ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 3, March 2015

Effective Cryptposystem using MRGA with Steganography

Kunal Jain[1], Jitender Singh[2], Rushikesh Kapadnis[3], Bharti Dhote[4]

Student, Computer Department, Sinhgad Institute of Technology, Lonavala, India [1,2,3]

Associate Professor, Computer Department, Sinhgad Institute of Technology, Lonavala, India [4]

Abstract: Management and efficiency of cryptography is not only based on the layer of cryptosystem but also on the generation of keys and exchange of this key's. One of the mostly used algorithm in today's cryptosystem is RSA for public key cryptography. But the problem with such cryptosystem is the part of key generation and key exchange. We know that ones the secure key is loss or regenerated this cryptosystem fails. To overcome this problem we want to suggest a different kind of cryptosystem, A Cryptosystem without any key. In this paper we suggest the combination of Magic Rectangle Generation Algorithm (MRGA) with Stenography is being proposed in this work. It is helpful to reduce the time and space to generate and store the different secure keys. This Magic rectangles are formed evenly on the basic of their seed number, row number, column number, start number, row sum and column sum. The generated encrypted text is very difficult to trace as value for row and column sum is very difficult to be traced. And with addition of Stenography it is very difficult to access by any middle man. The proposed work introduces another way of designing security without the use of key and overcoming the weakness of public key cryptosystems such as RSA, ElGAMAL etc. Encrypted file generated by this method will be completely different form the original plain text file and can be transfer securely over the internet.

Keywords: MRGA, Golden Rectangle, Steganography, LSB method, chipher text

I. Introduction

We have seen that over the past few years an increase in demand of data communication over the internet. Due to data communication over the internet it is very important that the data should be securely transmitted, means increase in security level. Therefore, secure transmission is done in the presence of the third party, through cryptography. There are two technique through which we can transfer our data securely symmetric and asymmetric key. Symmetric key cryptosystem is the technique in which sender and receiver require the same key that is used to encrypt and decrypt the data or message.The main drawback is sender and receiver must exchange a key in a secure way. To overcome this drawback public key cryptosystem is used. In this technique the public key is published to everybody, but the private key is kept secret and thereby this eliminate the exchange of key in a secure way [1].

But, if this private key is somehow cracked or know by the third party. Then the message is decrypted easily. So to overcome this drawback of key generating we are using Magic Rectangle Generation Algorithm (MRGA). In MRGA algorithm it is very difficult to decrypt the message. And we are adding one more level of security by hiding that encrypted message behind the image that is called steganography [2].

II. RELATED WORK

Gopinath Ganapathy and K Mani [2] enhanced the efficiency by providing additional level of security to the cryptosystem. This approach increased the security due to its complexity in encryption by using the magic square concept. Prasant Sharma, Amit Kumar Gupta et al [3] analysed the speed of RSA public key cryptosystem to reduce the time taken for finding factor for a large number. They proposed new algorithm and its performance was compared with Fermat's factorization Algorithm and trial division algorithm.Ravi Shankar Dhakar, Amit Kumar Gupta et al [4] improved the security of RSA cryptography algorithm based on additive homomorphic properties. The proposed algorithm is secured based on the factoring problem as well as decisional composite residuosity assumption.

Alaa Hussein Al Hamami et al [5] proposed enhancing the RSA algorithm through the use of additional third prime number in the composition of public and private key. This will increase the factoring complexity of the variable n, where the process of its analysis with the development of equipment and tools become much easier nowadays. Also itshow's the analysis of variable n will take a long time in the enhanced method for RSA cryptosystem algorithm and this indicates the increasing complexity in the analysis method.

Sami A Nagar and Saad Alshamma [6] proposed a new method to speed up the implementation of RSA algorithm during data transmission between different communication network and Internet. It introduced a new manner by which instead of exchanging the keys between gateways, the indexes refers to the fields, are getting exchanged. These fields are stored in the tables inside the database before starting to use RSA algorithm.

III.Proposed Methodology

The methodology of the proposed enhanced securitymodel is described in the following steps.

DOI 10.17148/IJARCCE.2015.4380

- Construct different singly even magic rectangle of order 16x24 as far as possible which are to be used like ASCII table.
- Each character of the plain text is converted into numerals using magic rectangle based on its position in plain text.
- The data which will be converted from plain text to chipper text and again to plain text that is called encrypted and decrypted is done using RSA algorithm.

Encrypted data is hide behind the images using steganography, algorithm used for steganography is S-DES.

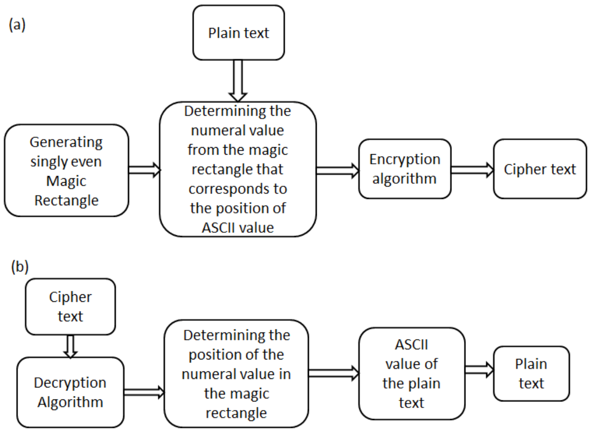

(a)
Plain text
Generating singly even Magic Rectangle
Determining the numeral value from the magic rectangle that corresponds to the position of ASCII value
Encryption algorithm
Cipher text
(b)
Cipher text
Decryption Algorithm
Determining the position of the numeral value in the magic rectangle
ASCII value of the plain text
Plain text

Fig 1. Security model (a)Encryption process, (b)Decryption process.

3.1MAGIC RECTANGLE GENERATION

Magic rectangle is generated through magic square. A magic square of order n are composed such that the sum of all entries along row, column and main diagonal are equal to magic constant of the square.

Example Of magic rectangle

4	9	2
3	5	7
8	1	6

The magic constant can be easily calculated by summing the value of 1…..N^2 and dividing by N, the number of rows and columns to find..

F (N) =N*(N^2+1)/1 (1)

For N=4 the magic constant is 34.

Magic rectangle is classified into three classes namely odd, doubly even (n is divisible by four) and singly even (n is even but it is not divisible by four). Magic rectangle of order (m*n) is an arrangement of the elements in such a way that the sum of all integers in row and column are equal.

The magic rectangle should be singly even.ie, the order of the matrix is even but not divisible by four such as 4x6, 8x12, 16x24 etc. Any order with even can be used in this work. It can be followed only the order 4x6, 8x12, 16x24 etc. The construction of magic rectangle is purely based on rules of magic rectangle or golden rectangle.

3.1.1GOLDEN RECTANGLE

A golden rectangle with longer side a and shorter side b, when placed adjacent to a square with sides of length a, will produce a similar golden rectangle with longer side a + b and shorter side a.

$\frac{a+b}{a}=\frac{a}{b}=\varphi$, then the relationship .A golden rectangle is one whose side lengths are in the golden ratio, 1: $\frac{1+\sqrt{5}}{2}$, which is 1: φ(the Greek letter phi), where φ is approximately.

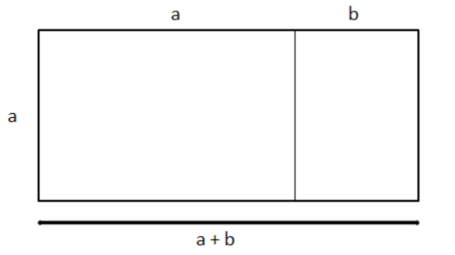


Fig 2. Perfect Rectangle

3.2STEGANOGRAPHY

Steganography is the method through which sender can transmit the secret or confidential message to the sender. In this method the confidential data or information is hide behind the other digital medium such as text, image, audio or video. The word steganography is of Greek origin and means "concealed writing" from the Greek words steganos meaning "covered or protected", and graphie meaning "writing". It is very high level of security technique for a long data communication.

There are various methods of steganography:

- Least significant bit (LSB) method
- Transform domain techniques
- Statistical methods

Distortion technique

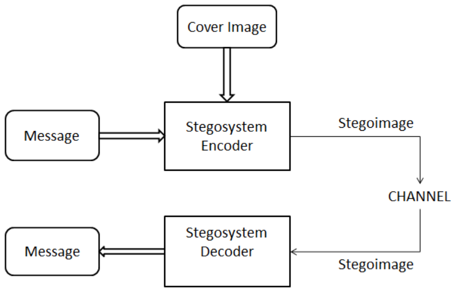


Fig 3. Steganographic Flow

3.3CREATION OF SINGLY EVEN MAGIC RECTANGLE

In this work, the singly even magic rectangle is generated by using any seed number, starting number and magic sum. The numbers are generated in consecutive order.

Notations used in this work are listed below:

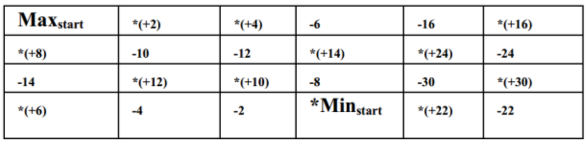
DOI 10.17148/IJARCCE.2015.4380

- MR :Magic Rectangle
- nxm :Order of MR

Where n=4x and m=6x
Where x=1, 2, 4, 8 etc.

- MRnxm :MR of order nxm
- MRB 4x6 :Base MR of order 4x6
- MRnxm rsum :Row sum of MR of order nxm
- MRnxm csum :Column sum of MR of order nxm

The values in the MRB4x6 are filled as shown in Fig 4. The function is called MR4x6 fill order (Minstar, Maxstart).



Max_{start}	*(+2)	*(+4)	-6	-16	*(+16)
*(+8)	-10	-12	*(+14)	*(+24)	-24
-14	*(+12)	*(+10)	-8	-30	*(+30)
*(+6)	-4	-2	***Min_{start}**	*(+22)	-22

Fig 4. Magic rectangle filling order

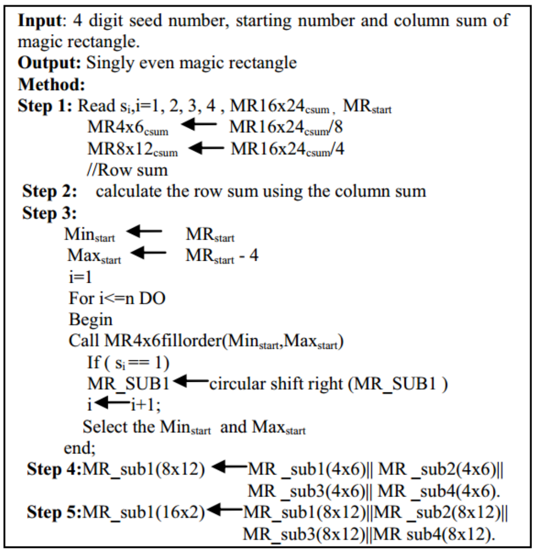
In table.1, '*' represents the places in magic rectangle to be filled, starting from Minstart and incremented by 2 each time to get the next number where as the empty places to be filled, starting from Maxstart and decremented by 2 to get the next number.

3.4MAGIC RECTANGLE GENERATION ALGORITHM

The MR algorithm started with the input values Minstart, Massmart, column sum and seed value. The seed value is the 4 bit binary value. If the input seed value is '1' bit, then either row or column of Magic Rectangle is shifted circularly. Otherwise shifting of row or column is not warranted.

Implementation of the below algorithm will create four magic rectangles. Finally these four MR are combined together to form the next level of MR by using the following method

MRixj=MR(i/2)x(j/2)||
MR(i/2)x(j/2)||MR(i/2)x(j/2)||MR(i/2)x(j/2)



```
Input: 4 digit seed number, starting number and column sum of
magic rectangle.
Output: Singly even magic rectangle
Method:
Step 1: Read $s_i$,i=1, 2, 3, 4 , $MR16x24_{csum}$ , $MR_{start}$
        $MR4x6_{csum}$ ← $MR16x24_{csum}$/8
        $MR8x12_{csum}$ ← $MR16x24_{csum}$/4
        //Row sum
Step 2:   calculate the row sum using the column sum
Step 3:
      $Min_{start}$ ←   $MR_{start}$
      $Max_{start}$ ←   $MR_{start}$ - 4
      i=1
      For i<=n DO
      Begin
      Call MR4x6fillorder($Min_{start}$,$Max_{start}$)
        If ( $s_i$ == 1)
        MR_SUB1←circular shift right (MR_SUB1 )
        i←i+1;
       Select the $Min_{start}$ and $Max_{start}$
      end;
Step 4:MR_sub1(8x12) ←MR _sub1(4x6)|| MR _sub2(4x6)||
                      MR _sub3(4x6)|| MR _sub4(4x6).
Step 5:MR_sub1(16x2)←MR_sub1(8x12)||MR _sub2(8x12)||
                     MR_sub3(8x12)||MR sub4(8x12).
```

Fig 5. MRGA Algorithm

RESULT AND DISCUSSION

The MRGA algorithm with steganography is implemented in Java. When the file size is increased, the encryption and decryption time will also be increased proportionately. instead of using ASCII, It takes additional time to generate magic rectangle. The security level of the cipher text is increased by the randomness of the value of magic square. The existing concept of magic square uses only one sum for matrix generation. Both column sum and row sum are used for matrix generation. In the aspect of security enhancement, one more input value called seed value is included. When the magic rectangle is constructed, the rectangle columns are circularly shifted right, Based on the seed value. An efficient steganographic method for embedding secret messages into cover images without producing any major changes has been accomplished -through Hash-LSB method. In this work, a new way of hiding information in an image with less variation in image bits have been created, which makes our technique secure and more efficient.

REFERENCES

[1]. A.J.Menezes ,P.C.Van Oorschot, and S.Vanstone , "Handbook of Applied cryptography", CRC Press, Boca Ration,Florida, USA,1997.

[2]. GopinathGanapathy, and K.Mani , " Add-On Security Model forpublic key Cryptosystem Based on Magic Square Implementation",ISBN 978-988-17012-6-8, Proceedings of the world congress on Engineering and Computer Science 2009 Vol I, San Fransisco, USA.

[3]. Sharma, P. Gupta, A.K. ; Vijay, A. "Modified Integer Factorization Algorithm Using V-Factor Method" Page(s): 423 - 425 ,978-0-7695-4640-7/12, IEEE 2012..

[4]. B.Schenier. "Applied Cryptography", John Wiley & Sons Inc, NewYork, Second Edition, 1996.

[5]. William Stallings, "Cryptography and Network Security", PrenticeHall, Upper Saddle River, New Jersy, USA, Second Edition, 1997.

[6]. S. M. Masud Karim, Md. Saifur Rahman, Md. Ismail Hossain "A New Approach for LSB Based Image Steganography using Secret Key", International Conference on Computer and Information Technology (ICCIT), Pages No. 286 – 291, 22-24 Dec., 2011.

[7]. N. F. Johnson, S. Jajodia, "Steganography: seeing the unseen", IEEE Computer, Vol. 31, Issue No. 2, Pages No. 26 - 34, Feb., 1998

[8]. Deepesh Rawat, Vijaya Bhandari, "A Steganography Technique for Hiding Image in an Image using LSB Method for 24 Bit Color Image", International Journal of Computer Applications, Vol. 64, Issue No. 20, Feb., 2013.

[9]. Yang, Chunfang., Liu, Fenlin., Luo, Xiangyang., and Zeng, Ying., "Pixel Group Trace Model-Based Quantitative Steganalysis for Multiple Least-Significant Bits Steganography", IEEE Transactions on Information Forensics and Security, Vol. 8, No. 1, January 2013.

[10]. Swati malik, Ajit "Securing Data by Using Cryptography with Steganography" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013

[11]. Ishwarjot Singh ,J.P Raina," Advance Scheme for Secret Data Hiding System using Hop field & LSB" International Journal of Computer Trends and Technology (IJCTT) – volume 4 Issue 7–July 2013

[12]. G. Manikandan, N. Sairam and M. Kamarasan "A Hybrid Approach for Security Enhancement by Compressed Crypto-Stegno Scheme ", Research Journal of Applied Sciences, Engineering and Technology 4(6): 608-614, 2012

[13]. Anil Kumar , Rohini Sharma, "A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique", International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE), Volume 3, Issue 7, July 2013

DOI 10.17148/IJARCCE.2015.4380