African Journal of Advanced Pure and Applied Sciences (AJAPAS)
Online ISSN: 2957-644X
Volume 3, Issue 2, April-June 2024, Page No: 86-95
Website: *https://aaasjournals.com/index.php/ajapas/index*
(1.55) :2023 معامل التأثير العربي SJIFactor 2023: 5.689 ISI 2022-2023: 0.557

Development of Hybrid Data Security System using LSB Steganography and AES Cryptography

Seddeq E. Ghrare [1*], Maisem A. Abouras [2], Ibrahim A. Akermi [3]
[1] Department of Electrical and Electronic Engineering, University of Gharyan, Libya.
[2] Department of Computer Science, University of Gharyan, Libya
[3] Department of Electrical and Electronics Engineering, The Higher Institute of Sciences and Technology, Zawia, Libya

[*]*Corresponding author: seddeq@jgu.edu.ly*

Received: February 28, 2024	Accepted: April 29, 2024	Published: May 09, 2024

Abstract:
With the rapid advancement in communication and information technologies, the volume of data shared online has witnessed exponential growth. Consequently, securing sensitive and confidential information has become imperative. Various techniques, including steganography, coding, and cryptography, are employed to protect such data. In this paper, we propose an efficient method that combines Advanced Encryption Standard (AES) cryptography with Least Significant Bit (LSB) image steganography. We begin by concealing the secret data within a cover image using the LSB technique. The steganographic image is created by embedding the secret data in the least significant bits of pixel values. Next, we apply the AES algorithm to encrypt the steganographic image, providing a higher level of security. The strength of our system lies in the dual application of cryptography and steganography. Cracking this cryptosystem requires breaking both the encryption and decryption keys, and extracting the hidden data which is considered difficult to achieve. Our experiments demonstrate that the proposed system achieves superior security and better steganographic image quality

Keywords: Cryptography, Steganography, LSB, AES.

Cite this article as: S. E. Ghrare, M. A. Abouras, I. A. Akermi, "Development of Hybrid Data Security System using LSB Steganography and AES Cryptography," African Journal of Advanced Pure and Applied Sciences (AJAPAS), vol. 3, no. 2, pp. 86–95, April-June 2024

Introduction

There are two main categories of information security techniques: cryptography and steganography. Encryption and decryption are the two fundamental cryptographic operations. The process of transforming original data into an unintelligible format using an encryption key is known as an encryption operation. Conversely, the process of retrieving the encrypted data with a decryption key is known as a decryption operation. The difficulty of acquiring the key value determines the strength of a cryptography algorithm. Steganography, on the other hand, involves the concealment secret information within a cover media to make its existence less apparent. Techniques used for information concealment involves watermarking and steganography. Watermarking focuses on protecting the ownership of digital content, while steganography aims to embed secret data into digital content so that it remains undetectable. Various digital media, such as images, videos, and audio files, can be used to hide secret data. However, digital images are often preferred for steganography due to their inherent redundancy, which makes them suitable for information embedding without affecting the images visual quality. Furthermore, compared to other digital material, images are frequently utilized on the internet and often elicit less suspicion [6, 7].

In this paper the main goal is to provide as higher level of security as possible, therefore the secret data is first hidden in the cover image using the Least Significant Bit (LSB) technique at various bit positions. Then, the resulting stenographic mage is encrypted using the Advanced Encryption Standard (AES) algorithm. The provided level of security is more efficient compared with that offered by each technique alone.

A. ***Lease Significant Bit (LSB) Technique***

The LSB is considered as one of the spatial domain techniques used for hiding secret information; it is the most widely known steganography algorithm which aims to temporarily saving the secret data into another carrier medium such as text, voice, picture or video file, without any noticeable changes in the carrier files. A simple data security system based on LSB steganography is showed in figure 1. In that system, the steganographic algorithm merges a carrier image and the sensitive data and produces a steganographic image as output keeping its quality as good as possible so that any changes could not noticed by the human eye (or ear, in the case of audio files). The steganographic image may be transmitted over the communication channel to the antented destination who can then perform the extraction algorithm to perfectly extract the secret data from the steganographic image.

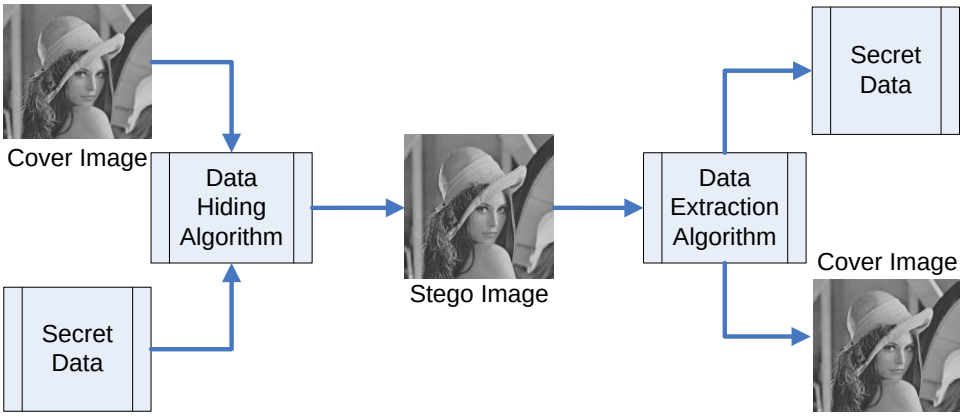

Figure 1. Image Steganography System.

The working principle of the LSB is based on modifying the binary bit that carries the least value in each pixel of the cover image. These modifications could be interpreted as random noise, which should not have any perceptible effect on the image. The LSB is considered an effective technique because changing the bits that carry the least value has a minimal impact on the overall pixel value, and therefore the change Is almost imperceptible to the human eye. [8].

For example, to hide the character "a" which represented in a binary form as 01100001 inside the cover image, eight pixels of the cover image are needed. In this case, the LSB of each pixel should be used to hide one bit of the character “a” as follows:

P1: 1001001***0***	P2: 0101001***1***	P3: 1001101***1***	P4: 1101001***0***
P5: 1000101***0***	P6: 0000001***0***	P7: 0111001***0***	P8: 0010101***1***

The application of decoding the cover reads the eight Least Significant Bits of those pixels to recover the hidden byte of the character "a". [9].

B. ***Advanced Encryption Standard Technique***

It is one of the most used cryptographic algorithms. Advanced Encryption Standard (AES) operates on data blocks that are represented as a 4 x 4 matrix. Iterative processes are used in AES. These processes are Substitution and Permutations. It contains on a set of related actions at each round. Each round contains on the following process. [10]

- First, the outputs produced by the substitution process are interchanged by the inputs.
- The bits are shifted in a cyclic mode.
- The columns are shuffled by transformation.
- The key is added with input using XOR operation.

The execution of the AES is carried out byte by byte, so that a plaintext of 128 bit is representing a block of 16 bytes which represents a 4x4 matrix. The number of the rounds of the AES depends on the key length. 128-Bit key requires 10 rounds, 92-Bit key involves 12 rounds, and 256-Bit key needs 14 rounds. A four transformation functions are required for the first round of encryption process [11].

The general block diagram of the AES encryption and decryption stages is indicated in figure 2.

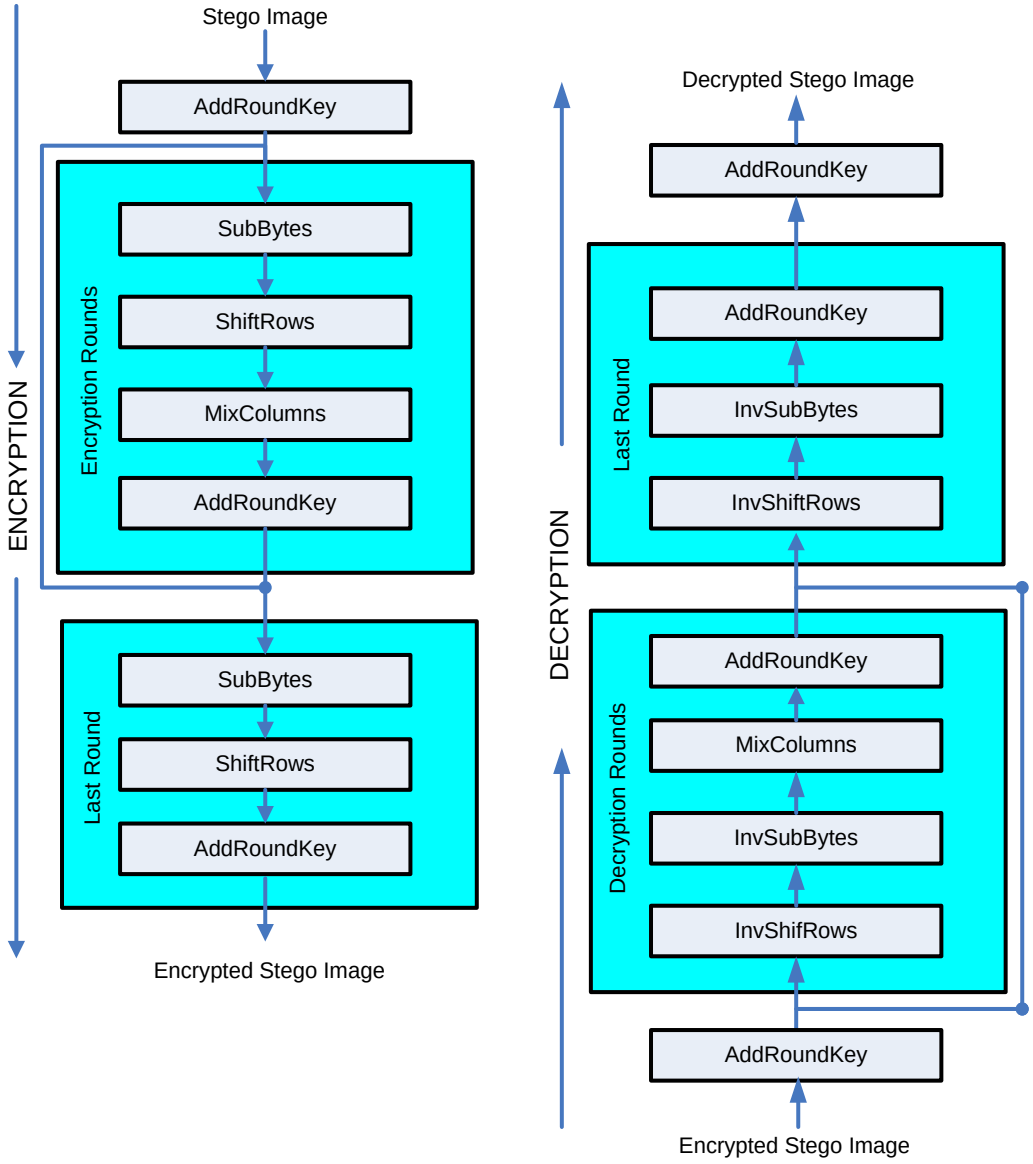

Figure 2. The AES Encryption and Decryption Stages.

From that figure, the steganographic image is fed to the encryption process in a form of 4x4 matrixes. To carry out the encryption process, a four-transformation operation are performed on each part of the steganographic image these operations are:

- Substitution Bytes
- ShiftRows
- MixColumns
- AddRoundKey

Not that the final round consists of only three transformation operations ignoring MixColumns.

The last transformation operations should be performed in a reverse mode to decrypt and retrieve the stego image as follows:

- Inverse Substitution Bytes
- Inverse ShiftRows
- Inverse MixColumns
- AddRoundKey

Material and methods

The proposed and implemented system is indicated in figure 3.

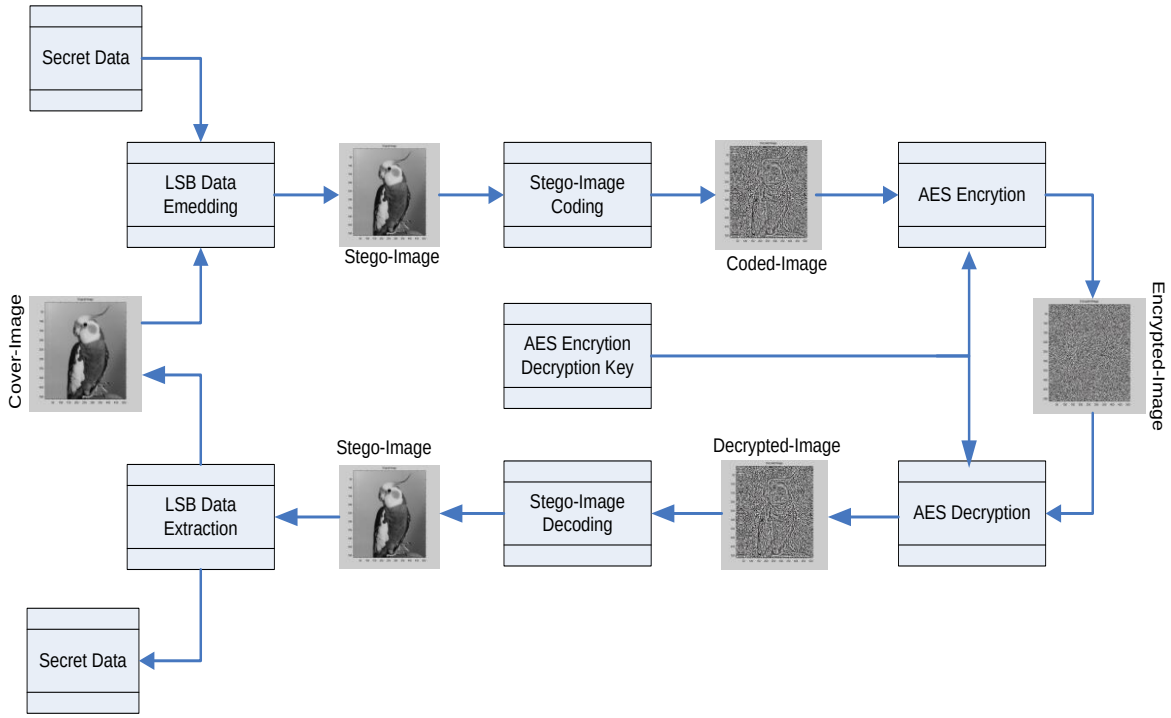

Figure 3 The Block Diagram of the Proposed Method.

The main steps of the proposed data security system are as below:

- Change the raw sensitive data into ASCII binary form.
- Embed the binary sensitive data inside the carrier image using LSB steganography, the produced image is representing steganographic image.
- Convert the gray scale steganographic image into binary image.
- Generate the 128-bit AES encryption key.
- Apply the ASE algorithm to encrypt the binary steganographic image.

The reverse steps should be performed to extract the original hidden sensitive data. These steps are as follows:

- Generate the 128-bit ASE decryption key.
- Decrypt the encrypted steganographic image, the produced image is the original binary steganographic image.
- Convert the binary steganographic image into its original form; the produced image is the original gray scale steganographic image.
- Extract the hidden sensitive data from the gray scale steganographic image.
- Convert the secret data into its original form.

Evaluation of Image Quality

Image steganography techniques depend on hiding the secret information inside the cover image, as a result the quality of the cover image will have some degradation, some of the implemented techniques tried to decrease such effect by implementing an improved mechanism to merge the ability of having invulnerable, as well as imperceptible steganographic image which carries hidden information. To measure imperceptibility, it is possible sometimes to compare the original cover image with the steganographic image subjectively depending on the human visual system. Unfortunately, such approach may be imprecise. Therefore, the most known evaluation metrics used to compare the cover images and steganographic images are:

- Mean Square Error (***MSE***)
- Peak Signal to Noise Ratio (***PSNR***)
- Structural Similarity Index Measure (***SSIM***)

The ***MSE*** provides an approximated amount of error between the original cover image and the stego image. If the original image and the stego image are of equal sizes, then the *MSE* can be computed using the following equation: [12]

$$MSE = \frac{1}{M \times N} \sum_{i=0}^{M} \sum_{j=0}^{N} \left(C(i, j) - S(i, j)\right)^2 \quad (1)$$

Where:
M, N are the dimensions of the image.
C(i,j) is the carrier) image
S(i,j) is the steganographic image

The ***PSNR*** can be computed as follows:

$$PSNR = 20\log\left(\frac{2^B - 1}{MSE}\right) \text{dB} \quad (2)$$

Where:
B is the number of bits representing each pixel. In the case of a grayscale image ***B=8***, so the ***PSNR*** is calculated by: [12]

$$PSNR = 10\log\left(\frac{(255)^2}{MSE}\right) \text{dB} \quad (3)$$

Structural Similarity Index Measure (***SSIM***) is the third known evaluation metric used in this study. ***SSIM*** is considered as an important quality metric to measure the similarity between any two images. Equation (4) is used to compute the ***SSIM***: [13]

$$SSIM(G1,G2)=b(G1,G2)c(G1,G2)s(G1,G2) \quad (4)$$

Where:
$b(G1,G2) = 2\mu_{G1}\mu_{G2} + C_1/\mu_{G1}^2 + \mu_{G2}^2+C_1$
$c(G1,G2) = 2\sigma_{G1}\sigma_{G2} + C_1/\sigma_{G1}^2 + \sigma_{G2}^2 + C_2$
$s(G1,G2) = 2\sigma_{G1G2} + C_3/\sigma_{G1} + \sigma_{G2} + C_3$
μ_{G1}, μ_{G2} represent the mean of G1and G2 respectively
σ_{G1}, σ_{G2} represent the variance of G1and G2 respectively
σ_{G1G2} represent the covariance of G1 and G2.
C1, C2, and C3 are small constants.

SSIM result is ranging between 0 to 1, where 0 interpreted that there is no correlation between G1 and G2, and 1 means ideal coincide (G1 = G2).

Results and discussion

In this paper, four 256x256 pixel gray-scale images “Bird”, “Cameraman”, “Baboon”, and “Lena” have been used and tested in the simulation process to investigate the efficiency of the proposed approach. These images are 8 bits per pixel and are shown in Figure 4

Figure 4 Test Images.

The test images indicated in Figure 4 have been used as a cover image to hide a secret data of size 64 KB. The produced images which carry the hidden secret data are called a steganographic images. In order to increase the security level for the secret data, those images are encrypted using ASE-128-bit encryption algorithm.

Figures 5, 6, 7, and 8 shows the simulation results obtained from the proposed system using the four test images. The first row of each figure shows the cover image and the encoded steganographic image. The second row shows the steganographic image encrypted by AES. The third row shows the decoded steganographic image and the reconstructed steganographic image.

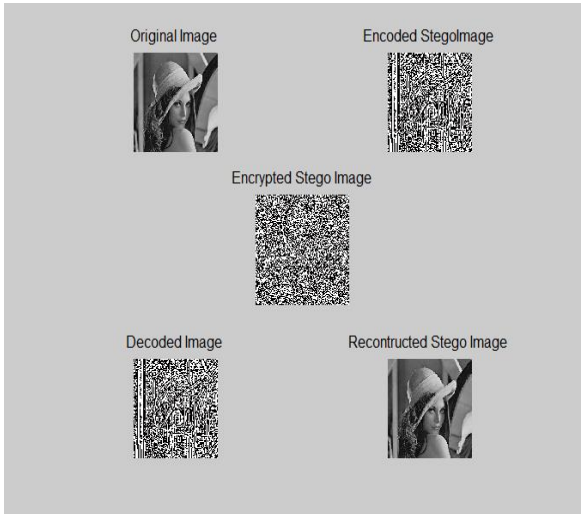

Figure 5. Original Image, Stego Image, Encrypted and Recovered Stego Image. (Lena)

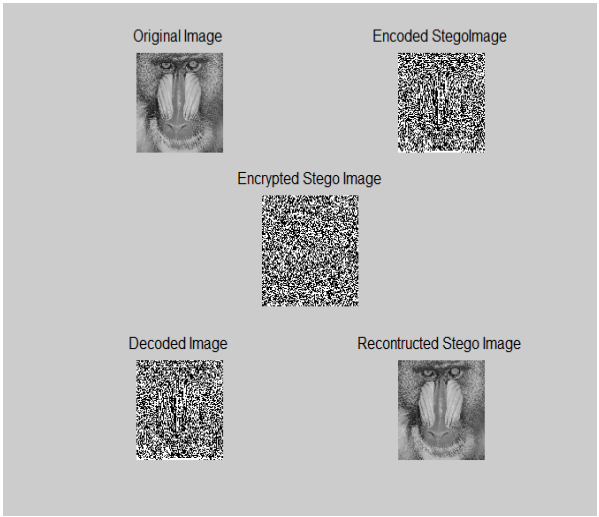

Figure 6. Original Image, Stego Image, Encrypted and Recovered Stego Image. (Baboon)

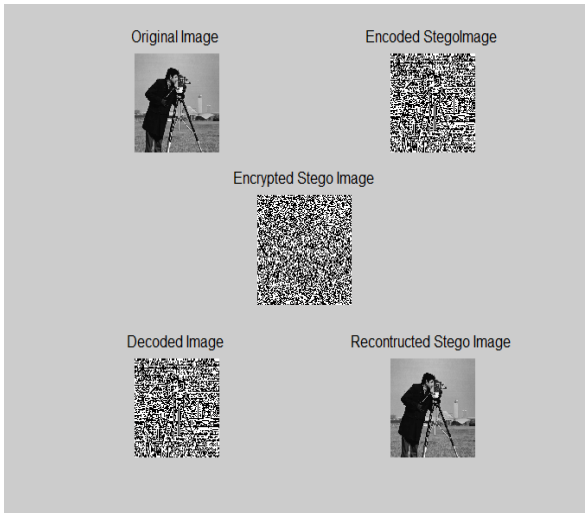

Figure 7. Original Image, Stego Image, Encrypted and Recovered Stego Image.(Cameraman)

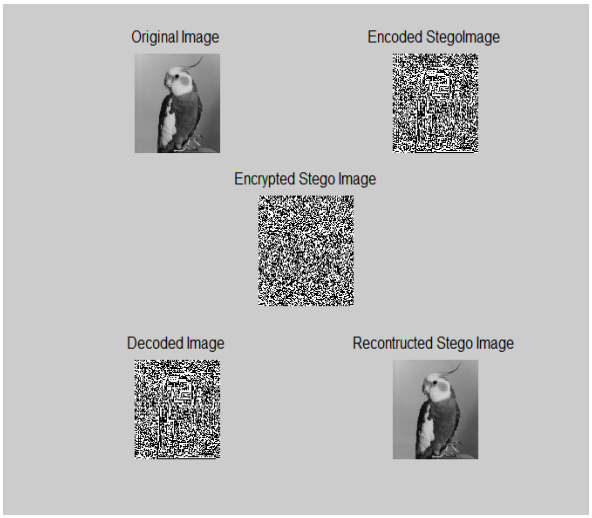

Figure 8. Original Image, Stego Image, Encrypted and Recovered Stego Image.(Bird)

Both objective and subjective evaluations were used to test the quality of the steganographic images. Objectively the PSNR and SSIM are calculated using the above equations and tabulated in Table 1. The obtained PSNR values are ranging from 41dB to 66dB, whereas the SSIM values were higher than 0.90. From Table 1, it's clear that the quality of the decrypted recovered stego images is acceptable. This is strongly supported by comparing the histograms of both original and reconstructed stego images. From figures 9 to 12, it can be seen that are both histograms for each image are almost identical.

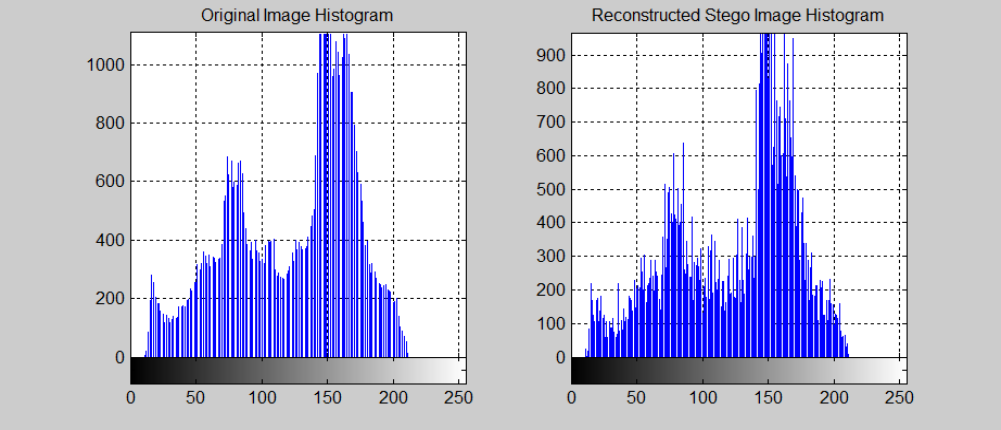

Figure 9. Histogram of Original Image and Reconstructed Stego Image. (Bird)

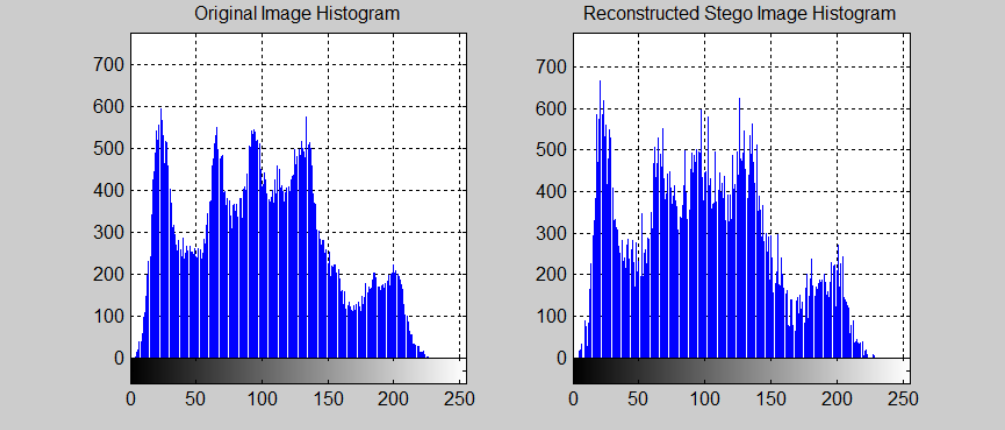

Figure 10. Histogram of Original Image and Reconstructed Stego Image. (Lena)

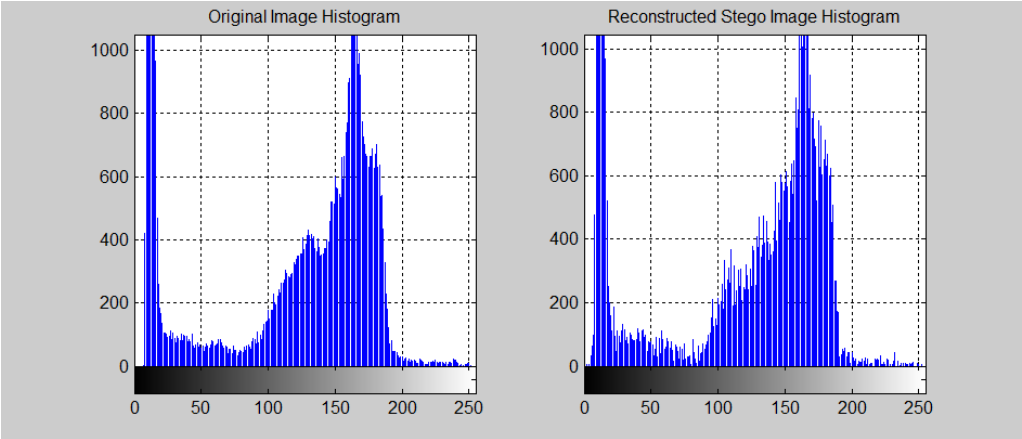

Figure 11. Histogram of Original Image and Reconstructed Stego Image (cameraman)

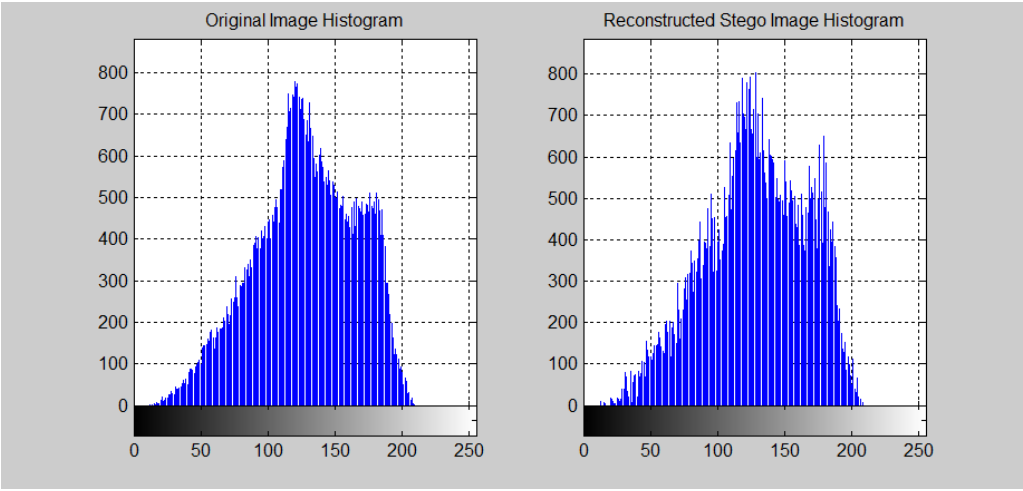

Figure 12. Histogram of Original Image and Reconstructed Stego Image. (B**aboon**)

Table 1 PSNR and SSIM Values for Stego-Image

Image		**Lena**	**Baboon**	**Cameraman**	**Bird**
LSB1	PSNR	61.4978	64.5387	58.4123	66.5060
	SSIM	0.9959	0.9961	0.9955	0.9973
LSB2	PSNR	58.4440	60.5298	54.4189	63.3998
	SSIM	0.9882	0.9920	0.9864	0.9960
LSB3	PSNR	48.4734	54.4952	45.3784	56.4711
	SSIM	0.9843	0.9881	0.9810	0.9941
LSB4	PSNR	43.4368	48.4627	41.1489	51.3791
	SSIM	0.9795	0.9832	0.9789	0.9899

Subjectively, in our case, the secret data was hidden in the carrier image at different bit positions of each pixel. When the secret data is hidden in any of the first four LSB positions (1st to 4th LSB), the steganographic image and the original carrier image were very identical, this indicates that the visual quality of the decrypted steganographic image is quite good. On the other hand, when the secret data is hidden in any of the second four LSB positions (5th to 8th LSB), the quality of the steganographic images were degraded. Figures 13 to 16 show a comparison between the original carrier images and their corresponding steganographic images using the first four LSB, whereas Figure 17 shows the effect of hidden data in the second four LSB.

a) Stegoo Images

b) Stegoo Images

Figure 13. Original Images and Corresponding Stego-Images using First LSB

a) Original Images

b) Stegoo Images

Figure 14. Original Images and Corresponding Stego-Images using Second LSB

a) Original Images

b) Stegoo Images

Figure 15. Original Images and Corresponding Stego-Images using Third LSB

a) Original Images

b) Stegoo Images

Figure 16. Original Images and Corresponding Stego-Images using Forth LSB

Original Lena Image | 5th LSB Stego Image | 6th LSB Stego Image | 7th LSB Stego Image | 8th LSB Stego Image

Figure 17. Original Images and Corresponding Stego-Images using Fifth LSB through Eighth LSB

Conclusion

In this paper, a hybrid data security system based on image steganography and cryptography is proposed. A secrete data of 64 KB size is first hidden inside different carrier images. Then the resulted stego images are encrypted using the AES algorithm in order to improve the security level for the secret data. The main advantage of the introduced method comes from the use of LSB steganography and AES cryptography respectively which provides a high level of security because any attempt to break this cryptosystem depends on breaking its encryption and decryption key. The used key is very hard to be recovered since it was generated in a form of 128-bit binary stream. The obtained results show that the presented method has a high security level and an acceptable steganographic image quality when the data is hidden in the first four LSB.

References

[1] William Stallings. 2005. "*Cryptography and Network Security",* 4th edition Principles and Practice

[2] M. B. Pramanik, "*Implementation of Cryptography Technique using Columnar Transposition*", international journal of computer applications, (0975-8887) – Jan. 2014.

[3] Fabien A. P. Petitcolas, Ross J. Anderson and Markus G. Kuhn, "*Information Hiding: A Survey*" Proceedings of the IEEE, special issue on protection of multimedia content, 87(7), 1999, pp. 1062–1078.

[4] Shieh, J. M., Lou, D. C. and Chang, M. C., "*A Semi-blind Digital Watermarking Scheme Based on Singular Value Decomposition*" Computer Standards & Interfaces, Volume 28, Issue 4, 2006, pp. 428-440.

[5] Lin, P. L., Hsieh, C. K. and Huang, P. W., "*A Hierarchical Digital Watermarking Method for Image Tamper Detection and Recovery*" Pattern Recognition, Volume 38, Issue 12, 2005, pp. 2519- 2529.

[6] Lin, C. C. and Tsai, W. H., "*Secret Image Sharing with Steganography and Authentication*" Journal of Systems and Software, Volume 73, Issue 3, 2004, pp. 405-414.

[7] Chang, C. C., Chen, T. S., and Chung, L. Z., "*A Steganographic Method Based upon JPEG and Quantization Table Modification,*" Information Sciences, 2002, pp. 123-138.

[8] Seddeq E. Ghrare, Hajer A. Emhemed, Abduladim M. Alamar, "*Digital Image Watermarking Method Based on LSB and DWT Hybrid Technique*", The 2022 IEEE International Conference on Sciences and Techniques of Automatic Control and Computer Engineering, (MI-STA2022), Sabratha University, 23,25 May 2022.

[9] Hassan Mathkour. Batool Al-Sadoon, Ameur Touir, "*A New Image Steganography Technique*" , 2008 IEEE 4th International Conference on Wireless Communications, Networking and Mobile Computing, October 12-17, 2008, Dalian, China.

[10] Mohammad Amjad, "*Security Enhancement of IPV6 Using Advance Encryption Standard and Diffie Hellman*", International Journal of Scientific Research in Network Security and Communication, Vol.5, Issue.3, pp.182-187, 2017.

[11]. Priya Deshmukh, "*An Image Encryption and Decryption Using AES Algorithm*", International Journal of Scientific & Engineering Research (IJSER), Vol.7, Issue.2, pp.210-213, 2016.

[12] Seddeq E. Ghare, Mohd. Alauddin M. Ali, A.A Khrwat, "*Development of Near Lossless Coding Algorithm for Medical Images using Grayscale and Binary Matrices*", Aljabal Journal for Applied Science and Humanities. Issue No. (2), December 2018.

[13] Seddeq E. Ghrare,, Haneen A. Barghi, " *Design and Implementation of Encryption and Decryption Technique Based on Hidden Encrypted Symmetric Key with Logical Shift and XOR Operation* ", The 2023 IEEE International Conference on Sciences and Techniques of Automatic Control and Computer Engineering,(MI-STA2023), University of Benghazi, 23,25 May 2023