International Journal on
"Technical and Physical Problems of Engineering"
(IJTPE)
Published by International Organization of IOTPE

ISSN 2077-3528
IJTPE Journal
www.iotpe.com
ijtpe@iotpe.com

March 2023 | Issue 54 | Volume 15 | Number 1 | Pages 102-109

STEGANOGRAPHIC DATA HIDING USING QUANTUM BEHAVED PARTICLE SWARM OPTIMIZATION AND AN ENHANCED AES ALGORITHM

M.L. Talal [1] I.A. Hassan [2] F.K. Zaidan [3] I.M. Badr [2]

1. Department of Economics, College of Administration and Economics, University of Diyala, Baqubah, Iraq
mohammedeco@uodiyala.edu.iq
2. Department of Information Technology, College of Medicine, University of Diyala, Baqubah, Iraq
ihsan@uodiyala.edu.iq, iman@uodiyala.edu.iq
3. Diyala Presidency, University of Diyala, Baqubah, Iraq, sc_fadhelzaidan@uodiyala.edu.iq

Abstract- Steganography is the process that by it can hide information to different digital media, for cloud and computer users over the internet, The digital market witnessed great growth, especially after the Internet revolution, which is why the need to protect the data transmitted over the Internet, which has led to the emergence of many methods and methods to protect user data. There are many methods and techniques for obtaining hidden data. Data embedding is commonly used for copyright in communications like images, text, audio, or other multimedia information, as well as in military communications for authentication and a variety of other uses. Despite this, new technologies are constantly being developed, such as swarm intelligence. Therefore, this research paper discussed security additions in the field of image LSB steganography using the technique of the algorithm of QPSO (Quantum particle swarm optimization) to include encrypted images using the enhanced AES algorithm. as well as the moral sense of human vision. The results show that the combination of these two methods has enhanced security against any attack or attempt to manipulate or sabotage.

Keywords: LSB, Steganography, QPSO, AES, *PSNR*.

1. INTRODUCTION

In our time, the world has become a small village thanks to the Internet and the connection of various devices such as tablets and smartphones [1]. Due to the huge amount of data that is transferred through these devices, it has become necessary to secure the transmission of this data through the network and to maintain the privacy of the information, in addition to the possibility of concealing part of this data using data masking technology. Hiding data is through a transmission medium such as image, audio, or video [2]. In image hiding, the secret data is concealed in a cover image, and the result is known as a Stego-image. The image quality should be acceptable so that other people are not drawn to it.

There are two types of steganography approaches for embedding data in images: transform domain techniques and special domain techniques [3]. The least significant bit technique, which embeds data in the LSB position of a bit pixel of a cover image, is the simplest and most popular in the special domain. Many image-hiding techniques based on LSB were proposed by the researchers. In this paper, the QPSO algorithm was used to refine the LSB algorithm and thus find good locations in the medium (image) to hide the encrypted confidential data.

Our method uses a combination of encryption and hiding techniques to increase security against potential attack types when exchanging data over the Internet. We encrypt the message by using the AES algorithm, which is one of the most powerful encryption algorithms. After that, we hide the message in the LSB of the best locations selected by the algorithm of QPSO. The other sections of this research paper are divided as follows: Section 2 presents the contribution of this paper. Section 3 describes the background of AES, QPSO, and LSB algorithms respectively. Section 4 reviews literature related to some of the related works. Section 5 presents the method proposed and its implementation. Section 6 in this part, the experimental results of the proposed data masking method are examined. In the last part (Section 7) a conclusion is presented for the results of this research paper in addition to future recommendations.

2. BACKGROUND

This section is concerned with selected topics, which are considered as the background for this paper.

2.1. Advanced Encryption Standard Algorithm (AES)

It is an encryption algorithm that means to take the place of the DES algorithm as a recognized standard in specific situations [2], [3]. AES (Rijndael algorithm) is a data encryption and decryption standard (AES). It was used in our paper because of its advantages in document security and because it has been proven to be safe according to NIST standards [4].

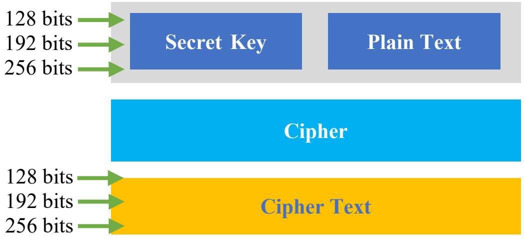

Figure 1. AES algorithm design

It is now employed by multinational corporations, this algorithm was chosen and because it has high accuracy and complexity at a very high level, making it more secure in encrypting the data, probably AES will stay secure for at least 20 years. There are three encryption models in the AES algorithm: 128-bit, 192-bit, and 256-bits. All coding models have a certain number of rounds (N_r) based on an agreement, and this agreement depends on the length of the keywords (N_k). For all encryption options, the size of the state block (N_b) remains constant. The block size of 128-bit refers to the state. Each state consists of four words [5]. Each of the words is defined as four bytes. The round key expansion of the key schedule function is the starting point for both encryption and decryption [6], [7]. The various key, state block, and round combinations are shown in Table 1. To convert the input (plain text) to the final output (ciphertext), the number of rounds for this conversion is determined, and this conversion is also done by the size of the key used in the encryption AES. Here are the round's numbers:

- For 128-bit keys, 10 rounds are required.
- For 192-bit keys, 12 rounds are required.
- 14 rounds for keys with 256 bits.

2.2. Least Significant Bit (LSB) Algorithm

The LSB algorithm is one of the most popular algorithms used to hide data and information in an image. In the LSB algorithm, all or some of the volumes (bytes) are changed to encrypted secret messages.

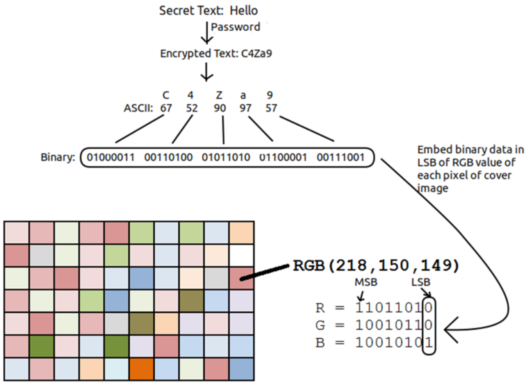

Figure 2. How LSB steganography works [8]

Because they are each represented by a byte, a bit of each RGB (Red, Green, Blue) component can be used. when using a 24-bit image. In this work, a secret message is only hidden in the blue color of the cover image, as shown as in Figure 2 [8].

2.3. Quantum Behaved Particle Swarm Optimization Algorithm (QPSO)

In [9], [10] The QPSO algorithm is proposed in this paper, as it depends on the potential well model. This algorithm is inspired by quantum mechanics and the SPSO algorithm [11]. According to the classical PSO algorithm [12], A particle can be defined based on its position on the x vector and the velocity vector v, and these two factors determine the particle's trajectory. Following Newtonian mechanics, the particle's motion is based on a predetermined trajectory.

However, in quantum mechanics, Since the x, and v vectors of the particle cannot be determined simultaneously, the trajectory term is meaningless. Some features of the QPSO algorithm differ from those of the SPSO algorithm. Firstly, QPSO is global convergent due to the exponential distribution of positions. In the QPSO algorithm, the average of the best position (*mbest*) is included in the evolution equation, and this thing is considered the second development of this algorithm. In SPSO, the affinity of the particle in QPSO is with the *mbest* site, taking into account the particles adjacent to it. The convergence of this particle depends on the best global position for it and independently [13].

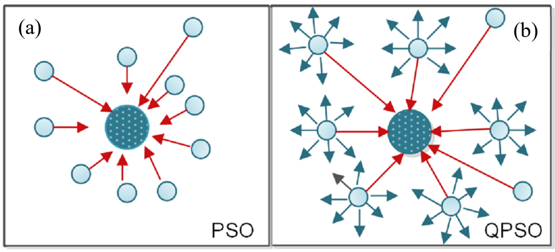

Figure 3. The Movement of Particles in (a) The PSO (b) the QPSO [11]

Instead of position and velocity, the quantum model of algorithm PSO depicts a particle's state as a wave function Ψ (x, t). The appearance of particles in any location, even if it is somewhat far from its current location, provided that it is within the possible region, and this depends on the probability density function based on the location of the particle in the field [10]. According to the iterative formula, the particles move [12], [11].

$$x(id+1) = p + a\left|mbest - x(id)\right| * \ln\left(1/u\right) ifk \geq 0.5 \quad \text{(a)} \qquad (1)$$

$$x(id+1) = p - a\left|mbest - x(id)\right| * \ln\left(1/u\right) ifk < 0.5 \quad \text{(b)} \qquad (1)$$

$$p = Qp_{id} + \left(1-Q\right) p_{gd} \qquad (2)$$

$$mbest = \frac{1}{M}\sum_{m}^{i=1} pi \qquad (3)$$

where, p_i is the best position of the particles and m is the number of the particles. The population's mean best *(mbest)* we can have defined as the average of all particles' best positions, where u, k, and Q are known as uniformly distributed random values between the range [0, 1]. The contraction expansion coefficient is the name of the parameter. After [10], the pseudo-code for the QPSO method is shown in Algorithm 1.

Algorithm 1. Pseudo code of QPSO algorithm

```
Initialize Swarm
Begin
While the condition termination is not met
Do
Calculate m_best by equation (3)
Update particle positions by using equation (1)
Update p_best
Update g_best
End do
End
```

3. RELATED WORKS

The Researchers in [14], The Least Significant Bit (LSB) algorithm was presented as a new Edge-to-Edge message entry technology. The edge area of the image is determined because human vision is incapable of detecting subtle changes in this area. Messages were double-protected by encrypting them with the One Time Panel (OTP) algorithm. To improve the encryption output, the message is converted to binary before encoding it first. This method can result in more verbal encryption of messages; this reduces the possibility of unauthorized parties decoding messages. As the value was measured by *PSNR* and *MSE*, a better insensitivity value was obtained. The histograms of the original and Stego images are also strikingly similar. Meanwhile, with a correlation coefficient (CC) of one, the messages can be extracted perfectly.

In an article [15], researchers propose a double layer of data security. The hidden information and encoded data that are entered into the jacket object via the LSB reflection algorithm are encoded using an elliptic curve coding algorithm. This technology combination has successfully met the benchmark for some basic characteristics such as data confidentiality and validation of integrity, ability, and robustness, demonstrating the excellent performance and effective implementation of this steganography process. This new method has been thoroughly tested with a variety of cloaking analysis attacks, including visualization, histogram, and chi-square. The experiment revealed that the Stego image provided a strong opposing force against all attacks. When compared to traditional methods, the ability to embed data has improved.

The researcher in the paper [16], proposes a new method of concealing the secret of the data a combination of AES and LSB technology. Users decide on image quality, which is based on several factors. Secret message lengths must be set. The user then has complete control over the volume output based on the requirements. In [17], the researcher suggested a strong masking method that is based on texture. This technique differs from traditional steganography in that it modifies an existing image, in which they conceal secret messages during the texturing process. And this texture is similar to the created Stego fabric sample picture, which maintains the local good looks. The researchers were able to achieve large embedding capabilities proportional to the dimensions of the composite tissue image. This technology also confirms that the entire hidden message can be extracted in the Stego-image.

Most crucially, the suggested steganography method eliminates the need for JPEG compression. We present a method in this article to enhance LSB algorithm by using QPSO algorithm to embed encrypted data using AES algorithm in the least significant bits of best locations that are selected using QPSO algorithm.

4. THE PROPOSED METHOD

The proposed method in this paper consists of four steps. First, it used 100×100 pixels' grayscale image a message input and then divided it into four segments using diagonal wise swapping. Secondly, it applied AES algorithm along the 256-bit key to encrypt the swapped message. Third, QPSO algorithm is used to find best locations of 1024×1024 pixels' color image as cover. Finally, we applied the LSB technique on the best locations of the cover image that are found by QPSO algorithm to hide the encrypted message. Figure 4 depicts our proposed encryption methods.

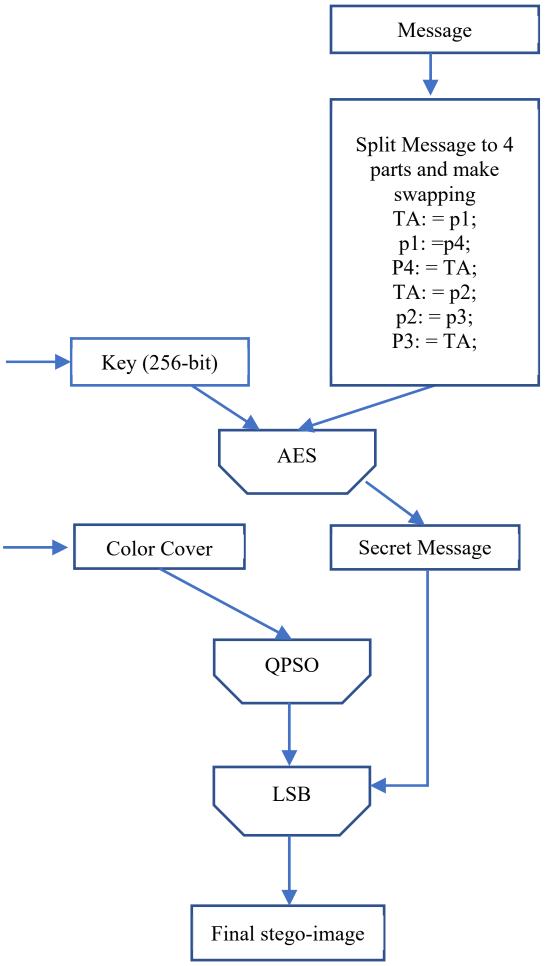

Figure 4. The proposed encryption method's methodology

At the side of the receiver, as shown in Figure 5, we chose the reverse fashion of that technique. The steps are described in full below.

4.1. Message Encryption

At the next steps we explain how the massage encryption:

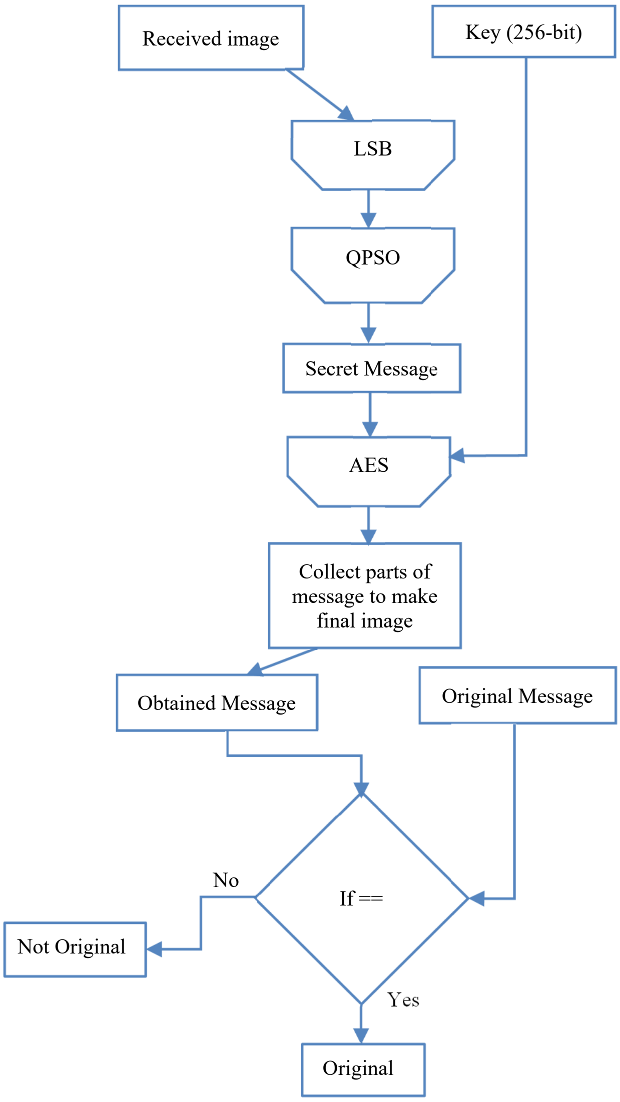

Figure 5. The proposed decryption method's methodology

4.1.1. Message Swapping

It is the first step of our scheme, First, using the diagonal wise swapping technique, split message image into four parts, each measuring 100×100 pixels or 200×200 pixels. Figure 6 depicts the entire process.

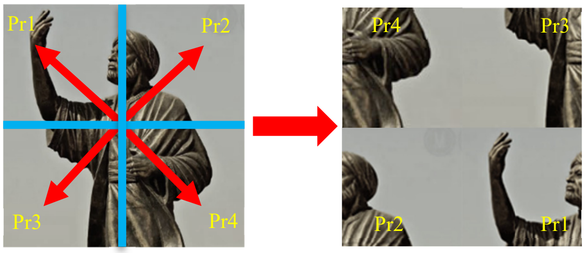

Figure 6. Diagonal wise message swapping

Swapping those four parts as follows:
TL: = Pr1; Pr1: = Pr4; Pr4: = TL;
TL: = Pr2; Pr2: = Pr3; Pr3: = TL;
where, TL is Temporary Location.

4.1.2. AES Algorithm Modification

This algorithm was developed in this study was used by increasing the size of data for each session in encryption and decomposition Encryption. The original method of this algorithm used 128-bit mass length and was developed to 512 bits per session with 256-bit key length and rotor number to 14 cycles as shown in Figure 7.

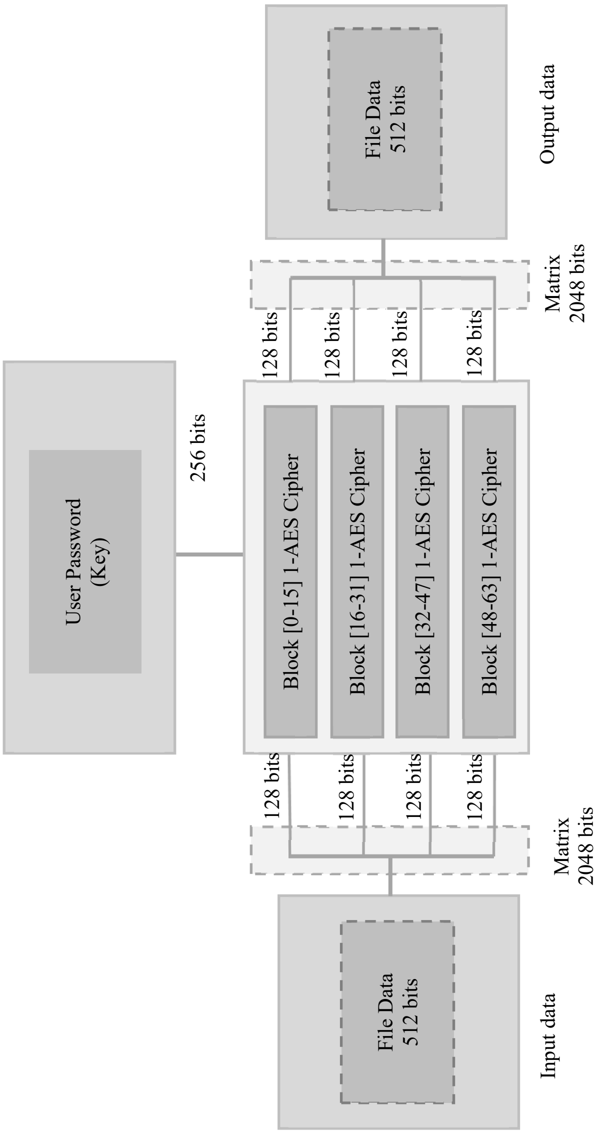

Figure 7. Modified AES encryption algorithm

In this method, data entry was performed by reading a 512-bit file and converted to a 2048-bit monochrome matrix. Further, it divided into four 128-bit single arrays according to sequences starting from (0-15) AES-1, (16-31) AES-2, (32-47) AES-3 and (48-63) AES-4. After data processing completed within each AES, the data converted into four single-bit 128-bit arrays. Later, all these matrices integrated into a single 2048-bit monochrome matrix. In the last part, data pushed to an external 512-bit file. This process completed until all data in the file is finished. In Algorithm 2, shown the pseudo-code for the altered algorithm of AES.

Algorithm 2. The modified AES algorithm's pseudo code

```
cipher (byte inb [16], byte out [16], key_array round_key [Nr+1])
begin
byte state [16];
state = in;
AddRoundKey (state, round_key [0]);
for i = 1 to Nr-1 stepsize 1 do
SubBytes(state);
ShiftRows(state);
MixColumns(state);
AddRoundKey (state, round_key[i]);
end for
SubBytes(state); ShiftRows(state); AddRoundKey (state, round_key [Nr]);
End.
```

4.1.3. Applying QPSO Algorithm

The QPSO algorithm is a powerful swarm intelligence search technique that is Used to hide secret messages by cover image by finding the best hiding spots. The fitness function is calculated using statistical calculations for each location in the cover image. These are the *X*-pos., *Y*-pos., variance, and mean calculations. The terms *X*-pos. and *Y*-pos. those refer to the coefficient's the 2D location in the cover image. The Equations (4) and (5) [18], [19] generate the mean and variance for each position.

$$Mean = \sum_{j=1}^{M} \left(X_i \right) / M \tag{4}$$

$$Variance = \left(X_i - mean \right)^2 / M \tag{5}$$

where, $X_i(j)$ represents the value in a specific position and M represents the number of locations in the cover image.

In QPSO technique, it is assumed that the bird (particle) exhibits quantum behavior and is flying in 2D space with a δ potential well cantered at a local attractor $f(p)$ (the current position of the bird's fitness) cover image,

4.1.4. The Secret Data Embedded

The (LSB) technique used now in this step, the insertion of the LSB is a method to include information in the image cover that involves replacing the LSBs of bytes in the cover image with bits of bytes from the secret message. In this work, the secret message is only hidden in blue. In Algorithm 3 the pseudocode of the message encryption algorithm is shown.

Algorithm 3. The encryption algorithm

Input: Watermark (message (W)): Gray level, Color Cover image (C).
Output: Encrypted watermark.
Step 1: read color image as a cover (C). Let (W) be an original message (Gray image) with size (100*100) or (200*200).
Step 2: Split (W) image to four parts {Pr1, Pr2, Pr3, and Pr4} as described in section 5.1.a.
Step 3: Using the AES Algorithm, as described in section 5.1.b, to encrypt the four swapped parts in order to generate new encrypted parts.
Step 4: By using QPSO algorithm as described in section to find best locations in cover image.
Step 5: To generate (C'), use the LSB Algorithm to hide the encrypted watermark (W') inside the round of color cover (C).

4.2. Message Decryption

In this step, Initially, as a first step, the QPSO algorithm is used in order to get the best sites in the Steo cover image. Then the watermark extracts using LSB algorithm. Second, the watermark was decrypted using the AES algorithm to obtain the original message, as illustrated in Figures 8 and 9. Algorithm 4 displays the pseudocode of the algorithm of Message Encryption. The pseudo code of the QPSO algorithm is applied to the stream of numbers to cover image at Algorithm 1 to find the best locations in the cover image.

Algorithm 4. Decryption algorithm

Input: Consider the color image (that received it stego-image)
Output: Watermark (message (W)).
Step1: QPSO algorithm is used to find best locations in the stego cover image.
Step2: Using the LSB algorithm, extract the received watermark and leave it alone (WR').
Step3: Split the watermark (WR’) to four parts {Pr1’, Pr2’, Pr3’ and Pr4’}.
Step4: Decrypting each part of the watermark (WR') with ASE (Advanced Encryption Standard) to obtain the original parts Pr1, Pr2, Pr3, and Pr4.
Step5: Swap the parts between them to get the proper message order to get an original message (WR).

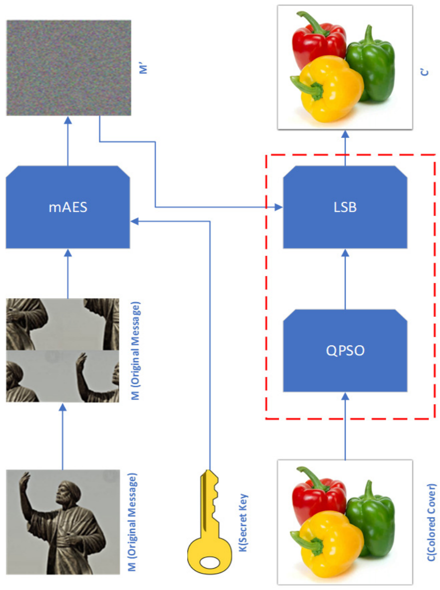

Figure 8. The Encryption Scheme

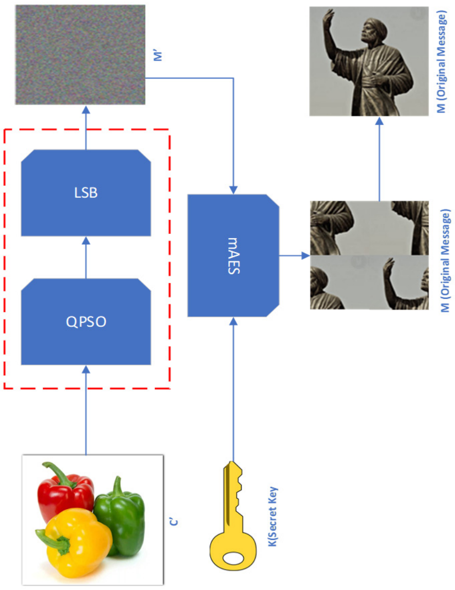

Figure 9. The Decryption Scheme

4.3. The Results and Analysis of Suggested Framework

The cryptographic methodology in the proposed method has been tested on various types and sizes of input images, as well as with different size keys of the AES encryption algorithm, the results shown the efficiency of it as shown in Figure 6. The cover data employed did not distort or lose information embedded and hidden in color images surrounding the area. The message of division and exchange between four parts, have increased the algorithm's strength. The encryption of hidden text with a modified AES algorithm makes the security of hidden information too strong and produced better results than existing methods. the performance evaluation of the steganography method using the parameters listed below [20]:

1) The Capacity: Indicates the maximum data that can be included within the image.

2) Robustness: means, the message that embedded arrives at the receiver unchanged as a result of attacks such as resize, compression, cropping, filtering, and rotation among others.

3) The measured the quality of Stego-image can be calculated by using *PSNR*, *MSE* and *NC* shown in Equations 6, 7, and 8, respectively.

- Normalization Correlation (*NC*):

$$NC = \sum_i sw(i) \times \frac{s(i)}{\sum_i \left(s(i)\right)^2} \qquad (6)$$

- Mean Squared Error (*MSE*):

$$MSE = \frac{1}{MN} \sum_1^M \sum_1^N \left(f_{ij} - g_{ij}\right)^2 \qquad (7)$$

where,

f: represents the matrix data of our original image
g: represents the matrix data of our degraded image in question
M: represents the numbers of rows of pixels of the images and *i* represents the index of that row
N: represents the number of columns of pixels of the image
j: represents the index of that column

- Peak Signal to Noise Ratio (*PSNR*):

PSNR is a quality metric that is being evaluated here for the purpose of embedding a signature.

$$PSNR = 10\log\left(\frac{L^2}{MSE}\right) \qquad (8)$$

where, L^2 is the maximum fluctuation in the input image data type.

Equation 8 shows the average number of bits that are embedded in the pixel and thus measures the performance of the modulation capacity. The higher *PSNR*, the better image's quality or in other words the less distortion. The higher *PSNR* value, the lower possibility of visual aggression to the eye human of the human [21]. When compared to traditional LSB, the results of this method reveal a high-quality image that includes an encrypted watermark (JPEG and BMP). Table 3 shows the results of the proposed method and the traditional LSB method, as well as the results of all images, showing that the Normalization Correlation is (*NC* = 1).

Table 1. The Stego-image *PSNR* and the value of *MSE*

Image size	Image type		*PSNR* value		*MSE* value		*NC* value	
	Bmp	Jpeg	Bmp	Jpeg	Bmp	Jpeg	Bmp	Jpeg
100×100	Lena	Lena	51.3254	51.2457	0.0412	0.0434	1	1
	Baboon	Baboon	57.1781	57.3315	0.0521	0.0515	1	1
	car	car	44.2788	44.0014	0.0407	0.0471	1	1
	Airplane	Airplane	58.0201	58.1412	0.0430	0.0421	1	1
200×200	Lena	Lena	55.1573	55.1536	0.0472	0.0525	1	1
	Baboon	Baboon	80.2855	80.3484	0.0530	0.0543	1	1
	car	car	52.1542	52.0183	0.0463	0.0528	1	1
	Airplane	Airplane	58.5427	58.6085	0.0519	0.0461	1	1

Table 2. *PSNR*'s values and *MSE*'s values in relation for traditional LSB

Image size	Image type		*PSNR* value		*MSE* value		*NC* value	
	Bmp	Jpeg	Bmp	Jpeg	Bmp	Jpeg	Bmp	Jpeg
100×100	Lena	Lena	51.5470	51.2574	0.0499	0.0445	1	1
	Baboon	Baboon	57.5000	57.4052	0.0539	0.0537	1	1
	car	car	45.2997	44.2452	0.0419	0.0485	1	1
	Airplane	Airplane	59.5270	58.3464	0.0440	0.0450	1	1
200×200	Lena	Lena	56.1690	56.2451	0.0441	0.0560	1	1
	Baboon	Baboon	81.2132	80.0207	0.0545	0.0557	1	1
	car	car	53.1919	53.2452	0.0478	0.0537	1	1
	Airplane	Airplane	60.1336	60.2345	0.0536	0.0492	1	1

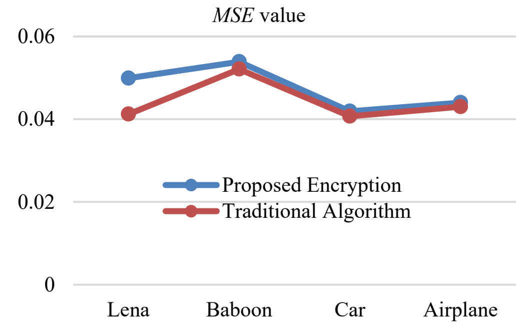

Figure 10. *MSE* compares of proposed system with traditional system

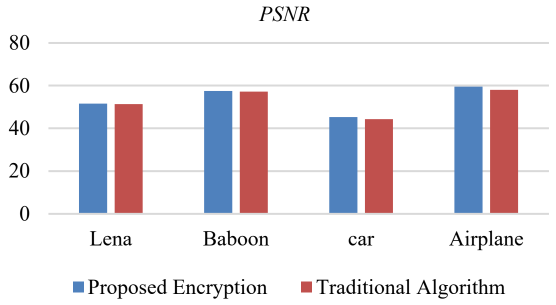

Figure 11. *PSNR* comparison of proposed and traditional systems

Stego images of the proposed approach as well as the comparative approach in this article maintain their quality, as demonstrated by the visualization test in Figure.10. The analysis of the LSB method and the QPSO algorithm with modified AES has been successfully implemented in this paper, and the results show that *PSNR* is high and *MSE* is low in LSB-based steganography [22], [23]. The proposed approach for extracting the secret text message is too complex, secure, and cannot be monitored by unauthorized users when the user sends it via the internet to another side. It should be noted that the approach proposed in this research paper allows converting any text or image into a set of bits and is later included in the image, and thus works to hide these media (images and texts).

5. CONCLUSION

Recently, several types of attacks could be targeting information over the internet. Steganography can be defined as the process of hiding important data by including it on normal data, such as images or texts, and then extracting this important data when it reaches its destination. There are numerous methods that could be used to avoid data detection during transmission. To secure the information during transmission, a hybrid of particle swarm optimization (QPSO) and Advanced Encryption Standards was used in this work. The proposed system can be used in Cloud Computing, IoT, and Servers. A set of high-quality standard images was used to test and evaluate the proposed system's performance. According to the results, the proposed system performed exceptionally well in terms of information security.

REFERENCES

[1] T. Halder, S. Karforma, R. Mandal, et al., "A Block-Based Adaptive Data Hiding Approach Using Pixel Value Difference and LSB Substitution to Secure E-Governance Documents", Journal of Information Processing Systems, Vol. 15, No. 2, pp. 261-270, 2019.

[2] S.A. Parah, J.A. Sheikh, J.A. Akhoon, N.A. Loan, "Electronic Health Record Hiding in Images for Smart City Applications: A Computationally Efficient and Reversible Information Hiding Technique for Secure Communication", Futur. Gener. Comput. Syst., Vol. 108, pp. 935-949, 2020.

[3] O.F. AbdelWahab, A.I. Hussein, H.F.A. Hamed, H.M. Kelash, A.A. M. Khalaf, H.M. Ali, "Hiding Data in Images Using Steganography Techniques with Compression Algorithms", Telecommunication Computing Electronics and Control, Vol. 17, No. 3, pp. 1168-1175, 2019.

[4] S.K. Rao, D. Mahto, D.A. Khan, "A Survey on Advanced Encryption Standard", International Journal of Science and Research, Vol. 6, No. 1, pp. 711-724, 2017.

[5] U. Farooq, M.F. Aslam, "Comparative Analysis of Different AES Implementation Techniques for Efficient Resource Usage and Better Performance of an FPGA", Journal of King Saud University, Computer and Information Sciences, Vol. 29, No. 3, pp. 295-302, 2017.

[6] H.A. Al Essa, A.S. Ashoor, "Enhancing Performance of AES Algorithm Using Concurrency and Multithreading", ARPN Journal of Engineering and Applied Sciences. Appl. Sci., Vol. 14, No. 11, 2019.

[7] M. Masoumi, "A Highly Efficient and Secure Hardware Implementation of the Advanced Encryption Standard", Journal of Information Security and Applications, Vol. 48, p. 102371, 2019.

[8] U. Cavusoglu, S. Kacar, I. Pehlivan, A. Zengin, "Secure Image Encryption Algorithm Design Using a Novel Chaos Based S-Box", Elsevier, Chaos, Solitons and Fractals, Vol. 95, pp. 92-101, February 2017.

[9] M. Hajihassani, D.J. Armaghani, R. Kalatehjari, "Applications of Particle Swarm Optimization in Geotechnical Engineering: A Comprehensive Review", Geotechnical and Geological Engineering, Vol. 36, No. 2, pp. 705-722, 2018.

[10] J. Sun, C.H. Lai, X.J. Wu, "Particle Swarm Optimization: Classical and Quantum Perspectives", CRC Press, 1st edition, Florida, USA, 2012.

[11] I.R. Mohammed, Z.T. Mustafa, "Image Steganography Based the Behavior of Particle Swarm Optimization", Journal of Theoretical and Applied Information Technology, Vol. 96. No 12, pp. 3696-3706, June 2018.

[12] F. Han, Y.W.T. Sun, Q.H. Ling, "An Improved Multiobjective Quantum-Behaved Particle Swarm Optimization Based on Double Search Strategy and Circular Transposon Mechanism", Complexity, 2018.

[13] G. Wang, "Research on Particle Swarm Optimization Algorithm Based on Quantum Computing Technology", American Journal of Electrical and Electronic Engineering, Vol. 8, No. 1, pp. 21-25, 2020.

[14] C. Irawan, C.A. Sari, E.H. Rachmawanto, "Hiding and Securing Message on Edge Areas of Image Using LSB Steganography and OTP Encryption", The 1st International Conference on Informatics and Computational Sciences (ICICoS), pp. 1-6, 2017.

[15] R. Shanthakumari, S. Malliga, "Dual Layer Security of Data Using LSB Inversion Image Steganography with Elliptic Curve Cryptography Encryption Algorithm", Multimedia Tools and Applications, Vol. 79, No. 5, pp. 3975-3991, 2020.

[16] A. Pandey, J. Chopra, "Steganography Using AES and LSB Techniques", International Journal of Scientific Research & Technology, Vol. 6, No. 6, pp. 620-623, 2017.

[17] Z. Qian, H. Zhou, W. Zhang, X. Zhang, "Robust steganography using texture synthesis", 12th International in Advances in Intelligent Information Hiding and Multimedia Signal Processing, Springer, pp. 25-33, Kaohsiung, Taiwan, 2017.

[18] X. Liao, Z. Qin, L. Ding, "Data Embedding in Digital Images Using Critical Functions", Signal Processing Image Communication, Vol. 58, pp. 146-156, 2017.

[19] H. Fadel, R.S. Hameed, J.N. Hasoon, S.A. Mostafa, B.A. Khalaf, "A Light-Weight ESalsa20 Ciphering Based on 1D Logistic and Chebyshev Chaotic Maps", Solid State Technology, Vol. 63, No. 1, pp. 1078-1093, 2020.

[20] M.A. Sabri, M.L. Talal, I.A. Hassan, "Image Processing for Tribble Faults of Features Images via SPM", International Journal of Computer Science and Wireless Security. Vol. 06, No. 05, pp. 1-5, September - October 2019.

[21] A. Bellat, I. Tyass, Kh. Mansouri, A. Raihani, "Optimization of Wind Farms by The Particle Swarm Algorithm Considering Gaussian Wake Model", International Journal on Technical and Physical Problems of Engineering (IJTPE), Issue 48, Vol. 13, No. 3, pp. 48-54, September 2021.

[22] S. Arslan, I. Iskender, "Design of Frameless Gimbal Motor for Uav Applications", International Journal on Technical and Physical Problems of Engineering (IJTPE), Issue 50, Vol. 14, No. 1, pp. 142-148, March 2022.

[23] A.Sh. Abdinov, R.F. Babayeva, "Flexible Photocells Based on Layered $A^{III}B^{VI}$ Semiconductor Compounds", International Journal on Technical and Physical Problems of Engineering (IJTPE), Issue 40, Vol. 11, No. 3, pp. 23-27, September 2019.

BIOGRAPHIES

First Name: **Mohammed**
Middle Name: **Layth**
Surname: **Talal**
Birthday: 30.03.1983
Birth Place: Baqubah, Iraq
Bachelor: Computer Science, Department of Computer Science, Al Yarmok University College, Baqubah, Iraq, 2006
Master: Information Technology, Department of Mathematics and Computer Science, Natural and Applied Science, Cankaya University, Ankara, Turkey, 2015
The Last Scientific Position: Lecturer, Department of Economics, College of Administration and Economics, University of Diyala, Baqubah, Iraq, 2014
Research Interests: Information Systems, Image Processing, Networking
Scientific Publications: 8 Papers, 1 Thesis

First Name: **Ihsan**
Middle Name: **Ali**
Surname: **Hassan**
Birthday: 21.02.1982
Birth Place: Baqubah, Iraq
Bachelor: Computer Science, Department of Computer Science, Almustenseria University, Baghdad, Iraq, 2006
Master: Information Technology, Department of Mathematics and Computer Science, Natural and Applied Science, Cankaya University, Ankara, Turkey, 2014
The Last Scientific Position: Lecturer, Department of Information Technology, College of Medicine, University of Diyala, Baqubah, Iraq, 2014
Research Interests: Information Systems, Image Processing, Medical Informatics, Cloud Computing
Scientific Publications: 8 Papers, 1 Book, 1 Thesis

First Name: **Fadhil**
Middle Name: **Kadhem**
Surname: **Zaidan**
Birthday: 01.03.1975
Birth Place: Baqubah, Iraq
Bachelor: Computer Science, Department of Computer Science, Al-Rafidian University College, Baghdad, Iraq, 1998
Master: Information Technology, Department of Mathematics and Computer Science, Natural and Applied Science, Cankaya University, Ankara, Turkey, 2016
The Last Scientific Position: Lecturer, Department of Information Technology, Diyala Presidency, University of Diyala, Baqubah, Iraq, 2016
Research Interests: Information Systems, Image Processing, Wireless Sensor Networks
Scientific Publications: 5 Papers, 1 Thesis

First Name: **Iman**
Middle Name: **Mudhehr**
Surname: **Bader**
Birthday: 05.08.1986
Birth Place: Baqubah, Iraq
Bachelor: Computer Engineering, Department of Software Engineering, University of Diyala, Baqubah, Iraq, 2008
The Last Scientific Position: Engineer, Department of Information Technology, College of Medicine, University of Diyala, Baqubah, Iraq, 2010
Research Interests: Software Engineering, Image Processing, Database
Scientific Publications: 1 Paper