Volume 3, Issue 1, January 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Image Encryption using Hybrid Genetic Algorithm

Shubhangini P.Nichat*, Prof.Mrs.S.S.Sikchi
M.E.II.nd Year, Department of Information Technology
PRMIT COET, SGB Amravati University, India.

Abstract*— *security of image is the serious issue now-a- days because of ever increases in multimedia development and brute force attacks. In this paper we are introducing a best hybrid model for image encryption composed of genetic algorithm and chaotic function. In the first stage of proposed method number of encrypted images is constructed using secret key and chaotic function. In the next stage, these encrypted images are used as initial population for genetic algorithm. In this proposed method genetic algorithm is used to obtain optimum result and in the last stage best cipher image is selected based on calculation of correlation coefficient and entropy. The image having lowest correlation coefficient and highest entropy is selected as best cipher image.

In this paper first time we are using genetic algorithm for encryption of images. Entropy and correlation coefficient obtained by using this method are 7.9978 and -0.0009 respectively.

Keywords—*chaotic function, genetic algorithm, correlation coefficient, entropy, secret key.*

I. INTRODUCTION

Owing to the advance in network technology, image security is an increasingly important problem. Popular application of multimedia technology and increasingly transmission ability of network gradually lead us to acquire information directly and clearly through images. Hence, image security has become a most critical issue. Image encryption techniques try to convert an image to another image that is hard to understand; to keep the image confidential between users, in other word, it is essential that nobody could get to know the content without a key for decryption. Furthermore, special and reliable security in storage and transmission of digital images is needed in many applications, such as pay-TV, medical imaging systems, military image communications and confidential video conferences, etc. In order to fulfill such a task, many image encryption methods have been proposed, but some of them have been known to be insecure, so we always in need to develop more and more secure image encryption techniques. Traditional data encryption techniques can be divided into two categories which are used individually or in combination in every cryptographic algorithm: substitution and transposition. In substitution technique, we symmetrically replace one symbol in the data with another symbol according to some algorithm; in a transposition technique, we reorder the position of symbols in the data according to some rule. Image encryption approaches fall into two broad categories: spatial domain methods and frequency domain methods. The term spatial domain refers to the image plane itself, and approaches in this category are based on direct manipulation of pixels in an image. In these algorithms, the general encryption usually destroys the correlation among pixels and thus makes the encrypted images incompressible. Frequency domain processing techniques are based on modifying the Fourier transform of an image. The Fourier transform can be reconstructed (recovered) completely via an inverse process insecure, so we always in need to develop more and more secure image encryption techniques. Chos theory is exists in many research areas have many benefits in the area of image encryption.choatic signals is having any advantages as sensitivity to initial condition, deterministic work, apparently accidental feature. Chaotic signals is having random, unpredictable behavior because of these advantages many researcher believe that this signal is having great advantages in the area of image encryption.

Genetic algorithm is the one type of search algorithm used in proposed method for optimization purpose. In the proposed method first plain input image divided into four equal parts and key is extracted from each part of image. Extracted key and chaotic function is then used to encrypt part of image. In this way initial population is formed which is used as input to the genetic algorithm.

II. LITERATURE REVIEW

Spatial domain:

Jiri Fridrich in 1997 has proposed an Block encryption algorithm in which certain invertible chaotic two-dimensional maps such as standard map, cat map, baker map is adapted to create new symmetric block encryption schemes..This scheme is especially useful for encryption of large amount of data, such as digital images also this scheme achieve lossless encryption with good sensitivity to change in key and exhibit good mixing property. Security analysis is not efficiently given in this work. To overcome disadvantage of this scheme a 2-D baker is first extended to 3-D and it then used to increase speed of security [1].

Jiun-In Guo and Jui-Cheng Yen in 1999 have presented an efficient mirror-like image encryption and visual cryptography algorithm based on a binary sequence generated from a chaotic system, an image is scrambled according to the algorithm. This algorithm consists of seven steps. Step 1 determines 1D chaotic system ant its initial point x(0) and

sets k=0.step 2generate the chaotic sequence from the chaotic system. step3 generates binary sequence from chaotic system. Step 4,5,6 and 7 rearrange image pixels using swap function. This algorithm possesses low computational complexity, high security and no distortion [2].

Jui-Cheng Yen and Jim-In Guo, in 2000 have proposed an image encryption/decryption algorithm and its VLSI architecture . According to a chaotic binary sequence, the gray level of each pixel is XORed or XNORed bit-by-bit to one of the two predetermined keys. Its features are as follows: (1) low computational complexity, (2) high security, and (3) no distortion [3].

Sobhy in 2001 used Lorenz equation for encryption, creating secure databases; secure Email, implemented in FPGA for real time images. In this paper the chaotic algorithm is used for encrypting text and images[4][5].

Chang-Mok Shin**,** Dong-Hoan Seo**,** Kyu-Bo Chol, Ha-Wmn Lee, and SmJmng Kimin 2002 have proposed the multi level image encryption in which binary phase exclusive OR operation and image dividing technique is used for encryption. First the multi level image having same gray levels are divided into binary images Then converted binary images to binary phase encoding and then encrypt these images with binary random phase images by binary phase XOR operation. By combining each binary encrypted images encrypted gray image was then obtained.

Aloka Sinha and Kehar Singh in 2003 have proposed a new technique for secure image transmission The digital signature of the original image is added to the encoded version of the original image. An appropriate error control code, such as a Bose-Chaudhuri Hochquenghem (BCH) code is used for image encoding . At the receiver end, after the decryption of the image authenticity. of image is verified by using digital signature. In the first step, an error control code is used which is determined in real-time, based on the size of the input image. Without the knowledge of the specific error control code, it is very difficult to obtain the original image and tamper with it. The dimension of the image also changes due to the added redundancy. This poses an additional difficulty to decrypt the image. Also, the digital signature is added to the encoded image in a specific manner. This information can be protected to make the system more secure. At the receiver end, the digital signature can be used to verify the authenticity of the transmitted image. A digital correlation technique or an optical correlator, in either the JTC or the VanderLugt geometry can be used to verify the authenticity of the decrypted image. This clearly solves the problem of image recovery and image degradation, unlike the previous methods. The added advantage is that there is no need to transmit the Keys separately [6].

Chang-Mok Shin**,** Dong-Hoan Seo**,** Kyu-Bo Chol, Ha-Wmn Lee, and SmJmng Kim in 2003 proposed the multi level image encryption by using binary phase exclusive OR operation and image dividing technique. The multi level image can be divided into binary images that have same gray levels. They converted binary images to binary phase encoding and then encrypt these images with binary random phase images by binary phase XOR operation. Encrypted gray image was then obtained by combining each binary encrypted images [7].

In 2003 Fethi Belkhouche and Uvais Qidwai used one dimensional chaotic map. It has been shown that the method can be used for binary images encryption with the possibility of using several keys such as the initial state, the external parameters and the number of iterations. It is also shown that the sensitivity to initial state plays an important role in chaotic encryption. Disadvantages of this scheme are small key space and weak security [8].

Zhang Han, Wang Xiu Feng, proposed in 2004 ,a novel image encryption scheme based on nonlinear chaotic map(NCM).There are two rounds in proposed image encryption scheme In each round the pixel gray value are modified from first pixel to last pixel firstly and modified pixel is encrypted from last pixel to first pixel in the inverse order .In order to accelerate encryption speed ,every time NCM is iterated. Failure of encryption owing to self similarity and visional psychological characteristics of image. Image encryption based on NCA shows the advantages of large key space , high-level security and good efficiency[9].

M.-R. Zhang, G.-C. Shao and K.-C. Yi in 2004used a T-matrix for image scrambling and its periodicity has been proved. The T-matrix has a simple conformation and a period twice as long as the Arnold matrix. It can be applied to image encryption and pre-processing in image processing such as image watermarking algorithms[10] .

In 2005 , Deng Shaojiang completed an image encryption by a chaotic neural system and the cat map. In this paper ,Liao's chaotic neural system, cat map and general cat map are introduced and analyzed respectively. Then new image encryption scheme by employing the Liao's chaotic system to generate parameters of general cat map is designed. In this paper ,general cat map is employed to shuffle the position of image pixels and another chaotic map is used to confuse the relationship between cipher image and plain image .The general Cat map's parameter are derived from the time delay chaotic neural system. The main advantage of this image encryption scheme are high security and fast speed.

Guosheng Gu and Guoqiang Han in 2006 incorporate permutation and substitution methods together, to present a strong image encryption algorithm .An optimized treatment and a cross-sampling disposal have been introduced for enhancing the irregular and pseudorandom characteristics of chaotic sequence[11]

Huang-PeiXiao , Guo-ji Zang in 2006 proposed scheme using two chaotic systems based on the thought of higher secrecy of multi-system. One of the chaotic systems is used to generate a chaotic sequence. Then this chaotic sequence was transformed into a binary stream by a threshold function. The other chaotic system was used to construct a permutation matrix. Firstly, the pixel values of a plain image have been modified randomly using the binary stream as a key stream. Secondly, the modified image was encrypted again by permutation matrix[12].

Frequency domain:

In 2000 , Cheng and Li proposed partial encryption to reduce encryption and decryption time in image processing. We have found two classes of algorithms that are suitable for partial encryption i) quardtree compression algorithm. ii) wavelet compression algorithm based on zerotrees having good compression performance.Both type of algorithms are suitable for low bit rate applications, and partial encryption scheme are proposed for them. In quardtree compression,two logical parts are produced-quardtree and parameter describing each part.Quardtree partial encryption scheme can be used for both lossy and lossless compression. Main limitation of our approach is that a different scheme has to be designed and analysedfor each compression algorithm [13].

In 2002, Droogenbroeck and Benedett proposed the selective encryption methods for uncompressed (raster) images and compressed (JPEG) images. An uncompressed (raster) gray level defines eight bitplains.The highest bitplains is more correlated to the original gray level image. On the other hand, least significant bitplains appear to be randomlike.Encrypting only bitlanes that contains only correlated values would decrease vulnerability to know plain-text attack.the proposed encryption scheme that consists of XORing the selected bitplains with the keythat has same number of bits that are to be encrypted. According to Droogenbroeck and Benedet, atleast four to five least significant bitplanes should be encrypted to achieve satisfactory visual degradation of images.second method is designed to selectively encrypt the JPEG compressed image.Huffman entropy encoding creates symbol based on run length coding [14].

In 2002 Podesser, Schmidt and Uhl proposed a selective encryption algorithm for the uncompressed (raster) images, that is quite opposite from the first method by Droogenbroeck and Benedett. In the raster image that consists of 8 bitplanes, Schmidt and Uhl's algorithm encrypts only the most significant bitplanes. After performing experiments Podesser ,Schmidt and Uhl came to the same conclusion that as Droogenbroeck and Benedett did beforePodesser,Schmidt and Uhl argue that the MSB bitplanes can bereconstucted with the aid of the encrypted remaining bitplanes.therefore they suggest encypting at least two or four bitplanes. Encrypting only two bitplanes is sufficient if severe alienation of the image data is acceptable,whereas encrypting four bitplanes provides higher security.It is up to the user t determine if the degradation method by encypting only two bitplanes is sufficient for given application or if more secure approach for encrypting four bitplanes is needed[15].

III. PROBLEM DISCRIPTION

Over the past decades, research in security has concentrated on the development of algorithms and protocols for encryption, authentication, and integrity of textual data or data with similar characteristics. Despite tremendous advances in security-specifically, the development of asymmetric cryptographic protocols and the inception of string symmetric ciphers-plenty of security problems still afflict systems. For example, hackers exploiting weaknesses in other systems and the use of inadequate (too short) cipher keys produce frequent news headlines about broken security systems.

A growing number of scientific groups in computer science and cryptography have confronted these challenges. Researchers are currently working on issues such as visual cryptography, mechanisms for the integrity of image material, digital signatures for multimedia data, and data hiding techniques. Data hiding, which has achieved the highest popularity, contemplates the crucial needs for protecting intellectual property rights on multimedia content like images, video, audio, and others. These needs demand robust solutions due to the explosion of publicly available multimedia information and the easiness with which this information can be distributed, copied and modified. Watermarking technology meets these demands and provides a feasible approach to protect against-and prove-illegal copying and redistribution in the digital world. This special theme issue presents four articles that discuss watermarking solutions for the dedicated media types such as images, video, and geometric models. They range from an overview of fundamental watermarking concepts to the latest research results.

Multimedia security in general is provided by a method or a set of methods used to protect the multimedia content. These methods are heavily based on cryptography and they enable either communication security, or security against piracy (Digital Rights Management and watermarking), or both. Communication security of digital images and textual digital media can be accomplished by means of standard symmetric key cryptography. Such media can be treated as binary sequence and the whole data can be encrypted using a cryptosystem such as Advanced Encryption Standard (AES) or Data Encryption Standard (DES). In general, when the multimedia data is static (not a real-time streaming) it can treated as a regular binary data and the conventional encryption techniques can be used. Deciding upon what level of security is needed is harder than it looks. To identify an optimal security level, the cost of the multimedia information to be protected and the cost of the protection itself are to be compared carefully. At present, there are many available image encryption algorithms such as Arnold map, Tangram algorithm, Baker's transformation, Magic cube transformation, and affine transformation etc. In some algorithms, the secret-key and algorithm cannot be separated effectively. This does not satisfy the requirements of the modern cryptographic mechanism and are prone to various attacks. In recent years, the image encryption has been developed to overcome above disadvantages as discussed in past research work.

IV.PROPOSED WORK

In the proposed method, the chaotic function Logistic Map and a key extracted from the plain-image are used to encrypt the image. The method mentioned is employed to produce a number of encrypted images using the plain-image. These encrypted images are considered as the initial population for 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.

1.Chaotic Function

Chaotic functions are similar to the noise signal. Chaotic signal plays very important role in case of encryption because of their advantages as sensitivity to primary condition, apparently accidental feature,and deterministic work the following equation shows most famous signal:

$$Xn+1=rXn\ (1-Xn) \quad (1)$$

A. formation of initial population

To form initial population first input image is divided into four equal parts. Then chaotic function logistic map is employed to separately encrypt pixels of each parts of image.

Image encryption is done by employing logistic map signal as follows:

a. First five pixels are selected from each part of image to form initial value. These selected five pixels are then used as encryption key to encrypt the part of image. In this way first member of population is formed.
b. Initial value of logistic map function can be determined by using following equation:

P=[P1, P2, P3, P4, P5] (Decimal) (2)

Following equation is then used to convert P into ASCII number as follows:

B=[P1,1, P1,2, P1,3, . . . , P2,1, P2,2, . . . , P5,7, P5,8] (ASCII). (3)

Next Equation is used to determine initial value of chaotic map function as follows:

$$U_{0k}=\frac{p_{1,1}\times 2^{39}+p_{1,2}\times 2^{38}+\cdots+p_{2,1}\times 2^{31}+\cdots+p_{5,7}\times 2^{1}+p_{5,8}\times 2^{0}}{2^{40}} \quad (4)$$

k=1, 2, 3, 4

c. For each part of plain image step b is repeated.
d. For encrypting pixels in each part f plain image following equation is used:

$$NewValue=round(U_{ik}\times 255)\otimes oldValue. \quad (5)$$

B. Genetic optimization

After forming initial population genetic algorithm is used for optimizing encrypted image. Genetic algorithm introduced in this paper uses crossover operation. Fitness function used in this paper is correlation coefficient between pairs of adjacent pixels. Best cipher image is selected on the basisi of calculation of entropy and correlation coefficient. Image having highest entropy and lowest correlation coefficient is selected as best cipher image and then this image is send to the destination.

Equation for calculationg entropy and correlation coefficient is as follows:

Entropy can be calculated as follows:

$$H(s)=\sum_{i=0}^{2^n-1} p(si)\log\left(\frac{1}{p(si)}\right) \quad (6)$$

Correlation coefficient can be calculated by using following equation:

$$r_{xy}=\frac{|cov(x,y)|}{\sqrt{D(x)}\times\sqrt{D(y)}} \quad (7)$$

Where, cov is covariance obtained using following equation:

$$cov(x,y)=\frac{1}{N}\sum_{i=1}^{N}(x_i-E(x))(y_i-E(y)) \quad (8)$$

$$E(x)=\frac{1}{N}\sum_{i=1}^{N}x_i \quad (9)$$

$$D(x)=\frac{1}{N}\sum_{i=1}^{N}(x_i-E(x))^2 \quad (10)$$

Where ,E(x) is mean and D(x) is variance.

V. CONCLUSION

In this paper , a novel encryption method is suggested for image encryption by using chaotic function and genetic algorithm. In this method , first images are encrypted using chaotic function and encryption key. In next stage genetic algorithm is used for optimization in which best cipher image is selected as best cipher image. Best cipher Images are selected based on correlation coefficient and entropy.

References

[1] Jiri Fridrich, “Image Encryption Based on Chaotic Maps”, Proceeding of IEEE Conference On Systems, Man, and Cybernetics, pp. 1105-1110, 1997.

[2] Jiun-In Guo, Jui-Cheng Yen, "A new mirror-like image encryption algorithm and its VLSI architecture", Department of Electronics Engineering National Lien-Ho College of Technology and Commerce, Miaoli, Taiwan, Republic of China in 1999.

[3] Jui-Cheng Yen, and Jiun-In Guo, "A New Chaotic Key-Based Design for Image Encryption and Decryption", IEEE International Symposium on ISCAS 2000, Geneva, pp. IV-49-IV-52, May. 2000.
[4] M.I.Sobhy, and A.R.Shehata, "Chaotic Algorithms for Data Encryption", IEEE Proceeding of ICASSP 2001, Vol 2, pp. 997-1000, May. 2001.
[5] M.I.Sobhy, and A.R.Shehata, "Methods of Attacking Chaotic Encryption and Countermeasures", IEEE Proceeding of ICASSP 2001, Vol 2, pp. 1001-1004, May. 2001.
[6] Aloha Sinha, Kehar Singh, "A technique for image encryption using digital signature", Optics Communications, ARTICLE IN PRESS, 2003, 1-6, www.elsevier.com/locate/optcom
.[7] 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.
[8] Fethi Belkhouche and Uvais Qidwai ,"Binary image encoding using 1D chaotic maps", IEEE Proceeding in the year 2003.
[9] Wang Ying, Zheng DeLing, Ju Lei, et al., "The Spatial-Domain Encryption of Digital Images Based on High-Dimension Chaotic System", Proceeding of 2004 IEEE Conference on Cybernetics and Intelligent Systems, Singapore, pp. 1172-1176, December. 2004
[10] M.-R. Zhang, G.-C. Shao and K.-C. Yi, " *T-matrix and its applications in image Processing*", IEEE Electronics Letters 9th December 2004 Vol. 40 No. 25
[11] Shaojiang Deng, Linhua Zhang, and Di Xiao, "*Image Encryption Scheme Based on Chaotic Neural System*", J. Wang, X. Liao, and Z. Yi (Eds.): ISNN 2005, LNCS 3497, pp. 868-872, 2005.
[12] 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.
[13] H. Cheng and X. Li, "*Partial Encryption of Compressed Images and Video*," IEEE Transactions on Signal Processing, 48(8), 2000, pp. 2439-2451.
[14] M. Van Droogenbroeck and R. Benedett, "*Techniques for a Selective Encryption of Uncompressed and Compressed Images*," Proceedings of Advanced Concepts for Intelligent Vision Systems (ACIVS) 2002, Ghent, Belgium, September 9-11, 2002.
[15] M. Podesser, H.-P. Schmidt and A. Uhl, "*Selective Bitplane Encryption for Secure Transmission of Image Data in Mobile Environments*," 5th Nordic Signal Processing Symposium, on board Hurtigruten, Norway, October 4-7, 2002.

