Visible Mosaic Image Based Secure Image Transmission Technique

[1]Pritesh B Jagdale, [2]Prof.P.P.Belagali

[1]PG Student, [2]Associate Professor
[1]Department of Electronics Engineering,[2]Department of Electronics & Communication Engineering
Dr.J.J.Magdum College of Engineering, Jaysingpur, India

***Abstract*—With the spread of digital data around the world through the internet, information security is becoming increasingly important in the modern networked age. In this paper new image steganography method is proposed, which creates automatically from an arbitrarily-selected target image a so-called secret fragment-visible mosaic image as a camouflage of a given secret image. The mosaic image is yielded by dividing the secret image into fragments and transforming their color characteristics to be those of the blocks of the target image. Skillful techniques are designed for use in the color transformation process so that the secret image may be recovered nearly losslessly. The method not only creates a steganographic effect useful for secure keeping of secret images, but also provides a new way to solve the difficulty of hiding secret images with huge data volumes into target images.**

***Index Terms*—Color transformation, data hiding, image encryption, mosaic image, secureimage transmission**

I. INTRODUCTION

In the digital world, data is the heart of computer communication and global economy. To ensurethe security of the data, the concept of data hiding has attracted people to come up with creativesolutions to protect data from falling into wrong hands.
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 makes 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].

.

II. RELATED WORKS

1. A New Secure Image Transmission Technique via Secret-fragment-Visible Mosaic Images by Nearly Reversible Color 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. 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 helps to rotate the tile images to a certain angle [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 requiredto 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].

III. Proposed Method

For 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

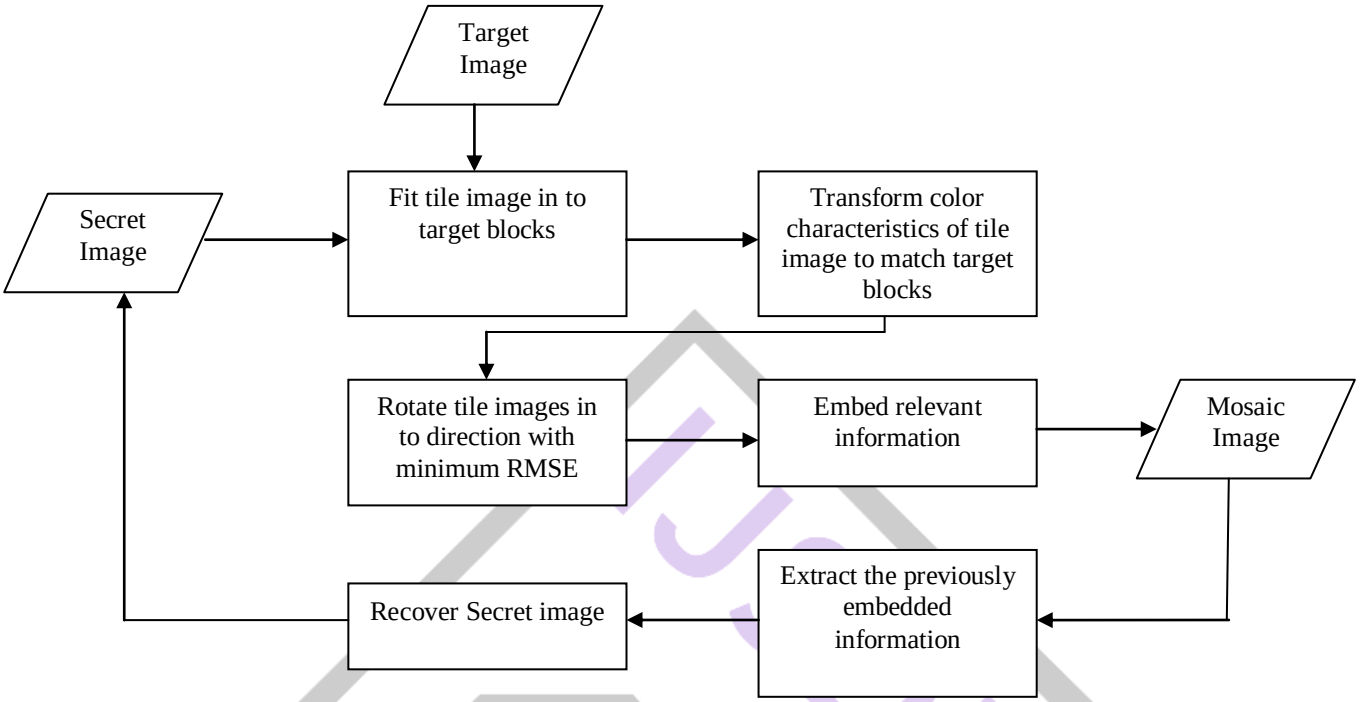

Figure: Flow Diagram

IV. Algorithm of Proposed Method

The proposed method includes two main parts of algorithm as shown by the flow diagram.

1) Mosaic image creation
2) Secret image recovery

In the first part, a mosaic image is obtained, which comprises of the fragments of an input secret image with color corrections according to a similarity criterion based on color variations. The part incorporates four stages: 1) fitting the tile images of the secret image into the target blocks of a preselected target image; 2) changing the color characteristic of every tile image in the secret image to turn that of thecorresponding target block in the target image; 3) pivoting every tile image into a direction with the minimum RMSE value with respect to its corresponding target block; and 4) implanting required information into the created mosaic image for future recuperation of the secret image.

In the second part, the implanted information is extracted to recuperate the secret image nearly losslessly from the generated mosaic image. The part incorporates two stages: 1) extracting the implanted information from the mosaic image for recovery of the secret image, and 2) recuperating the secret image using the extracted information.

Algorithm 1: Mosaic image creation

Input: a secret image, a target image, and a secret key.
Output: a secret-fragment-visible mosaic image.
Steps:
1: Take the input are secret image, target image and key.
2: Generate the tile blocks for secret image and target blocks for target image.
3: Calculate the mean and standard deviation for each tile block and target block.

$$\mu_c = \frac{1}{n}\sum_{i=1}^{n} c_i$$

Where c_i- pixel values of C-channels such as red, green and blue. n– No. of pixels.

$$\sigma_c = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(c_i - \mu_c)^2}$$

4: Calculate the average standard deviation for each block and sort them.

$$c_i = q_c(c_i - \mu_c) + \mu_c$$

Where q_c- standard deviation quotient

5: Sort the tile blocks and target blocks as per sorted average standard deviations respectively.
6: Map sorted tile blocks with the sorted target blocks.
7: Create mosaic image fitting tile box as per the mapped target blocks.
8: Transform the color of all the pixel of each tile image using means and standard deviations.
9: Rotate each transformed tile to 90,180 and 270 degrees and calculate root mean square error.
10: Retain the rotation with minimum RMSE.
11: Convert the mean and standard deviations for each tile block and mapped target block to binary.
12: Convert tile rotation performed into binary.
13: Embed data in to the corresponding tile box will get finally output mosaic image.

Algorithm 2: Secret image recovery

Input: a mosaic image images and secret key.
Output: the secret image.
Steps:
1: Extract the bit stream from mosaic image by performing reverse operation.
2: Decrypt the bit stream by using secret key.
3: Recover the desired secret image by rotating the tile images in a reverse direction.
4: Use the extracted mean and standard deviation quotients to recover the original pixel values.
5: Take the results as the final pixel values, resulting in a final tile image.
6: Compose all the final tile images to form the desired secret image as output.

V. EXPERIMENTAL RESULTS

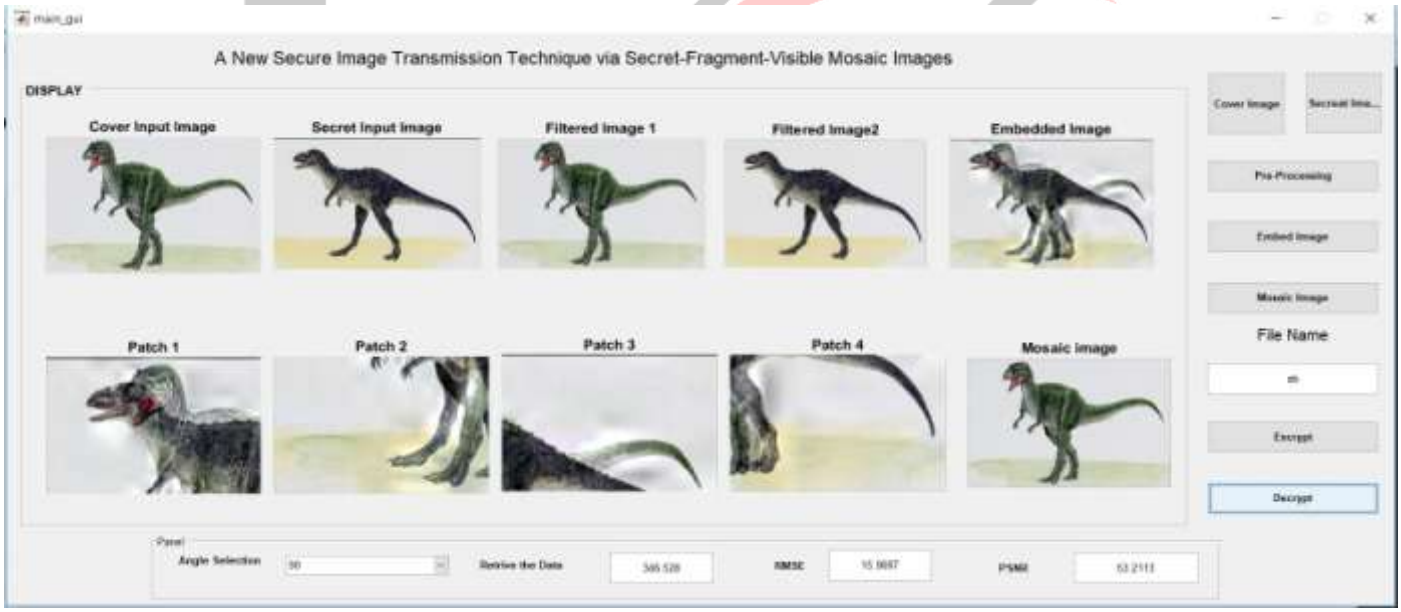

Figure: Mosaic image creation

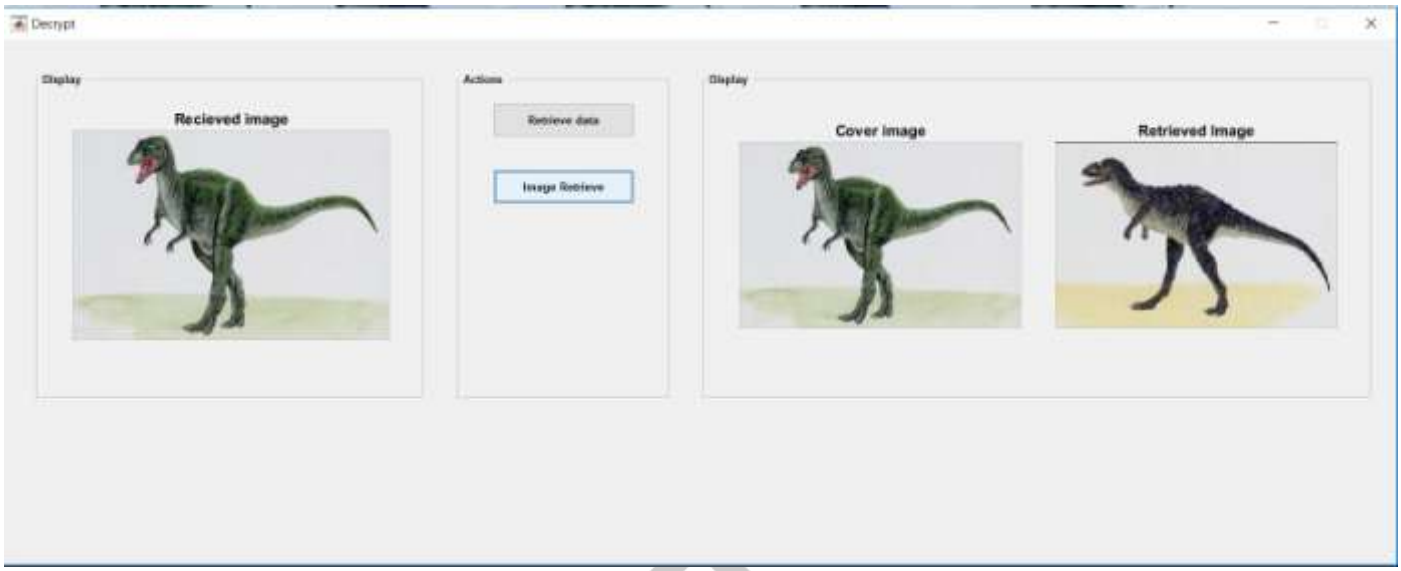

Figure: Image retrieve

A series of experiments have been conducted to test the proposed method using many secret and target images with different sizes. To show that the created mosaic image looks like the pre-selected target image, the quality metric of root mean square error (RMSE) is utilized, 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 Figure above, where last figure shows the created mosaic image using secret image and target image. The recovered secret image using a correct key is shown in second figure above which looks nearly identical to the original secret imagewith RMSE= 15.96 with respect to the secret image.

VI. 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.