

Hiding algorithm based fused images and Caesar cipher with intelligent security enhancement

Huda Hussein Abed, Aqeel Sajjad Shaeel, Ruaa Shallal Abbas Annoze

Engineering Technical College-Najaf, Al-Furat Al-Awsat Technical University, Najaf, Iraq

Article Info

Article history:

Received Mar 18, 2023

Revised May 21, 2023

Accepted Jun 4, 2023

Keywords:

1's complement
Caesar cipher
Fused images
Hiding algorithm
Intelligent methods

ABSTRACT

The process of sending confidential data through the communication media and in complete secrecy is now necessary, whether the data is related to patients, a particular military operation, or a specified office. On the other hand, with the development of various ciphering algorithms, and information hiding algorithms, there is a need to obtain ciphered and hidden data securely without the need to exchange secret keys between the two ends of the communication. In this paper, a hiding algorithm based on fused images and Caesar cipher with intelligent methods to strengthen the security of confidential information is proposed. Firstly, fused image scattering is obtained using 1's complement and circularly shifting the bits of fused pixels by specified positions before the hiding process. Secondly, the keys for the Caesar cipher are derived from the length of secret information according to the mathematical equation. Thirdly, strengthen the security of Caesar's cipher by taking a 1's complement of each letter in the cipher data. The results guarantee the security of the presented algorithm.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Huda Hussein Abed

Department of Communication Techniques Engineering, Engineering Technical College-Najaf, Al-Furat

Al-Awsat Technical University

Najaf, Iraq

Email: eng.huda2020@atu.edu.iq

1. INTRODUCTION

Due to the open nature of the internet, users face the danger of having their private information intercepted or distorted while taking advantage of the convenient electronic information exchange made possible by highly evolved internet and information technology. Thus, it is crucial to create secure communication methods [1]. The most important methods for information security are ciphering and information hiding [2]. Ciphering is a method for encoding and manipulating private data so that only authorized users may access or use it [3]. The science of information hiding is called steganography [4]. It is done by obscuring the existence of the information by blending it into other data [5]. A variety of digital mediums, such as image, video, audio, and text, can be utilized to conceal sensitive information [6], [7]. The information hiding idea is illustrated in Figure 1.

The vast majority of currently used methods to conceal information rely on image hiding algorithm. This method principally meets the imperceptibility criteria of hiding algorithm by making the little modifications made to the image imperceptible to the human visual system. Some of the image hiding algorithms used are spatial domain method, where the secret information is directly embedded in the pixel intensity, such as least significant bit technique, and another method of the image hiding algorithms is transform domain, where the secret information is concealed in the frequency domain of an earlier transformed image [8].

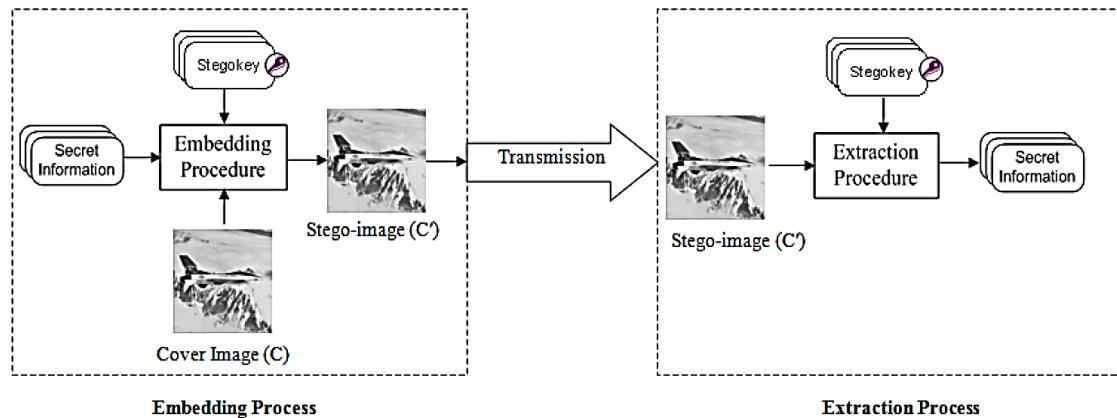


Figure 1. Depicts the information hiding idea [9]

The major problem of data concealing strategies is to include the most information possible while maintaining the image's quality, security, and method resilience to electronic attacks by hackers. Due to the vast number of available digital images on the web and the ease with which the images are used in a hiding process, several schemes have been proposed to hide data in images. Researchers have made an effort to create contemporary strategies to deal with the rapid evolution of hiding techniques [10].

Abdur *et al.* [11] described a hybrid security method that combines watermarking, steganography, and encryption. It consists of three essential parts: firstly, the secret image is ciphered utilizing the secret key. Secondly, the encrypted image embedded into the cover image utilizing the least significant bit (LSB) method to obtain the stego-image. Thirdly, the ownership of the stego-image has been ensured by using watermarking in spatial and frequency domains, respectively. Their suggested method offers great security against threats and assaults. Lotlikar [12] proposed data hiding method-based cryptography algorithms. The primary goal of their proposed method is to offer a safe means of sending and receiving sensitive and significant data between users in the form of images.

Susanto *et al.* [13] proposed a method for combination two security techniques, steganography and cryptography. The steganography technique is based on LSB that has benefits in data embedding capability and secret data imperceptibility. Since the LSB approach is so straightforward and predictable, additional encryption techniques are used to increase communication security. The secret data is encrypted using hybrid Beaufort Vigenere (HBV) before embedding it. HBV encryption is a combination of Vigenère cipher and Beaufort algorithm in order to increase data security.

Alabaichi *et al.* [14] proposed an image steganography utilizing LSB and secret map approaches that performs by applying 3D Chebyshev and 3D logistic maps in order to achieve excellent security. The proposed method is based on the idea of performing random embedding and choosing a pixel from the cover image. The suggested approach is thoroughly assessed using a variety of metrics, including correlation coefficient, homogeneity, information entropy, histogram, concealing capacity, key sensitivity, peak signal-to-noise ratio (PSNR), mean square error (MSE), and image fidelity. As a result, their proposed method effectively conceals sensitive information while maintaining a stego-image with high visual quality.

Almayyahi *et al.* [15] focused on creating a safe technique for concealing information in images using LSB. The Huffman algorithm is used to compress the secret message before it is moved on to the embedding step. Exclusive-NOR (XNOR) operation and the Fibonacci algorithm are then used to choose which pixels to insert secret information. These procedures lead to the creation of a stego-image with two secret keys. The evaluation step of their proposed method demonstrates both the rising security and imperceptibility.

Almazaydeh [8] presented an image steganographic method utilizing a canny edge detector that depends on embedding the private message bits using variable LSB length of one channel from the red, green, and blue (RGB) cover image. The blue channel was chosen because a steganography-based study revealed that blue color intensity is seen visually as being less distinct than red and green colors. Private bits are hidden up to four LSB bits which are chosen using a random number generator.

Ogundokun and Abikoye [16] proposed a modified LSB approach capable of concealing and preserving medical data in order to address the essential authentication problem. Their proposed method employed a logical bit shift operation. Their suggested protected medical information system was shown to be effective in concealing medical data and producing undetected stego-image.

An image steganography technique-based Alpha blending is proposed in [17] by utilizing Haar discrete wavelet transform (DWT). DWT is utilized for both the cover image and the secret image. The secret image is ciphered first and then fused to create the stego-image.

Nezami *et al.* [18] suggested a method that employs the hash function for steganography, and the Caesar cipher and Vigenère to encrypt the message before the hiding process. The proposed approach uses a cover image in the spatial to hide encrypted data. Comparing the suggested method to the conventional LSB steganography methodologies, security and speed are improved.

This paper introduces security procedures for confidential information by combining ciphering and information hiding techniques. Confidential information is ciphered using Caesar cipher with an intelligent method to generate Caesar key by deriving it from the length of confidential information according to a mathematical equation. Thus, the Caesar key exchange between the two ends of the connection is not required.

After that, a 1's complement is taken for each character in the encoding data to provide a second level of security, then the 1's complementary form is hidden using an information hiding technique in the spatial domain with intelligent methods for creating the medium of hiding technique. The hiding medium is created by fusing two images, then scattering the resultant fused image by 1's complement and circularly shifting the bits of fused pixels with specified positions before the hiding process. Thus, the security of the spatial domain pixels is reinforced.

The paper is categorized into the following categories: section 2 introduces the principle of Caesar cipher and fused image. In section 3, details of the proposed algorithm are presented. In section 4, the detailed results were summarized and discussed. Finally, section 5 is considered to be the conclusion of the paper.

2. PRINCIPLE OF CAESAR CIPHER AND FUSED IMAGE

2.1. Caesar cipher

Caesar cipher is an example of a substitution cipher, where each letter in the plaintext is changed to a letter that is moved a predetermined number of positions down the alphabet. Modular arithmetic is used to illustrate the encryption [19], [20]. Julius Caesar, the invention's name, is another name for the Caesar cipher [19]. For instance, if the shift was 3, A would become D, B would become E, and C would become F [21] as demonstrated in Figure 2.

One of the Caesar cipher's biggest flaws is that, even in cipher-text only scenarios, it is readily cracked. Various methods that break the text of the codes have been discovered utilizing frequency analysis and pattern words. One method is to employ brute force in order to match the frequency distribution for the letters. Because there are a finite number of shifts that might occur [22].

2.2. Fused images

Image fusion is the technique of taking the visually significant information from two or more images and merging them together to create a single fused image [23]. It is crucial that the image fusion be carried out without using any sort of final image distortion [24]. Figure 3 depicts the wavelet-based image fusion algorithm. The source images are decomposed into approximate coefficient and detailed coefficient at the necessary level utilizing DWT. The fusion rule is used to merge the approximate and detailed coefficients of both source images. By using inverse discrete wavelet transform (IDWT), the fused image is produced [25].

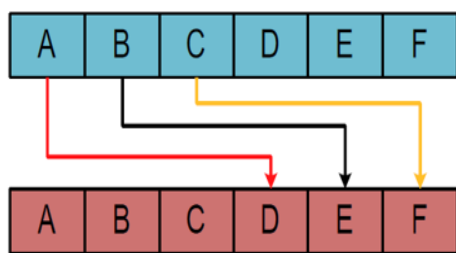


Figure 2. depicts the process of Caesar cipher [21]

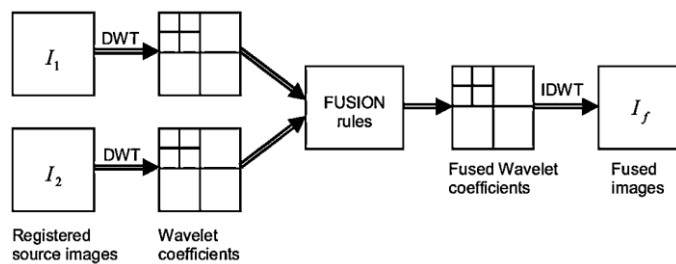


Figure 3. depicts the process of the fused image [25]

3. METHOD

The different steps employed to provide security in the proposed method are demonstrated in detail according to the following parts. Part 1 explains the detailed steps that are performed to reinforce the security of the pixels in the spatial domain before the hiding process, while the detailed steps to enhance the security of confidential data are explained in part 2. Finally, the entire proposed schemes at the sending and receiving ends, respectively, are shown in Figures 4 and 5.

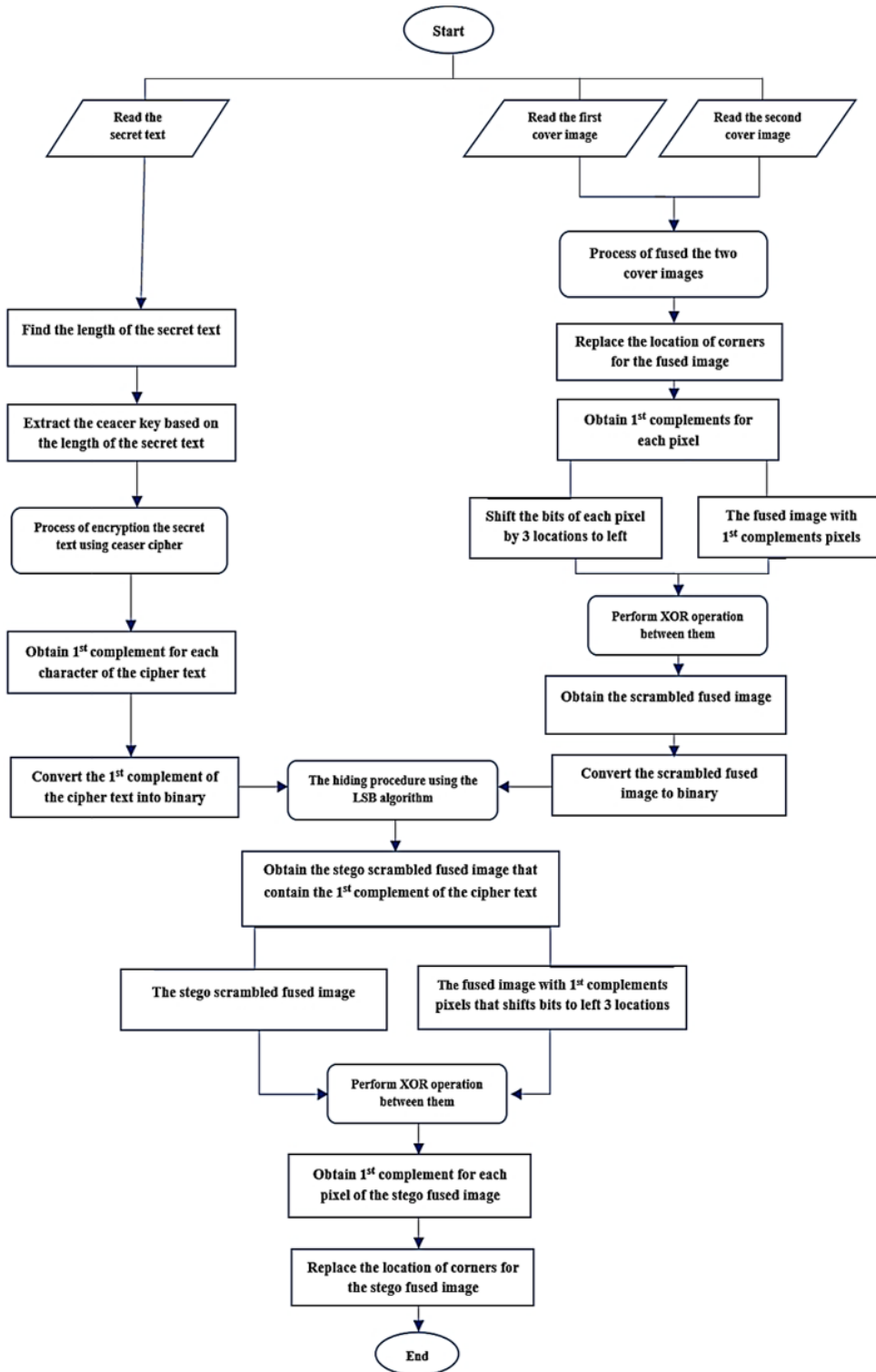


Figure 4. The steps employed for the sending part

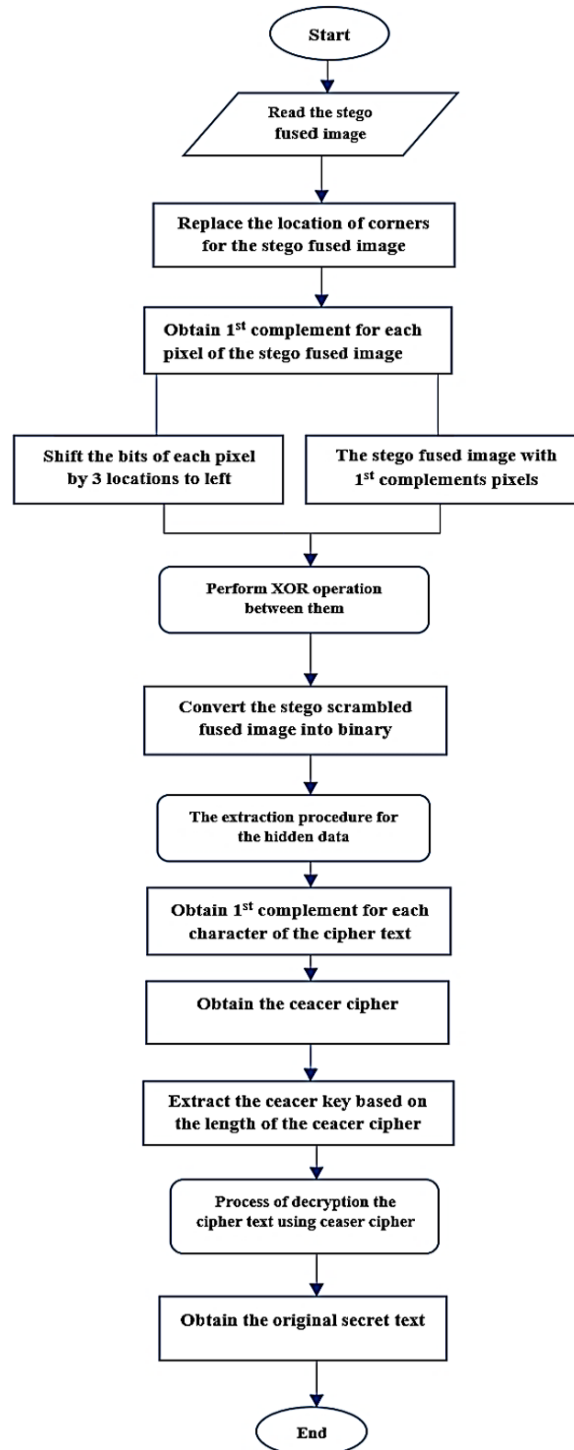


Figure 5. The steps employed for the receiving part

Part 1: the steps of the security procedure for creating the medium of hiding are explained as:

- Fuse two cover images of the same size after reading them to create a fused image.
- The positions of pixels for the fused image are shifted circularly by half its size in each dimension. Thus, the location of the corners for the fused image is replaced.
- The 1's complements for each pixel of the fused image are obtained and saved as a complementary image. After that, the bits per pixel are shifted by 3 locations to the left and saved as a shifted image. Finally, an XOR operation is performed between the complementary image and the shifted image to create a scrambled fused image with new pixel values used to hide secret bits.

Part 2: the steps of the security procedure for confidential data before hiding are explained as:

- a) After reading the secret text, it will be encrypted using Caesar cipher with a new method of formation the Caesar key depending on the length of confidential data according to a mathematical equation.
- b) The 1's complement for each letter in the cipher data is obtained to provide a second level of security.

4. RESULTS AND DISCUSSION

The execution of the suggested algorithm is performed by using MATLAB (R2021a). Two grayscale cover images of the same size are required to observe the achievement of the algorithm in offering security for secret information. The database of the signal and image processing institute "SIPI image database" is utilized for the examination. The steps employed for the proposed scheme at the sending part are demonstrated with detailed in the following Figures. Figure 6 illustrates the steps employed for the process of fusing two cover images, the first cover image in Figure 6(a), the first cover image after applying DWT in Figure 6(b), the second cover image in Figure 6(c), the second cover image after applying DWT in Figure 6(d), the process of fusing two cover images in frequency domain in Figure 6(e), and applying IDWT for the fused images in Figure 6(f). Figure 7(a) illustrates the corner replacement of the fused images, 1's complement for the pixels in Figure 7(b) and scrambled fused images in Figure 7(c). Figure 8(a) illustrates the secret information, cipher of secret information using the Caesar algorithm in Figure 8(b), and 1's complement of Caesar cipher in Figure 8(c). Figure 9 illustrates the steps employed for the formation of a Caesar key.

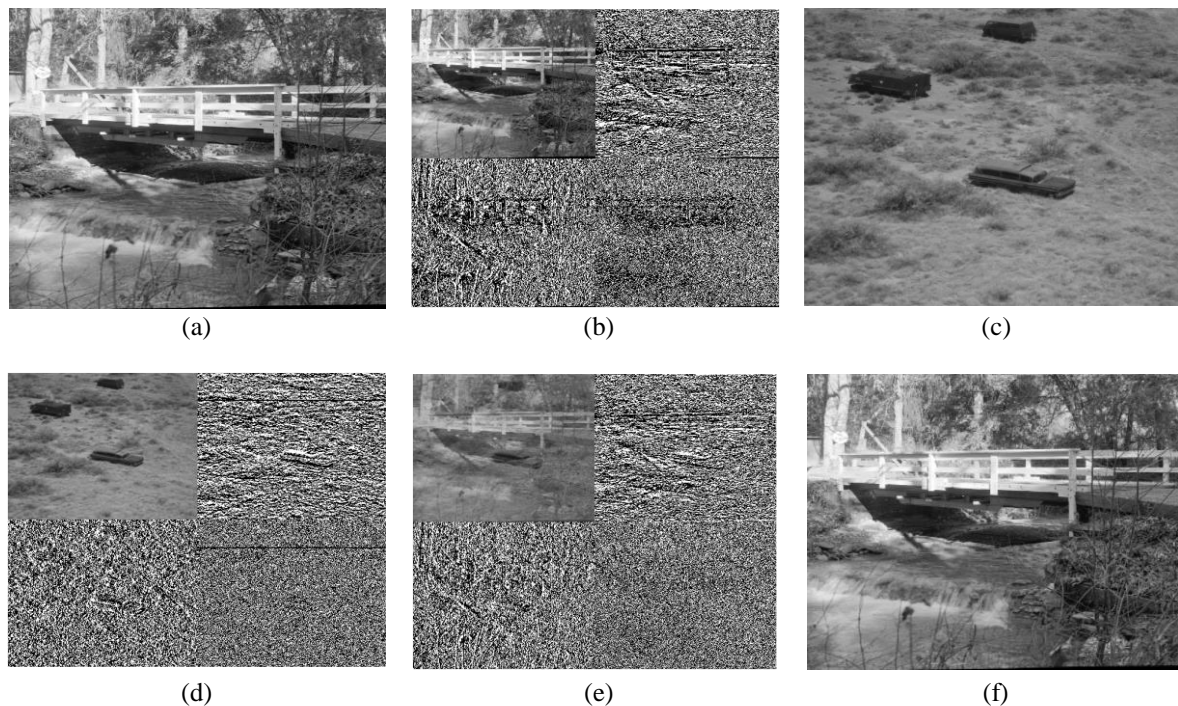


Figure 6. The steps employed for the process of fusing two cover images (a) 1st cover image, (b) decomposed 1st cover image using DWT, (c) 2nd cover image, (d) decomposed 2nd cover image using DWT, (e) fused two cover images, and (f) fused images in special domain

As illustrated in Figures 6 and 7, several security steps are performed to reinforce the security of the spatial domain pixels before the hiding process, so the attacker cannot know the pixel values utilized in the hiding process. On the other hand, two security steps are implemented to enhance the security of confidential data before the hiding process, as shown in Figures 8. In addition, the formation of the Caesar key based on the number of characters for the secret data enhances the Caesar cipher secrecy, as the exchanging process of the Caesar key between the sending and receiving parties is not required.

Table 1 shows the Caesar key for the different lengths of confidential data and the time required for the encryption and decryption processes, respectively. According to the Caesar key shown in Table 1, the key

is changed depending on the length of the confidential data, so it is possible to add data to the original secret data to obtain a different key instead of exchanging a new key between the two ends of the connection.

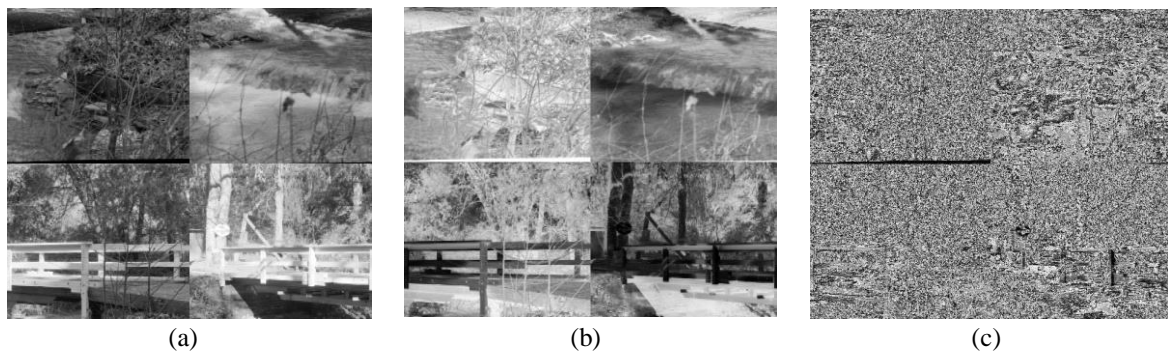


Figure 7. The steps employed for enhancing the security of fused images (a) fused images with corner replacement, (b) 1's complement for the pixels, and (c) scrambled fused images

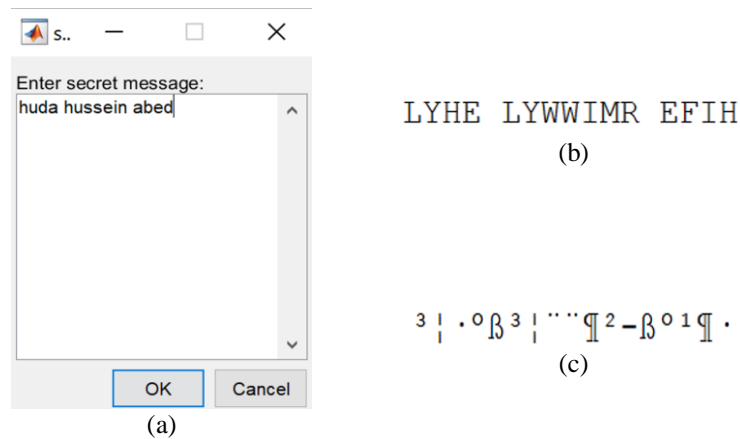


Figure 8. The steps employed for enhancing the security of secret information (a) secret information, (b) cipher of secret information using Caesar algorithm, and (c) 1's complement of Caesar cipher

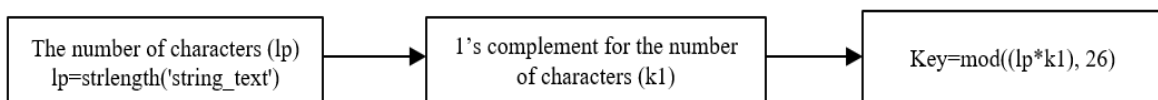


Figure 9. The formation of Caesar key

Table 1. The performance of the Caesar cipher with the formation of key

The number of characters	Caesar key	Time required for the encryption	Time required for the decryption
278 characters	8	0.002117 seconds	0.000634 seconds
626 characters	14	0.006566 seconds	0.002610 seconds
1093 characters	18	0.017665 seconds	0.000320 seconds

5. CONCLUSION




In this paper, a reliable algorithm for protecting confidential information utilizing fused images is proposed, where four levels of security are provided for the secret information. Firstly, confidential information is encrypted using Caesar cipher with a new method for the formation of the Caesar key. After that, the cipher form of encrypted data is complemented using 1's complement. That procedure enhances the security of Caesar cipher and thus provides a second level of security for secret information. A third level for

security is provided using fused two cover images, then scattering the resulting cover image by 1's complement and circularly shifting the bits of fused pixels with specified positions before the hiding process. Finally, the fourth level of security is provided by the hiding technique in the spatial domain, where the complemented form of cipher information is concealed in the scrambled fused image utilizing the LSB technique. Simulation results demonstrate that the proposed approach provides higher security for confidential information.




REFERENCES

- [1] S. Song, J. Zhang, X. Liao, J. Du, and Q. Wen, "A novel secure communication protocol combining steganography and cryptography," *Procedia Engineering*, vol. 15, pp. 2767–2772, 2011, doi: 10.1016/j.proeng.2011.08.521.
- [2] A. A. AL-Shaaby and T. AlKharobi, "Cryptography and steganography: New approach," *Transactions on Networks and Communications*, vol. 5, no. 6, Dec. 2017, doi: 10.14738/tnc.56.3914.
- [3] E. Agrawal and J. Jain, "A review on various methods of cryptography for cyber security," *International Journal on Recent and Innovation Trends in Computing and Communication (IJRITCC)*, vol. 6, no. 7, 2018.
- [4] E. Zinaly and A. Naghipour, "Audio steganography to protect the confidential information: A survey," *International Journal of Computer Applications*, vol. 169, no. 1, pp. 22–29, Jul. 2017, doi: 10.5120/ijca2017914561.
- [5] M. Begum and M. S. Uddin, "Digital image watermarking techniques: a review," *Information*, vol. 11, no. 2, Feb. 2020, doi: 10.3390/info11020110.
- [6] M. Hassaballah, M. A. Hameed, and M. H. Alkinani, "Introduction to digital image steganography," in *Digital Media Steganography*, Elsevier, 2020, pp. 1–15.
- [7] A. Rehman, T. Saba, T. Mahmood, Z. Mehmood, M. Shah, and A. Anjum, "Data hiding technique in steganography for information security using number theory," *Journal of Information Science*, vol. 45, no. 6, pp. 767–778, Dec. 2019, doi: 10.1177/0165551518816303.
- [8] L. Almazaydeh, "Secure RGB image steganography based on modified LSB substitution," *International Journal of Embedded Systems*, vol. 12, no. 4, 2020, doi: 10.1504/IJES.2020.107644.
- [9] S. Atawneh and P. Sumari, "Hybrid and blind steganographic method for digital images based on DWT and chaotic map," *Journal of Communications*, vol. 8, no. 11, pp. 690–699, 2013, doi: 10.12720/jcm.8.11.690-699.
- [10] Z. S. Younus and M. K. Hussain, "Image steganography using exploiting modification direction for compressed encrypted data," *Journal of King Saud University-Computer and Information Sciences*, vol. 34, no. 6, pp. 2951–2963, Jun. 2022, doi: 10.1016/j.jksuci.2019.04.008.
- [11] M. Abdur, R. Ahmed, M. Adnan, and A. Ahmed, "Digital image security: fusion of encryption, steganography and watermarking," *International Journal of Advanced Computer Science and Applications*, vol. 8, no. 5, 2017, doi: 10.14569/IJACSA.2017.080528.
- [12] S. Lotlikar, "Image steganography and cryptography using three level password security," *International Journal for Research in Applied Science and Engineering Technology*, vol. V, no. IV, pp. 1370–1374, Apr. 2017, doi: 10.22214/ijraset.2017.4244.
- [13] 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*, vol. 1201, no. 1, May 2019, doi: 10.1088/1742-6596/1201/1/012024.
- [14] A. Alabaichi, M. A. A. K. Al-Dabbas, and A. Salih, "Image steganography using least significant bit and secret map techniques," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 10, no. 1, pp. 935–946, Feb. 2020, doi: 10.11591/ijece.v10i1.pp935-946.
- [15] A. A. Almayyahi, R. Sulaiman, F. Qamar, and A. Essa, "High-security image steganography technique using XOR operation and fibonacci algorithm," *International Journal of Advanced Computer Science and Applications*, vol. 11, no. 10, 2020, doi: 10.14569/IJACSA.2020.0111064.
- [16] R. O. Ogundokun and O. C. Abikoye, "A safe and secured medical textual information using an improved LSB image steganography," *International Journal of Digital Multimedia Broadcasting*, pp. 1–8, Mar. 2021, doi: 10.1155/2021/8827055.
- [17] S. S. Tevaramani and R. J., "Image steganography performance analysis using discrete wavelet transform and alpha blending for secure communication," *Global Transitions Proceedings*, vol. 3, no. 1, pp. 208–214, Jun. 2022, doi: 10.1016/j.gltip.2022.03.024.
- [18] Z. I. Nezami, H. Ali, M. Asif, H. Aljuaid, I. Hamid, and Z. Ali, "An efficient and secure technique for image steganography using a hash function," *PeerJ Computer Science*, vol. 8, Nov. 2022, doi: 10.7717/peerj-cs.1157.
- [19] B. Purnama and A. H. H. Rohayani, "A new modified Caesar cipher cryptography method with Legible Ciphertext from a message to be encrypted," *Procedia Computer Science*, vol. 59, pp. 195–204, 2015, doi: 10.1016/j.procs.2015.07.552.
- [20] G. N. Salmi and F. Siagian, "Implementation of the data encryption using Caesar cipher and Vernam cipher methods based on CrypTool2," *Journal of Soft Computing Exploration*, vol. 3, no. 2, Sep. 2022, doi: 10.52465/josce.v3i2.86.
- [21] Y. N. A. Taher, K. A. Ameen, and A. M. Fakhrudeen, "An efficient hybrid technique for message encryption using Caesar cipher and deoxyribonucleic acid steganography," *Indonesian Journal of Electrical Engineering and Computer Science (IJECS)*, vol. 28, no. 2, pp. 1096–1104, Nov. 2022, doi: 10.11591/ijeecs.v28.i2.pp1096-1104.
- [22] A. Jain, R. Dedhia, and A. Patil, "Enhancing the security of Caesar cipher substitution method using a randomized approach for more secure communication," *International Journal of Computer Applications*, vol. 129, no. 13, pp. 6–11, Nov. 2015, doi: 10.5120/ijca2015907062.
- [23] S. Jadhav, "Image fusion based on wavelet transform," *International Journal of Engineering Research*, vol. 3, no. 7, pp. 442–445, Jul. 2014, doi: 10.17950/ijer/v3s7/707.
- [24] H. A. H. Mahmoud, "A novel image fusion scheme using wavelet transform for concealed weapon detection," *International Journal of Advanced Computer Science and Applications*, vol. 11, no. 2, 2020, doi: 10.14569/IJACSA.2020.0110239.
- [25] V. Naidu and J. Raol, "Pixel-level image fusion using wavelets and principal component analysis," *Defence Science Journal*, vol. 58, no. 3, pp. 338–352, May 2008, doi: 10.14429/dsj.58.1653.




BIOGRAPHIES OF AUTHORS

Huda Hussein Abed    Assistant Lecturer at Communication Techniques Engineering Department, Engineering Technical College-Najaf, AL-Furat Al-Awsat Technical University. She received Bachelor's and master's degrees in Communication Techniques from Engineering Technical College-Najaf, AL-Furat Al-Awsat Technical University, Iraq in 2010 and 2019, respectively. Her current research interests include communication security, digital image processing, steganography, and digital communication. She can be contacted at email: eng.huda2020@atu.edu.iq.



Aqeel Sajjad Shaeel    works at Laser and Optoelectronics Tech. Eng. Department, Engineering Technical College-Najaf, AL-Furat Al-Awsat Technical University. He received the B.Sc. in Electrical Engineering from University of Babylon. He received a M.Sc. in communication engineering from Amirkabir University of Technology. His research interests include LEO Satellite, information security, IoT, digital communication. He can be contacted at email: aqeelsajjad1@gmail.com.



Ruaa Shallal Abbas Anzoze    received her Bachelor of Communication Technical Engineering from Engineering Technical Collage-Najaf, Iraq, in 2006, and her M.Tech. of Communication System Engineering in the Department of Electronics and Communication Engineering in SHIATS, Allahabad, India, in 2014. She is currently a Ph.D. student at Tabriz university. Her area of interest includes digital signal processing, beam and channel estimation, and Antennas Design. She can be contacted at email: coj.rua@atu.edu.iq.