Journal of Basic and Applied Engineering Research
Print ISSN: 2350-0077; Online ISSN: 2350-0255; Volume 2, Number 2; January-March, 2015, pp. 144-148
© Krishi Sanskriti Publications
http://www.krishisanskriti.org/jbaer.html

Image Steganography Based On Reversible Color Transformation

Mr. Tushar C. Jiwane[1] and Mr. V.D. Alagdeve[2]

[1]M.Tech. Student Department of Electronics Engineering Yashwantraorao Chavan College of Engineering Nagpur, India
[2]Dept. of Electronics Engineering Yashwantraorao Chavan College of Engineering Nagpur, India
E-mail: [1]tusharcjiwane@gmail.com, [2]vilas_a23@rediffmail.com

Abstract—*this paper presents an image hiding method using secret fragment visible mosaic image based on reversible color transformation. In this, the secret image which to be hidden is divided into blocks or tiles and they are shuffled or reordered with respect to their matched target blocks which was selected on basis of image similarity criteria. In the existing method, an image similarity measure, h-feature is defined using the color distribution in the pixels. The h-feature is used to select the most appropriate secret image blocks for the target image blocks which take more consideration the relative intensity difference between compared image blocks which helps creating a mosaic image with minimum RMSE.*

Next, the color characteristic of each tile images is transformed with respect to the corresponding preselected target image blocks, which results into a mosaic image which looks like a preselected target image. Relevant schemes also suggested embedding relevant recovery information encrypted with a secret key into the mosaic image .By using this recovery information, the original secret image can be recovered nearly lossless with no serious distortion from created mosaic image.

Index Terms*: Mosaic Image, h-feature, RMSE*

1. INTRODUCTION

One of the most important factors of information technology and communication has been the security of information since the rise of the Internet. Cryptography was created as a technique for securing the secrecy of communication and many different methods have been developed to encrypt and decrypt data in order to keep the message secret. Unfortunately, sometimes it is not enough to keep the contents of a message secret, it may also be necessary to keep the existence of the message secret. The technique used to implement this, is called steganography.

This is accomplished through hiding information in other information, thus hiding the existence of the communicated information. Steganography is differs from cryptography in the sense that where cryptography focuses on keeping the contents of a message secret, steganography focuses on keeping the existence of a message secret . Steganography and cryptography are both ways to protect information from unwanted parties but neither technology alone is perfect and can be compromised. If the presence of hidden information is revealed or even suspected, the purpose of steganography is partly defeated.

In this paper, a new method based on secret fragment visible mosaic imaging is proposed which successfully hide the existence of a secret image as a disguise of cover image. Thus, image steganography has been achieved by changing the visual appearance of a secret image with respect to the target (cover) image. Mosaic image is the resultant output image of overlapping of two images in which one entire image is secretly embedded into another image without affecting visual appearance of cover image and in thus resulting into hiding the existence of secret image.

The resultant mosaic image, which looks like a preselected target image, is yielded by dividing secret image into rectangular fragments and fitting or randomly arranging those fragments into their respected preselected similar target blocks of target image and lastly transforming their color characteristics with respect to matching target blocks.

This paper is originally inspired by a method proposed by Lee and Tsai[1] in which a new secure image transmission method has been proposed which create a meaningful mosaic images by transforming a secret image into a mosaic one with the same data size for use as a camouflage of the target image. The proposed method not only creates a meaningful mosaic image in contrast to the image encryption method which create meaningless noise image which in turn may arouse an attacker's attention during transmission due to its randomness in form.

This proposed method can transform a secret image into a disguising mosaic image without any prior compression, which enables it to recover original secret image nearly lossless. While a data hiding method hided a highly compressed version of a secret image into a cover image, which makes it impossible to recover original secret image without any serious distortion or loss. In previous work where a new type of computer art image, called secret-fragment-visible mosaic image, was proposed by Lai and Tsai[2] in which resultant mosaic image is the rearrangement of the fragments of a secret image in disguise of another most similar image called the target image preselected from a database. But weakness of Lai and Tsai [2] is the requirement of a large image database so that user can select most similar target (cover) image for their secret image so, the generated mosaic image can be sufficiently similar to the selected target image. Using their method, the user is not allowed to select freely his/her favorite image for use as the target image. It is therefore desired, in this study to remove this weakness of requirement of large images database while keeping its merit, that is, it is aimed to design a new method that can transform a secret image into a secret fragment- visible mosaic image of the same size that has the visual appearance of any freely selected target image without the need of a database.

Specifically, after a target image is selected arbitrarily, the given secret image is first divided into rectangular fragments called tile images, which then are fit into similar blocks in the target image, called target blocks, according to a similarity criterion based on color variations. Next, the color characteristic of each tile image is transformed to be that of the corresponding target block in the target image, resulting in a mosaic image which looks like the target image. Relevant method also proposed to conduct nearly lossless recovery of an original secret image from a mosaic image .To further increase the robustness of the scheme, recovery process is controlled by a secret key, only the receiver who has a right key can decode the information and extract the secret image. This sort of provision prevents eavesdropper to extract secret image from such type of mosaic image.

In the remainder of the paper, the idea of the proposed method along with the detailed algorithm for creating mosaic image has been discussed. The feasibility of proposed technique and security issue, followed by conclusion are also being discussed.

2. BASIC IDEAS OF THE PROPOSED METHOD

The proposed method has been divided into two phases. The first phase includes creation of mosaic image and second phase includes recovering of original secret image from resultant mosaic image.

Phase I involves following stages to create mosaic image.

1. Dividing secret and target image into fragments of identical sizes.
2. Rearranging or fitting fragments of secret image with respect to their matching target blocks (fragments)
3. Performing color transformation on each tile image (fragments of secret image) with respect to their corresponding target blocks.
4. Rotating tile images into a direction with minimum RMSE corresponding to their matched target blocks.
5. Embedding relevant information for later recovery into resultant mosaic image.

Phase 2 includes

1. Extracting relevant recovery information from output mosaic image.
2. Recovering original secret image from mosaic image using extracted information.

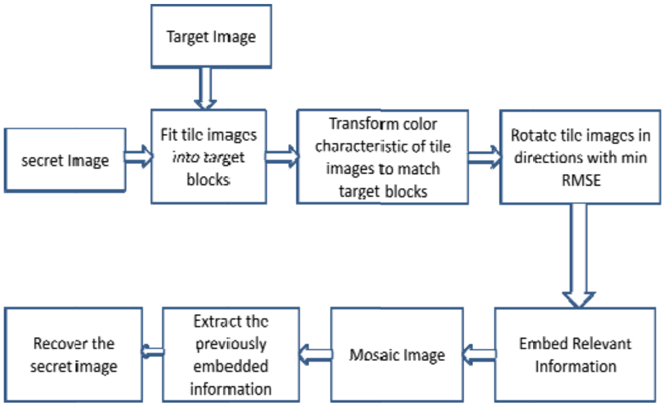
Target Image
secret Image
Fit tile images into target blocks
Transform color characteristic of tile images to match target blocks
Rotate tile images in directions with min RMSE
Embed Relevant Information
Mosaic Image
Extract the previously embedded information
Recover the secret image

Fig. 1: Flow diagram of the proposed method.

3. PROBLEM ENCOUNTERED IN MOSAIC IMAGE CREATION

A. Problem Of Fitting Tile Images Into Target Blocks

After dividing secret image into tile image, we have to find most similar target blocks from target image for each secret blocks. As both target images and secret image are identical in size ,so complete overlapping of secret image over target image can be possible, we will have to map each secret blocks into target blocks in a 1 to 1 manner.

For selecting appropriate target blocks for each tile images (secret blocks), we use h-feature based 1D color scale value, which taken into more consideration, the relative intensity difference between the compared image blocks as a similarity measure to find similarity in between target and secret blocks. First, we sort all tile images as well as target blocks corresponding to their h-feature values into an arrays and then map each tile image into sorted array to respective target blocks in sorted arrays. In this manner, we fit first tiles in sorted sequence to the first target blocks in sorted form and complete 1: 1 mapping. After deciding similar target blocks,

We repositioned or rearranged those tiles with respect to position of their corresponding target matching blocks.

B. Color Transformation Between Blocks

After rearranging or sorting tile images, the next step is to transform color characteristics of each tile images with respect to corresponding matched target blocks to make them look alike. As color characteristics of target blocks and secret blocks are different from each other, how to change their color distribution to make them look alike is the main problem. Reinhard et al.[3] proposed a reversible color transformation scheme, which borrows color characteristic of one image to another image in the lαβ color space. This method is a solution to our problems, except instead of using lαβ color space, we use generalized RGB color plane which reduce the complexity of method and also minimize volume of required information for later recovery.

These color transformation scheme simply matches the color characteristics of a secret image to their arbitrarily selected target image. This makes secret image to look alike target image, so after fitting secret image on to their cover image, resulted into meaningful mosaic image. Because of its changed color properties, physical existence of secret image has been concealed and also does not severely affect the visual appearance of cover image. This method enables the user to freely select cover images of his own choice .This method is completely reversible which enables it to recover secret image from mosaic image with no serious data loss. So, the recovered or extracted image is nearly identical to the original secret image. Because of these advantages, such type of image hiding technique is very much useful in covert communication or secure keeping of images.

The color transformation schemes changes the color characteristics of each tile images to their preselected matched target blocks as follows.

$$Ci'' = q_c (Ci - \mu_c) + \mu_c';$$

Where,

q_c= standard deviation quotient which is ratio of std deviation of a target block to corresponding std deviation of a secret block.

& μ_c, μ_c'= mean of a secret block and target block respectively, where c denotes C-channel values of pixels in red, green or blue plane respectively.

Ci is a pixel value of a untransformed secret blocks and

Ci" is a resultant pixel value of a transformed secret blocks in red, green or blue plane respectively.

To compute the original pixel values C(r,g,b) from Ci"(r,g,b), we use the inverse of a previous formulae ,

$$Ci = (1/q_{c)} (Ci'' - \mu_c') + \mu_c ;$$

To evaluate the original secret blocks from transformed one, we will require std deviation quotient(qc) of each color block of mosaic image as well as mean (μc) of an each untransformed tile images .This type of information has to be embedded along with the created mosaic image for successfully recovering of original secret image from mosaic image.

C. Handling Overflows and Underflows in Color Transformation

After the color transformation process is conducted, which transform each and every pixel value of an tile image into new ones with respect to their selected target blocks by above method, there are some pixel values in transformed domain which resulted into overflows or underflows .Underflows means the transformed pixel values less than 0, and overflows means the transformed pixel values more than 255.

To deal with this problem, we record residual value in the untransformed color space, by using following formulae,

$$Cs = (1/q_{c)} (255 - \mu_c') + \mu_c ;$$

$$C_L = (1/q_{c)} (0 - \mu_c') + \mu_C ;$$

Firstly compute the smallest possible color value in an untransformed domain which results in overflows by first eq. for each tile image and similarly, calculate the largest possible color value in an untransformed domain which results into underflows by second one for each tile image.

This above formulae gives the range of a color values in an untransformed domain which yielded into overflows and underflows after the color transformation. The pixel values greater than Cs in untransformed secret blocks (or tile image) i.e (Ci>Cs) resulted into overflows while values less than CL i.e. (Ci<CL) resulted into overflows after the color transformation.

After finding a values in an untransformed tile images that resulted into overflows or underflows, we record its residuals as | Ci-Cs | and | CL-Ci| for each untransformed value Ci which results into overflows and underflows respectively.

These residuals are required to get back the original pixel value from transformed tiles for recovering original secret image.

D. Rotating Tile Images In A Direction Of A Minimum MSE

After the color characteristics of a tile images is transformed, to further improves the color similarity in between target blocks and secret blocks, we rotate each color transformed secret blocks into one of the four directions 0o, 90o, 180o or 270o, which yielded a rotated version of transformed secret image with the minimum root mean square error value (RMSE) with respect to matched target blocks.

E. Embedding Recovery Information for Secret Image Extraction

In order to recover secret image from resultant mosaic image, we will require parameters of original secret image which involves std deviation and mean of each tile images, rotated direction of a tile images, residues and indexes of tile images. This type of information is needed to successfully extract original secret image with no information loss.

To embed this information along with the mosaic image, we use a very fast reversible digital watermarking technique proposed by Coltus and Chassery[4] which applies it to the least significant bit of pixels in created mosaic image to conduct data embedding. Unlike the classical LSB replacement methods [5], which substitute LSBs with message bits directly, the reversible contrast mapping method [4] applies simple integer transformations to pairs of pixel values.

This proposed scheme provides a high data embedding bit rate at a very low mathematical complexity, also providing robustness against cropping.

The information required to recover a original tile image which is mapped to a target block includes: 1) the index of Tile image; 2) the optimal rotation angle of Tile image; 3) the means of Tile image and the standard deviation quotients, of all color channels; and 4) the overflow/underflow residuals.

To further enhance the security of proposed method, the embedded information for later recovery has to be encrypted with a secret key. So, only the authenticated user or receiver has an access to the secret image by using this embedded information.

4. SECRET IMAGE RECOVERY

Step1:- Extracting Secret Image Recovery Information

In this phase, image information for secret image recovery has been extracted by using a secret key .This extracted parameter is then later on used for reversible color transformation.

Step2:- Extracting Secret Image

By using extracted information which involves tile image parameter, we can recover original secret image with no serious data loss from mosaic image by the inverse of the color transformation given in previous section.

5. EXPERIMENTAL OUTCOME ANALYSIS

It can be observed that the created mosaic image preserves more details of the target image when the tile image is of smaller size. Even the blockiness effect is decreased up to some extend and blurriness of a mosaic images can be reduced by using smaller tile images.

But using of a smaller tile image say of 8 * 8 size increases computational complexity as well as volume of a data used for later recovery. Therefore, it is feasible to use moderate sizes of tile image (16*16) to create mosaic image which resulted in somewhat lower mathematical complexity as well as volume of recovery data.

It can be seen that each output mosaic image has a blocky appearance which comes from a mosaic effect since mosaic image is yielded by changing the color characteristics of the fragments of the secret image and rearranging the resultant fragments. It can be seen from the results that the output mosaic image look similar to the pre selected target image even though the secret image is quite different from the target image in appearance.

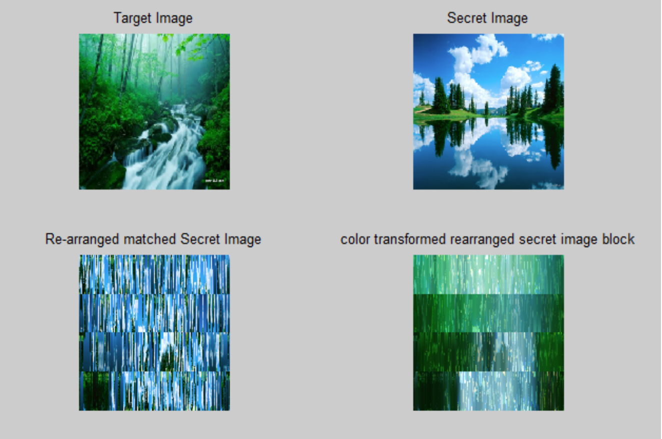
Target Image
Secret Image
Re-arranged matched Secret Image
color transformed rearranged secret image block

Fig. 2: Color transformed tile images w.r.to target blocks

Since mosaic image is created by dividing secret image into tile images and changing their color characteristic to be those corresponding target blocks, the global color characteristics of a transformed tile image and its corresponding target blocks are same, but their color distribution are quite different from each other.

Hence, although mosaic image which looks like a target image, the detail of each fragment of mosaic image have low similarity to their corresponding target blocks.

The limitation of this proposed method is that size of a target image must be same to that of a secret image. Suppose, if we have a very large secret image but only have a smaller target images for selection, then selected target image should be enlarged to match size of a secret image before mosaic image formation which then resulted into a blurred mosaic image.

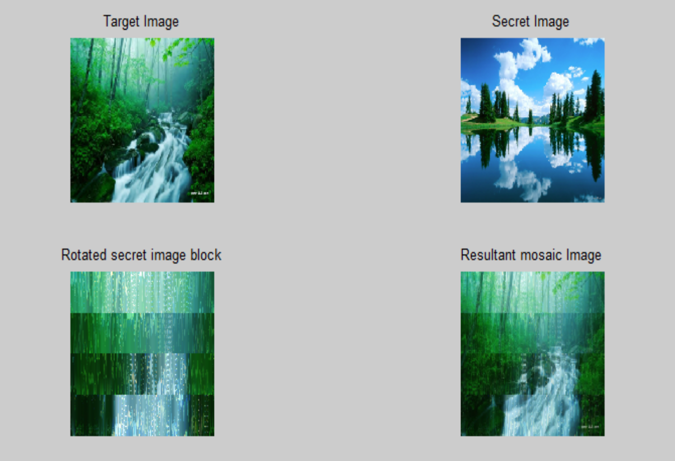

Fig. 3: Resultant mosaic image

6. SECURITY CONSIDERATION

As earlier mentioned, to enhance the security of a proposed method, we embed the recovery information encrypted with a secret key, so that only authorized user with a right key can access this information and used it for recovery of a secret image.

However, if an eavesdropper who don't have a key, try to decode secret image with all possible permutations of tile images in mosaic image. The number of all possible permutations will be n! , where n are total no of tile images used to form mosaic image. So, the probability to guess correct permutations of tile images is1/n! , which is very small, if no of tile images is large. In short, larger numbers of tile images should be used to increase the security of proposed method.

Even though if permutations of all tile images guessed right, unauthorized user does not have the correct parameters for recovering the original color appearance of a secret image since such parameters has been securely encrypted with a secret key.

So, this proposed method provides robust security to the secret image where an unauthorized user can't get the access of hidden information.

7. CONCLUSIONS

A new novel technique of image stagenography based on creation of a meaningful mosaic image, which looks like a freely selected target image, hiding an existence of a secret image beneath of a target image has been proposed. By the use of proper reversible color transformation schemes, secret fragment mosaic image can be created with no need of image database. Also, the original secret image can be recovered nearly lossless from mosaic image. Good experimental result has proved the feasibility of the proposed method.

REFERENCES

[1] Ya-Lin Lee, and Wen-Hsiang Tsai "A New Secure Image Transmission Technique via Secret-Fragment-Visible Mosaic Images by Nearly Reversible Color Transformation" IEEE transactions on circuits and systems for video technology, vol. 24, no. 4, april2014

[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] E. Reinhard, M. Ashikhmin, B. Gooch, and P. Shirley, "Color transfer between images," IEEE Computer. Graphic Application, vol. 21, no. 5, pp. 34–41, Sep.–Oct. 2001.

[4] 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.

[5] C. K. Chan and L. M. Cheng, "Hiding data in images by simple LSB substitution," Pattern Recognition.., vol. 37, pp. 469–474, Mar. 2004.

[6] D. Pomeranz, M. Shemesh, and O. Ben-Shahar, "A fully automated greedy square jigsaw puzzle solver," in Proc. IEEE CVPR, 2011,pp. 9–16