RESEARCH ARTICLE OPEN ACCESS

Reversible Color Transformation: Method To Secure Secret Image By Transforming Into Secret Fragment Visible Mosaic Image

Kirti Joge[1], Prof. V. K. Barbuddhe[2]
[1]*Student, Dept. of Electronics and Telecommunication Engineering, JCET Yavatmal, Maharashtra, India*
[2]*Asso.Prof, Dept. of Electronics and Telecommunication Engineering, JCET Yavatmal, Maharashtra, India*

ABSTRACT
Security of information is becoming main target for modern network age. Internet is the most popular medium for transferring of data. The images which are being transmitted are have various applications, such as confidential enterprise archives, etc. As these images contain secret information which have to protect from unauthorized receptors during transmission of these images hence, a new secure transmission technique is proposed, by transforming confidential or secret image into meaningful secret fragment mosaic image. This mosaic tile image is almost of same size and looks similar to the selected target image. The proposed method contains technique which forms the secret-fragment-visible mosaic image using reversible color transformation scheme. The blocks fragment of secret image are arrange in different ways to produce mosaic image which is seems to be different from secret image. The color transformation process is used, so that secret image may be recovered nearly losslessly. A key is embedded by a losslessly data hiding scheme into created mosaic image for recovery of the original secret image.

Keywords: Color Transformation, Data Hiding, Mosaic tile image, Secure image transmission, Secret fragment visible mosaic image.

I. INTRODUCTION

Internet becoming a wide network for transferring the data. The image from various sources can be transmitted for various purposes such as confidential enterprise archives, medical imaging systems, and military image databases. Because of such wide network the leakage chances of leakage of secret information will be increases. Some of the images can contain private or confidential information which must to protect from unauthorized receptor or hackers for example in military field it is very important to protect the secret information from third party during transmission. Many methods are proposed for the security of image such as cryptography and image steganography.

Cryptography is an art and science of protecting information from unauthorized attackers by changing its form. It gives four basic services such as confidential, authentication, data integrity, non-repudiation. Instead of these it have some issues as high availability, delay in time, high cost etc. which makes its performance as low.

Another method is image steganography, is a science of hiding image in cover media so that on one recognized secret image. But the drawbacks of these techniques are size and protection. One has to provide more padding around the secret image so that secret image should not be recognizable.[1-5]

Proposed work helps to overcome these drawbacks. This is a technique which transfers a secret image into a meaningful secret fragment visible mosaic image. This mosaic image is having same size as that of target image and also looks similar to it. The mosaic image is obtained by arranging blocks fragment of secret image. The secret image is first divided into rectangular fragments. Then they are fitted into the target blocks according to the color characteristics of both. The process of the transformation can be carried out with the help of some relevant embedded information which is also useful for losslessly recovery of secret image from the mosaic tile image. This works as a key which is being embedded while converting secret image into mosaic fragment image[6-9]. The LSB substitution technique of data hiding method is used to embed the key of 8 bit in proposed method. It can also provide the security consideration of embedded information.

II. IMPLEMENTATION

Embedding secret image into mosaic tile image with text such that it look similar to the target image which is select from the database is challenging part. If secret fragment mosaic image does not look like a target image then the third party may get hint about the image and then it is possible to find out the secret image. So the proposed work mainly include the two main phase as shown in diagram fig 1. These are mosaic tile image creation and secret image & secret text recovery. These two phases plays important role in securing the image. If there is imperfection in formation of mosaic tile image then the whole security factor is in danger. The second phase may use the key which is embedded in mosaic image for lossless recovery.

In the first phase, mosaic image consist of the fragments of the input secret image with the same color characteristic as that of target image which is selected from database. The first phase include four stages that are fit tile images into target, transform color characteristics of tile image to match target blocks, rotate tile image into directions with minimum RMSE and embed relevant information. In the second phase the secret image is extract from the mosaic tile image. This is important phase as it gives the original secret image to the authorized party. The whole procedure success is depending on these two phases. The second phase also includes the recovery of the secret image from the mosaic tile image. This phase also include stages such as extraction of the previously embedded information and recovery of secret image. This stage plays important role in the whole procedure, as it gives the original secret image to the authorized party.

The generation of the mosaic tile image may cause problem of color transformation between blocks. For the generation of mosaic image it is necessary that the tile image in the given secret image must be fit in the blocks of selected target image. Secondly, both contain the different color characteristic hence mosaic tile image is difficult to form[10]. To overcome this problem color transformation scheme is used to convert one color characteristic into another. This will solve the mosaic tile image formation problem. Further the essential information has to embed into the new tile image for the next step i.e. for the recovery of the secret image. The volume of required information is reduced for recovery purpose. By using this, the key will hide such a way that it does not seem to anyone. Generally the key is in the form of 8 bit digit within range of 0 to 255.

Next is the selection of the appropriate target blocks. There is one issue of choosing appropriate block for each tile image. For this purpose we used standard deviation of colors to select most similar color characteristic of block and tile image. The tile image and blocks are sorted out as per the standard value of deviation and form a sequence of both. To fit the target block first color transformation is carried out then it get rotate into 0^0,90^0,180^0,270^0 with minimum RMSE in this way first tile image get fit into the block as per following the sequence in this way all get fit with each other.

Handling overflow and underflow is another issue but it can be reduced. In some cases the pixel value may get overflow or underflow, here in this technique such values get converted into non-underflow and non -overflow. By this overflow and

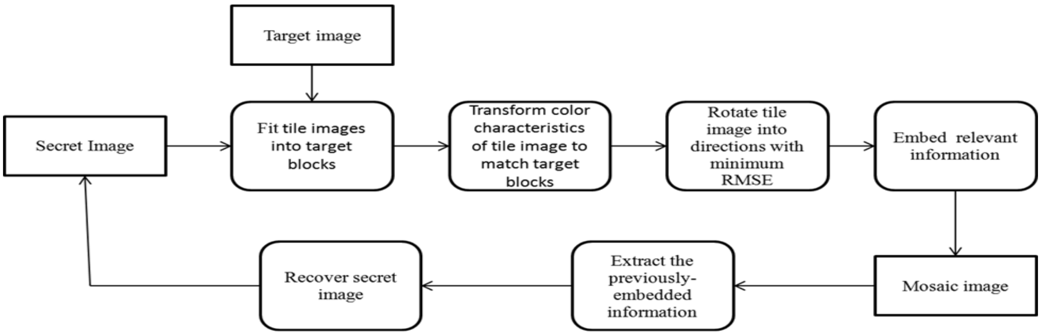
Target image
Secret Image
Fit tile images into target blocks
Transform color characteristics of tile image to match target blocks
Rotate tile image into directions with minimum RMSE
Embed relevant information
Mosaic image
Extract the previously-embedded information
Recover secret image

Fig: 1: Diagram of proposed work

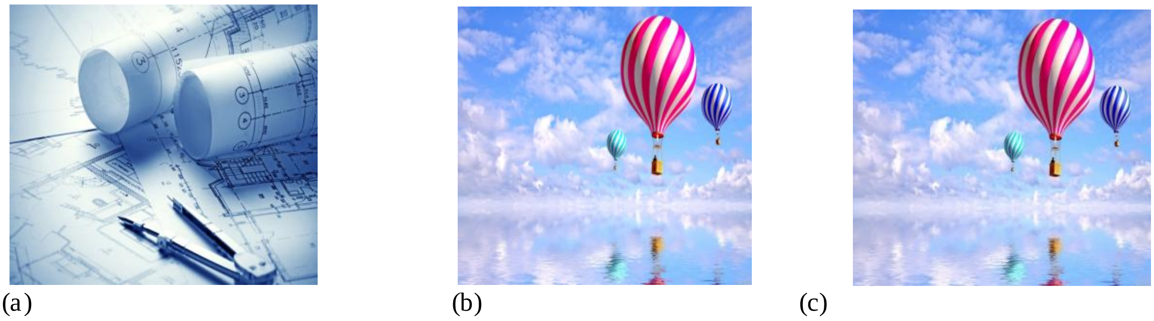
(a) (b) (c)

Fig: 2. The result of proposed method. (a) Secret image, (b) Target Image, (c) Secret fragment visible mosaic image underflow can be neglected.

The embedding of the information into the mosaic image is very essential as further this embedded information is used for the lossless recovery of the secret image. For the image recovery of the tile image from the target block must contain the index of block, optimal rotation angle of tile image, truncated mean of tile image and block, standard deviation. Using all this parameters mosaic tile image can be recovered into original secret image[11-14]. So using this technique the secret image convert into the mosaic tile image and also recover into the original secret image without any loss. In this way the security of confidential image is maintained.

Fig 2 shows result yielded by proposed method, the secret fragment mosaic image is obtained using this method which looks similar to that of target image.

III. PROCEDURE OF PROPOSED WORK

The whole process of the proposed work divided into some stages which are as follows

Stage 1: Creation of Mosaic Image

In this stage a secret image and target image are taken (as shown in fig. 2). If the size of target image is differ from secret image then change it,s size similar to secret image. The second step is to divide the secret image into tile image and target image into target block, then compute the mean and standard deviation of each tile image as well as target block. According to the computed mean and standard deviation all the values are arrange in a sequence, for both tile image and target block into 1-to-1 manner. By using this mosaic tile image is formed by fitting the tile image into the corresponding target block according to the sequence.

Stage 2: Color conversion between the tile Images and target blocks

Create a counting table with 256 entries each with an index corresponding to a residual value, and assign an initial value of zero to each entry. Here transformation of color is carried out. In the proposed work the RGB color model is used. While converting each pixel color characteristics, the problem of underflow and overflow is managed. They are not allowed to exceed above 255 bits to control overflow and not allow below 0 bit.

Stage 3: Rotating tile image

The RMSE value of transformed tile image is calculated at each directions $\theta = 0^o, 90^o, 180^o, 270^o$ while fitting into a target block. The tile image gets set at the direction which has smallest RMSE value.

Stage 4: Embedding key for recovery of secret image

A key is embedded in a mosaic image using data hiding technique [6-8]. A key plays a vital role in the lossless recovery of the secret image. This gives the security consideration to the proposed work. By using same key secret image will be recover. The output yielded by this method is shown in fig.2

IV. CONCULSION

The method is used to secure the secret image. The mosaic image is use as camouflage of secret image. A secret fragment mosaic image is obtained from proposed method which looks similar in shape and size as that of selected target image. By using proper pixel color transformation and skillful scheme the problem of underflow and overflow can be controlled. The database for target image need not to be maintained, this will come under one of the advantages of proposed method.

REFERENCES

[1]. R. J. Anderson, F.A.P Petitcolas, ”On the limits of steganography” *IEEE Journal on Selected Areas in Comm.*, vol. 16(4), pp 474-481,1998.

[2]. I. Avciabs, N. Memon and B.Sankur, ”Steganalysis using image quality metrics,” *IEEE Trans. Image Processing,* vol. 12, no.2, pp. 221-229, 2003.

[3]. A. D. Ker, ”Steganalysis of LSB matching in grayscale images,” *IEEE signal processing letters,* vol. 12, no.6, pp. 441-444, 2005.

[4]. Neil F. Johson, Sushil Jajodia,”Exploring steganography: Seeing the unseen,” *computer*,vol. 31, no.2, pp. 26-34, 2003.

[5]. N. Provos, P. Honeyman,”Hide and seek: an introduction to steganography,”*IEEE security and privacy*, vol. 1, no. 3 pp. 32-44, 2003.

[6]. W. Bender, D Gruhl, n. Morimoto, a. Lu, ”Techniques of data hiding,” *IBM system journal*. vol. 35, no.3.4,pp. 313-336, 1996.

[7]. C.K. Chan, L. M. Cheng, ”Hiding data in image by simple LSB substitution,” *Pattern Recognit.*,vol. 37, pp.469-474, 2004.

[8]. Z. Ni, Y. Q. Shi, N. Ansari, W.su, “Reversible data hiding,” *IEEE Trans. Ciruits System Vedio Technology*, vol. 16, no.3, pp. 354-362, 2006.

[9]. C.C. Chang, C.C. lin, C.S. Tseng, W.L. Tai, ”Reversible hiding in DCT-based Compressed images, *Inf.sci.*, vol. 117, no.13, pp. 2768-2786, 2007.

[10]. E. Reinhard, M. Ashikhmin, B. Gooch, P.Shirley,”Color transfer between images,” *IEEE Computer Graph Appl.*, vol. 21, no.5, pp. 34-41, 2001.

[11]. I.J. Lai, W.H. Tsai,”Secret-fragment mosaic image- A new computer art and it’s application,” *IEEE Trans. Inf. Forens. Secur.*, vol. 6, no.3, pp. 936-945, 2011.

[12]. Simone Bianco, Francesca gasparini, Alessandro Russo,Raimondo Schettini,”A

new method for RGB to XYZ transformation based on pattern search optimization, " *IEEE Trans. on consumer electronics*, vol. 53, no.3, pp. 1020-1028, 2007.

[13]. Anitha Devi M. D, K. B. ShivKumar, "Protection of confidential color image information based on reversible data hiding technique," *CoCoNet*, pg. 742-747.2015. recognition in RGB color image," *ICPR- 2000*, vol. 3, pp. 584-587, 2000.

[14]. Paschalakis, P. Lee,"Combined geometric transformation and illumination invariant object