International Journal of Engineering Research & Management Technology ISSN: 2348-4039
November-2015 Volume 2, Issue-6
Email: editor@ijermt.org www.ijermt.org

A Review on Secret Image Protection Technique via Secret-Fragment-Visible Mosaic Image

Ms.Namrata A. Khodke
M.E. Second Year
Computer Science & Engineering
College of Engineering & Technology
Amravati .Maharashtra

Dr. Siddharth A. Ladhake
Principal/Professor
Computer Science & Engineering
Sipna College of Engineering & Technology
Amravati .Maharashtra

ABSTRACT:
Nowadays requirement of secure transmission of data is important in our life. Image transmission is one of the applications that must be securely transmitted over the fraudulence network. Therefore a new approach for the secure image transmission is proposed, which transforms automatically a given huge-volume of secret image into a visible mosaic image of the same size. The mosaic image which looks similar to a randomly selected target image and may be used as a mask of the secret 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. A lossless data hiding scheme using a secret key is proposed for recovering the information which is embedded into the created mosaic image.

KEYWORDS: image processing, data hiding, color transformation, mosaic image.

INTRODUCTION:

Nowadays where nothing is secure, image security is also an important issue while transmitting images over the internet.Therefore it is necessary to secure secret image and protecting it over the network so that no unauthorized user can able to decrypt the image . These images may contain private or confidential information so that they should be protected from leakages during transmissions. Therefore many methods have been proposed for securing image transmission, from encryption and data hiding. In recent years data hiding has been proposed for the purpose of information assurance, authentication, fingerprint, security, data mining, and copyright protection, etc. In some last years different image encryption techniques were proposed. The main idea behind the image encryption is to transmit the image securely over the network so that no unauthorized user can able to decrypt the image without a secret key. Digital images are attractive data types with widespread use and many users are interesting to implement content protection on them to keep from copyright, preview or malfunction. On much system like military image databases, providing security is must. It is very important to protect confidential image data from unauthorized access. Encryption is the preferred technique for protecting the transmitted data. However, number of other techniques instead of encryption is also available for converting valuable piece of information into such form which access is prohibited to unauthorized users. There are various encryption systems for encrypting and decrypting images are available. In information systems, aspects of security like confidentiality, security, privacy and non-repudiation need to be achieved.

In the last some year image mosaic has become a popular topic in field of digital image processing and image based technique. To mosaic an image is to combine overlapped images so that the mixed image contains no obstructive limitations in the transition region while preserving the general appearance of the original images. Mosaic is nothing but the art of creating images with an assemblage of small pieces of

colored glass, stone, or other materials. This principle is utilized here in the area of image steganography. The new type of art image called secret-fragment-visible mosaic image contains small fragments of a given source image. Observing such a type of mosaic image, one can see all the fragments of the source image, but the fragments are so tiny in size and so random in position that the observer cannot figure out what the source image looks like. Therefore, the source image may be said to be secretly embedded in the resulting mosaic image, though the fragment pieces are all visible to the observer. And this is the reason why the resulting mosaic image is named secret-fragment-visible. Because of this characteristic of the new mosaic image, it may be used as a carrier of a secret source image in the disguise of another, a target image of a different content. It is useful for the application of covert communication or secure keeping of secret images.

RELATED WORK:

In traditional methods secret data can be hidden into image which is called as Steganography. In this method only secret data can be encrypted but not image. Secret
images can be hidden using water marking principles. Water marking is very simple process and it is weak that anyone can decrypt easily. Mosaic image technique is one of the efficient techniques to hide the secret images. This methodology needs another image which is said to be cover image. Creating mosaic image is also a art of computer. Many methods have been proposed to create different types of mosaic images by computer.

C. K. Chan and L. M. Cheng[1] proposed a data hiding method which hides a secret information into a cover image so that no one can realize that the secret data is embedded with the cover image. This data hiding scheme is done by simple LSB substitution with an optimal pixel adjustment process (OPAP) . The image quality of the stego-image can be greatly improved with low extra computational complexity. Sebastiano Battiato and Gianpiero Di Blasi proposed a novel approach for artificial mosaic generation based on Gradient Vector Flow (GVF) computation together with some smart heuristics used to drive tiles positioning. Almost all previous approaches filter out high frequencies in order to simplify mosaic generation. The GVF properties permit us to preserve edge information and maintain image details. The novelty of this approach is related to the heuristics which is used to follow principal edges and to maximize the overall mosaic area covering.

A data hiding technique called RCM, a modified version that allows robustness against cropping is proposed by Dinu Coltuc and Jean-Marc Chassery [4]. It also investigates the control of distortions introduced by the watermarking and analysed the mathematical complexity of the RCM watermarking, and a very low cost implementation is proposed. V. Sachnev, H. J. Kim, J. Nam, S. Suresh, and Y.-Q. Shi [8] presents a reversible or lossless watermarking algorithm for images without using a location map in most cases. This algorithm employs prediction errors to embed data into an image. A sorting Technique is used to record the prediction errors based on magnitude of its local variance. The proposed method is evaluated using different images and compared with four methods: those of Kamstra and Heijmans, Thodi and Rodriguez and Lee. The obtained results clearly indicate that the proposed scheme can embed more data with less distortion.

A technique of information hiding which consist of secret image is first divided into rectangular shaped small fragments (tile images) and then for creating mosaic image they are fix to its next target image selected from a database. Secret key selects randomly some blocks of mosaic images to embed the information of tile image .A hacker without the key cannot retrieve the secret information as t he key can reconstruct the secret image by retrieving the embedded information.This technique is presented by I-Jen Lai and Wen-Hsiang Tsai [9].

X. Li, B. Yang, and T. Zeng [10] proposed a Reversible image watermarking which enables the embedding of copyright or useful information in a host image without any loss of information. They

proposed a novel technique to improve the embedding capacity i.e. reversible watermarking using an adaptive prediction error expansion & pixel selection. This work is an improvement in conventional PEE by adding two new techniques adaptive embedding & pixel selection. W. Zhang, X. Hu, X. Li, and N. Yu[11] proposed a reversible data hiding and lossless data compression scheme. Generally RDH consist of two steps: first construct a host sequence with a sharp histogram via prediction errors and then embed messages by modifying the histogram with methods such as difference expansion and histogram shift. But in their research they focus on second stage and propose a histogram modification method for RDH which embeds the message by recursively utilizing the decompression and compression processes of an entropy coder. This method asymptotically approaches the rate-distortion bound of RDH as long as perfect compression can be realized i.e. the entropy coder can approach entropy. Therefore this method establishes the equivalency between reversible data hiding and lossless data compression.

Ya-Lin Lee and Wen-Hsiang Tsai [12] have proposed a new scheme for secure image transmission which converts a secret image into a meaningful mosaic image with the same size and looking like a preselected target image. Secret key controls transformation process and that secret image is only recover by that key without any loss from mosaic image The proposed method is extended by Lai and Tsai , in which a new type of computer art image, called secret-fragment-visible mosaic image, was introduced.. The mosaic image is the output of rearrangement of the fragments of a secret image in disguise of another image called the target image preselected from a database.

PROPOSED METHOD:

Security of digital images in transmission, publishing and storage become more important due to ease of access to open networks and internet. Uptill now number of image transmission techniques has been proposed but each of them has its own flaw which leads to insecure transmission of images over the internet. There are many approaches to avoid this problem like data hiding technique, encryption methods, JPEG compression etc. A main issue of the methods for hiding data in images is the hard to embed a large amount of information into a single image. So the secret image must be highly compressed in advance, if one wants to hide a secret image into a cover image with the same size. Therefore novel approach to secure image transmission is proposed which transforms a secret image into a mosaic image with the same size which looks like a preselected target image freely chosen by the user. The transformation process is controlled by a secret key, and only with the help of the secret key a person able to recover the secret image losslessly from the received mosaic image. In proposed system we are trying to remove the flaws of previously derived techniques and trying to implement new secure image transmission technique using visible mosaic images.

The proposed method is inspired from Lai and Tsai, who introduced a new technique of secret-fragment-visible mosaic image. But the weakness of Lai and Tsai method [12] is the requirement of a large image databases. So that the generated mosaic image will be sufficiently similar to the preselected target image Using Lai and Tsai method, the user is not able to select freely his/her favorite image for use as the target image. Therefore in this research a desired method is proposed so as to remove this weakness of the Lai and Tsai method by keeping its merit and 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 which is having the visual appearance of any freely selected target image without the need of a database.

The proposed method includes two main phases as shown in the flow diagram fig. Phase 1. creation of mosaic image and Phase 2:recovery of secret image

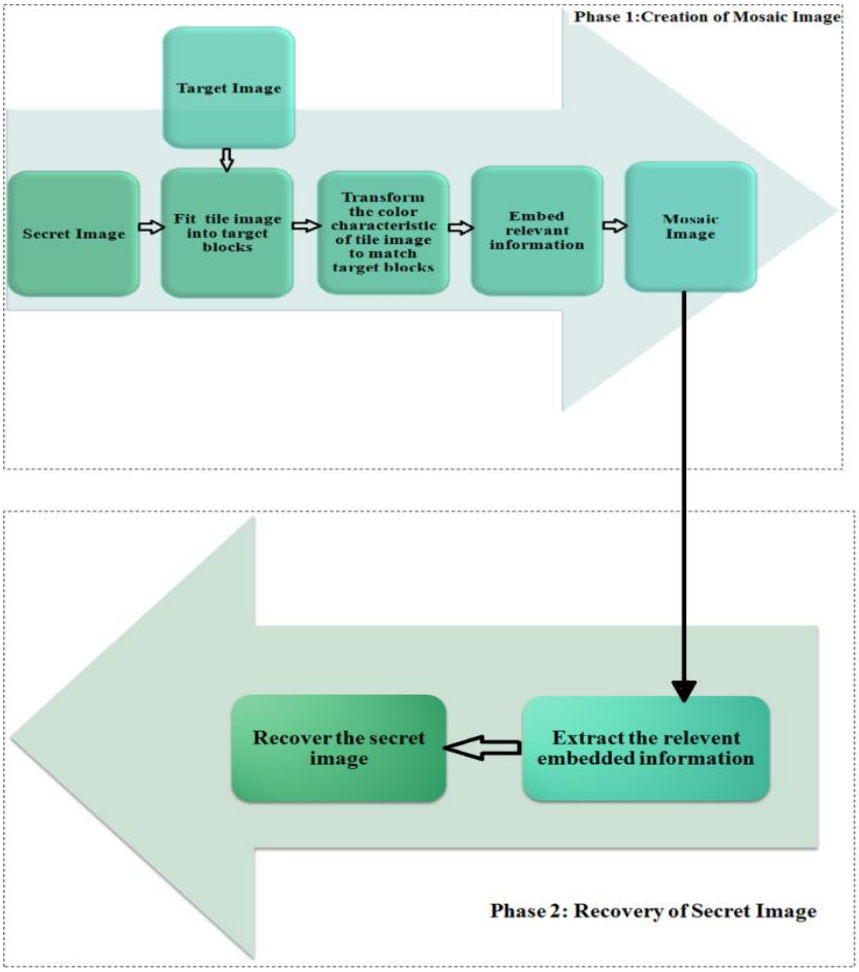

Fig. 1 Flow diagram of proposed method

In the first phase, mosaic image is created, which consists of the fragments of an input secret image having color corrections according to a similarity criterion based upon color variations. The phase consists of four stages.

1.we have to fit the tile images of the secret image into the target blocks of a preselected target image

2. Transform the color characteristic of each tile image in the secret image to become that of the corresponding target block in the target image. Since the color characteristics of Secret image and Target image are different from each other, we have to change their color distributions to make them look alike.

3.Rotate each tile image into a direction with the minimum RMSE value with respect to its corresponding target block.

4. at last in order to recover the secret image from the mosaic image, we have to embed relevant recovery information into the mosaic image. Here we use data hiding technique for embeding the data into mosaic image.

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

1.Extract the embedded information for secret image recovery from the mosaic image,. for extraction processes use a reverse version of the scheme which is used in data embedding.

2.Rrecover the secret image using the extracted information.

CONCLUSIONS:

In todays world,images and documents are travel widely and rapidly in multiple manifestations over the internet.Controlling and protecting secret image is an important issue.Therefore different image hiding techniques in recent years are surveyed. On the basis of these we may say all techniques are good for data hiding and have their own advantages and disadvantages .In order to provide better security to the images and considering all the flaws in previous techniques we have proposed a new image protection technique via secret-fragment-visible mosaic image so that no one can access the secret image which is in the open network and a good moasic image creation results are guaranteed.

REFERENCES:

1. C. K. Chan and L. M. Cheng, "Hiding data in images by simple LSB substitution," Pattern Recognition.., vol. 37, pp. 469–474, Mar. 2004.
2. SabuM.Thamp,"Information Hiding Techniques: A Tutorial Review", ISTE-STTP on Network Security & Cryptography , LBSCE 2004.
3. Zhicheng Ni, Yun-Qing Shi, Nirwan Ansari, and Wei Su," Reversible Data Hiding", IEEE transactions on circuits and system for video technology, vol. 16, no. 3, march 2006.
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. 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. 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.
7. 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.
8. 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.
9. 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.
10. 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.
11. 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.
12. Ya-Lin Lee, Student Member, IEEE, and Wen- Hsiang Tsai, Senior Member, "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.