Enciphering the information by using Range Table with Genetic Algorithms

B. Susheel Kumar
Department of CST
Yogi Vemana University Kadapa

Kanusu Srinivasa Rao
Department of CST
Yogi Vemana University Kadapa

Ratnakumari Challa
Department of CSE
RGUKT-RK Valley
AP-IIIT, Kadapa

ABSTRACT
At the present time, in contrast with the past usage of the internet has been added on. Each and every organization like Educational organizations, Government sectors, Business organizations etc is making the use of internet to enlarge their organizations. In such scenario great amount of sensitive information has being transmitted via the internet. Therefore it is vitally important to secure the information which is transmitting through the internet in order to keep it safe from the intruder attacks. To keep the information safe and secure the concept of cryptography has been developed. Different form of cryptographic algorithms are in use to enciphering the text. In this paper we will discuss about encoding the text by using range table with the help of genetic algorithms

Keywords
Cryptography, Plain text, Cipher text, Range Table, LSB, Genetic algorithms

1. INTRODUCTION
In these modern days the utilization of cryptography is essential to preserve the information from the intruders. The approach of recasting the plain text in the form of cipher text is entitled as Cryptography. The process of transforming plain text into cipher text is termed as encryption as well as the process of transforming the cipher text into plain text is termed as decryption. These encryption and decryption process will be done with the help of secret key which is shared among sender and receiver. Generally the encryption process is at sender side and the decryption process is at receiver side [1].

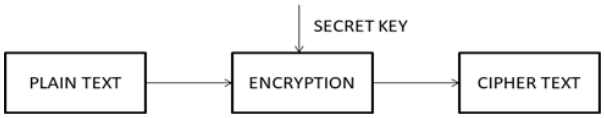

Fig 1: Encryption process

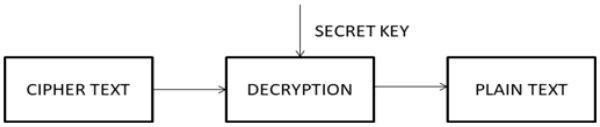

Fig 2: Decryption process

Although having so many security algorithms to hide the information intruders will make a way to break the security. Based on the kind of attack the attacks are categorized into two kinds Passive attacks, Active attacks respectively. Modification of information comes under the active attacks category whereas in passive attacks no modification of data occurs but intruders witness the network traffic.

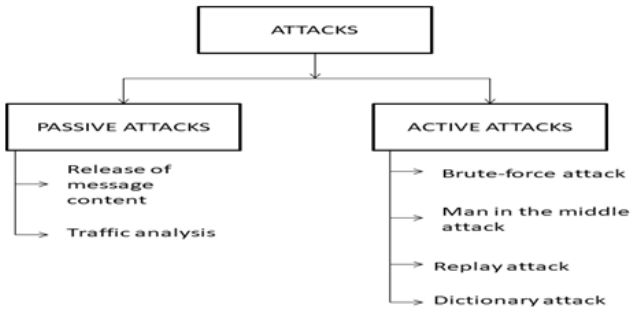

Fig 3: Attacks in cryptography

In the field of cryptography two kinds of encryption techniques are existing substitutional techniques as well as transpositional techniques namely. Substitutional approach each and every letter in the original text is fill in by the various text such as numbers, special characters, and letters [6,7].

Substitutional techniques include Ceaser Cipher, Monoalphabetic cipher, Playfair cipher, Hill cipher, Polyalphabetic cipher, and One time padding cipher. Ceaser cipher replaces the plain text letters with different letters by utilizing the formula y=(x+k)|26|. Monoalphabetic cipher can also be titled as Simple substitution cipher which simply substitutes the letters of plain text. Playfair cipher encrypts the data by using 5X5 table with the help of key. On the other hand Hill cipher works based on the formula C=(K.P) mod 26.

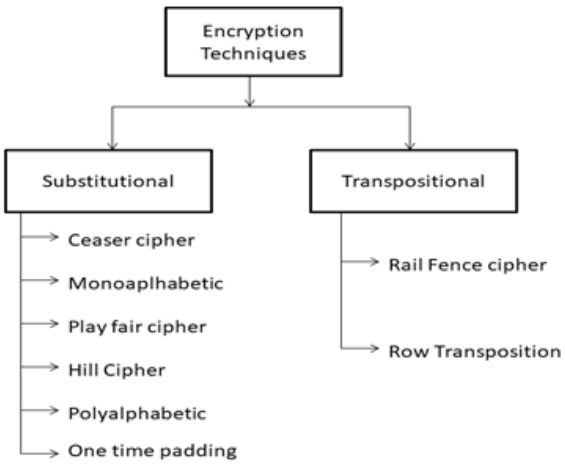

Fig 4: Encryption Techniques

Polyalphabetic cipher works by multiple substitutes of the plain text. The One time padding cipher encodes the text by use of key in the form of encryption which is equal to the length of the original text.

When we discuss about Transpositional approaches is all about rearrange the text and it have two kinds of encoding techniques namely Rail fence method and Row transposition method. The rail fence technique is also known as zig zag method in which the original text is written diagnolly based on the key size up side and down and then read it by row.

Where as in the case of Row transposition approach original text is written row wise according the key size and then read out by the column wise.

1.1 Rail Fence Cipher

Rail fence cipher comprises the plain text a sequence of diagonals and then read it row by row to create the cipher text. Following are the steps for Rail Fence Cipher [2].

Step1: Write down all the characters of plain text message in a sequence of diagnosis

Step 2: Read the plain text written in step 1, as a sequence of rows

To overcome the intruder attacks wide range of cryptographic algorithms are using in various organizations. In this paper to encode the text Least bit significant and Bit Flip Mutation in Genetic algorithms has been worn. LSB is applied in accordance with Range table.

1.2 LSB

LSB means Least significant bit which exchange the least significant bit in a byte to change the value of the byte in order to protect the plain text.

1.3 Genetic algorithms

Genetic algorithms are used to find the best-fit solution for the given problem. Usually Genetic algorithms are used in Artificial Intelligence for neural networks. Numerous kinds of genetic algorithms are present. In these genetic algorithms we use the Bit flip mutation form the mutation type [3,4] .

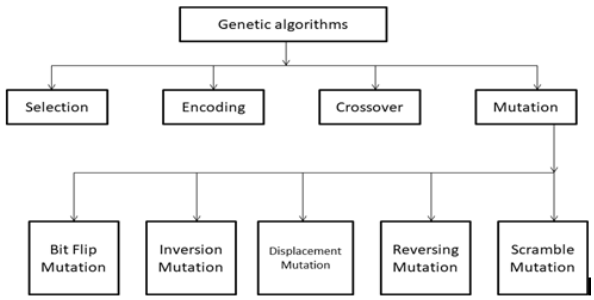

Fig 5: Types of Genetic algorithms

1.4 Range table

Range table is used to apply the LSB. Exchange the LSB bits by using the range table[5].

Table 1. Range table

RANGE	BITS TO REPLACE
0-16	1- BIT
17-32	2 -BITS
33-64	3- BITS
65-128	4 -BITS
129-255	5 -BITS

guidelines. In essence, we ask you to make your paper look exactly like this document. The easiest way to do this is simply to download the template, and replace the content with your own material.

2. LITERATURE SERVEY

This is the age of science where we deal with a huge set of data daily. Every day user shares huge amount of personal data in social sites, messaging applications, commercial sites and in other service based platforms. To accomplish transactions we need to share our credit/debit card number with passwords too, which makes the transaction very much sensitive. Randomness in the data is called Entropy. The entropy of data is directly proportional to the security of corresponding data. Security is the most favorable and mandatory feature of data transfer and storage based services. Since the quantity of data travel through the networks growing rapidly with respect to time thus enhancement in security is highly needed. According to the described variation of genetic algorithm users will have to give message as well as key also the help of these data sets, algorithm will give ciphertext and hence encryption has been achieved. At receiver's end decryption of data takes place. The key by which encryption has been done in this algorithm is combination of two matrix of equal length. It will increase the security because of dependency on both the matrix[8]. In view of the present chaotic image encryption algorithm based on scrambling (diffusion is vulnerable to choosing plaintext (ciphertext) attack in the process of pixel position scrambling), we put forward a image encryption algorithm based on genetic super chaotic system. The algorithm, by introducing clear feedback to the process of scrambling, makes the scrambling effect related to the initial chaos sequence and the clear text itself; it has realized the image features and the organic fusion of encryption algorithm. By introduction in the process of diffusion to encrypt plaintext feedback mechanism, it improves sensitivity of plaintext, algorithm selection plaintext, and ciphertext attack resistance. At the same time, it also makes full use of the characteristics of image information. Finally, experimental simulation and theoretical analysis show that our proposed algorithm can not only effectively resist plaintext (ciphertext) attack, statistical attack, and information entropy attack but also effectively improve the efficiency of image encryption, which is a relatively secure and effective way of image communication[9].

3. PROPOSED METHOD

In this section the proposed method is presented the method consists of encryption and decryption algorithms with flow charts.

3.1 Encryption Algorithm

Step 1: Consider 48n bit plain text

Step 2: Convert the original text into ASCII code

Step 3: Now convert ASCII code into Binary value

Step 4: Divide the values into two equal halves i.e. Left half and right half

Step 5: Again divide both the halves into 6 blocks of size 4

Step 6: Apply Rail Fence Cipher on both sides

Step 7: Now merge the bits into 3 bytes on both sides

Step 8: Apply the range table to replace the bits by using Least significant bit approach

Step 9: Now merge both the sides, We have 48n bit change

plain text.

Step 10: Apply the Bit Flip Mutation for changed output

Step 11: Convert the binary value into ASCII code

Step 12: We get the Final Cipher text.

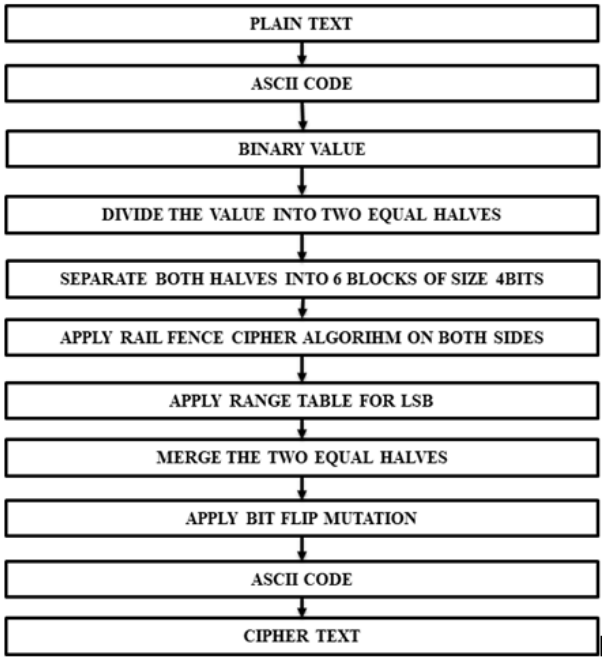

Fig 7: Flow chart for Encryption

3.2 Decryption Algorithm

Step 1: Consider the cipher text

Step 2: Convert into ASCII code

Step 3: Convert the ASCII code into Binary value

Step 4: Apply Bit Flip Mutation

Step 5: After applying the bit flip mutation we have changed cipher text

Step 6: Now divide the value into two equal halves i.e. left halve and right halve

Step 7: Again divide the both sides into 6 blocks of size 4

Step 8: Now apply the Rail Fence cipher algorithm on both sides

Step 9: Merge both sides into 3 bytes

Step 10: Apply range table to extract the Least significant bits

Step 11: Convert the binary values into ASCII code

Step 12: We get the plain text.

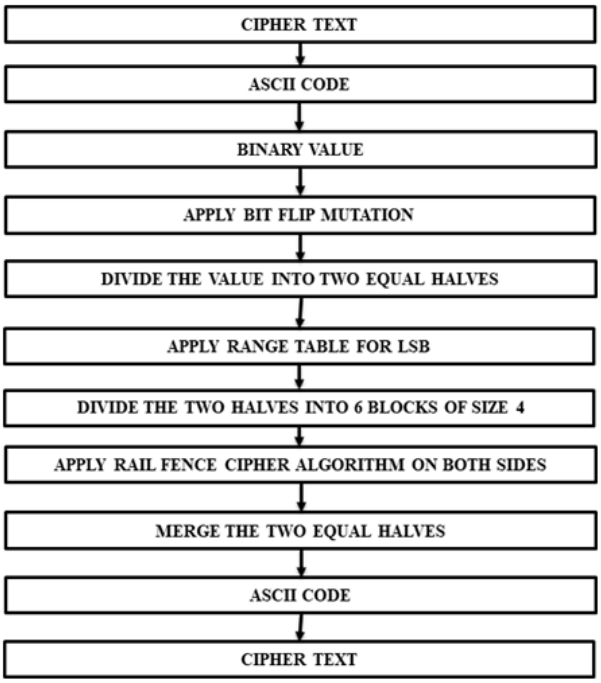

Fig 8: Flow chart for Decryption

4. EXPERIMENTAL RESULTS

The method is evaluated practically for different input values. The encryption and decryption results are presented in table2 and table3. The encryption algorithm used on the example word "STRING" and results are shown Table 2 followed by table**3.**

Table 2. Encryption process

PLAIN TEXT	ASCII	BINARY VALUE	TWO EQUAL HALVES		DIVIDE INTO 6 BLOCKS		RAIL FENCE	
					LHS	RHS	LHS	RHS
			LHS	RHS	6 BLOCKS OF SIZE 4	6 BLOCKS OF SIZE 4	6 BLOCKS OF SIZE 4	6 BLOCKS OF SIZE 4
S	83	01010011	01010011	01001001	0101	0100	0011	0010
T	84	01010100	01010100	01001110	0011	1001	0101	1001

R	82	01010010	01010010	01000111	0101	0100	0011	0010
I	73	01001001			0100	1110	0010	1110
N	78	01001110			0101	0100	0011	0010
G	71	01000111			0010	0111	0100	0111

Table 2. Encryption process continuation

MERGE		**RANGE TABLE FOR LSB**		**MERGE BOTH SIDES 48 BIT OUTPUT**	**BIT FLIP MUTATION**	**ASCII**	**CIPHER TEXT**
LHS	**RHS**	**LHS**	**RHS**				
3 BYTES	**3 BYTES**						
00110101	00101001	00110010	00101110	00110010	00100010	34	“
				00110101	00100101	37	%
00110010	00101110	00110101	00101001	00110011	00100010	34	“
				00101110	00111110	62	>
00110100	00100111	00110011	00100000	00101001	00111001	57	9
				00100000	00111001	57	9

Table 3. Decryption process

MERGE		**RANGE TABLE FOR LSB**		**MERGE BOTH SIDES 48 BIT OUTPUT**	**BIT FLIP MUTATION**	**ASCII**	**CIPHER TEXT**
LHS	**RHS**	**LHS**	**RHS**				
3 BYTES	**3 BYTES**						

00110101	00101001	00110010	00101110	00110010	00100010	34	“
				00110101	00100101	37	%
00110010	00101110	00110101	00101001	00110011	00100010	34	“
				00101110	00111110	62	>
00110100	00100111	00110011	00100000	00101001	00111001	57	9
				00100000	00111001	57	9

Table 3. Decryption process continuation

DIVIDE INTO 6 BLOCKS		**RAIL FENCE CIPHER**		**MERGE BOTH SIDES**		**MERGE BOTH SIDES 48 BIT OUTPUT**	**ASCII**	**PLAIN TEXT**
LHS	**RHS**	**LHS**	**RHS**	**LHS**	**RHS**			
6 BLOCKS OF SIZE 4	**6 BLOCKS OF SIZE 4**	**6 BLOCKS OF SIZE 4**	**6 BLOCKS 0F SIZE 4**	**3 BYTES**	**3 BYTES**			
0011	0010	0101	0100	01010011	01001001	01010011	83	S
0101	1001	0011	1001			01010100	84	T
0011	0010	0101	0100	01010100	01001110	01010010	82	R
0010	1110	0100	1110			01001001	73	I
0011	0010	0101	0100	01010010	01000111	01001110	78	N
0100	0111	0010	0111			01000111	71	G

5. CONCLUSION

In modern society it is essential to secure the information which is transmitting through the internet. Because with the increasing network security approaches security breaking methods are also increasing. And the intruders are becoming strong day by day with new hacking techniques. In this paper we have used the range table and bit flip mutation to preserve the information. Where range table is for LSB replacement and the bit flip mutation acts as a security concept in these paper.

6. REFERENCES

[1] William Stallings, "Cryptography and Network Security: Principles and Practices", 4th Edition, Prentice Hall, 2006, page numbers 30-39

[2] Hans Delfs and Helmut Knebl, "Introduction to

Cryptography: Principles and Applications", Springer, first edition, 2002, page numbers 11- 14.

[3] Katoch, S., Chauhan, S.S. & Kumar, V. A review on genetic algorithm: past, present, and future. Multimed Tools Appl 80, 8091–8126 (2021). https://doi.org/10.1007/s11042-020-10139-6

[4] K. F. Man, K. S. Tang and S. Kwong, "Genetic algorithms: concepts and applications [in engineering design]," in IEEE Transactions on Industrial Electronics, vol. 43, no. 5, pp. 519-534, Oct. 1996, doi: 10.1109/41.538609.

[5] Nasution, A & Efendi, Sahrul & Suwilo, S. (2018). Image Steganography In Securing Sound File Using Arithmetic Coding Algorithm, Triple Data Encryption Standard (3DES) and Modified Least Significant Bit (MLSB). Journal of Physics: Conference Series. 1007. 012010. 10.1088/1742-6596/1007/1/012010.

[6] Behrouz A. Forouzan, " cryptography and Network Security", Special Indian Edition, TATA McGraw Hill.. .

[7] S.Tanebaum, " Modern Operating Systems", Prentice Hall, 2003.

[8] S. Dubey, R. Jhaggar, R. Verma, D. Gaur, "Encryption and Decryption of Data by Genetic Algorithm", International Journal of Scientific Research in Computer Science and Engineering Vol.5, Issue.3, pp.42-46, June (2017).

[9] Jian Wang etc " Digital Image Encryption Algorithm Design Based on Genetic Hyperchaos", international journal of optics, Volume 2016 , https://doi.org/10.1155/2016/2053724.