ISSN 2347 - 3983

International Journal of Emerging Trends in Engineering Research (IJETER), Vol. 3 No.6, Pages : 304 - 307 (2015)
Special Issue of NCTET 2K15 - Held on June 13, 2015 in SV College of Engineering, Tirupati
http://warse.org/IJETER/static/pdf/Issue/NCTET2015sp58.pdf

SECURE IMAGE STEGANOGRAPHY via SECRET FRAGMENT MOSAIC IMAGES AND VISUAL CRYPTOGRAPHY

T.Hemanth Sai[1], M.Hemalatha[2]
PG Student (Embedded Systems), Department of ECE, Sri Venkateswara College of Engineering, Tirupati, India,
hemanthsai.theegal@gmail.com
[2]Assistant Professor, Department of ECE, Sri Venkateswara College of Engineering, Tirupati, India,
maddihemalatha@gmail.com

ABSTRACT

A new secure image Steganography is proposed, images from different sources are used to transmit via internet for so many purposes such as confidential achieves, military images, Medical image process. The large volume-sized secret image is transformed in to secret fragment visible mosaic image. It also handles the overflows and underflows in the transformed pixels.

The data hiding is based on Image encryption technique and recovered through Decryption. The secret image divided into blocks and transforms their block processed and color characteristics into blocks of target size. Secret Image is embedding in the target image by skilful technique. The information needed for recovering secret image which is embedded into processed mosaic image by a lossless with data hiding scheme using a key.

Keywords - Steganography, Data hiding, Image encryption, Secret Fragment Mosaic Image.

1. INTRODUCTION

Recently, many methods have been used for securing image transmission. The two common approaches are image encryption and data hiding. Image encryption is a technique that uses the natural property of an image, like high redundancy and strong spatial correlation, to get an encrypted image based on Shannon's confusion as well as diffusion properties.

The encrypted image is a noise image so none can obtain the secret image from it unless he/she has the correct key. However, the encrypted image is a useless file, which can't provide any additional information before decryption and may arouse an attacker's mind during transmission due to the randomness in form. An alternative for this problem is data hiding, which hides a secret message into a cover image due to that no one can think the existence of the secret data, in which the data type of the secret message learnt in this paper, is an image.

In this paper, a new technique for secure image transmission proposed, which transforms a secret image into a meaningful mosaic image with the same size and looking like a preselected target image. The transformation process is controlled by a secret key, and only with the key can a person recover the secret image nearly lossless from the mosaic image.

The proposed method is inspired by Lai and Tsai [1] in which a new type of computer art image, called secret-fragment-visible mosaic image, was proposed. The mosaic image is the result of rearrangement of the fragments of a secret image in disguise of another image called the target image preselected from a database. But an obvious weakness of Lai and Tsai [1] is the requirement of a large image database so that the generated mosaic image can be sufficiently similar to the selected target image. Using their method, the user is not allowed to select freely his/her favourite image for use as the target image.

It is therefore desired in this study to remove this weakness of the method while keeping its merit, that is, it is aimed to design a new method that can transform a secret image into a secret fragment-visible mosaic image of the same size that has the visual appearance of any freely selected target image without the need of a database.

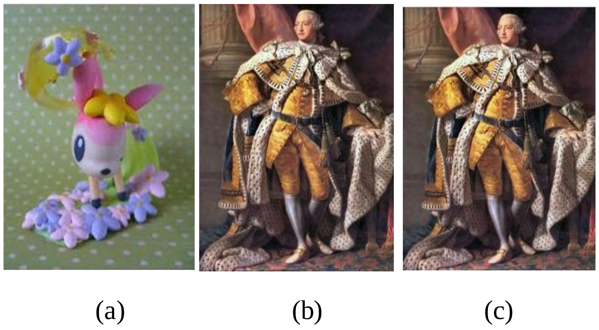

Figure 1. Result yielded by the proposed method. (a) Secret image. (b) Target image. (c) Secret-fragment-visible mosaic image created from (a) and (b) by the proposed method.

As an illustration, Fig. 1 shows a result yielded by the proposed method. Specifically, after a target image is selected arbitrarily, the given secret image is first divided into rectangular fragments called tile images, which then are fit into similar blocks in the target image, called target blocks, according to a similarity criterion based on color variations. Next, the color characteristic of each tile image is transformed to be that of the corresponding target block in the target image, resulting in a mosaic image which looks like the target image. Relevant schemes are also proposed to conduct nearly lossless recovery of the original secret image from the resulting mosaic image.

The proposed method is new in that a meaningful mosaic image is created, in contrast with the image encryption method that only creates meaningless noise images. Also, the proposed method can transform a secret image into a disguising mosaic image without compression, while a data hiding method must hide a highly compressed version of the secret image into a cover image when the secret image and the cover image have the same data volume. The Decryption person needs a key to get embedded secret image without the key the image can be extracted.

2. RELATED WORKS

Chin Chen chang, Min- Shian Hwang, and Tung Shou Chen [3] have given a fast encryption algorithm for secure image cryptosystems in 2001. Vector Quantization, cryptography and other theorem is the major platform for the cryptosystems to transmit images. It was a meaningful technique to lower bit rate image compression. In VQ firstly transformation of images into vectors takes place and further vector by vector then are sequentially encoded

W. B. Pennebaker tried to explain that the main obstacle in quantity of data required representing a digital image. For this we would have to make image compression standard to maintain quality of the images after compression. To meet all the needs the JPEG standard for image compression includes two basic methods having different operation modes: A DCT method for "loss" compression and a predictive method for "lossless" compression [4].

I-Jen Lai and Wen-Hsiang Tsai [2] have presented technique for information hiding, which proposes that secret image is divided into tile images and then for mosaic image they were fix to its next target image selected from a database. Secret key randomly selects few blocks of mosaic image to embedding the information of the tile image

Ya-Lin Lee and Wen-Hsiang proposed a technique that used for transmitting the secret image lossless and securely. This method transforms the secret image of large sized data into a mosaic tile image having the same size like that of the target image which is preselected from a database. This colour transformation was controlled and then the secret image is recovered lossless from the tile image with the help of the embedded extracted relevant information used for the recovery of the image [1].

3. PROPOSED METHOD

The proposed method contains two phases
1. Mosaic image Creation and
2. Secret image recovery

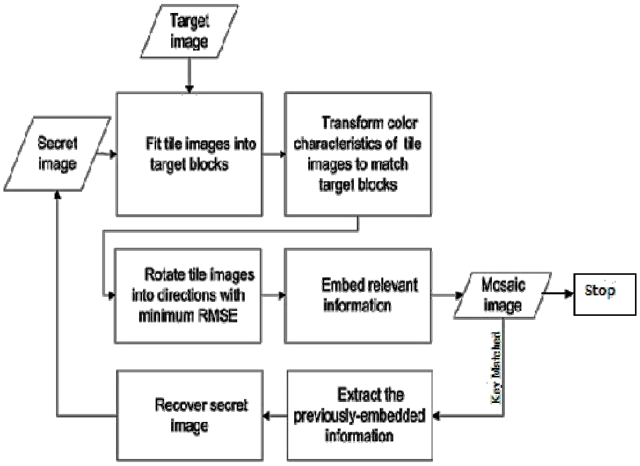
Target image
Secret image
Fit tile images into target blocks
Transform color characteristics of tile images to match target blocks
Rotate tile images into directions with minimum RMSE
Embed relevant information
Mosaic image
Stop
Key Matched
Extract the previously-embedded information
Recover secret image

Figure 2. Flow diagram of the proposed method

In the first phase, a mosaic image is created, which contains of the tiles of the input secret image with color transformations according to the embedded based. Image transmission technique contains four stages. 1) Fitting tile images of the secret image into target image; 2) Transforming the each tile of secret image to the corresponding target blocks of target image; 3) Rotating each tile with minimum RMSE value with respect to target block; 4) Embedding the secret image recovery information.

In the second phase, it contains two stages. 1) Extracting embedded information from recovery; and 2) Recovering the Secret image.

4. ALGORITHMS OF THE PROPOSED SYSTEM

The Detailed algorithms for mosaic image creation and secret image recovery may be stated in algorithm 1 and 2.

Algorithm 1: Mosaic Image Creation.

T-Target Image; S-Secret Image; F-Secret Fragment visible mosaic image

Stage 1: Fitting tile images of the secret image into target image

1. If the size of T is different from Size of S, Change the Sizes and Make them Identical.
2. Divide S into ‘n’ tiles and T into ‘n’ blocks.
3. Compute mean and standard deviation for each tile and block for three color channels.
4. Compute average Standard deviation.
5. Sort both tiles images and block images.
6. Based on Average Standard Deviation values of blocks, map tile between S and T
7. Create F

Stage 2: Transforming the each tile of secret image to the corresponding target blocks of target image

8. Create Counting Table TB with 256 entries, each with corresponding to a residual value and assign an initial value to zero
9. Calculate mean and standard deviation for each mapping from secret to target.
10. For Each pixel p_i in each block of F with the color value of c_i , transform c_i into a new value using $c_i'' = q_c(c_i - \mu_c) + \mu_c'$ if c_i'' is not less than 255 or if it is greater than 0 , then changes to be 255 or 0.
11. Compute a Residual value R_i for pixel p_i.

Stage 3: Rotating each tile images.

12. Compute the RMSE values
13. Rotate tile into the optimal direction with minimal RMSE value.

Stage 4: Embedding the secret image recovery information.

14. For each tile image T_i in Mosaic image F, construct a bit stream M_i for recovering T
15. Concatenate the bit stream M_is of all T_i in F; sue the secret key K to encrypt.
16. Embed the bit stream I into mosaic image F by the same scheme used in step 15.

Algorithm 2: Secret image recovery

T-Target Image; S-Secret image: F-Mosaic image

Stage 1: Extracting embedded information from recovery.

1. Extract the bit stream M_t by Secret key
2. Decompose M_t into n bit streams M_1 through M_n.
3. Decode $M_i$for each tile T_i to obtain data items.

Stage 2: Recovering the Secret image.

4. Recovering tile images by the following steps
   - Rotate tile in reverse direction and fit the resulting block content into T to form initial tile image.
   - Make use of Extracted Mean and related Standard Deviation quotients
   - Compute the original pixel value
   - Scan t to find out pixels
5. Compose all the final tile images to form the desired secret image S as output.

5. EXPERIMENTAL RESULTS

A series of experiments have been conducted to test the proposed method using many secret and target images with sizes 1024 ×768 or 768 ×1024. To show that the created mosaic image looks like the preselected target image, the quality metric of root mean square error (RMSE) is utilized. The RMSE values for θ = 90, 180 and 270 are 39.1915, 45.2545 and 50.5961 respectively, which is defined as the square root of the mean square difference between the pixel values of the two images.

An example of the experimental results is shown in Fig. 3; Fig. 3(c)-3(f) shows the created mosaic images using Fig. 3(b) as the secret image and Fig. 3(a) as the target image. The tile image sizes are 8 ×8, 16x16, 24x24 and 40x40 respectively. The recovered secret image using a correct key

(a) (b)

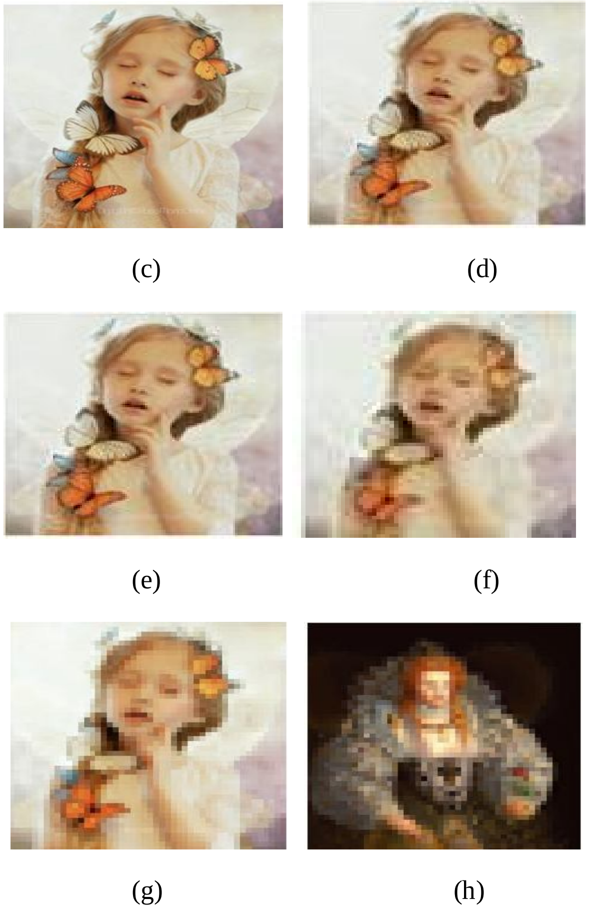

Figure 3. Experimental result of mosaic image creation. (a) Target image. (b) Secret image. (c) – (f) Mosaic images created with different tile image sizes: 8x8, 16x16, 24x24, 40x40. (g)- (h) block processed images of target and secret image

If the recovery key doesn't matches with the key used for hiding key then the process ends at that point, without any further process.

6. CONCLUSION

In this generation nothing is secure. A Secure image Steganography technique is proposed, where secret images are embed into an image and encrypted with a key to transmit. Mosaic image is formed with secret tile image and target image for the lossless data hiding and recovery. Experimental results are shown the feasibility of secure transmission of image in the proposed method is good. Future studies may be directed to applying proposed method to video, where video frames are used as target image.

REFERENCES

1. Ya-Lin Lee and Wen-Hsiang Tsai, "**A New Secure Image Transmission Technique via Secret-fragment-Visible Mosaic Images by Nearly Reversible Color Transformations**," IEEE Transactions on Circuits and systems for video Technology, vol. 24, no. 4, April 2014
2. J. Lai and W. H. Tsai, "**Secret-fragment-visible mosaic image—A new computer art and its application to information hiding**," IEEE Trans. Inf. Forens. Secur, vol. 6, no. 3, pp. 936–945, Sep. 2011.
3. Chin chenChang , MinShian Hwang and Tung Shou Chen," **A new image encryption algorithm for image cryptosystems**", the journal of system and software 58(2001).
4. W. B. Pennebaker and J. L. Mitchell, "**JPEG: Still Image Data Compression Standard**", New York, NY, USA: Van Nostrand Reinhold, pp. 34–38, 1993.
5. Zhicheng Ni, Yun-Qing Shi, Nirwan Ansari, and Wei Su," **Reversible Data Hiding**", IEEE transactions on circuits and system for vedio technology, vol. 16, no. 3, march 2006.
6. 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.
7. E. Reinhard, 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.