First International Conference on Emerging Trends in Engineering, Management and Scineces"
December 28-30, 2014 (ICETEMS-2014) Peshawar, Pakistan

"Hiding Information Using Techniques of Polybius Square and Steganography to ensure Security"

Muhammad Ismail
Computer Science Deptt,
City University of Science & IT.
Peshawar, Pakistan.
Stylish_ismail@yahoo.com

Taifoor zarin
Electrical Engineering Deptt,
City University of Science & IT.
Peshawar, Pakistan.
taifoorzareen@gmail.com

Najam Us Saqib
Computer Science Deptt,
City University of Science & IT
Peshawar, Pakistan
nsaqib92@yahoo.com

Abstract:
Nowadays it is very difficult to confidentially transferring of message or important data on any network because hackers and crackers always there in the wake of it. They always want to harm the person and in this case the sender or the receiver has to pay the price for it. Polybius checkerboard and steganography are the most effective methods to protect our network from attacker. So for this reason this research paper is proposed that we can make our work more secure by the techniques of Polybius checkerboard (Polybius square table) by applying Fibonacci sequence in it and steganography.

Keywords: Polybius Square, Steganography, Fibonacci sequence.

1. Introduction:

Steganography is well-known technique use for making the message or important data sending and receiving more securely but on the other hand Polybius square, also known as Polybius checkerboard play a very important role in security issues like encryption and decryption algorithm. In this paper, Polybius square and steganography both techniques are combined together for better security. Currently we have different techniques and methods for steganography [1] but combining steganography with Polybius checkerboard technique and develop one system the message or data will be much more secure and it will not be easy to break or hack the message which was sent or received by the sender or receiver.
First the message in text form will be encrypted using Polybius checkerboard technique [see section 2.2] by using the algorithm of Fibonacci sequence and then encrypted message will be hidden in any image file using steganography technique but will be of larger size than the original message so the image file

will be compressed using any compression technique like converting the image file into windows rar format (compressed) so the file will be approximately of same size of the original image. In this way, the image will not attract any attention that if anybody found the rar file, they will not attract towards the file that they may contain the secret text and is in the image file and if he found the text in image then it will be meaningless to them and the messagewill be more securely and more confidentially sent and received.

2. Steganography and Polybius Square:

2.1 Steganography:

In steganography, the message (can be in the form of text or sound) converted into image, sound or may be in the video file i.e. hiding data in data [2]. So that only the sender and the receiver knows about the existing of the hidden message. Like if the text is hidden in the image so the text replace with some pixels of image file (Figure 1) and the naked eye will not be able to see the difference between the original image and the text hidden image [3]. Only with the help of software like Stego, JPHIDE and JPSEEK, OutGuess, Steganos, FortKnox, one can find out the hidden data in it.

Figure 1: In these image the text is hidden in the second image but only be seen with software

2.2 Polybius Square:

Polybius square [4] is also known as Polybius checkerboard is use to encrypt the message (text) to make it unreadable by the third party. The encrypted text is called cipher-text. The original text can be obtained after getting the secret key called decipher becomes the plain-text [5].
Plain Text → Encrypted Algorithm → Cipher Text → Algorithm to break the Cipher Text → Decipher

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U

5	V	W	X	Y	Z

Table 1: the original Polybius Square

I and J combined together to make it fit in 5x5 grid. Each alphabet is represented by its coordinates in the square like PIANO becomes 35 24 11 33 34 [Table 2]

P	I	A	N	O
35	24	11	33	34

Table 2: word PIANO has cipher-text 3524113334

3. Fibonacci Numbers or Fibonacci sequence:

The starting values of Fibonacci series are 0 and 1; each number is the sum of previous two numbers [6] i.e. the "2" number can be obtained by adding the two numbers before it "1"+ "1", similarly 3 obtained by adding the two numbers before it 2+1 and 5 is 3+2 and so on.
0+1= 1
1+1= 2
2+1= 3
3+2= 5
5+3= 8
8+5= 13
13+8= 21
21+13= 34
34+21= 55
55+34= 89
89+55= 144 and so on….
The general formula of Fibonacci sequence is Fn= F n-1+F n-2.
Fn is term number "n"
Fn-1 is the previous term (n-1)
Fn-2 is the term before that (n-2)
The Fibonacci numbers are 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610, 987, 1597, 2584, 4181, …..

3.1 File Compression:

We have different software of compressing the file like ZIP, 7z, RAR etc. As WinRAR [7] is a powerful software compression tool that has responsibilities of data compression (reduce size of the file) and error recovery, developed by a Russian software engineer, Eugene Roshal. WinRAR is a compression algorithm to compress data and can compress files up to 8,589 billion GB in size (approximately 9×1018 bytes) which is 30 percent better than ZIP files.

4. Combining Technique of Polybius checkerboard and Steganography:

In this paper, Fibonacci sequence is used in Polybius square table to make the text complicated to break and to make it more complex (Table 3). 1 1 (Fibonacci numbers) are combined to remove repetition of identical numbers. The 6x6 grid is use for Polybius table. The last row and last column i.e. 6th row and 6th column is used for symbols and the remaining entities are filled with A, B, C, D, E, F, ….Up to Z. The Alphabet starts from backwards from Z to A in 5x5 order and the borders given by Fibonacci series and also in inverse format like sequence 0,1,1,2,3,5,8,13,21,34,55,89,144 becomes in row, starting with

144,89,55,34,21,13, and column becomes8,5,3,2,1/1,0 (1/1, as discussed in section 4)and table will be like this:

	144	89	55	34	21	13
8	Z	Y	X	W	V	:
5	U	T	S	R	Q	;
3	P	O	N	M	L	&
2	K	I/J	H	G	F	$
1/1	E	D	C	B	A	{
0	,	?	!	“	”	}

Table 3: Figure has Fibonacci sequence and alphabets in inverse order to make it complex

Let’s say the message to be encrypted is “hello, how are you?” From the table 3, the message can be encrypted to make it unreadable from the third person, who has no idea about the algorithm involve in it. Here is the Process Step by Step:

“	h	e	l	l	o	,	h	o	W	a	r	e	y	o	u	?	”
034	255	1144	321	321	389	0144	255	389	834	121	534	1144	889	389	5144	089	021

Table 4: using the complex table, encrypting of text

The message will be like this after encryption technique 034255114432132138901442553898341215341144889389514408902 1. This text is cipher-text. Place extra 00 before and after each alphabet or symbol to differentiate between words, so the cipher-text should be like this:
000340000255000011440000321000003210000389000001440000255000038900008340000121000053400000114400008890000389000051440000089000002100. The required cipher-text is obtained and has algorithm of Fibonacci sequence to decipher the text. Now add $ where space is required in sentence, becomes: “hello,$how$are$you?”
000340000255000011440000321000003210000389000001440$00255000038900008340$00121000053400000114400$00889000038900005144000008900000210 0
Finally the encrypted text is obtained and there is no need of any software to decrypt it. Using steganography technique (see section 2.1), the cipher-text is hidden into an image file. The text which is hidden in the image replaced some pixels of the image file and adjusts in it [7]. The resulted image may be of low quality but it can maintain good quality by using neural network and random selection of edged areas of pixels [8].Let’s say the original image has file size 1.13 MB and after being process of steganography, the size becomes 9 MB. Compression will be done using compression technique Windows rar format and then the image size will be 3.18 MB and also will be password protected so in this way the data will becompressed and fully secured.

5. Conclusions:

Polybius square is not much secure to send the intelligence secrets but through more complexity in the letters in the grid and by making the strong algorithm for it and also by developing a combined system for Polybius square and Steganography, we can give more security to the message to make it secure in the image file and no one knows that the image has hidden text in it and if he found the text which is already in encrypted form in the image file or it may be in the video file, it will be meaningless to the unauthorized person. The File compression Software’s like RAR etc are very costly and they are consuming too much time to compress data files. Although the evaluation and free version of these softwares are available but they are not reliable and fully featured as like registered versions. As future work, Polybius square and steganography, it gives the broad knowledge on almost all the principles where

a scholar have lot of scope for updating or invention of more secure algorithms to fulfill the global needs in Information Security.

6. References:

i. Deepak Singla (February 2012). Data Security and Integrity Using Data Hiding. Volume 2, Issue 2, Ijreas.
ii. Laurie Burton (January/February 2003). The Oregon Mathematics Teacher, Western Oregon University, Monmouth, Oregon.
iii. A. F. Horadam (1975). "Eight hundred years young." The Australian Mathematics Teacher.
iv. DomenicoBloisi and Luca locchi. Image Based Steganography and Cryptography, Dipartimento di InformaticaSistemistica, Sapienza University of Rome, Italy.
v. Bret Dunbar (January 2002). Steganographic Techniques and their use in an Open-Systems Environment, as part of the information security reading room, SANS institute.
vi. G. Julius Caesar and John F. Kennedy. Security Engineering: A Guide to Building Dependable Distributed Systems., Cryptography, Chapter 5.
vii. Imran Khan. An efficient Network Based Algorithm of Steganography for image. International Journal of Computer Technology and electronics engineering, Volume 1, Issue 2.
viii. Information hiding techniques A tutorial review by Sabu M. ThampiDept. of Computer Science and Engineering LBS college of Engineering, Kasaragod Kerala-671542, S.India.
ix. MiroslavDobsicek, Modern Steganography. Department of Computer Science and Engineering, Faculty of Electrical Engineering, Czech Technical University in Prague.
x. NielsProvas and Peter Honeyman, Hide and Seek: An Introduction to Steganography. University of Michigan, IEEE Security & Privacy.
xi. K. Solanki, O. Dabeer, B. S Manjunath, U. Madhow and S. Chandrasekaran. A Joint Source-Channel Coding Scheme for Image-Image Data Hiding, Dept. of Electrical and Computer Engineering, University of California at Santa Barbara.
xii. Hamid. A. Jalab, A. A. Zaidan, B. B. Zaidan (February 2010). New Design for INformatiuon Hiding with in Steganography Using Distortion Techniques, IACSIT International Journal of Engineering and Technology Vol. 2, No.1.
xiii. D. Sravana Kumar, CH. Suneetha, A. Chandrasekhar (March-April 2012). Novel Encryption Schemes Based on Catalan Numbers, Research and Applications (IJERA), Vol. 2, Issue 2.
xiv. DaraKirschenbaum (2000), Advances in Cryptography, History of Mathematics, Rutgers.
xv. LANAKI (January 1996), Classical Cryptography Course, Xenocrypt Morphology, Part II, President of the American Cryptogram Association from 1994-1996.
xvi. Tamas Denes, Cardan and Cryptography, The Mathematics of encryption grids, free lance expert.
xvii. Jose De Jesus Angel Angel and Guillermo Morales-Luna (2009), Cryptographic Methods during the Mexican Revolution, Cryptologia.
xviii. Eliot Feliciano. Early Development and Evolution of Cryptologic Fields and Functions, 460 Clandestine and Secure Communications.
xix. V. Kartalopoulos (2009). Security of Information and communication Networks, Institute of Electrical and Electronics Engineers.
xx. William Stallings. Cryptography and Network Security, 2nd Edition.
xxi. Richard A. Mollin. An Introduction to Cryptography, Discrete Mathematics and its Applications, 2nd Edition.
xxii. Bell, T.C., Witten, I.H. and Cleary, J.G. "Modeling for text compression," Computing Surveys 21(4): 557-591; December 1989.
xxiii. Timothy C. Bell, John G. Cleary, Ian H. Witten. Text Compression, Prentice Hall Advanced Reference Series, Computer Science.