ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Special Issue 9, May 2016

Genetic Algorithm based Image Cryptography

Vivina Glancy Machado [1], Sudeepa K. B. [2]

PG Student, Department of CSE, NMAMIT, Nitte, Udupi District, Karnataka, India[1]

Associate Professor, Department of CSE, NMAMIT, Nitte, Udupi District, Karnataka, India [2]

ABSTRACT: Fundamental technique used to protect the information over the internet is cryptography. Present day the securing the digital images are major area of concern, especially while dealing with digital images sent through the communication channel or where it may be stored. In all these cryptographic methods how the secret key used for cryptography is generated is an important factor. In this paper Genetic algorithm (GA) is used for the generations of these key sequences with the help of random number generator to make the key sequences complex. Genetic algorithms are a class of optimization algorithms. Key generation will go through a number of processes. This paper explains the advantages of using GA for generation of the key sequences in the image cryptography.

KEYWORDS: Genetic Algorithm, LFSR, Cryptography, Encryption, Decryption, PRN

I. INTRODUCTION

With the greater demand in the internet access, there is a need to secure the data over the internet from the unauthorized users. It is needed to control the unauthorized users from accessing and modifying of the valuable information. Various types of cryptographic schemes are developed to protect the valuable information.Along three independent dimensions Cryptographic systems are basically classified.

a. The operations used: Two general principles are used in all encryption algorithms: substitution, in which the each letter in the plain text is mapped in to another letter. Other principle is transposition in which the letters are re-arranged. These two operations are reversible.

b. The num of keys used in cryptography: If both the sender as well as the receiver use the same secret key for encryption and decryption, then it is called secret/symmetric/single key encryption. If both sender as well as the receiver uses two keys, one for encryption and other decryption, then it is called asymmetric/two-key/public key encryption.

c. The processing method of plaintext: Block cipher will take a block of the input text and produce output block for that block of input text passed. Stream cipher will process each input text continuously and produce the output text for that particular input text one after the other. There are basically-two types of cryptographic schemes, which are discussed below on the basis of key usage in sending and receiving end. 1. Asymmetric cipher system 2.Symmetric cipher system. In first system, two different keys are used for cryptography. One used for the encryption is called the public key, and the other used for decryption is called secret key. In the second, sender and receiver both use the same key for encryption as well as the decryption. The copies of the secret key must be obtained to Sender and receiver in a very secure manner. And they must be stored securely.

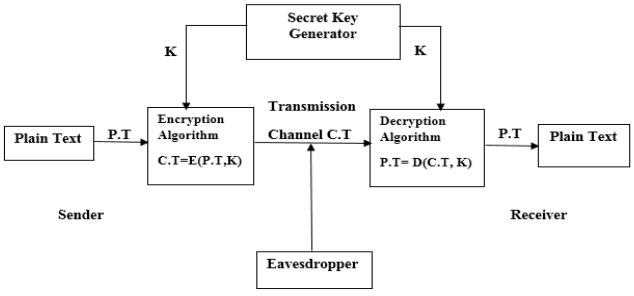


Figure 1: Block diagram of stream cipher system.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Special Issue 9, May 2016

It starts with the plain text block which is the original message to be sent to the receiver. The next block is about the encryption algorithm which uses the secret key K and performs various substitutions and transformation operations on the plain input text passed to get the ciphertext. The ciphertext can be represented as C.T=E (P.T ,K), where C.T is Cipher Text, the function E is the Encryption Algorithm. The C.T is then sent to the receiver through the transmission channel. The receiver uses the decryption algorithm to get the original plain text back. The block of eavesdropper explains that, he tries to find the key or the plain text using the information on the channel. This is called the attack. He does not have access to the secret key. The decryption algorithm block uses the same secret key K and performs reverse substitution and transformation operations on the cipher text, is called the decryption. The output of the decryption algorithm is represented as, P.T=D(C.T,K) where D is the decryption algorithm. The fifth block is the secret key generator block which generates the secret key which is used by both sender and the receiver.

Pseudo Random Number (PRN)

PRN sequence is generated by using mathematical formula such that the sequence cannot be predicted, and which is difficult to reproduce sequentially and reliably. A PRNG is an algorithm producing a sequence of random numbers which is depends on an initial seed value provided or any continuous input. Pseudo random numbers generated occur in such a sequence that two conditions must be met:

1. The distribution of values generated are uniform across a defined set interval or/ and
2. Prediction of future values on the basis of past or present ones is impossible.

Linear Feedback Shift Register (LFSR)

It consists of a series of finite stages holding one bit and a feedback function. The feedback function can be XOR, odd parity, sum, modulus operations. The input bit is the “seed” value. The bit positions selected and combined to get the feedback function result. The result sent back to the registers input . Maximum length of is 2^{n-1}, where n is the no. of flip flops. In LFSR, the feedback function is linear.

II. LITERATURE SURVEY

The random numbers are mainly used to get the unpredictable results. The following are some of the literatures in which FSR is used for the generation of the PRN sequences. Gove et.al[1], proposed a pseudo random number key generation technique to encrypt pass thought generated by the mu waves of brain. They used a non linear forward feedback shift register (NLFFSR) with a feedback func f and non linear func g, swapped characters as the input for generating a pseudo random number sequence and applied crossover technique to mu waves and generated pseudo random number sequence for generating the key for cryptography.

M.Sahithi et.al [2], presented the model for 8-Bit RN generation using Linear Feedback Shift Register(LFSR). Here 8 D-Flip Flops are used to generate pseudo random number sequcnce. D1,..,D8 are the inputs. Q1,…,Q8 are outputs. Q1, is XOR ed with output from leftmost Q8 to form the output of the feedback function.

GA concept is inspired by Darwin's theory of evolution [3]. He explained regarding the concept of natural selection that the slight variation in the trait helps the individuals to adapt to their environment and produce the new individuals which are fit for that environment. Genetic algorithms in particular became popular through the work of John Holland[4]. The various authors have proposed the genetic algorithm concepts. The literature survey has been done with the help of papers in which the crossover and mutation operators are used to generate the pseudo random number sequence.

Soniya Goyat [5], applied mutation and crossover techniques for generating a pseudo random number sequence and used a threshold value for selection of pseudo random number as a key for encryption.

Ankita Agarwal[6], used secret keys, mutation and crossover operator for encrypting an image. They have divided an image into 8-byte blocks and used secret key, crossover and mutation operators to change the bits of an image.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Special Issue 9, May 2016

Shubhangini P.Nichat [7] proposed a model for encryption of the image. The images are encrypted using chaotic function and encryption key and the optimization is done by the genetic algorithm in which best cipher image is selected based on correlation coefficient and entropy.

Manish Kumar and Haider Banka[8] proposed three mutation operators to produce next generation in Genetic Algorithm. The gap shift, full gap column remover and space merging mutation operators are used to solve the MSA problem. They have improved the quality of sequences using the proposed method.

III. GENETIC ALGORITHM

The genetic algorithms vary based on the problem to solve the particular problem. The genetic algorithms (GA's) process starts with an initial population composed of random chromosomes, which form the first generation. Crossover combines the parents and creates new generation by selecting the best solutions. The best solutions to the given problem are selected by applying crossover and mutation.
The basic Genetic Algorithm works as follows:
1. Initially, population of generated attempted solutions are considered.
2. Repeatedly do the following:
   2a. Each of the attempted solutions are evaluated
   2b. Best solutions subset is chosen
   2c. A new population is generated using best solutions.
3. The algorithm terminates when the satisfactory results are produced.

Crossover

Using crossover operator, we recombine the two parent strings to get better child string.Crossover operator has different types 1.one point , 2. two point 3. uniform crossover 4.arithmetic which are which are discussed below.
1. Single point crossover: At only one point the crossover is applied.
Before crossover:

1	1	1	1	0	1	0	1
1	1	1	0	1	1	0	1

After crossover:

1	1	1	1	0	1	0	1
1	1	1	0	1	1	0	1

Figure 2: Single/One point Crossover

2. Two point(Multi Point) crossover:
Before crossover:

0	1	0	1	1	0	1	0
1	0	0	0	1	1	0	0

After crossover:

1	1	0	0	1	0	1	0
0	0	0	1	1	1	0	0

Figure 3: Two(Multi) point Crossover

3. Uniform crossover: Choosing a random subset from parent 1 and the remaining bits from parent 2.
Before crossover:

1	1	1	0	0	0	1	1	1	0
0	0	1	1	0	1	0	0	1	0

After crossover:

0	0	1	1	0	1	0	0	1	0
1	1	1	0	0	0	1	1	1	0

Figure 4: Uniform crossover

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Special Issue 9, May 2016

4.Arithmetic crossover: Performing any of these operations- AND, OR, XOR.

Before crossover:

Parent 1

1	1	1	0	1	0	0	1

Child 1(AND)

1	0	1	0	0	0	0	1

After crossover:

Parent 2

1	0	1	1	0	0	0	1

Child 2(OR)

1	1	1	1	1	0	0	1

Figure 5: Arithmetic crossover

Mutation

Mutation can be explained as the chromosomes of child to be different from its parent. Mutation is an altering of one or more bits. It helps to maintain the genetic diversity between the generations. bit toggle and bit shift mutation are two Mutations.

Initially:

1	1	1	0	1	0	0	1

After mutating:

1	1	1	0	1	1	0	1

Figure 6: Mutation

IV. PROPOSED METHOD

V.

This paper proposes a new method for generating pseudo random number sequence using GA and LFSR, which is used for an image encryption.

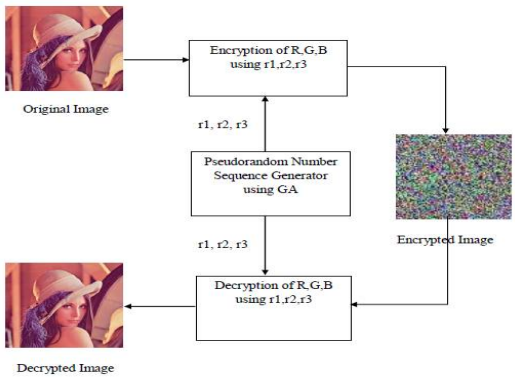


Figure 7: Proposed Method

The encryption of the image is performed by using the encryption algorithm. The encryption algorithm is defined as, $CT_i = (PT_i \oplus K_i) \bmod 2^b$ (b=8 when we use one color component of the pixel to be encrypted.) The next step is to generate the secret key K using pseudorandom number sequence generator with the help of GA which is discussed below.

Let us consider the polynomial of the type $F(x)=x^6+x^5+ x^4+x^3+x^2+x+c$ as shift registers. The coefficients r1, r2, r3, r4,r5,r6 r5 are for generating the PRN key sequence r1, r2, r3 which are used for encrypting the RGB components of the original image. Genetic Algorithm used for the generation of the pseudo random sequence r1, r2, r3 which are used for image cryptography.

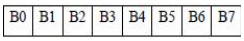
ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

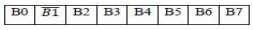
(An ISO 3297: 2007 Certified Organization)

Vol. 5, Special Issue 9, May 2016

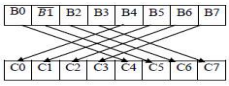
Step 1: The r1 is converted to its binary value.



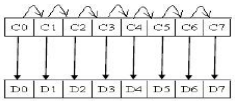
Step 2: Mutation (invert second bit)



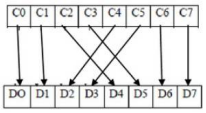
Step 3: Crossover



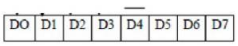
Step 4: XOR Operation



Step 5: Crossover



Step 6: Mutation



Step 7: Output of the Step 6 is converted into its decimal form and taken as r1.
These same sequences of operations are performed on r2 and r3 to get r2 and r3.
After generating three pseudorandom numbers, these are used for encryption of RGB components.

$CT_r = (PT_r + r1) \% 2^b$
$CT_g = (PT_g + r2) \% 2^b$
$CT_b = (PT_b + r3) \% 2^b$

After this, these RGB components are combined to get an encrypted image. After the encryption, the registers are shifted using LFSR as shown below in figure 8.

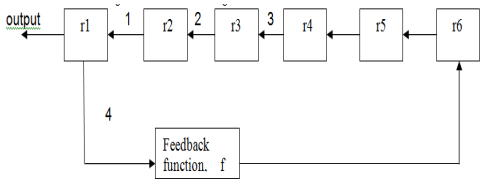


Figure 8 : Block diagram of shifting register values.

The decryption is the reverse process of encryption where we use the same PSN as a secret key.

$PT_r = (CT_r - r1 + 2^b) \% 2^b$
$PT_g = (CT_g - r2 + 2^b) \% 2^b$
$PT_b = (CT_b - r3 + 2^b) \% 2^b$

Without the knowledge of generated pseudorandom sequence it will not be possible for anyone to extract the message.

VI. RESULTS AND ANALYSIS

In this section, the proposed method efficiency is discussed. These evaluations are carried out by using the parameters; variance, standard deviation and entropy for the repetition of RGB components. The work has been tested for many images, but only “Lena.png” (size 512x512) encryption and decryption has been shown here.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Special Issue 9, May 2016

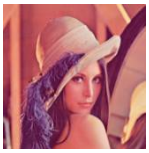


Fig9(a).Original Image Size:512x512

Fig9(b).Encrypted Image Size:512x512

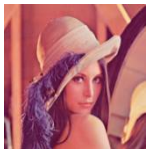


Fig9(c).Decrypted Image Size:512x512

It can be seen in the encrypted figures that the original image is not at all predictable.

Variance, Standard Deviation, Entropy:

Variance is defined as the mean squared deviation from the mean. The variance is calculated as:

$$\text{Variance } S^2 = \frac{(X - \overline{X})^2}{N}$$

The square root of the variance is standard deviation and is calculated as:

$$\text{Standar Deviation } S = \sqrt{\frac{(X - \overline{X})^2}{N}}$$

The table below shows the standard deviation, entropy and variance for the red, green, and blue pixel repetition of "Lena.png" original image and encrypted image.

	STDEV			ENTROPY			VARIANCE		
	RED	GREEN	BLUE	RED	GREEN	BLUE	RED	GREEN	BLUE
ORIGINAL IMAGE	1010.6059	676.39	1175.9	7.2531	7.594	6.9684	1.02E+06	457505.937	1.38E+06
ENCRYPTED IMAGE	31.844475	33.424	33.699	7.9993	7.9992	7.9992	1014.0706	1117.1451	1135.6549

Table 1: Standard Deviation, Entropy, Variance for RGB components of Original image and Encrypted image

It is clear from the table1 that, the standard deviation of the encrypted image is very less and thus it helps to confirm there is no information which predicts the original image. The entropy of the encrypted images is approximately 8.

VII. CONCLUSION

In this paper, a novel encryption scheme has been introduced for image encryption by implementing in genetic algorithm. Genetic Algorithm and LFSR are used to generate the pseudo random sequence which are used as the secret key in the image encryption. The LFSR is used to extend the length of the PRN sequence. From the obtained results, it is shown that this algorithm has achieved the objective set. Statistical analysis also shows the dimensions of original image and the encrypted are totally different from each other. The results are encouraging as far as the security of the cipher is concerned.

REFERENCES

[1] Gove, Nitinkumar Rajendra, Bedi Rajneesh kaur, "A New Approach for Data Encryption Using Genetic Algorithms and Brain Mu Waves", International Journal Of Scientific And Engineering Research, ISSN 2229 5558 Volume 2, Issue 5,May-2011.

[2]M.Sahithi, B.Murali Krishna ,M.Jyothi ,K.Purnima ,A.Jhansi Rani ,N.Naga Sudha, "Implementation of Random Number Generator Using LFSR for High Secured Multi Purpose Applications", (IJCSIT) International Journal of Computer Science and Information Technologies, ISSN: 0975-9646, Vol. 3 (1),pp 3287-3290 , 2012.

[3]Darwin, Charles, " On the Origin of Species", (1 ed.). ISBN 0-8014-1319-2, p. 61,24th nov 1859.

[4]John Holland. "Adaptation in natural and artificial systems: an introductory analysis with applications to biology, control, and artificial intelligence". The University of Michigan Press, ISBN 0262581116, second edition 1993 MIT press edition ,1975.

[5]Sonia Goyat, "Genetic Key Generation For Public Key Cryptography", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-3, July 2012 231.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Special Issue 9, May 2016

[6]Ankita Agarwal, "Secret Key Encryption Algorithm Using Genetic Algorithm'', International Journal of Advanced Research in Computer Science and Software Engineering,Volume 2,pp 216-218, Issue 4, April 2012.
[7]Shubhangini P.Nichat, "Image Encryption using Hybrid Genetic Algorithm", International Journal of Advanced Research in Computer Science and Software Engineering,Volume 3, Issue 1, January 2013.
[8]Manish Kumar and Haider Banka, "Changing Mutation Operator of Genetic Algorithms for Optimizing Multiple Sequence Alignment", International Journal of Information and Computation Technology.ISSN 0974-2239 Volume 3, 2013.