IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified

Vol. 6, Issue 3, March 2017

Enhanced Data Security with Magic Rectangle and Genetic Algorithm

Monali G. Pawar[1], Minal S. Chaudhari[2], Ankita K. Wani[3] and Dhiraj S. Mahajan[4]

Department of Computer Engineering, SSBT's College of Engineering and Technology, North Maharashtra University, Jalgaon, Maharashtra, India.[1,2,3,4]

Abstract: For many years, people were concerned with the secure transmission of data. The encryption is used to securely communicate data in open network. As each type of data has its own structure, different techniques should be used to protect confidential data. The existing algorithms used for encryption in cryptography have some flaws such as data easily retrieved using ASCII values for numerical representation. The proposed system combines cryptographic algorithm with steganography to protect data or message over network thereby enhancing the data security.

Keywords: Security, Cryptography, Steganography, Magic Rectangle, Genetic Algorithm.

I. INTRODUCTION

The internet is used for more rapid transmission of huge volume of important and valuable data which makes it susceptible to many kinds of attacks. So the information needs to be protected from unauthorized access and the other security issues. The techniques like Cryptography and the Steganography are classical approaches of data security. In Cryptography, the data is encrypted into an unreadable format during encryption process and during decryption data is again recovered in its original format. In Steganography, the data is embedded into a specific format of multimedia files to protect the sensitive information and during the recovery of data, the data is retrieved in its original format without any modification on its cover. Steganography and cryptography are the techniques used to hide information from unwanted parties but neither technique is alone sufficient. Once the method is known for hiding information then data can be recovered easily that's why steganography is somewhat defeated. The effectiveness of Steganography increases by combining it with cryptography.

In the proposed system, the cryptography and steganography are used to enhance the data security. In cryptography, the parameters used in encryption and decryption process of the algorithm play a key role for security. In RSA, the secret key is derived from the public key and chosen p, q values with very large size. But it is not fully secured because use of ASCII character. The characters can be easily retrieved using ASCII values of the characters. To overcome the described problem, the proposed system uses magic rectangle of the order 8 x 12. The table represents different numerical values, representing the position of ASCII values are taken from magic rectangle. In the proposed system steganography uses Genetic Algorithm which uses pixels selection of image where data is to be hidden so that it is protected from malicious attacks.

II. LITERATURE SURVEY

The content of the paper focuses on the research and contributions of various sources. The sources include:

[1] The paper describes the process for generation of the magic rectangle. Magic rectangle is powerfully used for data encryption and decryption. It is difficult to construct the table but it provides more secured data.

[2] The paper describes the operation of Genetic Algorithm. It also gives an overview about functioning of Genetic Algorithm with AES algorithm and its internal operators. Among three operators, it gives a deep idea of crossover and row /column shuffling of bits.

III. PROPOSED SYSTEM

The proposed system enhances data security by increasing the complexity of encryption and decryption process of data in cryptography and steganography.

Today, to transmit confidential information over the network, security is essential. Cryptographic algorithms play an important role to provide the data security against malicious attacks. Many people think that the efficiency of cryptographic algorithm depends only on its time taken for encryption and decryption.

However, the efficiency of cryptographic algorithm also depends on number of stages used to obtain cipher text to maintain data secrecy. The algorithms such as Magic Rectangle and Genetic algorithm are designed separately to maintain data secrecy. If one continues to use these algorithms individually, data may be lost as security provided by these algorithms can be easily compromised. To overcome the problem, proposed system combines Magic Rectangle and Genetic algorithm to enhance the security by increasing complexity of the encryption process.

DOI10.17148/IJARCCE.2017.63204

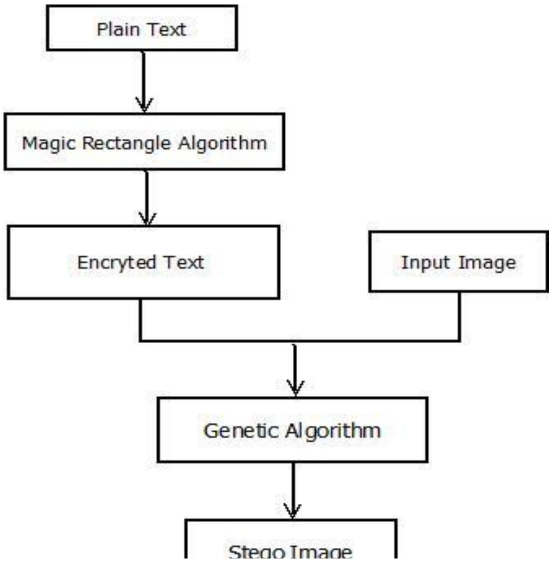


Figure 1. Architecture of Proposed System

As sender gives input, the magic rectangle is constructed based on some constraints such as seed value, min start, max start, column sum. To enhance data security, Genetic Algorithm hides encrypted data generated using magic rectangle into an image generating a complex cipher text.

3.1 MAGIC RECTANGLE

It constructs magic rectangle of order 8x12 and used in context of ASCII table with 128 values. The Magic rectangle contains totally 96 values. It has been divided into 4 quadrants, each consists of 128 characters. Each character of the plain text is converted into numeric value based on its position in magic rectangle in different quadrants. The encrypted text is obtained by converting original text into numeric values.

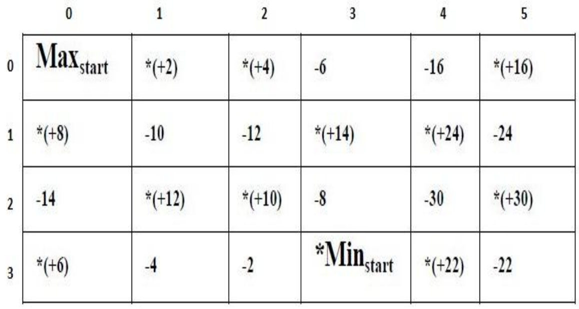
In the proposed work, the magic rectangle is generated by using any seed number, startingnumber and magic column sum. The numbers are generated in a consecutive order[1].

The Notations used in the present work are as follows[1]:

- MR :Magic Rectangle
- n*m :Order of MR
where n=4x and m=6x
where x=1, 2, 4, 8 etc.
- MRn*m :MR of order n*m
- MRB4*6 :Base MR of order 4*6
- MRn*mrsum :Row sum of MR of order n*m
- MRn*mcsum :Column sum of MR of order n*m

Magic rectangles are well-known for its very interesting and entertaining combinatorics.A magic rectangle is an arrangement of theintegers 1 to mn in an array of m rows andncolumns so that each row adds to the same total M and each column to the same total N.The totals M and N are termed the magic constants. Since the average value of the integersis A = (mn + 1)/2, we must have M = nA and N = mA . The total of all the integers inthe array is mnA = mM = nN. If mn is even mn+1 is odd and so for M = n(mn+1)/2 andN = m(mn + 1)/2 to be integers n and m must both be even. On the other hand if mn isodd then m and n must both be odd, by simple arithmetic. Therefore, an odd by even magicrectangle is impossible. Also, it is easy to see that a magic rectangle is impossible.The values in the MR4x6 are filled as shown in Figure 2. The function is called MR4*6 fill order (Minstart, Maxstart) [1].

In Figure 2, * represents the places in magic rectangle to be filled, starting from Minstartand incremented by 2 each time to get the next number where as the empty places to befilled, starting from Maxstart and decremented by 2 to get the next number [3].



	0	1	2	3	4	5
0	$\mathrm{Max}_{\mathrm{start}}$	*(+2)	*(+4)	-6	-16	*(+16)
1	*(+8)	-10	-12	*(+14)	*(+24)	-24
2	-14	*(+12)	*(+10)	-8	-30	*(+30)
3	*(+6)	-4	-2	$^{*}\mathrm{Min}_{\mathrm{start}}$	*(+22)	-22

Figure 2.Magic Rectangle Filling Order [1]

3.2.1 ALGORITHM FOR GENERATION OF MAGIC RECTANGLE [1]:

```
Require: 4 digit seed number, starting number and column sum of magic rectangle.
1: Read si, i=1, 2, 3, 4 ,
MR16x24csum , MRstart
MR4*6csum MR16*24csum/8
MR8*12csum MR16*24csum/4
2: calculate the row sum using the column sum
3: Minstart= MRstart
Maxstart= MRstart - 4
i=1
4: For i<=n DO
Call MR4x6 fillorder(Minstart,Maxstart)
5: if si == 1 then
6: MR SUB1 circular shift right(MR SUB1)
7: i=i+1
8: Select the Minstart and Maxstart
9: end if
10:MR sub1(8x12)jj= MR sub1(4x6)jj || MR sub2(4x6)jj || MR sub3(4x6)jj || MR sub4(4x6)
11:MR sub1(16x2)jj=MR sub1(8x12)jj || MR sub2(8x12)jj || MR sub3(8x12)jj || MRsub4(8x12)
```

3.1.2 ILLUSTRATION OF MAGIC RECTANGLE [1]

S1=0, S2=0, S3=1, S4=0

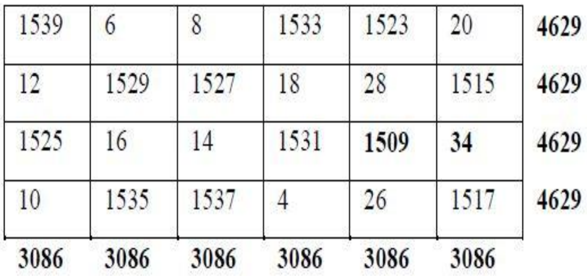
MR16x24, csum=12345

MR4x6,csum=12345/4=3086.25=3086

MR4x6, rsum= (3086/2) +3086=4629

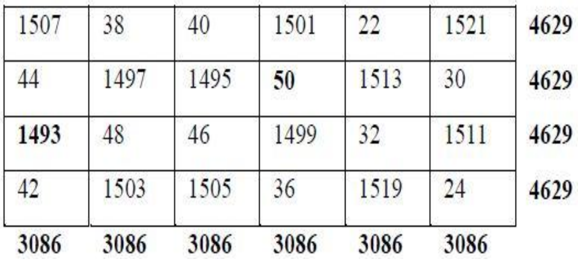
Magic rectangle 1 (MR sub1):

Minstart=4, Maxstart=1539,S1=0



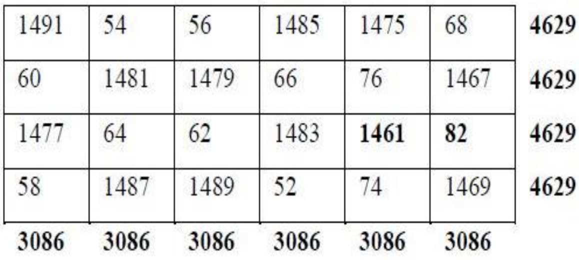
1539	6	8	1533	1523	20	**4629**
12	1529	1527	18	28	1515	**4629**
1525	16	14	1531	**1509**	**34**	**4629**
10	1535	1537	4	26	1517	**4629**
3086	**3086**	**3086**	**3086**	**3086**	**3086**	

Magic rectangle 2 (MR sub2):
Minstart= 36, Maxstart= 1507, S2=0



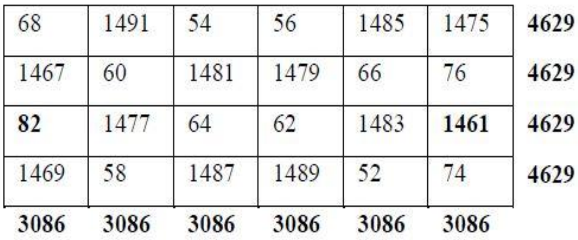
1507	38	40	1501	22	1521	**4629**
44	1497	1495	**50**	1513	30	**4629**
1493	48	46	1499	32	1511	**4629**
42	1503	1505	36	1519	24	**4629**
3086	**3086**	**3086**	**3086**	**3086**	**3086**	

Magic rectangle 3 (MR sub3):
Minstart=52, Maxstart=1491,S3=1



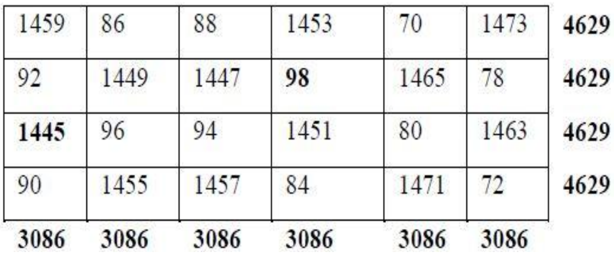
1491	54	56	1485	1475	68	**4629**
60	1481	1479	66	76	1467	**4629**
1477	64	62	1483	**1461**	**82**	**4629**
58	1487	1489	52	74	1469	**4629**
3086	**3086**	**3086**	**3086**	**3086**	**3086**	

The rectangle is shifted circularly one position to the right because of the seed value s3=1.



68	1491	54	56	1485	1475	**4629**
1467	60	1481	1479	66	76	**4629**
82	1477	64	62	1483	**1461**	**4629**
1469	58	1487	1489	52	74	**4629**
3086	**3086**	**3086**	**3086**	**3086**	**3086**	

Magic rectangle 4 (MR sub4):
Minstart=84, Maxstart=1459 ,S4=0



1459	86	88	1453	70	1473	**4629**
92	1449	1447	**98**	1465	78	**4629**
1445	96	94	1451	80	1463	**4629**
90	1455	1457	84	1471	72	**4629**
3086	**3086**	**3086**	**3086**	**3086**	**3086**	

Four 4x6 magic rectangles are generated as above. Combination of these four rectanglesforms the next level of MR of order 8x12 [1].

MRsub1(8X12) = MR sub1(4X6)$_{jj}$|| MR sub2(4X6)$_{jj}$ ||MR sub3(4X6)$_{jj}$ ||MR sub4(4X6):

The sample Magic rectangle of order 8x12 is represented in Figure 3.Similarly, MR sub1(8x12),MR sub2(8x12), MR sub3 (8x12) and MR sub4(8x12) are generated and concatenated toform MR(16x24). The process continues till magic rectangle of order 32x48 is obtained. InMR(32x48), there are totally 1536 values. Since the maximum size of character for ASCIIcode representation is 128, the obtained value (1536) will be divided into 12 quadrant of size 128. The plain text characters are replaced by the value in different quadrant consecutively [1].

3.2 GENETIC ALGORITHM

Genetic Algorithm is an optimization technique based on the random population of chromosomes. The algorithm is a computerized search and optimization algorithm based on Darwins principle of Natural selection which is a part of Evolutionary algorithms. The basic concept is to simulate processes in natural system necessary for evolution[2]. It involves three operators:

i) Selection or Reproduction
ii) Crossover
iii) Mutation

3.2.1 CROSSOVER

A crossover operator recombines two parent strings to create better offspring strings[2]. The three steps for proceeding crossover involves:
1.A random pair of strings called as chromosomes are selected by reproduction operator.
2.Crossover selects a cross-site based on the length of the string.
3.The position of two strings are swapped following the cross-site.

Many crossover operators are recently available. Most commonly used operators are:

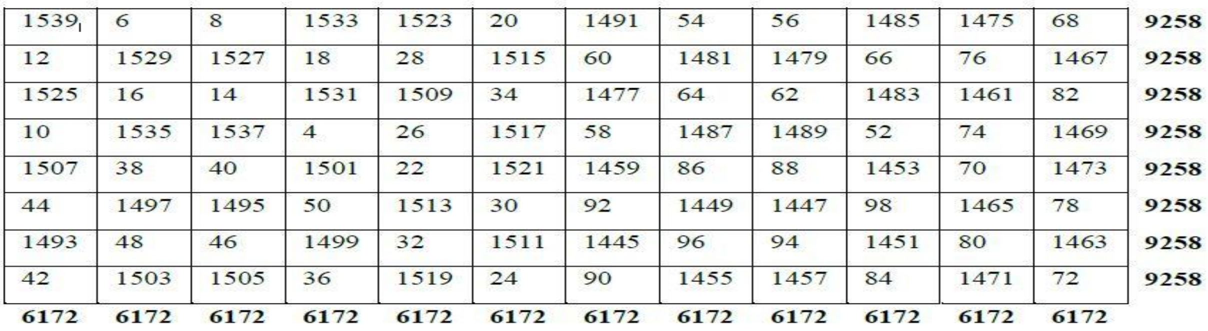
1.Single-point crossover
2.Two-point Crossover
3.Uniform Crossover

3.2.1.1 SINGLE-POINT CROSSOVER

Single-point crossover simply generates a cut-point and recombines the first part of first parent with the second part of second parent to produce one offspring and vice versa for second offspring. The cut points are selected along the length of two parent strings and bits next to the cut-points are exchanged[2].

A bit position along the two chromosomes is called as locus. Single point crossover swaps bit position before and after that locus to create single offspring i.e. one crossover point is selected. A binary string from starting point of the first parent is copied and rest part is copied from the second parent to generate child as shown in Figure 4 [2].

DOI10.17148/IJARCCE.2017.63204



1539	6	8	1533	1523	20	1491	54	56	1485	1475	68	**9258**
12	1529	1527	18	28	1515	60	1481	1479	66	76	1467	**9258**
1525	16	14	1531	1509	34	1477	64	62	1483	1461	82	**9258**
10	1535	1537	4	26	1517	58	1487	1489	52	74	1469	**9258**
1507	38	40	1501	22	1521	1459	86	88	1453	70	1473	**9258**
44	1497	1495	50	1513	30	92	1449	1447	98	1465	78	**9258**
1493	48	46	1499	32	1511	1445	96	94	1451	80	1463	**9258**
42	1503	1505	36	1519	24	90	1455	1457	84	1471	72	**9258**
6172	**6172**	**6172**	**6172**	**6172**	**6172**	**6172**	**6172**	**6172**	**6172**	**6172**	**6172**	

Figure 3. Magic rectangle of order 8X12 [1]

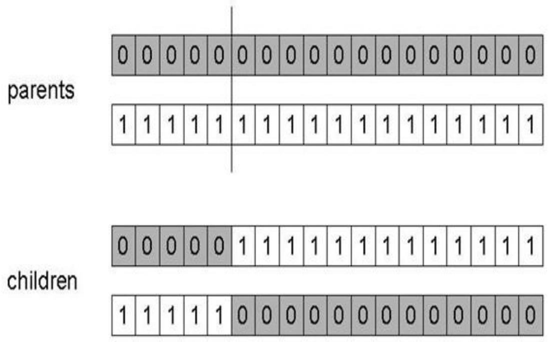


Figure 4. Single point crossover

IV. IMPLEMENTATION

Implementation involves the environment in which system is implemented and overall system development. Overall system development requires suitable environment and proper resources for successful completion. The proposed system is developed for enhancing the data security by adding multiple layers for encryption and decryption. The system combines cryptography and steganography together.

In order to obtain unbreakable cipher text, two algorithms are merged in the system. The input is taken either in the form of text, alphanumeric characters or special symbols. The ASCII value of a character or digit is replaced by its corresponding MR value. An image is taken for hiding the encrypted data. The Genetic algorithm is responsible for shuffling of pixels along with MR values. The proposed system is currently used for a single terminal. The encryption and decryption of data is done easily.
The flow of system development consists of sequence of implementation by which the system or software is implemented. Basic functionality, execution and steps of system execution are:

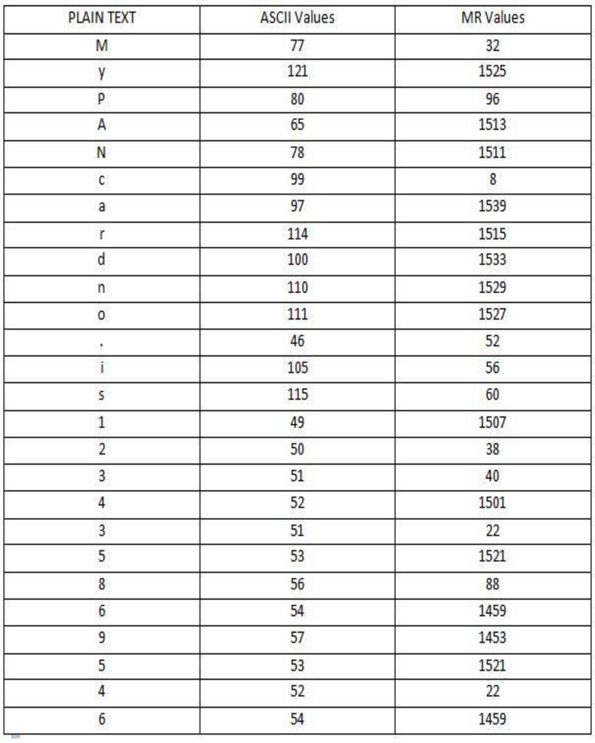
1. Enter text as an input.
2. GenerateMagic rectangle.
3. Encrypt the data using Magic Rectangle.
4. Browse for an image.
5. Embed encrypted data into the image using crossover Genetic Algorithm.
6. Finally, stego image formed.

V. RESULTS

All the results regarding enhanced data security with cryptography and steganography project is explained in Result**.**

The given message is “My PAN card No. is 123435869546”. At First, each and every character of the message is converted into the numerical value i.e. ASCII value. The ASCII value for each character is shown in table 1. To encrypt M, the value at the 77thpositionin the magic rectangle is applied. To encrypt y, the value at the 121th position in the magic rectangle is applied. Likewise, the value of each character is taken from the magic rectangle. As a result, the value of the cipher text is different for each character occurred in the input message. It is illustrated in table 1.

Table 1. ASCII Values and MR Values for Sample Text



PLAIN TEXT	ASCII Values	MR Values
M	77	32
y	121	1525
P	80	96
A	65	1513
N	78	1511
c	99	8
a	97	1539
r	114	1515
d	100	1533
n	110	1529
o	111	1527
.	46	52
i	105	56
s	115	60
1	49	1507
2	50	38
3	51	40
4	52	1501
3	51	22
5	53	1521
8	56	88
6	54	1459
9	57	1453
5	53	1521
4	52	22
6	54	1459

As an input is supplied to the proposed system the cipher text is created by using magic rectangle values then one image is selected to embed data into that image. The imagecanbe.JPEG, .PNG, .JPG, .GIF, .TIF, etc as shown in Figure 6. The cipher text is embedded into image by using the crossover genetic algorithm by using pixel selection. The cipher text contains the magic rectangle values of each character. The value of each character is split into 2 parts.

The magic rectangle value for ’M’ character is 32, it is split into 2 parts like 3 and 2. The given process continues for each character to generate cipher text and then the two columns of the pixels from the image are interchanged by their position to enhance the data security. An image (as shown in Figure 6) which is generated after applying the Crossover Genetic algorithm on the cipher text of the given input message is shown in Figure 7.

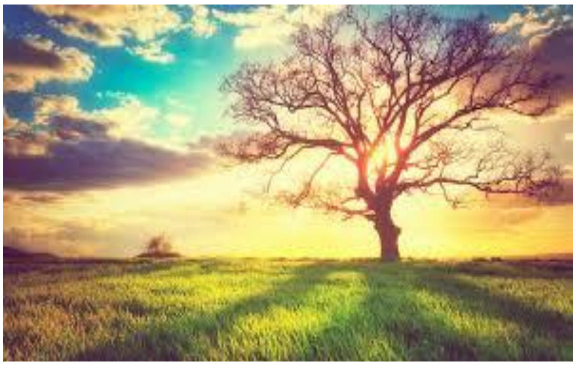


Figure 6.Image Used for Data Hiding

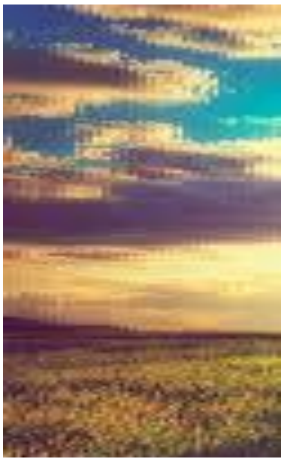


Figure 7.Stego Image

VI. CONCLUSION AND FUTURE SCOPE

In the proposed system, the efficiency of cryptographic algorithm is improved by adding number of stages. The stages increase the complexity of existing algorithms. The algorithm, alone does not provide as much efficient result as provided by the combination of algorithms in the proposed system. The proposed system is used to prevent the sensitive data with the use of Magic Rectangle and the part of Genetic algorithm. Magic Rectangle adds difficult MR values whereas Genetic makes the system unbreakable by shuffling of values with pixels. In future, the proposed system may be used for image encryption using magic rectangle.

REFERENCES

[1] Dr. D.I. George Amalarethinam and J. Sai Geetha, K.Mani, "Add-on Security Levelfor Public Key Cryptosystem using Magic Rectangle with Column/Row Shifting", International Journal of Computer Applications (0975 8887)Volume 96 No.14,June 2014.

[2] Pratiksha Sethi, V. Kapoor, "A Secured System for Information Hiding in ImageSteganography using Genetic Algorithm and Cryptography", International Journal ofComputer Applications-June 2016.

[3] WEN-YANG LIN, WEN-YUAN LEE+ AND TZUNG-PEI HONG, ”Adapting Crossover and Mutation Rates in Genetic Algorithms”, JOURNAL OF INFORMATION SCIENCE AND ENGINEERING 19, 889-903 (2003).

[4] Maria Angelova, Olympia Roeva, Tania Pencheva, ”Inter Criteria Analysis of Crossover and Mutation Rates Relations in Simple Genetic Algorithm”, Proceedings of the Federated conference on Computer Science and Information Systems pp. 419–424. ACSIS, Vol. 5

[5] Shen Wang, Bian Yang and Xiamu Niu, ”A Secure Steganography Method based on Genetic Algorithm”, Journal of Information Hiding and Multimedia Signal Processing Ubiquitous International Volume 1, Number 1, January 2010.

[6] Dr. D.I. George Amalarethinam, J.Sai Geetha,”Enhancing Security level for Public Key Cryptosystem using MRGA”, 2014 World Congress on Computing and Communication Technologies.

DOI10.17148/IJARCCE.2017.63204