ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

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

Namrata A. Khodke, Dr. Siddharth A. Ladhake

M.E.2nd Year, Dept. of CSE, Sipna COET Amravati, SGBAU, MH, India

Principal/Professor, Sipna COET Amravati, SGBAU, MH, India

ABSTRACT: The requirement of secure transmission of data is important in our life. Image transmission is one of the application 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, 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. Expert techniques are designed to conduct the color transformation process so that the secret image may be recovered nearly losslessly. Also, the original secret images can be recovered by using Shamir encryption and decryption algorithm, in which by combining minimum number of shares the original secret image can be retrieved.

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

I. INTRODUCTION

Today image security is an important issue while transmitting images over the internet for various applications such as for online personal photographs, albums, confidential organizational archives, military image database, storage systems, and medical imaging systems. These images may contain private or confidential information so that they should be protected from leakages/loss during transmissions. Therefore many methods have been proposed for securing image transmission, from encryption and data hiding. 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. But encrypted image will be the meaningless file, which is not able to provide additional information before decryption and may stimulate an attacker's attention during transmission process due to its randomness in form.

So far in cryptography lots of work have done related to text information. Encryption techniques so far used for text information may not work in same direction for visual. 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 addition to cryptography, steganography techniques are getting significantly more sophisticated and have been widely used. The steganography techniques are the perfect supplement for encryption that allows a user to hide information within an image. Thus, it is often used in conjunction with cryptography so that the information is doubly protected, that is, first it is encrypted, and then it is hidden so that an adversary has to find the hidden information after the decryption takes place.

What Is Secret Fragment Visible Mosaic Image?

Mosaic is 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

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

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.

In this technique, a novel approach to secure image transmission is proposed, which transforms a secret image into a mosaic image with the same size and looks like a preselected target image which is freely chosen by the user. The transformation process will be 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. The proposed method is inspired from Lai and Tsai [12], who introduced a new technique of secret-fragment-visible mosaic image.

II. RELATED WORK

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) . OPAP is proposed to enhance the image quality of the stego-image obtained by the simple LSB substitution method. In this proposed system, 8-bit grayscale images are selected as the cover media. These images are called cover-images. Cover-images with the secret messages embedded in them are called stego-images. For data hiding methods, the image quality refers to the quality of the stego-images. The worst case mean-square-error between the stego-image and the cover-image is derived. Experimental results show that the stego-image is visually indistinguishable from the original cover-image.

Sabu M Thampi[2] have presented a information hiding technique in which a brief history of steganography is explained along with techniques that were used to hide secret information. Textual, audio and image based information hiding techniques like Least Significant bit(LSB) insertion technique in which embed the information in graphical image file, masking and filtering techniques in which by making an image in a manner similar to paper watermarks and transformation techniques which is done by using discrete cosine transformation or wavelet transform to hide information in significant areas of image.Zhicheng Ni, Yun-Qing Shi, Nirwan Ansari, and Wei Su [3] have proposed a new data hiding technique , i.e. reversible data embedding technique, which can embed a large amount of data the PSNR of the marked image versus the original image is guaranteed to be higher than 48 dB which kept a large percentage of visual quality for all natural images.The reversible data embedding technique can be successfully applied to a wide range of images like texture images, medical images, aerial images and all of the 1096 images in CorelDraw database.

Dinu Coltuc and Jean-Marc Chassery [4] have presented a data hiding technique like RCM, a modified version that allows robustness against cropping. It also is investigates the control of distortions introduced by the watermarking. It also analysed the mathematical complexity of the RCM watermarking, and a very low cost implementation is proposed. Finally, the RCM scheme is compared with Tian's difference expansion scheme with respect to the bit-rate hiding capacity and to the mathematical complexity. It is shown that the RCM scheme provides almost similar embedding bit-rates when compared to the difference expansion approach, but it has a considerably lower mathematical complexity.

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. I-Jen Lai and Wen-Hsiang Tsai [9] have presented 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.

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.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

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.

In this way we have studied these literature work related to our proposed system .Therefore a new secret image protection technique is proposed using secret fragment visible mosaic image which will play vital role in protecting images from leakages and loss.

III. SYSTEM ARCHITECTURE

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 image transmission techniques have been proposed but each of them has its own flaws 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 includes two main phases as shown in the diagram of Fig.1. Creation of mosaic image and Fig.2. Recovery of secret image

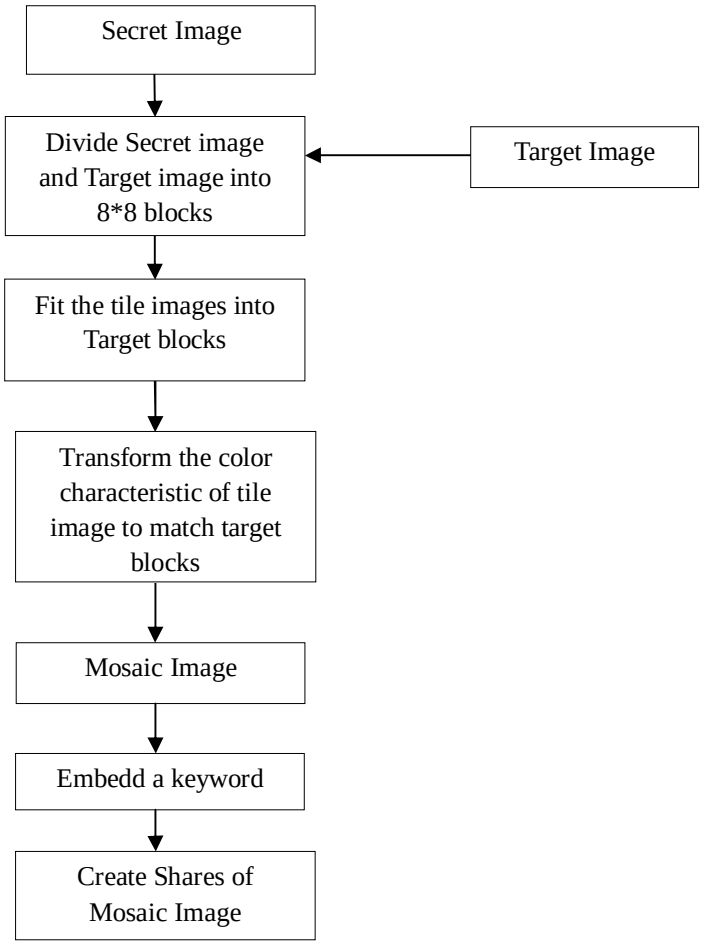

Fig.1. Creation of mosaic image

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

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. First we fit the tile images of the secret image into the target blocks of a preselected target image. Then transform the color characteristic of each tile image in the secret image to become that of the corresponding target block in the target image. And a mosaic image will be obtained. The whole process is controlled by a secret key. Then by applying Shamir's Encryption Algorithm we create shares of mosaic image.

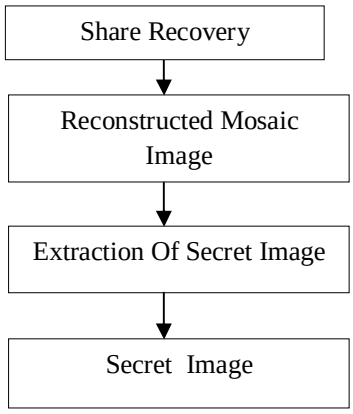

Fig.2.Recovery of secret image

In the second phase, Shares will be recovered by applying Shamir's Decryption Algorithm and we will obtain a desired Mosaic image. Then though extraction process we will get the secret image from mosaic image if the key get match.

IV. PROPOSED ALGORITHM

Algorithm 1: For Mosaic Image Creation

1. Load a Secret Image and a Target Image
2. Divide secret image and target image into 8*8 blocks
   Secret image =>Tile images, Target image => Target Blocks
3. Calculate mean and standard deviation of Tile images and Target blocks according to each plane and find out average standard deviation of each block
4. Sort the blocks of secret image and target image according to their calculated average standard deviation values
5. Map the blocks of sorted tile images to those in the sorted target blocks in a 1-to-1 manner; and according to the indices of the tile images reorder the mappings
6. By fitting the tile images into the respective target blocks create a mosaic image.
7. Apply Shamir's Encryption Algorithm and create shares of the mosaic image.

Algorithm2: For Recovery of Secret Image

1. Using Shamir's Decryption Algorithm, recover the mosaic image from shares .
2. Calculate mean and standard deviation of Mosaic image and Target image according to each plane and find out average standard deviation of each block
3. Sort the blocks of mosaic image and target image according to their calculated average standard deviation values
4. Map the blocks of sorted mosaic image to those in the sorted target blocks in a 1-to-1 manner; and according to the indices of the tile images reorder the mappings
5. And what will be the difference in between them that will be our desired Secret image.

In this way a new secret image protection technique has been proposed to securely transmit the secret image so that no unauthorized user can able to recover that image easily. First we use the concept of creation of Mosaic Image

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

and then will encrypt that image by using Shamir's Encryption algorithm and create number of shares and that shares are recovered by the receiver using Shamir's Decryption algorithm. Then from mosaic image we recover the desired secret image.

V. EXPERIMENTAL RESULTS

In the following table we have compare the values of MSE, PSNR , Correlation and Entropy which are obtained by two existing system and our proposed system.

Existing Method	Parameters	Values according to Existing System	Values according to Proposed System
A New Secure Image Transmission Technique via Secret-Fragment-Visible Mosaic Images by Nearly Reversible Color Transformations	MSE	0.948	0.0044759
	PSNR	55.09	71.622
	Correlation	0.90	1
	Entropy	5.89	6.8201
Secret-Fragment-Visible Mosaic Image–A New Computer Art and Its Application to Information Hiding	MSE	4.86	0.0005696
	PSNR	71.67	80.57
	Correlation	0.92	1
	Entropy	7.01	7.1108

Table 1. Shows the values of MSE, PSNR ,Correlation and Entropy which are obtained by two existing system and our proposed system.

In above table we have compared our system with the existing system. According to above comparison table we can observe that our proposed method is more effective in terms of MSE, PSNR, Correlation and Entropy.

VI. CONCLUSION & FUTURE SCOPE

In today's world where nothing is secure, the security of images is very important. A new secure image transmission method has been proposed, which can transform a secret image into a mosaic one and provide more image security. Also, the original secret images can be recovered by using Shamir encryption and decryption algorithm, in which by combining minimum number of shares the original secret image can be retrieved. The proposed algorithm is more challenging as well, because there is a significant cryptography provided for image security. In this paper, a new type of computer art image i.e. secret fragment visible mosaic image is proposed for providing a better security. In future we will apply this technique to audio/ videos and will try to improve the security issues of audio/video data.

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 vedio 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.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

[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 andsystems for video Technology, vol. 24, no. 4, April 2014.
[13] W. B. Pennebaker and J. L. Mitchell, *JPEG: Still Image Data Compression Standard*. New York, NY, USA: Van Nostrand Reinhold, 1993,pp. 34–38.
[14] 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.

BIOGRAPHY

Ms. Namrata A. Khodke is a M.E. 2nd Year student of Computer Science and Engineering Department, Sipna COET Amravati in 2016 from SGBA University, Amravati, MH, India.
Dr. Siddharth A. Ladhake is a Principal/Professor at Sipna COET Amravati, SGBAU, Amravati, MH, India.