

A Hybrid System Based on Three Levels to Hide Information using JPEG Color Images

Ali Mahmood Khalaf¹, Kamaljit Lakhtaria²

^{1,2} Department of Computer Science, College of Science
Gujarat University, Ahmadabad, Gujarat, India.

Article Info

Article history:

Received: 04, 07, 2024

Revised: 07, 09, 2024

Accepted: 15, 09, 2024

Published: 30, 09, 2024

Keywords:

Cryptography Algorithms

Steganography Techniques

Mixing AES-RSA Algorithms

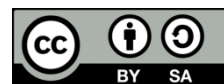
FSA

LSB Technique

ABSTRACT

Nowadays, due to the circulation of information among people, information security has become an important requirement to protect information from hacking. Many techniques have been discovered to protect this information and maintain its confidentiality from hacking, the most prominent of which are cryptography and steganography techniques. In this paper, a hybrid system based on three levels to hide information using Joint Photographic Experts Group (JPEG) color images, where this system works in both processes sender and receiver. The sender process at the first level uses a mixing of the Advanced Encryption Standard (AES) and Rivest Shamir Adleman (RSA), while at the second level uses a Fuzzy Stream Algorithm (FSA) adds a higher complexity and eliminates the non-linearity of the encrypted information. The third level is to hide encrypted information using the Least Significant Bit (LSB) technique, while the receiver process, performs the reverse process of three levels. This system provides high information embedding capability and the inability to perceive hidden information, the system was evaluated based on criteria like Peak Signal Noise Ratio (PSNR), Mean Square Error (MSE), Structure Similarity (SSIM), and correlation, which were characterized by high and good rates. The study was compared with modern steganography techniques.

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



Corresponding Author:

Ali Mahmood Khalaf

Department of Computer Science, College of Science

Gujarat University, Ahmadabad, Gujarat, India.

Email: alikhalf@gujaratuniversity.ac.in



1. INTRODUCTION

The Internet has led to rapid development in the field of information and its applications [1]. The exchange of information, such as online shopping methods, paying bills and credit cards, and personal files, has become very important among people, especially after the technological revolution, the emergence of computer networks, and the increase in the volume of this information. It is easy to exchange information (text, images, audio, and video) due to its breadth, hence the need for experts to do so. Information-hiding technology has also emerged to protect this information from external threats. Information-hiding technologies include cryptography, steganography, and watermarking [2]. Cryptography comes from two words, the first Crypto means hidden secret and the second graphein means covered writing, and security has become an important issue in industry and business management. In cryptography, plain text is converted into cipher text by algorithms, which are of two types: Symmetric encryption technology or Secret Key Cryptography (SKC) means encryption with one key for encryption and decryption at the same time and is represented by several algorithms including Data Encryption Standard (DES), Triple Data Encryption Standard (3DES), Twofish and Blowfish algorithm, and AES. The second encryption technology is asymmetric encryption technology or public key encryption (PKC), which consists of two keys, the first key for encryption and the second key for decryption. Types of cryptography algorithms are RSA, Elliptic Curve Cryptography (ECC), and Digital Signature Algorithm (DSA), and thus these technologies maintain the

confidentiality and integrity of this information [3-4]. In addition, other techniques and patterns are used in encryption, such as genetic algorithms that undergo crossover and mutation processes and choose the best solutions. Genetic Algorithms (GA) are used in encrypting images and diagnosing some diseases through decision-making [5]. Figure 1 shows that the cryptography techniques.

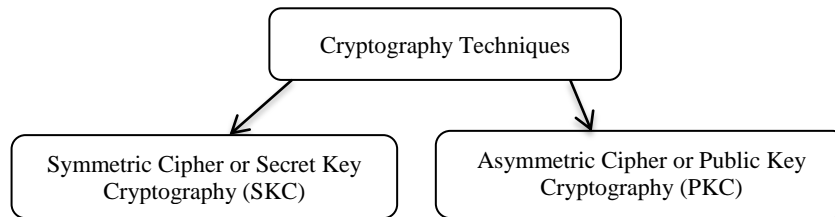


Figure 1: Cryptography Techniques [6]

The Greek term Steganography comes from two words: stegano, which means, hidden, and graphy, which means writing or drawing. Steganography aims to provide a secure connection with complete non-discovery and to avoid the emergence of confidential data transmission, as the concealment is done by embedding the secret message within an information carrier medium (text, image, audio, video), which makes it indefinable to the human eye, where it is indicated to the medium carrying the secret message in the name of (stego file). The steganography model consists of the secret message, the carrier, the Stego key, and the method of embedding to form the general steganography model. There are two steganography techniques such as spatial domain techniques, and frequency domain techniques [7-8]. Figure 2 shows steganography techniques.

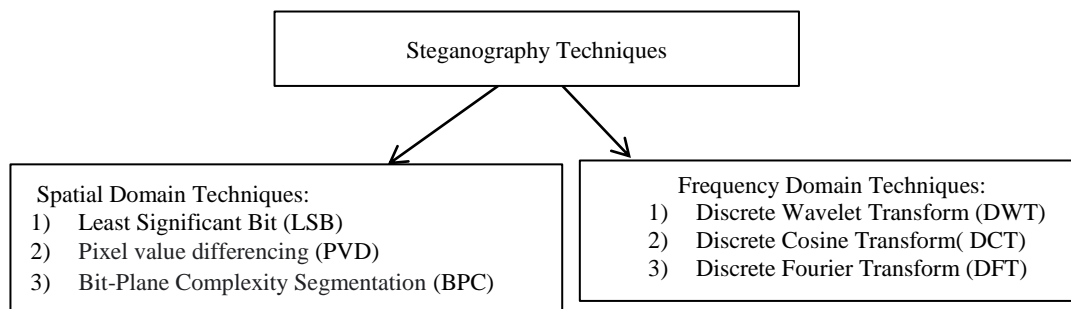


Figure 2: Steganography Techniques [9]

2. CONTRIBUTIONS AND OBJECTIVES

2.1 CONTRIBUTIONS

The contributions of this paper lie in designing a hybrid system to hide information for JPEG color image format by using encryption techniques, where the message is encrypted before hiding in the color images with the extension (.jpeg) by using the steganography techniques, and this gives a new direction by improving the current techniques in encrypting and hiding the message by using the cryptography and steganography techniques.

2.2 OBJECTIVES

- To design and develop a hybrid system to hide information for JPEG color images.
- Use of an easy to use and quick a hybrid system.
- Use an advanced and robust a hybrid system.

3. RELATED WORK

Shanthakumari and Smalliga, 2019 [10] Dual-layer security of image steganography based on IDEA and LSB algorithm in the cloud environment. In this paper, the IDEA was used with the technique of hiding the least significant bits to merge the secret information into the original image and extract it. Information was obtained and a reduction in problems related to security. The system was evaluated through the use of statistical methods and the results showed that the proposed technique outperforms current methodologies and solves a security problem. Ansari et al., 2020 [11] "A Multiple-Format Steganography Algorithm for Color Images". A new algorithm is presented, which is the first steganography technique that can work with multiple cover image formats TIFF, JPEG, BITMAP, PNG. Concepts such as capacity pre-estimation, adaptive partitioning schemes, and data propagation are used to encapsulate confidential data with security

enhancements. The proposed method was tested for its robustness against steganalysis with positive results obtained. Moreover, the comparative results of the proposed algorithm are very promising for three different cover image formats. Kareem et al., 2020 [12]. Hiding Encrypted Text in Image Steganography .In this paper, the researcher proposed a way to encrypt the text using Triple Data Encryption Standard (3DES) symmetric key algorithm to increase the security of confidential information, and the second stage is the stage of text hiding. This system was implemented using Java Platform Micro Edition to support mobile functions and applications. Sindhu and Singh, 2021 [13] Information Hiding Using Steganography .In this paper, the researcher has improved the hiding system by using the LSB algorithm to hide a text file inside the image, where an application program was provided to hide information for the purpose of how to use any type of image to hide any type of information to be hidden. The main work of this application is to support any type of image without the need to convert it to a bitmap, and the minimum file size to hide it because the maximum memory capacity in the images is used to hide the file. The results showed that this application plays an increasing role in the future of secure communications in the digital world. Chalooop and Abdullah, 2021 [14] Enhancing Hybrid Security Approach Using AES And RSA Algorithms. This paper presents an encryption method between people, institutions, or information available via the Internet. This research consists of two stages: the first is data encryption using the hybrid algorithm (RSA + AES) from the sender to the recipient over the network, and the second stage is the decryption stage. The paper results showed that the hybrid algorithm is better in terms of security. Tang et al., 2021[15] An adaptive fuzzy inference approach for color image steganography. This paper proposes a method to mask color images, considering the effect of image complexity such as pixel similarity, pixel brightness and color sensitivity. The system is designed using the chaotic method and random sequence on the secret message to generate the random sequence that prevents the secret message from attackers as a classifier that adopts the features of the cover image as explicit input values and produces semantic concepts corresponding to the payload of the image subclasses. The method hides a large amount of data with good hidden image quality from the human visual system and ensures confidentiality in communication. Experimental results show better mean square error, peak signal-to-noise ratio, structural similarity and payload, which confirms that the proposed method can lead to better performance than some recent works. Zulqarnain et al., 2021 [16] An Efficient Method of Data Hiding for Digital Colour Images Based on Variant Expansion And Modulus Function. In this paper, an information masking method based on the variable expansion modulus function is introduced. It provides high security for the color image. A new method has been developed that chooses both positive and negative difference values to hide confidential data. From the experimental results of the paper, method obtains a higher capacity with PSNR that was high as its effectiveness was tested on different types of standard color images and the results showed the inability to perceive the masking image compared to modern masking methods while maintaining the appropriate image quality. Abroshan, 2021 [17] A Hybrid Encryption Solution to Improve Cloud Computing Security and Asymmetric Cryptography Algorithms. In this paper an effective encryption system is proposed to improve security in cloud computing. The hybrid algorithm Blowfish and Elliptical Curve Cryptography (ECC) has been improved. Blowfish encrypts the data, and ECC will encrypt its key, which will increase security and performance. Moreover, digital signature technology is used to ensure data integrity, and the results show improvement in throughput, execution time, and memory consumption parameters. Naser et al., 2022 [18] Steganography and Cryptography Techniques Based Secure Data Transferring Through Public Network Channel. In this paper, two methods are presented to ensure safe transmission of the message. The message is encrypted as a first step using the Rivest Cipher 4 (RC4) algorithm, in order to increase the confidentiality of the message, and the second step is to include LSB by adding an extra layer of security. An improvement to the LSB method comes by replacing the adopted sequential selection method with a random selection of frames and pixels with two secret random keys. Therefore, the attacker is unable to find out the correct frames and pixels because the encrypted message remains protected even if the stego object is compromised. Among the most important findings of the paper is that the proposed system provides good performance when compared to a large number of previous studies. Hameed et al., 2022 [19] High Capacity Image Steganography System based on Multi-layer Security and LSB Exchanging Method. In this paper, a system of information steganography was proposed using the modified steganography technique (LSB), where the data that is encrypted and compressed using AES is included with Huffman coding, and one of the most prominent results reached is to provide the maximum load capacity with a high safety and reliability ratio, as the search indicators, Normalized Cross-Correlation (NCC), and the proposed method is immune to Graph and Chi-square.

Table 1. comparison between the cryptography algorithms and steganography techniques

No	Author Name and Years	Paper Title	Criteria	Results
1	Shanthakumari and Smalliga, 2019 [10]	Dual-layer security of image steganography based on IDEA and LSB algorithm in the cloud environment	IDEA, LSB	the results showed that the proposed technique outperforms current methodologies and solves a security problem.
2	Ansari et al., 2020 [11]	A Multiple-Format Steganography Algorithm for Color Images	LSB	The comparative results of the proposed algorithm are very promising for three different cover image formats.
	Kareem et al., 2020 [12]	Hiding Encrypted Text in Image Steganography	3DES, XOR	This system was implemented using Java Platform Micro Edition to support mobile functions and applications.
4	Sindhu and Singh, 2021 [13]	Information Hiding using Steganography	LSB	The results showed that this application plays an increasing role in the future of secure communications in the digital world.
5	Chalooop and Abdullah, 2021 [14]	Enhancing Hybrid Security Approach Using AES And RSA Algorithm	AES, RSA	The paper results showed that the hybrid algorithm is better in terms of security.
6	Tang et al., 2021 [15]	An adaptive fuzzy inference approach for color image steganography	Chaotic Theorem	Experimental results show better MSE, PSNR, and SSIM
7	Zulqarnain et al., 2021[16]	An Efficient Method of Data Hiding for Digital Colour Images Based on Variant Expansion And Modulus Function	Variant expansion Modulus Function	The results of the paper, a higher capacity with PSNR that was high as its effectiveness was tested on different types of standard color images and the results showed the inability to perceive the image.
8	Abroshan, 2021 [17]	A Hybrid Encryption Solution to Improve Cloud Computing Security and Asymmetric Cryptography Algorithms	Blowfish, ECC	The results of paper show improvement in throughput, execution time, and memory consumption parameters.
9	Naser et. al, 2022 [18]	Steganography and Cryptography Techniques Based Secure Data Transferring Through Public Network Channel	RC4, LSB	The paper is that the proposed system provides good performance when compared to a large number of previous studies.
10	Hameed et al., 2022 [19]	High Capacity Image Steganography System based on Multi-layer Security and LSB Exchanging Method	AES, LSB	The results is to provide the maximum load capacity with a high safety and reliability ratio.

4. A SURVEY OF ALGORITHMS AND TECHNIQUES

4.1 AES ALGORITHM

Encryption using the AES algorithm is a block cipher that uses a single key for encryption and decryption, and it is an encryption equivalent to Rijndael cipher, which is an encryption that deals with information at the byte or bit level, and this algorithm consists of three keys whose sizes are (128 with 10 rounds, 192 with 12 rounds and 256 with 14 rounds), and the algorithm consists of 16 bytes and is a (4 * 4) matrix. This algorithm consists of four main steps [20] :

4.1.1 SUB BYTE STATE

In this step, which 4 * 4 matrix converted to another table to use encryption process called S-Box, which is a pre-calculated table. As for the decoding process, it uses the inverse S-Box table, which includes the S- table.

4.1.2 SHIFT ROWS STATE

In this step, the rows are moved through multiple shifts except for row zero, which does not change and remains constant, in the first row it moves by 1 byte, the second row by 2 bytes, and the third row, by 3 bytes.

4.1.3 MIX COLUMN STATE

In this step, the bytes in each column are moved independently, and the aim of this step is to mix the input block 128 additionally. In the case of encryption, Shift Rows multiply the matrix resulting from the second step with a special algorithm of size 4×4 in this case of decoding; a special decoding matrix is used.

3.1.4 ADD ROUND KEY STATE

In this step, which is the last of the steps of this algorithm, the X-OR operation is used between the matrix in the output of the previous step with the key matrix, where the two matrices are 128 bits in size, and thus a matrix of 4×4 dimensions is formed with a size of 128 bits. The block diagram of AES algorithm is shown all steps below figure 3.

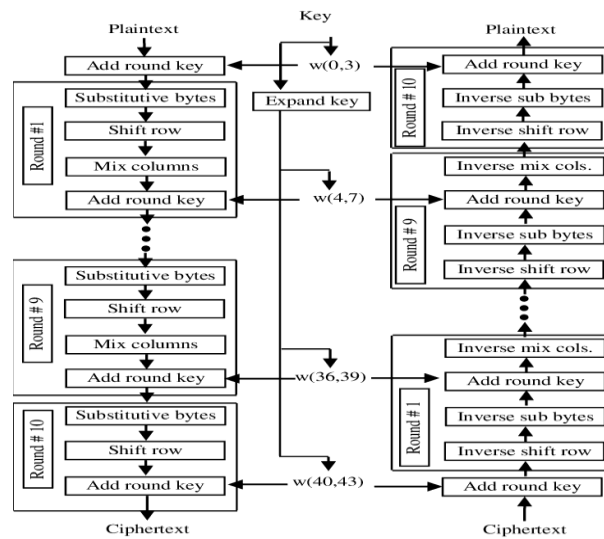


Figure 3. Block Diagram of AES Algorithm [20]

4.2 RSA ALGORITHM

It is an algorithm developed by the three mathematicians Rivest, Shamir, and Adelman in 1977. It is an asymmetric encryption algorithm that has two keys, the first for data encryption (the sender) and the second key for decryption of the data alongside (the recipient), and it is used in digital signatures and key exchange, as well as encryption and decryption. Resizable and key blocks of data [21]. The steps are shown below [22]:

4.2.1 KEY GENERATION

1. Select two prime numbers p and q .
2. Compute $n = p * q$
3. Compute the Euler's function $\phi(n) = (p - 1)(q - 1)$
4. Collect a random integer e where $1 < e < \phi(n)$ such that $\text{GCD}(e, \phi(n)) = 1$
5. Compute integer d , $1 < d < \phi(n)$ using the relation $e.d \equiv 1 \pmod{\phi(n)}$
6. Send public key (e, n)
7. Send private key (d, n)

4.2.2 ENCRYPTION

Encrypting the a plaintext, M using the public key e as,

$$C = M^e \pmod{n}$$

4.2.3 DECRYPTION

The encrypted text is decrypted using the private key d as,

$$D = C^d \pmod{n}$$

Figure 4 shows RSA encryption and Decryption algorithm.

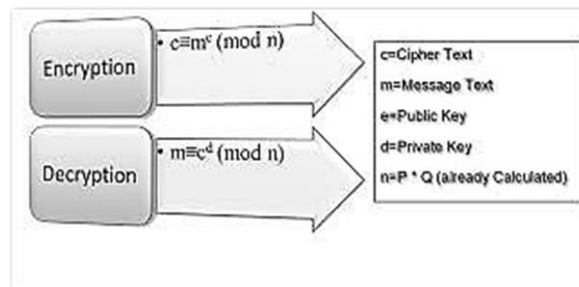


Figure 4. RSA Encryption and Decryption Algorithm [23]

4.3 FUZZY STREAM ALGORITHM (FSA)

FSA is the transformation of clear data into fuzzy data through the use of a set of fuzzy logic rules to produce random sequences with high characteristics. Through the use of membership functions, the resulting blurring is removed from the outputs to which the fuzzy principle has been applied [24]. The goal of using the fuzziness principle in encrypting data is to increase complexity and simulate randomness. To generate large amounts of key flow, streaming ciphers require pseudorandom generators by making the key flow periodic. By using a short switch, the long periodic switch current can be reproduced. Since long random bit strings are difficult to obtain, in most cryptographic applications you must be satisfied with a pseudorandom sequence. A PRNG is an efficient algorithm that takes truly random short key bits as input known as seeds and produces a long key stream as output. Every statistical test passed by PRNG shows that the generator does not have a particular statistical weakness. Firstly, the maximum period length of the sequence obtained from the driving part of Linear Feedback Shift Registers (LFSRs) and secondly, the highly nonlinear order of the fuzzy sum functions. They are considered two basic variables in the design of fuzzy rules. There are two types of memory vector stores M_0 , M_1 , and if-then fuzzy rules. Each storage contains two fuzzy variables that are created by the membership function F and the membership function R . Figure 5 illustrates FSA algorithm [25].

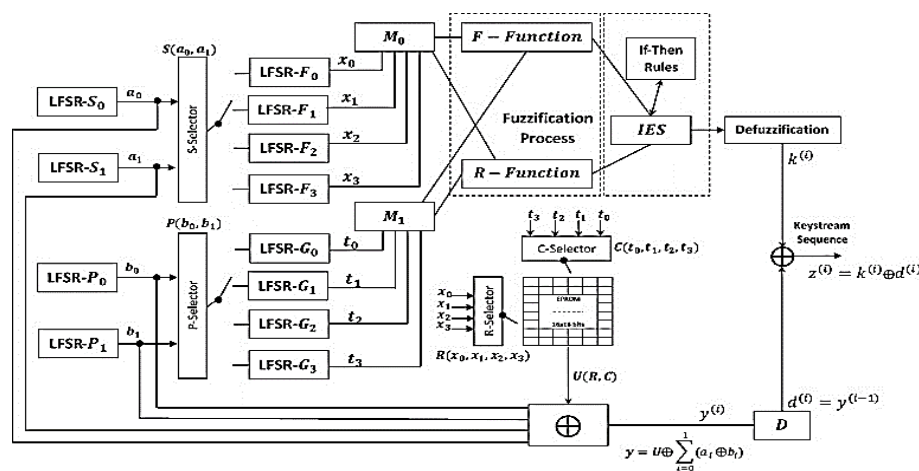


Figure 5. FSA algorithm [25]

4.4 LSB TECHNIQUE

LSB is the most common technology today in information cloaking, which means hiding information in the least important bits in the bit sequence [26]. Researchers in this technique have developed this technique by enhancing its capacity and lack of Perception and durability. To mask the data we use the least significant bits. We take eight bits from the secret byte and replace the smallest part of a string of eight binary sequences of the wrapper data with these secret bits and the process repeats until the secret data is successfully embedded. For example, if we want to hide the secret data, we have an eight-bit binary wrapper sequence of 1 byte 01101100 and a secret bit of 1, where we replace the LSB bit of the wrapper binary sequence with the secret bit, and the value of the wrapper binary sequence becomes 01101101 [27].

5. HYBRID SYSTEM

In this paper, a hybrid system for hiding information using JPEG color images will be developed. This system consists of three layers: the first is the encryption level, which includes the combination of modified AES-RSA encryption algorithms, which aims to increase the algorithm's complexity and thus achieve a high level of security. In the second is FSA level, which added more complexity to the system, making it difficult for the attacker to break and access the original information. The third layer is the LSB level, which hides the encrypted information inside the JPEG color images. Figure 6 shows a general diagram of a hybrid system.

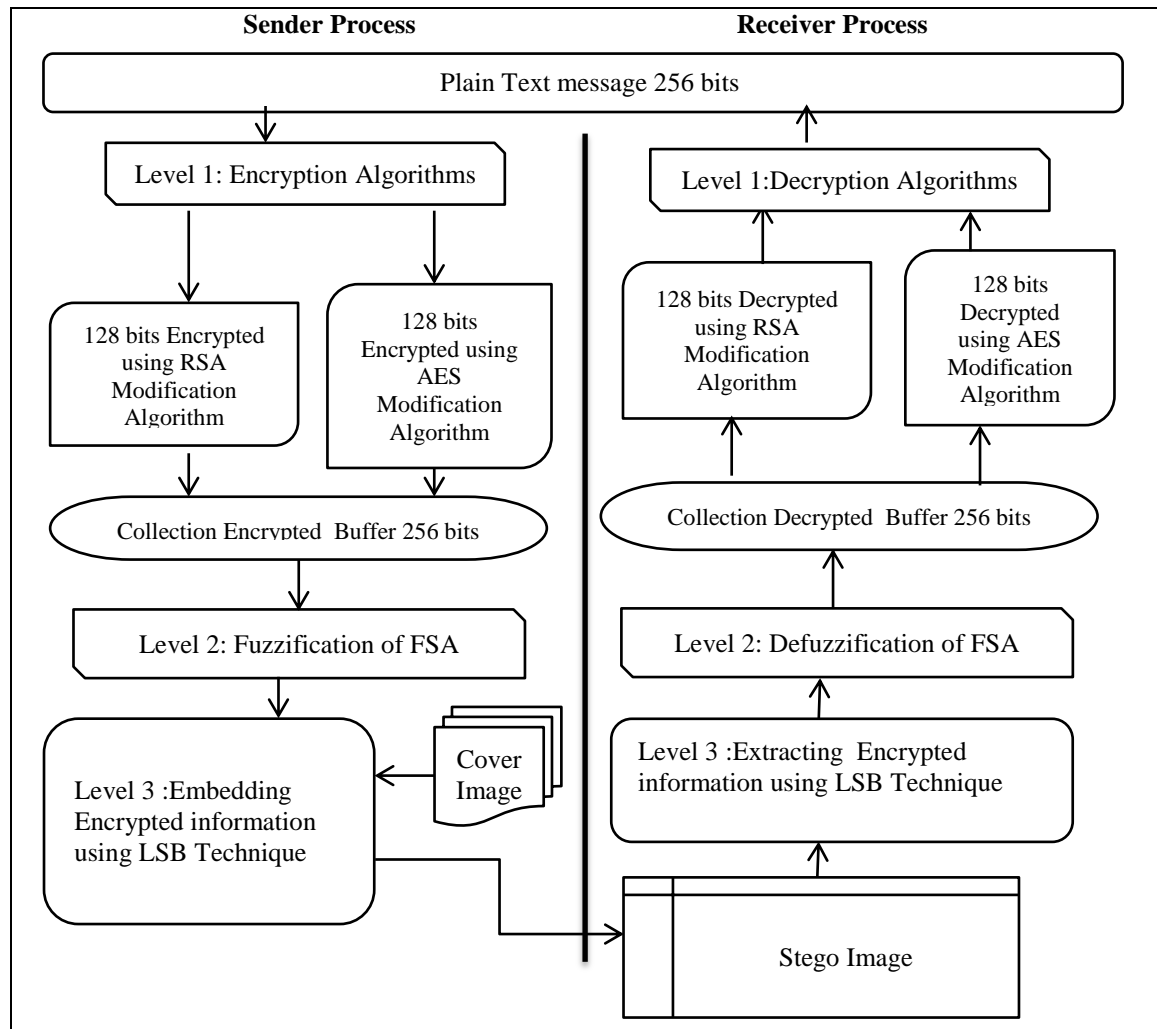


Figure 6. General Diagram of Hybrid System

5.1 SENDER PROCESS

5.1.1 LEVEL 1: ENCRYPTION ALGORITHMS (MIXING OF AES & RSA MODIFICATIONS ALGORITHMS)

The first level is the encryption of information where the 256-bit clear text is divided into two parts: the first part of 128 bits is encrypted using the modified AES algorithm with a symmetric key, where (four S-boxes) were added to generate the keys for this algorithm, and (four S-boxes) were also added in addition to the data encryption for this algorithm, where this process was added to increase the computational complexity of this algorithm, making it difficult for an attacker to hack and attack it. The second stage in this step is the encryption of information where the second part of 128 bits is encrypted using the modified RSA algorithm with two keys, thus adding a layer of complexity to the hybrid system. Figure 7 shows the encryption level.

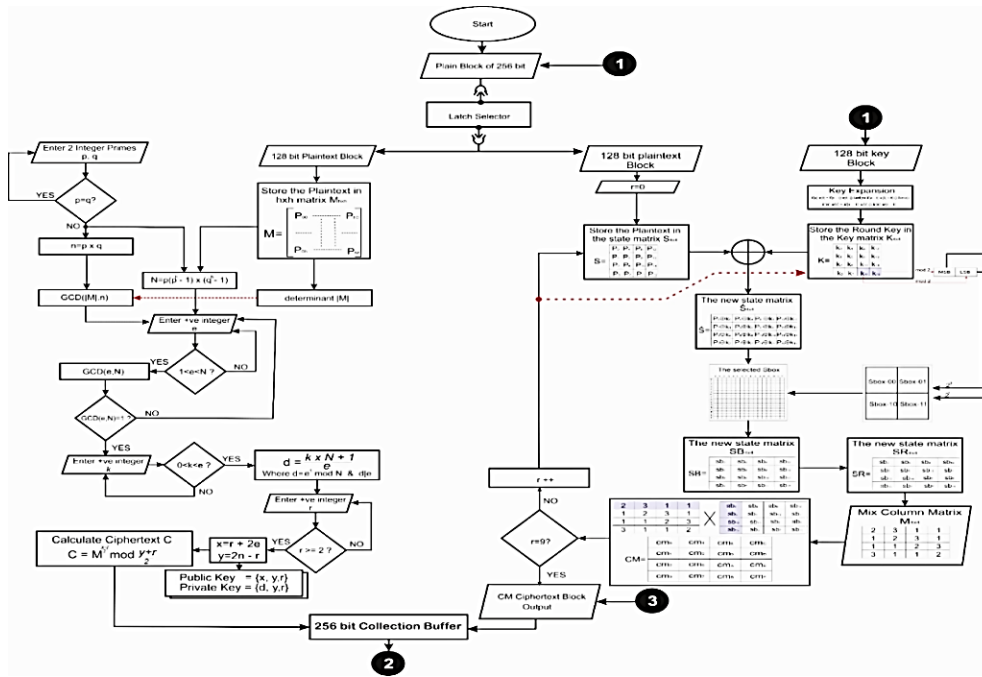


Figure 7. Encryption Algorithms Level

5.1.2 LEVEL 2: FUZZIFICATION OF FSA LEVEL

The second level, the fuzzification of FSA was used to increase the ambiguity and complexity in encoding the data, through the use of a specific set of rules for the fuzzy logic, where the aim of using the fuzzy logic algorithm was to increase the complexity of the data and add a layer to protect the hybrid system as well as eliminate non-linearity. Figure 8 shows the FSA algorithm level.

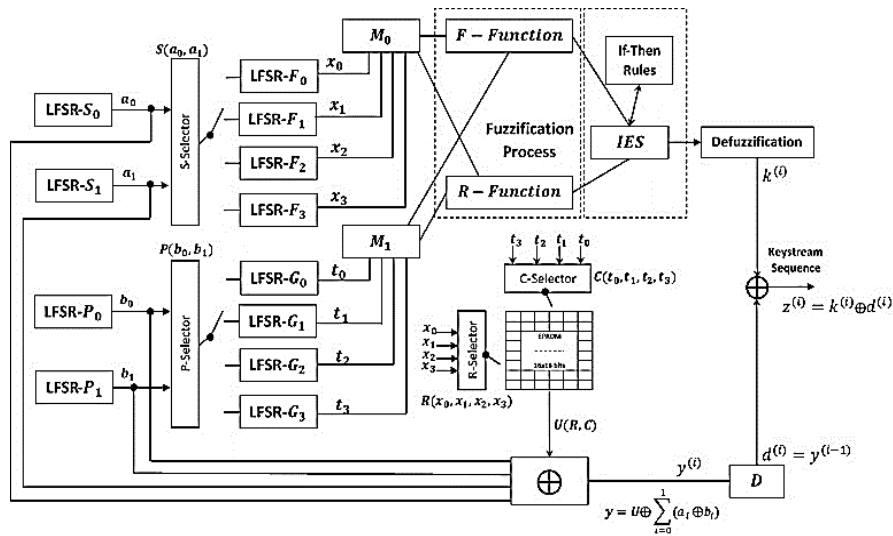


Figure 8. Fuzzification of FSA

5.1.3 LEVEL 3 : EMBEDDING ENCRYPTED INFORMATION USING LSB TECHNIQUE

The third level in this system includes the embedding of encrypted information using the LSB technique, where the information is hidden in LSB in the bit sequence so that there is no significant

interference with the information. The goal of this method is to protect the information and make it invisible and thus difficult to hack. Figure 9 shows the general diagram of the hybrid system. Figure 9 shows the LSB technique level.

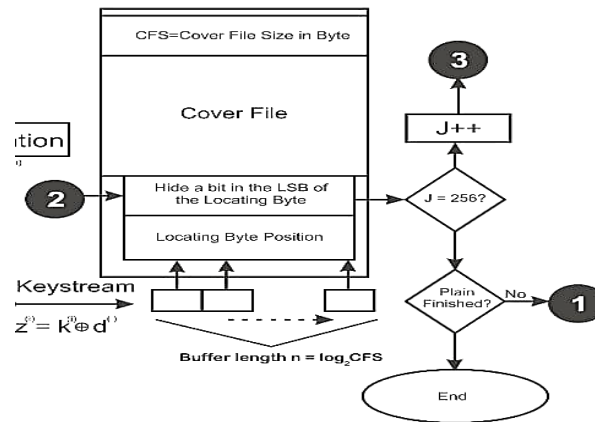


Figure 9. LSB Technique Level

5.2 RECEIVER PROCESS

5.2.1 LEVEL 1: DECRYPTION ALGORITHMS (MIXING OF AES & RSA MODIFICATIONS ALGORITHMS)

The first level is the decryption of information where the 256-bit encrypted text is divided into two parts: the first part of 128 bits is decrypted using the modified AES algorithm with a symmetric key, where (inverse four S-boxes) were added to generate the keys for this algorithm, and (inverse four S-boxes) were also added in addition to the data decryption for this algorithm, where this process was added to increase the computational complexity of this algorithm, making it difficult for an attacker to attack it. The second stage in this step is the encryption of information where the second part of 128 bits is decrypted using the modified RSA algorithm with two keys thus to get the plain text message 256 bits size.

5.2.2 LEVEL 2: DEFUZZIFICATION OF FSA LEVEL

The second level, FSA defuzzification, was used to remove the ambiguity and complexity in encoding data at this level using a specific set of rules for fuzzy logic.

5.2.3 LEVEL 3: EXTRACTING ENCRYPTED INFORMATION USING LSB TECHNIQUE

The third level in this system includes the extracting of encrypted information using the LSB technique, where the information is hidden in LSB in the bit sequence so that there is no significant interference with the information.

6. SAMPLE STEGO IMAGES

In the system proposed by this research, four color images with a size of 512 * 512 pixels (.jpeg) were selected from a database, to be suitable covers for the information to be hidden inside, and the figure 10 shows these images.

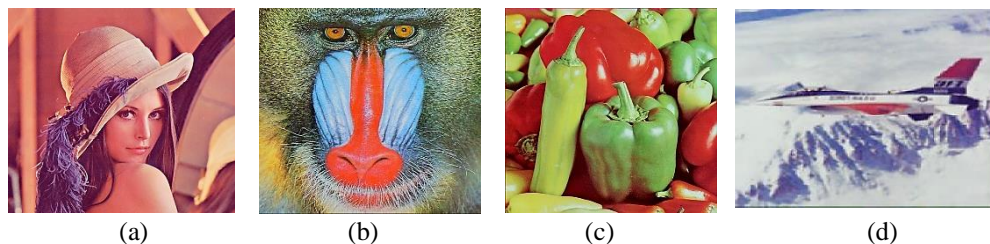


Figure 10. sample stego Images : (a) Lena (b) Baboon (c) Pepper (d) F16 [18] [20]

7. QUANTITATIVE ANALYSIS

There are many parameters used to test and know the sobriety of the hybrid system based three level to hide information using JPEG color images and the most prominent of these parameters are:

7.1 PSNR: it used to measure the quality of images before applying the current system and to measure the quality of images after applying the hybrid system, and it can be calculated by the following equation[28]:

$$PSNR = 10 \log_{10} \left[\frac{Max^2}{MSE} \right] \quad (1)$$

Where, max represents the maximum possible value of pixel in the image, and MSE is represents the Mean Square Error.

7.2 MSE: It used to measure the average error size between the image in the current system mode, and the image in the hybrid system mode, and it can be calculated by the following equation[29]:

$$MSE = \frac{1}{[R \times C]^2} \sum_{i=0}^n \sum_{j=1}^m (X_{ij} - Y_{ij})^2 \quad (2)$$

Where R and C are the number of rows and columns in the cover of image, X_{ij} is the intensity of the X_{ij} pixel in the cover of image, and Y_{ij} is the intensity of the Y_{ij} pixel in stego-image.

7.3 SSIM: Its measures the structural similarity between two of images. Ranges of values between -1 and 1. When two images nearly identical, their SSIM is close to 1. Accordingly. Formula is used to compute the SSIM between two of sequences sq1 and sq2 at a given pixel [30]:

$$SSIM = \frac{2 * \mu_1(p) \mu_2(p) + c_1}{\mu_1(p)^2 + \mu_2(p)^2 + c_1} \times \frac{2 * cov(p) + c_2}{s_1(p)^2 + s_2(p)^2 + c_2} \quad (3)$$

7.4 Correlation: it measures the similarity or discrimination between two signals or vectors in phase and magnitude, where the value of this indicator lies between -1 and 1, and it can be calculated by the following equation [31] :

$$Correlation = \frac{n \sum xy - (\sum x)(\sum y)}{\sqrt{n(\sum x^2) - (\sum x)^2} \sqrt{n(\sum y^2) - (\sum y)^2}} \quad (4)$$

Where, n is the number of pairs of data, x is the input image and y is the stego image.

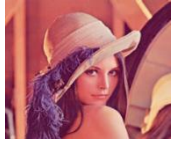



8. EVALUATION AND DISCUSSION OF RESULTS

In this experimental section, we conducted an experiment on colored images using the variable expansion and elastic modulus function and performed different simulations to evaluate the performance of the proposed method. A set of RGB images was applied for this purpose, where the masking was performed on a sample of images selected from the database, and these covers were (512*512) pixels, and all experiments of the proposed method were implemented by using Microsoft Visual Studio Community 2022 platform (64 bit), version 17.6.5 Visual Basic language to build the algorithms, under Windows 10 64 bit, Intel(R) Core(TM) i7-3230M CPU @ 2.60GHz, 8 GB DDR3 RAM and HDD SSD are the specifications of the device used. In this proposed system, the analysis was applied to know the PSNR and MSE test, and the histogram of the three covers was analyzed, and these results were also compared with previous studies.

8.1 ANALYSIS PSNR AND MES

In this paper, the hybrid method was applied to four-color image covers (Lena, Baboon, Pepper, F16) with a size of 512 * 512 RGB pixels (.jpeg) to hide the information inside them. Parameters were used, namely PSNR, which means signal-to-noise ratio, as well as MES, which means the difference between the original image and the stego image. The experimental results of these method shows that the overall PSNR value is large, and it shows the superior imperceptibility of the PSNR of the original images after the confidential data is embedded in them. , the visual appearance of the cached images looks better while the changes in the cover image are difficult to change according to the embedded secret data and also the MSE parameter has been applied and the results of information hiding in JPEG covers is difficult to recognize or detect by human vision. Table 2 shows results evolution of the proposed system.

Table 2. Results Evaluation of the Hybrid System

No. of Cover images	Cover images (512*512) RGB	Hidden Data in Bits	PSNR	MSE	SSIM	Correlation
1.	 Lena.jpeg (512*512)	1,635,241	70.45	1.75	1	1
2.	 Baboon.jpeg (512*512)	1,550,332	68.68	1.45	1	1
3.	 Pepper.jpeg (512*512)	1,462,582	67.74	1.34	1	1
4.	 Plan.jpeg (512*512)	1,393,974	65.36	1.18	1	1

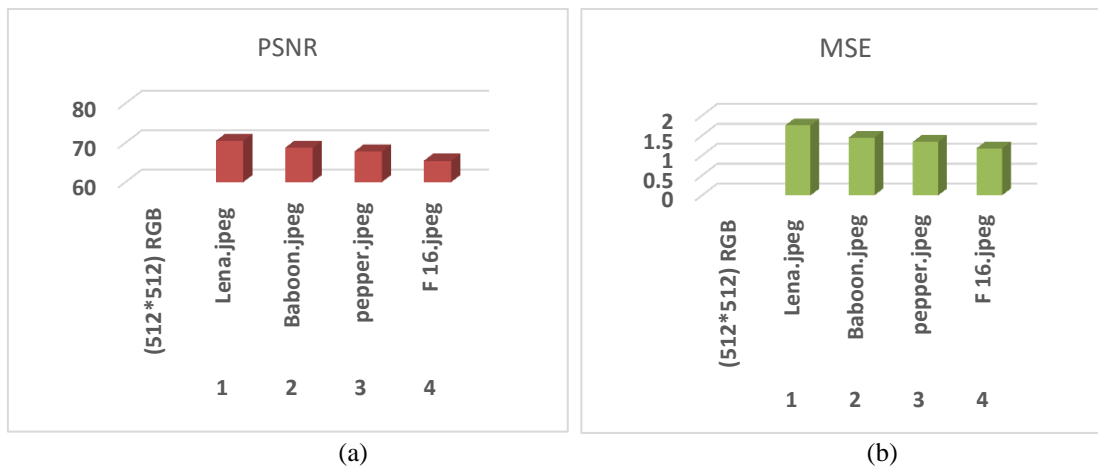

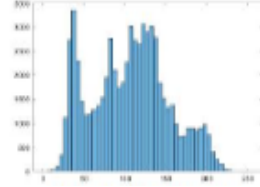
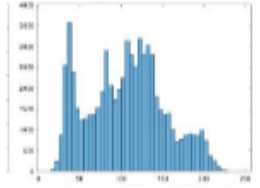

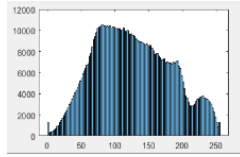
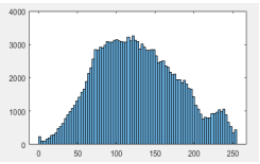

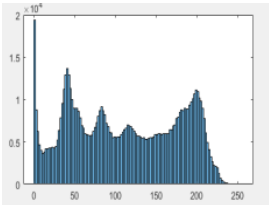
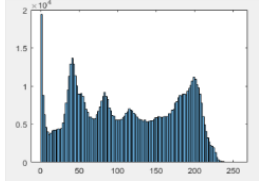

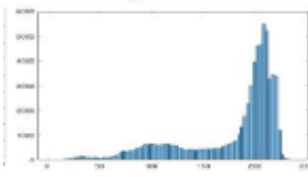
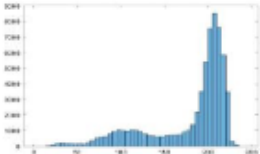


Figure 11. Results Evaluation of the Hybrid System: (a) PSNR (b) MSE

8.2 ANALYSIS HISTOGRAM FOR PIXELS DIFFERENCES

In this paper, the hybrid system was applied to hide information inside the covers of selected colored images within a database with dimensions of 512*512 (Lena, Baboon, Pepper and F16) with (.jpeg) format. The results were analyzed using a pixel histogram, which is one of the most common methods for analyzing secret data inside hidden images. The pixel difference histogram is calculated by adopting the differences of neighboring pixels with the incident series between the cover containing the hidden information and the original image. It turns out that there is a slight difference in the image that cannot be easily explained by the human eye. However, there is some change in image quality after text is included in it. To check how much the image changed after steganography, we calculated the difference between them. Table 3 shows the analysis histogram for original images and stego images.

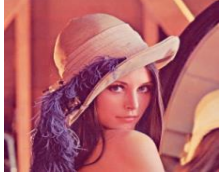
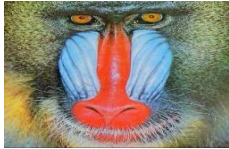


Table 3. Analysis of Histogram for original and stego images

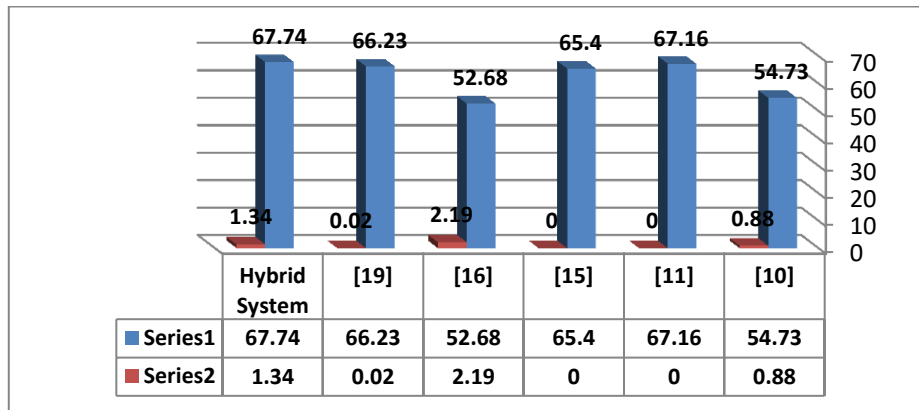
No. of Cover images	Cover images (512*512) RGB	Histogram for original image	Histogram for stego image
1.	 Lena.jpeg (512*512)		
2.	 Baboon.jpeg(512*512)		
3.	 Pepper.jpeg (512*512)		
4.	 F16.jpeg (512*512)		

8.3 COMPARISON OF THE HYBRID SYSTEM WITH PERVIOUS SYSTEMS

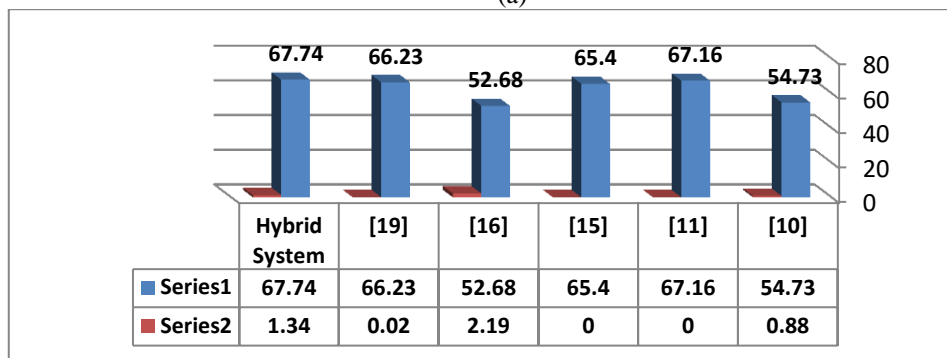
In this paper and through the application of the proposed method to hide information inside colored images, which are four images (Lena, Baboon, Pepper, F16) 512 * 512 pixels, where we made comparisons of this study with other previous studies [10] [11] [14] [15] [16] [19], and it was found that our study was much better in terms of the high value of PSNR and it was the value of MSE is low, the experimental results indicate that the use of color images in the proposed method provides better visual quality and embedding ability than other methods. Table 4 shows the compression results evaluation of the previous studies with hybrid System.

Table 4. Comparison Results Evaluation of the Previous Studies with Hybrid System

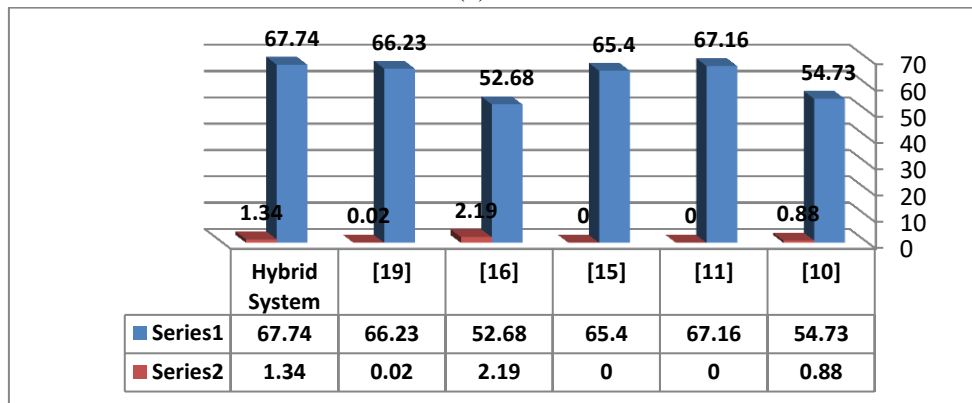
No. of Cover images	Cover images (512*512) RGB	Existing Systems	Hidden Data in bits	PSNR	MSE	SSIM	Correlation
1.	 Lena.jpeg (512*512)	Shanthakumari and Smalliga, 2019 [10]	638,976	54.85	0.85	0.99	-
		Ansari et al., 2020 [11]	286,720	66.67	-	-	-
		Tang et al. 2021 [15]	655,360	65.7	-	0.99	-
		Zulqarnain et al. 2021 [16]	1,263,354	54.74	1.89	-	-
		Hameed et al. [19]	401,408	66.02	0.0177	0.98	-
		Hybrid System	1,635,241	70.45	1.75	1	1
2.	 Baboon.jpeg(512*512)	Shanthakumari and Smalliga, 2019 [10]	638,976	54.62	0.90	0.99	-
		Ansari et al., 2020 [11]	286,720	69.45	-	-	-
		Tang et al. 2021 [15]	485,752	66.9	-	1	-
		Zulqarnain et al. 2021 [16]	1,420,631	46.37	2.06	-	-
		Hameed et al. [19]	401,408	67.84	0.018	0.98	-
		Hybrid System	1,550,332	68.68	1.45	1	1
3.	 Pepper.jpeg (512*512)	Shanthakumari and Smalliga, 2019 [10]	638,976	54.73	0.88	0.98	-
		Ansari et al., 2020 [11]	286,720	67.16	-	-	-
		Tang et al. 2021 [15]	655,360	65.4	-	0.99	-
		Zulqarnain et al. 2021 [16]	1,185,126	52.68	2.19	-	-
		Hameed et al. [19]	401,408	66.23	0.02	0.98	-
		Hybrid System	1,462,582	67.74	1.34	1	1
4.	 F16.jpeg (512*512)	Zulqarnain et al. 2021 [14]	1,253,349	54.08	1.74	-	-
		Hybrid System	1,393,974	65.36	1.18	1	1



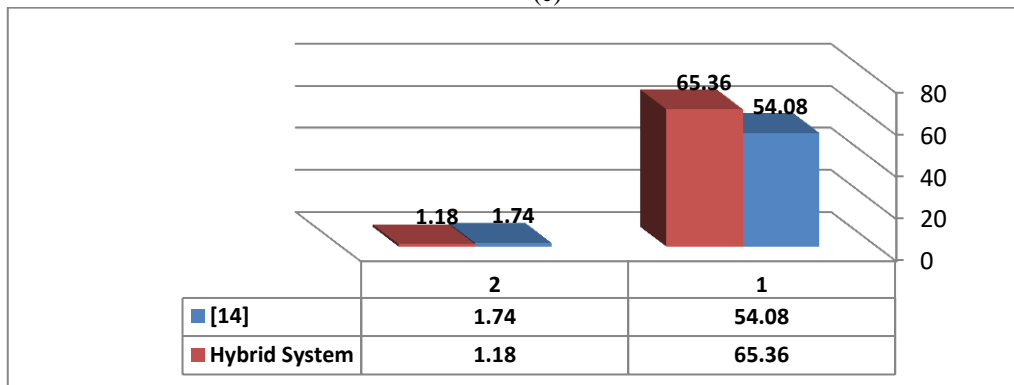
(a)



(b)



(c)



(d)

Figure 12. Comparison Results Evaluation of the Previous Studies with Hybrid System: (a) Lena (b) Baboon (c) Pepper (d) F-16

9. CONCLUSION











In this paper, a hybrid system based on three levels to hide information using JPEG color images, where this system works in both processes sender and receiver. The sender process at the first level uses a mixing of the AES and RSA, while at the second FSA level adds a higher complexity and eliminates the non-linearity of the encrypted information. The third level is to hide encrypted information using LSB technique, while the receiver process, performs the reverse process of three levels. This system provides high information embedding capability and the inability to perceive hidden information, the system was evaluated based on criteria like PSNR, MSE, SSIM, and correlation, which were characterized by high and good rates. The study was compared with modern steganography techniques.

REFERENCES

- [1] I. Kamil and M. A. Al-Askari, "A new approach to prediction of memory leak in high-performance computing (HPC) using message passing interface (MPI)," *International Journal of Advanced Studies (IJAS)*, vol. 3006, pp. 5828, 2024. [Online]. Available: <https://ijas.uodiyala.edu.iq/index.php/IJAS/index>. [Accessed: Sept. 16, 2024].
- [2] T. Zong, Y. Xiang and L. Natgunanathan, "Histogram Shape-based Robust Watermarking Method," in *IEEE International Conference on Communication (ICC)*, Sydney, NSW, Australia, 2014.
- [3] M. Rajkamal and B. Zoraida, "Image and Text Hiding using RSA & Blowfish Algorithms with Hash-LSB Techniue," *International Journal of Innovative Science, Engineering & Technology*, vol. 1, no. 6, pp. 81-89, 2014.
- [4] L. K. Yee and C. C. Wen, "Secret Channel Using Video Steganography," *International Journal on Informatics Visualization*, vol. 1, no. 4-2, pp. 240-245, 2017.
- [5] I. Alsaadi, N. S. Mohammed, and S. S. Mohammed, "Optimizing skin disease diagnosis using metaheuristic algorithms: A comparative study," *Iraqi Journal for Applied Sciences*, vol. 1, no. 1, pp. 72-80, 2024.
- [6] C. E. Andrews and L. T. Joseph, "An Analysis of Various Steganographic Algorithms," *International Journal of Advanced Research in Electronic and Communication Engineering (IJAREC)*, vol. 2, no. 2, pp. 116-123, 2013.
- [7] A. Uhl and A. Pommer, "Application Scenarios for the Encryption of Still Visual Data," *Advances in Information Security*, pp. 31-43, 2005.
- [8] K. Aishwary and A. Goyal, "Image Steganography using Dynamic LSB with Blowfish Algorithm," *International Journal of Computer & Organization Trends*, vol. 3, no. 4, pp. 10-13, 2013.
- [9] S. Yasser, "Stego Crypt: Arithmetic and Rudin- Shapiro Sequence- Based Bit Cycling and Blowfish," *The German University in Cairo, Cairo*, 2019.
- [10] R., Shanthakumari, and S. Malliga. "Dual-layer security of image steganography based on IDEA and LSBG Algorithm in the Cloud Environment" *Sādhanā* 44.5:pp. 119, 2019.
- [11] A. S. Ansari, M. S. Mohammadi and M. T. Parvez, "A Multiple Format Steganography Algorithm for Color Images," *IEEE Access*, vol. 8, no. 3, pp. 83926-83939, 2020.
- [12] H. R. Kareem, H. H. Madhi and K. A.-A. Mutlaq, "Hiding Encryption Text in Image Steganography," *Periodicals of Engineering and Natural Science (PEN)*, vol. 8, no. 2, pp. 703-707, 2020.
- [13] R. Sindha and P. Singh, "Information Hiding using Steganography," in *4th National Conference of Telecommunication, Universiti Teknologi Malaysia*, 2021.
- [14] S. G. Chalooop and M. Z. Abdullah, "Enhancing Hybrid Security Approach using AAES and RSA Algorithms," *Journal of Engineering and Sustainable Development*, vol. 25, no. 4, pp. 58-66, 2021.
- [15] L. Tang, D. Wu, H. Chen, H. Wang and J. Xie, "An Adaptive Fuzzy Inference Approach for Color image Steganography," *Soft Computing*, vol. 25, no. 16, pp. 10987-11004, 2021.
- [16] M. Zulqarnain, M. G. Ghouse, S. Wareesa, J. Ghulam and S. Amna, "An Efficient Method of Data Hiding for Digital Color Images Based on Variant Expansion and Modulus Function," *Journal of Engineering Science and Technology*, vol. 16, no. 4, pp. 4160-4180, 2021.
- [17] H. Abroshan, "A Hybrid Encryption Solution to Improve Cloud Computing Security and Asymmetric Cryptography Algorithms," *International Journal of Advanced Computer Science and Applications*, vol. 12, no. 6, pp. 31-37, 2021.
- [18] M. A. Naser, S. M. Al-alak, A. M. Hussein and M. J. Jawad, "Steganography and Cryptography Techniques Based Secure Data Transferring Through Public Network Channel," *Baghdad Science Journal*, vol. 19, no. 6, pp. 1362-1368, 2022.
- [19] R. S. Hameed, S. S. Mokri, M. S. Taha and M. M. Taher, "High Capacity Image Steganography System Based on Multi-layer Security and LSB Exchanging Method," *International Journal of Advanced Computer Science and Applications*, vol. 13, no. 8, pp. 108-115, 2022.
- [20] M. M. Abd Zaid and S. Hassan, "Modification Advanced Encryption Standard for Design Lightweight Algorithms," *Journal of Kufa for Mathematics and Computer*, vol. 6, no. 1, pp. 21-27, 2019.
- [21] N. A. P. M. S and S. K. J, "Modified RSA Encryption Algorithm using Four keys," *International Journal of Engineering Research & Technology (IJERT)*, vol. 3, no. 7, pp. 1-5, 2015.
- [22] S. O, "Enhancing RSA Security Capability using Public Key Modification," *International Journal of Research and Scientific Innovation (IJRSI)*, vol. VI, no. IX, pp. 10-15, 2020.
- [23] D. MADHURI, G. Annapurna, C. Venkataramana and G. Swetha, "Text Hiding Using RSA and Blowfish Algorithms with Hash-Based LSB Technique," *International Journal of Management, Information*, vol. 3, no. 4, pp. 5-12, 2015.
- [24] M. Ashfaq, "'A Tribute to Father of Fuzzy Set Theory and Fuzzy Logic'," *International Journal of Swarm Intelligence and Evolutionary Computation*, vol. 7, no. 2, pp. 3-5, 2018..
- [25] L. Dzitac, F. G. Filip and M.-J. Manolescu, "Fuzzy Logic Is Not Fuzzy: World-Renowned Computer Scientist Lotfi A.Zadeh," *International Journal of Computers Communications & Control*, vol. 12, no. 6, pp. 748-789, 2017.

- [26] N. M. Al-Aidroos and H. A. Bahamish, "Image Steganography Based on LSB Matching and Image Enlargement," International Journal of Engineering Research and Technology, vol. 1, pp. 1-7, 2012.
- [27] M. Mohamed, M. A. Mofaddel and T. Y. Abd El-Naser, ""Comparison Study between Simple LSB and Optimal LSB Image Steganography"," Sohag Journal of Sciences 8.1, pp. 29-33, 2023.
- [28] N. F. Johnson and S. Jajodia, Exploring Steganography: Seeing Unseen, George Mason University, 1998.
- [29] F. A. Jassim, "A Novel Steganography Algorithm for hiding text in image using five modulus Method," International Journal of Computer Applications., vol. 72, no. 17, pp. 39-44, 2013.
- [30] S. Bandi and M. Reddy, "Combined Audio Steganography and AES Encryption to hide text and image into audio using DCT," International Journal Recent Technol Eng, pp. 1732-1738, 2019.
- [31] S. A. Al-mola, N. H. Qasim and H. A. A. Alasadi, "Robust Method for Embedding an Image Inside Cover Image Based on Least Significant Bit Steganography," Informatica 46.9, vol. 46, no. 9, pp. 53-60, 2023.

BIOGRAPHIES OF AUTHORS

	<p>Mr. Ali Mahmood Khalaf Born in Iraq, Baghdad 1989. He received the B.Sc. degree in computer science from the University of Tikrit in 2011, IRAQ, and M.Sc. degree in Computer Science at Pune University in 2019, INDIA. He is a Ph.D. research scholar at Gujarat university College of Science in Computer Science Department, INDIA, with specialization in Cyber Security/ Information Security. His research areas are Information Technology (IT), Mobile Applications, Cyber Security, Information Security. He has published several scientific papers in national, international conferences and journals. He can be contacted at email: alikhalf@gujaratuniversity.ac.in</p> <p>Scopus®    </p>
	<p>Dr. Kamaljit Lakhtaria is Associate Professor at College of Science, University of Gujarat, INDIA. He Holds a PhD degree in Computer Science, at Saurashtra University in 2010, INDIA. His research areas are Information Technology (IT), Security, Network Security, Mobile Applications. He has published several scientific papers in national, international conferences and journals. He can be contacted at email: kamaljit.lakhtaria@gujaratuniversity.ac.in</p> <p>Scopus®    </p>