Image security using 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.
shubhanginichat@gmail.com
sikchismita@gmail.com

Abstract*— In this methodology, a new method based on a hybrid model composed of a genetic algorithm and a chaotic function is proposed for image encryption. In the proposed method, 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. In each stages of the genetic algorithm, the answer obtained from previous iteration is optimized so that the best encrypted image with the highest entropy and the lowest correlation coefficient among adjacent pixels is produced. In this method, the chaotic function is employed for initial encryption and the genetic algorithm is used to improve the encryption process of the image. The main innovation in this methodology is that this is the first time genetic algorithms are used in this way to encrypt images. Results obtained for correlation coefficients and the entropies of the images also prove the high efficiency of this method, compared with other methods in image encryption. Moreover, this method, compared to other methods mentioned in this paper, has a higher stability in the face of attacks common in this area.

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

I.INTRODUCTION

Owing to the advance in network technology, information 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 critical and imperative 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 with no loss of information. This is one of the most important characteristics of this representation because it allows us to work in the "Fourier domain" and then return to the original domain without losing any information. Encryption techniques based on various combinations of methods from these two categories are not unusual.

II.PROBLEM DESCRIPTION

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.

III. LITERATURE REVIEW

Modified AES Based Algorithm for Image encryption, 2007

M. Zeghid, M. Machhout, L. Khriji, A. Baganne, and R. Tourki analyze the Advanced Encryption Standard (AES), and in their image encryption technique they add a key stream generator (A5/1, W7) to AES to ensure improving the encryption performance[3].

Image Encryption Using Block-Based Transformation Algorithm, 2008

Mohammad Ali Bani Younes and Aman introduce a block-based transformation algorithm based on the combination of image transformation and a well known encryption and decryption algorithm called Blowfish. The original image was divided into blocks, which were rearranged into a transformed image using a transformation algorithm, and then the transformed image was encrypted using the Blowfish algorithm. Their results showed that the correlation between image elements was significantly decreased[4]

.

An Image Encryption Approach Using a Combination of Permutation Technique Followed by Encryption, 2008

Mohammad Ali Bani Younes and Aman Jantan introduce a new permutation technique based on the combination of image permutation and a well known encryption algorithm called RijnDael. The original image was divided into 4 pixels × 4 pixels blocks, which were rearranged into a permuted image using a permutation process, and then the generated image was encrypted using the RijnDael algorithm. Their results showed that the correlation between image elements was significantly decreased by using the combination technique and higher entropy was achieved[5]

Image Encryption Using Advanced Hill Cipher Algorithm, 2009

Bibhudendra Acharya, Saroj Kumar Panigrahy, Sarat Kumar Patra, and Ganapati Panda have proposed an advanced Hill (AdvHill) cipher algorithm which uses an Involutory key matrix for encryption. They have taken different images and encrypted them using original Hill cipher algorithm and their proposed AdvHill cipher algorithm. And it is clearly noticeable that original Hill Cipher can't encrypt the images properly if the image consists of large area covered with same colour or gray level. But their proposed algorithm works for any images with different gray scale as well as colour images[6]

New modified version of Advance Encryption Standard based algorithm for image encryption, 2010

Kamali S.H., Shakerian R.,Hedayati M. and Rahmani M. analysis Advance Encryption Standard(AES) algorithm and present a modification to the Advanced Encryption Standard (MAES) to reflect a high level security and better image encryption. Their result so that after modification image security is high. They also compare their algorithm with original AES encryption algorithm[7]

Image Encryption Using Affine Transform and XOR Operation, 2011

Amitava Nag, Jyoti Prakash Singh, Srabani Khan, Saswati Ghosh, Sushanta Biswas, D. Sarkar and Partha Pratim Sarkar propose 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. They redistribute the pixel values to different location using affine transform technique with four 8-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 total key size used in algorithm is 64 bit. Their results proved that after the affine transform the correlation between pixel values was significantly decreased[8]

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.

V.IMPLEMENTATION

i) Implementation

Implementation of proposed steganography application is always preceded by important decisions regarding selection of the platform, the language used, etc. these decisions are often influenced by several factors such as real environment in which the system works, the speed that is required, the security concerns, and other implementation specific details.

ii) Implementation requirements

The implementation of the proposed system will require a standard cover image along with a normal plain text file for performing the message embedding procedure. However the software requirements for performing the implementation will be:

- The language chosen for this project is Matlab
- The operating system used will be either Microsoft windows XP, Vista, 7

iii) Encryption Evaluation Matrix

- **Image Entropy**

Entropy is one of the prominent features in randomization. Information entropy is a mathematical theory for data communication and storage introduced in 1949 by Claude E Shannon. Equation 1 is introduced for obtaining entropy.

$$H(s) = \sum_{i=0}^{2^N-1} P(s_i)\log\left(\frac{1}{P(s_i)}\right) \qquad (1)$$

In which, N is the number of gray levels used in the image (for gray level images, N is 8), and $P(s_i)$ shows the probability of having a i^{th} gray level in the image. In images that are produced in a completely random way, N will be 8; which is considered as an ideal value. Our paper is shown entropy about 7.9978.

- **Correlation coefficient**

A good encryption algorithm is one in which the correlation coefficient between pairs of encrypted adjacent pixels in the horizontal, vertical, and diagonal positions are at the least possible level. The correlation coefficient is calculated by using equation 2.

$$r_{xy} = \frac{|\mathrm{cov}(x,y)|}{\sqrt{D(x)} \times \sqrt{D(y)}} \qquad (2)$$

In the above relation, x and y are the gray levels in two adjacent pixels of the image. In calculating the correlation coefficients, the following equations are employed:

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

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

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

To test the correlation coefficient between two adjacent vertical pixels, two adjacent horizontal pixels, and two adjacent diagonal pixels in a cipher-image, the following procedure is used: first, 2500 pairs of pixels are randomly selected, and then the correlation coefficient is obtained by using equation2

iv) Result Accomplished

- **Encryption Module**

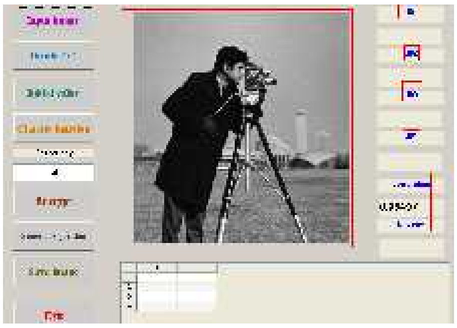

Figure 3 Visualizing input image in GUI

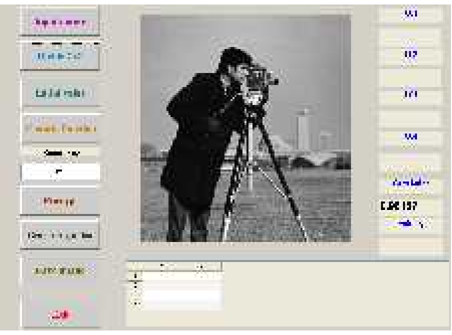

Figure 4. Dividing the input image into 4 parts.

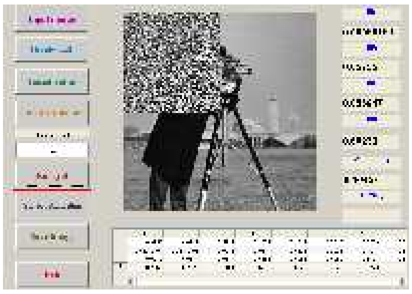

Figure 7. Performing encryption using Secret key-I

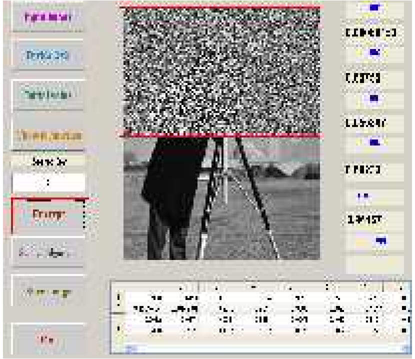

Figure 8. Performing encryption using Secret key-II

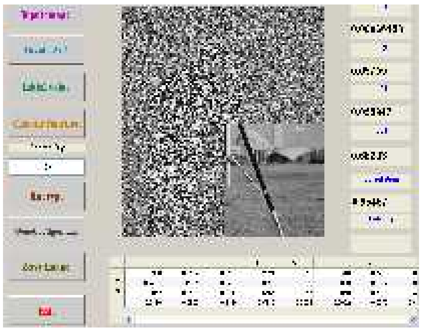

Figure 9. Performing encryption using Secret key-III

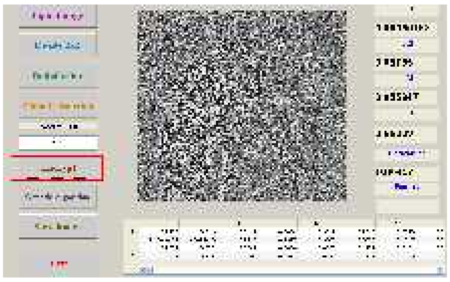

Figure 10. Performing encryption using Secret key-

Decryption Module

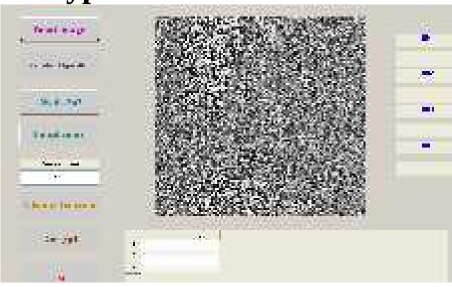

Figure 13. Uploading encrypted image to perform decryption

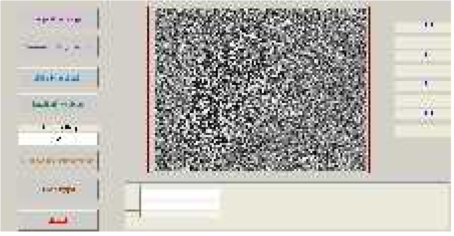

Figure 15. Dividing the encrypted image into 4 parts

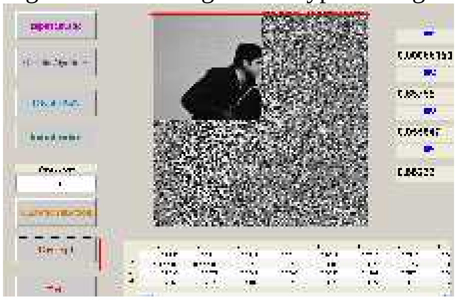

Figure 18. Decryption process in progress-I

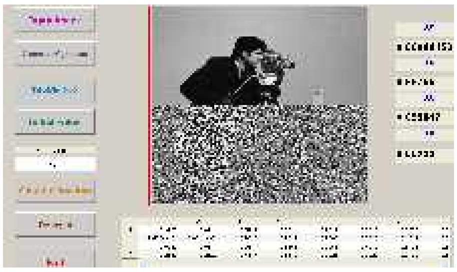

Figure 19. Decryption process in progress-II

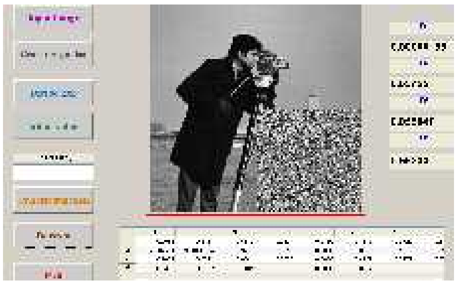

Figure 20. Decryption process in progress-III

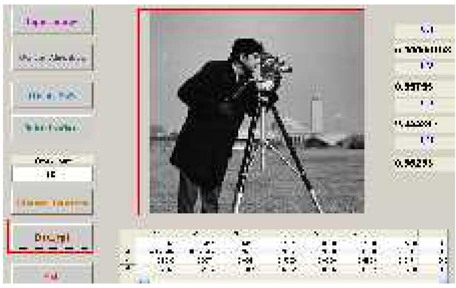

Figure 21. Visualizing final Decrypted image

V.CONCLUSION

In this project, a new method has been suggested for encrypting images by using the chaotic function logistic map and genetic algorithms. In this method, the chaotic function is employed for initial encryption and the genetic algorithm is used to improve the encryption process of the image. The main innovation in this paper is that this is the first time genetic algorithms are used in this way to encrypt images. Results obtained for correlation coefficients and the entropies of the images also prove the high efficiency of this method, compared with other methods in image encryption. Moreover, this method, compared to other methods mentioned in this paper, has a higher stability in the face of attacks common in this area. Security analysis experimental results show that, taking into account the trade-off between the attacks expenses and the value of information as well as the operational speed, this kind of image cryptosystems will be very practical.

VI. REFERENCES

[1]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.

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

.

[3] 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.

[4] Mohammad Ali Bani Younes and Aman Jantan ―Image Encryption Using Block-Based Transformation Algorithm‖ IAENG International Journal of Computer Science, 35,2008.

[5] 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.

[6] Bibhudendra Acharya, Saroj Kumar Panigrahy, Sarat Kumar Patra, and Ganapati Panda,‖ Image Encryption Using Advanced Hill Cipher Algorithm‖, International Journal of Recent Trends in Engineering, Vol. 1, No. 1, May 2009.

[7] Kamali, S.H., Shakerian, R., Hedayati, M.,Rahmani, M.,‖ A new modified version of Advance Encryption Standard based algorithm for image encryption‖,Electronics and Information Engineering (ICEIE), 2010 International Conference.

[8] 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).

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

[10] William stallings, ―Cryptography and Network Security: Principles & Practices‖, second edition.