AN AUTHENTICATION SYSTEM FOR AN IMAGE: SECRET MOSAIC IMAGING AND LSB SUBSTITUTION

Deepak.A.B.C[1], P.S.Shilpashree[2]

[1]*M.Tech Student, Siddaganga Institute of Technology, Tumakuru, Karnataka, (India)*

[2]*Assistant Professor, Dept. of Electronics and Communication, Siddaganga Institute of Technology, Tumakuru, Karnataka, (India)*

ABSTRACT

Authentication of Color Images in present world is the most challenging task for Image Processing engineers and cryptographers because of its redundancy and spatial correlation. In this paper we have implemented an approach for image authentication in disguise of another image using color transformation technique and mosaicking image. We have used simple LSB substitution for hiding data required for image recovery in the receiver side. A good experimental result is shown for the feasibility of the methodology.

Keywords: Color Transformation, Mosaic Image, Data Hiding, LSB Substitution.

I. INTRODUCTION

Image has a natural property of spatial correlation and high data redundancy. By using these properties of the image researchers worked on authenticating the image. Image Encryption algorithms make use of these natural properties of the image to authenticate the image. The authenticated image may arouse an attacker's attention to decrypt the image because of its high redundancy. Another method of authenticating the color image is data hiding where we use two types of entities to transmit the image secretly. One is an image which we required to transmit secretly called as secret image and another one is an image which is used to hide the secret image called as a carrier image. These encryption and decryption process is controlled by key at transmitter and receiver end. Without the key we cannot decrypt the image at receiver end.

Several data hiding techniques have been proposed in the literature includes LSB Substitution [1], histogram Shifting [2], difference expansion [3], prediction error expansion [4].

In this paper we have implemented an authentication system for an image which transforms a secret image into meaningful mosaic image which looks like a preselected carrier image. We are using a simple LSB Substitution to hide the data required for recovering secret image at receiver end. The method implemented in this paper is inspired by Lai and Tsai [5] and Lee and Tsai [6]. The mosaic image is the result of rearrangement of the fragments of a secret image in disguise of another image called the carrier image preselected from a preselected database.

The implementation method in this paper yields the result shown in Fig. 1. Specifically, a secret image and a carrier image first divided into rectangular fragments and then the secret image blocks is fit into carrier image

blocks according to a similarity criterion based on color variations. Next, the color characteristic of each secret image block is transformed to be that of the corresponding carrier block in the carrier image, resulting in a mosaic image which looks like the carrier image. The relevant information required for recovering the original image id hide into the created mosaic image. The image encryption algorithms yield a mosaic image which is meaningless. The data hiding method must be hide data in highly compressed manner into a disguising mosaic image without compression.

(a) (b) (c)

Fig.1.1: Result Yielded by the Implementation. (A) Secret Image. (B) Carrier Image. (C) Secret-Fragment-Visible Mosaic Image Created From (A) And (B) by The Implementation.

In the remainder of this paper, the idea of the implementation is described in Sections 2. In Section 3 we have discussed about the creation of secret fragment visible mosaic image. In Section4, experimental results are presented to show the feasibility of the method, and in Section 5, the security considerations of the implementation and Section 6 is followed by conclusion and Section 7 is Scope for the future work.

II. METHODOLOGY

Taking merits of [5] [6] we have implemented a method for authentication of image. The block diagram of the implementation is shown in Fig. 2.

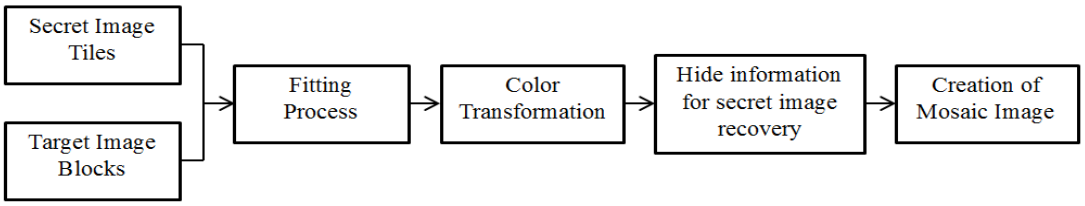

Fig. 2.1: Secret Fragment Mosaic Image Creation.

The implementation requires LSB substitution for data hiding discussed inChapter 2. The implementation includes two main phases as shown by the flow diagram of Figure. 3:1 and Figure. 3:2: 1) Mosaic image creation and 2) Secret image recovery.

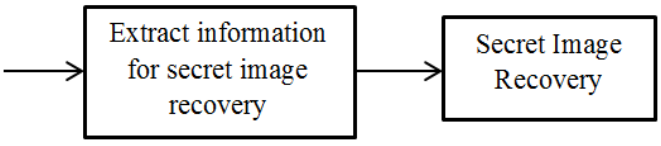

Fig. 2.2: Secret Image Recovery

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

1. Fitting the tile images of the secret image into the target blocks of a preselected target image;
2. Transforming the color characteristic of each color channel in tile image of the secret image to become that of the corresponding color channel of target block in the target image;
3. Embedding relevant information into the created mosaic image for futurerecovery of the secret image using simple LSB Substitution.

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

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

III. PROCESS OF CREATION OF MOSAIC IMAGE

3.2 Steps for Creating Mosaic Secret Fragment Visible Mosaic Image

1. Divide the secret S into n tile images and target image T into n target blocks.
2. Compute mean and standard deviation of each tile and block for three color channels according to following relations.

$$\mu_c = \frac{1}{n}\sum_{i=1}^{n} c_i, \qquad \mu_c' = \frac{1}{n}\sum_{i=1}^{n} c_i' \tag{1}$$

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

In which and denote the C-channel values of pixels Tile imagesand target blocks respectively, with $c = r, g,$ or b and C=R, G, or B.

3. Sort the tile image and target blocks according to standard deviation and 3 color channels, after that we get we get new tile images and target blocks and note down the indices values of the color pixels.
4. After we get the new tile images and target blocks and compute the average standard deviation of these tile images and target blocks.
5. Fit the tile images and target blocks according to average standard deviation and create mosaic image according to the indices values.
6. Perform the Color transformation according to the new tile images and target blocks according to the following equations.

New Color Values is find out by

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

It is observed that the new color mean and standard deviation values are equal to the Target blocks.
standard deviation quotient cannot be zero because the original pixel value cannot be recovered back.
The original values can be reconstructed by the following equation

$$c_i = \frac{1}{q_c}(c_i'' - \mu_c') + \mu_c \tag{4}$$

7. Embed the secret image recovery information into the Mosaic Image i.e., indices of location, mean of the target block and tile image and standard deviation using LSB substitution. .

3.2 Secret Image Recovery

1. At the receiving end extract the LSB bits.
2. Retrieve the Tile Images according to LSB bits Hidden at the transmitter end according to (4).

IV. EXPERIMENTAL RESULTS

We have conducted several experiments on several images of size 512 512 divided into 4 4. The Results of the implementation is shown in the following figures.

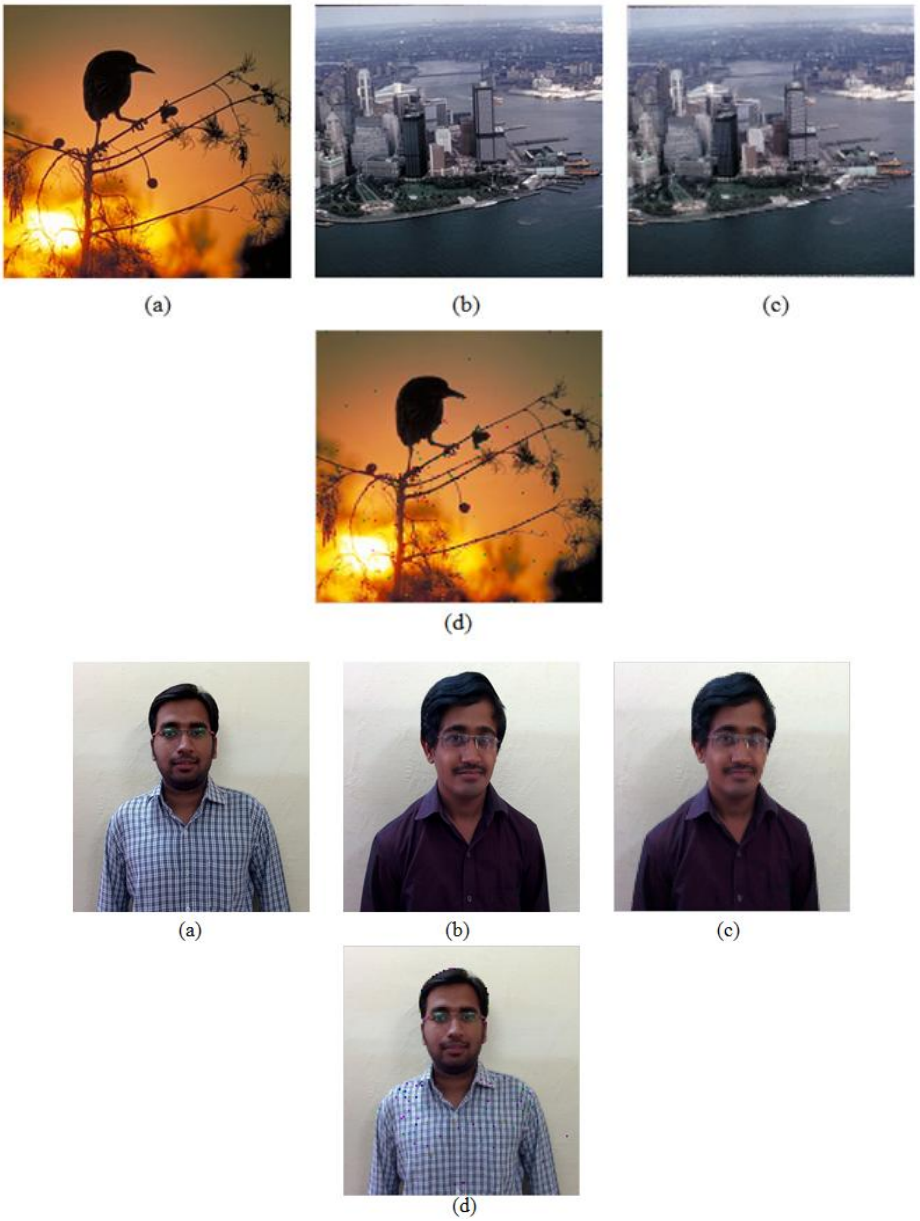

Fig. 4.1: (A) Secret Image, (B) Target Image, (C) Created Secret Fragment Visible Mosaic Image, (D) Recovered Secret Image from Mosaic Image

We have collected some medical image database for the secret image transmission as shown in the figure below. The medical image database may be secretly transmitted without distortion. The database is collected from a dermatologist having skin disease. The results are shown in the Figure 4.2.

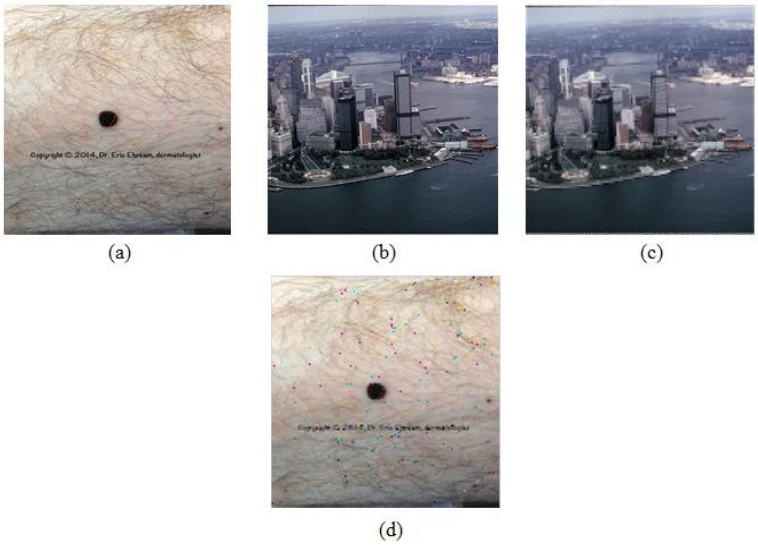

Fig. 4.2:(a) Pigmented lesion in Skin,(b) Target Image, (c) Mosaic Image,(d) Recovered Image (Courtesy: Dr. Eric Ehrsam (Dermatologist))

V. SECURITY ISSUES

In order to increase the security of the implementation of the authentication system, the embedded information for later recovery is encrypted. Only the receiver who has the decryption algorithm can recover the secret image. However, an eavesdropper who does not have the key may still try all possible permutations of the tile images in the mosaic image to get the secret image back. Fortunately, the number of all possible permutations here is $n!$, and so the probability for him/her to correctly guess the permutation is $p = 1/n!$ which is very small in value. For example, for the typical case in which divide a secret image of size 512×512 into tile images with block size 4×4, the value n is $(512 \times 512)/(4 \times 4) = 16,384$. So the probability to guess the permutation correctly is $1/n! = 1/16,384!$ So breaking the system by thisway of guessing is computationally infeasible.

Furthermore, even if one happens to guess the permutation correctly, such as the correctly guessed permutations, he/she still does not know the correct parameters for recovering the original color appearance of the secret image because such parameter information for color recovery is encrypted as a bit stream. Even so, it still should be assumed, in the extreme case, that he/she will observe the content of the mosaic image with a correct permutation, and try to figure useful information out of it. For example, an attacker might analyze the spatial continuity of the mosaic image in order to estimate a rough version of the secret image.

VI. CONCLUSION

The feasible and robust algorithm for image authentication is implemented andsecurity considerations of the algorithms are discussed. The authentication methods are based on creation of secret fragment visible mosaic image data and LSBsubstitution data hiding. The quality metrics of extracted secret image from thesecret fragment mosaic image is shown. The parameters considered for data hidingare indices of the secret blocks,

mean and standard deviation quotient discussedin Chapter 3. The method can create meaningful mosaic images but also cantransform a secret image into a mosaic one with the same data size for use as acamouflage of the secret image. The original secret images can be recovered nearlylosslessly from the created mosaic images. The $l\alpha\beta$ color space is used for colortransformation of secret image and cover image. It ensures to embed large imagedata into secret fragment visible mosaic image.

VII. SCOPE FOR FUTURE WORK

The algorithm for image authentication is implemented in MATLAB 2012a. For better speed and still more security reasons the algorithmcan be implemented in Open CV. In the implementation the key is not embedded into the secret fragment visible mosaic image. If this could be done the security consideration of the algorithms still improves. Without key recover the secretimage from secret fragment visible mosaic image. The secret fragment mosaic image is meaningless file without key at that instance. In the methodology the secret image is not correctly recovered from secret fragment visible mosaic image. If it is recovered correctly it shows the feasibility of the implementation.

REFERENCES

[1] C. K. Chan and L. M. Cheng, “Hiding data in images by simple LSB substitution,” Pattern Recognition..,vol. 37, pp. 469474, Mar. 2004.

[2] Z. Ni, Y. Q. Shi, N. Ansari, and W. Su, “Reversible data hiding,” IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354362, Mar. 2006.

[3] J. Tian, “Reversible data embedding using a difference expansion,” IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890896, Aug. 2003.

[4] V. Sachnev, H. J. Kim, J. Nam, S. Suresh, and Y.-Q. Shi, “Reversible water- marking algorithm using sorting and prediction,” IEEE Trans. Circuits Syst. Video Technol., vol. 19, no. 7, pp. 989-999, Jul. 2009.

[5] 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.

[6] Ya-Lin Lee and Wen-Hsiang Tsai, “A New Secure Image Transmission Technique via Secret-Fragment-Visible Mosaic Images by Nearly Reversible Color Transformations,” IEEE Trans. Circuits and systems for video technology., volume:24 , Issue: 4 ,pp. 695 – 703, April 2014.