A NEW SECURE IMAGE TRANSMISSION TECHNIQUE BY MOSAIC IMAGE CREATION

Aansu Sara Abraham , Shanavaz.K.T , Nikhil G Kurup

Abstract— Authentication of color images in present world is one of the challenging task for image processing engineers and cryptographers due to its redundancy and spatial correlation. A new secure transmission method converts a given large volume secret image into mosaic picture of the same size. The mosaic image, which seems to be like the subjectively chosen target image is utilized as the disguise of the secret image, is obtained by separating the secret image into parts and changing their characteristics to be that of the target image. Skillful techniques are used for color transformation so that any outsider cannot identify the presence of the secret image. The visual quality of the mosaic image is calculated using the quality metric Structural Similarity Index Measure (SSIM).

Keywords—color transformation, data hiding, image encryption, mosaic image, secure image transmission

---

Aansu Sara Abraham: M Tech Student Department of Electronics & Communication Engineering College of Engineering Kallooppara Pathanamthitta **,** Kerala
aansusaraabraham26@gmail.com
Shanavaz.K.T: Associate Professor Department of Electronics & Communication Engineering College of Engineering Kallooppara Pathanamthitta**,** Kerala
shanavazkt@yahoo.co.in
Nikhil G Kurup: Associate Professor Department of Electronics & Communication Engineering College of Engineering Kallooppara Pathanam-thitta**,** Kerala
nikhilgkurup@gmail.com

1. INTRODUCTION

In recent years with the development of internet and computer technology, multimedia data are used more and more widely, such as images, videos or audios. In order to provide secure some data's are need to be protected before transmission because it contains private and confidential data. For secure image transmission many methods have been proposed. Image encryption and data hiding are the two common approaches. Image encryption method makes use of natural property of the image like high redundancy and strong spatial correlation . Without correct key no one can obtain the secret image from the encrypted image since it is a noisy image. Before decryption the encrypted image cannot be able to provide any additional information due to its random nature. These may lead attention of the attackers during the transmission.

To avoid this problem, data hiding technique is used in which secret image is hidden using a cover image in which existence of the secret image cannot be identified. Histogram shifting, LSB substitution, difference expansion, discrete cosine/wavelet transformations, prediction-error expansion and recursive histogram modification are the techniques which are commonly used. In the proposed method a secret image and a target image are selected, in which both have same size. The two images are divided into parts: the secret image into tiles and the target image into blocks. According to the standard deviation of each block and tile, they are arranged in ascending order. Finally color transformation is done such that the mosaic image looks similar to that of target image. The visual quality is the characteristic of an image that measures the perceived

image degradation. Imaging systems may introduce some amounts of distortions in the signal. So the quality assessment is an important problem. The main goal of quality assessment is to supply quality metrics that can predict perceived image quality automatically. Many visual quality metrics are available which can be used to evaluate the quality of the images. Here Structural Similarity Index Measure (SSIM) is used to evaluate the visual quality of the mosaic image.

2. RELATED WORKS

Image encryption techniques make use of natural properties of image like high redundancy and strong spatial correlation. Shannon's confusion and diffusion properties [1]-[7] are also used to get an encrypted image. In [1], methods to adapt invertible two-dimensional chaotic maps on a square to create new symmetric block encryption schemes are used. In [2], a new scheme is introduced which employs the 3D cat maps to shuffle the positions of image pixels and uses another chaotic map to confuse the relationship between the cipher and plain image.. In [3], properties of confusion and diffusion are improved in terms of discrete exponential chaotic maps and designed a key for resistance to differential and static attack. In [4], Image encryption system based on fast chaos with stream cipher structure is proposed.

In [5] Symmetric key cryptography technique is used. In [6], the reasons of potential flaws in the original algorithm have been analyzed and corresponding enhancement measures are proposed. In [7], a robust chaos-based pseudorandom permutation-substitution scheme for image encryption is proposed.

Data hiding [8]-[18] hides a secret message into a cover image in such a way that no one can identify the presence of encrypted image. Data hiding method mainly utilize the techniques of LSB substitution [8], histogram shifting [9], difference expansion [10]-[11], prediction-error expansion [12]-[13], recursive histogram modification [14], and discrete cosine/wavelet transformations [15]-[18].

3. PROPOSED SYSTEM

The proposed method includes two main phases.

1)Mosaic image creation.

2)Image quality analysis.

A. Mosaic image creation

The mosaic image is yielded in the first phase, which consists of the fragments of an input secret image with color corrections done according to a similarity criterion based on color variations. The phase consists of five steps.

1) Compute the standard deviation of each tile image and target image.

2) Sort the tile images and block images according to the increasing order in standard deviation.

3) Fit tile images into target blocks.

4) Transform color characteristics of the tile image to match target blocks.

5) Each tile image is rotated into a direction with minimum RMSE with respect to target blocks.

The flow diagram for the first phase is shown in the Fig.1.

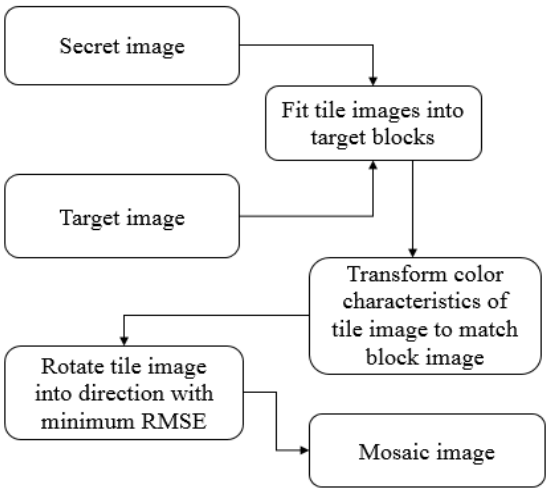


Fig. 1: Flow diagram of Mosaic image creation phase.

The mean and standard deviation of each tile image T_i and each block image B_j for i = 1 to n and j = 1 to n are given by

$$\mu_c = \frac{1}{n}\sum_{i=1}^{n} c_i \quad (1)$$

$$\mu_{c'} = \frac{1}{n}\sum_{i=1}^{n} c'_i \quad (2)$$

$$\sqrt{\frac{1}{n}\sum_{i=1}^{n}(c_i - \mu_c)^2} \quad (3)$$

$$\sqrt{\frac{1}{n}\sum_{i=1}^{n}(c_i' - \mu_c')^2} \quad (4)$$

in which c_i and c_i' denotes the C channel values of the pixels p_i and p_i'.

B. Image Quality Analysis

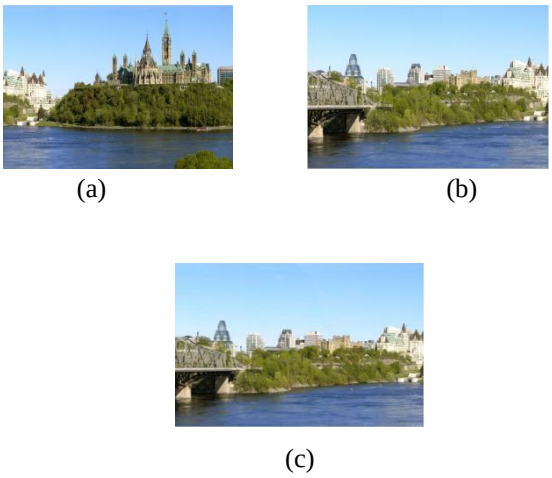
Many visual quality assessment metrics are available which can be used to evaluate the visual quality of the images. The visual quality metrics which are commonly used are Peak Signal to Noise Ratio(PSNR), Structural Similarity Index Measure (SSIM),Edge Similarity Score (ESS) and Luminance Similarity Score (LSS) . By quality evaluation it is possible to find how much security is provided by using these methods. Here more Structural Similarity Index Measure (SSIM) is used for image quality evaluation.

The Structural Similarity Index Measure (SSIM) [19] extracts separate scores from the image and combines them into the final score. First the visual influence is calculated locally and then luminance, contrast and structural scores are calculated globally. These separate scores are then combined with equal weight to form the SSIM score. The SSIM is a quality metric, a high metric score reflects a high quality, which gives a score in the range [0, 1].

4. EXPERIMENTAL RESULTS

The proposed method has been implemented on different secret and target images of size 1024 X 768 and 768 X 1024 pixels.

Fig. 2 shows the experimental result of mosaic image creation. The secret and target images selected have same size. Fig 2 (c) shows the mosaic image created from the above secret and target images. The quality is evaluated for the mosaic images with tile image size 8x8. While observing the SSIM score, the mosaic image created with tile image size 8x8 gives highest quality value.



(a) (b)

(c)

Fig.2: Experimental result of mosaic image creation. (a) secret image. (b) target image (c) mosaic image created with tile image size 8 x 8.

5. CONCLUSION

A new secure image transmission method has been proposed, which not only can create meaningful mosaic images but also can transform a secret image into a mosaic image with same data size which looks like the preselected target image. The visual quality of the mosaic image has been evaluated using the quality metric, Structural Similarity Index Measure (SSIM). In future this method can be extended to evaluate the quality of the mosaic image using content similarity.

References

[1]J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps," Int. J. Bifurcat. Chaos, vol. 8, no. 6, pp. 1259–1284, 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, no. 3, pp. 749–761, 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, no. 3, pp. 759–765, 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, no.4, pp, 1518-1529,2007

[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, no. 2, pp. 408–419, 2008.

[6]D. Xiao, X. Liao, and P. Wei, "Analysis and improvement of a chaosbased image encryption algorithm," Chaos Solit. Fract., vol. 40, no. 5, pp. 2191–2199, 2009.

[7]V. Patidar, N. K. Pareek, G. Purohit, and K. K. Sud, "A robust and secure chaotic standard map based pseudorandom permutationsubstitution scheme for image encryption," Opt. Commun., vol. 284, no. 19, pp. 4331–4339, 2011.

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

.

[9]Z. Ni, Y. Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354–362, Mar. 2006.

[10]J. Tian, "Reversible data embedding using a difference expansion," IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890–896, Aug. 2003.

[11]Y. Hu, H.-K. Lee, K. Chen, and J. Li, "Difference expansion based reversible data hiding using two embedding directions," IEEE Trans. Multimedia, vol. 10, no. 8, pp. 1500–1512, Dec. 2008.

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

[13]X. Li, B. Yang, and T. Zeng, "Efficient reversible watermarking based on adaptive prediction-error expansion and pixel selection," IEEE Trans. Image Process., vol. 20, no. 12, pp. 3524–3533, Dec. 2011.

[14]W. Zhang, X. Hu, X. Li, and N. Yu, "Recursive histogram modification: Establishing equivalency between reversible data hiding and lossless data compression," IEEE Trans. Image Process., vol. 22, no. 7, pp. 2775–2785, Jul. 2013.

[15]J. Fridrich, M. Goljan, and R. Du, "Invertible authentication," Proc SPIE, vol. 3971, 2001, pp. 197–208.

[16]C. C. Chang, C. C. Lin, C. S. Tseng, and W. L. Tai, "Reversible hiding in DCT-based compressed images," Inf. Sci., vol. 177, no. 13, pp. 2768–2786, 2007.

[17]S. Lee, C. D. Yoo, and T. Kalker, "Reversible image watermarking based on integer-to-integer wavelet transform," IEEE Trans. Inf. Forens. Secur., vol. 2, no. 3, pp. 321–330, Sep. 2007.

[18]W.-H. Lin, S.-J. Horng, T.-W. Kao, P. Fan, C.-L. Lee, and Y. Pan, "An efficient watermarking method based on significant difference of wavelet coefficient quantization," IEEE Trans. Multimedia, vol. 10, no. 5, pp. 746–757, Aug. 2008.

[19]Z. Wang, A. Bovik, H. Sheikh, E. Simoncelli, Image quality assessment: from error visibility to structural similarity, IEEE Trans. Image Process. 13 (4) (2004) 600-612.