

SecretFragment Visible Mosaic Image Technique for Information Hiding

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

¹PG Student, ²Associate Professor

¹Department of Electronics Engineering, ²Department of Electronics & Communication Engineering
Dr.J.J.Magdum College of Engineering, Jaysingpur, India

Abstract—New secure image transmission technique which transforms secret image into mosaic image of the same size. Mosaic image looks similar to a randomly selected target image and it is yielded by dividing the secret image into fragments and transforming their color characteristics to be those of the corresponding blocks of the target image. Skillful techniques are designed to conduct the color transformation process so that the secret image may be recovered nearly losslessly.

Index Terms—Color transformation, data hiding, image encryption, mosaic image, secure image transmission.

I. INTRODUCTION

Today, images from various sources are frequently utilized and transmitted through the internet for various applications, such as online personal photograph albums, 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. Nowadays, many methods have been proposed for securing image transmission. A new type of methods called secret-fragment-visible mosaic image, which contains small fragments of a given source image is proposed in this study. Observing such a type of mosaic image, one can see all the fragments of the source image, but the fragments are so tiny in size and so random in position that the observer cannot figure out what the source image looks like. Therefore, the source image may be said to be secretly embedded in the resulting mosaic image, though the fragment pieces are all visible to the observer. And this is the reason why the resulting mosaic image is named secret-fragment-visible.

The mosaic image is the result of rearrangement of the fragments of a secret image in disguise of another image called the target image which is preselected from the database. But an obvious inadequacy of Lai and Tsai [1] is that it requires a huge amount of database so that the created mosaic image should be sufficiently similar to the previously selected target image. Using their method the user is not allowed to pick energetically his/her adored image for use as a target image. Therefore in this technique it is desired to remove this weakness while keeping its benefits that is it is aimed to design a new technique that can transform the secret image into a secret-fragment-visible mosaic image of same size that has the same visual appearance of any freely selected target image without the need of a database. A mosaic image is the process of creating pictures or decorative patterns by cementing together small pieces of stone, glass or other hard materials of various colors. Mosaic contains more number of small images called tile images. Mosaic image can be created by dividing the original image into many tiles and for each tile, find another image with similar content from an image database. Finally we have to build the mosaic image by replacing all tiles by their similar images.

II. RELATED WORK

1. I. J. Lai and Tsai, proposed a “Secret-fragment-visible mosaic image-A new computer art and its application to information hiding [1]”, in this paper a new type of computer art image called secret-fragment-visible mosaic image is proposed which is created automatically by arranging small fragments of a given image in a mosaic form, and then embedding given secret image in the resulting mosaic image. This type of information hiding is useful for covert communication and secure keeping of secret images.

2. Y. Hu, et al, proposed a “Difference expansion based reversible data hiding using two embedding directions [2]”, current difference expansion embedding technique performs only one layer embedding in a difference image because of that there will be degradation in the image. So in this paper a new difference expansion embedding algorithm which is based on Harr wavelet transform is used, which make use of two embedding directions horizontal as well as vertical difference image for data hiding which refines the algorithm and makes it flexible to different types of images.

3. V. Sachnev, et al, proposed “Reversible watermarking algorithm using sorting and prediction [3]”, this algorithm uses a prediction errors to embed data into an image.

A sorting technique is used to record the prediction errors based on magnitudes of its local variance. This algorithm allows us to embed more data into the image with less distortion by using a reduced size location map.

4. X. Li, B. Yang, et al, proposed an “Efficient reversible watermarking based on adaptive prediction-error expansion and pixel selection [4]”, Prediction-error expansion is one of the important techniques of reversible watermarking which can embed a large payload into digital image with less distortion.

Pixel selection allows us to select pixels of smooth area for data embedding by decreasing maximum modification to pixel values. As a result, when compared with conventional prediction-error expansion we obtain more sharply distributed prediction-error histogram and a better visual quality of watermarked image.

5. S. Lee, et al, proposed “Reversible image watermarking based on integer -to-integer wavelet transform [5]”, this technique divides an input image into non-overlapping blocks and embeds a watermark into the high frequency wavelet co-efficient to avoid both overflow and underflow in the spatial domain. The payload to be embedded includes not only message but also side information used to reconstruct the exact original image. The experimental results show that the proposed scheme achieves a higher embedding capacity when compared to the existing reversible watermarking schemes.

6. W. H. Lin, et al, proposed an “Efficient watermarking method based on significant difference of wavelet coefficient quantization [6]”, this paper proposes a blind watermarking algorithm based on the significant difference of wavelet coefficient quantization for copyright protection. Every 7 non-overlap wavelet coefficient of the target image is grouped into a block. The largest 2 coefficient in a block are called significant coefficient and their difference is called significant difference. The local maximum wavelet coefficients are quantized in a block by comparing the significant difference value in a block with the average significant difference value in blocks. The maximum wavelet coefficient are so quantized that their significant difference between watermark bit 0 and 1 occupies large energy difference which can be used for watermark extraction.

The experimental results show that the proposed method is more effective than JPEG compression, low-pass filtering and Gaussian noise.

7. C. K. Chan and L. M. Cheng, proposed a “Hiding data in images by simple LSB substitution [7]”, it is a method of hiding the secret message into a cover image so that unauthorized observer will not realize the presence of hidden message.

In this paper, 8-bit gray scale images are selected as cover media and are called cover images. LSB is one of the common data hiding technique, which replaces the LSB’s of the cover image with the message bits.

Experimental results show that with low extra computation complexity we can get the enhanced image quality.

III. BASIC IDEA AND MOSAIC IMAGECONSTRUCTION

A) *The proposed method is shown by the flow diagram below.*

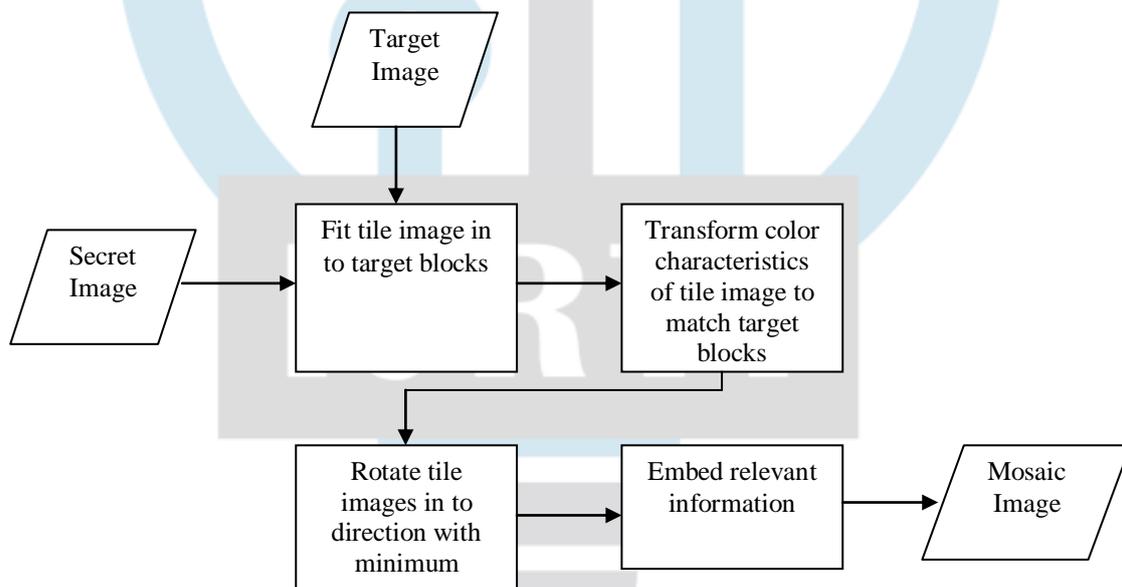


Fig.1. Flow diagram of proposed method.

Mosaic image is obtained with comprises of the fragments of an input secret image with color corrections according to a similarity criterion based on color transformation. The mosaic image creation phase 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 the corresponding 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.

B) *Algorithm: 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 s 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 into the corresponding tile box will get finally output mosaic image.

IV. RESULT



Fig 1: Target Image



Fig 2: Secret Image



Fig 3: Tile Embedded Image



Fig 4: Mosaic Image – Output

The first figure Fig.1 is the target image which is preselected from the database and is divided into target blocks and the second figure Fig.2 is the plane which is the secret image and it is divided into tile blocks. Third figure Fig.3 tile embedded image is the result of calculating mean, standard deviation and average standard deviation for each target block and tile block and

then sorting the blocks according to the result of average standard deviation. Next map the sorted target blocks with the tile blocks, fit these blocks in a mosaic form. Transform the color of all the pixels of each tile block using mean and standard deviation rotate each transformed tile block to 90, 180 and 270 degrees, and calculate the root mean square error. Fig 4 is the output mosaic image.

V. CONCLUSION

A new type of secure image transmission technique called secret-fragment-visible mosaic image creates a meaningful mosaic image of the same size and has the same visual appearance as the target image which is preselected from the database. This effect of information hiding is useful for covert communication or secure keeping of secret images. With this technique user can select his/her favorite image to be used as a target image without the need of large database. Also the original secret image can be recovered nearly losslessly from the created mosaic image.

REFERENCES

1. 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.
2. Y. Hu, H.-K. Lee, K. Chen, and J. Li, "Difference expansion based reversible data hiding using two embedding directions," *IEEE Trans. Multimedia*, vol. 10, no. 8, pp. 1500–1512, Dec. 2008.
3. V. Sachnev, H. J. Kim, J. Nam, S. Suresh, and Y.-Q. Shi, "Reversible watermarking algorithm using sorting and prediction," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 19, no. 7, pp. 989–999, Jul. 2009.
4. X. Li, B. Yang, and T. Zeng, "Efficient reversible watermarking based on adaptive prediction-error expansion and pixel selection," *IEEE Trans. Image Process.*, vol. 20, no. 12, pp. 3524–3533, Dec. 2011.
5. S. Lee, C. D. Yoo, and T. Kalker, "Reversible image watermarking based on integer-to-integer wavelet transform," *IEEE Trans. Inf. Forens. Secur.*, vol. 2, no. 3, pp. 321–330, Sep. 2007.
6. W.-H. Lin, S.-J. Horng, T.-W. Kao, P. Fan, C.-L. Lee, and Y. Pan, "An efficient watermarking method based on significant difference of wavelet coefficient quantization," *IEEE Trans. Multimedia*, vol. 10, no. 5, pp. 746–757, Aug. 2008.
7. C. K. Chan and L. M. Cheng, "Hiding data in images by simple LSB substitution," *Pattern Recognit.*, vol. 37, pp. 469–474, Mar. 2004.

