

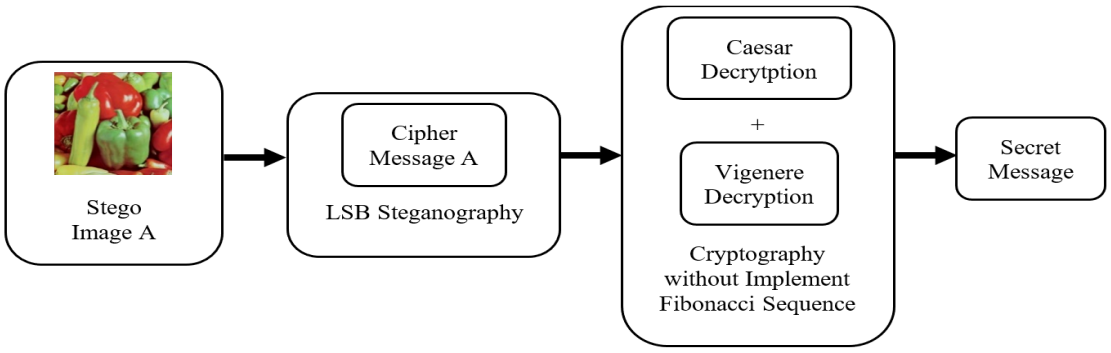


Figure. 3 Image encryption using Fibonacci

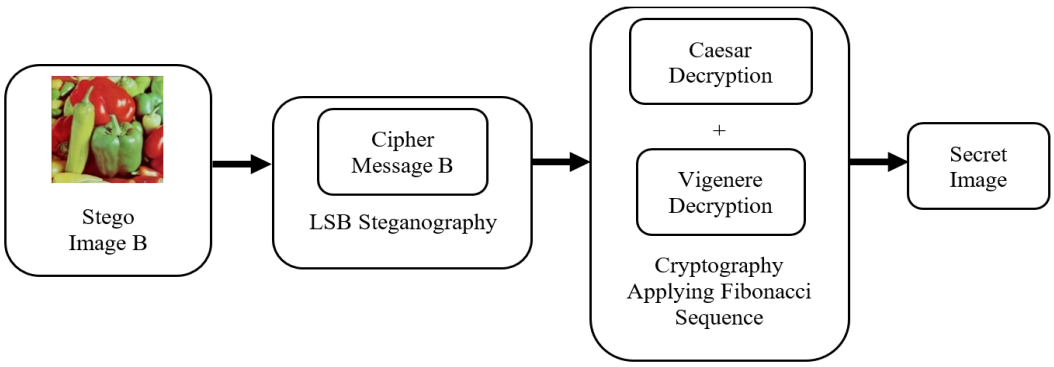


Figure. 4 Image decryption using Fibonacci

4. Prepare a cover image and perform message insertion using the LSB method.

Based on Fig. 2, schemes work as follows:

1. Choose Fibonacci's sequence theme.
2. Give a limit for Fibonacci's sequence.
3. From plain text, using the limited Fibonacci's sequence to do the 's encryption algorithm.

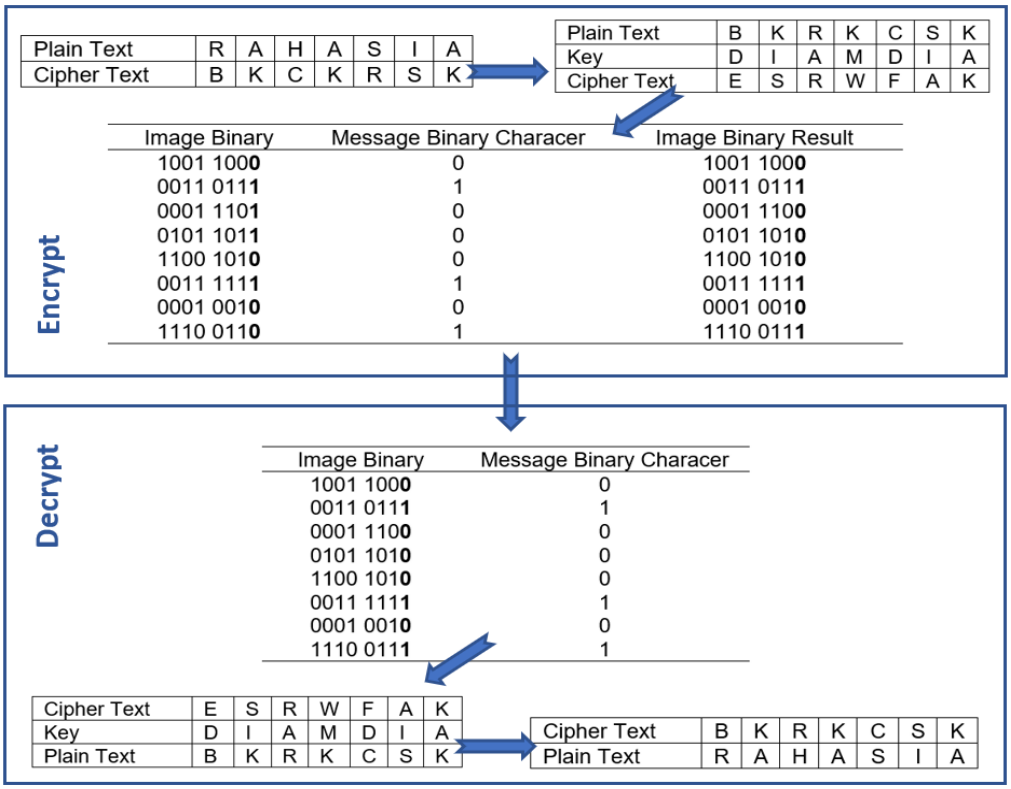


Figure. 5 Encrypt and decrypt illustration without Fibonacci

4. Choose an integer limit and sum the limited Fibonacci's sequence until equal to that integer.
5. Every member that had been built integer, then give the alphabet representation.
6. Use these alphabets to do Vigenere cipher algorithm.
7. Prepare cover image and do the LSB method to embed cipher text inside the image.

Based on Fig. 3, the scheme has been done using several stages:

1. Extract the cipher Text from Stego image.
2. Using the same word ‘key’, do Vigenere cipher’s decryption algorithm.
3. Using the same shift ‘key’, do ’s decryption algorithm.
4. Got the message back.

Based on Fig. 4, the scheme has been done in several stages:

1. Extract the Cipher Text from Stego Image.
2. Using the same Limited Fibonacci’s Sequence, get the ‘key’ for Vigenere and do Vigenere Decryption.
3. Shift back the alphabet-based Limited Fibonacci's Sequence for Caesar Decryption.
4. Got a message back.

Fig. 3 is a scheme for decrypting a message without applying the Fibonacci sequence. Meanwhile, Fig. 4 is a scheme for decrypting a message by applying the Fibonacci sequence. Both diagrams also use the same Stego Image input from the encrypted secret message. Due to retrieving the secret message, the same 'key' is reentered at the time of encryption. The result of cryptographic decryption produces the same plain text content based on Fig. 3 and Fig. 4.

Suppose, the secret message is "RAHASIA" using key shifting value (n) = 10 in and the keyword "DIAM" had been implemented in Vigenere cipher. Steganography Process of Message Insertion Using LSB Method Suppose, 8 pixels image with 8-bit binary formats. The ASCII value for the character 'E' is 69. Thus, the 8-bit binary form is '0100 0101'. Repeat with the next 8 image pixels for the next cipher Text character until all characters in the cipher text are inserted in the image as shown in Fig. 6. For the message decryption process, the process is carried out using the same secret message "RAHASIA" using key shifting value (n) = 10 in and the keyword is "DIAM" as shown in Fig. 6. The binary '0100 0101' is obtained. The binary value in decimal is 69. In the ASCII table, the value 69 had been representing the character 'E'.

A loop is performed on the next 8 pixels to extract the message characters until the cipher text is formed. Next, we encrypt the secret message by applying the Fibonacci sequence. However, it is necessary to first

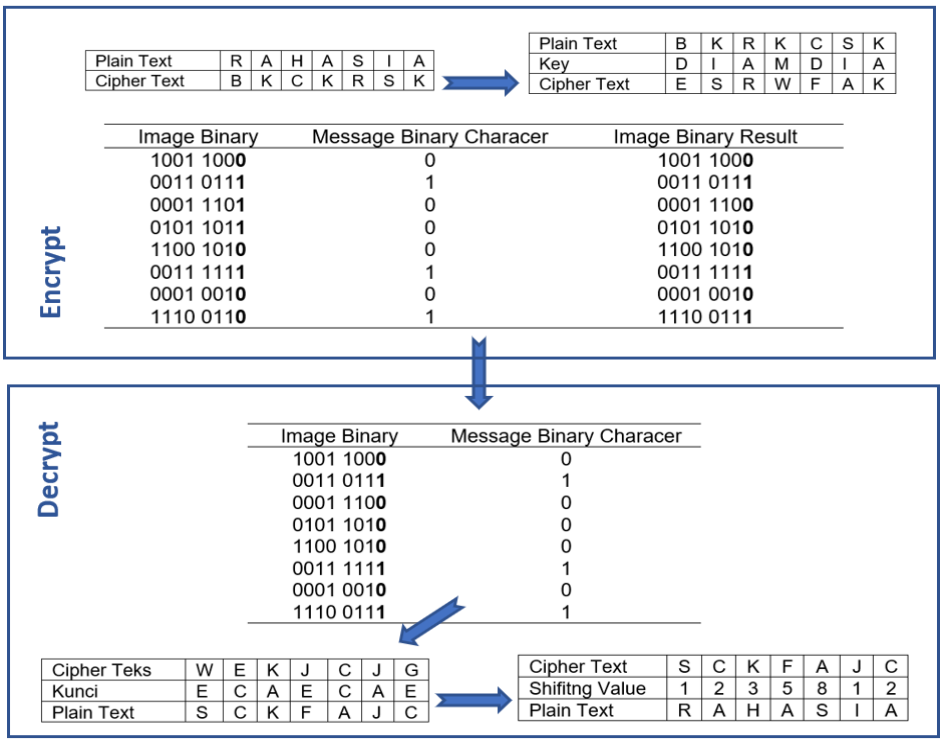


Figure. 6 Encrypt and decrypt illustration using Fibonacci

Table 2. Fibonacci representation

Fibonacci Number	1	2	3	5	8
Text Representation	A	B	C	D	E

understand how the Fibonacci sequence in this research works.

1. The Fibonacci values used are based on 1 and 2. Thus, the sequence obtained is F_{12} = 1, 2, 3, 5, 8, 13, 21, 55, 89, 144, ...
2. Give the limit value of the Fibonacci sequence $F_{12}(n)$, where n = 5. Thus, the sequence used is just F_{12} = 1, 2, 3, 5, 8.
3. A representation of the initial 5 alphabets was also obtained in Table 2.

Give a limit value with k = 12. Thus, we get the key combination for the Vigenere cipher by 12 = 8 + 3 + 1 = ECA. The process has been shown in Fig. 7. The encryption process using the Fibonacci sequence using Encryption process using Key shifting F12 = 1, 2, 3, 5, 8 and Limit value k = 12 = 8 + 3 + 1 = ECA. The steganography process of message insertion using the LSB Method has been done using converted value. Suppose, 8 pixels image with 8-bit binary format The ASCII value for the character 'W' is 87. Thus, the 8-it binary form is '0101 0111'. Repeat with the next 8 image pixels for the next cipher text character until all characters in the cipher text are inserted in the image.

8. Quality measurement

8.1 MSE and PSNR

This research measures the similarity and quality between images using several techniques. The aim is to prove that the two images being compared are not the same image. MSE (mean square error) is the most common method of measuring the quality between two images. The closer the MSE value is to 0, the better the quality of the comparison image. MSE has no units. The formula for finding the MSE value between two images is as in Eq. (13) for a grayscale image and Eq. (14) for a color image, where m is image length, n is image width, S_{xy} is Image before xy index pixel, C_{xy} is Image after xy index pixel.

$$MSE = \frac{1}{mn}\sum_{x=1}^{m}\sum_{y=1}^{n}\left(S_{xy} - C_{xy}\right)^2 \quad (13)$$

$$MES = \frac{1}{M \times \mathrm{N}}\sum_{x=1}^{x}\sum_{y=1}^{y}\sum_{z=1}^{z}\|C_i(x,y,z)S_i(,y,z)\|^2 \quad (14)$$

PSNR (peak signal to noise ratio) is used to calculate and compare the wave signal ratio value between two images. Contrary to MSE, the higher the PSNR value, the more similar the comparison images will be. The unit of PSNR is decibel (dB), with minimum value up to 40 dB [32, 33]. The formula for

finding the PSNR value of two images is shown in Eq. (15), where C_{max} is the maximum length or width of the image.

$$PSNR = 10 \log_{10}\left(\frac{C_{max}{}^2}{MSE}\right) \quad (15)$$

8.2 Entropy

Entropy is used to calculate a random statistical value to estimate the texture of an image. The higher the entropy value, the higher the image quality with the good value is close to 8 [34]. The entropy value can only be found in Greyscale images. Thus, RGB images must be converted to Grayscale. The formula for finding the entropy of an image is shown in Eq. (16), where p is the Sum of the x- and y-axis normalized histograms.

$$Entropy = \sum_{x=1}^{m} \sum_{y=1}^{n} (p_{xy} \log_2(p_{xy})) \quad (16)$$

8.3 UACI and NPCR

Unified averaged changed intensity (UACI) and number pixel changing rate (NPCR) represent the qualitative and quantitative values of a Stego image in its resilience to withstand various image attacks. The lower the UACI value, the better the resilience of the Stego image in resisting image attacks [35]. Conversely, the higher the NPCR value, the better the resilience of the Stego image in resisting attacks. Formulas for finding UACI and NPCR as shown in Eq. (17) and Eq. (18), where m is image length, n is image width, D is value 0 if pixels are equal (value 1 if the pixel values are different), $C_{1(xy)}$ is a picture before, $C_{2(xy)}$ is a picture after.

$$NPCR = \frac{\sum_{x=1}^{m} \sum_{y=1}^{n} (D_{xy})}{mn} \quad (17)$$

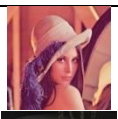
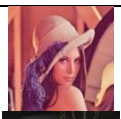
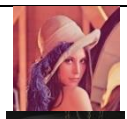
$$UACI = \frac{\sum_{x=1}^{m} \sum_{y=1}^{n} (|C_{1(xy)} - C_{2(xy)}|)}{mn} \quad (18)$$

9. Testing

Visually to the human eye, there are 5 images, each with a different extension had been processed as shown in Table. 3. The original image and the Stego Image, either by applying Fibonacci or without applying Fibonacci, look like there is no difference.

Thus, the computer can only detect the difference easily. This is done by performing the checking method with the proof in the next discussion as shown in Table 3. Based on Fig. 7 and Fig. 8, three out of four test images experienced an increase in

Table 3. Image visualization using and without Fibonacci

Image	Before Processing	After Processing	
		without Fibonacci	with Fibonacci
Lena.tiff			
Watch.png			
Opera.bmp			
Lochness.gif			

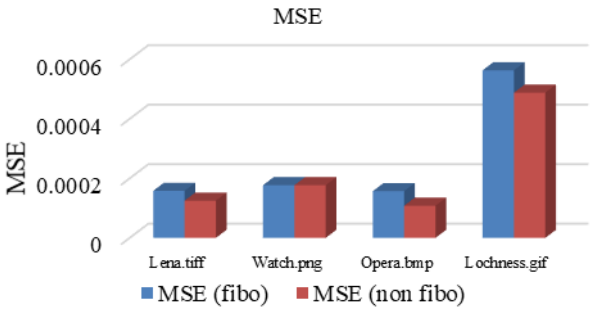


Figure. 7 Comparison of MSE

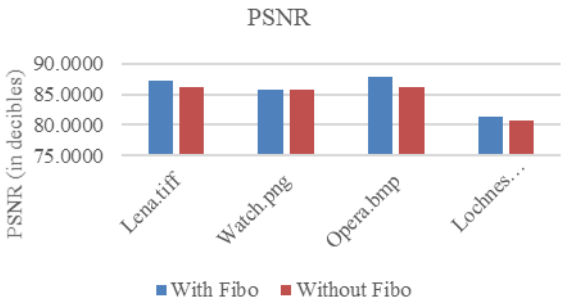


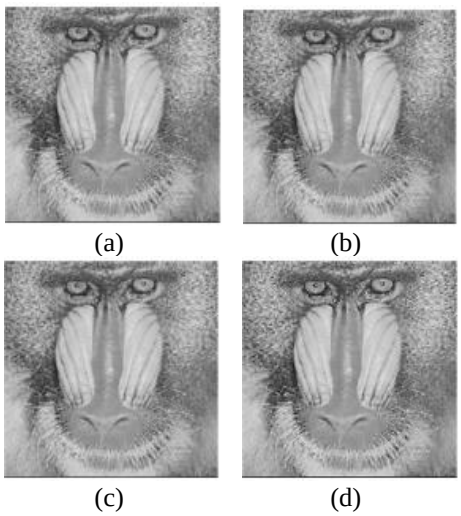
Figure. 8 Comparison of PSNR

PSNR. An interesting thing happens to images with the '.png' extension. The MSE and PSNR values obtained look the same. However, since the calculation does not have an 'inf', the difference must be at a small comma. The smallest PSNR value is obtained by images that have a '.gif' extension.

Another test using UACI and NPCR has been tested and produced good value with a range from 99,791 to 99,889. A good UACI value according to xxx, is close to 50% while the UACI is close to 100%. Here, our proposed method was produced close to standard values. This result is shown in Table 4.

Table 4. UACI-NPCR (in %)

Image	Without Fibonacci		With Fibonacci	
	NPCR	UACI	NPCR	UACI
Lena.tiff	99,112	34,195	99,878	49,002
Watch.png	99,025	34,091	99,889	48,723
Opera.bmp	99,048	34,111	99,791	49,003
Lochness.gif	99,214	34,403	99,818	49,020



(a) (b) (c) (d)

Figure. 9 The comparison results of our proposed method using grayscale in 512x512 pixels: (a) Cover image, (b) LSB, (c) Caesar-Vigenere-LSB, and (d) Caesar-Vigenere-LSB-Fibonacci

Table 5. Entropy value

Type	Size	Image	Entropy
Grayscale	512	Lena	7,9328
		Watch	7,9632
		Opera	7,9295
		Lochness	7,9339
Color		Baboon	7,8776
	1024	Lena	7,8883

The Fibonacci sequence has been shown to have an effect in increasing the PSNR value as shown in Table 4. Automatically, the imperceptible value of the image goes up. Although the increase in value is proven to be very small, at least, the tested classical cryptography can still apply the Fibonacci sequence to increase the Imperceptible value. The best result of this research is an increase in PSNR value of 1.627 from 86.184 dB to 87.8113 dB obtained from image files with the '.bmp' extension. The best results are obtained by images with the '.png' extension in terms of UACI values and consequent NPCR values for both without the Fibonacci sequence and with the Fibonacci sequence, where NPCR values are higher than UACI values. The limit of this research is only a small increase in the PSNR value and the vulnerability of the inserted secret message to be lost is very high if an attack occurs on the image.

Our entropy for all images is close to 8, and the grayscale image produces higher entropy than the color image as shown in Table 5. Based on experiments on images with different types and different sizes, it is known that the resulting entropy values are above 7, with the best standard entropy being close to 8. Comparison based on 40% embedding on grayscale and color images in our proposed method produces higher values. On the other hand, the UACI NPCR has proven good results even though it is not optimal for 100%, but the use of Fibonacci proves an increase in the UACI NPCR value.

10. Conclusion

There is an increase in the PSNR value in the encryption process that applies the Fibonacci sequence. Although there is an insignificant increase, the Fibonacci sequence still proves to be successful in increasing the value. The entropy obtained in the image shows a value of 7. That means the stego image is still well-readable. Except for the image with the '.gif' extension, the image shows a significant difference from the original image. Except for images with the '.gif' extension, NPCR values that are lower than UACI values indicate that images are highly vulnerable to losing secret messages in the event of an attack on them. The hypothesis of why there is only a very small increase in PSNR value is because the Fibonacci variation used should be varied more. For example, in Caesar's cipher encryption, forward and backward shifts of the alphabet are combined. Another hypothesis is that there is very little increase in PSNR value because the algorithm under study is a classical cryptographic algorithm.

Suggestions for this research, the results of the test of the effect of the Fibonacci sequence on classical cryptography are sufficient to be made as science and as a reference only. This research is good for education and additional reference. Preferably, there is no need to use this method in the scope of industrial and corporate work. The vulnerability of losing information when there is an attack on the image is already a fatal weakness when used in the scope of the world of work. Hope for future research, add methods such as Shifting Bit or applying the XOR concept. Or it can also be done by enriching the variation by utilizing the Fibonacci sequence.

Conflicts of interest

To the International Journal of Intelligent Engineering and Systems's policy and my ethical duty as a researcher, I certify that this manuscript has not been previously published, copied, or submitted

to another journal. I have reported them in full to the International Journal of Intelligent Engineering and Systems and obtained the consent of all authors to handle any possible conflicts of interest arising from this research.

Author contributions

Conceptualization, Christy Atika Sari and Muhammad Hafizh Dzaki; methodology, Christy Atika Sari; software, Christy Atika Sari; validation, Christy Atika Sari, Muhammad Hafizh Dzaki, and Eko Hari Rachmawanto; formal analysis, Christy Atika Sari; investigation, Christy Atika Sari and Rabea Raad Ali; resources, Christy Atika Sari and Mohamed Doheir; data curation, Christy Atika Sari; writing—original draft preparation, Christy Atika Sari; writing—review and editing, Christy Atika Sari; visualization, Christy Atika Sari; supervision, Christy Atika Sari; project administration, Christy Atika Sari and Rabea Raad Ali; funding acquisition, Muhammad Hafizh Dzaki and Mohamed Doheir.

Acknowledgments

This work was supported by Dian Nuswantoro University Grant Research 2023.

References

[1] M. S. Taha, M. S. M. Rahem, M. M. Hashim, and H. N. Khalid, "High payload image steganography scheme with minimum distortion based on distinction grade value method", *Multimed Tools Appl*, Vol. 81, No. 18, pp. 25913–25946, Jul. 2022, doi: 10.1007/s11042-022-12691-9.

[2] K. Muhammad, J. Ahmad, N. U. Rehman, Z. Jan, and M. Sajjad, "CISSKA-LSB: color image steganography using stego key-directed adaptive LSB substitution method", *Multimed Tools Appl*, Vol. 76, No. 6, pp. 8597–8626, 2017, doi: 10.1007/s11042-016-3383-5.

[3] M. R. Islam, T. R. Tanni, S. Parvin, M. J. Sultana, and A. Siddiqa, "A modified LSB image steganography method using filtering algorithm and stream of password", *Information Security Journal: A Global Perspective*, Vol. 30, No. 6, pp. 359–370, 2021, doi: 10.1080/19393555.2020.1854902.

[4] N. Jiang, N. Zhao, and L. Wang, "LSB Based Quantum Image Steganography Algorithm", *International Journal of Theoretical Physics*, Vol. 55, No. 1, pp. 107–123, 2016, doi: 10.1007/s10773-015-2640-0.

[5] S. Chakraborty, A. S. Jalal, and C. Bhatnagar, "LSB based non blind predictive edge adaptive image steganography", *Multimed Tools Appl*, Vol. 76, No. 6, pp. 7973–7987, 2017, doi: 10.1007/s11042-016-3449-4.

[6] O. Y. Abdulhammed, P. J. Karim, D. R. Arif, T. S. Ali, A. O. Abdalrahman, and A. A. Saffer, "A Secure Image Steganography Using Shark Smell Optimization and Edge Detection Technique", *Kurdistan Journal of Applied Research*, pp. 11–25, 2022, doi: 10.24017/science.2022.2.2.

[7] K. Joshi and R. Yadav, "A new LSB-S image steganography method blend with Cryptography for secret communication", in *2015 Third International Conference on Image Information Processing (ICIIP)*, 2015, pp. 86–90. doi: 10.1109/ICIIP.2015.7414745.

[8] J. N. Shehab, H. A. Abdulkadhim, and T. F. H. A. Tameemi, "Robust large image steganography using lsb algorithm and 5d hyper-chaotic system", *Bulletin of Electrical Engineering and Informatics*, Vol. 10, No. 2, pp. 689–698, 2021, doi: 10.11591/eei.v10i2.2747.

[9] S. Bukhari, M. S. Arif, M. R. Anjum, and S. Dilbar, "Enhancing security of images by Steganography and Cryptography techniques", In: *Proc. of 2016 Sixth International Conference on Innovative Computing Technology (INTECH)*, IEEE, pp. 531–534, 2016, doi: 10.1109/INTECH.2016.7845050.

[10] S. L. Chikouche and N. Chikouche, "An improved approach for lsb-based image steganography using AES algorithm", In: *Proc. of 2017 5th International Conference on Electrical Engineering - Boumerdes (ICEE-B)*, pp. 1–6, 2017, doi: 10.1109/ICEE-B.2017.8192077.

[11] A. Susanto, D. R. I. M. Setiadi, E. H. Rachmawanto, C. A. Sari, R. R. Ali, and I. U. W. Mulyono, "Dual Security Method for Digital Image using HBV Encryption and Least Significant Bit Steganography", *Journal of Physics: Conference Series*, Institute of Physics Publishing, 2019, doi: 10.1088/1742-6596/1201/1/012024.

[12] I. Gede, A. P. Dewangga, T. W. Purboyo, and R. A. Nugrahaeni, "A New Approach of Data Hiding in BMP Image Using LSB Steganography and Caesar Vigenere Cipher Cryptography", 2017, [Online]. Available: http://www.ripublication.com

[13] J. P. Sermeno, K. A. S. Secugal, and N. E. Mistio, "Modified Vigenere cryptosystem: An integrated data encryption module for learning management system", *International Journal of Applied Science and Engineering*, Vol. 18, No. 4 (Special Issue), pp. 1–10, 2021, doi: 10.6703/IJASE.202106_18(4).003.

[14] L. Voleti, R. M. Balajee, S. K. Vallepu, K. Bayoju, and D. Srinivas, "A Secure Image Steganography Using Improved Lsb Technique and Vigenere Cipher Algorithm", In: *Proc. of International Conference on Artificial Intelligence and Smart Systems, ICAIS 2021*, Institute of Electrical and Electronics Engineers Inc., pp. 1005–1010, 2021, doi: 10.1109/ICAIS50930.2021.9395794.

[15] N. Akhtar, S. Khan, and P. Johri, "An improved inverted LSB image steganography", In: *Proc. of 2014 International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT)*, IEEE, pp. 749–755, 2014, doi: 10.1109/ICICICT.2014.6781374.

[16] S. Pramanik, D. Samanta, S. Dutta, R. Ghosh, M. Ghonge, and D. Pandey, "Steganography using Improved LSB Approach and Asymmetric Cryptography", In: *Proc. of IEEE International Conference on Advent Trends in Multidisciplinary Research and Innovation, ICATMRI 2020*, Institute of Electrical and Electronics Engineers Inc., 2020, doi: 10.1109/ICATMRI51801.2020.9398408.

[17] A. Amirulhaqi, T. W. Purboyo, and R. A. Nugrahaeni, "Security on GIF Images Using Steganography with LSB Method, Spread Spectrum and the Vigenere Cipher," *International Journal of Applied Engineering Research*, Vol. 12, No. 23, pp. 13604–13609, 2017.

[18] M. S. Taha, M. S. M. Rahem, M. M. Hashim, and H. N. Khalid, "High payload image steganography scheme with minimum distortion based on distinction grade value method", *Multimed Tools Appl*, Vol. 81, No. 18, pp. 25913–25946, 2022, doi: 10.1007/s11042-022-12691-9.

[19] S. Rajendran and M. Doraipandian, "Chaotic map based random image steganography using LSB technique", *International Journal of Network Security*, Vol. 19, No. 4, pp. 593–598, 2017, doi: 10.6633/IJNS.201707.19(4).12.

[20] M. Juneja and P. S. Sandhu, "An Improved LSB Based Steganography Technique for RGB Color Images", *International Journal of Computer and Communication Engineering*, pp. 513–517, 2013, doi: 10.7763/ijcce.2013.v2.238.

[21] K. Prasad and H. Mahato, "Cryptography using generalized Fibonacci matrices with Affine-Hill cipher", *Journal of Discrete Mathematical Sciences and Cryptography*, Vol. 25, No. 8, pp. 2341–2352, 2022, doi: 10.1080/09720529.2020.1838744.

[22] G. Ch, H. Md, M. T, P. D, S. Ch, and P. R. K. K, "Fibonacci Multichaos Algorithm for Medical Image Encryption for Transmission Through Wavelet Transform Based OFDM System and Its VLSI Realization", *International Journal of Online and Biomedical Engineering (iJOE)*, Vol. 18, No. 06, pp. 133–139, 2022, doi: 10.3991/ijoe.v18i06.30281.

[23] K. Prasad and H. Mahato, "Cryptography using generalized Fibonacci matrices with Affine-Hill cipher", *Journal of Discrete Mathematical Sciences and Cryptography*, Vol. 25, No. 8, pp. 2341–2352, 2022, doi: 10.1080/09720529.2020.1838744.

[24] R. Verma, A. Kumari, A. Anand, and V. S. S. Yadavalli, "Revisiting Shift Cipher Technique for Amplified Data Security", *Journal of Computational and Cognitive Engineering*, 2022, doi: 10.47852/bonviewJCCE2202261.

[25] D. Gautam, C. Agrawal, P. Sharma, M. Mehta, and P. Saini, "An Enhanced Cipher Technique Using Vigenere and Modified", in *2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI)*, pp. 1–9, 2018, doi: 10.1109/ICOEI.2018.8553910.

[26] I. Gunawan, Sumarno, H. S. Tambunan, E. Irawan, H. Qurniawan, and D. Hartama, "Combination of Algorithm and Rivest Shamir Adleman Algorithm for Securing Document Files and Text Messages", *Journal of Physics: Conference Series*, Institute of Physics Publishing, 2019, doi: 10.1088/1742-6596/1255/1/012077.

[27] G. O. Asoronye, G. I. Emereonye, C. O. Onyibe, and I. A. Agha, "An Efficient Implementation for the Cryptanalysis of Caesar's Cipher", 2019.

[28] M. D. Pujitha, "Security Enhancement Using Caesar Cipher", *International Journal of Research Publication and Reviews*, Vol. 3, No. 11, pp. 9–16, 2022.

[29] Z. Qowi and N. Hudallah, "Combining and hill cipher in the generating encryption key on the vigenere cipher algorithm", in *Journal of Physics: Conference Series*, IOP Publishing Ltd, 2021, doi: 10.1088/1742-6596/1918/4/042009.

[30] M. Juneja and P. Singh Sandhu, "Improved LSB based Steganography Techniques for Color Images in Spatial Domain", *International Journal of Network Security*, Vol. 16, No. 6, pp. 452–462, 2014.

[31] K. Prasad and H. Mahato, "Cryptography using generalized Fibonacci matrices with Affine-Hill cipher", *Journal of Discrete Mathematical Sciences and Cryptography*, Vol. 25, No. 8, pp.

2341–2352, 2022, doi: 10.1080/09720529.2020.1838744.

[32] E. W. Abood *et al.*, "Audio steganography with enhanced LSB method for securing encrypted text with bit cycling", *Bulletin of Electrical Engineering and Informatics*, Vol. 11, No. 1, pp. 185–194, 2022, doi: 10.11591/eei.v11i1.3279.

[33] O. F. AbdelWahab, A. I. Hussein, H. F. A. Hamed, H. M. Kelash, and A. A. M. Khalaf, "Efficient Combination of RSA Cryptography, Lossy, and Lossless Compression Steganography Techniques to Hide Data", *Procedia Comput Sci*, Vol. 182, pp. 5–12, 2021, doi: 10.1016/j.procs.2021.02.002.

[34] X. Zhang, L. Wang, G. Cui, and Y. Niu, "Entropy-Based Block Scrambling Image Encryption Using DES Structure and Chaotic Systems", *Int. J. Opt.*, Vol. 2019, pp. 1–13, 2019, doi: 10.1155/2019/3594534.

[35] A. H. Khaleel and I. Q. Abduljaleel, "Secure image hiding in speech signal by steganography-mining and encryption", *Indonesian Journal of Electrical Engineering and Computer Science*, Vol. 21, No. 3, p. 1692, 2021, doi: 10.11591/ijeecs.v21.i3.pp1692-1703.