Journal of Techniques, ISSN: 2708-8383, Vol. 5, No. 1, 2023, Pages 38-43
DOI: https://doi.org/10.51173/jt.v5i1.1087

JOURNAL OF TECHNIQUES

Journal homepage: http://journal.mtu.edu.iq

*RESEARCH ARTICLE - ENGINEERING*

# Multistage Encryption for Text Using Steganography and Cryptography

**Mohammed Majid Msallam [1,2*], Fayez Aldoghan [2]**

[1] Control and Systems Engineering Department, University of Technology, Baghdad, Iraq

[2] Computer Engineering Department, Ankara University, Ankara, Turkey

[*] Corresponding author E-mail: mohammedarjeeli92@gmail.com

**Article Info.**

*Article history:*

Received
21 November 2022

Accepted
06 February 2023

Publishing
31 March 2023

**Abstract**

Recently, the movement of data between smart devices has piqued the world's curiosity because it transmits important and unimportant data via the Internet. Thus, important data must be encrypted during passing over a network so that information can only access by an intended receiver and processed by it. As a result, information security has become even more critical than before. Our proposal suggests a method to secure data in three stages using cryptography and steganography. The important message will divide into two parts a part will encrypt by Caesar Cipher and another by Vigenere Cipher. The ciphertext will process by Morse code and will then hide in a cover image using Least Significant Bits (LSB) technique. According to the value the of peak signal-to-noise ratio (PSNR) obtained in this work our proposal has an extra security level and robustness. Finally, our research provides more security because of the mixture between cryptography and steganography.



Publisher : Middle Technical University

**Keywords**: Caesar Cipher; Morse Code; Vigenere Cipher; Least Significant Bit; Multistage of Encryption.

## 1. Introduction

One of the most crucial challenges in information and communication technology research is to make more security for any system moving data via the internet. Where system security is becoming increasingly important whenever more important transmitted data so data of individuals must be secured by encryption when it moves via the internet. Since most individuals now access the internet through smart devices, their internet connection must be protected from unwanted attacks by outsiders and hackers. Conditions of system security must be satisfied to have a safe and secure internet connection such as authorized access to data. These specifications safeguard data from unauthorized access, data loss, unauthorized modifications, and other threats which are called for password authentication to access data and protect the smart devices of users and their data [1]. Where Fig. 1[1] shows the most important classification of security techniques that use to protect the system.

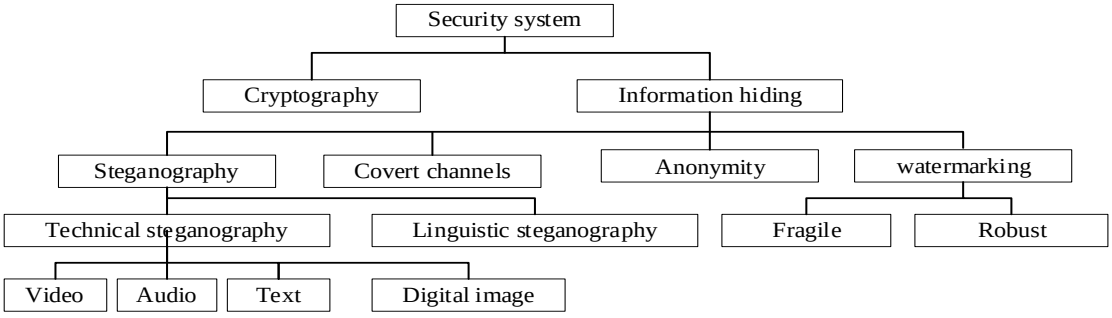



Fig. 1. Classification of security system techniques

Researchers of security for systems face an interesting problem because the technology and the method of hacking are become today developed. The foundation of modern communication is data, so the idea of data hiding was developed to safeguard information and ensure that it does not go to an unauthorized user. In another aspect, the mass of information is made distribution possible via the Internet or over computer networks. Since protecting access and use must be prevented by confidentiality and data integrity. Using steganography and cryptography are two methods to secure the information contained in the message and change its meaning to obfuscate it from unauthorized individuals who might intercept it. Steganography relies on encoding messages in multimedia files that are not expected by hackers [2].

| Nomenclature | | | |
|---|---|---|---|
| LSB | Least Significant Bits | PSNR | Peak Signal-To-Noise Ratio |
| Dev.-PSO | developed Particle Swarm Optimization | MSE | Mean Squared Error |
| RSA | Rivest–Shamir–Adleman | RSA | Rivest–Shamir–Adleman |

Shukur et al. [3] proposed a method to embed an important message in the cover image by determining an optimal path using the developed Particle Swarm Optimization (Dev.-PSO) and then hiding in the cover image using Least Significant Bits (LSB) technique. The performance of their work for peak signal-to-noise ratio (PSNR) and Mean Squared Error (MSE) after an intended attack such as after salt & pepper noise, Gaussian noise had the ability to survive for the stego image. The two-stage of security used that was cryptography and steganography by Voleti et al. [4]. They used the Vigenere Cipher algorithm in cryptography to encrypt secret text while the LSB technique was used to hide ciphertext in a cover image. A multistage of security was used was Caesar Cipher, Rivest–Shamir–Adleman (RSA), and LSB technique in 2022 by Sidi et al. [5]. The secret message was encrypted using Caesar Cipher at the first stage and then using RSA in the second stage to obtain ciphertext while the third stage was hidden the ciphertext using the LSB technique. In another framework [6], Caesar Cipher and Hill Cipher; which was modified into Morse code; were two-stage to obtain the ciphertext. The ciphertext was hidden in the cover image by the LSB technique. the result of their work is that difficult for irresponsible people or cryptanalysts to solve messages sent in the form of images because multistage encryption was used. In the hybrid multistage to encrypt data, Osman et al. [7] was proposed method to secure data building sequential and pseudo-random encoding/decoding algorithms to obtain the ciphertext. The stego image was obtained after hiding the ciphertext in the cover image. In their work, the user selects the method sequential or random to encrypt secure data after that the system hides it in a cover image. They found that it was suitable that the text size should be 15% smaller than the cover image and the performance of their work was more efficient and time consuming.

This paper is organized as a methodology and explains the methods of cryptography and steganography used in the section on the research method. While the results obtained from the implementation of our proposal and discussion for results are presented in the section on the results and discussion. Finally, the conclusion has been presented in the section on the conclusion.

## 2. Research Method

Steganography and cryptography both offer safe communications and can be utilized simultaneously, which is a crucial thing to remember. Execution of steganography and cryptography are different. While the encrypted file is recognized as having been transferred, the secret message, which is the transmitted file itself, cannot be recovered without the secret key. Confidentiality is aided by encryption, but protection ends after decryption. In steganography, the presence of the stego message is covered up with a cover file so that an adversary cannot tell that a message is present. As long as the stego file is recognized by the embedding mechanism used, the stego message can be extracted using the stego key [8]. Most researchers interested in information security use more than one stage of encryption to increase the robustness and security of the system. This motivation prompted us to propose a cryptographic system based on cryptography and steganography. Our system is from two stages of cryptography and one stage of steganography. In the first stage of our proposal, the important text will divide into two parts then the first part will encrypt by Caesar Cipher while the second part will be encrypted by Vigenere Cipher. In the second stage, the ciphertext will be modified into Morse code. In the third stage, the ciphertext will then be hidden in an image by using the LSB technique such as in Fig. 2.

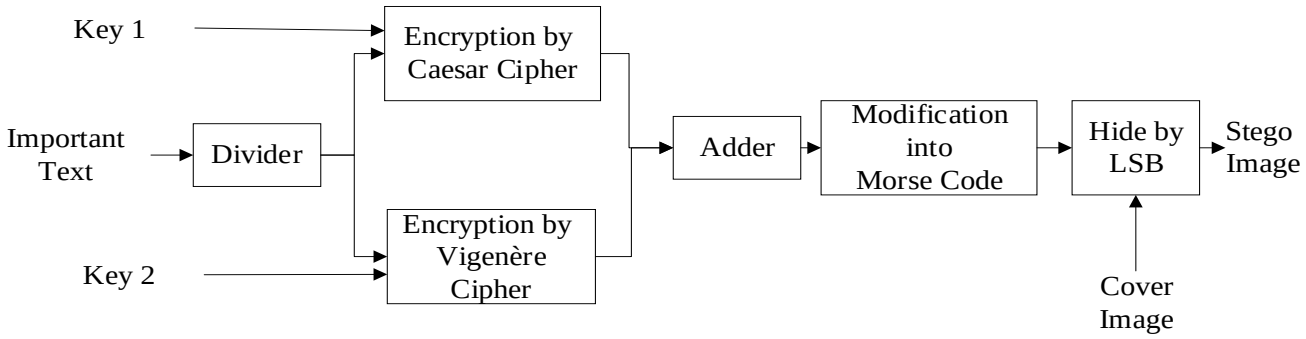



Fig. 2. Our system to protect important information

### *2.1. Caesar Cipher*

The Caesar Cipher is a simple method to encrypt a secret text by rotating the plaintext by the value of the key [9] such as in Fig. 3. Where the cipher text is becoming "DE" if an important message was "AB", and the key is equal to 3. The (1) and (2) are used to calculate a mathematical model for the Caesar cipher to encrypt and decrypt an important text[10].

$$\mathrm{Tc} = \mathrm{E}(\mathrm{P},\mathrm{K}) = (\mathrm{P} + \mathrm{K}) \bmod 36 \quad (1)$$

$$\mathrm{Td} = \mathrm{D}(\mathrm{C},\mathrm{K}) = (\mathrm{C} - \mathrm{K}) \bmod 36 \quad (2)$$

Where a Tc and Td are ciphertext and decrypted text. While a K and P are shifting key and plain text. The 36 that was used in this equation means that used the English alphabet and number in the use of important text. In this framework, Caesar Cipher uses to encrypt and decrypt secret text in the first part.

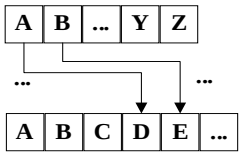



Fig. 3. Caesar encryption with key 3

*2.2. Vigenere Cipher*

A compound alphabet cipher called Polyalphabetic Substitution Cipher which was published in 1586 by French ambassador and cryptographer Blaise de Vigenere contains the Vigenere Cipher. The Vigenere Cipher is a technique for encoding alphabetic text that bases the Caesar cipher sequence on the letters in the keyword. Two methods are often used to implement the Vigenere Cipher Substitution approach [11].

1) By utilizing a Caesar cipher series based on the letters in the password, the numeral, Vigenere Cipher with numerals encrypts the text of the alphabet.
2) Vigenere Cipher letters are written in 26 rows, each row shifting to the left of the previous row to make one of the 26 possible Caesar Cipher. In accordance with the repeating key, each letter is supplied on a separate line.

In our framework, the Matrix of Vigenere Cipher is used to encrypt and decrypt secret text in the second part. If the plaintext SIX is encrypted with the key DFH, S is changed to V in the D row. I is changed to N in the F row, and X is changed to E in the H row such as show in Fig. 4.

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

Fig. 4. Example to encrypt by Vigenere Cipher

*2.3. Morse code*

Morse code is a method to modify the text used in encryption. Dots and dashes are standardized sequences of two different signal durations that are used in communication to represent text characters in Morse code [12]. In our work, ciphertext modifies to Morse code using Table 1 [13].

Table 1. Morse codes for characters and number

| Character | Symbols | Character | Symbols | Character | Symbols | Character | Symbols |
|---|---|---|---|---|---|---|---|
| A | .- | J | .--- | S | ... | 1 | .---- |
| B | -... | K | -.- | T | - | 2 | ..--- |
| C | -.-. | L | .-.. | U | ..- | 3 | ...-- |
| D | -.. | M | -- | V | ...- | 4 | ....- |
| E | . | N | -. | W | .-- | 5 | ..... |
| F | ..-. | O | --- | X | -..- | 6 | -.... |
| G | --. | P | .--. | Y | -.-- | 7 | --... |
| H | .... | Q | --.- | Z | --.. | 8 | ---.. |
| I | .. | R | .-. | 0 | ----- | 9 | ----. |

*2.4. Least Significant Bits (LSB) technique*

The least significant bit (LSB) technique is a straightforward method for including data in image files. The most basic steganographic algorithms directly embed the message's bits in the cover image's least significant bit plane in a deterministic sequence. A fundamental LSB substitution

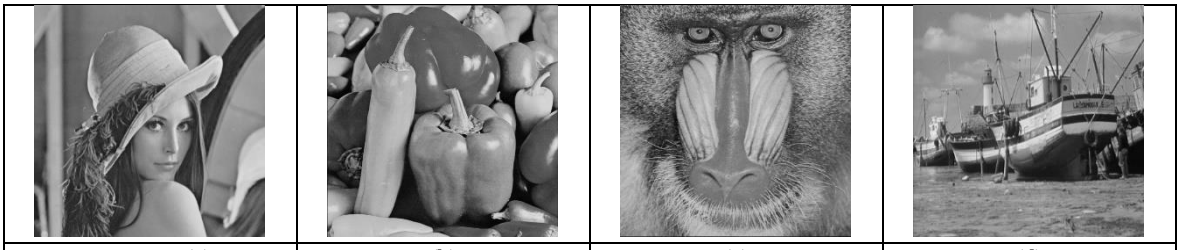
procedure involves converting m samples of a secret message from integer numbers to binary. In the end, the secret message bits will replace every single bit pixel of the cover image [14]. Instead of dots, spaces, dashes, and slashes, a binary format is used in this work such as in Table 2 which the ciphertext change to binary format using to decrease the number of pixels that use in the process of a substitute.

Table 2. Morse code in binary format

| Punctuation Marks | Character | Binary |
|---|---|---|
| Dot | . | 00 |
| Space | | 01 |
| Dash | - | 10 |
| Slash | / | 11 |

## 3. Results and Discussion

Lenna, Peppers, Baboon, and Boat are images that are used as cover data of size 512×512 and grey colour as shown in Fig. 5. In MATLAB R2018b, our work was programming.



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

Fig. 5. The cover image of (a) Lenna, (b) Peppers, (c) Baboon, and (d) Boat

The secret message has 104 characters that divide into two parts. The first 52 characters are encrypted by Caesar Cipher while the other 52 characters are encrypted by Vigenere Cipher. The ciphertext of Caesar Cipher and the ciphertext of Vigenere Cipher collect in one stream and coding by morse codes. The result of these processes is shown in Table 3.

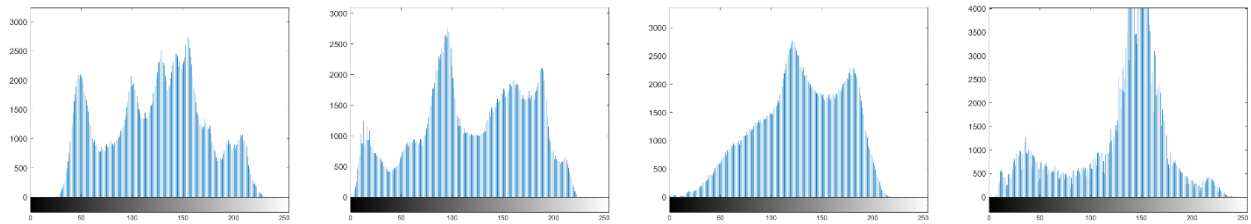
Table 3. Result of our work

| The process | The result |
|---|---|
| The secret text | albert einstein was born in 1955 in germany and got swiss and american nationality his parent had jewish |
| The ciphertext | doehuw hlqvwhlq zdv eruq lq 4b88 lq jhupdq1 dqg jrw fjvff naq nzrevpna angvbanyvgl uvf cnerag unq wrjvfu |
| Morse codes | -.. --- . .... ..- .-- /.... .-.. --.- ...- .-- .... .-.. --.- /--.. -.. ...- /. .-. ..- --.- /.-.. --.- /....- -... ---.. ---.. /.-.. --.- /.--- .... ..- .--. -.. -<br>-.- .---- /-.. --.- --. /.--- .-. .-- /..-. .--- ...- ..-. ..-. /-. .- --.- /-. --.. .-. . ...- .--. -. .- /.- -. --. ...- -... .- -. -.-- ...- --. .-.. /..- ...- ..-.<br>/-.-. -. . .-. .- --. /..- -. --.- /.-- .-. .--- ...- ..-. ..- |

The coded text is hidden at the cover image to get the stego image. the stego image of Lenna, Peppers, Baboon, and Boat is shown in Fig. 6 and the histogram of the stego images and the cover images are shown in Figs. 7 and 8.

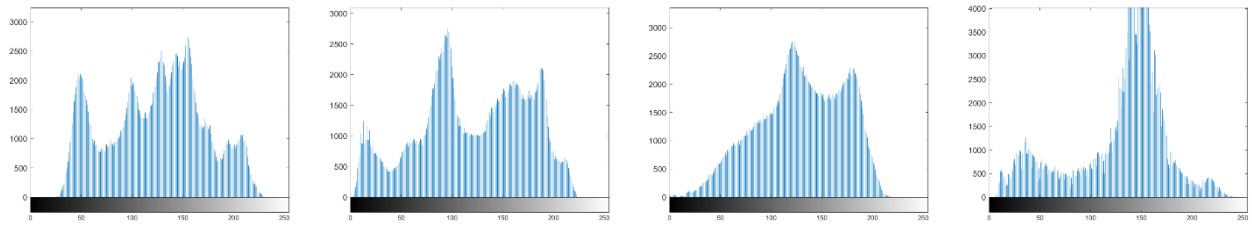
(a) (b) (c) (d)

Fig. 6. The stgno image of (a) Lenna, (b) Peppers, (c) Baboon, and (d) Boat



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

Fig. 7. Histogram of cover for (a) Lenna, (b) Peppers, (c) Baboon, and (d) Boat



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

Fig. 8. Histogram of stego for (a) Lenna, (b) Peppers, (c) Baboon, and (d) Boat

The relative between a stego image to an original image is peak signal-to-noise ratio (PSNR) which is defined in (3) [15]. if the number of PSNR is higher, it means the quality of the stego image is good.

$$\text{PSNR (db)} = 10 \log_{10} \frac{(2^{\text{n}}-1)^2}{\text{MSE}} \quad (3)$$

Where n is equal to 8 and its meaning is the number of bits per pixel of the image and MSE is the Mean Squared Error (MSE) between the stego image and the cover image that is defined in (2) [14].

$$MSE = \frac{1}{W \times H} \sum_{r=0}^{W-1} \sum_{c=0}^{H-1} (I(r,c) - D(r,c))^2 \quad (4)$$

Where I (r, c) and D (r, c) are a pixel value of a cover image and a stego image at a location r and c while W and H are the numbers of the rows and the columns in an image.

The average error between the cover image and the stego image is known as the mean absolute error (MAE) and is defined in (5) [16]. The quality of the stego image improves with decreasing MAE values.

$$\text{MAE} = \frac{1}{W \times H} \sum_{r=0}^{W-1} \sum_{c=0}^{H-1} |I(r,c) - D(r,c)| \quad (5)$$

Where I (r, c) and D (r, c) are the cover pixel value of image and the stego image respectively. W and H are the numbers of the rows and the columns in an image.

The values of MSE, PSNR, and MAE for the Lenna image, the Peppers image, the Baboon image, and the Boat image are shown in Table 4. The values of MSE and MAE are equal because the change in difference value is ±1.

Table 4. Result

| Image | MSE | PSNR | MAE |
|---|---|---|---|
| Lenna | 0.00046921 | 81.41 | 0.00046921 |
| Peppers | 0.00054169 | 80.79 | 0.00054169 |
| Baboon | 0.00048447 | 81.27 | 0.00048447 |
| Boat | 0.00042725 | 81.82 | 0.00042725 |

The Comparison of our work and Arroyo [17] is shown in Table 5 for the value of PSNR. The size of the image is 512×512 and the color mode is grayscale. The Size of the secret message is 16kB. Where the quality of the image in our work is high than [17] so that the doubt of hackers is less in the presence of important data. The doubt of hackers is less in the presence of important data due to the higher image quality.

Table 5. Value of PSNR for our proposal and [17]

| Image | Arroyo [17] | | Our | |
|---|---|---|---|---|
| | MSE | PSNR | MSE | PSNR |
| Lenna | 0.09353 | 58.42 | 0.079525 | 59.12 |
| Peppers | 0.09386 | 58.40 | 0.079716 | 59.11 |

## 4. Conclusion

The combination of steganography and cryptography to secure important data makes a robust system. The Vigenere Cipher, Caesar Cipher, and Morse Cipher used cryptography while LSB used steganography. The three stages of encryption in our framework make that it difficult for the hacker to know the content of the important message. where the secret message is divided into two parts then each part is encrypted by a method. the ciphertext is code using Morse codes then hidden in a cover image using LSB. The PSNR among the cover image and stego image gives a higher value which means the eyes of humans cannot observe or suspect that there is hidden data.

## Acknowledgment

We would like to thank our colleagues Sarah Kareem Salim and Huda Ismail Olewi at the University of Misan to encourage us and give us advice and support to complete this research work.

**Reference**


[1] M. Alotaibi, D. Al-hendi, B. Alroithy, M. AlGhamdi, and A. Gutub, "Secure Mobile Computing Authentication Utilizing Hash, Cryptography and Steganography Combination," Journal of Information Security & Cybercrimes Research, vol. 2, no. 1, pp. 73–82, 2019.

[2] S. Ahmed Laskar, "High Capacity data hiding using LSB Steganography and Encryption," International Journal of Database Management Systems, vol. 4, no. 6, pp. 57–68, 2012.

[3] W. A. Shukur and K. K. Jabbar, "Information hiding using LSB technique based on developed PSO algorithm," International Journal of Electrical and Computer Engineering, vol. 8, no. 2, pp. 1156–1168, 2018.

[4] 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," Proceedings of the International Conference on Artificial Intelligence and Smart Systems, pp. 1005–1010, 2021.

[5] E. V. Sidi, I. Diop, and K. Tall, "A New hybrid approach of Data Hiding Using LSB Steganography and Caesar cipher and RSA algorithm (S-ccr)," 2022 International Conference on Computer Communication and Informatics, pp. 25–28, 2022.

[6] M. Azmi and Z. Zulkarnaen, "Implementasi Kombinasi Caesar Cipher dan Hill Cipher Menggunakan Modifikasi Sandi Morse Untuk Pengamanan Pesan Berbasis Teks," Jurnal Teknologi Informasi dan Multimedia, vol. 3, no. 1, pp. 8–13, 2021.

[7] O. M. Osman, M. E. A. Kanona, M. K. Hassan, A. A. E. Elkhair, K. S. Mohamed, "Hybrid multistage framework for data manipulation by combining cryptography and steganography." Bulletin of Electrical Engineering and Informatics vol 11, no. 1, pp. 327-335,2022.

[8] J. M. Ahmed and Z. Ali, "Information Hiding using LSB technique," International Journal of Computer Science and Network Security, vol. 11, no. 4,, pp. 18–25, 2011.

[9] G. Song, K. Jang, and H. Kim, "Grover on Caesar and Vigenère Ciphers" Cryptology ePrint Archive, 2021.

[10] Z. Qowi and N. Hudallah, "Combining caesar cipher and hill cipher in the generating encryption key on the vigenere cipher algorithm," Journal of Physics: Conference Series, 2021.

[11] R. Hammad, K. A. Latif, A. Z. Amrullah, Hairani, A. Subki, P. Irfan, M. Zulfikri, L. Z. A. M, M. Innuddin, and K. Marzuki "Implementation of combined steganography and cryptography vigenere cipher, caesar cipher and converting periodic tables for securing secret message," Journal of Physics: Conference Series, p.1-6, 2022.

[12] S. N. Deshpande, V. A. Deshmukh, G. D. Arjun, H. R. Goskonda, A. R. Butala, and D. S. Datar, "Human Computer Interaction through Morse Code," International Journal of Research in Engineering and Science, vol. 9, no. 7, pp. 54–61, 2021.

[13] R. Seetharaman et al., "FPGA Based Morse Code Communicator for Visual and Speech Impaired People using Basys-3," Proceedings of the International Conference on Electronics and Renewable Systems (ICEARS 2022), no. Icears, pp. 1889–1894, 2022.

[14] H. A. Abdulkadhim and J. N. Shehab, "Audio steganography based on least significant bits algorithm with 4D grid multi-wing hyper-chaotic system," International Journal of Electrical and Computer Engineering, vol. 12, no. 1, pp. 320–330, 2022.

[15] N. F. H. Al Saffar, I. R. Al-Saiq, and R. R. M. Abo Alsabeh, "Asymmetric image encryption scheme based on Massey Omura scheme," International Journal of Electrical and Computer Engineering, vol. 12, no. 1, pp. 1040–1047, 2022.

[16] Y. Moussa and W. Alexan. " Message Security Through AES and LSB Embedding in Edge Detected Pixels of 3D Images." 2020 2nd Novel Intelligent and Leading Emerging Sciences Conference (NILES). IEEE, 2020.

[17] J. C. T. Arroyo, "An Efficient Least Significant Bit Image Steganography with Secret Writing and Compression Techniques," International Journal of Advanced Trends in Computer Science and Engineering, vol. 9, no. 3, pp. 3280–3286, 2020.