ARTICLE

AN EFFICIENT STEGANOGRAPHY ALGORITHM USING VISUAL CRYPTOGRAPHY AND AES ENCRYPTION

Velumurugan Andi* and Logashanmugam Edeswaran

Dept. of Electronics and Communication Engineering, Sathyabama University, Chennai, INDIA

ISSN 0976-3104

ABSTRACT

In this paper, an efficient approach for securing information is presented by the combination of steganography, cryptography, and visual cryptography. Steganography is a process by which the transmitting information is secured in a defined manner. At first, the secret information is divided into two shares by random grid techniques as similar in visual cryptography. Then, one of the shares is embedded by Least Significant Bit (LSB) into the cover image. Finally, Advanced Encryption Standard (AES) is used for encrypting the embedded image. The cipher key for encrypting the data is generated by the use of Discrete Cosine Transform (DCT) on the cover image. To recover the secret image, both cipher key, and the remaining share are required which increases the level of security.

KEY WORDS
Steganography, discrete cosine transform, visual cryptography, advanced encryption, decryption

Received: 22 Aug 2016
Accepted: 28 Aug 2016
Published: 5 Oct 2016

INTRODUCTION

Steganography is data hiding method used to hide the secret information into the cover information. The cover data can be in any form such as documents and media files. Many studies have been done in connection with steganography. The secret information is hidden in random pixels [1]. The selection of random pixels is based on location, shape, and colour of the pixels in the cover image. After selecting the random pixels, LSB approach is used to hide the secret information. A modified LSB image steganography technique is described in [2]. Braille method is used for representing secret data by six bits only. Among the six bits, three bits are hidden in the red layer; two bits are on the green layer and one bit in the blue.

Genetic algorithm and visual cryptography based algorithm is designed [3] to transmit over networks. At first, LSB approach is used for hiding secret into cover. The security of the secret data is increased by modifying the location of pixels based on genetic algorithm. This data is split by visual cryptography into two shares. In order to retrieve the secret data, the receiver has to apply the reverse process using the secret key. An approach for multiple secret sharing schemes is discussed [4]. From the two secret data, only two shares are created by XOR operations and then, they are encrypted. While decoding, the secret data cannot be validated if decryption is not possible.

A simple approach for better security is achieved [4,5] by using LSB based steganography. The Advanced Encryption Standard (AES) cryptography will change the secret message into cipher text and to ensure two layer security of the message. The LSB bit is used for storing the status bit and not the message bit. An AES based secured steganography system is implemented in [6] which uses 128 bit for both plain text and secrete key. The state-of-art steganography approaches are reviewed [7]. The different types of steganography such as image steganography, audio steganography, and video steganography are focused.

A reliable steganography approach both in a gray and colour image is described [8]. The secret data is embedded in randomly scattered pixels which increase the security of the data. A robust audio steganography is designed in the temporal domain [9]. For additional security, AES is used. The embedded sequence is changed dynamically and randomly. A combination of cryptography and steganography is used for security [10]. The security level is increased in the key level by SHA-1. LSB is used for embedding process, and AES is used for encrypting the cover data.

In this paper, an efficient approach for hiding data is presented using visual cryptography, AES encryption, and LSB embedding process. The paper is arranged in the following order. In section 2, the methods and materials used by the proposed approach are discussed. The results obtained by the proposed system are discussed in section 3, and finally, the conclusion is given in section 4.

***Corresponding Author**
Email:
an.velmurugan@rediffmail.com
Tel.: +919841727370

MATERIALS AND METHODS

The proposed steganography algorithm is built by the use of two well-known techniques namely LSB embedding process and AES encryption. The level of security of the secret image is increased based on these two algorithms. Steganography is a data hiding method used to hide the secret information into the cover information. The proposed work mainly focuses on the LSB technique to hide the secret messages into the cover image. Advanced Encryption Standard (AES) is used for encrypting the embedded image. The main feature of the proposed work is two level securities with DCT based cipher key generation. The proposed steganography algorithm using visual cryptography and AES encryption is shown in [Fig.1].

IIOAB JOURNAL
ISSN: 0976-3104

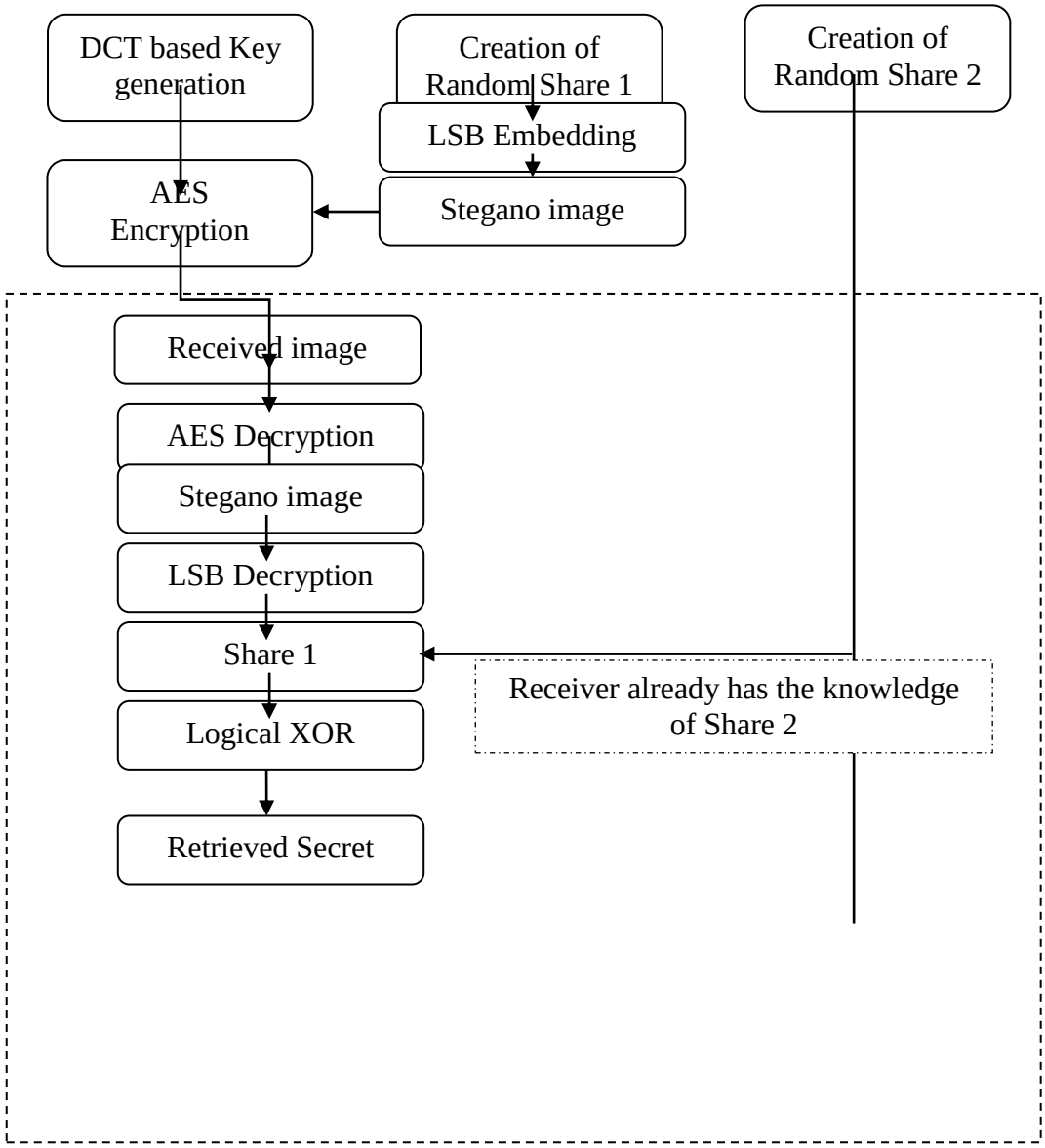

Fig. 1: Block diagram of the proposed steganography algorithm using visual cryptography and AES

Visual Cryptography

Three algorithms for encryption are discussed in [11] by random grids. The given binary secret image is encrypted into two cipher grids of the same size. The first cipher grid is created by assigning each and every pixel with either 0 (black) or 1(white). By the use of secret image and the first cipher grid, the second cipher grid is created. Both cipher girds are required to recover the secret image. Thus, one of the two random grids is given to the receiver for verification. If the random grids are stacked with logical XOR operation, the secret image is revealed. The proposed approach uses the same technique to generate two shares from the secret image. Then one of the shares is embedded into the cover image for first level security.

LSB embedding process

To hide the cipher grid into the digital cover image or else another media is based on Least Significant Bit modification technique. LSB is one of the spatial domain methods. The LSB of the binary sequence of each pixel is replaced with the binary of the secret message. It provides high security for transmitting much information and easy to implement and to combine with other hiding techniques. For an 8-bit grayscale image, each pixel is represented by 8 bits. The last bit in a pixel is called as Least Significant bit as its value will affect the pixel value only by "1".

IIOAB JOURNAL
ISSN: 0976-3104

AES Encryption and Decryption

In December 2001, the NIST published a symmetric key block cipher is called as AES [12]. AES encrypts and decrypts a data block of 128-bits. It depends on some rounds. The input to the algorithm is a single 128-bit block. The block is represented as a row of the matrix of 16 bytes. The process of converting the original data to ciphertext is called encryption. It is achieved by applying mathematical transformations. These transformations are called as encryption algorithms and require an encryption key. The proposed system uses DCT [13] for generating the key. Decryption is the reverse process which outputs the original data from the cipher text using the same key.

RESULTS AND DISCUSSION

This section gives the simulation results of the proposed system described in the above section. [Fig. 2] shows the secret image and their corresponding two shares created by random grid techniques. In random grid techniques, one share is created by generating random numbers of 0's and 1's. The second share is created using XOR approach by the use of the first share.

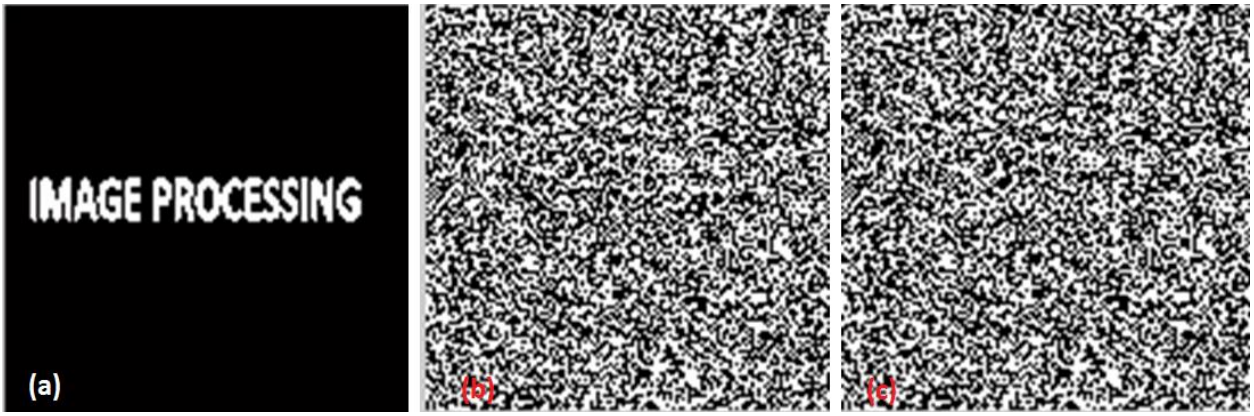

Fig. 2: (a) Secret image **(b)** Share 1 **(c)** Share 2

After share creation, the second share is given to the receiver to verify the data. The next step is the application of embedding technique. The first share is embedded into the cover image by LSB process. [Fig. 3] shows the cover image and the embedded image.

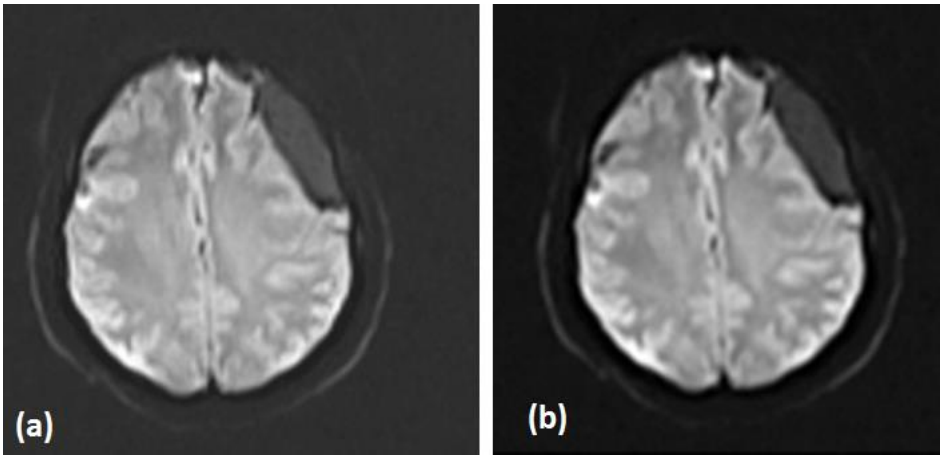

Fig. 3: (a) Cover image **(b)** Embedded Image

From the [Fig. 3], it is observed that there is no difference between the cover image and embedded image. Thus, no body has the knowledge that the secret image is hidden into that cover image. Further, the security of the secret image is increased by the use of AES encryption. The key for encryption is obtained by DCT decomposition of the cover image. From the AC and DC coefficients, 126-bit key is generated and then the embedded image is encrypted using it. This encrypted image is transmitted. At the receiver side, the receiver decrypts the image at first. Then, the first share is retrieved by the reverse LSB process.

Finally, the secret image is obtained by the XOR operation of retrieved first share and the second share in the receiver hands. Fig. 4 shows the AES encryption and decryption images along with retrieved secret image.

IIOAB JOURNAL
ISSN: 0976-3104

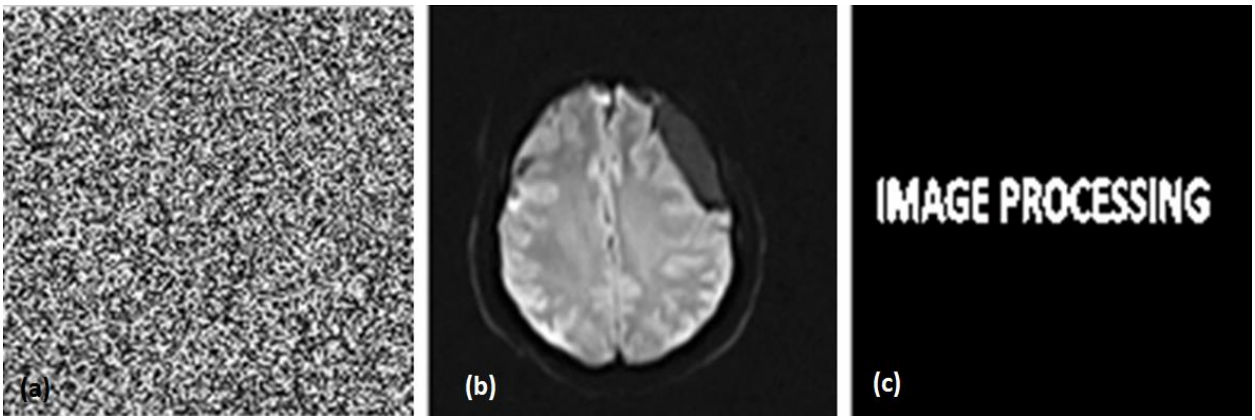

Fig. 4: (a) Encrypted Image **(b)** AES Decrypted Image **(c)** Retrieved Secret image

CONCLUSION

In this paper, an efficient steganography algorithm using visual cryptography and AES encryption is presented. Visual cryptography technique is applied to generate two shares from the secret image. Then, one of the shares is embedded into the cover image using LSB procedure. The cipher key is generated using DCT transform and used with AES algorithm to encrypt the embedded data. The level of security of the secret image is higher than the standard steganography and encryption algorithm as the proposed system combines the visual cryptography into them. Hence, without the knowledge of the second share, no one can recover the secret information. In future, the proposed system can be extended to identify the tampered regions if anyone attempts to recover the secret and modify the information.

CONFLICT OF INTEREST

There is no conflict of interest.

ACKNOWLEDGEMENTS

None.

FINANCIAL DISCLOSURE

None.

REFERENCES

[1] Diwedi S, Agrawal D.[2013] Random image steganography in spatial domain" Emerging trends in VLSI, embedded system, nano electronics and telecommunication system (ICEVENT), 2013 international conference on. IEEE, pp. 1-3.

[2] Emam MM, Aly AA, Omara FA. [2015] A Modified Image Steganography Method based on LSB Technique. International Journal of Computer Applications, 125(5).

[3] Rehana BR, Pradeep DS. [2014] Best Approach for LSB based Steganography Using Genetic Algorithm and Visual Cryptography Secured Data Hiding and Transmission over Networks," International Journal of Advanced Research in Computer Science and Software Engineering, 4(6).

[4] Khairnar S, Kharat R. [2016] A Secure and Verifiable Multi Secret Sharing Scheme for Encrypting Two Secret Images into Two Shares. International Journal of Computer Applications, 134(11):27-29.

[5] Islam MR, Siddiqa A, Uddin MP, Mandal AK, Hossain MD. [2014] An efficient filtering based approach improving LSB image steganography using status bit along with AES cryptography. IEEE International Conference on Informatics, Electronics and Vision, pp. 1-6.

[6] Ramaiya M, Hemrajani N, Saxena AK. [2013] Secured Steganography Approach Using AES. International Journal of Computer Science Engineering and Information Technology Research, 3:185-192.

[7] Kamble MPR Waghamode MPS Gaikwad MVS, Hogade MGB. (2013) Steganography Techniques: A Review. International Journal of Engineering 2(10).

[8] Fridrich J, Goljan M, Du R. [2001] Reliable detection of LSB steganography in color and grayscale images. In Proceedings of the 2001 workshop on Multimedia and security: new challenges (pp. 27-30).

[9] Kanhe A Aghila, G Kiran, CYS Ramesh, CH Jadav G, Raj MG. [2015] Robust Audio steganography based on Advanced Encryption standards in temporal domain. IEEE International Conference on Advances in Computing, Communications and Informatics, pp. 1449-1453.

[10] Thomas SE. Philip ST, Nazar S, Mathew A, Joseph N. (2012) Advanced Cryptographic Steganography Using Multimedia Files. In International Conference on Electrical Engineering and Computer Science.

[11] O Kafri and E Keren. [1987] Encryption of pictures and shapes by random grids," Optics Letters, 12(6): 377 - 379.

[12] Daemen J, Rijmen V. [2013]The design of Rijndael: AES-the advanced encryption standard. Springer Science & Business Media.

[13] Lin SD , Chen CF.[2000] A robust DCT-based watermarking for copyright protection. IEEE Transactions on Consumer Electronics, 46(3): 415-421.