A Fast and Secure Transmission of Image by using Mosaic

Deepali G. Singhavi
(PG Scholar)
Department of Computer Science and Engineer
Government College of Engineering
Amravati, India

P. N. Chatur, PhD
(Head of Department)
Department of Computer Science and Engineering
Government College of Engineering
Amravati, India

ABSTRACT

When Images are transmitted through network it may happens that any third person or any unauthorized user may try to read the contents of the secret image that may contain some confidential information. To prevent Image containing private and confidential information from leakage some security is needed. The commonly used methods for image security are Encryption and data hiding. Among them data hiding is seen to be most commonly used method for information security. Now a day's a new concept of mosaic image is used in the field of data hiding for secure image transmission. In this paper for secure image transmission a new type of mosaic image is created called as secret fragment visible mosaic image by dividing secret image into small tiles and then arranging these tiles in a puzzled format with the help of another image called as carrier image. To enable resultant mosaic image to look exactly similar to selected target image reversible color transformation is proposed. The information required for recovering the secret image is embedded into the mosaic image by using enhanced LSB algorithm. Further to allow fast transmission of image lossless compression is performed on resultant mosaic image.

General Terms

Security, Data Hiding, Mosaic image.

Keywords

Data Hiding, Mosaic image, Secret fragment visible mosaic image, AES security algorithm.

1. INTRODUCTION

In the present world as more and more information is generated and transferred through network, the information being transmitted becomes more and more valuable and security of this data becomes a major issue. This information varies from text to multimedia data, multimedia data includes a major amount of images, images are transferred for various applications that include medical image system, personal photographs, military images, and confidential documents that may contain some private or confidential information that is required to be protected from eavesdroppers or from any unauthorized person. There are different approaches that are in use to enable image security, the commonly used approaches are steganography and cryptography. Cryptography is a technique that uses various encryption and decryption methods to keep the original message secret. As in cryptography the encrypted image is visible to user and is in noise or unreadable form it attracts the attention of hacker or eavesdroppers. So to make the secret image more secure the concept of steganography is introduced that embed the secret message behind a carrier to make it invisible while communication. The two methods differ from the fact that cryptography tries to keep the content of message secret whereas the steganography tries to keep the existence of message itself secret. In Image steganography the existence of secret image is made hidden by hiding it behind another image. To make secret image more secure a new concept of mosaic image is in use along with steganography called as mosaic image steganography. Mosaic is a kind of art in which small pieces of material such as glass, stone are composed together to form a single image. In digital form small fragments of images called as tiles are arranged to form a single image called as mosaic. Creation of mosaic by computer is a new research area now a day's. Different mosaics can be created from a single image depending on their choice of tiles and their placement in resulting image. There are different types of mosaic that includes crystallization mosaic, ancient mosaic that are created by dividing the secret image into tiles and then reconstructing the image by properly painting the tiles so these types of mosaic can also be called as tile mosaic. Other types of mosaic includes photo-mosaic, and puzzle image mosaic that are formed by painting or covering the given sources image by fitting different images from the database hence they can also be called as multipicture mosaic image. A special kind of mosaic include secret fragment visible mosaic image that are created by dividing secret image into small fragments called as tiles and then arranging these tiles in a random or puzzled sequence with the help of another image called as carrier image. The resultant mosaic is such that all fragments of secret image are visible to user but as they are arranged in puzzled form no one will be able to guess or read the contents of secret image. In this paper a new method for the creation of secret fragment visible mosaic image is proposed along with a reversible color transformation method to enable exact recovery of secret image. To further allow exact recovery of image some information of secret image are embedded into mosaic image by using a new steganography algorithm that is enhanced least significant bit algorithm. To enable fast transmission of secret image a lossless compression is done on resultant mosaic image. There are two types of compression lossy and lossless. Lossy compression tries to compress the file to save storage space by discarding extra image content from original image. On the other hand lossless compression, tries to represent data in mathematical form without removal of any information contents. The advantage of lossless compression is that it keeps the content of original image as it is without any loss, although it does not compress the original image to a very small size. Thus the resultant mosaic image can be saved by using a lossless compression while transmission.

2. RELAED WORK

Steganography is a commonly used technique that provides security by hiding the existence of secret message. Many different types of steganography algorithm are proposed to hide secret message. The commonly used steganography algorithm is least significant bit algorithm that hides secret message by replacing least significant bits of carrier by secret message. In most commonly used Least significant bit algorithm only last bit of cover message is replaced by secret message thus 1 bit can be embedded into 8 bit gray scale image and 3 bits can be embedded into 24 bit color image. J. Tian [1] proposed a reversible data embedding algorithm also called as lossless data embedding method that uses difference value of neighboring pixel to embed secret message. Z. Ni, Y. Q. Shi, N. Ansari, and W. Su [2] proposed a reversible data hiding method that can recover the secret message losslessly, the method generates histogram for the given secret image and determines the zero point and peak point, the points or pixels values between zero and peak point are used to embed secret message. D. Coltuc and J. M. Chassery [3] proposed a method that first performs integer transform on pair of pixels then uses simple LSB method to embed secret message. S. Lee, C. D. Yoo, and T. Kalker[4] proposes a reversible watermarking technique based on integer to integer transform that first divides secret image into block and uses high frequency wavelet coefficients of each block to embed secret message.

Mosaic is new type of art in which small pieces of material are fragmented together to create a single image. Creation of mosaic by computer is a new area of research, many different authors have classified mosaic image into different type and have presented different way of creating them. Battiato et al. [5] tries to classify mosaic into four basic types in which the first two types of mosaic includes crystallization mosaic, ancient mosaic that are created by dividing the source image into small fragments and then reconstructing the image by properly painting the tiles so these types of tiles are generally called as tile mosaic. Other two types of mosaic include photo mosaic and puzzle image mosaic that are created by painting the source image using varies small images from database so they are also called as multi-picture mosaic. Kim and Pellacini [6] proposed and created a new type of mosaic called as jigsaw image mosaic that is formed by composing or fitting images of arbitrary shapes selected from database. Di Blasi et al. [7] present a variation to jigsaw image called as puzzle image mosaic where arbitrary shapes tiles are used to form the final picture it gives better computation time as compare to jigsaw mosaic.

I-Jen Lai and Wen-Hsiang Tsai [8] have presented a method for image security that combines or make use of mosaic image along with steganography called as mosaic image steganography. They proposed a new kind of mosaic called as secret fragment visible mosaic for securely transmitting the secret image. Mosaic image is formed by dividing the given source image into small tiles and then selecting a proper matching image from database that will act as target image or cover image according to some similarity criteria then arranging this tiles to form a resultant image called as secret fragment visible mosaic image. Benefit of resultant mosaic image is that all the tiles of secret image are visible to user but they are so tiny in size and are placed in random position that no one is able to read or guess the secret image.

3. PROPOSED WORK

Here in this paper a new method for creation of secret fragment visible mosaic is proposed which tries to remove drawbacks of I-Jen Lai and Wen-Hsiang Tsai [8]. The drawback of above method includes 1) it require large database to be created from where a target image appropriate to given secret image is selected 2) It is time consuming to select a target image that will satisfy some similarity criteria from database 3) The target image should be in double size to that of secret image and 4) User is not able to select image of his/her choice as target image. The proposed method includes following phases and are shown in fig(1).

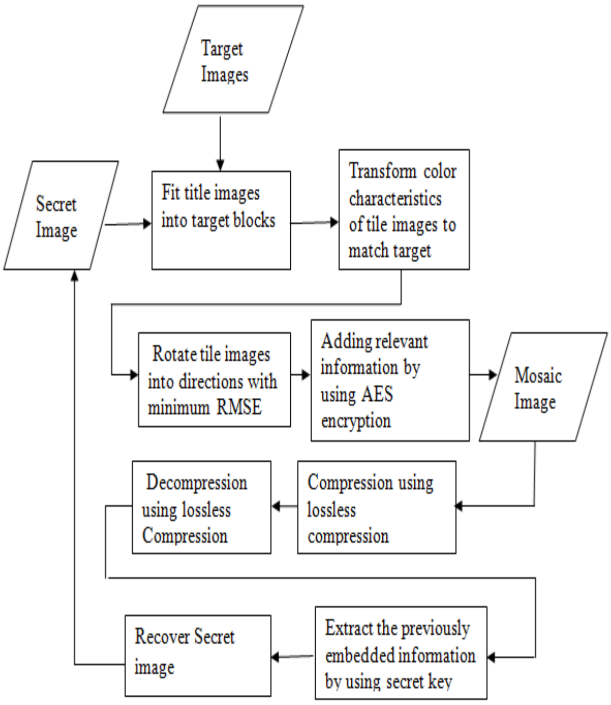
Target Images
Secret Image
Fit title images into target blocks
Transform color characteristics of tile images to match target
Rotate tile images into directions with minimum RMSE
Adding relevant information by using AES encryption
Mosaic Image
Compression using lossless compression
Decompression using lossless Compression
Extract the previously embedded information by using secret key
Recover Secret image

Fig 1. Flow Diagram of Proposed Method

3.1 Mosaic Image Creation

The first Step of mosaic image creation is selection of target image. The method proposed by I-Jen Lai and Wen Hsiang Tsai required that the target image should be selected from database and it should match some similarity criteria to be selected as target image and finally it should be double in size to that of secret image, to remove this drawbacks the proposed method allow user to select any image of their choice and of any size as target image. But to allow the mosaic image with little quality drop lose but not more it is suggested that the target image selected should be of same background as that of secret image. Next step is to divide both secret image and target image into fragments such that both images contain same number of blocks and that is too of same size, to assure this the target image and secret image are required to be of same size. To assure this the proposed method will first check whether secret image is of same size as of target image or not if not it will resize it to make it of the same size as that of target image. Then to split secret image and target image into same number of blocks same splitting criteria is used to split them After splitting the main problem and question is how to find out or get perfect position where each tiles of secret image is to be placed. To find the best fit block of target image for each tiles of secret image the standard deviation of each tiles is used as a similarity measure criteria. That is standard deviation for each blocks of target image and for each tiles of secret image is calculated. Then all the tiles of secret image are arranged in ascending order and also blocks of target image in ascending order according to their standard deviation. Then the first tile image in a sequential order is placed at a position of first block in a sorted sequence of target image, and also 2nd block in sorted sequence of tile image is placed at a position of second block in a sorted sequence of target image. Similarly the same step is repeated for rest of tiles block to create final mosaic image called as secret fragment visible mosaic image. To recover the secret image a recovery file is created that will contain information where each tiles of secret image are placed in resultant mosaic image. During the process of creation of secret fragment visible mosaic image after getting the new position for each tiles of secret image this new position of tile is added into the recovery file that will contain index of each tiles block along with its old and new position respectively for future use. Hence the resultant mosaic didn't contain any information of stored image, it only contain the fragments or tiles of secret image. For constructing final output from mosaic image the recovery file will be needed that will act as position file that will contain original position of each tile images. The file would be combined and merge with output image and is send to receiver without any loss. For security concern encryption algorithm are used with a secret key such that without a proper decryption algorithm or without a correct key no third person will be able to read the file or recreate the secret image. After creating a mosaic and generating a recovery file reversible color transformation is performed on mosaic image to make it look similar to selected target image and to reduce the distortion.

let us consider S and T as two pixel sets described by $\{p_1,p_2,\ldots\ldots p_n\}$ and $\{p_1',p_2'\ldots\ldots\ldots p_n'\}$ respectively, where S is used to represent tiles of secret image and T is used to represent block of target image. Let us further consider that each pixel p_i is represented by color (r_i, g_i, b_i) and each pixel p_i' is represented by color (r_i', g_i', b_i'). Next mean and standard deviation of S and T is computed respectively by using formula given below.

$$\mu_c = \frac{1}{n}\sum_{i=1}^{n} c_i \quad , \quad \mu_c' = \frac{1}{n}\sum_{i=1}^{n} c_i' (1)$$

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

Where in this equations c_i and c_i' denotes C channel values of each pixel p_i and p_i' respectively, with c = r, g, or b and C= R, G, or B. In next step new color (r_i'',g_i'',b_i'') for each p_i in S is computed by using formula given below

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

Where q_c is the standard deviation coefficient calculated by using $q_c = \sigma_c'/\sigma_c$ and c = r, g, or b. Now original color value that is (r_i, g_i, b_i) of p_i is computedby using inverse of equation (3) which is given by

$$c_i = (1/q_c)(c_i'' - \mu_c') + \mu_c$$
(4)

After performing color transformation the overflow and underflow values of pixels is handled by converting pixel value above than 255 to 255 and pixel value below than zero to 0 respectively. Then the tile images of resulting mosaic S' is rotated after color transformation in direction 0^0, 90^0, 180^0, 270^0 to yield minimum root mean square error with respect to target image T. In order to reconstruct secret image some recovery information is embedded for exact recovery that includes the optimal rotation angle and the means of S and T and the standard deviation quotients of all color channels along with the tiles original and new positions. A file is created that contain all this information for recovery and called as recovery file. To allow only the intended user to recreate the mosaic the recovery file is encrypted by using a secret key and by using AES encryption algorithm that is very efficient algorithm to provide security. And this encrypted file is send to receiver for recovery. So only the intended receiver will be able to decrypt the recovery file with the correct key and thus able to recover the secret image.

3.2 Compression and Decompression

As transmitting multimedia Data through internet it generally takes time for uploading to transfer and similarly for downloading. To enable user to reduce this time and enable fast transmitting image a lossless compression algorithm is performed on mosaic image. There are two types of compression algorithm lossless and lossy compression. Lossy compression reduces the size of file by eliminating excess image data from original image. Whereas lossless compression on the other hand does not removes any original image but represent image in mathematical form to reduce its size. The original image integrity is maintained and the original image and the decompressed image is bit-by-bit similar to each other. The advantage of lossless compression is it maintains the original image content intact without any loss. Here in this paper for compression lossless version of JPEG lossy compression algorithm is implemented.

3.3 Recovering secret image from mosaic

For recovery of secret image, first the recovery file that contain information for secret image recovery is reconstructed from the input decompressed image. To read the contents of recovery file it is needed to decrypt the content of file by using the decryption algorithm with the same key with which encryption is performed. After decrypting the file by using AES decryption algorithm that contain information such as optimal rotation angle, the means of S and T and the standard deviation quotients of all color channels along with current and original position of each every tile blocks. By using this value first each tile images of mosaic image is rotated in reverse direction by using extracted optimal rotation angle and then the color of secret image is recreated by using inverse of color transformation by using formula given in equation (4) and by using extracted mean and standard deviation value of secret and target image. After recreating color the final step is to place each and every tile images at their proper position to get final secret image for this the content of recovery file is used to know image original position and then each tile block is placed at their original position to get the final secret image.

4. EXPERIMENTAL RESULTS OF MOSAIC IMAGE CREATION

For the experimental result to create secret fragment visible mosaic image the sample images that is secret image of fig(2) and target image of fig(3) is used to create mosaic image of fig(4).

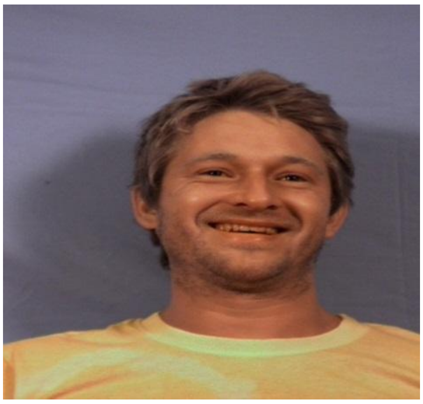

Fig 2. Secret Image

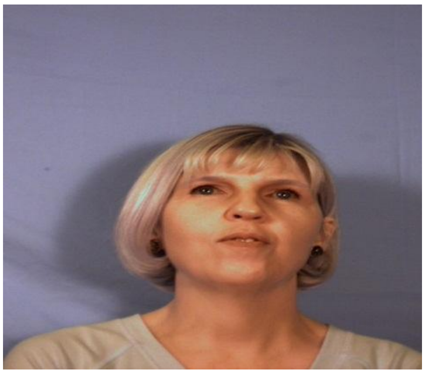

Fig 3. Target Image

Here first the resolutions of both inputted file that is of both secret image and target image is checked. The mosaic image is to be created of same size as that of secret image and also the target image and secret image is to be divided into same number of blocks to implement our algorithm. So to satisfy this requirement first the resolution of secret image is checked and if its resolution is same as that of target image then the mosaic image creation is started directly and if its resolution is different from that of target image then the secret image is resized to make its resolution to be same as that of target image. In above example both target image and secret image are of resolution 480 * 640 so the mosaic creation is started directly without resizing secret image. In next step both target image and secret image is divided into same number of tiles for this both secret image and target image are divided into small tiles of resolution 3*4 as both images are of same size so it creates same number of tiles of secret image as that of number of blocks of target image of same size. For example of fig (2) and (3) it creates 25560 tiles for both secret image and target image. After that it will calculate standard deviation of each tile of secret image and target image by using equation (2) and then both tiles of target image and secret image are arranged in ascending order of standard deviation. Then the first tile in sorted sequence of secret image is placed into the position of first block in the sorted sequence of target image same step is repeated for second tile of secret image and so on. Atlast it will create final secret fragment visible mosaic image that is shown in fig (4).

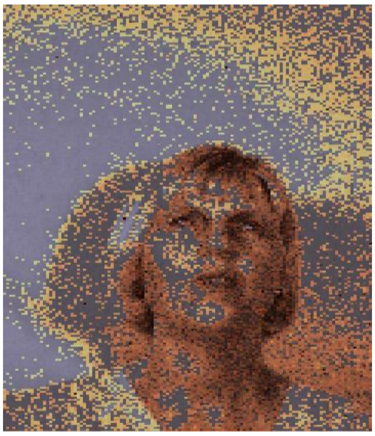

Fig 4. Secret Fragment Visible Mosaic Image

After that color transformation is applied by using equation (3) to make color characteristic of mosaic image to be same as that of target image. After that the underflow and overflow values of pixels are checked and handled. At last each and every tiles of mosaic image is rotated in direction 0^0, 90^0, 180^0, 270^0 to minimize the root mean square error value. At last AES encryption algorithm is implemented to transfer the recovery information along with mosaic image for exact recovery of secret image. The final mosaic image obtained after color transformation and embedding is shown in fig (5).

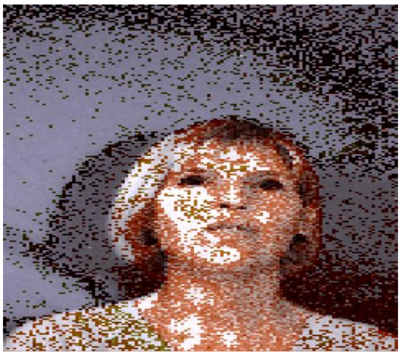

Fig 5. Mosaic Image after color Transformation

This mosaic image is compressed by using lossless JPEG compression to reduce its size from 90KB to 34KB for fast transmission. At the receiver end the image is first decompressed and then secret image is recovered from mosaic image. The final secret image is shown in fig (6).

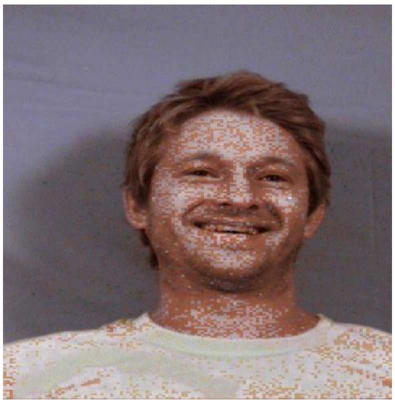

Fig 6. Resultant Secret Image

5. CONCLUSION

A new method for creation of secret fragment visible mosaic image has been proposed in this paper. The method creates mosaic image by using any target image selected by user of their choice of any size. The mosaic image created is of same size as that of target image. The resultant mosaic image is such that all the fragments of secret image are visible to user but they are so small and random in position that no third person will be able to read its content. To allow mosaic image to look similar to secret image and to reduce the resultant distortion a color transformation is performed on mosaic image. And to allow fast and secure transmission of secret image a lossless JPEG compression is performed on mosaic image and an encryption algorithm is performed on recovery file by using a secret key so that no one would be able to read the secret image from mosaic image without having the correct key.

6. FUTURE WORK

The future work may be directed to extendthe proposed method for gray scaleimages tocreate gray scale mosaic image that can be used to provide security to legal documents.

7. ACKNOWLEDGMENTS

My thanks goes to my guide who have guided me for development of this project.

8. REFERENCES

[1] S. Battiato, G. Di Blasi, G. M. Farinella, and G. Gallo, “Digital mosaic framework: An overview,” Eurograph.—Comput. Graph. Forum, vol. 26, no. 4, pp. 794–812, Dec. 2007.

[2] J.Kimand F. Pellacini, “Jigsaw image mosaics,” in Proc SIGGRAPH, San Antonio, TX, Jul. 2002, pp. 657–664.

[3] G. Di Blasi, G. Gallo, and M. Petralia, “Puzzle image mosaic,” in Proc. IASTED/VIIP, Benidorm, Spain, Sep. 2005, pp. 33–37.

[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] 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

[6] 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

[7] 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.

[8] 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.

[9] Y. L. Lee and W. H. Tsai, “A New Secure Image Transmission Technique via Secret-Fragment-Visible Mosaic Images by Nearly Reversible Color Transformations,” IEEE Trans. on circuit and systems for video Tech., vol. 24, no. 4, Apr. 2014, pp. 695-703.

[10] S. Gupta, G. Gujral and N. Aggrawal, “Enhanced Least Significant Bit algorithm For Image Steganography,” IJCEM International Journal of Computational Engineering & Management, Vol. 15 Issue 4,pp. 40-42, July 2012.