Scientific Journal Impact Factor (SJIF) : 1.711
International Journal of Modern Trends in Engineering and Research
ISSN (ONLINE) : 2349 - 9745 ISSN (PRINT) : 2393 - 8161

MOSAIC IMAGE STEGANOGRAPHY BASED COLOUR TRANSFORMATION FOR ENHANCED SECURITY

Merin Joseph[1] , Soumi CG[2]

[1,2]*Department of Computer Science, IIET, Nellikuzhi*

Abstract—A new secure image transmission method is proposed, Here it uses the technique of Steganography and Cryptography, Which transforms automatically a given large-volume secret image into a so-called secret-fragment-visible mosaic image of the same size. The mosaic image which looks similar to an arbitrarily selected target image and may be used as a disguise of the secret image is yielded by dividing the secret image into fragments and transforming their color characteristics to be individuals of the corresponding blocks of the target image. Then applying encryption method and adding relevant information /key and get back the data with decrypting by the give key for improving security, Skillful techniques are designed to behavior the color transformation process so that the secret image may be recovered nearly lossless. A scheme of handling the overflows/underflows in the converted pixels' color values by recording the color differences in the untransformed color space is also proposed. The information required for recovering the secret image is embedded into the created mosaic image by a lossless data hiding scheme using a key. Good experimental results show the feasibility of the proposed method.

Keywords—Steganography,Cryptography,Mosaic image.

I. INTRODUCTION

At the present time, images from various sources are transmit and received beyond the internet used for a variety of applications, such as online personal photograph albums, secret medical imaging systems, and military image databases. The images generally contain hidden information i.e they must be protected from leakages through attacks during transmissions. Several methods have been proposed in aid of securing image transmission, designed for there are two common approaches- image encryption and data hiding. Image encryption is a technique with the purpose of encrypt image into noise form, using high redundancy and strong spatial correlation. The encrypted image is presently a noiseful image file that no one can achieve or recognize the secret image from it except has the correct key. On the other hand, the encrypted image is a worthless, noiseful image, which is totally inoperative before decryption and may stimulate an attacker's attention during transmission because of its uncertainty in form.

Another way for secure image transmission is data hiding. Data hiding is different from an image encryption, data hiding that hide secret image into a cover image so that no one can recognize the survival of the secret information. The main problem of the methods for data hiding is that around is difficulty in embedding a bulky amount of information cannot hide into a single image. In particular, if one needs to hide a secret image into a cover image with the equal size, the secret image should be highly compressed into move ahead. The recent technique for secret image transmission is proposed by the help of secret image and target image. In this paper, a new method for secure image transmission through combined steganography and cryptography is proposed. Select two images such as secret and target image. After selecting the target image, the known secret image is first divided into number of rectangular fragments called tile images, which then are fit into similar blocks in the target image, called target blocks, according to a similarity of color transformation [1]. After that, the color features of each tile image is transformed into the former color, ensure in a

mosaic image which looks like the target image. Ensuring a mosaic image add an applied by a cryptography. Appropriate schemes are also proposed to conduct nearly lossless recovery of the original secret image from the resulting mosaic image.

Figure 1. Result yield with the proposed method. (a) Secret image. (b) Target image. (c) Secret-fragment-visible mosaic image formed from (a) and (b) by the proposed method.

As an illustration, Fig. 1 shows a result yielded by the proposed method. In particularly, after a target image is selected randomly, the given secret image is first divided into rectangular fragments called tiles, which then are fit into related blocks in the target image, called target blocks, based on a resemblance principle of color characteristics. In addition, the color characteristic of all tile images is altered to the color characteristics of the corresponding target block of the above said target image. It forms a mosaic image which looks similar to the target image.

Concurrent methods are also proposed near implement-to lossless recovery of the original secret image from the ensuing mosaic image. The proposed method is innovative anywhere into a meaningful mosaic image is formed, where seeing that in the image encryption method that only meaningless noise images are created. Furthermore, this process know how to transform a secret image into a disguising mosaic image without compression, at the same time as a data hiding method have to hide a highly compressed image into a mosaic image when the secret image and the cover image have the same data size.

II. RELATED WORKS

This section describes a variety of existing schemes which are compared in this paper. Several contributions have been made in the field of information security. Up to date year both steganography and cryptography attain a diversify stage of security. A New Secure Image Transmission Technique via Secret-fragment-Visible Mosaic Images by Nearly Reversible Colour Transformations[1] In this paper, Yak-Lin Lee shows a technique for the transmission of the secret image and the target image are selected without the use of database and without any restrictions on the selections.

The original idea of the mosaic image steganography has been proposed by Secret-Fragment-Visible Mosaic Image–A New Computer Art and Its Application to Information Hiding by Lai and Tsai [2]. This colour transformation is controlled and the secret image is recovered lossless from the mosaic tile image with the help of the extracted relevant information generated for the recovery of the image. The drawback of this paper is that it cannot be applied to the images of other colour models other than RGB, along with some security considerations in case of hacking the image being passed [1]. Hiding data in images by simple LSB substitution [5], In this paper, important data are embedded in the cover image to protect the original data from illegal access. Genetic algorithms are

used to hide data in rightmost k LSB's of cover image. The drawback here, is when the size of storing message is increased, image quality of the cover image degraded gradually [5].

Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption [6], In this paper, Ked Ma shows a method for data hiding into an image by reserving room before encryption of the image. This paper shows that first enough space is reserved in the image after which it is converted into encrypted form [6]. A Keyless Approach to Image Encryption, by Indian Institute of Technology Rookie [3], this paper shows a keyless approach to encryption methods which are used to encrypt images. We make the use of this paper to apply the keyless approach in the proposed method. This is done by generating relevant information with the help of some RMSE value which help to rotate the tile images to a certain angle [3]. JPEG: Still Image Data Compression Standard [4] Here, W. B. Penne baker tries to explain that the main obstacle in many applications is the quantity of data required to represent a digital image. For this we would need an image compression standard to maintain the quality of the images after compression. To meet all the needs JPEG standard for image compression [4].

III. PROPOSED WORK

The purpose this paper propose a technique of combining cryptography and steganography to solve the problem of unauthorized information or data access. Steganography also can be implemented to cryptography so that it increases the security of this data. Proposed method includes by three phases: mosaic image creation, Encryption and Decryption used by a secret key and finally get the secret image recovery.

In the mosaic image creation initially choose the secret and target image. Secret image and target image having same size, secrete image is divided into number of fragments called tile images. Next, target image it again separated taken with same number of tiles as that of secrete image then apply the colour transformation on it the fit that tiles of secret image into target block and form a mosaic image. The phase include four stage i.e a) Fitting the tile images of the secret image into the target blocks of a pre-selected target image; b) Transforming the colour characteristic of each tile image in the secret image to become that of the corresponding target block in the target image; c) Rotating each tile image into a direction with the minimum RMSE value with respect to its corresponding target block; d) Embedding relevant information into the created mosaic image for future recovery of the secret image.

In the second phase, consist of applied a visual cryptography. In the first phase created by a mosaic image, then the mosaic image will be applied a encryption and decryption used by a key. AES method will be applied in encryption and decryption process .Adding a information or a key by the encryption, then the process of encryption will be completed after the decryption process will be started. The process of encryption and decryption key must be same. Decryption process by a completed then get the mosaic Image And in the third phase, the embedded information is extracted to recover nearly listlessly the secret image from the generated mosaic image.

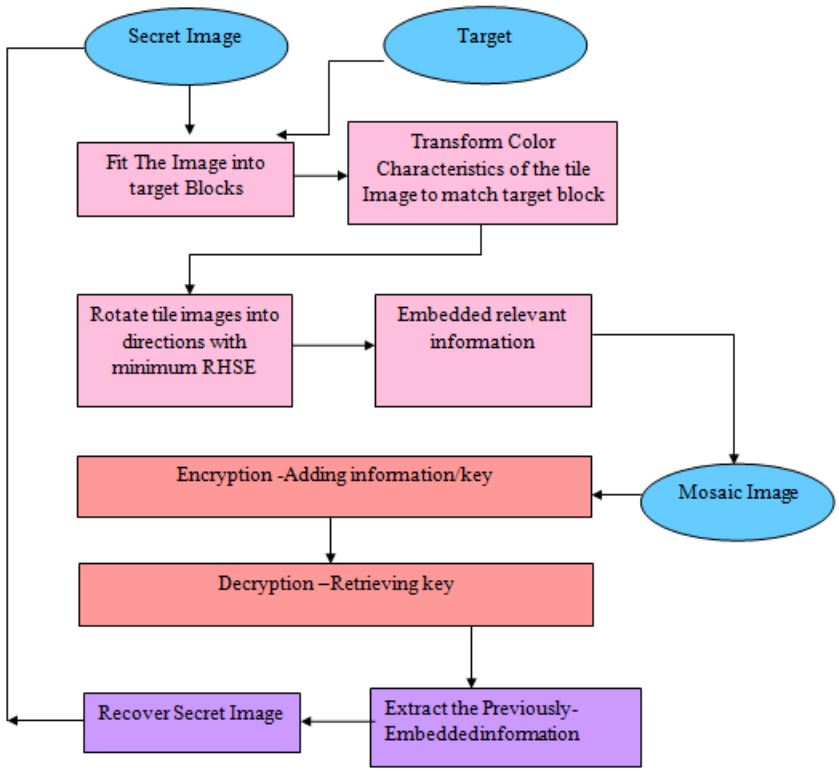

Figure 2 . Processes for secret-fragment-visible mosaic image creation and secret image recovery

The phase includes two stages: In the recovery of secret image module firstly take mosaic image then extract embedded information from it and recover the information and secret image. The module includes two stages: Extracting the embedded information for secret image recovery from the mosaic image; Recovering the secret image using the extracted information. The combination of these two methods will enhance the security of the data embedded and will satisfy the requirements such as capacity, security and robustness for secure data transmission .The intended receiver should be able to recover the embedded data successfully, without any errors.

IV. ALGORITHM OF THE PROPOSED METHOD

Algorithm 1: secret-fragment-visible mosaic image creation.

Input: A secret image S; a target image T; and a random number generator by using AES and secret key K.
Output: A secret-fragment-visible mosaic image F.

Stage 1: Fitting tile images block of secret images into tile images block of target blocks
Stage 2:Transforming colour transformation between the every tile of secret image to the corresponding target blocks of target image
Stage 3: Rotating the entire tile images.
Stage 4: Embed information for recovery purpose and apply AES Encryption.

Algorithm 2: secret image recovery.

Input :A mosaic image F with n tile images {T1, T2, ,Tn} and the random number generator by AES and the secret key K.
Output: The secret image S.

Stage 1: Extracting the embedded information's from recovery

Stage 2: Recovering the Secret image

V. RESEARCH METHODOLOGY

The method is divided into two modules- sender and receiver module. The sender and receiver module contains two main techniques: cryptography and steganography. Sender part contains loading a secret and target image, after the selection process should be completed, fitting the tile images into the target. Mosaic image created by the process of mapping, transformation and rotation. After created a mosaic image must be embedding an additional information or key, and then starting the process of encryption. The second module contains the extracting information, finally retrieve the required image. The flow of the research is:

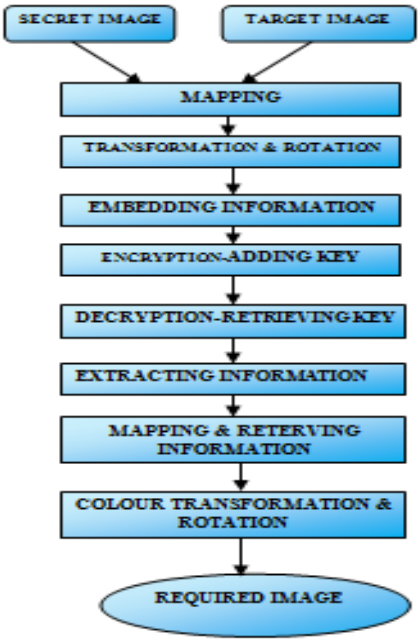

Fig 3 Flow chart of mosaic image creation and secret image recovery

The proposed tactic is implementing by MATLAB programming. It has chiefly two phases. Within the encryption phase, initial choose our secret image and subsequently arbitrarily choose our target image. For encryption, use AES algorithm and key based random permutation .Using LSB method, we can produce an successful mapping sequence and using LSB method then sequence is again permuted. On the decryption phase provide the same key and recover the secret image. Activity is done by MATLAB. At this time the secret image is successfully hide into the target image by means of providing both the images have the equal size .It is a lossless secret image hiding technique.

VI. EXPERIMENTAL RESULTS

The proposed method is experiment through MATLAB. The mosaic image is to be initially encrypted to produce the decrypt image using substitution cipher method. A key is use during the encryption which is base on symmetric cryptosystem where identical key is used for both encryption and decryption process. Then the cipher text is embedding inside the JPEG image using AES method that embeds the information in the frequency domain. The generated Stego-image is sent over improving to the intentional recipient. The entire idea of the proposed method is to form a method that enables secure data communication between sender and receiver. By this approach the secret image is effectively embed into the cover images. In the way of recovery the mosaic image is initial extract from the Stego-image. The mosaic image is at that time decrypted by producing the key used

in encryption to get back the original image based on color transformation. But the key does not match, the original information will remain unreadable.

The known secret image is first separated into rectangular fragments called tile images, which followed by fit into similar blocks in the target image, called target blocks, according to a Similarity principle based on color variations. After that, the color characteristic of every tile image is changed to be that of the equivalent target block in the target image, resultant in a mosaic image which looks similar to the target image. Relevant scheme are also planned to conduct nearly lossless revival of the original secret image. The Root Mean Square Error (RMSE) is a used to compute the error between recover image and original image. This calculated difference is called residuals and the RMSE serve to cumulative them into a single measure of analytical power.

Fig 4 an experimental result of mosaic image creation. (a) Secret image. (b) Target image. (c) Mosaic image created among tile image size 8×8. (d) Recovered secret image use a correct sequence with PSNR = 48.67 and with RMSE =0.978 with respect to secret image (a) . (e) Recovered secret image using a wrong sequence. (f)-(h) Mosaic images created with different tile image sizes 8×8,16×16, 24×24, 32×32

The output is tested among a variety of inputs. A relative study with dissimilar tile image sizes be present finished and check the RMSE values of every one. The result shown in figure.4, where figure 4a) represent a secret image have the size 1024×768 or 768 ×1024 and figure 4 b) represent the target image since the same size as the secret image and figure 4 c) show the produced mosaic image via figure 4 a) and figure 4 b). Figure 4 d) represents the improved secret image from the mosaic image with a accurate sequence and having PSNR=48.67 and RMSE=0.978 with the secret image. We cannot feel the dissimilarity between the two images because PSNR is larger than 30 and RMSE is closer to 1.0. PSNR values are larger than 47 and RMSE values close to 1.0. Back to negotiations on figure 4) figure 4(e) show the recovered image having a incorrect sequence, which is a noisy image Figure 4(f),4(g) and4(h) shows different tile images. The laboratory analysis of these figures results that the formed mosaic image retain more detail of the target when the tile image contain smaller size (eg:, 4×4 and 8×8).Figure 4 established this concept. In figure 4a) the tile image size is 8×8 and have smaller RMSE values and when the tile image size is bigger like 32×32 ,the created mosaic image at rest look relatively similar.

VII. CONCLUSION

The work accomplished during this project can be summarized with the following points. In this project we have presented a new system for the combination of Steganography and cryptography using four keys which could be proven a highly secured method for data communication. Steganography, especially combined with cryptography, is a powerful tool which enables people to communicate without possible eavesdroppers even knowing there is a form of communication in the first place. The proposed method provides acceptable image quality with very little distortion in the image. The main advantage of this Steno/Crypto System is that the method used for encryption, AES, is very secure and the LSB embedding with RGB color transformation Steganography techniques are very hard to detect.

.

REFERENCES

.

[1] L. H. Zhang, X. F. Liao, and X. B. Wang, "An image encryption approach based on chaotic maps," Chaos Solti. Fact., vol. 24, no. 3, pp. 759– 765, 2005

[2] Z. Ni, Y. Q. Shi, N. An sari, and W. Su, "Reversible data hiding," IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354–362, Mar. 2006.

[3] I. J. Lai and W. H. Tsai, "Secret-fragment-visible mosaic image—A new computer art and its application to information hiding," IEEE Trans. Info Forensic. Secure., vol. 6, no. 3, pp. 936–945, Sep. 2011.

[4] E. Rein hard, M. Ashikhmin, B. Gooch, and P. Shirley, "Color transfer between images," IEEE Comput.Graph. Appl., vol. 21, no. 5, pp. 34–41, Sep.–Oct. 2001.

[5] J. Fridrich, M. Goljan, and R. Du, "Invertible authentication," Proc.SPIE, vol. 3971, 2001, pp. 197–208.

[6] T. S. Cho, S. Avidan, and W. T. Freeman, "A probabilistic image jigsaw puzzle solver," in Proc. IEEE CVPR, 2010, pp. 183–190.

[7] C. C. Chang, C. C. Lin, C. S. Tseng, and W. L. Tai, "Reversible hiding in DCT- based compressed images," Inf. Sci., vol. 177, no. 13, pp. 2768–2786, 2007.

[8] J. Tian, "Reversible data embedding using a difference expansion," IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890–896, Aug. 2003.

[9] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, "Image quality assessment: From error visibility to structural similarity," IEEE Trans. Image Process., vol. 13, no. 4, pp. 600–612, Apr. 2004.

[10] D. Coltuc and J.-M. Chassery, "Very fast watermarking by reversible contrast mapping," IEEE Signal Process. Lett., vol. 14, no. 4, pp. 255–258, Apr. 2007.

.