Volume 6, Issue 8, August 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Different Image Encryption Techniques-Survey and Overview

Gajendra Singh Chandel
SSSIST, Sehore, Madhya Pradesh, India

Vinod Sharma
SSSIST, Sehore, Madhya Pradesh, India

Uday Pratap Singh
MITS, Gwalior, Madhya Pradesh, India

Abstract—Rapid growth of digital communication and multimedia application increases the need of security and it becomes an important issue of communication and storage of multimedia. Image Encryption is one of the techniques that is used to ensure high security. Various fields such as medical science military in which image encryption can be used. Modern cryptography provides essential techniques for securing information and protecting multimedia data. In last some years, encryption technology has been developed quickly and many image encryption methods have been used to protect confidential image data from unauthorized access .In this paper survey of different image encryption techniques have been discussed from which researchers can get an idea for efficient techniques to be used.

Index Terms—Component, formatting, style, styling, insert. (key words)

I. INTRODUCTION

Due to some inherent feature of image like low cost and high availability, usage of communication network has increased and it becomes a reason for rapid growth of the internet in the digital world today. In our society digital images play a more significant role than the traditional texts and it need serious protection of user's privacy for all applications. So the security of digital images has become more important and attracted much attention . the security of digital image can be achieved by digital image encryption technique. Basically Image Encryption means that convert the image into unreadable format so that third party cannot interpret them. Many digital services require reliable security in storage and transmission of digital images [1].

To prevent image from unauthorized access, Encryption techniques of digital images play a very important role .Since Digital images are exchanged over various types of networks and a large part of this digital information is either confidential or private. So Encryption is the preferred technique for protecting the transmitting information. There are various encryption systems to encrypt and decrypt image data. but, it can be say that there is no single encryption algorithm which satisfies the different image types [2].

In general, most of the available traditional encryption algorithms are used for text data. Although we can use the traditional encryption algorithm to encrypt images directly, this may not be a good idea for some reasons. First, image data have their special features such as high redundancy, and high correlation among pixels. second, they are usually huge in size, that makes traditional encryption methods difficult to apply and slow to process. third, the decrypted text must be equal to the original text but this requirement is not necessary for image data because characteristic of human insight, a decrypted image containing small distortion is usually acceptable .So the algorithms that are good for textual data may not be suitable for multimedia data, Even though triple data encryption standard (T-DES) and international data encryption algorithm (IDEA) can achieve high security, they may not be suitable for multimedia applications Therefore, well known encryption algorithms such as Data Encryption Standard (DES), Advanced Encryption Standard (AES), and International Data Encryption Standard (IDEA) were built for textual data not for multimedia data [3-4].

II. VARIOUS IMAGE ENCRYPTION METHODS

There are various types of image encryption methods. The image encryption algorithms can be categories into three major groups.

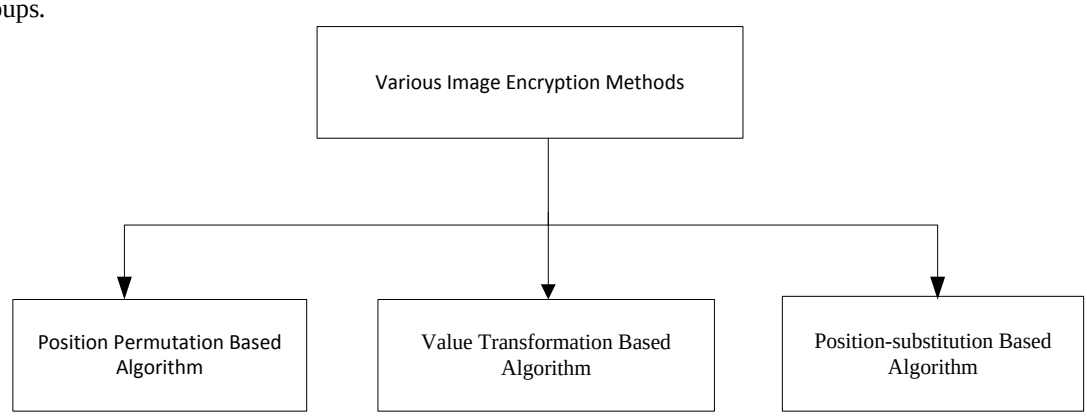

Figure 3.1 Various Image Encryption Methods.

© 2016, IJARCSSE All Rights Reserved

Position Permutation (Transposition) Based Algorithm.
Value Transformation (Substitution) Based Algorithm.
Position- Substitution Based Algorithm

A. Position Permutation (Transposition) Based Algorithm

Transposition means rearranging elements in the plain image. the rearrangement of element can be done by bit, pixel, and block wise . The permutation of bits decreases the perceptual information, whereas the permutation of pixels and blocks produce high level security. In the bit permutation technique, the bits in each pixel are permuted using the permutation keys with the key length equal to 8. In the pixel permutation, 8 pixels are taken as a group and permuted with the same size key. In this investigation the combination of block, bit, and pixel permutation are used respectively. The Position Permutation Based Algorithm is use for the various techniques.

B. Value Transformation Based Algorithm

Values Transformation Based algorithm is based on the technique in which the value of each pixel is change to some other value. The new value of pixel is evaluated by applying some algorithm on pixel .Basically algorithm is mathematical computation where we take input as a pixel value compute it, with some formulas and produce a new value for that pixel . Value Transformation Based Algorithm are Digital Signatures and Lossless Image Compression and Encryption Using SCAN, Image Cryptosystems, Color Image Encryption Using Double Random Phase Encoding, Image Encryption Using Block-Based Transformation Algorithm and affine Transform etc.

C. Position- Substitution Based Algorithm

This technique is combination of both position permutation and value transformation. Position permutation and value transformation can be combined. In this technique first pixels are reordered and then a key generator is used to substitute the pixel values. The Position-Substitution Based Algorithm is use for the various techniques

III. PERFORMANCE PARAMETERS

The performance of the encryption technique is measured by some of the basic parameters which are listed below: [6].

A. Visual Degradation (VD):

Visual degradtation identifies the perceptual distortion of the image data with respect to the plain image.

B. Compression Friendliness (CF):

Compression Friendliness measures no or very little impact on data compression efficiency on the image. Some encryption schemes impact data compressibility or introduce additional data that is necessary for decryption.

C. Format Compliance (FC):

Format Compliance parameter is used to measures compliance the encrypted bit stream with the compressor. standard decoder should be able to decode the encrypted bit stream without decryption.

D. Encryption Ratio (ER):

This measures the amount of data to be encrypted. Encryption ratio should be minimized so that the computational complexity can be reduced.

E. Speed (S):

This parameter measures how fast the encryption and decryption algorithms enough to meet real time requirements.

F. Cryptographic Security (CS):

Cryptographic security is used to identifies whether encryption scheme is secure against different plaintext-cipher text attack.

IV. LITERATURE REVIEW

In 2008 **Mohammad Ali Bani Younes and Aman Jantan** [7] proposed a block-based transformation algorithm based on the combination of image transformation and a well known encryption and decryption algorithm called Blowfish. First of all the original image was divided into blocks, Before going through an encryption process,these blocks are transformed. At the receiver side these blocks are retransformed in to their original position and decryption process is performed. Advantage of this approach, is that it reproduce the original image with no loss of information for the encryption and decryption process we used a blowfish algorithm. The results implies that when we increased the number of blocks by using smaller block sizes , decreased correlation and increased entropy.

In 2008 **Mohammad Ali Bani Younes and Aman Jantan** [8] introduced a new permutation technique based on the combination of image permutation followed by encryption I.e. well known encryption algorithm called RijnDael. Their proposed technique work as follows: The original image was divided into 4 pixels × 4 pixels blocks then the blocks were transformed into new locations which were rearranged to make a permuted image using a permutation process presented , and then the generated image was encrypted using the RijnDael algorithm. The correlation between image pixels was

© 2016, IJARCSSE All Rights Reserved

significantly decreased ,due to rearrangement of the blocks and therefore it becomes very difficult to predict the value of any given pixel from the values of its neighbors. Furthermore, this process of dividing and shuffling the positions of image blocks confuses the relationship between the original image and the generated one .At the receiver, the original image can be reproduced by the inverse permutation of the blocks.

Amitava Nag et.al. [9] proposed a two phase encryption and decryption algorithms that is based on shuffling the image pixels using affine transform and they encrypting the resulting image using XOR operation in year 2011. with the help of four 8-bit key applied, the pixel values are redistributed on different location using affine transform technique. In the next stage the transformed image divided into 2 pixels x 2 pixels blocks and every block is encrypted using XOR operation by using four 8-bit keys. The key used in this algorithm is s 64 bit long . Their results proved that after the affine transform the correlation between pixel values was significantly decreased.

Yicong Zhou and Sos Agaian [10] introduces a new method of applying the image steganography concept for image encryption. They used the concept of e PLIP (Parameterized Logarithmic Image Processing) addition to embed the scrambled original image into a selected cover image, it generates an encrypted image. The parameterized logarithmic image processing (PLIP) model is a mathematical framework based on set of precise operations that can be applied to the processing of intensity images valued in a bounded range. Result analysis shows that the algorithm has a very large key space and can withstand several common attacks.

In 2011 **Yun sen and Gunayi Wang** [11] proposed a modified chaotic map technique In order to improve the security of chaotic encryption algorithm. One of the advantage of their technique is that when we compared it with original logistic map, their proposed map makes it always be chaotic, and expands the iteration range from original (0, 1) to (0, 4λ) (λ>0.25). This is important for expanding key space of chaotic sequence and enhancing rate of change of chaotic signal. An encryption algorithm is designed based on this chaotic map and some analysis is presented to show its good efficiency. Experimental results show that the modified Logistic map possesses faster encryption , faster sequence generation rate , bigger key space and speed against the original logistic map in 2011.

In 2012 **Qiudong Sun et.al.** [12] presented a random scrambling algorithm based on bit-planes decomposition of image. Their Algorithm starts by decomposing a gray image into bit-plane images, each image for saperate bit plane . In the next step every bit plane image is shuffled by using a random scrambling algorithm. At last , all the shuffled bit plane images are merged according to their original levels on bit-planes and we obtained an encrypted image. Experimental results show that the proposed algorithm scrambled an image effectively as well as changed its histogram apparently. It has better efficiency and properties than the general random scrambling method. Therefore it has more stable scrambling degree than the classical method like Arnold transform.

In 2012 **Sukalyan Som and Atanu Kotal** [13] presented multiple chaotic maps based a new symmetric image encryption algorithm. In the proposed algorithm, with the help of generalized Arnold Cat Map , the plain image is first scrambled. Further, the scrambled image at a particular iteration is encrypted using chaotic sequences generated by one-dimensional Logistic Map after preprocessing them to integers. The results indicates that the proposed algorithm can successfully encrypt and decrypt grayscale images with secret keys. it also exhibit that the proposed method is secure , loss-less, and efficient .

In 2013 **A.Kester** [14] proposed a new technique that contribute to the general body of knowledge in the area of cryptography application by developing a new cipher algorithm for image encryption of m*n size by shuffling the RGB pixel values. With the help of RGB pixels ,this algorithm ultimately encrypts and decrypts the images. The algorithm was implemented using MATLAB. In this method, neither the bit values of the pixel are affected and nor pixel expansion at the end of the encryption and the decryption process. In place of the numerical values are transposed, reshaped and concatenated with the RGB values , it shifted away from its respective positions and the RGB values interchanged in order to obtain the cipher image. This shows that, the total change in the sum of all values in the image is zero. Therefore there is no change in the total size of the image during encryption and decryption process. Advantage of their method is that the characteristic sizes of image will remain unchanged, while the encryption process is being performed.

V. PERFORMANCE COMPARISON IN TABULAR FORM

This section presents performance and comparison among image encryption schemes with respect to various parameters as shown in Table 1

Table 1 Comparison of Different Encryption methods:

Encryption Technique	Method used	Advantages	Disadvantages
Encryption Image Encryption Using Block-Based Transformation Algorithm,2006	original image is divided into blocks, which are rearranged into a transformed image using a transformation algorithm presented, and then the transformed image was encrypted using the Blowfish algorithm.	No key generator, correlation between image elements decreased and higher entropy.	Image loosing and lower Correlation, no standard technique is used for block transformation.
A Combination Of Permutation Technique	First pixels is shuffles based on permutation techniques used and	Higher Entropy and Correlation	Permutation process is too complex, Time taking and

© 2016, IJARCSSE All Rights Reserved

Followed By Encryption, 2008	then shuffled pixels is encrypted using RijnDael algorithm.	between image elements decreased	also chances of mistakes are high
Image Encryption Using AffineTransform And XOR Operation, 2011	redistribute the pixel values to different location using affine transform technique transformed image is then encrypted using XOR operation	Better Solution and Correlation between pixels values significantly ecreases	Lengthy ,complicated,Time Consuming and chances of mistakes is high.
Image Encryption Using the Image Steganography Concept and PLIP Model, 2011	To encrypt to original image it is embedded into the cover image, it fuses the scrambled original image with the cover image using the PLIP addition via specific parameters.	Large key space, can withstand several common attacks.	Due to lots of mathematical computational ,it takes long time to encrypted the image , correlation between pixels still exists;
An Image Encryption Scheme Based on Modified Logistic Map,2011	a modified chaotic map, which is based on the Logistic map, is used for image encryption	bigger key space, faster sequence generation rate, faster encryption speed	Due to its its high-level simplicity, possible to decrypt image, correlation between pixes exists , sensitive to initial values.
Image Encryption Based on Bit-plane Decomposition and Random Scrambling,2012	Decomposes a gray image into several bit-plane images Then shuffles them by a random scrambling algorithm separately. Lastly, merges the scrambled bit-plane images according to their original levels on bit-planes and gained an encrypted image	better efficiency, more stable scrambling degree than the classical method, image histogram is changed apparently,	Very time consuming , Some sort of security problem , Key is sensitive to crack. No ecific technique is used for scrambling .
Confusion and Diffusion of Grayscale Images Using Multiple Chaotic Maps,2012	the plain image is first scrambled using generalized Arnold Cat Map. Further, the scrambled image at a particular iteration is encrypted using chaotic sequences generated by one-dimensional Logistic Map	loss-less; secure and efficient; low correlation among pixels; a very large key space; high sensitivity to secret keys;	Time taking and risky, no changes in shuffled histogram , quality of encryption is low.
A cryptographic Image Encryption technique based on the RGB PIXEL shuffling, 2013	image encryption by shuffling the RGB pixel values.	effective in terms of the security analysis, increase of security of the image against all possible attacks	R,G,and B Pixels shuffling takes more times then other metods, Lot of confusion in process, Permutation process is too complex, Time taking and alsochances of mistakes are high

VI. CONCLUSION

After studying the papers, we conclude that some problem in the previous image encryption and decryption algorithms are exists. First of all the majority of encryption algorithm are based on Scrambling algorithms in which pixel exchanging happened. This scheme encrypts the image but cannot change the histogram of an image. So, their Security performances may not good. 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 exists. Also, there is no encryption algorithm exists that can give attention to both the pixel exchanging and gray level exchanging concept. In addition to these there are some other problem exists such as 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, the following suggestions can be drawn: To protect multimedia contents, pixel permutation based algorithm should be implemented or used . 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.

REFERENCES

[1] I. Öztürk and I. Sogukpınar, "Analysis and comparison of image encryption algorithms", Transactions on Engineering, Computing and Technology, vol. 3, pp. 1305-5313, 2004.

[2] Aloha Sinha, Kehar Singh, "A technique for image encryption using digital signature", Optics Communications, Vol-2 I 8 (2203),229-234.

© 2016, IJARCSSE All Rights Reserved

[3] V. Potdar and E. Chang, "Disguising text cryptography using image cryptography", International Network Conference in Plymouth, UK, 6 - 9 July, 2004.

[4] X. Li, J. Knipe, and H. Cheng, ," Image Compression and Encryption Using Tree Structures" , Pattern Recognition Letters, Vol. 18, No. 8, pp. 2439 2451, 1997.

[5] Marwa Abd El-Wahed, Saleh Mesbah, and Amin Shoukry," Efficiency and Security of Some Image Encryption Algorithms", , Proceedings of the World Congress on Engineering, London, U.K,.Vol I 2008 .

[6] Payal Sharma, Manju Godara, Ramanpreet Singh ," Digital Image Encryption Techniques: A Review", International Journal of Computing & Business Research, 2012.

[7] Mohammad Ali Bani Younes and Aman Jantan," Image Encryption Using Block-Based Transformation Algorithm", IAENG International Journal of Computer Science, 35:1, IJCS_35_1_03,2006.

[8] Mohammad Ali Bani Younes and Aman Jantan ,"an image encryption Approach using a combination of permutation technique followed by Encryption", International Journal of Computer Science and Network Security, VOL.8 No.4, April 2008.

[9] Amitava Nag, Jyoti Prakash Singh, Srabani Khan, Saswati Ghosh, Sushanta Biswas, D. Sarkar Partha Pratim Sarkar, "Image Encryption Using Affine Transform and XOR Operation",IEEE International Conference on Signal Processing, Communication, Computing and Networking Technologies, 2011.

[10] Yicong Zhou, Sos Agaian," Image Encryption Using the Image Steganography Concept and PLIP Model", Proceedings of 2011 International Conference on System Science and Engineering, Macau, China - June 2011.

[11] Yue Sun, Guangyi Wang," An Image Encryption Scheme Based on Modified Logistic Map", Fourth International Workshop on Chaos-Fractals Theories and Applications,2011.

[12] Qiudong Sun, Wenying Yan, Jiangwei Huang, Wenxin Ma," Image Encryption Based on Bit-plane Decomposition and Random Scrambling", 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet), 2012 .

[13] Sukalyan Som, Atanu Kotal," Confusion and Diffusion of Grayscale Images Using Multiple Chaotic Maps", National Conference on Computing and Communication Systems (NCCCS),2012.

[14] Quist-Aphetsi Kester," A cryptographic Image Encryption technique based on the RGB PIXEL shuffling", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 2, January 2013.

© 2016, IJARCSSE All Rights Reserved