ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 4, Issue 1, pp: (184-188), Month: January - March 2016, Available at: www.researchpublish.com

Secure Mosaic Image Transmission Technique

Haritha G[1], Smitha C Thomas[2]

M.G University, Mount Zion College of Engineering, Pathanamthitta, India

Abstract: **A new impregnable image transmission technique is proposed here, which transforms automatically a huge-size of secret image into the secret-fragment-visible mosaic image of the same size. The mosaic image is looks similar to an arbitrarily selected target image. It can be obtained by fragmenting the secret image and transforming their color characteristics corresponding to the blocks of the target image. Here the dexterous techniques are designed to conduct the color transformation process then the secret image can be recover without any loss. The converted Pixels' color values having overflows/ underflows can be handled by recording the color differences in the transformed color spaces is also proposed. The mosaic image is embedded by the information required to recover the secret image using a lossless data hiding scheme along with a key.**

Keywords: **Color transformation, data hiding, image encryption, mosaic image, secure image transmission.**

I. INTRODUCTION

Currently, images from the wide variety of sources are frequently utilized and can transmitted through the internet for multiple applications, such as confidential enterprise archives, online personal photograph albums, document storage system, military image database, medical imaging systems, confidential enterprise archives etc.

It may include private or confidential information, so that it could be protected from leakages at the time of transmissions. Now a days many methods are here for the secure image transmission, the one is image encryption and the other is the data hiding technique. The mosaic image creation is the latest technology which providing the image transmission as the most secure and efficient way. Multiple level of security will be ensure here at the entire process.

II. EXISTING SYSTEM

A. Image Encryption Method

B. Data Hiding Method

Image Encryption Method:

The existing techniques are image encryption and data hiding methods. An image having the natural property will be used in the image encryption technique. It consists of high redundancy and also very strong spatial correlation, to get an encrypted image on the basis of Shannon's confusion and diffusion properties. After the encrypted image it will be a noise image, so nobody can obtain the secret image unless they did not have the correct key. However the encrypted image is an absurd file, which cannot provide the additional information before the decryption process. It will leads to the attacker's attention during the transmission because of the randomness.

Data Hiding Method:

Data hiding is the another technique, which is an alternative to avoid the problems caused by the image encryption. It hides a secret image into a cover image or the target image. Here, nobody can recognize the existence of the secret image. LSB substitution, recursive histogram modification, histogram shifting, discrete cosine/wavelet transformations, difference expansion, prediction-error expansion etc is the existing data hiding methods. Thus, a main issue related with hiding data in images is that embedding a huge amount of message data into a single image. The secret image should be highly compressed in advance while we wants to hide a secret image into a target image having the same size.

Here, a new technique for secure image transmission is proposed , it transforms a secret image into a meaningful mosaic image having the same size and it will looks like the preselected cover image, a secret key is controlled by the transformation. The secret image can be losslessly recover by a person using this secret image. Lai and Tsai is proposed by this method, here a latest kind of computer art image developed named it as secret-fragment-visiole mosaic image. The mosaic image is the final result of rearrangement of the fragment of the secret image camouflage of another image called the target image preselected from a database.

III. PROPOSED SYSTEM

The proposed method consists of mainly two phases they are,

1. ***Mosaic Image Creation***
2. ***Secret Image Recovery***

In the primary step, The Mosaic image is yielded and it consists of the fragments of the secret image having the color transformations according to the similarity criterion based on the color variations. The first phase include four stages.

1. Mosaic image creation:

i) Secret image consists of the tile images should be fit into the preselected target image having the target blocks.

ii) The color characteristics of each tile image in the secret image could be transforming to become that of the corresponding target block in the target image.

iii) With respect to the corresponding target block, rotating each tile image into direction with the minimum RMSE value.

iv) For future recovery of the secret image, the relevant information should be embedding into the created mosaic image.

2. Secret image recovery:

i) Secret image can be recovered from the mosaic image by extracting the embedded information from the mosaic image.

ii) Using the extracted information, recovering the secret image.

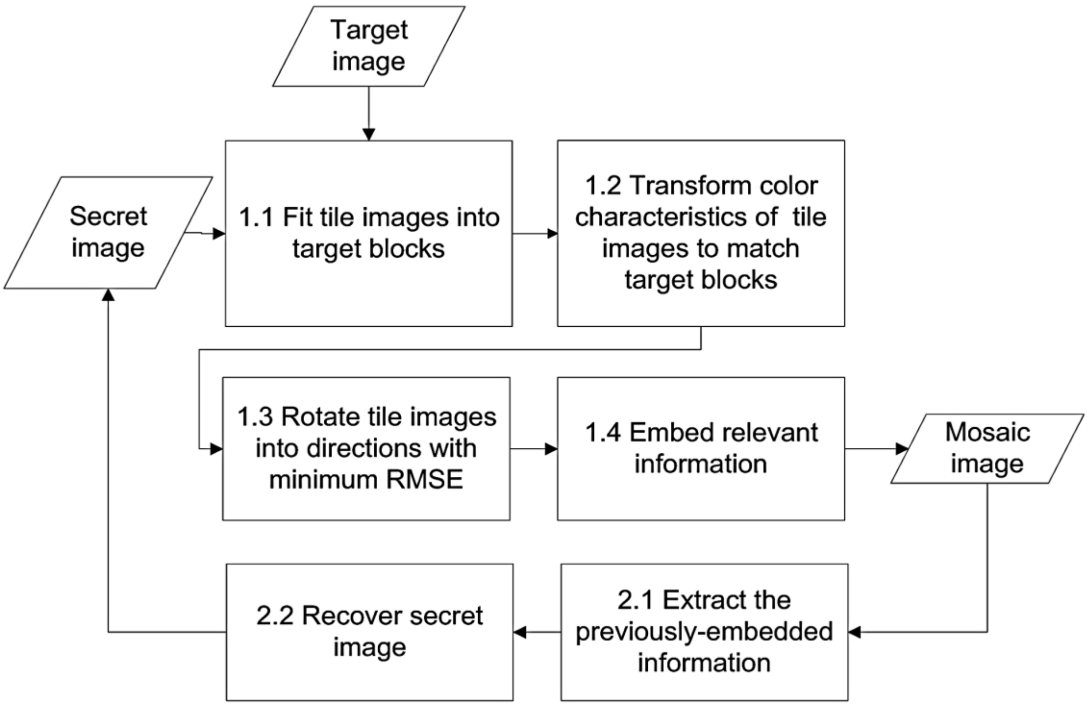

Fig. 1 Diagram of the mosaic method

IV. IDEAS OF MOSAIC IMAGE GENERATION

Main Modules are as follows,

1. IMAGE PRE-PROCESSING:

The requirements of the modules include,

- Extracting frames from cover image.
- Select a frame as cover image.
- Select a secret image.
- Tile image creation.

2. CREATE MOSAIC IMAGE:

The requirements of the module include:

- Calculate the mean and standard deviation
- Sorting tiles in the cover blocks
- Mapping tile images to cover blocks in 1to 1 manner
- Performing the color conversion between the tile images and cover block
- Rotating the tile images

Step 1: Fit Tile Image Into Target Image:

Mosaic image consists of the fragments of an input secret image and target image. Fragment the secret image *S* into n tile images {*T1, T2,…,Tn*} and target image *T* into n blocks {*B1, B2 …, Bn*} with each *Ti* or *Bi* of size *NT*.

Step 2: Transformations Color Characteristics Of Tile Image To Target Blocks:

Each tile image *T* in the given secret image has to fit into a target block *B* in a preselected target image. Since the color characteristics of *T* and *B* are different from each other. proposed a color transfer scheme used to converts the color characteristic of an image to be that of another in the l α β color space. The proposed system will use RGB color space instead of the l α β to reduce the volume of the required information for recovery of the original secret image.

Considered *T* and *B* be described as two pixel sets {p1, p2…, pn} and {p'1, p'2…, p'n} respectively. The color of each pi denoted by (ri, gi, bi) and that of each p'i by (r'i, g'i, b'i). Used standard deviations of *T* and *B*, respectively (1), in each of the three color channels R, G, and B by the following formulas:

$$\mu_c = \frac{1}{n}\sum_{i=1}^{n} c_i \qquad \mu'_c = \frac{1}{n}\sum_{i=1}^{n} c'_i$$

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

$$\sigma'_c = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(c'_i - \mu'_c)^2}$$

In which *ci* and *c'i*denote the C-channel values of pixels *pi* and *p'i*respectively, with c = r, g or b and C=R, G or B Next, we compute new color values (r''i, g''i, b''i) for each pi in *T* by

$$c''_i = q_c(c_i - \mu_c) + \mu'_c$$

Where qc= σ'c /σc is the standard deviation quotient and c = r, g or b. It can be check out easily that the new color mean and variance of the resulting tile image T are equal to those of B, respectively.The original color values are (ri, gi, bi) can be compute from the new ones (r''i, g''i, b''i) we can use the following formula that is the inverse of above equation.

$$c_i = \frac{1}{q_c}(c''_i - \mu'_c) + \mu_c$$

Furthermore, system has to embed sufficient information about the new tile image T into the created mosaic image for use in the later stage of recovering the original secret image. For this, we can use above equation to compute the original pixel value of pi.

Step 3: Rotating the Tile Image:

In transforming the color characteristic of a tile image T to be that of a corresponding target block B as described above. System use the standard deviation of the colors in the block as a measure to select the most similar B for each T. Sort all the tile images to form a sequence, Stile, and all the target blocks to form another, Starget, according to the standard deviations and average values of the three color channels. Then, fit the first in Stile into the first in Starget, fit second Stile into the second in Starget and so on. Additionally, after a target block B will be chosen to fit a tile image T and after the color characteristic of T is transformed, system conduct a further improvement to the color similarity in between the resulting tile image T and the target block B by rotating T into one of the four directions, such as 0o, 90o, 180o and 270o, which yields a rotated version of T with the minimum root mean square error (RMSE) value with respect to *B* among the four directions for final use to fit *T* into *B*.

3. COMPRESSION AND ENCRYPTION

Requirements of the module include: Bit stream creation, Compression and encryption of the bit streams.

4. EMBEDDING

Requirements of the module include: Embed the bit stream in to different frames, Choose an order ,Order is embed into key frame, Unlike the classical LSB replacement methods ,which substitute LSBs with message bits directly, the reversible contrast mapping method will applies as simple. Integer transformations to pairs of pixel values.

5. SECRET IMAGE RECOVERY

Requirements of the module includes: Extract the bit streams, decrypt the bit streams, decompression, recovering the secret image.

Step 1: Extract the bit stream from mosaic image F by performing reverse operation.

Step 2: Decrypt the bit stream by using secret key K.

Step 3: Recover the desired secret image S by rotating the tile images in a reverse direction.

Step 4: Use the extracted mean and standard deviation quotients to recover the original pixel values.

Step 5: The results of the final pixel values, resulting in a final tile image.

Step 6: Compose all the final tile images to form the desired secret image S as output.

Fig. 2. Result yielded by the proposed method(a) Secret image.(b) Target mage (c) Secret-fragment-visible mosaic image created from (a) and (b) by the proposed method.

Fig. 2 shows a result yielded by the mosaic method. Specifically, after arbitrarily selected a target image, then the given secret image fragmented into rectangular blocks called tile images. The tile images are then fit into similar blocks in the cover image or the target image, called target blocks, according to a similarity criterion based on color variations. After that , the color characteristic of each tile image is transformed into that of the corresponding target block in the target image, resulting in a mosaic image.

Mosaic image is looks same as that of the target image. Relevant schemes are also proposed to conduct the recovery of the original secret image from the resulting mosaic image having. Here this method introduces a new technique that is the meaningful mosaic image creation, in the case of image encryption method that creates the meaningless noise images only. In this mosaic method without compression, it transform a secret image into a disguising mosaic image. The highly compressed version of the secret image into a cover image and the cover image have the same data volume could be followed in the data hiding method.

IV. CONCLUSION

The new most secure image transmission method has been proposed, here in which it not only can create meaningful mosaic images but also can turn a secret image into a mosaic one having the same size of data for use as a camouflage of the secret image. For handling overflows and underflows in the converted values of the pixels' colors proper pixel color transformations as well as a skillful scheme are using here. The secret-fragment visible mosaic images with very high visual similarities to that of the arbitrarily-selected target images can be obtained without the requirement of a target image database. From the created mosaic images the original secret images also can be recovered nearly losslessly. Future studies may be directed to applying the proposed method to images of color models other than the RGB.

ACKNOWLEDGEMENT

I would like to extend my gratitude to the reference authors, as well as reviewer of my paper.

REFERENCES

[1] J. Fridrich, "Symmetric ciphers based on two-dimensional chaoticmaps," *Int. J. Bifurcat. Chaos*, vol. 8, 1-12- 1998.

[2] G. Chen,Y. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps," *Chaos Solit. Fract.*, vol. 21, 17-10-2004.

[3] L. H. Zhang, X. F. Liao, and X. B. Wang, "An image encryption approach based on chaotic maps," *Chaos Solit. Fract.*, vol. 24, 8-7- 2005.

[4] H. S. Kwok and W. K. S. Tang, "A fast image encryption system based on chaotic maps with finite precision representation," *Chaos Solit. Fract.*,vol. 32, 4-8- 2007.

[5] S. Behnia, A. Akhshani, H. Mahmodi, and A. Akhavan, "A novel algorithm for image encryption based on mixture of chaotic maps, *Chaos Solit. Fract.*, vol. 35, 10-9- 2008.

[6] D. Xiao, X.Liao, and P. Wei, "Analysis and improvement of a chaos based image encryption algorithm," *Chaos Solit. Fract.*, vol.50, 3-7-2009.

[7] V. Patidar, N. K. Pareek, G. Purohit, and K. K. Sud, "A robust and secure chaotic standard map based pseudorandom permutation substitution scheme for image encryption," *Opt. Commun*., vol. 284, 9-8-2011.

[8] Z. Ni, Y. Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," *IEEE* Trans. Circuits Syst. Video Technol., vol. 16, March 2006.