International Journal of Research and Development in Applied Science and Engineering (IJRDASE)
ISSN: 2454-6844

A Genetic Algorithm Optimized Security using Chaotic Key Generation Scheme for Image Encryption

Ankita Bajpai
Dept of Information & Technology,
U.P.T.U., Lucknow, India
bajpai.ankita0@gmail.com

Dr. Akash Awasthi
Dept of Information & Technology,
U.P.T.U., Lucknow, India
sanjay.sachan@gmail.com

Abstract- ***This work incorporates the concepts and application of cryptography as an essential mode for protecting, information related to image data. The objective of our work is fulfilling the importance of security demand as increasing day by day with the advent of online transmission and storage. The security of digital images is attracting a huge amount of research focus for the applications were these digital images data base are stored in hardware memory or sending over the communication channel networks. We have incorporated Genetic algorithms as optimization algorithms for generating robust encryption keys. We have effectively solved the encryption decryption problem objective by using genetic algorithms through modelling algorithm by a simplified version of genetic processes that generates chaos function based encryption key.***

Keywords- GA, Chaotic Function, Image Encryption, Signal Processing, Logistic Map.

1.Introduction:

There are few approaches designed for protecting data and securing systems. One of them is data encryption (cryptography). Only a person who possesses appropriate key (or keys) can decrypt the encrypted data. The drawback of this data protection strategy is that once such a data is decrypted by a pirate, there is no way to protect the data and track the illegal distribution. Also it is impossible legally to prove the ownership. The next approach to protect the intellectual property rights is encryption. Encryption is a technique for embedding hidden data that attaches copyright protection information to digital information. This provides an indication of ownership of the digital data.

Encryption is closely related to steganography in that they are both concerned with covert communication and belong to a broader subject known as information hiding. Steganography, derived from Greek, literally means "covered writing" is the art of hiding information inside other data in ways that prevent the detection of hidden message. A steganographic system is typically not required to be robust against intentional removal of the hidden message. On the other hand, the encryption requires that the hidden message should be robust to attempts aimed at removing it. In the case of copyright protection the copyright information should resist any modifications by pirates intending to remove it. This is a significant step forward compared to a common steganography.

Security in transmission of digital images has its importance in today's image communications, due to the increasing use of images in industrial process, it is essential to protect the confidential image data from unauthorized access, Image security has become a critical issue. The difficulties in ensuring individuals privacy become increasingly challenging. Various methods have been investigated and developed to protect data and personal privacy. Encryption is probably the most obvious one. In order to protect valuable information from undesirable readers, image encryption is essential.

There are different algorithms in the spatial and transform domains for digital encryption. The techniques in the spatial domain still have relatively low-bit capacity and are not resistant enough to lossy image compression and other image processing. For instance, a simple noise in the image may eliminate the watermark data. On the other hand, frequency domain-based techniques can embed more bits for watermark and are more robust to attack. Some transforms such as Discrete Cosine Transform (DCT) and

Discrete Wavelet Transform (DWT) are used for encryption in the frequency domain. Most DCT-based techniques work with 8 × 8 blocks. These transforms are being used in several multimedia standards such as MEPG-2, MPEG-4, and JPEG2000. In addition, different watermark algorithms have been proposed using DCT and DWT. In considering the attacks on watermarks, the robustness feature of an algorithm becomes very important. In this regard, we classify a watermark method as robust if the watermark data embedded by that algorithm in an image or any other data, cannot be damaged or removed without destroying or damaging the data itself. Therefore, an attack is successful if it can eliminate the watermark without damaging the image itself. The question is, which transform watermark algorithms are more robustness to different attacks compared to other techniques? We perform a comparative study on different transform watermark algorithms and compare their robustness. In fact the robustness of the algorithms is dependent on the frequency at which the watermark data is added. We have performed evaluation by having in mind that the embedded watermark should be invisible so we have kept the Peak Signal to Noise Ratio (PSNR) value of the images constant at 35dB and compared the robustness of the different methods.

2. Related Work:

In 2012 ,Aarti Soni, Suyash Agrawal suggested a method based on Genetic Algorithm which is used to generate key by the help of pseudo random number generator. Random

number will be generated on the basis of current time of the system. Acoording to the,Using Genetic Algorithm we can keep the strength of the key to be good, still make the whole algorithm good enough. Symmetric key algorithm AES has been proposed for encrypting the image as it is very secure method for symmetric key encryption.

In 2012 ,Seema,Sheetal Sharma presented a new embedding and extracting method with DWT-SVD,in order to improve the robustness and imperceptibleness of the algorithm. The approximation matrix of the third level of image in DWT domain is modified with SVD to embed the singular value of watermark to the singular value of DWT coefficient. The proposed embedding and extracting method was employed to accelerate the hybrid DWT-SVD encryption g and to avoid the leak of watermark. This hybrid technique leads to optimize both the fundamentally conflicting requirements. The experimental results show both the good robustness under numerous attacks and the high fidelity.

In 2012 ,Sonia Goyat work explored the different techniques of cryptography in order to prove that the natural selection based techniques are as good as the rigorous mathematical techniques. 12 papers and thesis have been studied by her in order to reach the conclusion.

In 2012,V.Srikanth, Udit Asati, Viswajit Natarajan, T.Pavan Kumar, Teja Mullapudi, N.Ch.S.N.Iyengar proposed a technique where the image encryption is done using breaking and merging of bits. As followed in other encryption techniques the image is first broken down into blocks also known as a grid. Then the initial transformation steps are performed and then functions similar to Vernon cipher are used to locate the pixels and further genetic algorithm is used to encrypt the images using one point cross-over.

In 2012,Ankita Agarwal suggested a new method based on Genetic Algorithm (GA) which is used to produce a new encryption method by exploitation the powerful features of the Crossover and Mutation operations of (GA).

In 2013, Shubhangini P.Nichat, Prof.Mrs.S.S.Sikchi, introduced a 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.

3. Methodology:

A The Concepts of Image Encryption:

Image encryption is necessary for future multimedia Internet applications. Password codes to identify individual users will likely be replaced are biometric images of fingerprints and retinal scans in the future. However, such information will likely be sent over a network. When such images are sent over a network, an eavesdropper may duplicate or reroute the information. By encrypting these images, a degree of security can be achieved. Furthermore, by encrypting noncritical images as well, an eavesdropper is less likely to be able to distinguish between important and non-important information [3, 4].

Image encryption can also be used to protect privacy. An example for image encryption to protect privacy is in medical imaging applications. Recently, in order to reduce the cost and to improve service, electronic forms of medical records have been sent over networks from laboratories to medical centers.

According to the law, medical records, which include many images, should not be disclosed to any unauthorized persons. Medical images, therefore, should be encrypted before they are sent over networks [8].

Unlike the conventional cryptographic algorithms, which are mainly based on discrete mathematics, chaos-based cryptography is relied on the complex dynamics of nonlinear systems or maps, which are deterministic but simple. Chaotic maps present many desired cryptographic qualities such as simplicity of implementation that leads to high encryption rates, and excellent security. Therefore, it can provide a fast and secure means for data protection, which is crucial for image data transmission over fast communication channels, such as the broadband Internet communication [5, 6].

The main obstacle in designing image encryption algorithms is that it is rather difficult to swiftly confuse and diffuse data by traditional means of cryptology. In this respect, chaos-based ciphers have shown their superior performance. It has been proved that in many aspects that chaotic maps have analogous but different characteristics as compared with conventional encryption algorithms.

The Ciphering of image is actually an important issue. One essential difference between text data and image data is that the size of image data is much larger than the text data. The time is very important factor for the image encryption [1]. Two levels of time are found, the first is the time to encrypt, and the other is the time to transfer images. To minimize it, the first step is to choose a robust and easy method to implement cryptosystem. Two approaches of select encryption where wavelet-based methods are used for compression. The first attempt was to hide the choice of filters, while the second approach of selective encryption was based on wavelet packets and the decomposition tree is keep secret. The use of genetic algorithm is very important tool to find more secure image, where genetic algorithm gives suitable key stream.

The Encryption Evaluation Metrics

In this section, we will discuss, in detail, two families of encryption metrics; the first family evaluates the ability of the encryption algorithm to substitute the original image with uncorrelated encrypted image. In This family, five

metrics, which are the histogram deviation DH, the correlation coefficient rxy, the irregular deviation DI, the histogram uniformity, and a proposed encryption quality metric, are studied. The second family evaluates the diffusion characteristics of the encryption algorithm. In this family, three metrics, which are the Avalanche effect, NPCR and UACI, are studied.

i. The Correlation Coefficient:

A useful measure to assess the encryption quality of any image cryptosystem is the correlation coefficient between pixels at the same indices in the plain and the cipher images. This metric can be calculated as follows:

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

where x and y are the gray-scale values of two pixels at the same indices in the plain and cipherimages. In numerical computations, the following discrete formulas can be used:

$$E(x)=\frac{1}{L}\sum_{i=1}^{L} x_l$$

$$D(x)=\frac{1}{L}\sum_{i=1}^{L}\left(x_l - E(x)\right)^2$$

$$cov(x,y)=\frac{1}{L}\sum_{i=1}^{L}\left(x_l - E(x)\right)\left(x_l - E(y)\right)$$

where L is the number of pixels involved in the calculations. The closer the value of *xy r* to zero is, the better the quality of the encryption algorithm.

4 Use of Genetic Algorithms in encryption:

The genetic algorithm is optimization and search technique based on the principles of genetics and natural selection.

GA composed of five components that are random number generator, fitness evaluation unit and genetic operators for reproduction, crossover and mutation operations. The initial population required at the start of the algorithm is a set of number strings generated by the random number generator. Each string is a representation of a solution to the optimization problem being addressed. Associated with each string is a fitness value (fval) computed by the evaluation unit. The reproduction operator performs a natural selection function known as "seeded selection". Individual strings are copied from one set to the next according to the fitness values, the higher the fitness value, the greater is the probability of a string being selected for the next generation. The crossover operator chooses pairs of strings at random and produces new pairs. The mutation operator randomly mutates or reverses the values of bits in a string. A phase of algorithm consists of applying the evaluation, reproduction, crossover and mutation operations. A new generation of solutions is produced with each phase of the algorithm.

i. Chaotic function based key generation:

The cryptosystems, based on widely-used one-dimensional discrete chaotic maps, such as Logistic map, are very good in security. As known Logistic map is defined as: x_{n+1} = k*xn* (1 - xn), where k = (0, 4), n = 0,1,. . . [9].The parameterk and initial value x0 may represent the key. The parameter k can be divided into three segments, which can be examinedby experiments on following conditions: x0 = 0.3. When k = (0, 3), the calculation results come tothe same value after several iterations without any chaotic behavior. When k = (3, 3.6), the phase space concludes severalpoints only in this phase the functionshows periodicity. While k = (3.6, 4), it becomes a chaotic functionwith periodicity disappeared. So we can draw the following conclusions: (1) The Logistic map does not satisfy uniformdistribution property. When k = (0, 3.6) the points concentrate on several values and could not be used for encryptionpurpose. (2) Cryptosystems based on Logistic map can be used to generate key and posses strong security.

ii. Design Algorithm:

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.

A. 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:

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

B. 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)

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).

C. Genetic optimization:

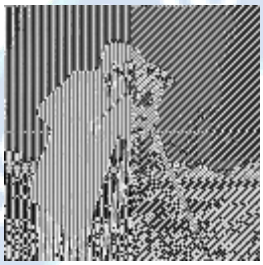
After forming initial population genetic algorithm is used for optimizing encrypted image. Genetic algorithm introduced in this paper uses crossover operation. Fitness function used in this paper is correlation coefficient between pairs of adjacent pixels. Best cipher image is selected on the basis of 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.

5. Result and Discussion:

In this work we are working on encryption decryption. We have taken two images "cameraman.tif" and "lena.jpg" as a input image then we encrypt this image and use two different noises gaussian and salt and pepper noise after that decrypt them. We run this process five times for different density to check our result. (e.g. we have taken density 0.5e-3 to 0.5e-5 for gaussian noise and 0.1 to 0.3 for salt and pepper noise)

Gaussian Noise



(a) Encrypted Image for 0.5e-5

(b) Decrypted image for 0.5e-5

(c) Encrypted Image for 0.5e-4

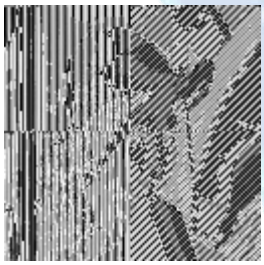
(d) Decrypted image for 0.5e-4

Fig 1: Result for Gaussian Noise

Salt & Pepper Noise

(a) Encrypted Image for 0.25

(b) Decrypted image for 0.25



(c) Encrypted Image for 0.1

(d) Decrypted image for 0.1

Fig 2: Result for Salt and Pepper Noise

6.Conclusion

In this work, we have applied a method related to Genetic Algorithm which is used to generate key by the help of random key generation by logistic map chaotic function. Random keys are generated on the basis of current time of the system and thereafter best key is selected that can provide high level of security to encrypted image. It has been observed that in the absence of noise the algorithm is completely capable of recovering image. The testing over the presence of noise is also observed for image data and in such cases the image able to get recovered with small amount of presence of noise. By the incorporation of Genetic Algorithm the developed algorithm keep the strength of the key to be good that makes the whole algorithm good enough. Chaotic function based key generation algorithm has been implemented for encrypting

the image and it has been found as very secure method for image data by key encryption.

References:

[1] O. S. Faragallah, Utilization of Security Techniques for Multimedia Applications, Ph. D. Thesis, Department of Computer Science and Engineering, Faculty of Electronic Engineering, Menofia University, 2007.
[2] A. J. Menezes, P. C. V. Oorschot and S. Vanstone, Handbook of Applied Cryptography , CRC Press Boca Raton ,USA, 1996.
[3] L. Qiao, Multimedia Security and Copyright Protection , Ph. D. Thesis, Department of Computer Science, University of Illinois at Urbana-Champaign, Urbana, Illinois, USA, 1998.
[4] S. Li, G. Chen and X. Zheng, Chaos-Based Encryption for Digital Images and Videos , Chapter 4 in Multimedia Security Handbook, CRC Press LLC, February 2004.
[5] Y. Mao and M. Wu, A Joint Signal Processing and Cryptographic Approach to Multimedia Encryption , IEEE Transactions on Image Processing, Vol. 15, No. 7, pp. 2061-2075, July 2006.
[7] Y. Mao, Research on Chaos-Based Image Encryption and Watermarking Technology, Ph. D. Thesis, Department of Automatation, Nanjing University of Science & Technology, Nanjing, China, August 2003.
[8] J. Daemen and V. Rijmen, AES Proposal: Rijndael , AES Algorithm Submission, 1999.