International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

# Secret Fragment Mosaic Images: A Secure Method for Image Transmission

**Shabana Vathelil Subair[1], Timna P Elizabeth[2]**

[1]Final Year M. Tech. (Cyber Security), KMP College of Engineering, Perumbavoor, Kerala, India

[2]Assistant Professor, Department of Computer Science and Engineering, KMP College of Engineering, Perumbavoor, Kerala, India

**Abstract:** ***Images from various sources are often used and are transmitted through the internet for various purposes, such as confidential enterprise archives, document storage systems, medical imaging systems, and military image databases. These images may contain secret or confidential information since it should be protected from leakage during transmissions. An approach for secure image transmission is needed, which is to transform a secret image into a meaningful Secret Fragment Mosaic image with size almost same and looking similar to the preselected target image. The mosaic image is the outcome of arranging of the block fragments of a secret image in a way so as to disguise the other image called the target image. The mosaic image, which looks similar to a randomly selected target image, which is used for hiding of the secret image by color transforming their characteristics similar to the blocks of the target image. Such technique is necessary so for the lossless recovery of the transmitted secret image. The appropriate information is embedded into the mosaic image for the recovery of the transmitted secret image.***

Keywords: Color transformation, data hiding, encryption of image, mosaic image, secure transmission of image

## 1. Introduction

Nowadays, images from various sources are often used and are transmitted through the internet for various applications, such as confidential enterprise archives, document storage systems, medical imaging systems, and military image databases. These images usually contain private or confidential information so that they should be protected from leakages during transmissions. Recently, many methods have been proposed for securing image transmission, for which two common approaches are image encryption and data hiding.

Encryption of image is a technique that make use of the natural property of an image, such as high redundancy and strong spatial correlation, to get an encrypted image. The encrypted image is meaningless and this may arouse the third parties attention due to its randomness in form during transmission. Another method for secure image transmission is data hiding that hides a secret entity into a cover image so that a third party cannot found the presence of the secret entity. The problem of data hiding is the difficulty in embedding large volume of secret entity into a single image. If anyone wants to hide a secret entity into a cover image, the secret entity must be highly compressed earlier. During retrieval this will cause distortion of the secret entity.

In this paper, we propose an approach for secure image transmission is needed, which is to transform a secret image into a meaningful Secret Fragment Mosaic image with size almost same and looking similar to the preselected target image. The mosaic image is the outcome of arranging of the block fragments of a secret image in a way so as to disguise the other image called the target image. The mosaic image, which looks similar to a randomly selected target image, which is used for hiding of the secret image by color transforming their characteristics [5] similar to the blocks of the target image. Such technique is necessary so for the lossless recovery of the transmitted secret image. The appropriate information is embedded into the mosaic image for the recovery of the transmitted secret image [1] [2]. The rest of this paper organized as follows: Section 2 discusses related works. Section 3 discusses proposed system. Section 4 covers the detailed algorithms for mosaic image creation and secret image recovery and Section 5 concludes the paper.

## 2. Related Works

This section describes the various existing schemes which are compared in this paper.

### 2.1 A New Secure Image Transmission Technique via Secret-fragment-Visible Mosaic Images by Nearly Reversible Colour Transformations.

In this paper, Ya-Lin Lee propose a technique for the transmitting of the secret image securely and lossless. This method transforms the secret image into a mosaic tile image having the same size like that of the target image which is preselected from a database. 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 [1].

### 2.2 A Keyless Approach to Image Encryption, by Indian Institute of Technology Roorkee.

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 [2].

### 2.3 JPEG: Still Image Data Compression Standard

Here, W. B. Pennebaker 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 the JPEG standard for image compression includes two basic methods having different operation modes: A DCT method for "lossy" compression and a predictive method for "lossless" compression [3].

To securely transmit a secret image and recovering it without any loss by method of creating a mosaic image. The proposed method is new in that a meaningful mosaic image is created.

The proposed method includes two main phases

1) Mosaic image creation
2) Secret image recovery

## 3. Proposed System

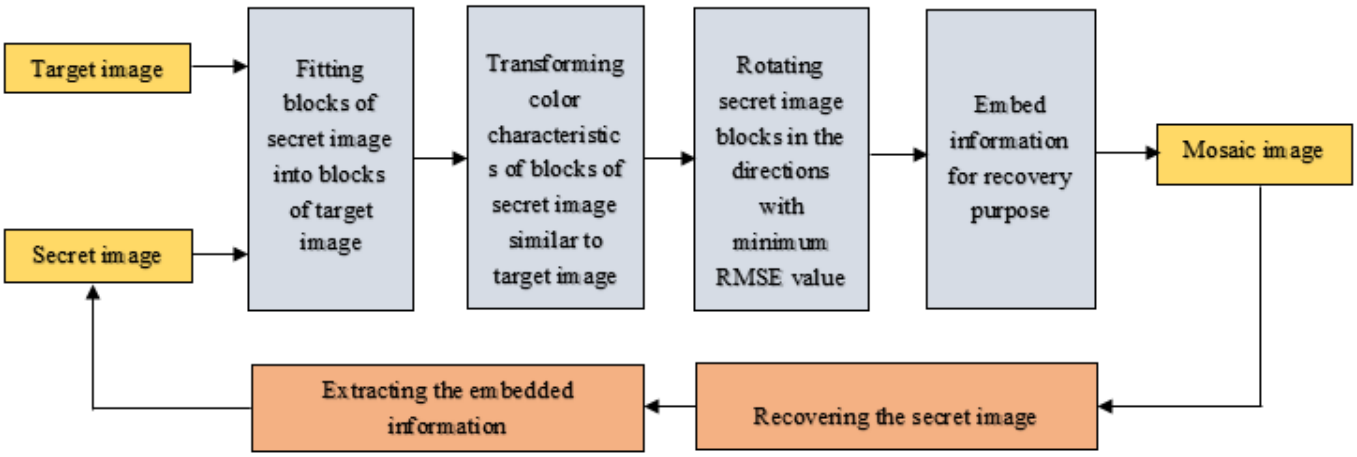


**Figure 1:** Flow Diagram of proposed method

The result is the mosaic image, which consists of block fragments of an input secret image which has color characteristics same as that of a preselected target image.

## 4. Algorithm of Proposed Method

The detailed algorithms for mosaic image creation and secret image recovery may now be described in Algorithms 1 and 2 respectively.

**Algorithm 1** Mosaic image creation
T-target image, S-secret image, F-mosaic image

**Stage 1. Fitting blocks of secret images into blocks of target blocks**

1. If the size of T is different from S, change the size
2. Divide S and T into n blocks of same size
3. Compute the means and the standard deviations(SD) of each tile [1]
4. Compute the average SD
5. Sort the tile images in S and T
6. Map tile between S and T
7. Create F

**Stage 2. Transforming color characteristics of blocks of secret image similar to target image**

8. For each mapping from secret to target calculate the mean and SD
9. Each pi in each block of F with color value ci, transform ci into a new value using ci''=qc(ci-μc) + μc'
   a. If ci'' is not less than 255 or if it is not greater than0, then change to be 255 or 0

**Stage 3. Rotating secret image blocks in the direction with minimum RMSE value**

10. Compute the RMSE values
11. Rotate tile into the optimal direction with the smallest RMSE value

**Stage 4. Embed information for recovery purpose**

12. For each tile image in F, construct a bit stream M for recovering T
    - Index, rotation angle θ°, means and the SD quotients
13. Generate a bit stream Mt by K
14. Embed Mt into F

**Algorithm 2** Secret image recovery
T-target image, S-secret image, F-mosaic image

**Stage 1. Extracting the embedded information.**

1. Extract the bit stream Mt by K
2. Decompose Mt into n bit streams
3. Decode M for each tile image to obtain the data items
   - Index, rotation angle θ°, means and SD quotients

**Stage 2. Recovering the secret image.**

4. Recover tile images by the following steps
   - Rotate tile in the reverse direction and fit the resulting block content into T to form an initial tile image
   - use the extracted means and related SD quotients
   - compute the original pixel value
   - scan T to find out pixels with values 255 or 0
   - take the results as the final pixel values
5. Compose all the final tile images to form the desired secret image S

## 5. Conclusion

Images from different sources are transmitted through the internet for various applications. These images usually contain private or secret data so that they should be protected from leakages during transmissions. A method is proposed to securely transmit a secret image that create mosaic images which also can transform a secret image into a mosaic tile image with the same size of data for concealing the secret image. This is done by the use of proper color transformations pixel by pixel in mosaic tile images with large color similarities. The original secret image can be reconstructed nearly lossless from the created mosaic images.

## References

[1] A New Secure Image Transmission Technique via Secret-fragment-Visible Mosaic Images by Nearly Reversible Color Transformations, Ya-Lin Lee, Student Member, IEEE, and Wen-Hsiang Tsai, Senior Member, IEEE Transactions on Circuits and systems for video Technology, vol. 24, no. 4, April 2014
[2] I. 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] A Keyless Approach to Image Encryption, Siddharth Malik, Anjali. Sardana Indian Institute of Technology Roorkee, India. 2012 International Conference on communication Systems.
[4] JPEG: Still Image Data Compression Standard, W. B. Pennebaker and J. L. Mitchell, New York, NY, USA: Van Nostrand Reinhold, pp. 34–38, 1993.
[5] 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.

## Author Profile

**Shabana Vathelil Subair** received the B.Tech degree in Computer Science & Engineering from Mahatma Gandhi University, Kottayam in 2012 and currently pursuing final year M.Tech degree in Computer Science and Engineering with specialization in Cyber Security from KMP College of Engineering, Perumbavoor.

**Timna P Elizabeth** received B.Tech degree in Computer Science & Engineering from Mahatma Gandhi University Kottayam in 2012 and received M.E in Computer Science from Anna University Chennai in 2014 and currently working as assistant professor in KMP College of Engineering, Perumbavoor in Computer Science and Engineering Department.