A New Secure Image Transmission Technique via Secret-Fragment-Visible Mosaic Image

Jyoti R H, Prof Jyoti Neginal

Abstract— **A new secure image transmission technique is proposed, which changes naturally a given huge volume secret image into a secret-fragment-visible image called mosaic image of the same size. The mosaic image, which appears to be like an discretionarily chose target image and may be utilized as a disguise of the secret image, is yielded by separating the secret image into sections and changing their shading attributes to be those of the comparing pieces of the target image. Skillful techniques are intended to lead the shading change process so that secret image may be recuperated almost losslessly. A scheme of handling overflows/underflows in the changed over pixels shading values by recording the shading contrast in the untransformed shading space is additionally proposed. The data needed for recuperating the secret image is embedded into the created mosaic image by a lossless information concealing plan using a key. Good experimental results demonstrate the achievability of the proposed method.**

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

I. Introduction

Currently, images from different sources are oftentimes used and transmitted through the web for different applications, for example online personal photograph albums, confidential enterprise archives, restorative imaging framework, military picture databases. These images generally contain private or confidential data so that they ought to be shielded from leakages during transmissions. Recently numerous techniques have been proposed for secure image transmission, for which two basic methodologies are image encryption and data hiding.

Image encryption is a method that makes utilization of the characteristic property of an image, such as high redundancy and strong spatial correlation, to get a scrambled image. The scrambled image is a useless document, which can't give extra data before unscrambling and may stir an assailant's attention during transmission because of its irregularity in structure.

An alternative method to avoid this problem is the data hiding that hides a secret message into a cover image so that no one can realize the existence of the secret image. But the main issue of data hiding is that if one wants to hide a secret image into a cover image with the same size, the secret image must be exceptionally compacted ahead of time. However for many applications, such as transmitting medical pictures, legal documents, and military images and so on that contain confidential information, in such cases data compression operations results in a loss of important information.

A new technique for secure image transmission is proposed, which transforms a secret image into a significant mosaic image with the same size and resembling a preselected target image. The transformation process is controlled by a secret key and only with the secret key can a person recover the secret image nearly losslessly from the mosaic image. The proposed strategy is enlivened by Lai and Tsai [1], in which a new sort 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 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 colours. 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.

Manuscript received May, 2015.

Jyoti R H *Department of Computer Science and Engineering, Visvesvaraya Technological University, Belgaum / Godutai Engineering College for Women, Gulbarga, India, 9035198384.*

Prof. Jyoti Neginal *Department of Computer Science and Engineering, Visvesvaraya Technological University, Belgaum / Godutai Engineering College for Women, Gulbarga, India, 9986700546*

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 technique 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 are 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 coefficient 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 grayscale 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. Methodology

A. The proposed method includes two main phases as shown by the flow diagram below.

1) *Mosaic image creation*
2) *Secret image recovery*

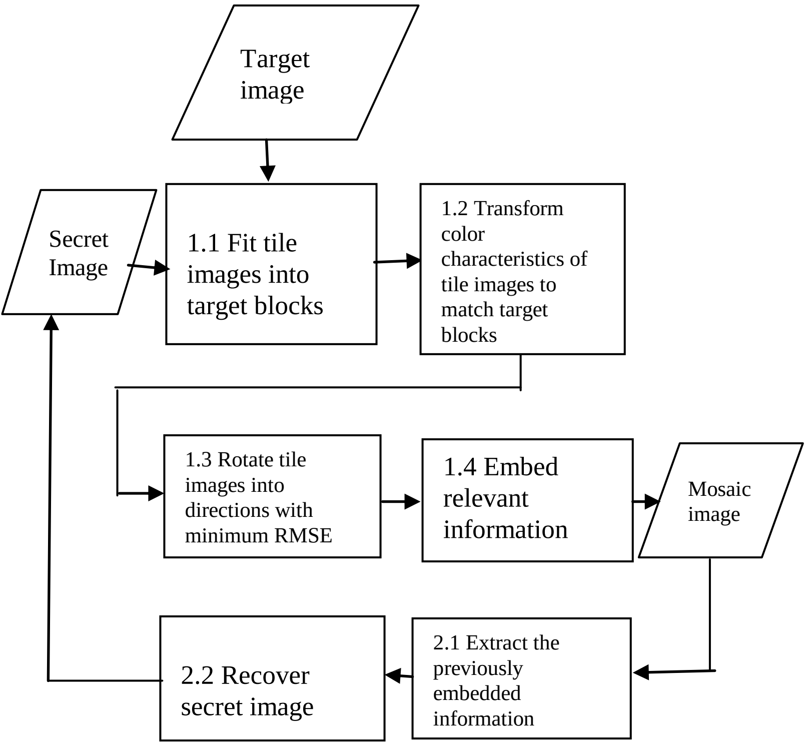
Target image
Secret Image
1.1 Fit tile images into target blocks
1.2 Transform color characteristics of tile images to match target blocks
1.3 Rotate tile images into directions with minimum RMSE
1.4 Embed relevant information
Mosaic image
2.1 Extract the previously embedded information
2.2 Recover secret image

Fig. 1. Flow diagram of proposed method.

In the first phase, 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 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.

In the second phase, the implanted information is extracted to recuperate the secret image nearly losslessly from the generated mosaic image. The phase 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.

B. *Algorithm 1: Mosaic image creation*

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

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

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

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

Step 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
Step 5: Sort the tile blocks and target blocks as per sorted average standard deviations respectively.
Step 6: Map sorted tile blocks with the sorted target blocks.
Step 7: Create mosaic image fitting tile box as per the mapped target blocks.
Step 8: Transform the color of all the pixel of each tile image using means and standard deviations.
Step 9: Rotate each transformed tile to 90,180 and 270 degrees and calculate root mean square error.
Step 10: Retain the rotation with minimum RMSE.
Step 11: Convert the mean and standard deviations for each tile block and mapped target block to binary.
Step 12: Convert tile rotation performed into binary.
Step 13: Concatenate the bit stream and compress into data to be embedded into the corresponding tile box of the mosaic image.
Step 14: Will finally get the output of mosaic image.

Algorithm 2: Secret image recovery

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

IV. RESULT AND DISCUSSIONS

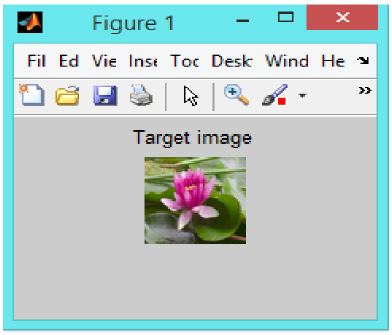

Fig 1: Target Image

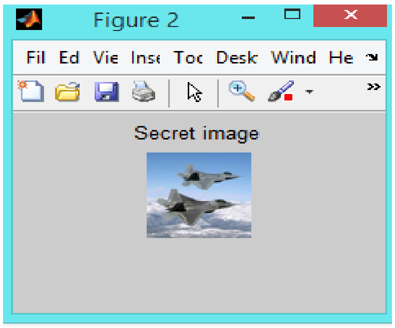

Fig 2: Secret Image

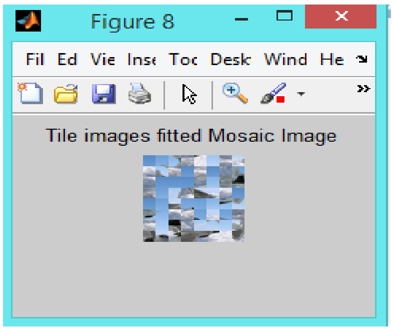
Figure 8
Fil Ed Vie Inse Toc Desk Wind He
Tile images fitted Mosaic Image

Fig 3: Tile Images Fitted Mosaic Image

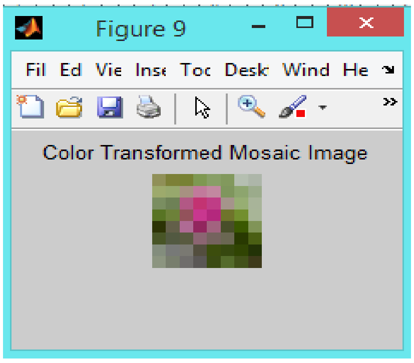
Figure 9
Fil Ed Vie Inse Toc Desk Wind He
Color Transformed Mosaic Image

Fig 4: Color Transformed Mosaic Image

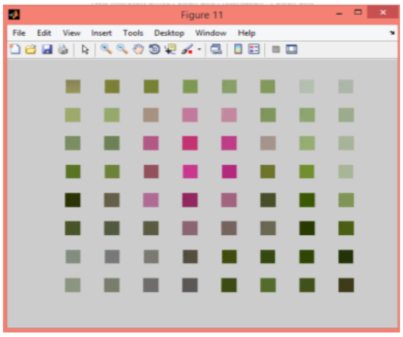

Fig 5: Embed Relevant Information

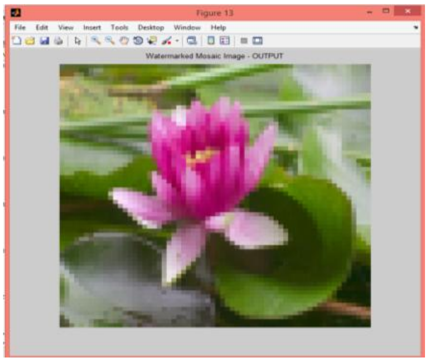
Figure 13
File Edit View Insert Tools Desktop Window Help
Watermarked Mosaic Image - OUTPUT

Fig 6: Water Marked Mosaic Image – Output

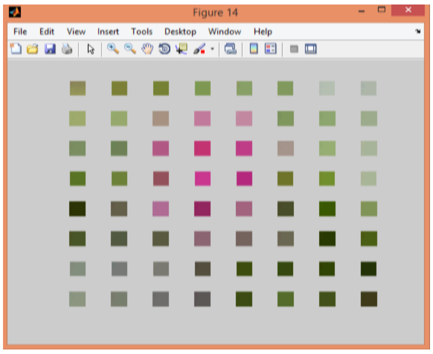

Fig 7: Extract Relevant Information

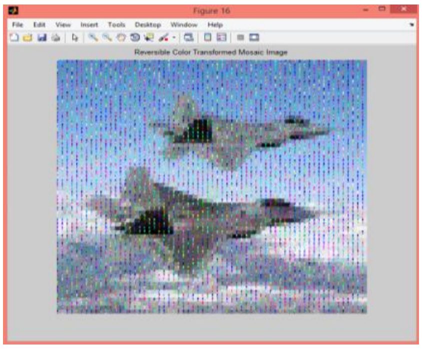
Figure 16
File Edit View Insert Tools Desktop Window Help
Reversible Color Transformed Mosaic Image

Fig 8: Reversible Color Transformed Mosaic Image

The first figure is the target image which is preselected from the database and are divided into target blocks and the second figure is the plane which is the secret image and it is divided into tile blocks.

Third figure 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.

In fig 4 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.

In fig 5 embed the relevant information for future recovery of the secret image nearly losslessly. Fig 6 is the output of the watermarked mosaic image. In fig 7 we do the reverse process to recover the secret image by extracting the information that we embedded in the mosaic image. In fig 8 we recover the secret image using the extracted information.

V. CONCLUSION

A new secure image transmission technique creates a meaningful mosaic image and can also transform the secret image into a secret-fragment-visible mosaic image of the same size and has the same visual appearance as the target image which is preselected from the database. With this technique user can select his/her favourite 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 basedreversible 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 LSBsubstitution,” *Pattern Recognit..*, vol. 37, pp. 469–474, Mar. 2004.

Jyoti R H received the B.E degree in computer science and Engineering from Visvesvaraya University Technology, Karnataka, India in 2012, now doing M.Tech (4th sem) degree in computer science from Visvesvaraya University, Godutai Engineering College for Women Gulbarga, Karnataka, India in 2015(Pursuing).

Prof Jyoti Neginal received the B.E degree in computer science and engineering from Visvesvaraya University, Belgaum, Karnataka, India in 2006, M.Tech in computer science and engineering from Visvesvaraya University, Poojya doddappa Appa College of engineering Gulbarga, Karnataka, India in 2012, working as Asst. Prof in Godutai Engineering College for Women.