Image Encryption methodology: A survey of the state of the art

[1]Pragya Tiwari, [2]Pradeep Tripathi

Department of Computer Science and Engineering,
Vindhya Institute of Technology & Science, Satna (M.P)

***Abstract*: In present days security is main concern during transmission of information in many places such as banking, marketing, Ecommerce. Encryption is the field which provides the security during transmission of information. This papers discuss the various techniques developed for image encryption. This study extends to the performance parameters used in encryption processes and analyzing on their security issues and also useful for the researchers to carry out further enhancement of the present methods.**

***Keywords*: image encryption, DNA encoding, Scan plans, chaotic system,**

I. INTRODUCTION

In the recent years the rapid growth in transmission of information such as text, multimedia data over internet and local networks and local area networks and use of this system has encouraged activities such as unauthorized access, illegal usage, and disruption, alteration of transmitted and stored data. Security concerns with regards to such data transmission and storage has been a major concern of both the transmitters and receivers. Encryption is one of the best solution for security during transmission and storage [1-2].

Encryption is the process of transforming a piece of information (known as the plaintext) using an algorithm (known as the cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key. The output is known as the cipher text. The reverse process of transforming cipher text to plaintext is known as decryption (sometimes called as decipherment) [3-4]. Encryption and decryption process is as shown in figure 1.

In this paper we discuss the different approaches that have been developed in the past for encrypting the image. Images are different from text. Although we may use the traditional cryptosystems to encrypt images directly, it is not a good idea for two reasons. One is that the image size is almost always much greater than that of text. Therefore, the traditional cryptosystems need much time to directly encrypt the image data. The other problem is that the decrypted text must be equal to the original text. However, this requirement is not necessary for image data. Due to the characteristic of human perception, a decrypted image containing small distortion is usually acceptable [5-6].

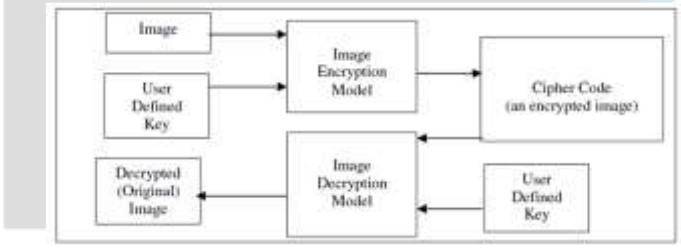

Figure 1: Block Diagram of Image Encryption and Decryption Process

II. SELECTIVE AND NON SELECTIVE METHOD

Most of the algorithms specifically designed to encrypt digital images are proposed in the mid-1990s. There are two major groups of image encryption algorithms: (a) non chaos selective methods and (b) Chaos based selective and non-selective methods. Most of these algorithms are designed for a specific image format compressed or uncompressed, and some of them are even format compliant. There are methods that offer light encryption (degradation), while others offer strong form of encryption [7].

In this section we discussed some of the existing methods based on both chaotic and non chaotic methods for the image encryption.

Jiun et al. [3] have presented an algorithm which was mirror like. In this algorithm there were 7 steps. In the first, 1-D chaotic system is determined and its initial point x (0) and sets k = 0. Then, the chaotic sequence is generated from the chaotic system. After that binary sequence is generated from chaotic system. And in last 4 stages image pixels are rearranged using swap function according to the binary sequence.

Fethi et al. [8] used the method that can be used for binary images encryption with the possibility of using several keys ex: initial state, the external parameters and iterations' number. Guosheng et al.[9] made a new highly optimised image algorithm using permutation and substitution methods. It was done in order to enhance the pseudorandom characteristics of chaotic sequences, an optimized treatment and a cross-sampling disposal is used.

Huang et al. [10] made an algorithm using two chaotic systems. One chaotic system generates a chaotic sequence, which was changed into a binary stream using a threshold function. The other chaotic system was used to construct a permutation matrix. Firstly, using the binary stream as a key stream, randomly the pixel values of the images was modified. Then, the modified image was encrypted again by permutation matrix. Aradhana et al. developed a hybrid algorithm are image encryption which used 1D logistic map for permutation and DNA encoding is used for diffusion. They found that the hybrid approach is more attractive as compare to the single images [7]

III. BLOCK BASED TRANSFORMATION

The transformation process refers to the operation of dividing and replacing an arrangement of the original image. The image can be decomposed into blocks; each one contains a specific number of pixels. The blocks are transformed into new locations. For better transformation the block size should be small, because fewer pixels keep their neighbors. In this case, the correlation will be decreased and thus it becomes difficult to predict the value of any given pixel from the values of its neighbors. At the receiver side, the original image can be obtained by the inverse transformation of the blocks [11]. A algorithm of the transformation method is given below.

The transformation technique works as follows: the *original* image is divided into a random number of blocks that are then shuffled within the image. The generated (or transformed) image is then fed to the Blowfish encryption algorithm [11]. The main idea is that an image can be viewed as an arrangement of blocks. The intelligible information present in an image is due to the correlation among the image elements in a given arrangement. This perceivable information can be reduced by decreasing the correlation among the image elements using certain transformation techniques. The secret key of this approach is used to determine the seed. The seed plays a main role in building the transformation table, which is then used to generate the transformed image with different random number of block sizes [12-13].

Amitava et, al. introduced a new algorithm using affine transform and was based on shuffling the image pixels. It was two phase encryption decryption algorithm. Firstly using XOR operation they encrypted the resulting image and then using the affine transformation, the pixel values were redistributed to different locations with 4 bit keys. The transformed image then divided into 2 pixels x 2 pixels blocks and each block is encrypted using XOR operation by four 8-bit keys. The result proves that the correlation between pixel values was significantly decreased after the affine transform [14].

Chang-et al. [15] proposed an algorithm which was multilevel form of image encryption using binary phase exclusive OR operation and image dividing technique. The same grey level multi-level image is divided into binary images. Then binary pictures is regenerate to binary phase encoding and then these images are encrypt with binary random phase images by binary phase XOR operation

IV. IMAGE ENCODING

Chin et al. [16] used vector quantization for designing better cryptosystem for images. The scheme was based on vector quantization (VQ), cryptography, and various others number theorem. In vector quantization (VQ) firstly the images are decomposed into vectors and then sequentially encoded vector by vector. . Then traditional cryptosystems from commercial applications can be used.

Shuqun et al. [17] have proposed a new method to encrypt color images using existing optical encryption systems for gray-scale images. The color images are converted to their indexed image formats before they are encoded. In the encoding subsystem, image is encoded to stationary white noise with two random phase masks, one in the input plane and the other in the Fourier plane. At the decryption end, the color images are recovered by converting the decrypted indexed images back to their RGB (Red-Green-Blue) formats. The proposed single-channel color image encryption method is more compact and robust than the multichannel methods.

V. OTHER METHODS

Maniccam et al. [18] have presented a new algorithm which does two works: lossless compression and encryption of binary and gray-scale pictures. The compression and encryption schemes are based on SCAN patterns generated by the SCAN methodology. The SCAN is formal language-based 2D spatial-accessing methodologies generate a wide range of scanning paths or space filling curves.

Zeghid, et al. [19] analyze the Advanced Encryption Standard (AES), and in their image encryption technique they add a key stream generator (W7,A5/1) to AES for ensuring the encryption performance. Kamali et al. [18] presented a modification to the Advanced Encryption Standard (MAES) to provide a high level security and better image encryption. The result shown by them was higher than that of original AES encryption algorithm.

Sesha et al. [20] introduced an algorithm on the basis of random pixel permutation with the motivation to maintain the quality of the image. It had three phases in the process of encryption. The phase one was the image encryption. The phase two was the key generation phase. And the phase three was the identification process. This provide confidentiality to colour image with less computations. Rasul et al. [21] proposed a new method based on a hybrid model composed of a genetic algorithm and a chaotic

function for image encryption. In their technique, first a number of encrypted images are constructed using the original image with the help of the chaotic function. In the next stage, these encrypted images are employed as the initial population for starting the operation of the genetic algorithm. Then, the genetic algorithm is used to optimize the encrypted images as much as possible. In the end, the best cipher-image is chosen as the final encryption image.

VI. CONCLUSION

Nowadays, the security for the data has become extremely important since the communication by transmitting of digital products over the open network occur very often. In this paper, various works on the encryption techniques are studied and analyzed well to promote the performance of the encryption methods also to ensure the security proceedings. Each technique has its merits and demerit, which might be suitable for different applications. Everyday new encryption technique is evolving hence fast and secure conventional encryption techniques will always work out with high rate of security. From this studied it is also found that the use of hybrid technique is more efficient as compare to the individual.

REFERENCES

[1] John Justin M, Manimurugan S , "A Surve on Various Encryption Techniques ", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-1, March 2012.

[2] Ephin M, Judy Ann Joy and N. A. Vasanthi, " Survey of Chaos based Image Encryption and Decryption Techniques " , Amrita International Conference of Women in Computing (AICWIC'13) Proceedings published by International Journal of Computer Applications (IJCA).

[3] Jiun-In Guo, Jui-Cheng Yen, "A new mirror-like image Encryption algorithm and its VLSI architecture", Pattern Recognition and Image Analysis, vol.IO, no.2, pp.236-247, 2000.

[4] Aradhana Soni & Anuja Kumar Acharya; A Novel Image Encryption Approach using an Index based Chaos and DNA Encoding and its Performance Analysis; International Journal of Computer Applications (IJCA); Volume 47 - Number 23; 2012.

[5] Z.Li F.Sun, S.Liu and Z.L. A novel image encryption scheme based on spatial chaos map. chaos. Solitons and Fractals, 38(2):631–640, April/June 2008.

[6] Shiguo Lian Ljupco Kocarev. Chaos-based cryptography: theory, algorithm and application. Version 2.5. Springer, Point Roberts, WA, USA, 2011.

[7] Xianglian Xue Xiaopeng Wei Qiang Zhang, Ling Guo. An image encryption algorithm based on dna sequence addition operation. In IEEE, 2009.

[8] Fethi Belkhouche and Uvais Qidwai , "Binary image encoding using 1D chaotic maps", IEEE Proceeding in the year 2003.

[9] Guosheng Gu ,Guoqiang Han, "An Enhanced Chaos Based Image Encryption Algorithm", IEEE Proceedings of the First International Conference on Innovative Computing, Information and Control (ICICIC'06) in 2006.

[10] Huang-Pei Xiao Guo-Ji Zhang, "An Image Encryption Scheme Based On Chaotic Systems", IEEE Proceedings of the Fifth International Conference on Machine Learning and Cybernetics, Dalian, 13-16 August 2006.

[11] Mohammad Ali; Bani Younes and Aman Jantan. Image encryption using block-based transformation algorithm. IAENG International Journal of Computer Science, 35:1–3, 2008.

[12] Mohammad Ali Bani Younes and Aman Jantan, "An Image Encryption Approach Using a Combination of Permutation Technique Followed by Encryption" , IJCSNS International Journal of Computer Science and Network Security, VOL.8 , April 2008.

[13] Seyed Mohammad Seyedzade, Reza Ebrahimi Atani and Sattar Mirzakuchaki, "A Novel Image Encryption Algorithm Based on Hash Function", 6th Iranian Conference on Machine Vision and Image Processing, 2010.

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

[15] Chang-Mok Shin, Dong-Hoan Seo, Kyu-Bo Chol, Ha-Wmn Lee, and SmJmng Kim, " Multilevel Image Encryption by Binary Phase XOR Operations", IEEE Proceeding in the year 2003.

[16] Chin-Chen Chang, Min-Shian Hwang, Tung-Shou Chen, "A new encription algorithm for image cryptosystems ", The Journal of Systems and Software 58 , 83-91,2001. Rinki Pakshwar et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 4 (1) , 2013, 113 - 116 www.ijcsit.com 115.

[17] Shuqun Zhang and Mohammed A. Karim, "Color image encryption using double random phase encoding", Microwave and Optical Technology Letters Vol. 21, No. 5, 318-322 , June 5 1999.

[18] S.S.Maniccam, N.G. Bourbakis, "Lossless image compression and encryption using SCAN", Pattern Recognition 34,1229-1245,2001.

[19] M. Zeghid, M. Machhout, L. Khriji, A. Baganne,R. Tourki, "A Modified AES Based Algorithm for Image Encryption", World Academy of Science, Engineering and Technology 27, 2007.

[20] Sesha Pallavi Indrakanti,P.S.Avadhani, "Permutation based Image Encryption Technique", International Journal of Computer Applications (0975 – 8887) Volume 28 ,No.8, 2011.

[21] Rasul Enayatifar , Abdul Hanan Abdullah, "Image Security via Genetic Algorithm", 2011 International Conference on Computer and Software Modeling IPCSIT vol.14.