International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 8, August - 2014

An Image Encryption using Multilevel Randomized Genetic Algorithm Techniques

Badinedi Siva Rama Krishna Kumar[1]
M.Tech Student
Department of Computer Science & Engineering
VVIT, Nambur (V), Guntur (Dist.), India

Mulla Almas[2]
Assistant Professor
Department of Computer Science Engineering
VVIT, Nambur (V), Guntur (Dist.), India

Abstract: **Security plays an imperative role in every field of today's digital communication era. Many encryption techniques evolved through years for securing data (text, images etc). In this paper, we bring in a new image encryption mechanism that inherits process of Genetic algorithms. It applies two basic operations of Genetic algorithms (crossovers and mutations) continually for some rounds on pixel vectors of an image. The basic advantage of this approach is, it induces randomness in selecting rounds, crossover and mutation operations. Our results show that, it results in achieving high security.**

Keywords: Encoding, Decoding, Crossover and Mutation

I INTRODUCTION

Security of data (text, images, multimedia etc) has been given top most priority in almost every field. Possibility of loss of confidentiality and integrity always exist, if no proper security measures are taken. Cryptography [1] is one such area which generates secret codes to transform intelligible information to unintelligible. It provides various techniques to prevent confidentiality and integrity threats from eavesdropper. In this, sender applies mathematical function on plain text known as encryption and receiver does reverse operation on cipher text known as decryption to get original data.Two categories (Symmetric key and Asymmetric key) of cryptography mechanisms are in use based on usage of key. In symmetric key sender and receiver uses same key for encoding and decoding. But in asymmetric key, both parties use different keys, one for encoding and other for decoding.

Present work introduces a symmetric key cryptography mechanism that implements Genetic operators on images. Genetic operators are a part of Genetic Algorithms (GA). GA [2],[3] is a heuristic search that implements machine learning techniques to solve optimization problems. GA [4] is a field of artificial intelligence that imitates natural selection process. GA is majorly used in the fields of mathematics, physics, pharmacometrics, bioinformatics and phylogeneticsetc and works on population of data items.Crossover, Mutation and Reproduction are three basic operations of Genetic algorithms. Reproduction also called as Selection operator generates clones of better items in a given population. Crossover attempts to recombine two different items of parents to yield a better offspring. Mutation avoids homogeneity in the given population by adding new bits of information randomly.

Rest of the paper proceeds in the following fashion. Section II gives background work on this area and proposed image encryption scheme is presented in Section III. Decryption process is specified in Section IV. We demonstrate an example in Section V and conclude the paper in Section VI.

II BACKGROUND WORK

Image encoding process differs from information encoding because of large volumes of pixels and information redundancy. Many encryption mechanisms have been in use to secure images from possible threats based on genetic algorithms or others. A. Tragha et al.[5], described a new symmetrical block ciphering system named ICIGA (Improved Cryptography Inspired by Genetic Algorithms) which generates a session key in a random process. The block sizes and the key length are variable and can be fixed by the user at the beginning of the ciphering. ICIGA is an enhancement of the system (GIC) "Genetic algorithms Inspired Cryptography".Spillman [6] introduced a genetic algorithm based approach for the cryptanalysis of substitution cipher. It explored the option of random type search to

discover the key (or key space) for a simple substitution cipher.Spillman [7] successfully applied a genetic algorithm approach for the cryptanalysts of a knapsack cipher also. In 2006, Garg studied that the efficiency of genetic algorithm attack on knapsack cipher can be improved with variation of initial entry parameters.

Garg [8] study gives the base that genetic algorithm can be used to break S-DES. Garg [9] explored the use of memetic algorithm to break a simplified data encryption standard algorithm. Nalini [10] compared the attack of SDES using Optimization Heuristics technique and GA based techniques. The results show that GA based approach minimizes the time complexity.Ankita Agarwal [11] proposed "Secret Key Encryption Algorithm using Genetic Algorithm" which encrypts image by applying single crossover and single mutation operations. It has three short comings. Firstly it does only single crossover and mutation operations on each vector of 8 pixels. Second, it does not result high confusion and diffusion on each vector. Finally, the cipher image produced after the process is clearly identifiable with original image.

Our approach is an extension to [11] that tries to avoid existing problems. In this paper we try to apply multiple crossovers and mutations on each vector. Therefore it scrambles, modifies more pixels and hence the resulted cipher image is not easily identifiable from the original ones. Another advantage of this approach is, the pixels to go through multiple crossovers and mutations in each vector are randomly selected based on keys thus achieving high security in the process.

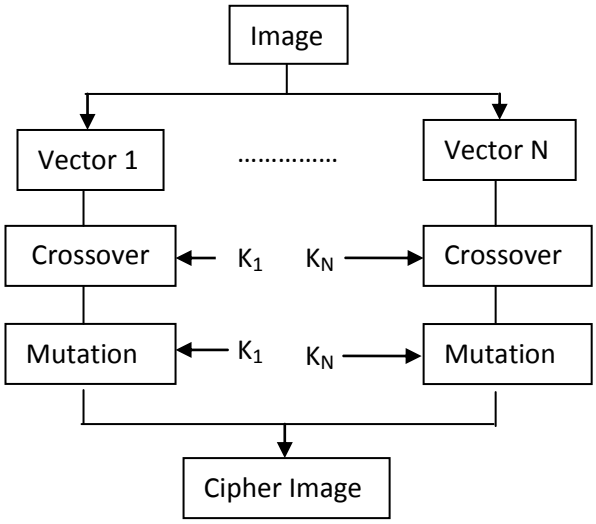

Fig 1: Block Diagram of the Encryption

III ENCRYPTION

The block diagram of the encryption is given in figure 1 and algorithm is presented in figure 2. The encryption process starts with constructing N vectors of pixels by reading successive 8 pixels from given image. Since each vector contains 8 pixels, it constructs N keys of size 8 bits and computes their values randomly using random generator. In third step, it expands each key of size 8 bits to 16 bits by concatenating key value to its ones complement (~).

1. Read image into N vectors of 8 pixels
2. Construct N keys of size 8 bits
3. Expand N keys to 16 bits by
   $K_i = K_i \,||\, \sim (K_i)$, $1 \le i \le N$

4. For each vector V in V_1 to V_N
   a) Form 5 sub keys from K_V
      a = D(K_V(1-3))
      b = D(K_V(4-6))
      c = D(K_V(7-9))
      d = D(K_V(10-12))
      e = D(K_V(13-15))
   b) Swap Pq and Pr pixels in V for each q in {a,b,c,d,e} and r = next value of q in circular fashion, $q \neq r$

   End For

5. For each vector V in V_1 to V_N
   a) If MSB(K_V) is 0
      $NK_V = K_V$(8-15)
      Else
      $NK_V = K_V$(0-7)
      End If
   b) For i = 1 to 8 pixels in V
      If NK_V(i) == 1
      Pi = 255 – Pi
      End IF
      End For

6. Construct Cipher Image
7. Write N keys of size 8 bits to key file

Fig 2: Proposed Encryption Algorithm

The resulted N vectors are distributed in parallel to crossover and mutation phases. Step 4 demonstrates crossover process which goes in two steps. First step forms 5 values {a,b,c,d,e} which is done by extracting 3 bits of corresponding key values from MSB -1 to LSB excluding MSB bit. Each set of 3 bits will give index of a pixel in a vector V. Here D is a function that finds decimal values of 3 bits. Second step in the crossover simply swaps the pixels in

vectors based on obtained 5 values where Pq and Pr denote two pixels occupying positions q and r in a vector.

Mutation procedure is given in step 5 which is operated on N vectors similar to Crossover. For each vector it again constructs a new 8 bit key (NK_V), one bit for each pixel from the expanded key (K_V) of corresponding vector. This is done by checking MSB of expanded key. If MSB is 0 then new key gets higher byte of K_V and gets lower byte in case MSB is 1. The second step of mutation subtracts each pixel value from 255 where the corresponding bit in NK_V is 1, otherwise pixel is left unchanged. Finally cipher image is constructed from merging N vectors and N keys are then written to key file which are given in steps 6 and 7.

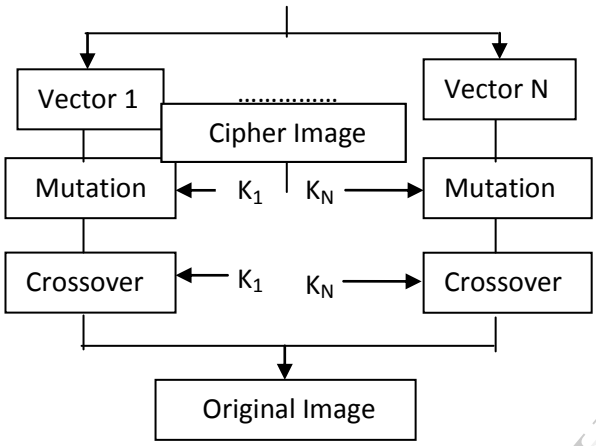

Fig 3: Block Diagram of the Decryption

IV DECRYPTION

Decoding mechanism is quite simple that simply does reverse mechanism of the encryption process which is given in figure 3. Similar to encoding process, it initially reads cipher image into N vectors of 8 pixels and also reads 8 bit keys from the key file. Then each vector goes to mutation and crossover rounds for getting modification unlike encryption. All vectors after processed through two operations are combined to get original image.

V ILLUSTRATIVE EXAMPLE

We try to exhibit the multiple crossover and mutation techniques with a simple example in this section.

V = {101, 200, 75, 96, 143, 80, 157, 62}

K_V = 10010111

K_V = 1001011101101000

Here V denotes a vector of 8 pixels which form a portion of an image. Second and Third lines give key of V constructed initially of size 8 bits and then expanded to 16 bits by appending its ones complement to it. Crossover process then forms a set of 5 values by extracting 3 bits from expanded key from MSB – 1 position to LSB as shown below.

a = 1 (001), b = 3 (011), c = 5 (101)

d = 5 (101) and e = 0 (000)

Here maximum 5 exchanges can be done based on five values. The exchange process based on 5 values and resultant vector v is given below.

Case 1: **a ≠ b** swap 1 and 3 pixels in V

V = {101, **96**, 75, **200**, 143, 80, 157, 62}

Case 2: **b ≠ c** swap 3 and 5 pixels in V

V = {101, 96, 75, **80**, 143, **200**, 157, 62}

Case 3: **c = d** No swapping in V

V = {101, 96, 75, 80, 143, 200, 157, 62}

Case 4: **d ≠ e** swap 5 and 0 pixels in V

V = {**200**, 96, 75, 80, 143, **101**, 157, 62}

Case 5: **e ≠ a** swap 0 and 1 pixels in V

V = {**96**,**200**, 75, 80, 143, **101**, 157, 62}

Mutation Process follows Crossover whose new key will be **NK_V = 01101000**since MSB of K_V is 1 where new key gets lower byte of K_V. Changeover of pixel values based on their key bit values is shown in following table.

0	1	1	0	1	0	0	0
96	55	180	80	112	101	157	62

From the entire process it is clear that initial vector V = {101,200,75,96,143,80,157,62} and modified vector after encoding process V^1 = {96,55,180,80,112,101,157,62}.

VI CONCLUSIONS

Our approach employs multiple crossover and mutation techniques on vectors of 8 pixels that try to solve problems in Secret Key Encryption Algorithm using Genetic Algorithm. In this, each vector undergoes only one crossover and mutation operation. Hence it does not produce high diffused and confused cipher image. The original image can be easily recognized from cipher image. But in our approach, cipher image will be completely different from original ones and it cannot be easily revealed. If an eavesdropper has to do brute force attack on the cipher image, then he require N trials

$$N = \sum_{k=1}^{n} 2^8$$

Where n is the number of vectors of 8 pixels resulted from the image. We strive to integrate more confusion and diffusion mechanisms in our future work.

REFERENCES

[1]N.Koblitz"A Course in Number Theory and Cryptography", Springer-Verlag, New York, Inc., 1994.
[2] David E Goldberg, „Genetic algorithms in search, optimization and machine learning",Addision- Wesley Pub.Co.1989.
[3] A.J.Bagnall, "The Applications of Genetic Algorithms in Cryptanalysis", School of Information Systems, University Of East Anglia, 1996.
[4]http://en.wikipedia.org/wiki/Genetic_Algorithms
[5]Tragha A., Omary F., Mouloudi A.,"ICIGA: Improved Cryptography Inspired by Genetic Algorithms", Proceedings of the International Conference on Hybrid Information Technology (ICHIT'06), pp. 335-341, 2006.
[6]SpillmanR,Janssen M, Nelson B and Kepner N, "Use of Genetic Algorithm in Cryptanalysis of Simple Substituion Cipher" Cryptologia, Vol.17, No.4, pp. 367-377, 1993.
[7]SpillmanR,"Cryptanalysis of Knapsack Ciphers using Genetic Algorithms", Cryptologia, Vol.17, No.4, pp. 367-377, 1993.
[8]GargPoonam, Genetic algorithm Attack on Simplified Data Encryption Standard lgorithm, International journal Research in Computing Science, ISSN1870-4069, 2006.
[9]GargPoonam, Memetic Algorithm Attack on Simplified Data Encryption Standard Algorithm, proceeding of International Conference on Data Management, February 2008, pg 1097-1108 .
[10]Nalini, Cryptanalysis of Simplified data encryption standard via Optimization heuristics, International Journal of Computer Sciences and network security, vol 6, No 1B, Jan 2006.
[11] Ankita Agarwal, "Secret Key Encryption Algorithm using Genetic Algorithm", International Journal of Advanced Research in Computer Science and Software Engineering, vol 2, Issue 4, pg 216 – 218, April 2012.

AUTHORS

Badinedi Siva Rama Krishna Kumar is pursing Master of Technology in Computer Science and Engineering from JNTU Kakinada. He has received Bachelor of Technology in Computer Science and Engineering from Acharya Nagarjuna University in 2012. His research interests are Information Security and Web Technology.

ShaikMulla Almasis working as AssistantProfessor in VVIT, Andhra Pradesh, INDIA. She has received B.Tech from JNTU Hyderabad and M.Tech from ANU. Her researchinterests are Networking and Cryptography.