International Journal of Research in Advent Technology, Vol.5, No.2, February 2017
E-ISSN: 2321-9637
Available online at www.ijrat.org

Secret-Fragment-Visible Mosaic Image Technique for Secure Image Transmission

Ms. Harsha Mahajan[1], Prof. Pankaj Salunkhe[2]
Department of Electronics and Telecommunication1, 2, Yadavrao Tasgaonkar Institute of Engineering and Technology, Karjat, Maharashtra[1, 2]
Email: mahajanharsha9@gmail.com[1], pasalunkhe@gmail.com[2]

Abstract- This Hiding the data in digital images has been area of interest in the digital image processing domain. Although so much work has been carried out in the literature to resolve the issues like increasing the data capacity, creating the secret image alike of target image but most of the works fails to meet the practical requirements. This paper presents an approach where mosaic image generation has done by dividing the secret image into fragments and transforming their respective color characteristics into corresponding blocks of the target image. Usage of the Pixel color transformations helps to yield the lossless recovered image based on the untransformed color space values. Generation of the key plays an important role to recover the data from the secret image in lossless manner.

Index Terms- Data hiding, Mosaic Image, Secure image transmission, Color transformation Introduction

1. INTRODUCTION

As the world changes technology is also changing rapidly. Security of a data or information is very important now a day in this world. And everybody want a secure network, for transmission of his information. In advancement of network technology domain, large amount of multimedia information is transmitted over the Internet conveniently. Various confidential data such as Government, Military, Banking and other secured data, space and geographical images taken from satellite and commercial important document are transmitted over the Internet. Being a well secure network there is also a chance of hacking a data, most of the banks and other organization where data security is important are well secured but there is also a possibility of online fraudulent. While using secret information we need more secure information hiding techniques. Nowadays digital images are used for many applications in order to protect information from leakages during transmission. Image encryption and data hiding are two methods used for secure transmission. In encryption technique due to randomness in structure of image there are chances of attack. To avoid this problem data hiding techniques are utilized. LSB substitution, Histogram shifting, Difference expansion, Prediction error expansion are existing data hiding techniques.

The main difficulty of these techniques is embedding large amount of message data into a single image. In order to embed secret image into a cover image of the same size, the secret image is to be highly compressed. In many applications such data compression is difficult [1]. In this paper a new technique of secure image transmission is proposed. In this method a secret image is transformed into a mosaic image of the same size and created image is looking same as that of cover image. The transformation is controlled by a secret key and can be recovered by secret key. In order to create secret-fragment-visible mosaic [4] image the secret image is divided into tile forms and target image is divided into blocks, and then according to similarity criterion secret tiles are fitted into target blocks. The color characteristics of each tile image is transformed [3] into corresponding block. Relevant recovery information is also embedded for lossless recovery of secret image.

2. PROPOSED TECHNIQUE

The two main steps included in the proposed method are
A) Mosaic image creation
B) Secret image recovery

2.1 Mosaic image creation

The first step of Mosaic image creation consist of four main phases

- Fitting tile of secret image into blocks of target blocks.
- The color characteristic transformation of each of tile image to become as that of corresponding target block.
- Each tile image is rotated into a direction with minimum RMSE value with respect to target block.

- Relevant information is embedded to recover the secret image from mosaic image

Earlier Lai and Tsai proposed the technique on using of mosaic image creation using secret-visible fragments [4]. But for implementing this technique large image database was required. The user was not allowed for selecting target image of his own choice and the generated mosaic image was grayscale mosaic image.

The proposed technique can overcome above issues. In this technique the generated mosaic image having color characteristics same as that of target image. The secret image is first fragmented into tiles T and target image is fragmented into blocks B. The color characteristic of tile image T is different from color characteristic of target block image B. Each tile image is fitted into target block B. The color transformation technique is used for transforming the color of tile image. In color transformation scheme, the RGB color space of image is converted into lαβ color space in order to reduce the volume of required recovery information. The mean and standard deviation of each tile T and block image B is calculated.

For tile image,

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

And standard deviation is

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

For block image,

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

And standard deviation is

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

$c_i and\ c_i'$ in above equation (1) and (2) denote the c-channel values for pixels of tile image (p_i) and pixels of block image (p_i'). The new pixel values (p_i'') are calculated for newly generated tile image T' as below.

$$c_i'' = q_c\,(c_i - \mu_c) + \mu_c' \quad \ldots\ldots\ldots\ldots\ldots\ldots (3)$$

$q_c = \frac{\sigma_c}{\sigma_c'}$ Which is called as standard deviation quotient.

Original color values for recovered secret image can be computed by taking inverse of equation (3)

$$c_i = \left(\frac{1}{q_c}\right)(c_i'' - \mu_c') + \mu_c$$

…… (4)

Using these mean and standard deviation values the color characteristics of tile image T are transformed into target image block B. Reinhard *et al*. proposed above color transformation technique. For choosing an appropriate target block B for each tile image T, sorting is done according to the values of standard deviation.

According to average values of standard deviations of three color channels sequence of tiles and blocks are formed. The we fit tile into target block. After choosing target block and color transformation further improvement on color similarity is conducted by rotating tile into one of four directions $0^0, 90^0, 180^0\ and\ 270^0$. This rotation is based on minimum value of RMSE of T with respect to B among the four directions. After the color transformation process is conducted some pixel values in new tile image T' might have overflows or underflows. The overflows/underflows values are converted into non-overflows/non-underflows values. Their differences are recorded as residuals values for construction further recovery information. Huffman encoding table is constructed to encode residuals to reduce the number of required bits to represent them.

After fitting an appropriate tile into an appropriate block recovery information regarding secrete image is embedded. LSB substitution technique is utilized for embedding relevant recovery information in which message bits are directly placed at Least Significant Bits position. The Reversible contrast mapping method [2] [5] applies simple integer transformations to pair of pixel values. This method gives high data embedding capacity close to highest bit rates with lowest complexity.

2.2 Secret image recovery

A) Extracting the embedded information
B) Recovering the secret image using extracted information

For recovering the tile image T from target block B, the required information includes index of B, the optimal rotation angle of T, the truncated means of T and B, standard deviation quotients of all color channels and the overflow/underflow residuals. This are integrated as a five component bit stream as

$$M = t_1 t_{2\ldots\ldots} t_m r_1 r_2 m_1 m_2 \ldots . m_{48} q_1 q_2 \ldots\ldots\ldots q_{21} d_1 d_2 \ldots . d_k$$

Further we also have to embed some related information about mosaic image generation process into mosaic image for recovery of secrete image. This information includes the number of iterations conducted in the process of embedding bit stream M and the total number of used pixel pairs in last iteration for embedding M and Huffman table for encoding the residuals. For recovering the secrete image, first the embedded information bits are

extracted by applying reverse version of reversible contrast mapping. The extracted bit stream is decrypted using key. Using this information the secrete is recovered from mosaic image.

3. ALGORITHM OF PROPOSED METHOD

Algorithm 1 Mosaic Image creation

Input: A target image T, Secret image S, Secret key K

Output: A secret-fragment –visible mosaic image F

Step 1: Select a input secret image S, target image T and secret key k

Step 2: Generate the tiles fragments of secret image and blocks of target imag

Step 3: Calculate the mean and standard deviation of each tile and target block

Step 4: Calculate the Average standard deviation of each tile and block

Step 5: Sort all the tile and blocks according to average standard deviation value

Step 6: Map sorted tile into sorted block and create mosaic image

Step 7: Transform all the color values of tile corresponding to target block color

Step 8: Calculate the RMSE value and rotate the tile in the direction of minimum RMSE with angles such as 0^0, 90^0, 180^0 or 270^0

Step 9: Convert the rotation angle, residuals into binary and construct a bit stream and embed it into newly generated tile image

Step 10: Finally the output mosaic image F is obtained

Algorithm 2 Secret Image Recovery

Input : A mosaic image F, secret key k

Output: Secret image S

Step 1: Extract the embedded information bit stream from mosaic image

Step 2: Decrypt the bit stream by using secret key

Step 3: Recover the secret image by rotating the tiles in reverse direction

4. EXPERIMENTAL RESULTS

Figure 1 shows the target image selected for covering our secret image. Figure 2 shows the secret image which is to be transmitted. The generated mosaic image is represented in Figure 3 with color transformation. And finally the recovered secret image is shown in the Figure 4

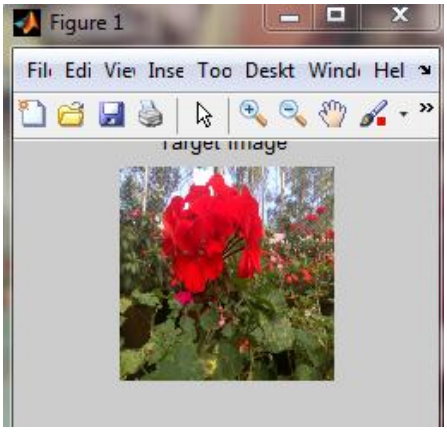

Figure 1. Target Image

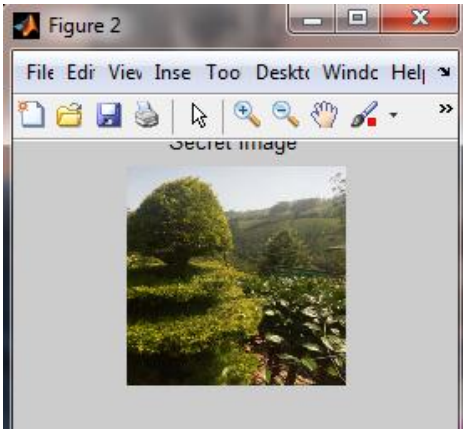

Figure 2. Secret Image

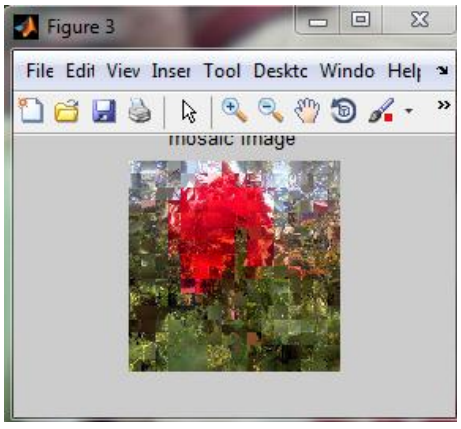

Figure 3. Resultant Mosaic Image

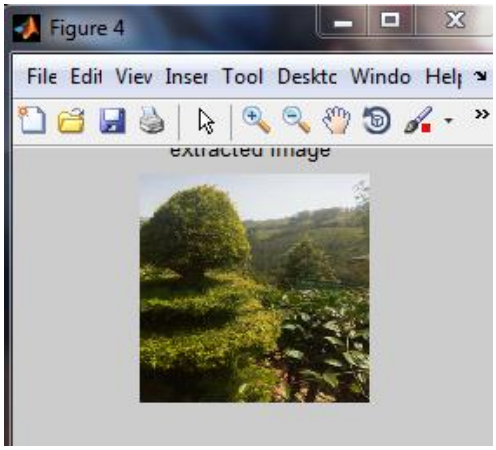

Figure 4. Extracted secret Image

5. CONCLUSION

A new secure image transmission method has been proposed, which not only can create meaningful mosaic images but also can transform a secret image into a mosaic one with the same data size for use as a camouflage of the secret image. By the use of proper pixel color transformations as well as a skillful scheme for handling overflows and underflows in the converted values of the pixels' colors, secret-fragment visible mosaic images with very high visual similarities to arbitrarily-selected target images can be created with no need of a target image database. Also, the original secret images can be recovered nearly losslessly from the created mosaic images.

REFERENCES

[1]. W. B. Pennebaker and J.L. Mitchell, *JPEG: Still Image Data Compression Standard.* New York, NY USA; Van Nostrand Reinhold, 1993, pp. 34-38.

[2]. C. K. Chan and L. M. Cheng, "hiding data in images by simple LSB substitution", *Pattern Recognit.,vol. 37, pp. 469-474, Mar. 2004*

[3]. 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. 2011.

[4]. 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.

[5]. D. Coltuc and J. M. Chassery, "Very fast watermarking by reversible contrast mapping", *IEEE Signal Process. Lett.*, vol. 14, no. 4, pp. 255-258, Apr. 2007.