International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 04 | Apr-2016 www.irjet.net p-ISSN: 2395-0072

Improving Security Of Mosaic Images By Cryptographic Algorithm And Compression Technique

Ms. Nilam Gandhe[1], Prof. Mr. Mayur Dhait[2]

[1] *Department of Computer Science and Engineering,*

RTMNU University , A.C.E. Wardha , Maharashtra , India.

[2] *Department of Electronics and Communication,*

RTMNU University , A.C.E. Wardha , Maharashtra , India.

Abstract - *A new technique is proposed for secure image transmission, which automatically transforms large-volume secret image into secret-fragment-visible mosaic image of the same size. The mosaic image is obtained by dividing the secret image into fragments and transforming their color characteristics to be those of the corresponding blocks of the target image. It looks similar to an arbitrarily selected target image and may be used as a camouflage of the secret image. We proposed a approach to enhance security of the mosaic image by providing better Encryption logic which provide faster encryption. And for the sake of transmission we proposed JPEG lossless compression technique which provide good compression ratio.*

***Key Words*: image encryption, decryption, mosaic image, image compression, jpeg.**

1.INTRODUCTION

Now a days, for various applications images are frequently utilized and transmitted from various sources through the internet, these images usually contain secret personal information so they should be protected from leakages during transmissions. Many methods have been proposed for securing image transmission, two common methods are image encryption and data hiding.

In the process of data encryption like images the encrypted image is a noise image so that no buddy can obtain the secret image from it without the correct key. However, the encrypted image is called a meaningless image, which do not give additional information before its decryption and may arouse an attacker's attention at the time of transmission because its in shuffle form. The other method is Data hiding which used to avoid this problem [6] that hides a secret message into a cover image because of that no one can realize the existence of the secret data.

A main problem of the method for hiding data in images is the difficulty to embed a large amount of message data into a single image. In case, if one wants to hide a secret image into a cover image with the same size, the secret image must be highly compressed in advance. But, for many applications, such as keeping or transmitting medical pictures, military images, legal documents, etc., such type of data compression technique are usually impractical. The user cannot select freely his/her favorite image for use as the target image. Therefore in this study to remove this drawback of the method while keeping its merit, it is needed 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 [2].

A new technique is use for secure image transmission, that transforms a secret image into a meaningful mosaic image with the same size and looks like a preselected target image. The given secret image is first divided into rectangular fragments called tile images, which are then 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 that of the corresponding target block in the target image, resulting in a mosaic image which looks like the target image. For loading and transferring of image efficiently the lossless compression is applied on mosaic image. And encryption algorithm [8] to improve the security of mosaic image so any one cryptographic algorithm is applied on compressed mosaic image to securely transferring.

2. REVIEW OF LITERATURE

The author in this paper[1] is shows a technique for the transmission of the secret image securely with no loss. This method convert the secret image into a mosaic tile image having the same size looking like that of the target image which is preselected from a database. This color transformation is controlled and the secret image is get back without loss from the mosaic tile image with the help of the

extracted relevant information which are generated for the recovery of the image.

The author in this paper[2] is presented A new type of computer art image called secret-fragment-visible mosaic image , which is created automatically from a given secret image which are divided into a small fragments and by composing all those small fragments to become a target image in a mosaic form, achieving an effect of embedding the given image visibly but secretly in the resulting mosaic image. This effect of information hiding is helpful for covert communication or keeping of secret images secure. To create this type of mosaic image from a given secret color image, need to transformed the 3-D color space into a new 1-D color scale, based on finding the similarity of a new image for selecting a target image from a database that is the most similar to the given secret image. A fast greedy search algorithm is proposed to find a similar tile image in the secret image to perfectly fit into each block in the target image. The relevant information of the tile image fitting sequence is place up into randomly-selected pixels in the created mosaic image by a lossless using LSB replacement scheme with a secret key; without the key, the secret image cannot be recovered. The aim to design this method, specially for dealing with color images, is also extended to create grayscale mosaic images which are useful for hiding text-type grayscale document images.

The author in this paper[3] is describes a method for a more general form of color correction that receive one image's color characteristics from another. They described core strategy in every way is to choose or select an appropriate color space and then to apply simple operations there. When a typical three channel image is described in any of the most conventional color spaces, there will be correlations between the different channels' values.

The author in this paper[4] is describes a new image encryption scheme using a secret key of 144-bits is proposed. In the substitution process of the scheme, image is divided into blocks and subsequently into color components. Each color component is modified by performing bitwise operation which depends on secret key as well as a few most significant bits of its previous and next color component. The substitution process takes three rounds to complete. A feedback mechanism is also applied by modifying used secret key after encrypting each block to make cipher more robust. Further, resultant image is partitioned into several key based dynamic sub-images. Each sub-image passes through the scrambling process where pixels of sub-image are reshuffled within itself by using a generated magic square matrix. Five rounds are taken for scrambling process. The propose scheme is simple, fast and sensitive to the secret key. Due to high order of substitution and permutation, common attacks like linear and differential cryptanalysis are infeasible. The experimental results show that the proposed encryption technique is efficient and has high security features.

The author in this paper[5] is describes JPEG: Still Image Data Compression Standard Here, W. B. Pennebaker tries to explain that the main impediment in many applications is the perceived length of data required to represent a digital image. For this we would need an image compression standard to maintain the quality and clarity of the images after compression. To meet all the needs of the JPEG standard for image compression includes two basic methods having different operation modes: A predictive method for "lossless" compression and a DCT method for "lossy" compression.

3. PROPOSED SCHEME

The proposed method includes phases as shown by the flow diagram.

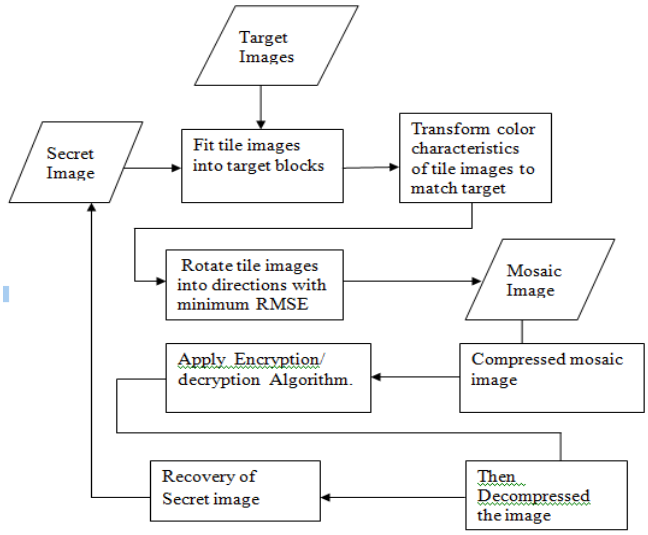


Fig -1: Block Diagram of Proposed Method

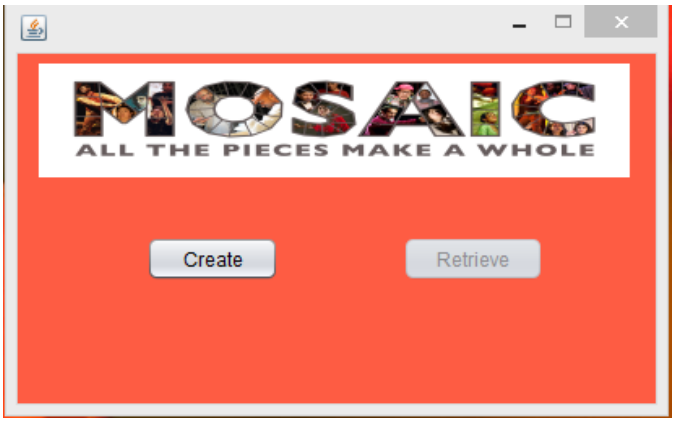
In the first phase, a mosaic image is yielded, which consists of the fragments of an input secret image with color corrections according to a similarity criterion based on color variations. These phase includes Three stages: 1) fitting the tile images of the secret image into the target blocks of a preselected target image; 2) converting the color characteristic of each tile image in the secret image to the corresponding target block in the target image; 3) rotating each tile image into a different direction with the minimum RMSE value with respect to its corresponding target block. In second phase we will perform lossless compression on mosaic image and then perform the encryption on compressed image then we transmit the image securely. In the Third phase, the secret image is recover nearly losslessly from the generated mosaic image. These phase includes two stages: 1) we will first decrypt the encrypted image and 2)perform decompression on image for recovering the secret image from mosaic image.

Algorithm 1 Mosaic image creation:

Input: a secret image , *a target image* .
Output: mosaic image .
Stage 1. fitting the tile images into the target blocks.
Stage 2. performing color conversions between the tile images and the target blocks.

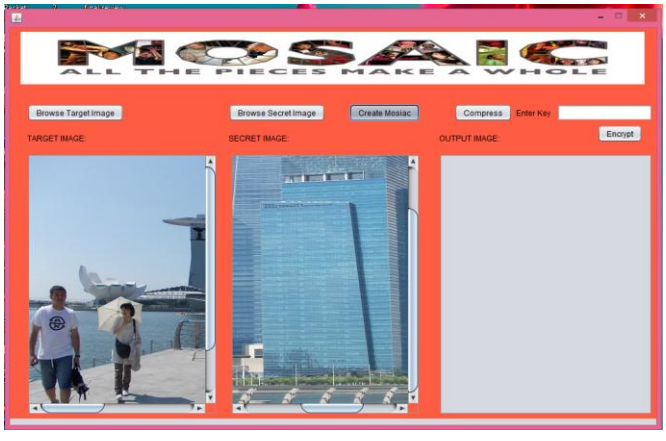
Stage 3. rotating the tile images.
Stage 4. record the secret image recovery information.

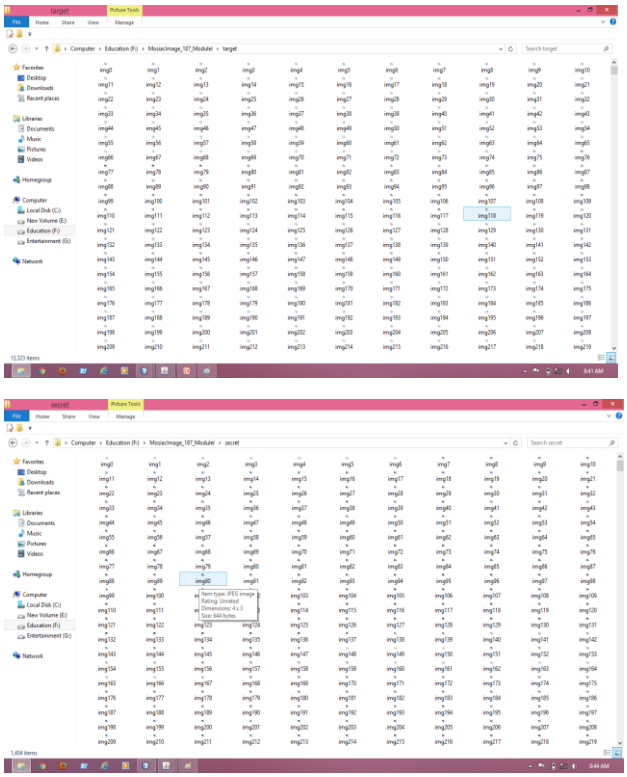
4. IMPLIMENTATION



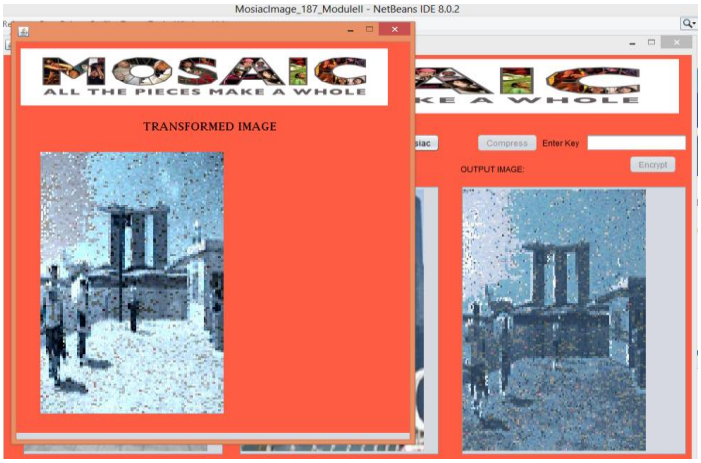
This is a home page to create a mosaic image and retrieve the secret image.

Here we select target image and secret image after that create mosaic image it will compress and encrypt by entering a key.





After selecting target image and secret image it will divided into a tiles.



This is a transformed image called mosaic image which is looking like a target image.

5. CONCLUSIONS

The proposed method to securely transmit a secret image, which can created mosaic images which also can transform a secret image into a mosaic image with the same size of data for concealing the secret image. The technique encryption algorithm is use to improve the security of mosaic image and also there is need to transfer an image by compressing it allows to loading and transferring it in an efficient form and to recover it with minimum loss. We will try to maintain PSNR ratio of the recreate Image.

REFERENCES

[1] Ya-Lin Lee, Wen-Hsiang Tsai, "A New Secure Image Transmission Technique via Secret-fragment-Visible Mosaic Images by Nearly Reversible Color Transformations," IEEE Transactions on Circuits and systems for video Technology, vol. 24, no. 4, April 2014.

[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. A shikhmin, B. Gooch, and P. Shirley, "Color transfer between images," IEEE Comput. Graph. Appl., vol. 21, no. 5, pp. 34–41,Sep.–Oct. 2001.

[4] Narendra K Pareek "design and analysis of a novel digital Image encryption scheme," International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.2, March 2012

[5] W. B. Pennebaker and J. L. Mitchell, "JPEG: Still Image Data Compression Standard", New York, NY, USA: Van Nostrand Reinhold,pp. 34–38, 1993.

[6] 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.

[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, no. 19, pp. 4331–4339, 2011.

[8] Ismail Amr Ismail, Mohammed Amin and Hossam Diab, (2010) "A digital image encryption algorithm based a composition of two chaotic logistic map", International Journal of Network Security, Vol. 11, No. 1, pp. 1-10.

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

[10] C. H. Yang, "Inverted pattern approach to improve image quality of information hiding by LSB substitution," *Pattern Recog.*, vol. 41, no. 8,pp. 2674–2683, 2008.

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

[12] 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.

[13] 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.

[14] R. Z. Wang, C. F. Lin, and J. C. Lin, "Image hiding by optimal LSB substitution and genetic algorithm," *Pattern Recog.*, vol. 34, no. 3,pp. 671–683, 2001.

[15]Ghosh,D.Park,S.Kaabouch,N.Semke,W."Quantum evaluation of image mosaicing in multiple scene categories " IEEE Conference on Electro/Information Technology,pp 1-6,2012.