AJMS
Asian Journal of Mathematical Sciences

RESEARCH ARTICLE

A PROPOSED SYSTEM TO HIDE INFORMATION BASED FOUR ALGORITHMS FOR IMAGE STEGANOGRAPHY

***Ali Mahmood Khalaf, Dr. Kamaljit Lakhtaria[1]**

[*,1]*Department of Rollwala Computer Science, Gujarat University,Gujarat Universit, Ahmadabad, Gujarat, India*

Corresponding Email: alikhalaf@gujaratuniversity.ac.in

Received: 15-06-2023; Revised: 25-07-2023 ; Accepted: 10-08-2023

ABSTRACT

Nowadays, protecting important information, such as images, audio and video files, has become a matter and must be protected from hacking because the circulation of this information takes place through unsecured communication channels. Scientists have discovered many of these techniques to protect information, such as: cryptography and steganography. In this research, a proposed system to hide information based four algorithms for image steganography. The first step using AES modified algorithm, while in the second step using RSA modified algorithm to increase the complexity and high security. The third step fuzzy stream algorithm was used to increase the complexity and eliminate on the non-linearity of the encrypted information. Third step apply LSB technique was used, which is the technique of hiding the information. This system provides a high ability to include information and an inability to perceive hidden information through the use of a many of indicators and PSNR, MSE and SSIM and that were characterized by high and good rates with modern hiding techniques.

Keywords: Cryptography, Steganography, FS algorithm, RSA Modified, AES Modified.

INTRODUCTION

Sensitive information at the present time, such as: banking services, online shopping, paying bills, and military information, all of this information has expanded due to the progress in the possibility of the Internet and the spread of this data easily in cyberspace and making this information available to all people has claimed to be increasing threats to privacy, as the necessity has called for Protect this information and make it encrypted and completely private to ensure its confidentiality and integrity. No one can access this information except through persons authorized to access the original information. Among the important techniques to protect this information and to avoid it from being hacked are: cryptography and steganography [1][2].

Cryptography

The principle of cryptography is one of the requirements of wartime. It is the process of converting plain text into unreadable text (encrypted) for people who are not authorized to access the original information, using different encryption algorithms. The principle of encryption is the encryption of the original data by the sender and it cannot be decoded in some cases. It is very difficult to hack it except by the person receiving it using the encryption key. There are five goals to achieve successful encryption: authentication, which means verifying the information and its validity, privacy, which includes data privacy and transfer, integrity, which is that the information is protected against the unauthorized person accessing this information, and integrity, which means the integrity of the information. To ensure that it is not modified, in addition to the absence of denial non-repudiation between the sender and the recipient, and they cannot conflict about sending the message [3][4][5].

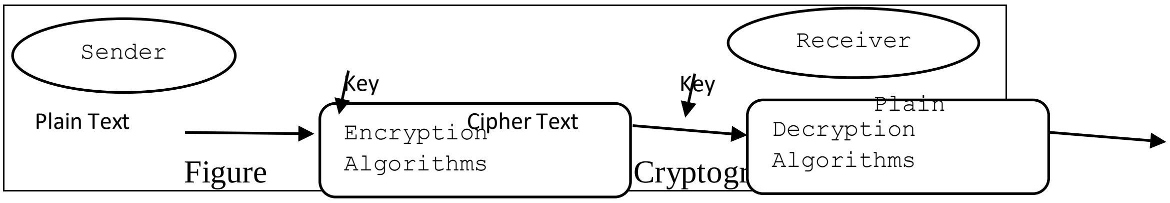


Figure Cryptogr

Steganography

Steganography is a Greek word that was used by the scientist Johannes Trithemius in 1499. It means "hidden writing", and in other words it means "covered writing". Steganography is considered one of the techniques of hiding information, as its concept is carried out by transferring a secret message from the sender to The recipient via a digital transmission medium (text, image, audio, video) so that it does not raise suspicion for the person who wants to know the existence of the original message. There are many ways to hide information, including [6]:

1. Spatial Domain Technique
2. Frequency Domain Technique
3. Spread Spectrum
4. Statistical Technique
5. Masking and Filtering
6. Vector Embedding
7. Distortion of Technique

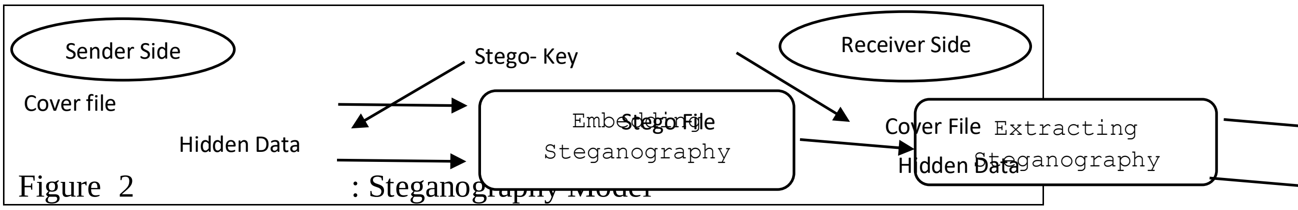


Figure 2 : Steganography Model

LITERATURE REVIEW

ALabaichi et al. [7] "Image steganography using least significant bit and secret map techniques."In this paper, a new method was proposed for hiding information using mapping techniques and hiding information with the least significant bits. It showed good results for the proposed algorithm and proved its resistance to external attacks through the use of a number of indicators and comparing it with similar algorithms.

Chaloop and Abdullah [8] "Enhancing Hybrid Security Approach Using AES And RSA Algorithms" . This paper 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 results of this paper showed that the hybrid security algorithm is better in terms of security.

Zulqarnain et al [9] "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. From the results of experimental for the research, we prove that the developer method obtains a higher capacity with a peak PSNR signal ratio 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 [10] "Enhancing Hybrid Security Approach Using AES And RSA Algorithms".In this paper an effective encryption system is proposed to improve security in cloud computing. The hybrid algorithm (Blowfish, ECC) has been improved. The data is encrypted using the Blowfish algorithm, and the elliptic curve algorithm encrypts its key, which will increase security and performance. Moreover, to ensure the integrity of the information, digital signature technology was used, and the results showed an improvement in productivity, execution time, and memory consumption parameters.

Guru and Ambhaikar [11] "AES and RSA-based Hybrid Algorithms for Message Encryption & Decryption”. In this research, a hybrid encryption algorithm that combines AES and RSA algorithms is proposed in this research to overcome the problems between file encryption and security. The experimental results indicate that the hybrid algorithm possesses a high level of security in data encryption.

Naser et al. [12] "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 first step using the RC4 algorithm to encrypt the message, in order to increase the confidentiality of the message, and the second step is to include LSB technique by adding an extra layer of security. Through the technique of replacing sequential selection with random selection of frames and pixels, the improvement in the LSB technology comes so that it is difficult for the attacker to penetrate the information, and the results of the research were good compared to previous studies.

Hameed et al. [13]” 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, NCC, and The proposed method is immune to Graph and chi-square.

Yassin [14] “Data Hiding Technique For Color Images Using Pixel Value Differencing And Chaotic Map. “ In this study, a complex chaotic map is used to select the parameters to embed the secret message. The cover image is transformed through integer wavelet transform (IWT). Adaptive embedding is based on the intensity variation between pairs of pixels using PVD and replacing the least significant bit to make the method safer. Experimental results show a high signal-to-noise ratio with improved capacity compared with other techniques.

Baharudin, et al. [15] "Text Steganography using The Second Quotient Remainder Theorem and dark Colour Schemes." In this research, the green and blue color technique (RGB) was used to obtain the hiding process with the use of the remainder theory (SQRT) to avoid color suspicion with the use of a PRNG also to generate the dynamic hidden messages with the generation of a Homophonic table. The results of this research showed that the secret message can be represented dynamically hiding capacity increased to 77.4%. Otherwise, the specific color succeeds in avoiding the suspicion generated in Stego's text.

Sead el at. [16] "Robust Method For Embedding An Image Inside Cover Image Based On Least Significant Bit Steganography." In this research, an effective safe method was proposed to preserve the original information, which includes two stages. The first stage is to encrypt a secret image using an encryption algorithm in order to increase the security of the information. The second stage, embedding the most significant bits (MSB) of the encrypted image into the least significant bits (LSB) of the cover image to establish the Stego image. One of the most prominent results is that the proposed method which includes encoding and embedding algorithms has an effective role in embedding the secret image and preserving the good visual quality of the stego images. The extraction algorithms had better and faster results to recover the original information.

Srinivasarao et al. [17] “A Smart Strategy for Data Hiding using Cryptography and Steganography“.In this research, a hybrid system was designed based on the use of encryption and information steganography techniques. In the first stage, the "play fair fair" encryption method is used to encrypt the hidden text content, which provides security in terms of the effective level. In the second stage, the techniques of Discrete Cosine Transform (DCT) and Exclusive Boolean OR (XOR) are combined with encrypted messages hidden inside the image. The results of this research were well compared to previous studies.

Sahin [18] “Memristive chaotic system-based hybrid image encryption application with AES and RSA algorithms” .In this paper, we propose a two-stage image encryption model, the first stage is the logistic map, chaotic Lorenz system and memristor-based super similar system, and the second stage with AES and RSA encryption algorithms. The results of this research showed the effectiveness of the proposed image encryption scheme in terms of security, speed, and reliability and provide valuable insights for the development of chaos-based encryption systems in the future. This research was evaluated through statistical tests and compared with previous studies.

PROPOSED WORK

A proposed system to hide information based on four stepsbased four algorithms for image steganography:

1) First Algorithm (AES Modified)

The first step encryption and decryption of information using the modified AES algorithm with a symmetric key, where (Four - S- Boxes) were added to generate the keys for this algorithm, as well as (Four-S-Boxes) were added to the data encryption aspect of this algorithm, where this process was added To increase the computational complexity of this algorithm, as it is difficult for an attacker to crack and attack it.

2) Second Algorithm (RSA Modified)

The second step to encrypt and decrypt the information using the modified RSA algorithm with two keys, thus adding additional complexity to this algorithm.

3) Third Algorithm (Fuzzy Stream)

The third step, the fuzzy logic algorithm 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 and thus it is difficult to The attacker breaks it and accesses the original information.

4) Fourth Algorithm (LSB Technique)

The fourth stepof this system is the technique of steganography in the least significant bits, which is one of the steganography techniques. It is considered the most common technique today in information steganography, which means hiding information in the least important bits in the sequence of bits so that no high interference occurs on the information and thus it is discovered. The aim of this method is to protect the information and make it invisible and therefore difficult to penetrate. Figure 3 shows the scheme of the proposed system.

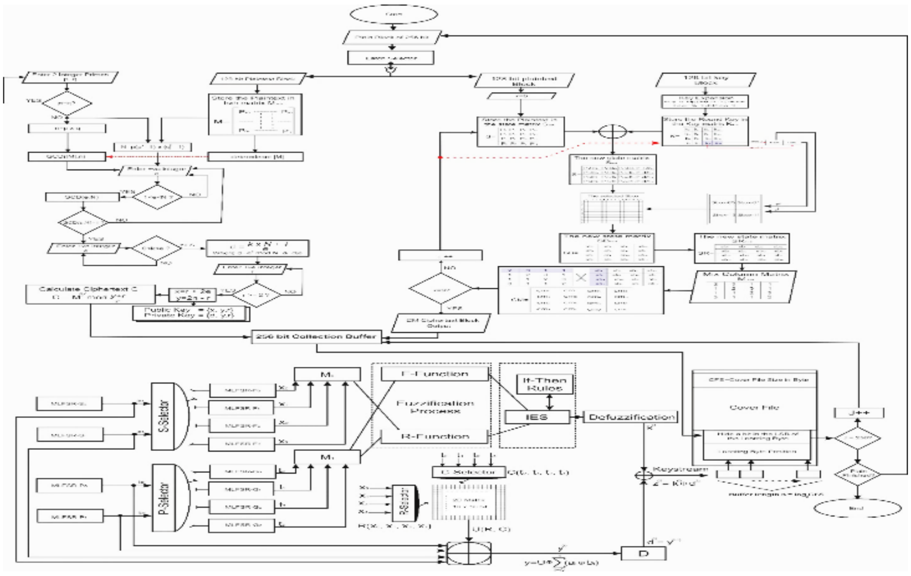


Figure 3- Block Diagram of hybrid System

COVERS SELECTION FILE

In the proposed system, four color images with adifferent images sizes (.bmp) were selected from a database, to be suitable covers for the information to be hidden inside, and the figure 4 shows these images.

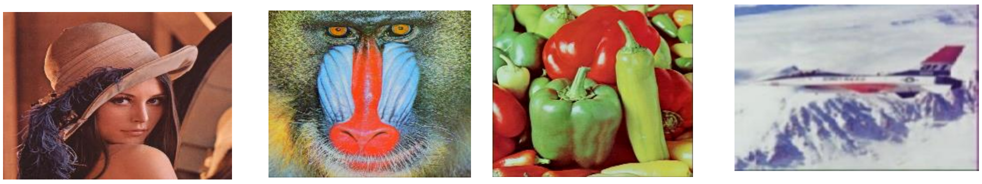

(a) Lena **(b) Baboon** **(c) Pepper** **(d) Jet**

Figure 4- Sample of Covers File

QUANTITATIVE ANALYSIS

There are many parameters used to test and know the sobriety of a hide information based four algorithm for image steganographyand the most prominent of these parameters are:

3.1 *Peak Signal to Noise Ratio (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 [19]:

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

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

3.2 *Mean Square Error (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 [20]:

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

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.

3.3 Structural Similarity (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 [21]

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

RESULTS EVALUATION AND DISCUSSION

In this experimental section, we conducted experiment on colour images to hide information based four algorithms for image steganography to evaluate the performance of the proposed method. A set of RGB images has been applied for this objective. All the experiments of the In this proposed method, the results were evaluated and discussed, where steganography was performed on a sample of images selected from the database, and these images are covers suitable for steganography, and these covers with a different images sizes, uses for the stego-images, All the experiments of the proposed method were implemented through the use of the platform Microsoft Visual Studio Community 2022 (64-bit), Version 17.6.5 Visual Basic language to construct the algorithms, under Windows 10 64-bit, The CPU Intel(R) Core(TM) i7-3230M CPU @ 2.60GHz, RAM 8 GB DDR3 and HARD SSD are the device specifications used.In this proposed system, analysis was applied to find out the PSNR and MSE test, the histogram of the three covers was analyzed, and these results were also compared with previous studies.

1. Analysis PSNR and MES

In this research, the hybrid method was applied to five color image covers (Lena, Baboon, Pepper and Jet) with a different images size (.bmp) 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 of the original image and the stego image.

The experimental results of this 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, 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 are where the concealment is difficult to recognize or detect by human vision. Table 1 shows results evolution of the proposed system.

Table 1 Results Evaluation of the proposed System

No. of Cover images	Name of Covers images with extension	Cover images Sizes	Hidden Data in Bits	PSNR	MSE	SSIM

1.	Lena.bmp	512*512	1,802,240	74.45	0.00095	1
2.	Baboon.bmp	512*512	1,550,332	71.52	0.00087	1
3.	Pepper.bmp	512*512	1,462,582	69.71	0.00061	1
4.	Jet.bmp	512*512	1,331,697	67.73	0.00026	1

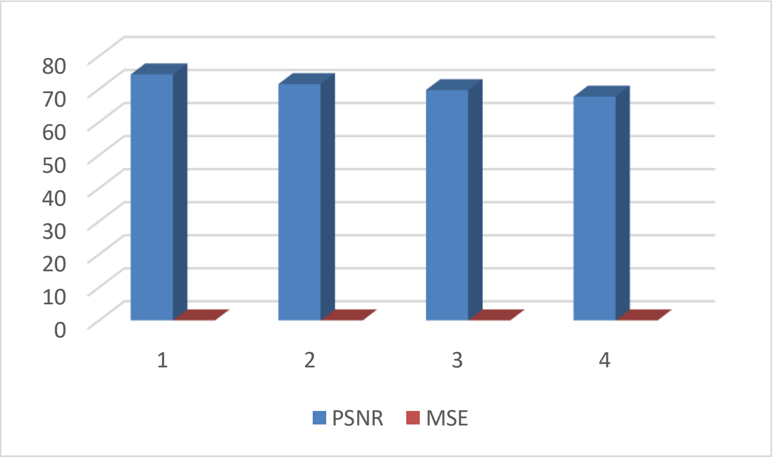
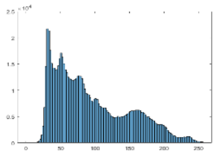
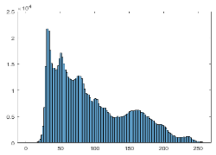
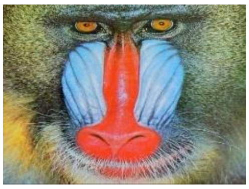
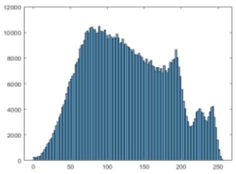
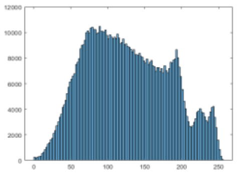
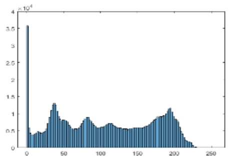
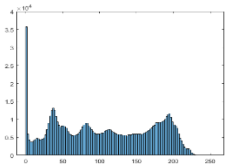
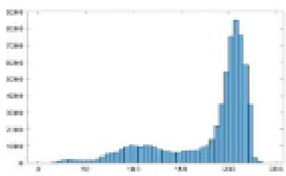
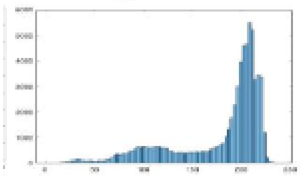


Figure 5- Results Evaluation of the proposed System: PSNR and MSE

2. Analysis Histogram for Pixels Differences

In this research, the proposed system was applied to hide information inside the covers of selected colored images within a database with different dimensions sizes (Lena, Baboon, Pepper and Jet) with (.bmp) file 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 2 shows the analysis histogram for original images and stego images.

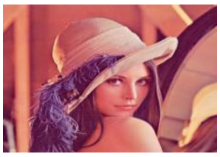
Table 2 Analysis of Histogram for original and stego images

No. of Cover images	Cover Images	Cover Images Sizes	Histogram for original image	Histogram for stego image
1.		Lena.bmp 512*512		
2.		Baboon.bmp 512*512		
3.		Pepper.bmp 512*512		
4.		Jet.bmp 512*512		

3. Comparison of the Hybrid System with pervious Systems

In this research and through the application of the proposed method to hide information inside colored images, which are four images (Lena, Baboon, Pepper and Jet) 512 * 512 pixels, where we made comparisons of this study with other previous studies [15] [13] [7], 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. The table 3 shows that.

Table 3 Compression Results Evaluation of the pervious studies with Proposed System

No. of Cover images	Cover images (512*512) RGB	Existing Systems	PSNR	MSE
1.	 Lena.bmp (512*512)	**Proposed System**	**74.45**	**0.00095**
		[15]	65.459	0.0016
		[13]	50.12	0.63
		[7]	39.1357	2.9967
2.		**Proposed System**	71.52	0.00087
		[15]	68.115	0.00889

	512)	[13]	46.01	1.62
		[7]	45.9012	1.5887
3.	 Pepper.bmp (512*512)	**Proposed System**	69.71	0.00061
		[15]	68.0068	0.0088
		[13]	50.00	0.64
		[7]	45.0216	2.0621
4.	 Jet.bmp (512*512)	**Proposed System**	67.73	0.00062
		[9]	54.08	1.74

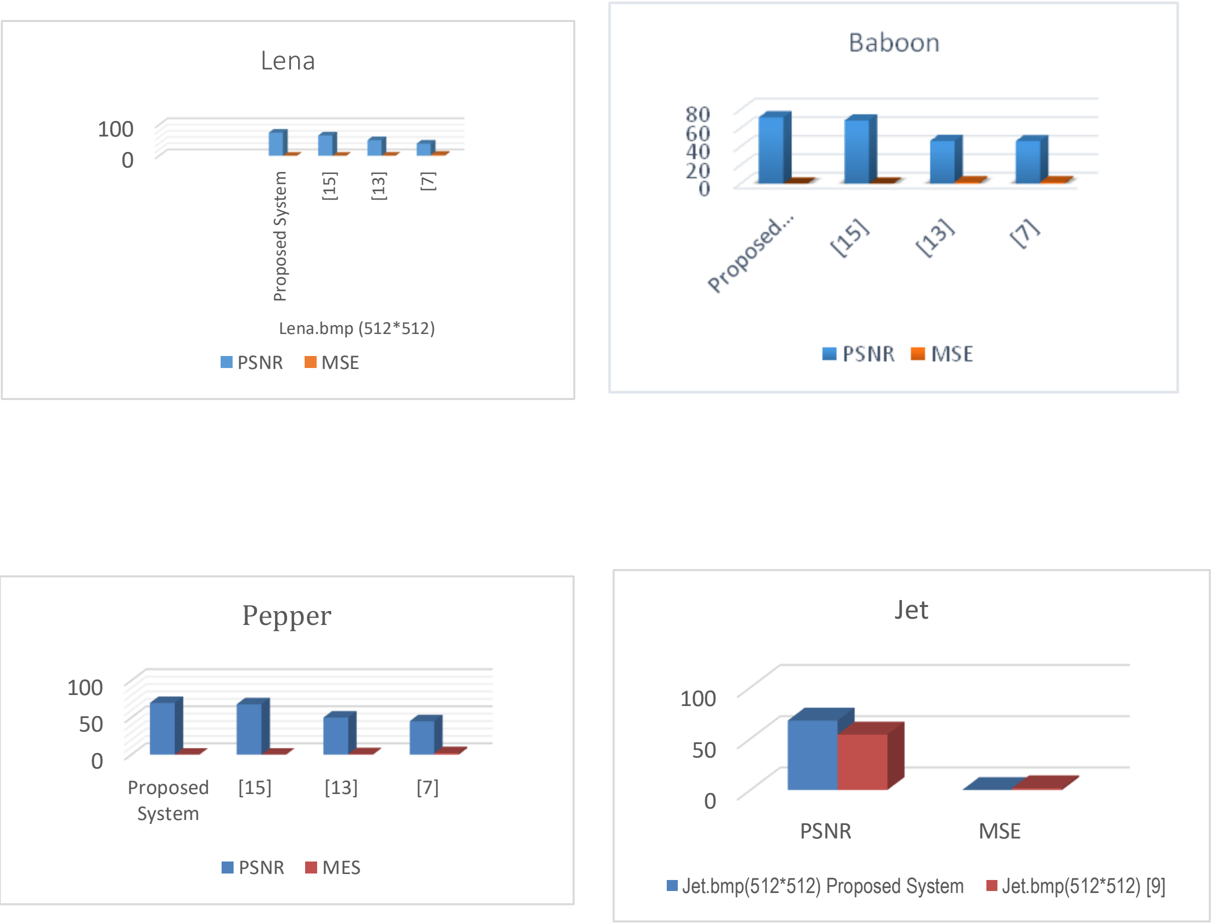


Figure 6-Compression pervious studies with Hybrid System : (a) Lena (b) Baboon (c) Pepper (d) Jet

CONCLUSION

A hybrid system based on four steps to hide information based four algorithms for image steganography: the first step using symmetric cryptography AES modified algorithm. In the second step of this system using asymmetric RSA cryptography algorithm was used to add more complexity and security. The third step, applied fuzzy stream algorithm was used in order to increase the complexity of the system and eliminate on the non-linearity of the encrypted information. In the fourth step, the LSB steganography technique was used, which is the technique of hiding information encoded with the least significant bits and making it invisible. Four color images with the extension (.bmp) with 512*512 pixels were used from data set and tests were conducted on them. Among the most prominent results of this research is that. This system provides a high ability to include information and an inability to perceive hidden information through the use many of parameters (PSNR, MES and SSIM), and the use of a histogram analyzes which were distinguished by high and good rates while maintaining the original image quality. The study was compared with modern hiding techniques.

REFERENCES

1. Bono, S.C., Green, M., Stubblefield, A., Juels, A., Rubin, A.D., Szydlo, M. (2005) Security analysis of a cryptographically-enabled RFID device. In: SSYM’05: Proceedings of the 14th Conference on USENIX Security Symposium, August 1-5, 2005, Baltimore, USA

2. Karthilkeyan B, Narla Sai Teja, Kolisetty Sarath Chandra, “data masking using cryptographic techniques in steganography”, International Journal of Innovative Technology and Exporing Engineering (IJITEE), ISSN:2278-3075, Volume-8, Issue-8, June, 2019.

3. M. Marwaha, R. Bedi, A. Singh, and T. Singh, “Comparative analysis of cryptographic algorithms”. Int J Adv Engg Tech/IV/III/July-Sept, 16, 18. 2013.

4. [S. Rani, and H. Kaur. “Technical review on symmetric and asymmetric cryptography algorithms”. International Journal of Advanced Research in Computer Science, 8(4). 2017.

5. A. G. Walia. “Cryptography Algorithms: A Review.” International Journal of Engineering Development and Research. 2014.

6. Rajkamal, M., and B. S. E. Zoraida. "Image and Text Hiding using RSA & Blowfish Algorithms with Hash-Lsb Technique." *Int. J. Innov. Sci. Eng. Technol* 1.6 (2014).

7. ALabaichi, Ashwak, Maisa'A. Abid Ali K. Al-Dabbas, and Adnan Salih. "Image steganography using least significant bit and secret map techniques." *International journal of electrical & computer engineering (2088-8708)* 10.1 (2020).

8. Chaloop, Samir G., and Mahmood Z. Abdullah. "Enhancing Hybrid Security Approach Using AES And RSA Algorithms." *Journal of Engineering and Sustainable Development* 25.4 (2021): 58-66.

9. Zulqarnain, Muhammad, Et Al. "An Efficient Method Of Data Hiding For Digital Colour Images Based On Variant Expansion And Modulus Function." *Journal Of Engineering Science And Technology* 16.5 (2021): 4160-4180.

10. Abroshan, Hossein. "A hybrid encryption solution to improve cloud computing security using

symmetric and asymmetric cryptography algorithms." *International Journal of Advanced Computer Science and Applications* 12.6 (2021): 31-37.

11. Guru, Mr Abhishek, and Asha Ambhaikar. "AES and RSA-based Hybrid Algorithms for Message Encryption & Decryption." *Information Technology in Industry* 9.1 (2021): 273-279.

12. Naser, Mohammed Abdullah, et al. "Steganography and Cryptography Techniques Based Secure Data Transferring Through Public Network Channel." *Baghdad Science Journal* 19.6 (2022): 1362-1362

13. Hameed, Rana Sami, et al. "High Capacity Image Steganography System based on Multi-layer Security and LSB Exchanging Method." *International Journal of Advanced Computer Science and Applications* 13.8 (2022).

14. Yassin, Nisreen IR. "DATA HIDING TECHNIQUE FOR COLOR IMAGES USING PIXEL VALUE DIFFERENCING AND CHAOTIC MAP." *Jordanian Journal of Computers and Information Technology* 8.3 (2022).

15. Osman, Baharudin, et al. "Text Steganography Using The Second Quotient Remainder Theorem And Dark Colour Schemes." *Journal of Computational Innovation and Analytics (JCIA)* 2.1 (2023): 21-40.

16. Almola, Sahera A. Sead, Najat Hameed Qasim, and Hamid Ali Abed Alasadi. "Robust Method For Embedding An Image Inside Cover Image Based On Least Significant Bit Steganography." *Informatica* 46.9 (2023).

17. Srinivasarao, Tumma, et al. "A Smart Strategy for Data Hiding using Cryptography and Steganography." (2023).

18. Sahin, M. Emin. "Memristive chaotic system-based hybrid image encryption application with AES and RSA algorithms." *Physica Scripta* 98.7 (2023): 075216.

19. Johnson, Neil F., and Sushil Jajodia. "Exploring steganography: Seeing the unseen." Computer 31.2 (1998): 26-34.

20. Jassim, Firas A. "A novel steganography algorithm for hiding text in image using five modulus method." arXiv preprint arXiv:1307.0642 (2013): pp. 39-44.

21. Bandi, Siddalingesh, and HS Manjunatha Reddy. "Combined audio steganography and AES encryption to hide the text and image into audio using DCT." Int. J. Recent Technol. Eng 8.3 (2019): 1732-1738.