ISSN (online): 2349-6010

Secure Image Transmission via Mosaic Images using Genetic Algorithm

Rincy Medayil John
PG Student
Department of Computer Science and Engineering
St. Joseph's College of Engineering and Technology Palai, Kerala, India

Jacob P. Cherian
Assistant Professor
Department of Computer Science and Engineering
St. Joseph's College of Engineering and Technology Palai, Kerala, India

Abstract

A technique for secure image transmission is proposed, that transforms a secret image into a secret-fragment-visible mosaic image using Genetic Algorithm. The created mosaic image looks similar to a randomly selected target image which is used as a mask of the secret image. Mosaic image is obtained by dividing the secret image into fragments and fitting these tile fragments into the blocks of the target image. Genetic Algorithm is used to generate a mapping sequence for tile-block fitting. After the tiles are fitted into the target image, color characteristics of tile images are transformed to be those of the corresponding blocks of the target image. A lossless data hiding scheme using a key is used for embedding the secret image recovery information into the created mosaic image. The recovery of the secret image is by using the same key and the tile-block mapping sequence. The use of Genetic Algorithm results in better clarity of the retrieved secret image.
Keywords: Genetic algorithm, Mosaic image, PSNR, Target blocks, Tile images

I. INTRODUCTION

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

Encryption of an image is a technique which uses the natural properties of images, such as high redundancy and spatial correlation between pixels. Image encryption techniques convert original image to another image that is hard to understand; to keep the image secret between users, in other words, nobody could obtain the content without a key for decryption. But, the encrypted image still is a meaningless file, which cannot give more information before the decryption is done. Hence it may evoke an attacker's notice during the transmission of the image because of its randomness in nature.

Another possibility to avoid this problem is hiding of data that hides a secret message into a cover image so that no one can recognize the existence of the secret data, in which the type of data of the secret message that is examined in this paper is an image. The existing methods of data hiding mostly utilize the techniques such as LSB substitution, histogram shifting, discrete cosine/wavelet transformations, recursive histogram modification etc. A main issue of the methods for hiding data in images is that it is difficult to embed a large amount of message data into a single image. i.e, if one wants to hide a secret image into a cover image with the same size; the secret image should be highly compressed in advance. For example, for a data hiding technique with an embedding rate of 0.5 bits per pixel, a secret image with 8 bits per pixel must be compressed at a rate of at least 93.75% prior in order to hide into a cover image. But, for many applications, such as keeping or transmitting, military images, legal documents, medical pictures etc., that are valuable with no allowance of severe distortions, such data compression methods are usually not practical. Moreover, most image compression methods are not appropriate for line drawings and textual graphics, in which sharp contrasts between adjacent pixels are usually distorted to become noticeable artifacts.

In this paper, a new technique for secure image transmission is proposed, that transforms a secret image into a meaningful mosaic image with the help of genetic algorithm. A secret key is used for the transformation process, and only with the key can a person recover the secret image nearly losslessly from the mosaic image. The proposed method is persuaded by Lee and Tsai [1], in which a new type of computer art image, named secret-fragment-visible mosaic image, was proposed. The mosaic image is the result of rearrangement of the fragments of a secret image in mask of another image called the target image.

GA can be regarded as a randomized search procedure that is commonly used for solving the optimization problems [14]. A solution in the problem domain corresponds to an individual in a genetic algorithm, which is represented by a chromosome containing many genes. An objective function named the fitness function is used to evaluate the quality of each chromosome. In general, GA is mainly comprised of the three operators, namely, (1) reproduction, (2) crossover, and (3) mutation. Reproduction retains the current chromosome's genes, crossover join up existing genes into new combinations, and mutation produces new genes. The procedure of GA is started by defining an initial population in the first generation, and during each next generation, the individuals in the population undergo reproduction, crossover and mutation operations, to produce their offspring. Then a

All rights reserved by www.ijirst.org

fitness function is applied to each offspring to find its quality. The individuals with high quality will survive and form the population of the next generation. This process will repeat for many times until a constant number of iterations are exceeded or a predefined requirement is satisfied.

II. LITERATURE SURVEY

A. Secret-Fragment-Visible Mosaic Image

A new computer art and its application to information hiding [2]. In this paper, Lai and Tsai proposed a secret-fragment-visible mosaic image. It is the result of rearrangement of the fragments of a secret image in mask of another image called the target image which is selected priory from a database. The demerit of Lai and Tsai is that it needs a large image database so that the created mosaic image appropriately resembles the selected target image. 2. A New Secure Image Transmission Technique via Secret-Fragment-Visible Mosaic Images by Nearly Reversible Colour Transformations [2]. In this paper, a technique for secure image transmission is proposed by Ya-Lin Lee and Wen-Hsiang Tsai, that transforms a secret image into a mosaic image with the same size and looking like a preselected target image. A secret key is used for the transformation process, and only with the key can a person recover the secret image nearly losslessly from the mosaic image. The drawback of Lee and Tsai is that the mosaic image is created by fitting the tiles images into the target blocks based on the mean and standard deviation values. Hence the recovered secret image has distortions when compared to the input secret image. 3. Very fast watermarking by reversible contrast mapping [13]. D. Coltuc and J.-M. Chassery proposed a spatial domain reversible watermarking scheme that achieves high-capacity data embedding without any additional data compression. The scheme is based on the reversible contrast mapping (RCM), a simple integer transform defined on pairs of pixels. RCM is perfectly invertible, even if the least significant bits of the transformed pixels are lost. The data space occupied by the LSBs is suitable for data hiding. Here, a modified version of the basic RCM watermarking scheme is introduced that allows robustness against cropping. 4. Image hiding by optimal LSB substitution and genetic algorithm [14]. In this paper, R. Z. Wang, C. F. Lin and J. C. Lin proposed image hiding by genetic algorithm. GA can be regarded as a randomized search procedure that is usually used to solve the optimization problems. The advantages of the proposed method include the size of the embedded data can be very large, and the quality of the embedding result is not degraded significantly, the randomized process can make the embedded data meaningless to the grabbers, so the data can be protected well and the embedding result utilizing the proposed genetic algorithm is near optimal, and the processing time is acceptable.

III. PROPOSED ARCHITECTURE

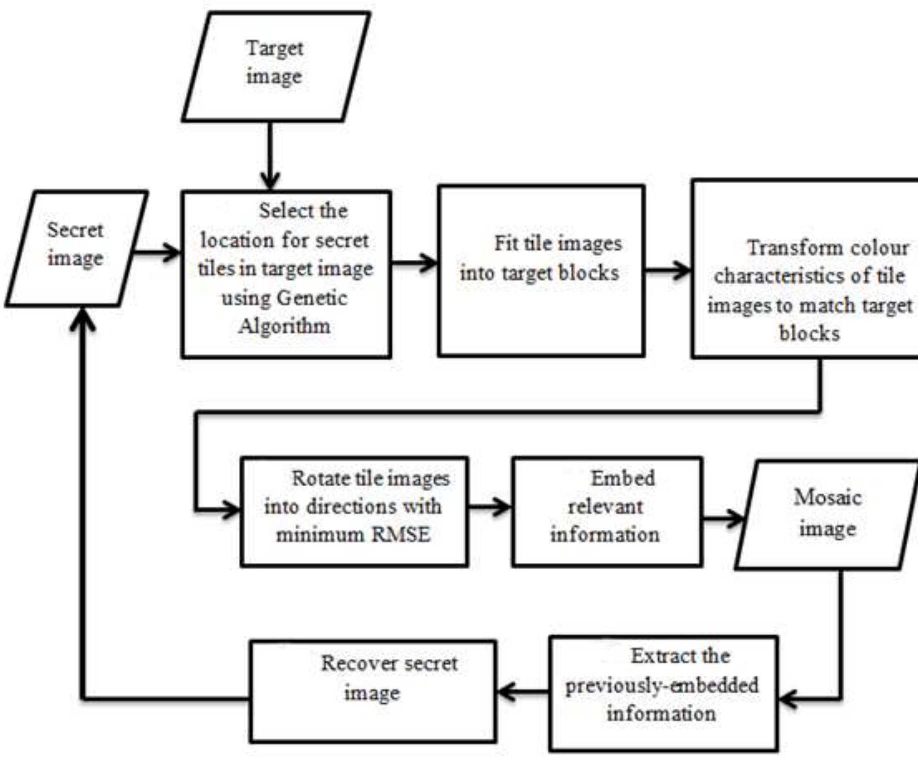

Fig. 1: Block diagram of the proposed method.

The proposed method consist of two main phases as shown by the block diagram
1) Mosaic image creation 2) Secret image recovery.

All rights reserved by www.ijirst.org

In the first phase, a mosaic image is yielded, which consists of the fragments of an input secret image with color corrections conforming to a similarity criterion based on color variations. The phase includes four stages:

1) Fitting the tiles of the secret image into the target blocks of a preselected target image using genetic algorithm
2) Transforming the color characteristics of tile images in the secret image to become that of the corresponding target block.
3) Rotating each tile image into a direction with the minimum RMSE value with respect to its corresponding target block
4) Embedding relevant information into the created mosaic image for future recovery of the secret image.

In the second phase, the information that is embedded is extracted to recover nearly losslessly the secret image from the generated mosaic image. The phase consists of two stages:

1) Extracting the embedded information for secret image recovery from the mosaic image
2) Recovering the secret image using the extracted information.

A. Mapping of Tile Images into Suitable Target Blocks

The Secret image is divided into rectangular shaped fragments called tile images of equal size and they are fitted into the blocks of target image that are selected arbitrarily. Mapping of tile images into target blocks are done using Genetic Algorithm. The population size and maximum number of generation is set as 10. First, an initial population of 10 mapping sequences is created. The next generations are created by the operations selection and crossover. The crossover probability is set to 0.6. PSNR values are considered as the fitness values. PSNR is peak signal to noise ratio. The threshold fitness value (PSNR value) is set as 40. Create mosaic image by fitting the tile images based on the optimal mapping sequence.

B. Color Transformations between Blocks

The color distributions of tile image T in the given secret image and target block B in targets image are changed to make them look alike. T and B be described as two pixel sets $\{p_1, p_2, \ldots, p_n\}$ and $\{p'_1, p'_2, \ldots, p'_n\}$, respectively. Let the color of each p_i be denoted by (r_i, g_i, b_i) and that of each p'_i by (r'_i, g'_i, b'_i). At first, the means and standard deviations of T and B are computed respectively, in each of the three color channels R, G, and B by the following formulas:

$$\mu_c = \frac{1}{n}\sum_{i=1}^{n} c_i \quad (1) \qquad \sigma_c = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(c_i - \mu_c)^2} \quad (3)$$

$$\mu_c' = \frac{1}{n}\sum_{i=1}^{n} c_i' \quad (2) \qquad \sigma_c' = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(c_i' - \mu_c')^2} \quad (4)$$

In which c_i and c'_i denote the C-channel values of pixels *pi* and p'_i, respectively, with $c = r, g,$ or b and C=R, G, or B. Next, we determine new color values (r''_i, g''_i, b''_i) for each p_i in T by

$$c_i'' = q_c(c_i - \mu_c) + \mu_c', \quad (5)$$

In which $q_c = \sigma_c'/\sigma_c$ is the standard deviation quotient where $c = r, g,$ or b. It can be verified easily that the new color mean and variance of the resulting tile image T' are equal to those of target block B, respectively. To compute the original color values (r'_i, g'_i, b'_i) of p_i from the new color values (r''_i, g''_i, b''_i) ,we use the following formula which is the inverse of (5):

$$c_i = (1/q_c)(c_i'' - \mu_c') + \mu_c. \quad (6)$$

After the color transformation process is conducted as described, some pixel values in the new tile image T' might have overflows or underflows. To deal with this problem, such values are converted to be non-overflow or non-underflow ones and record the value differences as residual values for use in later recovery. Specifically, we convert all the transformed pixel values in T' which are not smaller than 255 to be 255, and all those values not larger than 0 to be 0. Next, we calculate the differences between the original pixel values and the converted values as the residuals and keep them as part of the information associated with T'. The residuals are encoded in order to reduce the number of required bits to represent them.

C. Rotating the Tile Images

After the color characteristic of T is transformed, a further improvement on the color similarity between the resulting tile image T´ and the target block B is made by rotating T´ into one of the four directions, 0^o, 90^o, 180^o, and 270^o, which yields a rotated version of T´ with the minimum root mean square error (RMSE) value with respect to B among the four directions for final use to fit T into B.

D. Embedding the Secret Image Recovery Information

To recover the secret image from the mosaic image, relevant recovery information has to embed into the mosaic image. Here, the information embedded is the index of the target block and the optimal rotation angle. The information that is to be embedded is

All rights reserved by *www.ijirst.org*

encrypted with a key. For embedding, a technique proposed by Coltuc and Chassery [13] was adopted and is applied it to the least significant bits of the pixels in the created mosaic image to conduct data embedding. Other than the classical LSB replacement methods, which substitute Least Significant Bits with message bits directly, the reversible contrast mapping method applies simple integer transformations to pairs of pixel values. Specifically, the method conducts forward and backward integer transformations as follows, respectively, in which (x, y) are a pair of pixel values and (x', y') are the transformed ones

$$x' = 2x - y, \quad y' = 2y - x \tag{7}$$

$$x = \left\lceil \frac{2}{3}x' + \frac{1}{3}y' \right\rceil, \quad y = \left\lceil \frac{1}{3}x' + \frac{2}{3}y' \right\rceil \tag{8}$$

The method yields high data embedding capacities close to the highest bit rates and has the lowest complexity reported so far.

E. Extracting the Secret Image Recovery Information and Recovering the Secret Image

The mosaic image is segmented for extracting the secret image recovery information that was embedded into it by reversible contrast mapping. The information embedded is the index of the target block and the optimal rotation angle. The extracted information is then decrypted using the same key that was used for encrypting it. Using the extracted information, compose all the final tile images to construct the desired secret image as output.

IV. RESULT AND DISCUSSION

The proposed method is simulated using Matlab 2010.In the proposed method, genetic algorithm is used to create a mosaic image effectively. i.e, tile images are fitted into appropriate blocks of target image using genetic algorithm rather than the previous method [1] that makes use of the standard deviation values of the tile images and the target blocks. In the previous work, the mean and average standard deviations of all the tiles and blocks are computed and the tiles and blocks are sorted according to the computed average standard deviation. Then the tiles are mapped to the blocks in a one-one manner.

Fig. 2: Target image

Fig. 3: Secret Image

All rights reserved by *www.ijirst.org*

PSNR = 19.2918

Fig. 4: Recovered secret image by Lee and Tsai [1] method

PSNR = 33.5722

Fig. 5: Recovered secret image by proposed method

From the obtained PSNR values, it is clear that the secret image can be recovered nearly losslessly from the mosaic image by the proposed method that uses genetic algorithm for the tile-block fitting.

Table below shows the PSNR values of the recovered secret images

Table – 1
Comparison of PSNR values

PSNR values without using genetic algorithm	*PSNR values using genetic algorithm*
19.2918	*33.5722*
18.2166	*30.4578*
16.5648	*32.1337*
18.4678	*34.4163*
17.3559	*31.7823*
19.4828	*34.6861*

The table values show a better result for the proposed method. High PSNR value indicates that the recovered secret image is nearly similar to the original secret image. Thus with the help of genetic algorithm an optimal tile-block fitting can be obtained which results in better clarity of the recovered secret image.

All rights reserved by *www.ijirst.org*

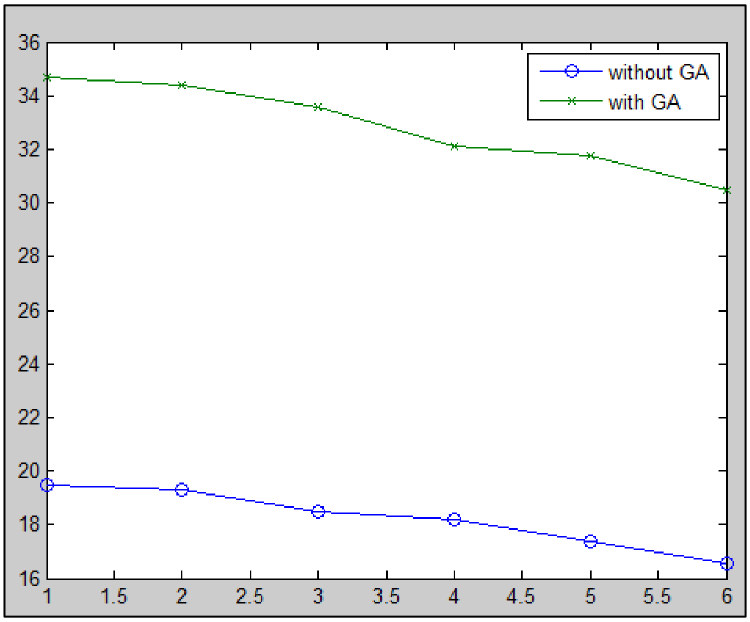

Fig. 6: Graph of PSNR values (with and without GA)

V. CONCLUSIONS

A secure image transmission is proposed, which transforms a secret image into a meaningful mosaic image with the help of genetic algorithm. The mosaic image is obtained by rearranging the fragments of a secret image in disguise of the target image. After the tiles are fitted into the blocks of target image, color transformation of the tile images are done. The tiles are then rotated for further improvement of color similarity. This results in a mosaic image which looks like the target image. Genetic Algorithms (GAs) are search algorithms based on the mechanics of the natural selection process. Genetic Algorithm has the ability to create an initial population of feasible solutions, and then recombine them in a way to guide their search to only the most optimistic areas of the state space. Genetic algorithm provides an optimal tile-block fitting sequence so that the secret image can be recovered from the mosaic image nearly losslessly. By proposed method, a meaningful mosaic image is created, in contrast to the image encryption technique which only creates meaningless noise images. Also, the proposed method transforms a secret image into a disguising mosaic image without compression, where a data hiding method must need a highly compressed version of the secret image to hide it into a cover image when the cover image and the secret image have the same data size.

REFERENCES

[1] Ya-Lin Lee and Wen-Hsiang, “A New Secure Image Transmission Technique via Secret-Fragment-Visible Mosaic Images by Nearly Reversible Color Transformations,” IEEE Trans. Circuit and system for video tech., vol. 24, no. 4, pp. 695–703 Apr. 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] Z. Ni, Y. Q. Shi, N. Ansari, and W. Su, “Reversible data hiding,” IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354–362, Mar. 2006.
[4] J. Tian, “Reversible data embedding using a difference expansion,” IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890–896, Aug. 2003.
[5] 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.
[6] 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.
[7] 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.
[8] W. Zhang, X. Hu, X. Li, and N. Yu, “Recursive histogram modification: Establishing equivalency between reversible data hiding and lossless data compression,” IEEE Trans. Image Process., vol. 22, no. 7, pp. 2775–2785, Jul. 2013.
[9] C. C. Chang, C. C. Lin, C. S. Tseng, and W. L. Tai, “Reversible hiding in DCT-based compressed images,” Inf. Sci., vol. 177, no. 13, pp. 2768–2786, 2007.
[10] 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.
[11] 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.
[12] C. K. Chan and L. M. Cheng, “Hiding data in images by simple LSB substitution,” Pattern Recognit.., vol. 37, pp. 469–474, Mar. 2004.
[13] 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.
[14] R. Z. Wang, C. F. Lin, and J. C. Lin, “Image hiding by optimal LSB substitution and genetic algorithm,” Pattern Recog., vol. 34, no. 3, pp. 671–683, 2001.

All rights reserved by *www.ijirst.org*