IJCSN - International Journal of Computer Science and Network, Volume 3, Issue 6, December 2014
ISSN (Online): 2277-5420 **www.IJCSN.org**
Impact Factor: 0.274

Review on Various Methods for Secure Transmission of Images for Maintaining Image Integrity

[1] Prashant Dahake , [2] Sonali Nimbhorkar

[1] M.Tech Student, Department of Computer Science and Engineering, G.H. Raisoni College of Engineering, Nagpur, Maharashtra, India

[2] Department of Computer Science and Engineering, G.H. Raisoni College of Engineering, Nagpur, Maharashtra, India

Abstract - The System Security is important for secure communication. Biometric fingerprint authentication requires physical presence of human being; it can't be traceable as well as forgeable. By using data compression method size of data can be reduced and requires less memory space. When data is transmitted through network secretly, there may be chance that secret data may lost or damaged. In order to provide secrecy and integrity to data, there are various security mechanism are available. Biometric key can be generated from fingerprint which is further used for encryption purpose. This paper shows different mechanism which is necessary for secure transmission of image data and the pros and cons of the algorithms to provide an overview of the latest approaches in the field are discussed

Keywords - *mosaic image, encryption, data hiding, biometric, and compression, PSNR, etc.*

1. Introduction

In order to make key management unique, untraceable, and secure, the simplest way is to use biometrics [1]. To protect user authenticity use of biometric is one of the important method so only legitimated user can send or receive data. Biometric is the simplest way in order to make key management secure, untraceable and unique. It uses one or more intrinsic behavioral or physical characteristics. These characteristic includes fingerprints, palm prints, retina or iris, facial structure, etc. The images from various sources are frequently used and transmitted through the internet for various applications, such as online images, medical images, military image database, Personal photograph album, document storage system etc. Confidential and private information is present in those images. Therefore they should be protected during transmission from leakage. Cryptography plays an important role in secure transmission of image. It protects images from various attacks so no one able to use it. For efficient transmission of images through the network data size must be reduced, So that it is transmitted at faster rate.

In this paper we present a survey of the current secure image transmission of data, different way of key generation from biometric fingerprint and different image compression technique and methods were discussed. The rest of this paper is organized as follows. We discuss the current literature and discuss the method for mosaic image creation, different data hiding techniques and biometric key generation technique, image compression technique in section 2. After that In Section 3 we discussed about image parameters, section 4 contain summary of all discussed method in the tabular form. In section 5 we conclude the paper and shows possible areas of enhancement and our future plan for secure transmission of image data.

2. Methods of Image Security Review

2.1 Mosaic Image

Lai and Tsai [2] use another method in which mosaic image was generated which is the combination of secret image and target image. For embedding secret image into target image, algorithm searches similar target image inside database, so there is tough task to maintain database. They proposed method for RGB images; it can be further used for creation of grayscale mosaic images which are used for hiding text grayscale document images.

There are various mosaic image formation technique.

1. Crystallization Mosaics
2. Ancient Mosaics

3. Photo-Mosaics
4. Puzzle image Mosaics

The first two types of mosaics decompose a source image into tiles image (with different color, size and rotation) and reconstruct the image by properly painting the tiles images. Hence they come under the categories of tile mosaics. The last two kinds of mosaics are obtained by fitting images from the database to cover a source image. Hence they may be grouped together under the denomination of multi-picture mosaics. H. Narasimhan and S. Satheesh [3] deals with algorithm for generating photo mosaic image. A photo mosaic image is assembled from small images called tiles. When a generated photo mosaic image is viewed from a distance, it looks like a desired target image. The process of generating photo mosaic image can also be considered as optimization problem, where a set of tile images needs to be arranged to look like a target image. The randomized iterative improvement algorithm is used to generate photo mosaics image. They clearly show that the proposed method is more efficient than earlier genetic algorithm.S. Battiato, C. Guarnera and all [4] deal with the Mosaics images that are the artwork constituted cementing together small colored tiles. They suppose to be the first example of image synthesis technique based on discrete primitives. a digital mosaic creation is a challenging task. Many factors like position, orientation, size and shape of tiles images are taken into account in the mosaic image generation in order to densely pack the tiles they propose a novel technique to produce a traditionally looking mosaic from a digital source picture. The new technique tries to overcome the difficulties that depend on edge detection.

In [5] Hae-Yeoun Lee proposed an algorithm that build the photo-mosaic image using photos. The algorithm combines 4 steps: partition and feature Extraction, color adjustment, redundancy removal, block matching, the input image is divided into the small part called block to extract feature. Each block is then matched to find similar photo in database by comparing similarity with Euclidean distance between the blocks. The intensity of each block is adjusted to improve the similarity of image.

2.2 Data Hiding

Suk-Ling Li, Kai-Chi Leung and all [6] proposed a data hiding technique which makes a use of LSB technique. A new scheme is proposed to solve the problem in which the embedded secret data cannot be extracted correctly. In order to enhance and improve the image quality of the stego-image and to increase the embedding capacity of the source-image, a method to insert secret data into the host-image the adaptive LSB substitution technique based on the pixel-value differencing is discussed.

2.3 Image Encryption

Gaurav Bhatnagar, Q. M. Jonathan Wu [1] makes an use of fractional Fourier transform for multimedia encryption. Biometric key is generated from biometric iris. This paper proposes an efficient method for generating biometrically encoded bit-stream from biometrics and it is further used for generation of biometric key. Smitha.M, Dr.V.E.Jayanthi and all [7] proposed an image encryption method which makes a use of two keys, one for encryption and other for compression plus data hiding. The least Significant bits (LSBs) of the encrypted image are compressed using a data hiding key to create space to embed an additional data. Haar wavelet compression and run length coding is employed for faster transmission and to reduce the image size. Kshiramani Naik and Arup kumar Pal [8] proposed an image encryption method which makes an use of confusion and diffusion. Confusion means scrambling of pixels of an image and diffusion means diffusion of bit planes. Scrambled image is decomposed into their binary bit-planes. Each bit plane is encrypted using distinct Binary key matrix by using X-OR operation. It is a two step image encryption algorithm. In [9] I. Iqbal, W. Masood proposed a new method is introduced for image area selection that will select maximum information area for encryption based on percentage of coefficients. Non-encrypted area is permuted with the encrypted area that will further increase the security of the image and peak signal to noise ratio values show a large difference in between the original and encrypted images.

2.4 Biometric Key Generation.

In [10] B. Raja Rao, Dr. E.V.V. Krishna Rao and all deal with the biometric key generation from fingerprint minutia point. For that purpose they used elliptic curve technique. For key generation algorithm makes an use of following steps.

- Finger Print image Enhancement
- Histogram Equalization
- Fingerprint Image Binarization
- Thinning
- Minutiae Extractor
- Key Generator

Vladimir Yu. Gudkov and Oleg Ushmaev [11] they proposed an approach to key Generation from fingerprint

images based on topological descriptors of minutiae point neighborhood. This approach generate biometric key of variable length. Process of topological model generation is divided into two stages. At very first stage, standard fingerprint processing techniques are applied. So that accurate minutia points are obtained. Fingerprint image is filtered, and Minutiae point locations and local ridge flow directions are determined. They proposed an approach to generation keys from fingerprint biometrics based on topology of fingerprint patterns.

It has the following advantages.

1) Topological descriptors are very stable fingerprint features. They don't depend on elastic deformations and finger alignment.
2) The approach allows varying decryption rate and key length.

In [12] Haiyong Chen, Hongwei Sun and all deal with biometric key management. They propose a scheme that uses variant biometric samples to generate constant and repeatable keys. Biometrics encryption, it is a process that securely binds a cryptographic key to a biometric, and re-creates the key only if the correct live biometric sample is presented during key formation. Biometrics encryption seems to be a secure method. R. Sashank Singhvi, S.P.Venkatachalam and all [13] Biometric authentication plays an important role in different area. Besides that, the storage space for biometric templates and encryption keys is important issue in that area since the negotiation of templates compromises the information protected by those keys. Author developed a new technique, which needs neither the storage of biometric templates nor the private keys, by openly producing the keys from the statistical characteristics of biometric data.

2.5 Image Compression

Image Compression is a very important field in the era of communication. Therefore it is important to understand literature for image compression, as the demand for images has increase over the year, which requires fast transmission. So this leads to the need for compression of image data to save transmission time and storage space. In this paper we discussed different image compression algorithms used to reduce size of images without reduction in image quality. Compression can be classified into two types Lossy and Lossless compression. In Lossless compression there is no information loss and the image also retains its quality it can be remodeled exactly the same as the original. Lossless methods cannot provide enough compression ratios. Two essential and basic parts are reducing redundancy and irrelevancy. Reducing Redundancy focuses to reproduce exactly from the image. Parts of the image are omitted unnoticed by the receiver from naked eye namely Human Visual System in irrelevancy reduction.

Krishan Gupta, Mukesh Sharma and all [14] deal with the KMP compression technique. It is a lossless image compression method; it has simple implementation and has less utilization of memory. This method allows the compression of pixel repeated in all direction. All direction means not only in horizontally or vertically or diagonally but also in anywhere in the image. As image are made of pixel here pixel means representation of different color in image which can be repeated anywhere in image. KMP technique is very power full technique to compress images of highly repeated ration of same pixel in whole image. Syed Ali Hassan, Mehdi Hussain [14] proposed a method of lossless image compression in spatial domain. Algorithm divides image into number of blocks and each pixel in that block is represented using variable length bits. Variable bits calculation is dependent on pixel values of each block. The main advantage of this method is that it dependent upon pixels correlation within a block.

R.E. Chaudhari and S. B. Dhok [15] proposed fast fractal image compression based on wavelet transform. Fractal compression algorithm is a lossy compression method for digital image data, based on fractals. This method is best suited for natural images depending on the concept that some parts of an image often resemble other parts of the same image. Fractal method converts this procedure into mathematical data called "fractal codes". With fractal compression, encoding is very costier because of the searching used to find the self-similarities inside image. Decoding, however, is quite fast process. while this asymmetry has so far made it not practical for real time applications. In [16] Ponomarenko, N.N., K.O. Egiazarian and all proposed image compression method in which Benefits of various approaches are combined by DCT based compression method. Firstly, Image is divided into variable size blocks using partitioning in vertical and horizontal direction. For reducing statistical redundancy by a bit plane of each image block. In decompression of images blocking artifacts can be eliminated by post filtering. Significantly better compression results are shown than JPEG and other techniques.

3. Image Quality Parameters

To check the quality of image only size of original image and its visible quality is not sufficient. Image quality is

one of the features of an image that gives idea about whether image gets distorted or not as compared to original image. For more accurate result there are various parameter of image was discussed in literature, such as peak signal to noise ratio (PSNR), Spectral Distortion (SD), and Structural Similarity Index Measure (SSIM) etc. peak signal to noise ratio is the ratio of original image to distorted image or ratio of original image to decrypted image. Higher the PSNR value higher the similarity between two images. Spectral distortion (SD) shows spectral similarity between two images. It shows spectrum of original image and encrypted image as well as spectrum of original image and decrypted image. Structural Similarity Index Measure (SSIM) is also one of the parameter which is used to check the quality of transmitted image. It indicates structural similarity between the images [1].

4. Review Table

Table 1: Methods Review

Sr. No.	*Method*	*Description*
1	Mosaic image method	Secret image is divided into several parts such that they look like tiles or diamond shape.
2	Data hiding method	It is a steganography method in which secret data is hided inside the any multimedia data.
3	Image Encryption	Distorted or scrambled image is generated which is very difficult to analyzed. In image encryption key is used to encrypt the image.
4	Image Compression	To reduce the bandwidth requirement of transmission channel and for increasing transmission speed image compression techniques are useful.
5	Image parameters	PSNR, SD, SSIM these are the some image parameters of image, to check the quality of transmitted image with respect to original image.
6	Biometric key	For encryption of image data key is generated from biometric fingerprint.

5. Conclusions

In this paper, different methods for mosaic image creation, biometric key generation and image compression algorithm are studied. Also various image parameters were discussed. Data hiding technique also discussed. In future hybrid technology will be implemented such that there is one single system which performs all operation as mentioned in literature, also focused will be on better mosaic image creation method such that image integrity must be maintained.

References

[1] Gaurav Bhatnagar and Q. M. Jonathan Wu, "Biometric Inspired Multimedia Encryption Based on Dual Parameter Fractional Fourier Transform", IEEE Transaction on Systems, Man, and Cybernetics: Systems 2014.

[2] I-Jen Lai, Wen-Hsiang Tsai, "Secret-Fragment-Visible Mosaic Image–A New Computer Art and Its Application to Information Hiding", Information Forensics and Security, IEEE Transactions on , vol.6, no.3, pp.936,945, Sept. 2011.

[3] H. Narasimhan and S. Satheesh, "A randomized iterative improvement algorithm for photo-mosaic generation", in Proc. NaBIC, Coimbatore, India, Dec. 2009, pp. 777–781.

[4] S. Battiato, G. Di Blasi, G. Gallo, G. C. Guarnera, and G. Puglisi, "Artificial mosaic by gradient vector flow", in Proc. Eurographics, Creete, Greece, Apr. 2008, pp. 53–56.

[5] Hae-Yeoun Lee, "Generation of Photo-Mosaic Images through Block Matching and Color Adjustment", International Journal of Computer, Information, Systems and Control Engineering Vol:8 No:3, 2014.

[6] Suk-Ling Li, Kai-Chi Leung, Cheng, L. M. Chi-Kwong Chan, "Data Hiding in Images by Adaptive LSB Substitution Based on the Pixel-Value Differencing", First International Conference on Innovative Computing, Information and Control, vol.3, no., pp.58,61, Aug. 30 Sep-2006.

[7] Smitha, M., Jayanthi, V.E., Merlin A, "Image encryption using separable reversible data hiding scheme", Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT), vol., no., pp.1, 6, 4-6 July 2013.

[8] Naik, K. Pal, A.K., "An image cryptosystem based on diffusion of significant bit-planes of a scrambled image with generated binary key matrices" , Computational Intelligence and Computing Research (ICCIC), 2013 IEEE International Conference on , vol., no., pp.1,4, 26-28 Dec. 2013.

[9] Ullah, I; Iqbal, W.; Masood, A, "Selective region based images encryption", 2nd National Conference on Information Assurance (NCIA), vol., no., pp.125,128, 11-12 IEEE 2013.

[10] B. Raja Rao, Dr.E.V.V.Krishna Rao, "Finger Print Parameter Based Cryptographic Key Generation", International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 2, Issue 6, November- December 2012.

[11] Gudkov, V.Y.; Ushmaev, O., "A Topologic Approach to User-Dependent Key Extraction from Fingerprints", International Conference on Pattern

Recognition (ICPR), 2010 20th, vol., no., pp.1281, 1284, 23-26 IEEE Aug. 2010.

[12] Haiyong Chen, Hongwei Sun, Kwok-Yan Lam, "Key Management Using Biometrics," The First International Symposium on Data, Privacy, and E-Commerce, 2007., vol., no., pp.321, 326, 1-3 IEEE 2007.

[13] R. Sashank Singhvi, S.P. Venkatachalam, P.M. Kannan and V. Palanisamy, "Cryptography key generation using biometrics", International Conference on Control, Automation, Communication and Energy Conservation (INCACEC), Pp. 1 – 6, 2009.

[14] Gupta, K. Sharma, M. Sharma, P., "Lossless compression based Kmp technique", Optimization, Reliability, and Information Technology (ICROIT), 2014 International Conference on , vol., no., pp.401,404, 6-8 Feb. 2014.

[15] Chaudhari, R.E.; Dhok, S.B., "Wavelet transformed based fast fractal image compression", International Conference on Circuits, Systems, Communication and Information Technology Applications (CSCITA), 2014, vol., no., pp.65,69, 4-5 April 2014.

[16] Ponomarenko, N.N.; Egiazarian, K.O.; Lukin, Vladimir V.; Astola, J.T., "High-Quality DCT-Based Image Compression Using Partition Schemes", Signal Processing Letters, IEEE , vol.14, no.2, pp.105,108, Feb. 2007.

[17] Jiantao Zhou, Xianming Liu, Oscar C. Au, Fellow, and Yuan Yan Tang, "Designing an Efficient Image Encryption-Then-Compression System via Prediction Error Clustering and Random Permutation", IEEE Transactions on information forensic and security,vol.9,No.1,january 2014**.**

[18] R. Tao, X. Meng, and Y. Wang, "Image encryption with multiorders of fractional Fourier transforms," IEEE Trans. Inf. Forensics Security, vol. 5, no. 4, pp. 734–738, Dec. 2010.

First Author Pursuing M.Tech from G.H. Raisoni college of engineering, Nagpur**,** Maharashtra, India.

Second Author working as assistant professor in G.H. Raisoni College of Engineering Nagpur, Maharashtra, India and she has published many no. of research papers in international journals and her area of interest is network security.