Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 6.017

IJCSMC, Vol. 6, Issue. 11, November 2017, pg.25 – 30

Bit Adjusting Image Steganography in Blue Channel using AES and Secured Hash Function

S.M. MOHIDUL ISLAM[1], MD. ALTAB HOSSIN[2], RAJEEV KUMAR SHAH[3], PRAKASH KUMAR BIPIN[4]
[1]COMPUTER SCIENCE AND ENGINEERING DISCIPLINE, KHULNA UNIVERSITY, BANGLADESH
[2]MANAGEMENT SCIENCE AND ENGG. DEPT., UNIVERSITY OF ELECTRONIC SCIENCE AND TECHNOLOGY OF CHINA, CHINA
[3]MANAGEMENT SCIENCE AND ENGG. DEPT., UNIVERSITY OF ELECTRONIC SCIENCE AND TECHNOLOGY OF CHINA, CHINA
[4]SCHOOL OF ECONOMICS, WUHAN UNIVERSITY OF TECHNOLOGY, CHINA
[1] MOHID@CSE.KU.AC.BD, [2] CHNSCH@163.COM, [3] RAJEEVSHAH97@YAHOO.COM, [4] PRAKASH_BPN@YAHOO.COM

Abstract- Transmitting secret information through internet requires more security because of interception and improper manipulation by eavesdropper. One of the most desirable explications of this is "Steganography". This paper proposes a technique of steganography using Advanced Encryption Standard (AES) with secured hash function in the blue channel of image. The embedding system is done by dynamic bit adjusting system in blue channel of RGB images. It embeds message bits to deeper into the image intensity which is very difficult for any type improper manipulation of hackers. Before embedding text is encrypted using AES with a hash function. For extraction the cipher text bit is found from image intensity using the bit adjusting extraction algorithm and then it is decrypted by AES with same hash function to get the real secret text. The proposed approach is better in Pick Signal to Noise Ratio (PSNR) value and less in histogram error between stego images and cover images than some existing systems.

Keywords- AES-128, SHA-512, Cover Image, Stego image, Bit Adjusting, Blue Channel

I. INTRODUCTION

Today's large desire for internet applications is to transmit data in a safe and secure manner. Data transmission through internet is not safe because of improper manipulation by the hackers. Therefore, the better explication of this problem is Steganography. Steganography means hiding some information like data, image, code into a medium and retrieving the information losslessly [1]. A great deal of steganography is when a third party attack the cover work, the secret data must be unnoticed. Fig.1 shows the basic of steganography.

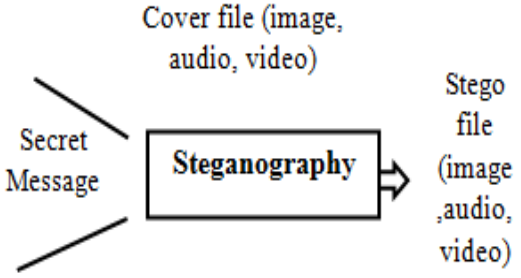


Fig. 1: Steps of Steganography

Images are the most popular cover medium used for steganography. Color images have intensity from the darkest and lightest of three different colors, Red, Green, and Blue. Image steganography techniques are divided into two groups: spatial domain and frequency domain [1]. The techniques of spatial domain use pixel gray level and their color values for encoding the message bits. The techniques of frequency domain encode the message bits in the transform domain coefficient of the image. In steganography field, there are many works have been done in spatial domain as well as frequency domain. There are many applications also invented to break the systems.

V. Lokeswara Reddy et. al. [2] proposed a method where data is encrypted by Data Encryption Standard (DES), a symmetric algorithm and then the encrypted data is embedded into image by using LSB method. For data extraction first the encrypted text which is hidden into image is extracted, then the encrypted text is decrypted again by DES and the real data is found. They use DES which is a better symmetric algorithm, but DES is one time broken. DES is more secure when there is a use of hash key, but there is no hash key used here. Mamta Juneja et. al. [3] proposed a work which is done by the improved LSB technique. Before embedding, the data is encrypted and the encryption is done by the SDES algorithm. Then the data is embedded into the image. The images are divided into some smooth areas and the edges. LSB technique is applied in the edge areas. In case of decoding, first the cipher text is extracted and then the cipher text is decrypted by SDES. Advantages are using improved LSB for embedding. The limitations are SDES is very low encryption without substitution method, embedding the bits are embed into the edge area which is the insecure process against steganalysis, if the stego image is rotated and then extracted; it lose many of the secret data which is embedded into image.

The characteristics of good steganography are: Perceptibility, Capacity, and Robustness. In most cases, capacity is not as essential as the other two and whereas watermarking favors robustness most perfectly, steganography considers perceptibility as the most important. The proposed system pass a text message through an image file in a robust and advanced secured way, where text remains unchanged. For this purpose, we encrypt secret text by an encryption algorithm with secured hash function and then embed the cipher text into the image using bit adjusting algorithm. To retrieve the data from the image, we extract the cipher text from the image and then we decrypt the cipher text by the same algorithm with a same key. Then we get the real secret text in a robust and lossless way. Thus we ensure the accuracy, Security of the secret data, and Good stego image quality.

The rest of the paper is organized as follows. In Section II proposed methodology is described. Experimental result is outlined in section III. Finally conclusion is drawn in section IV.

II. PROPOSED METHOD

In the proposed method, Advanced Encryption Standard (AES) with Secured Hash Algorithm (SHA) is used for data encryption and decryption. AES is a symmetric algorithm, which means we can do both encryption and decryption by AES. It is a lossless data encryption method. A hash function, SHA-512 is used with AES enhancing the combination of the key in AES. We use bit-adjusting method for embedding of the encrypted data in the cover Image. The whole work is divided into two parts: encoding and decoding.

A. Encoding Process

In Encoding system, secret text message is embedded into a cover image. Encoding is performed using two different algorithms: one for encryption and other for embedding.

1) Encryption: We use cryptographic encryption algorithm AES to encrypt the text. We take secret text as input and then encrypt the text with AES-128 with SHA-512. Then we get the cipher text of the text. Then we embed the cipher text into a cover image file which will give more security in the case of steganalysis. AES-128 is a symmetric cipher algorithm. It has 128 bit block size and after using the key size like 128 bit, 192 bit and 256 bit, the name of AES is chosen. We use AES-128, where the key size is 128 bit. SHA- 512 is a kind of SHA-2. It gives a better hash in case of encryption and decryption with AES.

2) Embedding: After encoding cipher text is embedded to the cover image. We embed the cipher text into the blue channel of the pixels in the image. We use blue channel of the pixel because human rarely can detect the change in blue channel with naked eye. For embedding we use bit adjusting algorithm in the RGB pixels in the image. Fig. 2 shows the architecture of bit adjusting embedding algorithm and the steps are described in the following:

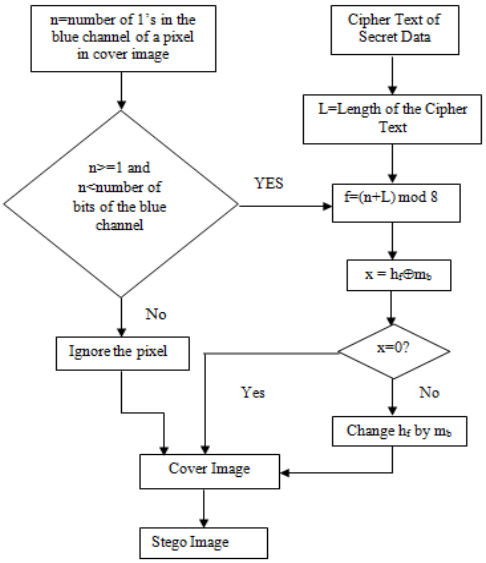


Fig. 2: Bit adjusting Embedding architecture of Cipher Text

Step 1: convert the cipher text into bits and compute the length *L* of the bits.
Step2: Compute *n*, the number of 1's from the blue channel of the pixel in cover image.
Step 3: If *n* is equal or greater than one and less than number of all the bits of the blue channel of the pixel, then it is a candidate for bit embedding otherwise the pixel will not be considered and go to the next pixel of the cover image
Step 4: calculate *f= (n+L) mod 8*, here *L* means the length of the bits of cipher text and 8 is the number of bits in one pixel.
Step 5: Calculate $x=h_f$ *xor* m_b (h_f = bit of the candidate in position *f* and m_b is the message bit to embed). m_b is counted from the least significant bits to the most significant bits.
Step 6: If $x = 0$, that means the text bit is same as host candidate bit , then there is no need to change and if $x = 1$, that means text bit and the host candidate bit is different, then change h_f by m_b.

B. Decoding Process

The inverse of encoding is decoding. In the decoding process, first we extract the cipher text from the stego image. Then we decrypt the cipher text with the same symmetric algorithm AES-128 with SHA-512. After this, we get out real secret text message. Like encoding, decoding is performed using two different algorithms: one for extraction and other for decryption.

1) Extraction: Extraction is the inverse process of embedding. Fig. 3 shows the bit adjusting extraction architecture and the steps are described in the following:

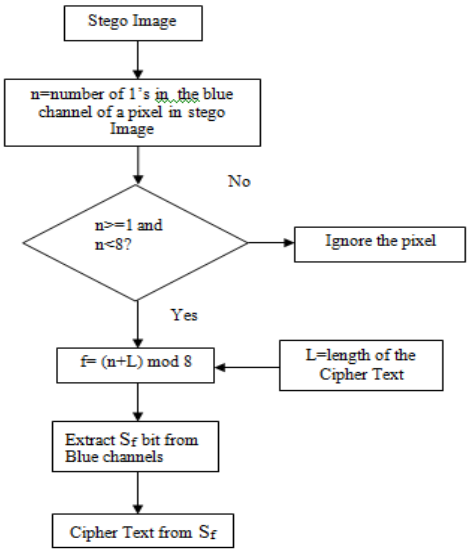


Fig. 3: Architecture of bit adjusting extraction process

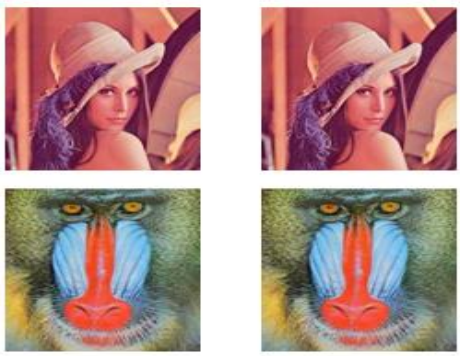
Step 1: Compute *n*, the number of 1's from the blue channel of pixel of stego image
Step 2: If *n* is greater than or equal to 1 and less than number of all the bits of the selected blue channel of the pixel, then it is a candidate for bit extraction otherwise don't consider the pixel and go to next pixel.
Step 3: calculate $f = (n+ L) \bmod 8$, where *L* is the length of the cipher text and 8 is the number of bits in one pixel.
Step 4: Then extract the bit S_f (S_f = bit of the stego blue channel in position *f*).
Step 5: repeat the steps 1 to 4 until all the bits (equal to *L*) of the cipher text is extracted.
Step 6: After finding all the bits, convert it into text, which is the cipher text.

2) Decryption: Decryption means converting cipher text into real text. After extraction process, we get the cipher text which is needed to decrypt to obtain the real secret text message. In decryption, we take cipher text of the previous steps as input and then decrypt the cipher text with same AES-128 with SHA-512. Finally we get the secret text which was embedded into the cover image.

III. EXPERIMENTAL RESULTS

Different sizes of images are used for experiment. Some well known images that are used in image processing field are used here for evaluation such as Lena, Baboon, Pepper, Fruits, and Drawing. To evaluate the performance of the proposed method, we measure the stego image quality, PSNR (Pick Signal to Noise Ratio), and Histogram error of the images.

Fig. 4 shows examples of cover image and their corresponding stego image. As more data in the image is added, the stego image quality is got down. But in our work the stego image quality remains good after embedding sufficient secret data. That means eavesdropper cannot see any change in the image visually.



(a) (b)
Fig.4: (a) cover image (b) stego image

we calculate the PSNR which is ratio between maximum power signal and distorting of noise to estimate the image quality. $PSNR = 10\,log\,10\,(\frac{C_{max^2}}{MSE})$, where MSE means the mean square error between cover image and stego image. Table 1 shows the calculated PSNR of stego images.

TABLE I
PSNR VALUE OF VARIOUS STEGO IMAGES IN PROPOSED SYSTEM

Image Name	PSNR (dB)
Lena	52.3646
Baboon	43.7594
Pepper	46.9322
Fruits	72.7676
Drawing	68.8769

Comparing with [3] of Mamta Juneja et. al., we got better PSNR. Table 2 shows the comparison value.

TABLE II
PSNR COMPARISON

Image Name	PSNR of [3]	PSNR of Proposed System
Lena	47.5897	52.3646
Baboon	36.3637	43.7594
Pepper	45.9238	46.9322

To do performance evaluation we also calculate the histogram error. Histogram error is the square error between the histogram of cover image and stego image. Fig. 5 and Fig. 6 shows the histogram error of Lena and Baboon images respectively, where *x*-axis denotes the pixel intensity of a gray level of a image and *y*-axis denotes the amount of pixels in the gray scale level.

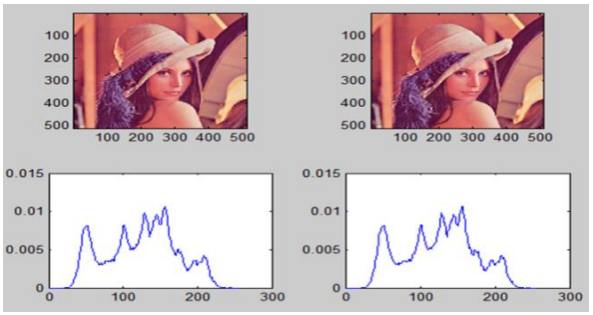


Fig. 5: Histogram of Lena

The histogram error of Lena image is=0.00195.

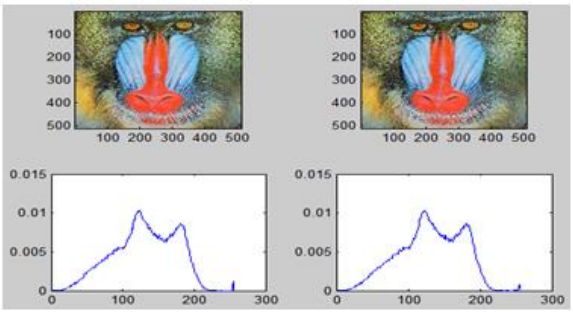


Fig.6: Histogram of Baboon

The histogram error of Baboon image is = 0.00975. We see here that the histogram error is very low. We evaluate others images as well. The experimental results show that all of the characteristics of good steganography are preserved in stego images and the proposed method shows robust result than several existing methods.

IV. CONCLUSION

In this paper, we proposed a system that can steg a textual message in a proper secure way. In encryption module, we choose robust symmetric algorithms with secured hash function that is most effective for encryption of a text. We use hash function that give us a extended combination of hash key for encryption. In embedding and extraction, we use the bit adjusting method which helps the message bits to go deeper in to image intensity. Message capacity and stego-image quality are two important criteria in evaluating a steganogarphic method. The approach of bit adjustment based image steganography fulfill the criteria. We see that our implemented system work effectively and efficiently in a most secured, robust, error free way for textual message of high capacity.

REFERENCES

[1] T. Morkel, J.H.P. Eloff, and M.S. Olivier, "An Overview of Image Steganography,**"** Information and Computer Security Architecture (ICSA) Research Group, Department of Computer Science, University of Pretoria, 0002, Pretoria, South Africa.

[2] V. Lokeswara Reddy, A.Subramanyam, and P. Chenna Reddy, "A Novel Approach for Hiding Encrypted Data in Image, Audio and Video using Steganography ," *International Journal of Computer Applications* ,Vol. 69, No.15, May. 2013.

[3] MamtaJuneja, Dr. Parvinder, and S. Sandhu, "An Improved LSB based Steganography Technique for RGB Color Images," in *Proc. ICLCT'13,*

June 17-18, 2013.
[4] FrankHartung and Martin Kutter, "Multimedia Watermarking Techniques", *Proceedings of the IEEE*, Vol. 87, No. 7, pp. 1085 – 1103.
[5] Hemalatha S, U Dinesh Acharya, Renuka A, and Priya R. Kamath, "A Secure Color Image Steganography in Transform Domain," *International Journal on Cryptography and Information Security*, Vol.3, No.1, Mar. 2013.
[6] M.Jyotheeswari and Kadapa,Y.S.R. "A Novel Steganographic System for Data Hiding in Video," *International Journal of Computer Applications*, Vol. 82, No. 11, Nov. 2013.
[7] RajkumarYadav, "A Novel Approach For Image Steganography in Spatial Domain Using Last Two Bits of Pixel Values," *International Journal of Security*, Vol.5, Iss.2, pp. 51-61.
[8] R. Amirtharajan, Sandeep K. Beher, Motamarri A. Swarup, Mohamed Ashfaaq, John Bosco, and BalaguruRayappan, "Colour Guided Colour Image Steganography,",*Universal Journal of Computer Science and Engineering Technology*, Vol.1, pp.16 – 23, 2010.
[9] Hemalatha.S, U.DineshAcharya, and Renuka.A, "Comparison of Secure and High Capacity Color Image Steganography Techniques in RGB and YCBCR domains," *International Journal of Advanced Information Technology*, Vol.3, No.3, pp.1-9, 2013.
[10] GurmeetKaur and AartiKochhar "A Steganography Implementation based on LSB & DCT," *International Journal for Science and Emerging Technologies with Latest Trends*, vol.4, iss.1, pp.35-41, 2012.

