International Journal of Innovative Research in Technology and Management (IJIRTM), Volume-3, Issue-2, 2019
ISSN: 2581-3404 (Online)

Selective Image Encryption: Survey and Discussion

Shafeeq Ahmed[1], Prof. Hitesh Gupta[2], Prof. Vijay Kumar Trivedi[3]

[1]M. Tech Scholar, Department of CSE, LNCT, Bhopal (India)

[2]Professor, Department of CSE, LNCT, Bhopal (India)

[3]Professor, Department of CSE, LNCT, Bhopal (India)

[1]ahmedshafeeq13@gmail.com, [2]hitesh034@gmail.com, [3]vkt911@gmail.com

ABSTRACT

This Selective image encryption is a current research trend being investigated to minimize the encryption time of digital images. It does not strive for maximum security, but trades off security for computational complexity. It involves representing the most meaningful parts of an image. This paper provides an extensive analysis of selective image encryption techniques based various methods in spatial as well as frequency domain. All of the encryption process is carried out using three major encryption techniques: value substitution, scrambling positions, or a combination.

Index Terms: - Frequency Domain, Scrambling, Substitution method.

INTRODUCTION

All recently, the rapid growth in multimedia technology and the rapid increase of Internet use have introduced a great number of users to generate, transmit and store a huge amount of digital images with private information. Unfortunately, numerous potential threats violate the privacy of these contents, in both storage and transmission domains. In accordance with these growing threats, the security of digital images has become a major challenge in the digital age [1].
One of the most effective approaches to deter malicious attacks while preserving confidentiality and achieving access control of digital images is through encryption. Nevertheless, the huge size, complex structure and statistical properties of digital images make the computational overhead and processing time involved during encryption and decryption a major bottleneck, especially for real time applications.

Several encryption schemes have been proposed with respect to the approach in construction for both storage and transmission domains, which are generally categorized into full encryption and selective (or partial) encryption schemes. Encryption operation involves implementing encryption methods to entire or partial image information using either standard block ciphers like AES, DES, etc., or using stream ciphers. Furthermore, several random permutation algorithms and chaotic based cryptosystems [2] have been used to encrypt entire or partial image data.

However, the security level that is provided by the random position permutation schemes is frail under the known-text attack and several decryption methods have been proposed to recover the corresponding original image [3]. On the other hand, the main constraint of chaos based encryption schemes is that the finite accuracy of numerical calculations can lead to an arbitrarily change of major chaos properties such as the external parameters or initial conditions. Furthermore, most of chaos cryptosystems were shown some weakness against one or more attack types. Notwithstanding their performance is generally high, but their security is not likely to compete the security levels provided by standard ciphers [4].

Selective image encryption is a current research trend being investigated to minimize the encryption time of digital images. It does not strive for maximum security, but trades off security for computational complexity. It involves representing the most meaningful parts of an image. Consequently, the encryption process is carried out on the most significant bits, pixels or blocks using three major encryption techniques: value substitution, scrambling positions, or a combination.

Typically, full and selective image encryption schemes depend on whether the image is compressed or uncompressed. The original image is viewed as a two dimensional array of pixels. Full image encryption is realized by treating the two dimensional array of pixels as a one dimensional textual bit stream.

Therefore, any conventional cryptographic techniques can be applied directly to encrypt the entire bit stream or the entire compressed encoded bit stream .When selective encryption is applied on still visual image data, visual inspection methods are carried out first to determine the most meaningful optical parts of the image, according to various aspects, such as boundaries or object backgrounds, followed by encryption; other parts of the image are left unencrypted.
On the other hand, selective image encryption schemes in the compression domain are mainly accomplished in respect to the compression execution. Here, selective encryption can be carried out before compression on raw image data or during image compression stages, in addition to the partial encryption of a compressed encoded bit stream. Accordingly, in order to meet the selective encryption schemes in the compression domain, many studies have looked in to how to overcome the security and computational complexity problems of selective encryption of digital images on the different compression stages.

In this paper, the feasibility and performance of selective image is studied, The rest of this paper is organized as follows: Section II presents an overview of selective image encryption methods; finally, section III concludes the paper.

II RELATED WORK

Wherever The main idea in the image encryption is to transmit the image securely over the network so that no unauthorized user can able to decrypt the image. The image data have special properties such as bulk capacity, high redundancy and high correlation among the pixels that imposes special requirements on any encryption technique. To study and analyze more about the encryption techniques, the following literature survey has done and discussed in this chapter.

A. Region of Interest Based Selective Medical Image Encryption Using Multi Chaotic System

K Prabhavathi et.al. [5] proposes a chaos based image encryption conspire utilizing Lorentz map and Logistic condition with numerous levels of diffusion. In this work, they advise a selective-image encryption scheme composed of two chaotic systems. The method merge the usual bit flow ciphers expertise and the spatial-domain encryption of digital imagery. One of the chaotic systems used is the logistic map which is worn to produce a chaotic series. Using chaotic series the image is confused. The other chaotic system is use is the Lorenz map which is use to build a change medium P. As per the conventional bits flow ciphers expertise, using the binary stream the pixel standards of a basic image is adapted arbitrarily. Then by the permutation matrix P the customized picture is encrypted. Thus the combination of two methods enhances the safety of the encryption system successfully. in the anticipated system chaotic map is worn to provide more encryption charge and high level of safety, since chaos chart have pseudorandom assets and non-periodicity as the chaotic sign are typically noise-like and estimate some limit value as result. More security is provided in medical field, since confusion uses logistic map and diffusion uses Lorenz map.

A.. Region Based Selective Image Encryption D. K.C.Ravishankar and M.G. Venkateshmurthy

[6] proposed a technique which segments the image into regions of fixed size. These regions act as units for processing the image. Selective Encryption makes it possible to encrypt only a part of the image leaving the rest of the image unaltered. Here, the regions covering the part of the image are considered for encryption. Selective Reconstruction deals with decrypting only a part of the encrypted image. Both the methods give a fair amount of reduction in the encryption time. Once the segmentation and permutation of regions is completed, the regions are encrypted independently.

B.. 2D Sine Logistic modulation map for image encryption

Zhongyun Hua et.al.[7] introduce a new two-dimensional Sine Logistic modulation map (2D-SLMM) which is derived from the Logistic and Sine maps. Several assessment methods, including the trajectory, Lyapunov exponent and Kolmogorov entropy, have been used to evaluate the chaotic performance of 2D-SLMM. Analysis and evaluation results have shown that 2D-SLMM has the wider chaotic range,better ergodicity and hyperchaotic property, and that it has better chaotic performance than existing chaotic maps. To demonstrate the performance of 2D-SLMM in security applications, a chaotic magic transform (CMT) has been introduced. It can quickly shuffle neighboring pixels within an image. Using 2D-SLMM and CMT, we have proposed a new image encryption algorithm. The experimental results have shown that the proposed algorithm can protect different types of images with a high security level and low time complexity.

C.. A Survey on Emerging Challenges in Selective Color Image Encryption Techniques

Lahieb Mohammed Jawad and Ghazali Sulong [8] reviewed an extensive variety of literary works on selective image encryption with discussions on the difficulties of the various famous strategies, which were talked about three categories: selection region of interest, selective image encryption algorithms, and key managements. From this survey based on these categories, it can be derived the main challenge of the selective image encryption strategies that use less space for encryption but still security is low. There is a more guarantee of security for full encryption than for encryption at certain regions. Therefore, with consideration of the security problem of selective encryption, one can devise means of addressing its limitations. For instance, since colored images are better off for region segmentation, it can be used to determine the best Region of Interest (ROI), which is a viable option for addressing the security challenges of selective encryption.

D.. A Random Selective Block Encryption Technique for Secure Image Cryptography Using Blowfish Algorithm

Amandeep Kaur et.al. [9] proposed a technique for image encryption and decryption with random selective selection and Blowfish algorithm .The technique select refine part and encrypt decrypt block an algorithm for Random selective block encryption is the code block. The records are divided into set of Pixels of identical length. Some pixel blocks are selected and just the selected pixel sets are encrypted the symmetric key technique is used in this algorithm for Encoding and decoding are used by the identical key in both parts. Random the randomly selected region of image is taken for compression of image .the selected refined region is further process for reducing PSNR, MSER while with encryption and decryption process.

E.. Color Image Encryption by Component Based Partial Random Phase Encoding

Shyamli Jain, Ajay Khunteta [10] proposed an encryption and decryption idea on colour image by using component based Partial Random Phase Encoding (PRPE) and Fractional Fourier Transformation. The encoding converts the input RGB colour image into HSV (Hue, Saturation, Value) format. In the formation of HSV, the order of Hue and Saturation contains phase masking of higher same order while V consists of lower order than H and S. A Fractional Fourier transform pretend as a key which offers extra degree of security in different orders. By using correct keys and Fractional orders, primary images can be recovered. The HSV image has reverted back to the RGB format again in decryption method. The level of encryption of various techniques compute the robustness of image and it is verified by mean square error (MSE) as well as peak signal to noise ratio (PSNR) value. Simulation results of versatile analysis shows that this algorithm provides high security and resourceful for colour image.

F. . A New Chaotic Image Encryption Algorithm

F. Haojiang Gao et.al. [11] have proposed a new image encryption scheme based on a chaotic system. It is based on power and tangent function instead of linear function. It uses chaotic sequence generated by NCA map to encrypt image data with different keys for different images. plain- image image can be encrypted by use of XOR operation with the integer sequence.

G.. A New Modified Version of Advanced Encryption Standard Based Algorithm for Image Encryption

A. Seyed Hossein Kamali, Reza Shakerian [12] proposed a new encryption scheme as a modification of AES algorithm based on both Shift Row Transformations. In this if the value in the first row and first column is even, the first and fourth rows are unchanged and each bytes in the second and third rows of the state are cyclically shifted right over different number, else the first and third rows are unchanged and each byte of the second and fourth rows of the state are cyclically shifted left over different number of bytes..Experimental result shows that that MAES gives better encryption results in terms of security against statistical attacks and increased performance.

H.. New algorithm for color image encryption using chaotic map and spatial bit level permutation

J. Rui liu, Xiaoping tian " [13] proposed a new algorithm for color image encryption using chaotic map and spatial bit-level permutation (SBLP).Firstly, use Logistic chaotic sequence to shuffle the positions of image pixels, then transform it into a binary matrix and permute the matrix at bit-level by the scrambling mapping generated by SBLP. then use another Logistic chaotic sequence to rearrange the position of the current image pixels. Experimental results show that the proposed algorithm can achieve good encryption result and low time complexity, This makes it suitable for securing video surveillance systems, multimedia applications and real-time applications such as mobile phone services.

I. . Medical Imaging Security Using Partial Encryption and Histogram Shifting Watermarking

Hiba Abdel-Nabi and Ali Al-Haj [14] proposed a simple and efficient joint reversible data hiding and encryption algorithm for watermarking medical images while providing high embedding capacity. The proposed algorithm combines reversible data hiding techniques with standard encryption techniques in order to provide the needed security of transmitted and stored medical images. The algorithm utilizes substitution-based encryption and transposition-based encryption to achieve high degree of entropy in the encrypted watermarked images. The operation of the algorithm is based on dividing the original medical image randomly into two halves, each of which is assigned a different watermark. One of the watermarks is embedded before encryption and the other watermark is embedded after encryption. Aside from providing high entropy, the proposed algorithm provides relatively high embedding capacity because of the existence of two watermarks, while keeping low computational complexity.

J. . A Novel Selective Encryption DWT-based Algorithm for Medical Images

Med Karim Abdmouleh et.al. [15] presents a new approach to crypto-compression of medical images , which consists in applying partial encryption in the components of the DWT matrix. The basic idea of this approach takes advantage of the fact that after application of the DWT on an image, a large part of the energy is concentrated in the sub-band LL. This approach is secure and compatible with the JPEG2000 standard. Its main advantages are speed and efficiency. Indeed, it allows to considerably reduce the processing time in the encryption-decryption process thus ensuring the optimization of transmission and secure storage of medical images. This is due to the fact that only 6.25% of the DWT matrix coefficients are encrypted in this approach. Moreover, it is effective since it provides encrypted images that are not interpretable medically even after attack.

K.. Partial Image Encryption using block wise shuffling and chaotic map

Panduranga H T et.al [16] presents a partial image encryption based on block wise shuffling with the help of chaotic map.Pixel positions are permuted with in the block by using chaotic map. Partial encrypted images are obtained by selecting the different block size .their method work as follows: Input image is taken of size nxn and Initial block size is 4x4 means that input image is divided into several 4x4 blocks and pixel values in this blocks are shuffled using choatic map to get partial encrypted image, in order to get different partial encrypted images they select different block size and each time previous partially encrypted image act as a input image. The MSE and NPCR comparison of proposed technique with the existing encryption techniques shows that the proposed technique gives better security than the existing techniques. Decryption follows the reverse process of encryption. The analysis and experimental results show that the proposed scheme can achieve the concept of partial encryption.

After reading the literatures, we find some problem in the previous image encryption and decryption algorithm. The majority of them are Scrambling algorithms based on pixel exchanging, which cannot change the histogram of an image. Hence, their Security performances are not good. Also, there is no Scrambling algorithm that can give attention to both the pixel exchanging and gray level exchanging simply. Some of the techniques are value transformation based algorithm. It changes the pixel value making the image meaningless, but after transformation still the relation between pixel is exit. The total keys size and computation used in previous algorithm is very large. So time complexity is high. . On the basis of study of all the above mentioned research papers thoroughly, the following suggestions can be drawn: To protect multimedia contents, combination of pixel permutation and pixel substitution based algorithm should be implemented. More complex & compressed algorithm should be used to provide high speed and security to the System. Modified version of various algorithms is used to increase the security level.

III CONCLUSION

This paper provides an extensive analysis of selective image encryption techniques based various methods in spatial as well as frequency domain. Most works in this domain use pixels based permutation by using chaos-based techniques and other random permutation methods. However, while such encryption schemes provide an efficient performance, security levels are not likely to compete with the security levels provided by standard ciphers which are less affected by attacks. Thus, selective encryption of visual images based on symmetric ciphers is a more acceptable trade-off between security and performance.

REFERENCES:-

[1] L. Tang, Methods for Encrypting and Decrypting MPEG Video Data Efficiently , Proceedings of The 4th ACM International Conference on Multimedia, pp. 219 229, 1996.

[2] G. Jakimoski and L. Kocarev, Analysis of Some Recently Proposed Chaos-Based Encryption Algorithms , Physics Letters A, Vol. 291, No. 6, pp. 381-384, 17 December 2001.

[3] M. Ashtiyani, P. M. Birgani, and H. M. Hosseini, Chaos-Based Medical Image Encryption Using Symmetric Cryptography , 3rd International Conference on Information and Communication Technologies: From Theory to Applications (ICTTA), pp. 1-5, 7-11 April 2008.

[4] John Justin M, Manimurugan S, "A Survey on Various Encryption Techniques", (IJSCE) ISSN: 2231-2307, Volume-2, Issue-1, March 2012.

[5] K Prabhavathi, Sathisha C P, Ravikumar K M,"Region of Interest Based Selective Medical Image Encryption Using Multi Chaotic System", International Conference on Electrical, Electronics, Communication, Computer and Optimization Techniques (ICEECCOT), 2017.

[6] K.C. Ravishankar, M.G. Venkateshmurthy "Region Based Selective Image Encryption" 1-424-0220-4/06 2006 IEEE.

[7] Zhongyun Hua, Yicong Zhou, Chi-Man Pun, C.L. Philip Chen, "2D Sine Logistic modulation map for image encryption", Information Sciences—Informatics and Computer Science, Intelligent Systems, Applications, Volume 297 Issue C, March 2015 Pages 80-94.

[8] Lahieb Mohammed Jawad, and Ghazali Sulong, "A Survey on Emerging Challenges in Selective Color Image Encryption Techniques", Indian Journal of Science and Technology, Vol 8(27), DOI:10.17485/ijst/2015/v8i27/71241, October 2015.

[9] Amandeep Kaur, Gurjeet Singh, "A Random Selective Block Encryption Technique for Secure Image Cryptography Using Blowfish Algorithm", 2nd International Conference on Inventive Communication and Computational Technologies (ICICCT) 2018.

[10] Shyamli Jain, Ajay Khunteta ,"Color Image Encryption by Component Based Partial Random Phase Encoding", International Conference on Inventive Research in Computing Applications (ICIRCA),2018.

[11] H.Gao,Y.Zhang, S. Liang, D.Li "A New Chaotic Image Encryption Algorithm "Chaos, Solitons and Fractals 29 (2006) 393–399.

[12] S.H. Kamali, R. Shakerian "A New Modified Version of Advanced Encryption Standard Based Algorithm for Image Encryption" 2010 International Conference on Electronics and Information Engineering (ICEIE 2010).

[13] R. liu, X. tian "New algorithm for color image encryption using chaotic map and spatial bit level permutation "Journal of Theoretical and Applied Information Technology 15 September 2012. Vol. 43 No.1, 2005 - 2012 JATIT & LLS.

[14] Hiba Abdel-Nabi and Ali Al-Haj,"Medical Imaging Security Using Partial Encryption and Histogram Shifting Watermarking", 8th International Conference on Information Technology (ICIT),2017.

[15] Med Karim Abdmouleh, Ali Khalfallah and Med Salim Bouhlel," A Novel Selective Encryption DWT-based Algorithm for Medical Images", 14th International Conference on Computer Graphics, Imaging and Visualization,2017.

[16] Panduranga H T, Dr.Naveenkumar S K, Kiran," Partial Image Encryption using block wise shuffling and chaotic map", Proceedings of International Conference on Optical Imaging Sensor and Security, Coimbatore, Tamil Nadu, India, July 2-3, 2013.