International Journal of Science and Research (IJSR)
ISSN: 2319-7064
ResearchGate Impact Factor (2018): 0.28 | SJIF (2019): 7.583

Image Steganography Based on Improved LSB Embedding and AES Cryptography

Abhishek Singh

School of Computer Science and Engineering, Galgotias University, Greater Noida, India

Abstract: ***Steganography is the art of hiding important information in various multimedia files. The sender and the intended receiver is aware of the existence of important message. Image Steganography is a technique of using an image file as a cover object. Cryptography is used to protect the information from the unintended user, by the encryption and decryption techniques, for secure communication. In this paper, LSB Steganography method is the proposed technique which focused on RGB colour image because it is uncompressed and suitable than any other image format. AES cryptography technique has also been used in the proposed method, for enhanced security.In this research, the performance of a combination of LSB-AES algorithms on various cover image sizes is analysed. To measure performance and image quality PSNR and MSE is used. The original image will be compared by the resulting image. Hence the proposed technique of steganography and cryptography is efficient for hiding the information inside the image, with more security.***

Keywords: Steganography, Cryptography, Encryption, Decryption, LSB, AES

1. Introduction

In today's world, the security for online communication and information technology can be achieved using the techniques of Steganography and Cryptography. Steganography can be achieved through hiding the secret information in various forms such as text, image, audio or video files. The purpose of Steganography passes only when the presence of hidden information is not revealed or even suspected by the unintended user. . Cryptography is the process of converting plain text into cipher text using encryption techniques for secure transmission of messages.

The efficient and secure steganography, which is widely used is image steganography. The embedding of important message into the cover image will be performed using improved LSB embedding technique. Thefeatures such as simple algorithm, encryption fast, easy to implement, a large amount of hidden data, makes this technique more efficient. The cover image used is RGB colour image. This paper is based on the combined use of Steganography and cryptography. In this paper an improved LSB combined with AES cryptography is proposed for the information hiding and secure transmission of message to the legal receiver. With the proposed technique, the security is upgraded by the encryption algorithm better than the common LSB embedding steganographic method, with better resulting Image quality.

2. Related Work

There are various techniques available for implementing steganography with various multimedia such as image, audio and video.S.M. Masud Karim, M.S. Rahman, and M.I. Hossain proposed a new approach based on LSB using secret key. The secret key encrypts the hidden information and then it is stored into different position of LSB of image. [1].X. Qing., X. Jianquan and X. Yunhua proposed a method in which the information is hidden in all RGB planes based on HVS (Human Visual System)[2].S. Sarreshtedari and S. Ghaemmaghami [3] proposed a method to achieve a higher quality of the Stego image using BPCS (Bit Plane Complexity Segmentation) in the wavelet domain.Kim, Chang and Yang suggested that the data hiding (DH) may embed secret data, copyright information, and annotation into various media such as image, audio, video, or text. They further propose that "the embedded data should be invisible to a watchdog, and meanwhile the secret data have to stay hidden in a cover signal without detection from steganalysis tools"[4].G. Divya Sri, A. Ramani[5] the secret message is encrypted using RSA and Column Transposition technique. The encrypted message is embedded into the image using the LSB technique. Whenever the combination ofCryptography and Steganography have been used then the level of security has been increased rather than using the Steganography alone.

3. Proposed Technique

A digital coloured image contains different pixels. In the proposed technique, we used colour image.. The pixels of colour image can be represented as mixture of red, green and blue colour with suitable proportions. A stream of 8 bits represent each colour level of Red, green and blue. Thus total 24 bits are required to represent a pixel of colour. Thus an image is an array of many bytes each representing a single colour information present in a pixel.

The proposed technique consists of two main parts:

1) Conversion of secret message into cipher text using AES Cryptography.
2) Hiding cipher text in the cover image using the improved LSB Technique.

In this technique, 128 bits AES Cryptographic algorithm is used, which takes a password and encrypts the plain text to cipher text.The AES algorithm uses a round function that is composed of four different byte-oriented transformations.In this method of encryption, the plaintext (which is the information that needs to be encrypted) is separated into blocks. The block size of AES is 128-bits, so it splits the data into a four-by-four column of sixteen bytes (there are

eight bits in a byte and 16 x 8 = 128). For 128 bits, the total 10 rounds are required. The data passes through the byte substitution, shift rows, mix columns and round key steps up to nine times each, being transformed at every stage. The resultant encrypted information is in hexadecimal form.
Example:

Table 1: AES CIPHER

Plain text	Password	Cipher Text
Hello, this is classified document.	1234567890123456	C698C97017D285F1F7C6494 41C5993757E3378224E1A83 7420BE55A2B1C632AD5BA F63312DF3F546E0F2F5B29B A49942

Following the above procedure, results in the cipher text. After this encryption technique, we will perform embedding of this cipher text into the RGB pixels of the colour image, with the improved LSB embedding algorithm.The proposed method follows a directional embedding technique for achieving maximum image quality in the stego image. To reduce the bit changes in the cover image, this method performs a selection of appropriate direction for embedding of secret byte.

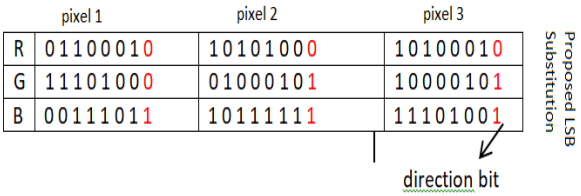

Figure 1: LSB Embedding of the byte 00001111 using the proposed technique.

As we can see in the Fig.1,that 00001111 is embedded in the RGB pixels of the cover image in one direction. The bits of three pixels of red, green and blue channels are substituted sequentially. The 9th bit shows the direction bit i.e. '0' shows the reverse order and '1' shows the forward order. Thus, the proposed algorithm minimizes the number of alterations in the cover image.

3.1. Proposed combined algorithm for image Steganography

Input- Secret message, Password, Cover Image

Output- Stego image with embedded cipher

1) Read the secret message from user input.
2) Take the password to be used for encryption.
3) The output of the encryption will be cipher text, this will be the message in the hexadecimal form which is to be embedded in the cover image.
4) Now, a cover image should be taken of 360*360 pixels.
5) Select the 3 pixel of RGB colour image and change these into binary bits.
6) Next, convert the cipher text into binary format.
7) Then, replace the last bits of pixels of all the RGB channels of the colour image using the proposed LSB substitution technique.
8) The resultant image will be the stego image embedded with the secret message.

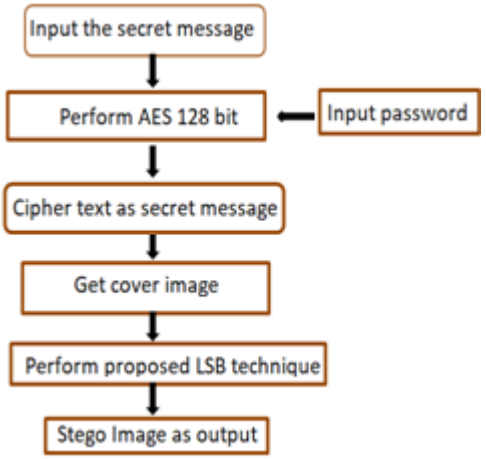

Figure 2: Flowchart of Proposed Technique of Image Steganography

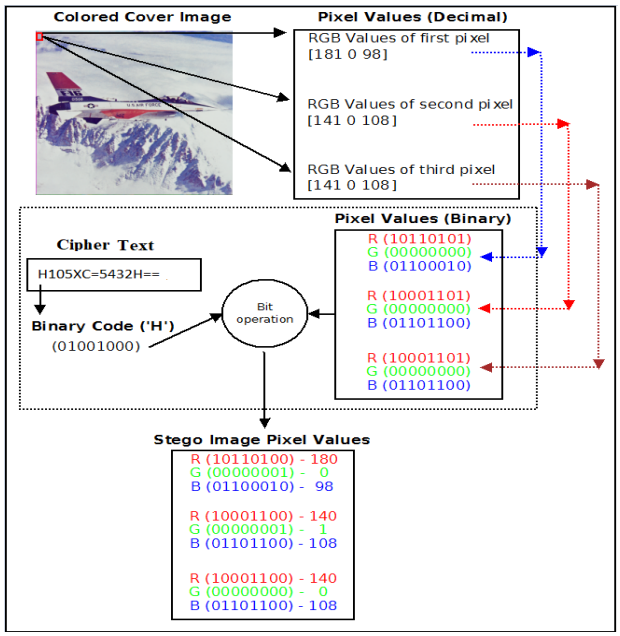

Figure 3: Example of embedding of text into pixels of colour image

4. Experimental Results

The proposed technique of combined LSB embedding and AES encryption technique is better than simple LSB substitution technique in many aspects such as the security, image quality and efficiency. A 24-bit image Lenna.png as shown in Fig.4. was used as the cover image. The outputs of the algorithm were remarkably similar to the original images. The message hidden in the image is given in Table 2:

Table 2: Concealing of secret message in image

Image	Image size	Cipher size	Original message	Password	Cipher Text
Lenna . png	460 kb	96 Characters	Hello, this is classified document	12345678 90123456	C698C97017D2 85F1F7C649441 C5993757E3378 24E1A837420B E55AB1C632A5 BAF63312DF35 46E0F2F5B29B A49942

The proposed algorithm changes very small number of bits when embedding a large cipher. As the algorithm can use all the pixels to hide data, a 512x512 size cover image can hide at most 4000 character which is of course a big cipher. For a larger cover image and larger cipher, one can use more than 50 pixels to hide the cipher size. Moreover, it is not necessary to work with LSBs of the colour components.

Figure.4 :The input(Left) and corresponding output(Right) of program using the proposed technique

4.1. Evaluation of Image Quality:

For comparing Stego images with cover results it requires a measure of image quality. Commonly used measures are Mean-Squared Error, Peak Signal-to-Noise Ratio

4.1.1. Mean Square Error(MSE):

The mean squared error (MSE) of an estimator is one of many ways to quantify the difference between values implied by an estimator and the true values of the quantity being estimated.

$$MSE = \frac{1}{N}\sum_{i=1}^{N}(c_i - s_i)^2 \qquad (1)$$

4.1.2. Peak Signal-to-Noise Ratio:

In the objective evaluation method, the most commonly used index is the peak signal to noise ratio (Signal to Noise Ratio Peak, PSNR) [6]. In the calculation of PSNR, we must first calculate the Square Error Mean (MSE) between the hidden image and the cover image.

$$PSNR = 10 \cdot \log_{10}\left(\frac{MAX_I^2}{MSE}\right) \qquad (2)$$

Generally speaking, the larger the value of PSNR, the more similarity between the hidden image and the cover image. In experience, the quality of the image is acceptable if the PSNR value is higher than 28dB.

We have calculated MSE and PSNR values by giving high capacity secret message in different images as shown in Fig.5.

Figure 5: Different Cover Images

Table 3: MSE and PSNR of different cover images

Image format	MSE	PSNR
Baboon.jpg	0.3973	52.1606
Pepper.jpg	0.3953	52.1771
Lenna.png	0.3956	52.1773

As we can see the image quality is not much affected due to the proposed technique. The proposed technique provides double layer security using AES encryption algorithm.

5. Conclusion

In the proposed technique, we have introduced the new method of embedding important message into the image using the LSB substitution method that can improve the quality of the stego image. We have used the concept of cryptography to enhance the security. This ensures, to a large extent, that theimportant information cannot be accessed by any unauthorised user. The cryptographic technique used is AES, by which the secret message is secured by two security layers. Thus, the proposed technique fulfils the requirement of the Steganography technique.

6. Acknowledgments

I feel great pleasure in acknowledging the help given by various individuals throughout the project work. This project is itself an acknowledgement to the inspiration, drive and technical assistance contributed by many individuals. I take this opportunity to express my immense gratitude to my project guide in my research. I am grateful for their prolonged interest in my work and excellent guidance. They have been a constant source of motivation to me

References

[1] S.M. M. Karim, M.S. Rahman, and M.I. Hossain “A New Approach for LSB Based Image Steganography using Secret Key.”, Proceedings of 14th International Conference on Computer and Information Technology, IEEE Conference Publications, pp 286 – 291, 2011.

[2] X. Qing., X. Jianquan and X. Yunhua., “A High Capacity Information Hiding Algorithm in Colour Image.”, Proceedings of 2nd International Conference on E-Business and Information System Security, IEEE Conference Publications, pp 1-4, 2010

[3] S. Sarreshtedari and S. Ghaemmaghami, “High Capacity Image Steganography in Wavelet Domain”, Proceedings of 2010 7thIEEE Consumer Communications and Networking Conference(CCNC), USA, IEEE Conference Publications, pp. 1-5, 2010

[4] Kim C., C. C. Chang, C. N. Yang & Zhang J. Baek. (2018). Special Issue: Real-Time Data Hiding and Visual Cryptography. Journal of Real-Time Image Processing, 14(1), 1-4.

[5] G. Divya Sri, A. Ramani, A. Jhansi Priya, B. Santhi, SK. Wasim Akram, "*Design of Image Steganography using Asymmetric Key Cryptography*", International Journal of Computer Sciences and Engineering, Vol.7, Issue.3, pp.19-22, 2019.

[6] Li Li. Study [D] based on the LSB information hiding technology, Beijing University of Posts and Telecommunications, 2011.

[7] Divya Soi, Bhupinder, "*A Robust Hybrid Algorithm for Image Steganography*", International Journal of Computer Sciences and Engineering, Vol.8, Issue.2, pp.59-68, 2020.
[8] Avinash Rai, Vivek Todkar, "*Optimization of Secure Data for Steganography and Digital Watermarking Scheme*", International Journal of Computer Sciences and Engineering, Vol.7, Issue.6, pp.1036-1040, 2019.
[9] Yogesh Gyarsia, Shiv Tiwari, "*Steganography With Improved Cryptography*", International Journal of Computer Sciences and Engineering, Vol.07, Special Issue.10, pp.162-166, 2019.
[10] X. Zhou, W. Gong, W. Fu and L. Jin, "An improved method for LSB based color image steganography combined with cryptography," *2016 IEEE/ACIS 15th International Conference on Computer and Information Science (ICIS)*, Okayama, 2016, pp.1-4.