# Optimized Data Encryption System Based on GA

K.Thamodaran
*Head, PG and Research Dept. of C.S.,*
*Marudupandiyar College,*
*Thanjavur, Tamilnadu,India.*

***Abstract—*** *Encryption techniques are playing vital role to alter the digital data in to another form which is tough to understand and maintain the data confidentiality. In this paper an optimized data encryption system based on interweaving technique and Genetic Algorithm(GA) is developed which provide solutions to the issues such as statistical attacks, confidentiality, illegal duplication and manipulation of digital data. GA is an important optimization technique and is employed to optimize the performance of our proposed system. The transposition or permutation of characters in the plaintext is responsible for confusion, and the influence of each bit of the secret key on each plaintext causes diffusion. The 256 bit symmetric key is generated with help of GA and integrated for encryption.*

**Keywords —** *Cryptography, Decryption, Encryption, Genetic Algorithm, Interweaving, Secret Key.*

## I. INTRODUCTION

In modern communication world, owing to speedy growth of the internet the security of digital contents has become more significant and challenging one. To exchange the data between two parties on the network, it is very essential to provide authentication and confidentiality. Confidential data is challenging to exposing its meaning to an eavesdropper. Cryptography means study of secret writing. Cryptography is related to information theory and security such as confidentiality, data integrity, data authentication and secure transmission over insecure networks. A cryptographic algorithm or function is used in the encryption and decryption process with help of secret key. Secret key plays a vital role in symmetric key encryption method. The size of the key is very significant in the symmetric key encryption [1],[2],[3],[4]. The size of block and length of the key are variable and be capable of perform the ciphering process and fixed based on the requirements. The ICIGA system is an enhancement of the system known as Genetic algorithms Inspired Cryptography (GIC) [5],[6].

Nitin Kumar, Rajendra Bedi, Rajneesh Kaur have offered a security system through brain Mu waves, genetic algorithms and pseudorandom binary sequence. This methodology of securing the confidential data is highly safe and reliable [7]. Ankita Agarwal have presented an encryption scheme with help of Genetic Algorithm which is used to produce a new encryption method by exploitation the powerful features of the Crossover and Mutation operations of GA[8]. Faiyaz Ahamad proposed a system which employed GA to generate Pseudo random numbers. The encryption process follows the working of the crossover operator and mutation operator. It uses the concept of memetic algorithms and pseudorandom binary sequence. In key generation procedure nine parameters of linear congruential generators are used [9].Soniya Goyat presented security scheme using Genetic Algorithm to produce strong key for better encryption and decryption. The author used a threshold value for selection. The coefficient of correlation is used to check the randomness of the sample. [10]. S.Mishra, S. Bali have offered a security system by means of genetic algorithms and pseudorandom binary sequence to develop the secret keys for encryption and decryption[11].

Dr.Dilbag Singh, Pooja Rani, Dr. Rajesh Kumar have proposed an algorithm using genetic algorithm for cryptography to find an optimized solution for a given problem. The concept of genetic algorithm has been incorporated within cryptography algorithm to get an optimized solution and within minimum possible time[12]. Dutt I, Paul S. Chaudhuri SN. have offered network security system through genetic algorithm to send a message in a secure manner to the receiver. This system provide the facility to sender who enters a complete message and can encode the message by utilizing crossover and mutation of genetic algorithm[13]. Sindhuja K and Devi PS have dealt the security system with help of genetic algorithm for sending a secured message to the receiver. This algorithm assists the user and generates new cipher text every time. Receiver on the other hand, will receive the message in the encoded cipher text form and will recover the original message by mapping the cipher text in the decryption algorithm [14]. Prasenjit Kumar Das, Pradeep Kumar have offered a cryptographic system using genetic algorithm and blowfish algorithm for image encryption and decryption. The Genetic algorithm is used to establish the key which is an important aspect in any cryptographic algorithm. The approach is to providing high level of security to the image with less computational head to improve the image security[15]. Shruti Sekra, Samta Balpande, Karishma Mulani proposed a image security scheme through Genetic Algorithm. In this scheme, the message or the text file is considered as input from the user which needs to get embedded in the image file. It focuses on hiding secret messages inside a cover image. The most important property of a cover image is the amount of data that

can be stored inside it without changing its visible properties [16].

In this paper, a proficient optimized data encryption system is developed with help of interweaving technique and genetic algorithm for data confidentiality and authentication. The rest of this paper is organized as follows. The section II provides the features of genetic algorithm and its importance in generating secret keys. In section III, the information regarding interweaving technique and its significance in making diffusion are offered. The section IV explains about proposed optimized data encryption method. The experimental results and security analysis are presented in section V and section VI concludes this paper.

## II. GENETIC ALGORITHM

In 1970, John Holland, University of Michigan has developed Genetic Algorithm based on the mechanics of biological or natural evolution. GA is a Directed search algorithm and recognizes the adaptive processes of natural systems also maintain the robustness of natural systems. Fundamentally Genetic algorithm is a heuristic search, optimization and machine learning techniques based on the principles of the Darwinian idea of Survival of the fittest and natural genetics[17]. Genetic Algorithms is a class of probabilistic optimization technique with good heuristics that is usually applied to discrete optimization problems. GA can deliver fast and favourable solutions over a large search space. To model the problem as a GA problem, the fitness function, chromosome and GA operators should be defined. In GA based optimizations, the problem to be addressed is defined as an objective function that indicates the fitness of any possible solution. According to the problem specific constraints, a population of candidate is initialized, named as chromosome, which is a finite-length string. During practical GA based optimization processes, three GA operators known as reproduction, crossover, and mutation, are applied to the chromosomes repeatedly and measured [18].

### *A. Selection*

Selection of both parents is random in nature. Chromosomes in forthcoming generation, i.e. child chromosomes relies on parents selected here. It is quantitative criterion based on fitness value to choose the chromosomes from population which are going to reproduce.

### *B. Crossover*

In crossover operation two chromosomes are taken and a new is generated by taking some attributes of first chromosome and the rest from second chromosome. Crossover operation is classified in to three namely Single Point Crossover, Two Point Crossover, Uniform Crossover.

### *C. Mutation*

Mutation is used to maintain genetic diversity from one generation of population to the next. It is similar to biological mutation. GAs involves string-based modifications to the elements of a candidate solution. These include bit-reversal in bit-string GAs. This operator randomly flips some of the bits in a chromosome.

The Simple Genetic Algorithm is as follows.

Produce an initial population of individuals
Evaluate the fitness of all individuals
While termination condition not fulfilled do
Select fitter individuals for reproduction
Recombine between individuals
Mutate individuals
Evaluate the fitness of the modified individuals
Generate a new population
End while

## III. INTERWEAVING TECHNIQUE

The proposed encryption system make use of interweaving technique to improve the level of security of encrypted data. An interweaving technique represents transposition of the binary bits, coefficients and blocks to the adjacent rows and columns. As a result the interweaving process makes confusion and diffusion in the given data at each stage. Let P be a matrix of (M x N =512 x 512) bits. The matrix P contains the bits values or coefficients of data matrix. Q is the interviewed matrix. In order to find the number of blocks exist in the matrix, divide the width and height of matrix by width and height of block size 4096 bits (M x N=64 x 64). In this scheme the matrix size is (512 x 512). So that ((512 x 512 bits) / (64 x 64 bits ))= 64 blocks. Consider the binary bits of modified data matrix Q. Consider m=n=p. $[q_{ij}]$, i = 1 ..m, j = 1 .. l, Where l=(n*8).

Initially rotation is activated in circular manner that is the first row moves in the left direction and observe that it expects the form $[a_{12}, a_{13}, \ldots, a_{1n}, a_{11}]$. Here, each element has moved one step left and the first element has moved right to the last position. This practice is passed out for rows 1, 3, 5... and so on. Likewise, succeed a circular shift of the columns towards up numbered 2, 4, 6,... etc. After implementation of the aforesaid steps, the resultant interweaved data matrix Q is arrived. The above practice finishes the process of interweaving. An inverse interweaving is used to get original data matrix.

## IV. Proposed Optimized Data Encryption System Using Genetic Algorithm

In this proposed optimized data encryption system genetic algorithm (GA) and interweaving technique are utilized. An interweaving technique is integrated to accomplish shuffling of bits, coefficients and blocks which remarkably decreases the correlation among data bits. With the intention of increasing the security, the sign bit of the data coefficients are encrypted. The GA is employed to generate the secret key and sub keys to regulate the encryption process. Pseudo random numbers are selected as parents in nature and utilized to generate 256 bit lengthy secret key and 64 bit lengthy sub keys to increase the robustness of the encryption process.

### *A. Procedure for Key generation*

An excellent cryptosystem should in fact vary the aspects of its encryption method in a symmetric key dependent way, though high security does not require the combination of distinct encryption algorithms. In order to perform data encryption the secret keys and sub keys are generated with help of genetic algorithm (GA). The generated binary strings are for genetic operations. In this system, the number of populations is 256. The selection rate is 50%, that is only the 128 populations with higher fitness values are kept for the next iteration, and the remaining 128 are produced by the crossover operation. The 25% of all the bits(64 bits) are randomly selected for mutation and purposely flipped. The main idea of using GA is to create effective secret keys for encryption.

Four sequences $S_1$, $S_2$, $S_3$ and $S_4$ with $k_1$, $k_2$, $k_3$ and $k_4$ are taken as seed values respectively. Sequence $S_1$ is utilized to encrypt the sign-bit of the selected coefficients to diffuse the statistics, $S_2$ is occupied to perform pixel permutation and $S_3$ is applied to attain coefficient permutation. The sequence $S_4$ is included using $k_4$ as the seed value, which is integrated to accomplish block permutation.

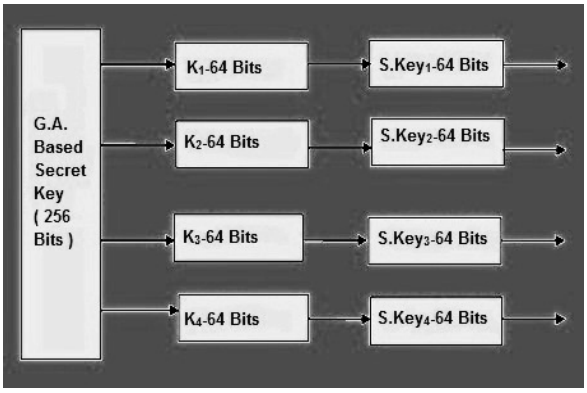


Fig. 1: GA Based Secret Key Generation System

### *B. Algorithm for Encryption*

The proposed data encryption system is performing encryption through genetic algorithm and interweaving technique. The data bits are encrypted through an EX-OR operation with a secret key. An interweaving technique is used to shuffle the data bits for making more confusion.

**Step 1.** Generate the secret key $S_k$ by means of GA.
**Step 2.** Select data bits from the data matrix and perform encryption process by doing EX-OR operation by means of the given secret key.
**Step 3.** The sign-bit of the coefficients are encrypted using the sub-key $k_1$.
**Step 4.** Select the coefficient bits for interweaving with help of the sub-key $k_2$.
**Step 5.** Select the coefficients for interweaving with help of the sub-key $k_3$.
**Step 6.** Select the data blocks to perform interweaving by means of sub-key $k_4$.

### *C. Algorithm for Decryption*

The Decryption algorithm is as follows:

**Step 1.** Consider the encrypted data matrix throughout the proposed system for decryption.
**Step 2.** Generate the secret key $S_k$ by means of GA.
**Step 3.** The secret sub key $k_4$ is applied to perform inverse interweaving of blocks.
**Step 4.** The secret sub-key $k_3$ is used to perform inverse interweaving of coefficients.
**Step 5.** Select the coefficient bits for inverse interweaving with help of the sub-key $k_2$.
**Step 6.** The sign-bit of the coefficients are decrypted using the sub-key $k_1$.
**Step 7.** Select data bits from the data matrix and perform decryption process by doing EX-OR operation by means of the given secret key.

## V. Experimental Results and Security Analysis

### *A. Key Space Analysis*

The key space should be sufficiently large to make the brute-force attack insignificant in the well cryptosystem. Key space means the total number of different keys can be exercised to perform encryption and decryption processes. A 256 bits key is engaged in this system. If any trespasser has attempted to break the key, as a result the attacker has to try out $2^{256}$ ($2^{256} \approx 1.1579 \text{ X } 10^{77}$) combinations of the secret key. The data encryption by the use of such a large key space is more than enough for better security.

### *B. Key sensitivity analysis*

Three slightly changed secret keys are used to test the sensitivity analysis of key by means of encryption and decryption processes. Initially, the test data (plaintext) to be encrypted is shown in figure 2. The test data is encrypted with help of key-1 and the ciphered data is shown in figure 3. Then encrypted data is decrypted with help of key-1 and the deciphered data is shown in figure 4. Consecutively LSB one element of key-1 is changed to form the key-2 and is used to encrypt the same test data to get the encrypted data and the same is shown in figure 5. Similarly MSB one element of key is changed to form the key-3 and is utilized to encrypt the same test data to get the encrypted data and the same is shown in figure 6.

The word cryptography comes from latin crypt, meaning secret and graphia, meaning writing cryptography's literally, the science of secret writing, the study of how to obscure what you write so as to render it selectively unintelligible.

Fig. 2: Plain Text

TêzTlaÃh]fN80-wb.Œ`)öwGðd9{ç¾aŒB˜`r6B®jfmdt!?e,=Q|(âê{™_r±Xôw=ñ¶¨C…[pôthÜltgOs‘ QçgJ¤næÿY|rp;£DJ□à GpºGzOda7SH†BñÄa~¸$1×Hm?â8B•"í%çL`BÂå¨dº>YäÄyò□wòMfe]ÍG<; H&BrÊO2çCØIÖåV$g4ÑrPca¢ieªo_T;^àÊx,vXtUp<[xá½§ 27 àbgËmWj•O8d¶nâiZÛ‘ {rRÃ□ñšS.p p)x?=t0f¿(%c…_åÞÅ*Ú4äçgvlùrà1HN?ogëJñ~{.áOmëIg2□?úæ²k"ƒqS9§Eògp=äe.ÅfjâZ□htr†Á.1o äxEdÓ7t?X©KX`6<àÖuÄp□Pg 27 Rþ$vdL?ðÌÃ~æâr:x□[úà:*Kr4vp□Tô5a¸(†áöÚý0àE§x□%ÚC"n] å;Ð^)ä«(@MKà^v:Å=g¬T°p”^áÈ^Äiä^gÌyg=“pæf*jLB!IZö,^SrY~PWHák9□I0t93ê%[á[n©I Pg·.~ ,ŒOkãdÉbâ¶3o!B=rÁ?u<ñ”F'óPpGtÉ3¶"çJ¿Z'xæŠbeZr}q"¾Zà§\6DOpÙ4Fù<a□>{y¹0ñ□Y}{2727¦ î5´v(ò%w#0zaX{veeaZ>□Dá6i=t‡UYRhäPAÄ1ÕrÒE3,à«~T@e~e_e□ÛEðgñ[Q©%÷N‘5™|'hZEæ et®DjhE9at2fSt\äcSŽb¢ülòß(SJHâzCO*Û$á>1nMSäQêmgåkHLââ0òòðK:7c$äuùïwâ"žBBQréRZf äB27¤z›t){Ï'27l

Fig. 3: Encrypted Text Using Key-1

The word cryptography comes from latin crypt, meaning secret and graphia, meaning writing cryptography's literally, the science of secret writing, the study of how to obscure what you write so as to render it selectively unintelligible.

Fig. 4: Decrypted Text Using Key-1

Ë&µYöŽ(x²RG«CáºMúytKtCÂ3á”N-g¬mµK÷oæI%>P¢TtÚ'%—g3t!KøIóaC'‡_÷ä_87C ó~<F6ò)²4t¼6□,oUô\e,<d'f}ñ¶G!q¼Dm|¼ç#I‘d¼if}$`,Ì[Á□Yeô1a/w1?çh™*nböé`æWäV]itq¯ÞLçæ$ `'"žBpç3/¬-ãbr_X□¨(òór¾0œxâK«lûô;m€rp·ä¾Hu&© "i& oBr]ñ$öû-NWaBS³tbeàþmë]‘Gt®;□G¥$ q6O|elñ§^œ~ç’3¡Wôoô=´÷#d€QûIö?(‡Q£^rzAý—á08-xžt™H48K?ä²uN6n=!ò1Abçè>\&É-vM¬7ó□àw+Õò%gÍ%□ 9ƒ:ŽttƒLÊ2ÅLçKJ«$yxà4+_²IrêrfkúmäF{I-1guzR.¹JdãzÔ-ùYä‹xÂ^™urÔO>PmYIáH*Gvûtn m;HD`S-Ÿ\ò5-aÓ9ä8B«+%,e□+ª™t3*$|>J äð 28 åWZDâÊ{ êt¿T±gháž 28 ¶‖u)vL7ãä=JÝwZ5eáf½f·pñŒ¨$88[u£yp^¨gôî?F³tgFgx□ÄkáävQgXy`#¥t|{S¦,ä|:^Zxe¡We) ØeeÂu¦ená3v(P¯eæXa_l~áÖHIB"GbGV³]eö\Ù#<ä„#7%E 3)□(J'Ã5

Fig. 5: Encrypted Text Using Slightly Modified Key-2

.Œ`)öwGðd9{ç¾aŒB˜`r6B®jfmdt!?e,=Q|(âê{™_r±Xôw=ñ¶¨C…[pôthÜltgOs‘QçgJ¤næÿY«|rp;£DJ□à GpºGzOda7SH†BñÄa~¸$(1×Hm?â8B•"í%çL`BÂå¨dº>YäÄy8ò□wòMfe]ÍG<-.;H&BrÊO: 2çCØIÖåV$g4ÑrPca¢ieªo_T;^àÊx,vXtUp<[xá½§ 28 àbgËmWj•O8d¶nâìZÛ‘{r*RÃ□ñšS.pp)x?=t0f¿(% c@…_åÞÅ*Ú4äçgvlùrà1HN?ogëJñ~{.áOmëIg2□?úæ²k"ƒqS9§Eògp=+äe.ÅfjâZ□htr†Á.1oäxEdÓ7t?X ©K«X`6<àÖuÄp□Pg28Rþ$vdL?ðÌÃ~æâdnCr:x□[úà:*Kr4vp□Tô5a¸(†áöÚý0àE§x□%ÚC"n]å;Ð^)ä«(@ MKà^v:Å=g¬T°p”^áÈ^Äiä^gÌyg=“pæf*jLB!IZö,^SrY~PWHák9□I0t93ê%[á[n©I Pg·.~"æ,ŒO#qkãdÉ bâ¶3o!B=rÁ?uÿ<ñ”F'óPpGtÉ3¶"çJ¿Z'xæŠbeZ}q"¾Zà§\6DOpÙ4Fù<a□>{y¹0ñ□Y}{2828¦î5´v(ò%w#0z >aX{veeaZ>□Dá6i=t‡UYRhäPAÄ1ÕrÒE3,à«~T@e~e_e□ÛEðgñ[Q©÷N‘5™|'hZEæet®DjhE9at2fSt\ä cSŽÿ¢ülòß(SJHâzCO*Û$á>1nMS|{S¦,ä|:^Zxe¡We)ØeeÂu¦ená3v(P¯eæXa_l~áÖHIB"GbGV³]eö\Ù#<ä„ #7

Fig. 6: Encrypted Text Using Slightly Modified Key-3

QêmgåkHLââ0ò(8ä~!®{$…,Ã\çR□œf®V□OªqRBìòðK:7c$äuùïwâ"žBBQréRZfäB 28 ¤z›t){Ï' 28 l Ë&µYöŽ(x²Rr«CáºMúytKtCÂ3á”N-â¬mµK÷oæI%>P¢TtÚ'%—g3t!KøIóaC'‡_÷ä_87C ó~<F6ò)²4t¼6□,oUô\e,<d'f}ñ¶G!q¼Dm|¼ç#I‘d¼if}$`,Ì[Á□Yeô1a/w1?çh™*nböé`/æWäV]itq¯ÞLçæ$ `'"žBpç3/¬-ãbr_X□¨(òór¾0œxâK«lûô;m€rp·ä¾Hu&©"i&oBr]ñ$öûNWaBS³tbeàþmë]‘Gt®;□G¥$xvixed €QûIö?(‡Q£^rzAý08-xžt™H48K?ä²HuN6n=!ò1Abçè>\&ÉvM¬73o!B=ó□àw+Õò%gÍ%□9ƒ:ŽttƒLÊ2 ÅLçKJ«$yxà4+_²IrêrfkúmäF{I-1guzR.¹JdãzÔùYä‹xÂ^™urÔO>PmYIáH*Gvûtnm;HDS-Ÿ\ò5-aÓ9ä8B «+%,e□+ª™êt¿T±ghS¦,ä|:^Zxe¡We)ØeeÂu¦ená3v(P¯eæXa_l~áÖHIB"GbGV³]eö\Ù#<ä„#%3)|)<”&rw23

Fig. 7: Unsuccessful Decrypted Text Using Slightly Modified Key-2

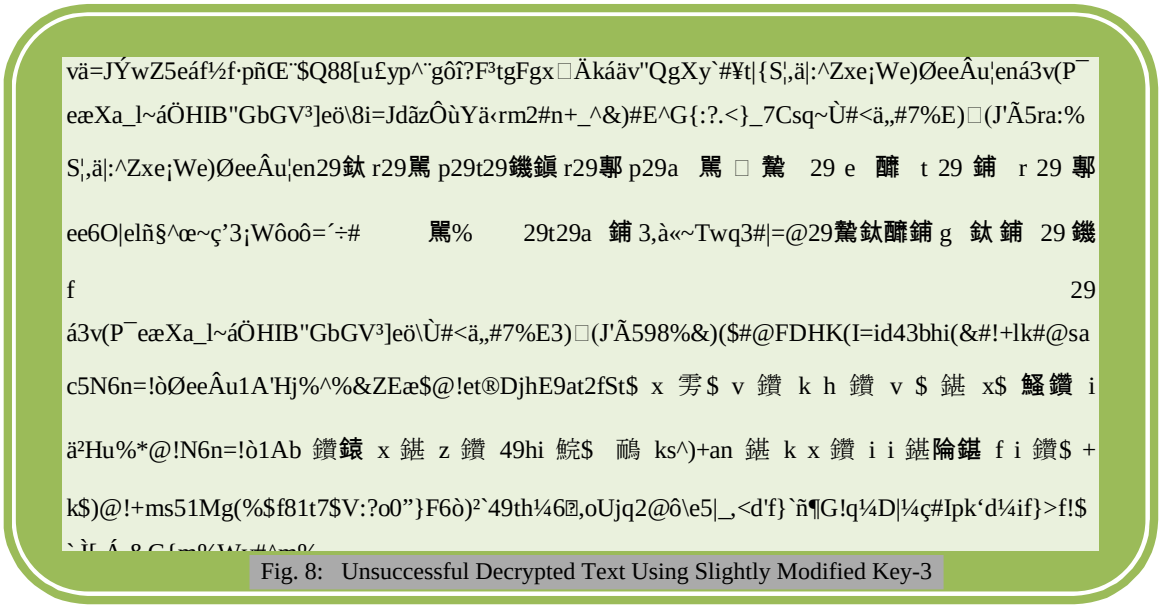


Fig. 8: Unsuccessful Decrypted Text Using Slightly Modified Key-3

Additionally the encrypted test data via slightly modified keys are compared. It is monitored that the encrypted data shown in figure 3 is varied from the encrypted data shown in figure 5. Similarly the encrypted data shown in figure 3 is varied from the encrypted data shown in figure 6. Since matching the results of three encrypted data sets related with the above mentioned slightly modified keys, there is no similarity between the encrypted data sets even though these data sets have been created via slightly modified secret keys. Finally, when a secret key-1 is utilized to encrypt the data matrix and a slightly modified key-2 and key-3 generated by modifying one element of key-1 are used to decrypt the same ciphered test data, both decryptions are failure as shown in figure 7 and figure 8.

## VI. Conclusion

In this paper, an efficient security system with help of an interweaving technique and genetic algorithm for data encryption is proposed. An interweaving technique is occupied to execute shuffling of bits, coefficients, blocks. Subsequently the sign bit values of selected coefficients are encrypted to reduce the correlation among the data bits. The proposed scheme performs bit shuffling in selected rows and columns of each block are used to further reduce the correlation. A secure key matrix is generated (512-bits) and used to perform the encryption. From the experimental results, it is evident that the proposed encryption scheme offers better results. This system attains the advantages of using interweaving technique and GA. The level of security can be more improved if necessary, by increasing the number of permutation rounds selected rows and columns of each block.

## References

[1] Bruce Schneider, "Applied Cryptography", *John Wiley and Sons*, 1996.

[2] Menzes A. J., Paul, C., Van Dorschot, V., Vanstone, S. A., "Handbook of Applied Cryptography", *CRS Press 5th Printing*,2001.

[3] Trappe.W, Washington.L.C., "Introduction to Cryptography: with Coding Theory", *Prentice-Hall, Upper Saddle River, NJ*, 2002.

[4] Stallings W. Cryptography and Network Security- *Principles and Practices. 3rd ed. Upper Saddle River, NJ: Prentice Hall*; 2003.

[5] A. Tragha, F. Omary, A. Kriouile, ,Genetic Algorithms Inspired Cryptography A.M.S.E Association for the Advancement of Modeling & Simulation Techniques in Enterprises, *Series D : Computer Science and Statistics*, November 2005.

[6] Behrouz A.Forouzan , "Cryptography and Network Security " ,*TMH*, 2010.

[7] Nitin Kumar, Rajendra Bedi, Rajneesh Kaur, "A New Approach for Data Encryption Using Genetic Algorithms and Brain Mu Waves",*International Journal of Scientific and Engineering Research*, Volume 2, Issue 5, pp1-4, May 2011.

[8] Ankita Agarwal , "Secret Key Encryption Algorithm Using Genetic Algorithm", *International Journal of Advanced Research in Computer Science and Software* Engineering, Volume 2, Issue 4, pp216-218, April 2012 .

[9] Faiyaz Ahamad, Saba Khalid, Mohd. Shahid Hussain published a paper entitled, "Encrypting Data Using The Features of Memetic Algorithm and Cryptography" *at International Journal of Engineering Research and Applications*, Vol. 2, Issue 3, pp.3049-3051. May-Jun 2012.

[10] Sonia Goyat, "Genetic Key Generation For Public Key Cryptography", *International Journal of Soft Computing and Engineering*, Volume-2, Issue-3, pp 231-233, July 2012 231.

[11] S.Mishra, S. Bali "Public Key Cryptography Using Genetic Algorithm", *International Journal of Recent Technology and Engineering* , Volume-2, Issue-2, pp 150-154, May 2013.

[12] Dr.Dilbag Singh, Pooja Rani, Dr. Rajesh Kumar, "To Design a Genetic Algorithm for Cryptography to Enhance the Security", *International Journal of Innovations in Engineering and Technology* Volume 2, Issue 2, pp 380-385, April 2013.

[13] Dutt I, Paul S. Chaudhuri SN. Implementation of network security using genetic algorithm. *International Journal of*

*Advanced Research in Computer Sci ence and Software Engineering*, 2013; 3(2):234–41.

[14] Sindhuja K, Devi PS. A symmetric key encryption technique using genetic algorithm, *International Journal of Computer Science and Information Technology*, Vol. 5, no.1, pp 414–416, 2014;

[15] Prasenjit Kumar Das, Pradeep Kumar , "A Novel Cryptography Approach Based On Genetic Algorithm", *International Journal of Engineering Sciences & Research Technology*, pp 771-776, March, 2015.

[16] Shruti Sekra, Samta Balpande, Karishma Mulani, " Steganography Using Genetic Encryption along with Visual Cryptography", *SSRG International Journal of Computer Science and Engineering*, Volume 2, Issue 1,pp 5-9, January 2015.

[17] David E Goldberg, "Genetic algorithms in search, optimization and machine learning", *Addision- Wesley Pub.Co*.1989.

[18] Anil Kumar and M. K. Ghose,"Overview of Information Security Using Genetic Algorithm and Chaos", *Information Security Journal: A Global Perspective*, vol 18,pp 306–315, 2009.