RESEARCH ARTICLE OPEN ACCESS

Image Hiding Technique Based on Secret Fragment Visible Mosaic Image

Chetan G.Tappe[1], A.V. Deorankar[2]

[1]*P.G. Student, Department of Computer Engineering, Govt. College of Engineering, Amravati, India*[1],
[2]*Associate Professor, Department of Information Technology, Govt. College of Engineering, Amravati, India*

Abstract:

As we know that, the process of hiding data behind any one of the multimedia elements is called steganography. It is used in many areas where the safety risk is very high. The normal encryption and decryption mechanisms will increase the protection but anyone can break the security by analyzing the secret information. Where in steganography the hacker may not know whether the data is secret or not. Thus steganography is better than encryption in many conditions. In the past lot of steganography algorithms have been proposed. But still those algorithms are not in case perfect solutions. In this paper we proposed a new idea of steganography. The idea behind our proposed method is, the cover image will be altered based upon the secret image. The secret image will be divided into number of blocks and these blocks will be shuffled logically and then it will be merged with the cover image to generate the Segno image. Our suggested method, originally designed for allocating with color images, but also be extended to for gray scale images.

Keyword— **Data hiding, encryption, secret-fragment visible mosaic image, security, secure image transmission.**

I. INTRODUCTION

Currently, images from various bases are frequently used and transmitted through the internet for various applications, such as online personal photograph albums, private enterprise archives, document storage systems, medicinal imaging systems, and army image databases. These images usually contain private or confidential information so that they should be protected from leakages during communications. Newly, many methods have been proposed for securing image transmission, for which two common approaches are image encryption and data hiding. Another normally used method for secure image transmission is data hiding, in data hiding secret image is hidden behind a carrier; carrier can be anything an image, document, audio file and a video file. Now a day for secure image transmission a new concept is being in used that is of mosaic image in the field of data hiding. Mosaic is a new type of art in which parts of small material such as plastic, glass and small tiles are combined to form a single image called as mosaic image. Design of mosaic image is a new research area in the field of digital image processing. Here in this paper we proposed a new method of creating a mosaic image i.e. a secret fragment visible mosaic image. A secret fragment detectable mosaic image is an image formed by dividing a given secret image into small tiles and conveying these tiles of secret image in cover of another image called as transferor image. The resultant mosaic image is such that it inserts the source image covertly such that all the fragments of the secret image are noticeable to user but they are so tiny in size and chance in position such that the viewer cannot able to guess or figure out how the secret image or source image would looks like. Thus the resulting mosaic image can be used for covert message or for secret image transmission. In this paper a new method for creating a secret fragment visible fusion

image is proposed that hides the fragments of secret image behind a carrier image of the same size as that of the transferor image by using standard deviation as a similarity measure to form a resultant mosaic image, It is perceived that the color of the image is an effective feature that affect the overall appearance of the resultant mosaic image so we extract the color distribution of the image for effective image similarity measure to form the mosaic image. The detailed method of mosaic image creation is given in this paper. Data confidentiality issues can be found in various range of sources such as healthcare records, criminal justice investigations and Proceedings, economic institutions and businesses, biological traits, residence and geographic records and society. As more and more systems are connected to the Internet today providing security to data and data secrecy has become increasingly important.

Mosaic is a new type of artwork and it can be composed by small pieces of materials mainly including tile. The mosaic images are created perfectly and it has been widely used. Mosaic image creation has now become a recent technique. Four types of mosaic images namely crystallization mosaic, ancient mosaic, photo mosaic and puzzle image mosaic are proposed in the first two types, the source image is split into tile image and then it is reconstructed by painting the tiles and they are named as tile images. The next two types include obtaining target image and with the help of database, cover image has been obtained. They may be called as multi-picture mosaics. The previously mentioned mosaic image namely crystallization mosaic uses voronoi diagram. The main concept of voronoi diagram includes by using different sites. The blocks are placed in the sites randomly. Based on the original image, the blocks are being filled by the colors. Similarly, another type of mosaic image namely Jigsaw image mosaic, proposed by Kim and Pellacini . It is a kind of puzzle image. Here, the tile images are arranged in puzzle format. So that, the original image may not be visible to people. It can be performed by placing tiles along the edge direction. These methods include repetition of tile images. This was denoted as an optimization problem. In order to overcome that, a randomized iterative algorithm and conventional genetic algorithm has been proposed by Secret-Fragment-Visible-Mosaic image is a new type of art image. The source image has been dividing into smaller fragments. This mosaic image contains those smaller fragments. The fragments are too small in size. So that, people who are observing cannot point out how does the source image look likes. Hence the source image can be embedded secretly in the resulting mosaic image. We are proposing a new concept named information hiding in this paper. The information will be in the form of image. This image is said to be the secret image. Hence we are providing security in the form of image. How the process involved in information hiding. The secret image is first divide into nine parts. Proper target image have to be selected. The selection process depends upon the file. The target image should be selected from the file and that target image should be a correct match for the source image. The target image we have select should be dual in size then the source image. Mosaic image is then generated. The tile images can be used frequently. By using a secret key, the mosaic image has been put under the method and thus we are achievement the secret image after inserting process. The hacker without knowing the key cannot reconstruct back the mosaic image and thus the secret image cannot be viewed.

This paper is organized as follows; in section II, basic idea and construction of database are described. In section III, creation of Secret-Fragment-Visible-Mosaic Image are discussed and in section IV & V, secret image recovery and extension to gray scale images are defined and security measures are provided in section VI and then we conclude in section VII.

II. PROPOSED METHOD

In this section the method for the creation of secret fragment visible mosaic image is given; the detailed system architecture of the proposed method is shown in figure (1).

Phase 1: Target images are selected similar to the secret image.

Phase 2: Secret-Fragment-Visible Image has been created.

Phase 3: Secret image has been recovered from the mosaic image.

A. Basic idea database

As a phase 1 includes normal database construction. Phase 2 target image selection and construction of mosaic image. For target image selection, DB should previously contain all the details of the target image. The URL of all images which is going to be selecting as target image has been stored in the DB. The images in the DB should be accurately divided and all their histogram values ought to be finding out. Let us consider 5 as an example. Let the DB contains 5 images, Among the 5 images, we have to pick an image which is more similar to the secret image. After obtaining the target image, mosaic image have to be generated. The tile images we obtained are fitted into the target image blocks. And thus inserting provides more security.

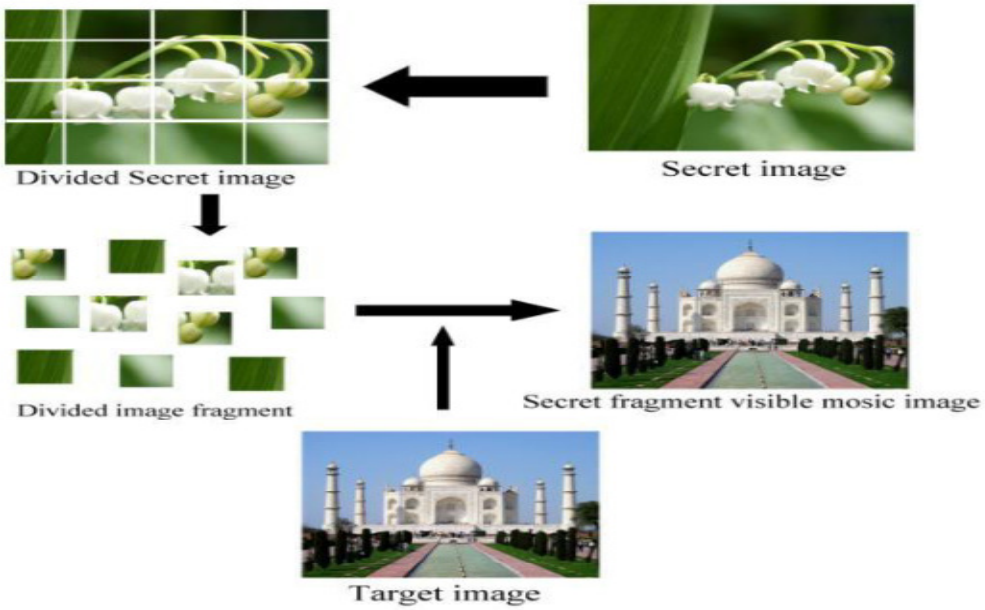

Fig.1. Creation of secret fragment-visible mosaic image.

Phase 3 includes recovery of secret image. After inserting, the Secret-Fragment-Visible-Mosaic image will be obtained. By using the secret key, we can obtain the secret image from the fitting mosaic image. The acquired secret image will be in puzzle form. In-order to obtain the perfect secret image, key generation technique has been used. Finally we obtain the secret image without any leakage of information.

B. Database creation

For the construction of DB, the first aim we should have is the database should be as large enough as possible. Since the images require more storage and depending upon their sizes, the DB should be large. A target image has chosen from the DB. It should match the secret image. Similar can be performed by calculating the h' values of both the target and secret images. Both are splitted into 9 blocks and each block's h-value should be found out. 6 to 7 block matching are more than enough for us to select the target image. 7 can be taken as maximum. The image which is having 7 or more than 7 matching can be taken as the target image. This target image should be dual in size as previously said. We mainly focus on the color. Three basic colors red, blue, green plays the major role since these three are more complex to human eye. We can convert the colors using h-feature value of all the three colors.

C. Target image

First of all, target image should be a selection of before constructing the mosaic image. The most parallel target image can be found out by using Greedy search algorithm. For that, proper image should be chosen from the DB. The DB contains details of number of images. Before finding the target image, we have to measure for image similarity. Based on the comparison we can proceed. The selected target image & secret image's h- feature value. Let us consider S as secret image and D as target image. We have to find image similarity between these two

III. MOSAIC IMAGE CREATION

The creation of Secret-Fragment-Visible-Mosaic Image Fig. 1. includes 3 stages namely.

A. Selecting the target image.

B. Fitting the image into target block.

C. Inserting the tile image fitting data.

A. Selecting the target image

Selection of target image mainly involves in the selection of the most similar target image. As mentioned previous, the secret image and target image has been divided into blocks. All the blocks of target image are measured in order to h-values. After finding h-feature values of all the blocks, each block has been compared with each and every blocks of the secret image. For 1st block may match with the 9th block and so on. The viewer does not have any chance to know about the matching.

B. Fitting the images into Target blocks

After manipulative all the values, the images should be fit into the target blocks. Perfect target blocks from the target image are selected by execution Greedy-search process. This greedy search algorithm finds the most similar image. The tile images are then fitted into the target blocks in order to generate Secret-Fragment-Visible-Mosaic Image.

C. Inserting tile image fitting data

The results of the target block including width and height of the target block are transformed into binary string and they are inserted. The binary string is inserted at the first ten pixels of 1st block. All blocks from 1 to 9 are similarly inserted in raster-scan order by lossless LSB replacement. Each block is 1st divided into two sub-divisions. The 1st sub-division consists of 0 – 8 pixels. The first division consists of key and retrieval information. The second block consists of 9 to remaining pixels. By using Random class method, we can obtain the correct key during key generation. Thus embedding takes place and finally secret key has been recovered.

IV. IMAGE RECOVERY

In this stage, we are going to regain the secret image which is hidden behind the target image.ie we are recovering the secret image from the mosaic image. It involves 2 steps as follows.

i) Recovering tile image fitting information

Here, we are retrieving the already fitted tile image.ie the tile image we had already fitted has to be removed back from the mosaic image. This can be done using reverse version of lossless LSB replacement. This reverse version is being used because, during fitting, we had used the lossless LSB replacement method. This reverse version method produces perfect tile image by extracting the recovery sequence. This process has to be done from the first block till the last. Here, the reverse version of lossless LSB plays a major role in extracting the tile images.

ii) Recreating the secret image

The misplaced tile images are recreated here. The retrieved image is in the puzzle format. This puzzle-form image blocks are to be restored using raster-scan order. For ex, we can obtain the image in the order of 9, 8, 7 etc., this image is known as puzzle-format image. We are now creating it and obtaining as 1, 2, 3 etc., blocks. Hence the secret image has been reconstructed and obtained without any loss of information.

V. GRAY SCALE MOSAIC IMAGES

If the secret image we have taken is color, the target image we have to select should also be a color image. In proposed, we are using color image and hence we are conclusion h-value. This can be extended to the gray-scale creation. Suppose our secret image is a gray-scale image, the following process should be made. At first, the DB should have the storing of all the details of target image. The color image DB should be converted to gray-scale DB. Here, we are finding y-feature value instead of h-value. The image similarity can be obtained by finding.

$$m(s, d) = |ys - yd| \qquad (1)$$

Similarly the secret image been restored and the secret image can be obtained without any loss.

VI. SECURITY COMMUNICATION

We are providing security by hiding the image as fragments. Using secret key, we are recovering back the secret image without any loss by providing security. Without knowing the key, no one can know what the image looks like. Suppose if the reverse order LSB replacement has been known, one can find the secret image. In order to avoid this, we are providing added secret key. Without knowing this, no one can obtain the secret image. This kind of security can be provided in case of networks while sending and receiving data. Hence security has been provided strongly in this paper.

VII. CONCLUSION

The proposed system has obtained a lot of scope in providing data hiding. This method can be used in army applications in order to maintain secrecy. The communication we are providing should be secure. This method can be extended by using smaller DB and it can be done using gray-scale images and they may be useful for hiding gray-scale document involving data image.

REFERENCES

[1] Y. Dobashi, T. Haga, H. Johan, and T. Nishita, “A method for creating mosaic image using voronoi diagrams,” in Proc.Eurographics, Saarbrucken, Germany, Sep. 2002, pp. 341- 348.

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

[3] Battiato, G. M. farinella, and G. Gallo,“Digital mosaic framework: An overview,” Eurograph.Comp. Graph. Forum,Vol.26, no. 4, pp. 794 – 812, Dec.2007.

[4] 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] Y. L. Lee and W. H. Tsai, "A New Secure Image Transmission Technique via Secret-Fragment-Visible Mosaic

[6] Images by Nearly Reversible Color Transformations," IEEE Trans.on circuit and systems for video Tech., vol. 24, no. 4,pp. 695-703,april 2014.

[7] Reinhard, M. Ashikhmin. B. Gooch, and P. Shirley, “Color Transfer between images”, IEEE Comp. Graph. Appl., vol. 21, no. 5, pp. 34-41, Sep.-Oct. 2001.

[8] W. Liu,W. Zeng, L. Dong, andQ.Yao, “Efficient compression of encrypted gray scale images,” IEEE Trans. Image Process., vol. 19, no. 4, pp. 1097–1102, Apr. 2010.