Hybrid information security system via combination of compression, cryptography, and image steganography

Wid Akeel Awadh[1], Ali Salah Alasady[2], Alaa Khalaf Hamoud[1]
[1]Department of Computer Information Systems, University of Basrah, Basrah, Iraq
[2]Department of Computer Science, University of Basrah, Basrah, Iraq

Article Info

Article history:

Received Aug 22, 2021
Revised Jun 21, 2022
Accepted Jul 15, 2022

Keywords:

Compression
Cryptography
Image steganography
Information security
Peak signal to noise ratio
Structural index similarity

ABSTRACT

Today, the world is experiencing a new paradigm characterized by dynamism and rapid change due to revolutions that have gone through information and digital communication technologies, this raised many security and capacity concerns about information security transmitted via the Internet network. Cryptography and steganography are two of the most extensively that are used to ensure information security. Those techniques alone are not suitable for high security of information, so in this paper, we proposed a new system was proposed of hiding information within the image to optimize security and capacity. This system provides a sequence of steps by compressing the secret image using discrete wavelet transform (DWT) algorithm, then using the advanced encryption standard (AES) algorithm for encryption compressed data. The least significant bit (LSB) technique has been applied to hide the encrypted data. The results show that the proposed system is able to optimize the stego-image quality (PSNR value of 47.8 dB) and structural similarity index (SSIM value of 0.92). In addition, the results of the experiment proved that the combination of techniques maintains stego-image quality by 68%, improves system performance by 44%, and increases the size of secret data compared to using each technique alone. This study may contribute to solving the problem of the security and capacity of information when sent over the internet.

Corresponding Author:

Wid Akeel Awadh
Department of Computer Information Systems, University of Basrah
Basrah, Iraq
Email: wid.jawad@uobasrah.edu.iq

1. INTRODUCTION

Today, with the rapid growth of the Internet, the usage of digital communication as a means of exchanging data is also on the rise. The security and integrity of data communicated over the internet network are one of the most serious issues in digital communication. Therefore, researchers are trying to get new and updated solutions and techniques to secure sensitive data being sent and received over the internet without any hacking or disclosure by hackers [1]. To provide security and integrity to users in protecting their information from unauthorized people, in this paper, we discuss the most widely utilized data security techniques are cryptography and steganography [2], [3].

Cryptography is the science of hiding information to keep it secret from unauthorized people [2]. In the past, this technology was limited to the encryption and decryption of messages exchanged using secret keys, but today, three different techniques are used, namely: symmetric key encryption, asymmetric key encryption, and hashing [4], [5]. The information to be hidden is commonly called “plain text” and the process of hiding it is called “encryption”. The original encrypted text is called “cipher text”, and the set of rules used in encrypting the original text is called “encryption algorithm”. The encryption typically relies on an “encryption key,” which is the input to the algorithm and the message. To obtain the message from the encrypted text, the recipient must have a “decryption algorithm” that uses a suitable “decryption key” to obtain the original text [6]. Any encryption system has specific security conditions, which are authentication, privacy and confidentiality, and integrity [7]. Advanced encryption standard (AES) [8], data encryption standard (DES) [9], Rivest cipher 4 (RC4) [10], Rivest–Shamir–Adleman (RSA) [11], and other cryptographic algorithms are among the most widely used today.

Meanwhile, steganography is a method of hiding secret data using a cover image in a way that does not invite suspicion or draw attention and is not understood by intruders and attackers. Thus, confidential information is not available to network users, but its content remains preserved for relevant authorities that are familiar with how to extract this content [12]. The stego-system can hide the secret information into the cover media using certain algorithms. A secret message may be an image, text, audio, video or anything that can be represented in the form of bits [13]. After the secret data are embedded in the cover image, also called a stego-object, sending to the receiver begins by selecting the suitable channel where the decoder system is used with the same stego-method for obtaining original information from the sender [14]. Steganography techniques such as least significant bit (LSB) are widely used, which are frequently applied in various studies. In order to decrease the storage space, speed up the transfer of files and reduce storage hardware and network bandwidth costs, images can be compressed. So, when we combine cryptography and steganography, we will have a double layer of security.

Compression is the technique of reducing the number of bits required to represent the data with the same or a little less (accepted) accuracy [15]. There are 2 types of compression: lossy and lossless compression [16]. Lossy compression is those in which there is a loss of fidelity for natural images like photographs [17]. There are various lossy compression methods like transform coding [18], discrete cosine transform (DCT) [19], discrete wavelet transforms (DWT) [20], chroma subsampling [21], fractals lossless compression is generally used for medical imaging, drawings, comics. There are various methods for lossless compression like run-length coding, predictive coding, entropy coding, Huffman coding, Lempel Ziv Welch (LZW) [16], [22], [23]. So, DWT technique is applied for image compression. It supports all types of images like joint photographic experts group (JPEG), Bitmap (BMP), and portable network graphics (PNG). DWT is effective and robust in its set of images. It is best suited to time-limited data [24].

The objective of this study is to suggest a hybrid security system for ensuring data security and resolving the problem of the capacity of data exchanged over the internet, using an intelligent mix of algorithms to hide a sensitive image inside another one. This system includes three layers: The first layer aims to reduce the size of the embedded data by compression before encryption using the DWT algorithm. The second layer is cryptography, which uses an AES algorithm that requires an agreed-upon secret key for encryption and decryption (symmetric key encryption) between the sender and the receiver, to encrypt the secret image and convert it into a cipher image. In the third layer, the encrypted image is hidden using LSB steganography to obtain a stego-image output file. Figure 1 illustrates the overview of the proposed system steps.

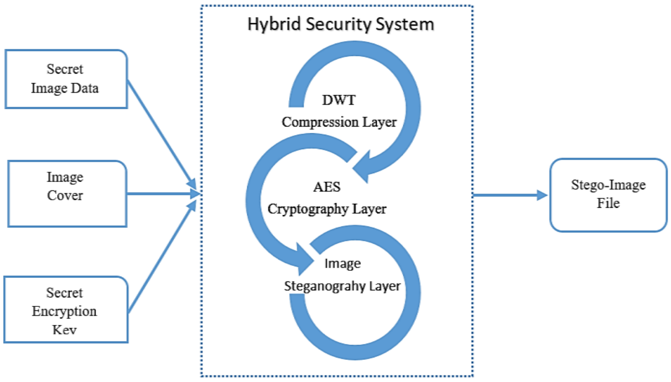


Figure 1. Steps of the proposed system

The following are the major contributions made by this paper: i) introduce a hybrid security system that provides high security, capacity, and image quality; ii) reduce physical space on different storage media, when compression algorithm has been used; and iii) determine the AES algorithm that is used to encrypt secret data as an additional layer before LSB steganography layer, LSB algorithm was used to increase the security of the system against trackers' attempts to detect which data to hide. In this way, the stego-images quality is improved, as well as making it more difficult to retrieve the secret data.

The rest of the paper is divided into six sections. Following the introduction, section 2 discusses the related work. Section 3 describes the proposed system, which includes details about the embedding phase and extraction phase. While section 4 defines the method. Section 5 explains the results obtained and the last section provides a conclusion and future works.

2. RELATED WORK

Numerous works can be used to secure data using image steganography, incorporating cryptography and steganography. In this section, we carefully review several methods that are related to our approach. Arroyo *et al.* [25] suggested a method for securing sensitive text data that combined cryptography, compression, and steganography. According to the results, combining the methods outperforms utilizing solely the LSB steganography technique. Following that, Wahab *et al.* [26] proposed using a combination of RSA and Huffman coding, Run-length encoding (RLE), or DWT to compress and secure messages to produce a high-quality stego-image. The results of the experiments show that the proposed module has a higher quality and storage capacity than other strategies.

Arroyo and Delima [27] introduced a new approach to hiding data. Simulation results revealed that the combination of the two methods had paved the way to more secure storage and data transmission. Arroyo *et al.* [28] developed a strategy for improving information security by introducing multiple levels of security processes, such as encryption, compression, and steganography. The proposed method differs from the simple LSB method in that it not only overcomes the security and payload capacity issues but also enhances the stego-image quality.

Chawan [29] presented a novel that included a variety of steganography techniques. There are three methods are used. The first is an encryption method that ensures the security of the hidden message. The second is a technique that compresses data to reduce the sensitive data's occupational capacity. The third is a technique that hides the sensitive data in the cover image to produce a stego-image. The stego-image’s quality can be considerably improved with this strategy while incurring minimal additional processing cost. The worst MSE is calculated between the stego-image and the cover image. Hamza *et al.* [30] proposed a technique in which the compressed and encrypted secret data bits are divided into pairs of two bits and pixels of the cover image are also arranged in four pairs. The four pairs of secret data are compared to the four pairs of each cover pixel, yielding sixteen matching possibilities. This technique improves the security of the stego-image and embedding capacity. Table 1 provides a summary of methods used in related work. Data security can be improved by using numerous measures at once. Incorporation, on the other hand, will increase computation time, necessitating the use of a correct merging mechanism.

Table 1. A summary of methods used in related work

Research	Compression	Cryptography	Steganography
[25]	Huffman Coding	Polybius Cipher	LSB
[26]	Huffman or DWT	RSA	LSB
[27]	Goldbach code	----	LSB
[28]	Huffman coding	Vigenère cipher	LSB
[29]	LZW	AES	knight tour algorithm
[30]	LZW	AES	LSB

3. THE PROPOSED SYSTEM

Data security and capacity are the most critical factors to consider when transmitting sensitive data via the Internet, to prevent attackers from stealing data and accessing it for a specific purpose. Therefore, in this study, we propose a hybrid system to hide a secret image in another one. This system applies three algorithms: DWT compression algorithm, AES cryptography algorithm, and LSB steganography algorithm to improve data security and capacity. Figure 2 illustrates the hybrid system architecture of the proposed method. The proposed method includes two main phases of embedding and extraction.

3.1. Embedding phase

This phase entails all of the activities that must be completed to hide and secure the secret image inside the cover image. The sender compresses the secret image using the DWT algorithm and encrypts the compressed image using AES algorithms so that ciphered bits are generated before embedding these bits into the cover image using the LSB algorithm. Stego-images can be transferred to the receiver through the internet.

3.2. Extraction phase

In the extraction phase, to recover the secret image, the cipher image will be extracted from the stego-image. Following that, the ciphered data is then decrypted using the AES method using the same key used in the encryption process. Finally, the secret image is decompressed using the DWT algorithm.

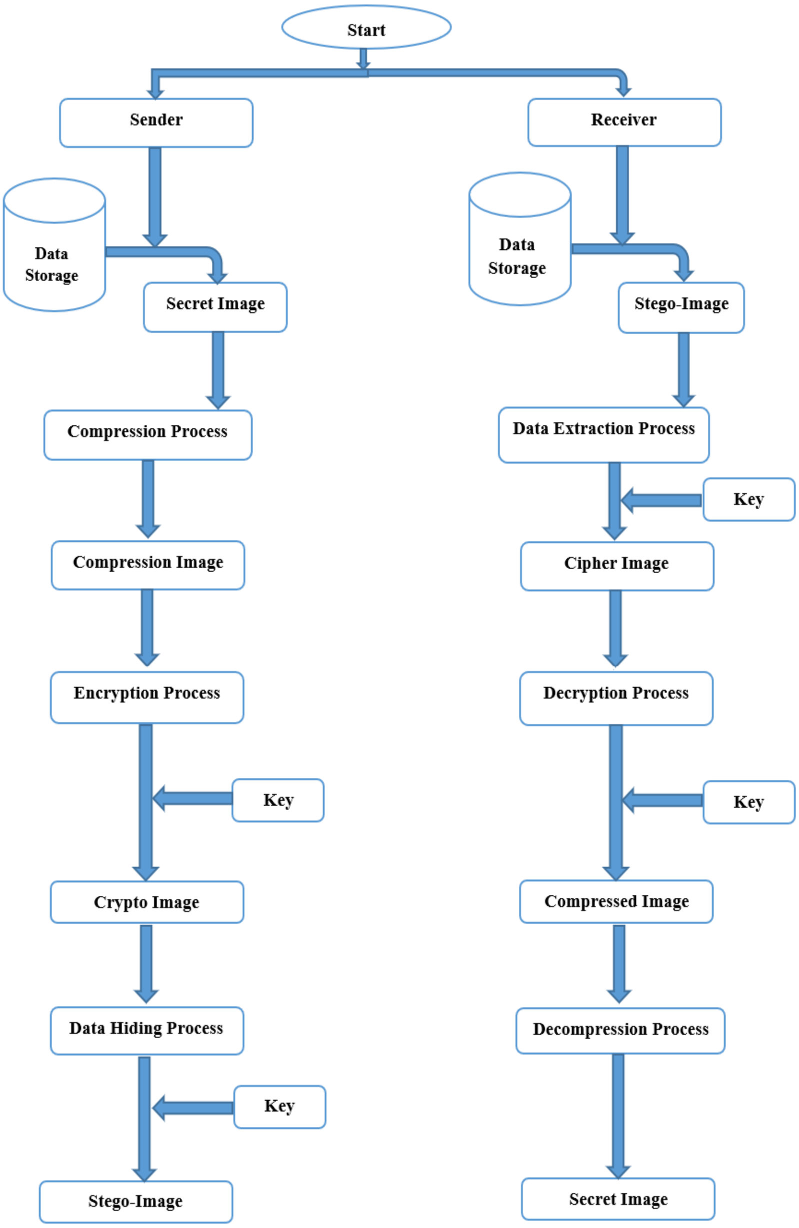


Figure 2. The hybrid security system architecture of the proposed method

4. METHOD

4.1. Technology detail

4.1.1. Discrete wavelet transform

In DWT, the wavelets are sampled discretely. The main benefit of having a DWT is its provision of a temporal resolution because of its Fourier transforms. DWT is used to collect (in time) frequency and location information [31]. Wavelets are local signals in scale and time that have irregular shapes, and several forms with an average value of zero. Wavelets integrate to zero and oscillate up and down along the axis. Several wavelets show a property ideal that is suitable for a compact signal presentation that resides orthogonally, guaranteeing that information is not over-represented. The signal is decomposed into shifted and scaled representations or components of the actual wavelets by using a wavelet transform. The wavelets coefficients are reduced to remove a few specifics until the decomposition is completed [16]. One of the benefits of using DWT is its ability to distinguish small details in a signal. Thus, small wavelets may be employed to detect very small features in a signal, whilst large wavelets can recognize coarse details. Several different wavelets can be used (such as HAAR, DAUBECHIES), and thus DWT is most suitable for image compression and produces a signal representation that is sparser than other types of techniques [32].

4.1.2. Advanced encryption standard

Rijndael is a symmetric block cipher algorithm that has been chosen as the AES by the National Institute of Standards and Technology (NIST) [33]. This technique is used as a replacement for the data encryption standard (DES). As a part of the encryption, AES uses a single key that may have a length of 128, 192, or 256 bits [34]. In AES, the same key is used for both encryption and decryption and is therefore called an asymmetric encryption algorithm. By comparison, asymmetric encryption algorithms use two different keys, public and private. An encryption key is simply a binary data string used in the encryption [35]. The important matter is to keep the encryption key confidential when using the same one to encrypt and decrypt the information and to use keys that are difficult to guess. Several keys can be created by programs that have been used for this particular task, and another way is to derive the keys from the passphrase. Good encryption systems never use a single passphrase as the encryption key [36].

4.1.3. Least significant bit steganography

LSB is a simple stenographic algorithm widely used to embed the secret image within an image cover. Pixels of cover Image and secret image can be converted to binary form. The LSB of the cover image is substituted with one bit of secret image. When the secret image has been embedded in the cover image, the result of the hiding is called a stego-image [37]. Standard operations involving LSB schemes can be explained mathematically, as [38]. Suppose (C) is a cover image used to hide sensitive information. The size of the cover image (C) is [X*Y] pixels, with each pixel equal to 24-bit value to store 8 bits on the values of color red, green, and blue (RGB), as defined in (1).

$$C = \{cij \,|0 \le i \le X, 0 \le Y, cij \, \epsilon \{ 0,1,2, \dots, 255 \} \tag{1}$$

The secret image (M) can be hidden in each pixel of the cover image (C) by processing the (K-LSB). The noise observed after embedding is proportional to the value of (k), as defined in (2).

$$S'_i = \sum_{j=0}^{nk-1} s_{i*k+j} * 2^{k-1-j} \tag{2}$$

The hiding process ends once all sensitive information is hidden in the cover image (2). If the value of (k) is increased to enhance the cover image's capability, the stego-object quality decreases and can show the presence of hidden data under the cover image.

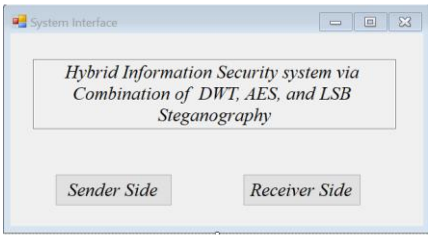
4.2. System interfaces

A Visual Basic.Net language was used to design and implement the proposed system for the security of sensitive data. This language is chosen because it offers high-performance numerical computation, data analysis, and its functions are easy to use. The goal of this implementation is to study the three-layer security system concept, as well as to test various scenarios to advance this significant academic research field. The implementation of the proposed system interface can be observed in Figure 3. Running the system implementation begins with the system interface that guides the user through asking about the mechanism that the user should select, i.e. Sender Side or Receiver side.

If Sender Side is selected, then the module performs the following procedure, as shown in Figure 4:

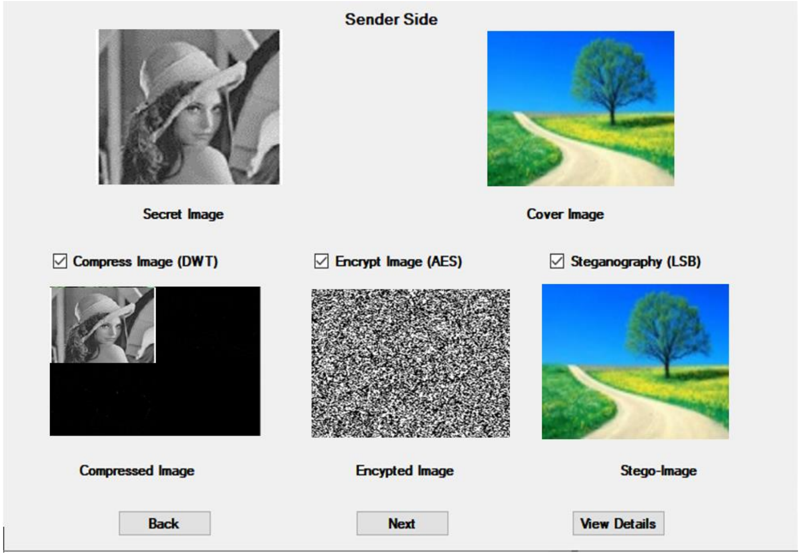
- Step 1: select a cover image as a stego-image.
- Step 2: select a secret image as an original image.
- Step 3: as the first layer, compress the secret image using the DWT algorithm by checking the “compress image (DWT)” checkbox, view the compressed image in the compressed image area.
- Step 4: within the second layer, the program converts the compressed image into an array of binary bytes to be encrypted using AES algorithm, to implement this layer, check the “Encrypt image (AES)” checkbox, then enter the secret key to encrypt the secret data, its length 128 bits as shown in Figure 5.

- Step 5: check the “Steganography (LSB)” checkbox to embed the secret image in the cover image, as the final layer of the proposed system. This layer requires converting the cover image pixels into binary form. Each pixel in the RGB cover image represents an 8-bit byte. Therefore, using the LSB image-based steganography in our original system, we could hide in each pixel 1 bits of secret data.
- Step 6: when choosing the view details, performance metrics of the experiment will appear in new window, as shown in Figure 5.



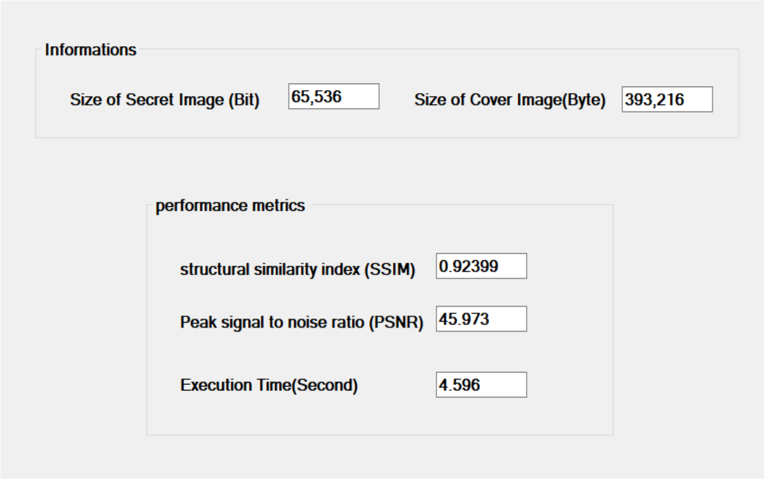
Hybrid Information Security system via Combination of DWT, AES, and LSB Steganography

Figure 3. Main system interface


Sender Side

☑ Compress Image (DWT) ☑ Encrypt Image (AES) ☑ Steganography (LSB)

Figure 4. Proposed system interface (sender side)


Informations

Size of Secret Image (Bit) 65,536 Size of Cover Image(Byte) 393,216

performance metrics

structural similarity index (SSIM) 0.92399

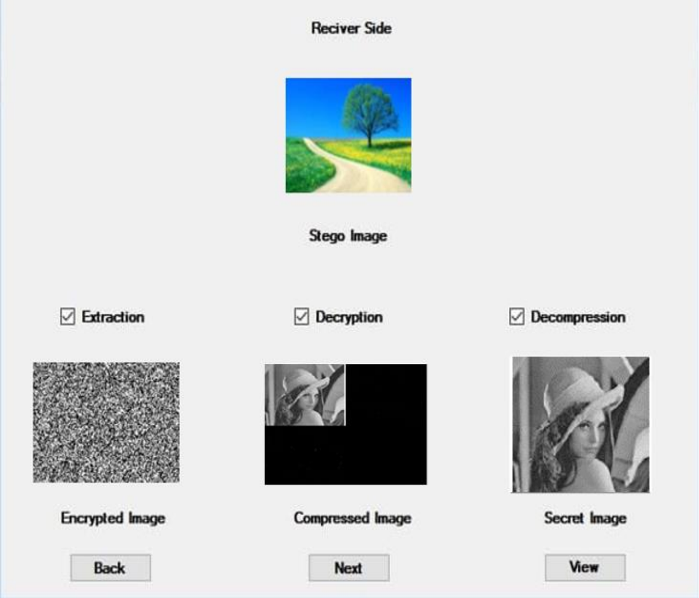
Peak signal to noise ratio (PSNR) 45.973

Execution Time(Second) 4.596

Figure 5. Information of performance metrics of experiment

If Receiver Side is selected, then the module performs the following procedure, as shown in Figure 6.

- Step 1: select a stego-image.
- Step 2: click "Extraction" to extract the encrypted data from the cover image and show it in the encrypted image area.
- Step 3: click "Decryption" check box. Using the same secret key in the encryption process, view the compressed image.
- Step 4: click "Decompression" check box to obtain the secret image, view the original image in the secret image area.



☑ Extraction ☑ Decryption ☑ Decompression

Figure 6. Proposed system interface (receiver side)

5. RESULTS AND DISCUSSION

In the proposed method, the secret image is compressed and encrypted and then hidden within cover images, as described previously, to be analyzed and compared. To make this explication clearer, we chose 40 differently sized cover images and compared the performance metrics after doing a series of experiments. In this paper, we employed the following performance metrics:

Structural index similarity (SSIM) is a metric for determining how similar two images are. The higher the value, the better. This criterion compares the quality of a given image to a distortion-free reference image. When it comes to image steganography. The stego-image is being inspected, while the host image is being used as a reference. In the context of image steganography. the examined image is the stego-image, and the host image is considered as the reference image. This criterion is calculated using (3):

$$SSIM\ (C,S) = \frac{(2\mu c\mu s+C1)(2\sigma cs+C2)}{(\mu^2 c+\ \mu^2 s+C1)(\sigma^2 c+\ \sigma^2 c+C2)} \tag{3}$$

where c1 and c2 are two variables that help to stabilize the division when the denominator is weak. Furthermore, and show the variables' average and covariance.

Peak signal-to-noise ratio (PSNR) is defined as the ratio of the signal's greatest value to the magnitude of the noise that affects it. It is calculated using (4).

$$PSNR = 10.Log_{10}\left(\frac{Max_I^2}{MSE}\right) \tag{4}$$

The PSNR is used to calculate the difference in quality between the cover image and the stego-image [39]. A greater PSNR indicates that the PSNR is better. The proposed method's performance was evaluated using the performance metrics: PSNR and SSIM, to hide secret images. Table 2 presents the results of performance metrics of implementing this proposed method on the 40 images. Table 2 results are represented graphically in Figures 7 and 8. Performance analysis for the proposed method in Figure 7 shows that the PSNR is generally similar, with an average of 47.8 dB. The average value shows that the stego-image's quality is still in the good category. In general, if the PSNR value is more than 30 dB, it is nearly hard for human eyes to identify the visual quality distortion in the stego-image. The high PSNR values imply a well-hidden image with negligible noise effect during the process, which we can confirm using LSB. The SSIM values based on our suggested approach are also measured for the steg-image. As shown in Figure 8, the average value of SSIM was found to be 0.92. In other words, high SSIM values indicate that the method generated minimal modifications in stego-images.

Table 2. Results of performance metrics using the proposed method

Stego-Image	PSNR	SSIM	Stego-Image	PSNR	SSIM
Image1.jpg	45.973	0.92567	Image21.jpg	49.366	0.92143
Image2.jpg	50.01	0.91216	Image22.jpg	48.783	0.92684
Image3.jpg	46.133	0.92243	Image23.jpg	50.265	0.91873
Image4.jpg	48.959	0.91277	Image24.jpg	49.287	0.92208
Image5.jpg	47.477	0.92118	Image25.jpg	50.979	0.91739
Image6.jpg	46.486	0.92373	Image26.jpg	46.032	0.92739
Image7.jpg	51.462	0.91168	Image27.jpg	45.873	0.92932
Image8.jpg	48.951	0.91150	Image28.jpg	44.981	0.93329
Image9.jpg	51.967	0.91047	Image29.jpg	48.648	0.92542
Image10.jpg	45.898	0.92995	Image30.jpg	45.885	0.92837
Image11.jpg	49.645	0.92714	Image31.jpg	49.537	0.92275
Image12.jpg	44.563	0.92972	Image32.jpg	46.821	0.92784
Image13.jpg	48.90	0.92701	Image33.jpg	45.890	0.92744
Image14.jpg	47.223	0.92156	Image34.jpg	44.234	0.93341
Image15.jpg	50.234	0.91874	Image35.jpg	47.637	0.92633
Image16.jpg	45.829	0.92813	Image36.jpg	45.927	0.92265
Image17.jpg	50.899	0.91784	Image37.jpg	48.289	0.92927
Image18.jpg	45.999	0.93689	Image38.jpg	46.931	0.92567
Image19.jpg	44.401	0.93148	Image39.jpg	48.836	0.92547
Image20.jpg	48.129	0.92421	Image40.jpg	49.452	0.92433

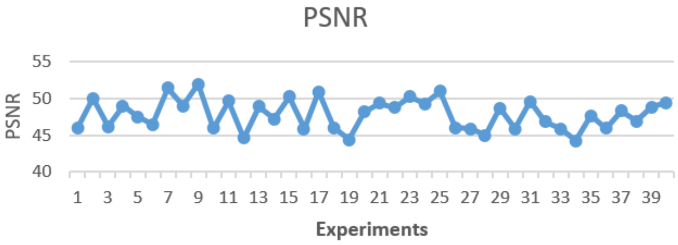


Figure 7. The PSNR value of stego-image

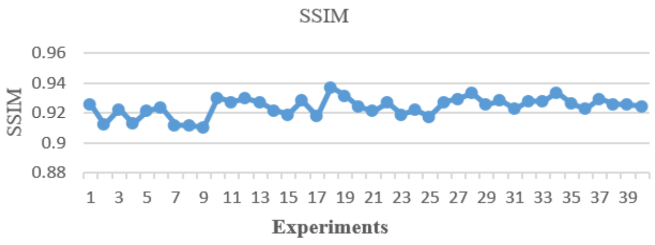


Figure 8. The SSIM value of stego-image

The implementation of the three layers (combining the compression, cryptography, and steganography techniques) sequentially and the implementation of each technique independently were also compared in this study. We compared the PSNR and execution time calculated for each test for the same secret images; the secret image used in all experiments is the standard Lena picture. Table 3 shows the performance comparison between experiments in the embedding phase. In the first experiment, the secret image was directly hidden without being compressed or encrypted, and the PSNR value was (65.4) and the execution time (6.75 seconds). Observe that, the first experiment was the worst with respect to security and performance. The secret image was hidden in the second experiment after it was compressed without encryption, and the PSNR (45.2) and execution time were recorded (5.19 seconds). Note that the second experience was better in terms of performance, and the level of security did not improve well. And in the third experiment, the secret image was hidden after encrypting it without compressing it. The value of PSNR (65.4) and the execution time was (8.09 seconds). Note that the third experience was better in terms of security, but the performance of the system is bad. After the fourth experiment implementation, we notice the proposed system consume less execution time than if the techniques of encryption and steganography are running independently and the PSNR was low compared to others because the secret data was compressed.

In general, our research has found that combining procedures of compression, encryption, and steganography methods can improve system security and its performance more than executing the algorithms independently. The results also showed that the proposed method maintains the stego-image’s quality by 68% and improves the system's performance by 44%. This fact of the system performance and security issues are getting clearer as the data in real-world applications grows.

Table 3. The performance comparison between experiments in the embedding phase

Secret Image	Compression	Encryption	Steganography	PSNR (dB)	Execution time (second)
	NO	NO	Yes	65.4	6.790
	YES	NO	YES	45.2	5.193
	NO	YES	YES	63.2	8.093
	YES	YES	YES	44.3	4.596

6. CONCLUSION AND FUTURE WORKS

This paper presented a hybrid security system for hiding secret image data within another image files, assuming high security as well as capacity. In the proposed method, a DWT algorithm was used to decrease the secret image size. An AES algorithm was used to ensure secret image security and use the LSB technique to hide secret image data in the cover image. Depending on the results of the experiments, it can be concluded that the stego-image's quality is still good, with an average PSNR of 47.8 dB and an average SSIM of 0.92. The results of the proposed method also proves that the combination of techniques enhances data security and system performance because it has hybrid layers of security.

As future work, this combined hybrid security system is to be improved by supposing the LSB of the cover image used to hiding process are randomly and evenly distributed, to be tested and compared. Also, planning is to be done to study different other ways to enhance the capacity and the security of the system for personal use with PC applications. The system can be further improved to support other languages and their features, which may need some more focused research.

REFERENCES

[1] M. Alkhudaydi and A. Gutub, "Securing data via cryptography and arabic text steganography," *SN Computer Science*, vol. 2, no. 1, Jan. 2021, doi: 10.1007/s42979-020-00438-y.

[2] N. Kheshaifaty and A. Gutub, "Preventing multiple accessing attacks via efficient integration of captcha crypto hash functions," *International Journal of Computer Science and Network Security*, vol. 20, no. 9, pp. 16–28, 2020.

[3] A. Gutub and F. Al-Shaarani, "Efficient implementation of multi-image secret hiding based on LSB and DWT steganography comparisons," *Arabian Journal for Science and Engineering*, vol. 45, no. 4, pp. 2631–2644, Apr. 2020, doi: 10.1007/s13369-020-04413-w.

[4] W. A. Awadh, A. S. Hashim, and A. K. Hamoud, "A review of various steganography techniques in cloud computing," *University of Thi-Qar Journal of Science*, vol. 7, no. 1, pp. 113–119, May 2019, doi: 10.32792/utq/utjsci/vol7/1/19.

[5] M. G. Alkhudaydi and A. A. Gutub, "Integrating light-weight cryptography with diacritics arabic text steganography improved for practical security applications," *Journal of Information Security and Cybercrimes Research*, vol. 3, no. 1, pp. 13–30, Dec. 2020, doi: 10.26735/fmit1649.

[6] A. S. S. Al-Mozani and W. A. J. Awadh, "A new text steganography method by using non-printing unicode characters and unicode system characteristics in English/Arabic documents," *Journal of Thi-Qar Science*, vol. 3, no. 3, pp. 192–200, 2012.

[7] B. Seok, J. C. S. Sicato, T. Erzhena, C. Xuan, Y. Pan, and J. H. Park, "Secure D2D communication for 5G IoT network based on lightweight cryptography," *Applied Sciences*, vol. 10, no. 1, Dec. 2019, doi: 10.3390/app10010217.

[8] B. Langenberg, H. Pham, and R. Steinwandt, "Reducing the cost of implementing the advanced encryption standard as a quantum circuit," *IEEE Transactions on Quantum Engineering*, vol. 1, pp. 1–12, 2020, doi: 10.1109/TQE.2020.2965697.

[9] B. Umapathy and D. Kalpana, "A survey ON cryptographic algorithm for data security IN cloud storage environment," *European Journal of Molecular and Clinical Medicine*, vol. 7, 2020

[10] F. Thabit, S. Alhomdy, and S. Jagtap, "A new data security algorithm for the cloud computing based on genetics techniques and logical-mathematical functions," *International Journal of Intelligent Networks*, vol. 2, pp. 18–33, 2021, doi: 10.1016/j.ijin.2021.03.001.

[11] N. A. Al-Juaid, A. A. Gutub, and E. A. Khan, "Enhancing PC data security via combining RSA cryptography and video based steganography," *Journal of Information Security and Cybercrimes Research*, 2018, doi: 10.26735/16587790.2018.006.

[12] N. A. F. Abbas, N. Abdulredha, R. K. Ibrahim, and A. H. Ali, "Security and imperceptibility improving of image steganography using pixel allocation and random function techniques," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 12, no. 1, pp. 694–705, Feb. 2022, doi: 10.11591/ijece.v12i1.pp694-705.

[13] W. A. Awadh and A. S. Hashim, "Using steganography for secure data storage in cloud computing," *International Research Journal of Engineering and Technology(IRJET)*, vol. 4, no. 4, pp. 3668–3672, 2017.

[14] X. Liao, J. Yin, M. Chen, and Z. Qin, "Adaptive payload distribution in multiple images steganography based on image texture features," *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 2, pp. 897–911, 2022, doi: 10.1109/TDSC.2020.3004708.

[15] P. V. Sundara Rajan and L. Fred A, "Efficient oppositional based optimal Harr wavelet for compound image compression using MHE," *Biomedical Research*, vol. 29, no. 10, pp. 2169–2178, 2018, doi: 10.4066/biomedicalresearch.29-18-501.

[16] D. Mody, P. Prajapati, P. Thaker, and N. Shah, "Image compression using DWT and optimization using evolutionary algorithm," *SSRN Electronic Journal*, 2020, doi: 10.2139/ssrn.3568590.

[17] F. Mentzer, L. Van Gool, and M. Tschannen, "Learning better lossless compression using lossy compression," in *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, Jun. 2020, pp. 6637–6646, doi: 10.1109/CVPR42600.2020.00667.

[18] B. Chmiel *et al.*, "Feature map transform coding for energy-efficient CNN inference," in *International Joint Conference on Neural Networks (IJCNN)*, Jul. 2020, pp. 1–9, doi: 10.1109/IJCNN48605.2020.9206968.

[19] J. Zhang, Y. Liao, X. Zhu, H. Wang, and J. Ding, "A deep learning approach in the discrete cosine transform domain to median filtering forensics," *IEEE Signal Processing Letters*, vol. 27, pp. 276–280, 2020, doi: 10.1109/LSP.2020.2966888.

[20] B. Belkacemi, S. Saad, Z. Ghemari, F. Zaamouche, and A. Khazzane, "Detection of induction motor improper bearing lubrication by discrete wavelet transforms (DWT) decomposition," *Instrumentation Mesure Métrologie*, vol. 19, no. 5, pp. 347–354, Nov. 2020, doi: 10.18280/i2m.190504.

[21] K. L. Chung, J. S. Cheng, and H. B. Yang, "Effective chroma subsampling and luma modification for RGB full-color images using the multiple linear regression technique," *IEEE Access*, vol. 8, pp. 118315–118323, 2020, doi: 10.1109/ACCESS.2020.2999910.

[22] W. A. Awadh, A. S. Alasady, and H. I. Mustafa, "Predictions of COVID-19 spread by using supervised data mining techniques," *Journal of Physics: Conference Series*, vol. 1879, no. 2, May 2021, doi: 10.1088/1742-6596/1879/2/022081.

[23] A. S. Hashim, W. A. Awadh, and A. K. Hamoud, "Student performance prediction model based on supervised machine learning algorithms," *IOP Conference Series: Materials Science and Engineering*, vol. 928, no. 3, p. 32019, Nov. 2020, doi: 10.1088/1757-899X/928/3/032019.

[24] P. G. S. P. Yadav, A. Prof, and H. Amhia, "A review article of image fusion technique using wavelet transform," vol. 7, no. 1, pp. 208–212, 2021.

[25] J. C. T. Arroyo, "An improved image steganography through least significant bit embedding technique with data encryption and compression using polybius cipher and huffman coding algorithm," *International Journal of Advanced Trends in Computer Science and Engineering*, vol. 9, no. 3, pp. 3376–3383, Jun. 2020, doi: 10.30534/ijatcse/2020/137932020.

[26] O. F. A. Wahab, A. A. M. Khalaf, A. I. Hussein, and H. F. A. Hamed, "Hiding data using efficient combination of RSA cryptography, and compression steganography techniques," *IEEE Access*, vol. 9, pp. 31805–31815, 2021, doi: 10.1109/ACCESS.2021.3060317.

[27] J. C. T. Arroyo and A. J. P. Delima, "LSB image steganography with data compression technique using goldbach G0 code algorithm," *International Journal of Emerging Trends in Engineering Research*, vol. 8, no. 7, pp. 3259–3264, Jul. 2020, doi: 10.30534/ijeter/2020/62872020.

[28] 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, Jun. 2020, doi: 10.30534/ijatcse/2020/124932020.

[29] A. T. Chawhan *et al.*, "A high secure and robust LSB image steganography using hybrid encryption, LZW compression and knight tour algorithm," in *Journal of Xidian University*, 2019, vol. 13, no. 4, pp. 1–9.

[30] A. Hamza, D. Shehzad, M. S. Sarfraz, U. Habib, and N. Shafi, "Novel secure hybrid image steganography technique based on pattern matching," *KSII Transactions on Internet and Information Systems*, vol. 15, no. 3, pp. 1051–1077, Mar. 2021, doi:

10.3837/tiis.2021.03.013.

[31] P. Khare and V. K. Srivastava, “A reliable and secure image watermarking algorithm using homomorphic transform in DWT domain,” *Multidimensional Systems and Signal Processing*, vol. 32, no. 1, pp. 131–160, Jan. 2021, doi: 10.1007/s11045-020-00732-1.

[32] M. Anasuodei and O. Friday Eleonu, “An enhanced satellite image compression using hybrid (DWT, DCT and SVD) algorithm,” *American Journal of Computer Science and Technology*, vol. 4, no. 1, p. 1, 2021, doi: 10.11648/j.ajcst.20210401.11.

[33] V. Shah and C. K. Kumbharana, “Design, development, and implementation of an image steganography algorithm for encrypted (using AES) and non-encrypted text into an image,” in *Advances in Intelligent Systems and Computing*, vol. 1187, Springer Singapore, 2021, pp. 313–320, doi: 10.1007/978-981-15-6014-9_36.

[34] M. A. Islam, M. S. Sarker, M. S. Hossen, A. H. Mridul, M. A. Hasib, and M. I. Jabiullah, “A multi-layer cryptosystem for secure data transmission using PRNG,” in *3rd International Conference on Intelligent Sustainable Systems (ICISS)*, Dec. 2020, pp. 1189–1196, doi: 10.1109/ICISS49785.2020.9315882.

[35] M. A. Ulkareem, W. A. Awadh, and A. S. Alasady, “A comparative study to obtain an adequate model in prediction of electricity requirements for a given future period,” in *International Conference on Engineering Technology and their Applications (IICETA)*, May 2018, pp. 30–35, doi: 10.1109/IICETA.2018.8458079.

[36] A. Saber and W. Awadh, “Steganography in MS excel document using unicode system characteristics,” *Journal of Basrah Researches*, vol. 39, no. 1, pp. 10–19, 2013.

[37] 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, Nov. 2021, doi: 10.1080/19393555.2020.1854902.

[38] M. Pelosi and C. Easttom, “Identification of LSB image steganography using cover image comparisons,” *The Journal of Digital Forensics, Security and Law*, 2021, doi: 10.15394/jdfsl.2021.1551.

[39] E. A. Abbood, R. M. Neamah, and S. Abdulkadhm, “Text in image hiding using developed LSB and random method,” *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 8, no. 4, pp. 2091–2097, Aug. 2018, doi: 10.11591/ijece.v8i4.pp2091-2097.

BIOGRAPHIES OF AUTHORS

Wid Akeel Awadh was born in Basrah, Iraq in 1984. She earned a bachelor's degree in Computer Science from Basrah University in 2006 and a master's degree in the same area from the same university in 2012. She is working as a lecturer in the Department of Computer Information Systems, Computer Science and Information Technology College, Basrah University, Iraq. She has sixteen papers in the field of computer science (information security and data mining cloud computing). She can be contacted at email: wid.jawad@uobasrah.edu.iq.

Ali Salah Alasady was born in Basrah, Iraq in 1985. He earned a bachelor's degree in Computer Science from Basrah University in 2007 and a master's degree in the Information Technology field from the Tenaga University, Malaysia in 2014. He is working as a lecturer in the Department of Computer Science, Computer Science and Information Technology College, Basrah University. He has sixteen papers in the field of computer science (information security and data mining and cloud computing). He can be contacted at email: Ali_s.hashim@uobasrah.edu.iq.

Alaa Khalaf Hamoud is a lecturer in Computer Information Systems, University of Basrah, Iraq. He received B.Sc. degree from Computer Science Department, University of Basrah in 2008 with first ranking college student. He also received his M.Sc. degree from the same department with first ranking department student. He participated in (seven months) IT administration course in the Technical University of Berlin, Germany. His scientific interests are data mining and data warehousing. He can be contacted at email: alaa.hamoud@uobasrah.edu.iq.