Image Encryption and Decryption in Public Key Cryptography based on MR

D.I.George Amalarethinam
Associate Professor & Director- MCA,
Jamal Mohamed College
Trichy, India
di_george@ymail.com

J.Sai Geetha
Assistant Professor, Dept of Computer Science
Nehru Memorial College, Puthanampatti
Trichy, India
jsaigeetha99@gmail.com

Abstract— In the past decade, image encryption is given much attention in research of information security and a lot of image encryption algorithms have been introduced. Due to some intrinsic features of images like bulk data capacity and high data redundancy, the encryption of image is different from that of text; therefore it is difficult to handle them by traditional encryption methods. In the proposed work, a new image encryption algorithm based on Magic Rectangle (MR) is being applied. To begin with, the plain-image is converted into blocks of single bytes and then the block is replaced as the value of MR. Further, the control parameters of Magic Rectangle (MR) are selected randomly by the user. Subsequently the image is being encrypted with public key cryptography algorithms such as RSA, ElGamal etc. The experimental result shows that the proposed algorithm can successfully encrypt/decrypt the images with separate secret keys, and the algorithm has good encryption effect. Cipher text developed by this method will be entirely different when compared to the original image file and will be suitable for the secured transmission over the internet. Thus, this model provides an additional level of security to public key algorithm and efficient utilization of memory.

Keywords— Communication Security, Image Encryption and Decryption, Public Key Cryptography, Public key, Secret key, Magic Rectangle.

I. INTRODUCTION

Computer has become an essential device now a days. The main use of computer is to store data and send it from one location to other. The information that is shared must be transferred in a secured manner. To ensure secured transmission of information, data is encrypted to unreadable formats by an unauthorized person. Cryptography is the science of information security which has become a very critical aspect of modern computing systems towards secured data transmission and storage. The exchange of digital data in cryptography results in different algorithms that can be classified into two cryptographic mechanisms: symmetric key in which same key is used for encryption and decryption and asymmetric key in which different keys are used for encryption and decryption [1]. Asymmetric key algorithms are more secured when compared with symmetric key algorithms.

Nowadays, information security is primarily based on data storage and transmission. Images are broadly used in numerous processes. As a result, the safety of image data from unauthorized access is crucial at the hands of user. Image encryption plays a significant role in the field of information hiding. Image hiding or encryption methods and algorithms ranges from simple spatial domain methods to more complicated and reliable frequency domain.

The parameters used in encryption and decryption process of the algorithm plays a vital role for security such as key streams in one time pad, the secret key in Data Encryption Standard algorithm, the prime p and q in RSA etc. Of all the encryption algorithms available, RSA(Rivest, Shamir, Adlemen) accounts for highly reliable one. In RSA, the secret key is derived from the public key and choosing p and q with very large size. Even though the above parameters are considered, it is not fully secured. The conventional method of image encryption is done through any one of the technique such as RGB color shuffling, bits manipulation, chaotic mapping method etc. Of all the methods stated above, the result of encryption is in the form of cipher image. It takes more time for encryption and decryption process and the inefficient use of memory in this kind of cryptosystem results in reduction of transmission speed. To overcome this problem, this paper tries to develop a entirely different method by introducing a special singly even magic rectangle [2] of the order 32 x 48. Thus preferably different numerals representing the bytes of image values are taken from magic rectangle instead of taking patterns or bits for encryption. The encryption process is being performed using RSA cryptosystem.

II. RELATED WORK

Quist-Aphetsi Kester[3], proposed the work sets out to contribute to the general body of knowledge in the area of cryptography application and by developing a cipher algorithm for image encryption of m*n size by shuffling the RGB pixel values. Finally, the algorithm made it possible for encryption and decryption of the images based on the RGB pixel.

Musheer Ahmad and M. Shamsher Alam [4] proposed a new image encryption algorithm based on three different chaotic maps. In this work, the plain-image is first decomposed into 8x8 size blocks and then the block based shuffling of image is

978-1-4799-7623-2/15/$31.00 ©2015 IEEE

carried out through 2D Cat map. In addition, the control parameters meant for shuffling are randomly generated by employing 2D coupled Logistic map. Subsequently the shuffled image is encrypted through chaotic sequence generated by one dimensional Logistic map.

Varsha Bhatt and Gajendra Singh Chandel[5] proposed a new algorithm that deals with the representative image encryption techniques, position permutation, naive, substitution transposition and value transformation. Selective techniques will be described, assessed and matched up with respect to security level and encryption speed.

Hiral Rathod, Mahendra Singh Sisodia et.al[6], introduced a new permutation technique based on the combination of image permutation and developed an encryption algorithm called "Hyper Image Encryption Algorithm (HIEA)". The selected image will be converted into binary value blocks, which will be rearrange into a permuted image using a permutation process, and then the generated image will be encrypted using the HIEA algorithm.

Manoj. B, Manjula et.al[7] **,** proposed a method in which the image data is an input to AES Encryption to obtain the encrypted image. The encrypted image is used as input to AES Decryption to get the original image. In this paper, 128 bit AES is used for image encryption and decryption which is synthesized and simulated on FPGA family of Spartan-6 (XC6SLX25) using Xilinx ISE 12.4 tool in Very high speed integrated circuit Hardware Description Language (VHDL).

Mohammad Ali Bani Younes and Aman Jantan[8] introduced a block-based transformation algorithm using the combination of image transformation and a well known encryption and decryption algorithm namely Blowfish. The initial image was separated into blocks. The divided blocks were rearranged into a transformed image using a transformation algorithm. Then the transformed image was encrypted by applying the Blowfish algorithm. The results concluded that the correlation between image elements was significantly decreased.

A.Naresh Reddy, Rakesh Nayak and S. Baboo [9] presented the comparative study of RSA and NTRU ("non trivial ring units" or "n^{th} degree truncated polynomial ring units" or "Number Theory Research Units") algorithms for images as input and the results were assessed and compared so as to identify the appropriate method for the business needs.

III. PROPOSED METHODOLOGY

The images used will have their bytes extracted; the bytes values are transposed as MR values and further encrypted to obtain cipher text. The ciphering of the images for this work will be done only by using the byte values of the images. In this method, the RGB values of the image are not changed. Also there is no need to RGB expansion at the end of the encryption and decryption process. The numerical values of the MR are displaced from their respective positions and encrypted in order to obtain the cipher text. Therefore there is no change in the total size of the image during encryption and decryption process. The characteristic of image remains unchanged during the encryption process. The processing model of image encryption and decryption process is represented in fig.1.

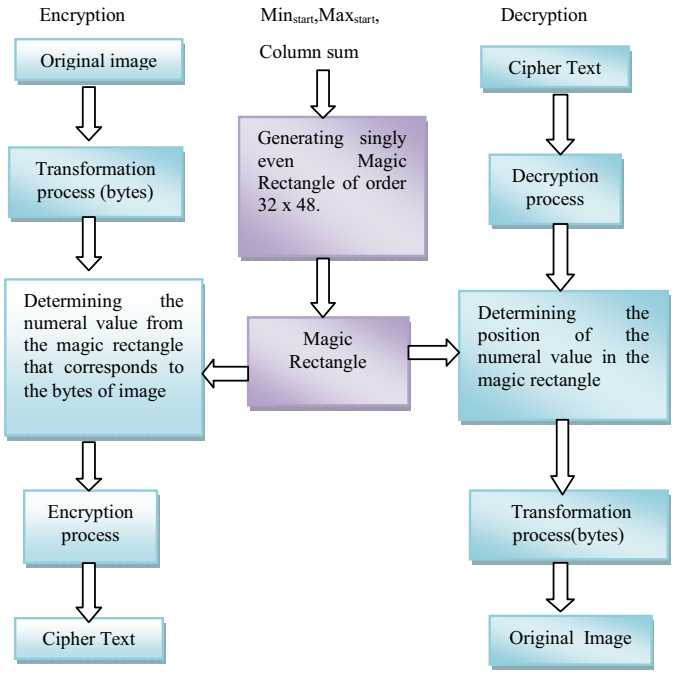

Fig.1. Model for Image Encryption and Decryption process

3.1.Construction of Magic Rectangle

3.1.1. Magic Square

The magic rectangle is similar to magic square. A magic square is defined as an arrangement of integers of order nxn matrix. The important feature of a magic square is that the sums of all the elements in every column, row and along the two main diagonals are equal. The magic constant of a magic square depends only on n and has the value

$$M(n) = n(n^2+1)/2$$

Magic square can be classified into three types: odd, doubly even (n divisible by four), singly even (n is even and not divisible by four). [2][10].

3.1.2. Magic Rectangle

A magic rectangle of order mxn is an arrangement of integers such that the sums of all the elements in every row are equal and also the sums of all the elements in every column are equal. The magic rectangle is in the category of singly even.ie, the order of the matrix is even but not divisible by the numeral 04 such as 4x6, 8x12, 16x24, 32x48 and so on. Any order with even number can be used in this work. It can be followed only the order 4x6, 8x12, 16x24, 32x48 etc. The size of the rectangle is purely based on the rules of perfect rectangle or

golden rectangle and also the singly even magic rectangle. It follows the methodology of divide and conquer strategy [11].
In magic rectangle, column sum is fixed as 32x48. The existing column sum is divided by two and then apply in 16x24. Further the column sum is divided by two and apply in 8x12 matrix etc.This approach is adopted from divide and conquer strategy.
The column sum is taken as even value then it matches exactly in magic rectangle. In case if the column sum is taken as odd value, then the column sum is reduced by one because of fractional value. This paper focuses only a singly even magic rectangle implementation and their usefulness for public key cryptosystem for image encryption and decryption process i.e. the order of magic rectangle must be even.

3.2.Creation 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 [12].

The proposed work uses the notations as listed below:

- MR :Magic Rectangle
- nxm :Order of MR
  where n=4a and m=6a
  where a=1, 2, 4, 8 etc
- MR_{nxm} :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 MRB_{4x6} are filled as shown in Table 1. The function is called MR4x6 fill order (Min_{start}, Max_{start}).

Table 1. Magic Rectangle Filling Order

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

In Table.1, '*' represents the places in magic rectangle to be filled having its starting point from Min_{start} and incremented by 2 each time to get the next number. The places without '*' in magic rectangle to be filled having its starting point from Max_{start} and decremented by 2 to get the next number.

3.3. Image Encryption and Decryption Algorithm

In image encryption process, the given image is converted into the sequence of bytes. When the bytes are converted to the numeric integer value, it may contain positive or negative value as stored in Byte array (Barray). Before encryption, the value in Byte array has been converted as positive values. These values forms the position of MR. Finally, the encryption process is being performed using any algorithm available in the public key cryptography. Then the resulting cipher text is modified to retain the original sign based on the bytes generated at the initial stage. The entire process can be reversed in the decryption process as illustrated in fig.2.

```
//Encryption
 Input:Image file (gif/bmp/jpg)
Output:Cipher text(Numeric Value)
Method:
Step1: Read Image File
Step2:Covert Image file into
        Sequence of bytes Array
Step3: For i= 0 to Barray.length
         //Bytearray
         Begin
              Flag=0;
              If Barray[i] <0 then
                 Begin
                    pos=-Barray[i];
                    Flag=1;
               end
              else
                 pos=Barray[i];
          Rarray[i]=MRarray[pos];
 /*MagicRectagle array and  Result
array*/
 Step 4:  Encrypt using Algorithm
          If Flag=1 then
            Cipher[i]=-Cipher[i];
            //Cipher array
          End
 Step 5: Produce Cipher Text
```

```
//Decryption
Input:Cipher Text (Numeric Value)
Output: Image file (gif/bmp/jpg )
Method:
 Step1: Read Cipher text
 Step2: For i= 0 to Cipher.length
//cipher array
            Begin
              Flag=0;
              If Cipher[i] <0 then
              Begin
                 Cipher[i]=-Cipher[i];
                  Flag=1;
              End
 Step 3:  Decrypt using Algorithm
           Pos =Marray[i];
           //MagicRectaglearray
            If   Flag=1 then
                 Barray[i]=-Pos
 Step 4: Convert Byte Array into
           Image
 Step 5: Produce original Image
```

Fig.2. Pseudo code for Image Encryption and Decryption process

3.4 Characteristics of an Image Cryptosystem

For studying characteristics of image encryption, the first step is to analyze the implementation differences between image and text data.

1. During the encryption process of text data, the decrypted text must be equal to the original text in a full lossless manner. However, this requirement is not necessary for image encryption; the cipher image can be decrypted to an original image in some lossy manner.
2. Text data is a sequence of words which can be encrypted directly by using block or stream ciphers. However, digital image data are represented as 2D array.
3. Since the storage space of a picture is very large, the process of encryption / decryption of the picture is very difficult. One of the best method is image compression which reduces both its storage space and transmission time.

In general, there are three basic characteristics in the information field: privacy, integrity and availability. For privacy, an unauthorized user cannot disclose a message. For integrity, an unauthorized user cannot modify or damage a message. As far as availability is concerned, message is made available only to the authorized users. An image cryptosystem cannot be called as a perfect cryptosystem even if it has a highly security mechanism, but it must also have elaborate overall performance. The image security requires following characteristics:

1. The encryption system should be computationally secured. It requires an extremely long time to attack and any

unauthorized user should not be able to read privileged image.
2. The security mechanism must be as widespread as possible.
3. The security mechanism should be flexible.
4. There should not be a large expansion of encrypted image data.

IV.EXPERIMENTS AND RESULTS

The proposed methodology is implemented in Java. The time taken for encryption and decryption of various size of image files are measured. For instance, the given image rose.jpg is converted into numerical value by using magic rectangle. To describe it in a detailed manner, the image file is changed into byte array. The byte array consists of negative values before replaced by the value of Magic Rectangle. Those negative values are replaced as positive values and an identification tag has been provided to it. The converted values indicate the position of MR. The encryption process carried out with MR and again original image is reconstructed by the decryption process. This concept is illustrated in the fig.3.

4.1 Experimental results of RSA algorithm using Magic Rectangle.

For the present experiment, the configuration of the system used is Pentium Core I3 CPU -3217U @2.80Ghz and 32-bit Operating System. The algorithm was applied on a Joint picture Expert Group (JPEG) image that has various size of pixels with 256 colors. Table. 2 represents the cipher text generated by RSA without using MR as shown below.

Table 2. Encryption and Decryption of Image file without using MR value

Encryption		Decryption	
ImageFile (bytes)	**Cipher Text**	**Cipher Text**	**Image File(bytes)**
40	388	388	40
12	476	476	12
32	119	119	32
40	388	388	40
16	248	248	16

Whenever the byte values of image are repeated, the value of the cipher text remains same. Hence the intruders easily identify the byte values of original image. It can be avoided by using MR as proved in Table 3.

Table 3. Encryption and Decryption of Image file Using MR

Encryption			Decryption		
ImageFile (bytes)	**MR Value**	**Cipher Text**	**Cipher Text**	**MR Value**	**Image File(bytes)**
40	1525	626	626	1525	40
12	6	325	325	6	12
32	198	111	111	198	32
40	1536	144	144	1536	40
16	1475	25	25	1475	16

Encryption and decryption time of four test images are measured before compression using RSA with Magic rectangle and listed in Table 4.

Table 4. Encryption and Decryption of image file before compression

Image size(KB)	**Encryption time(ms)**	**Decryption time(ms)**	**Total Time(ms)**
hill.jpg(68.9)	172	234	406
Rose.jpg(125)	453	547	1000
Plant.jpg(231)	640	750	1390
god.jpg(309)	797	1141	1938

The graphical representation of the above data is illustrated in fig.4. It is observed that the decryption time is always greater than the encryption time. The file size is directly proportionate to the total time for encryption and decryption. Whenever the file size increases, so does the processing time.

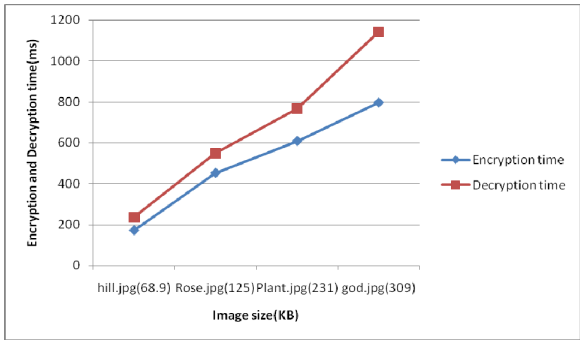

Fig.4. Encryption and Decryption of image file before compression

Encryption and decryption time of the selected four images are measured after compression using RSA with Magic rectangle and tabulated in Table 5. It is observed that using the compression technique, the file size is reduced as approximately half of the original size. It helps to reduce the processing time.

Table 5. Encryption and Decryption of image file after compression

Image size(KB)	**Encryption time(sec)**	**Decryption time(sec)**	**Total Time(sec)**
Hillc.jpg(38.8)	172	234	406
Rosec.jpg(91.8)	453	547	1000
Plantc.jpg(112)	562	688	1234
Godc.jpg(109)	515	735	1250

Table 5 value is illustrated by means of graph as in Fig..5

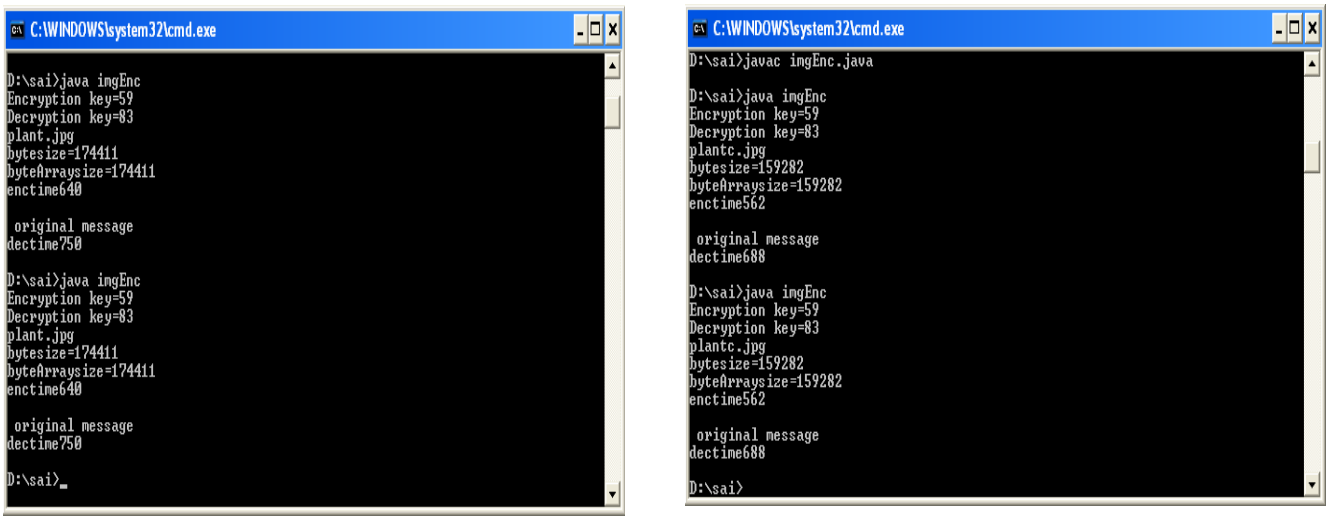

Fig.6 Sample output of the image encryption and decryption time before and after compression

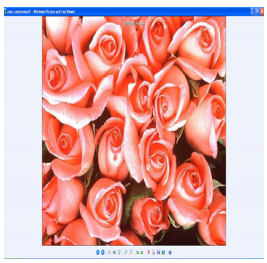

Fig.3a Original Image

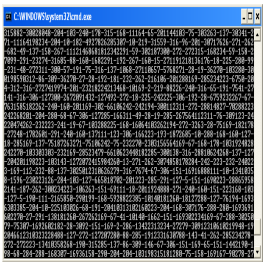

Fig.3b Cipher text

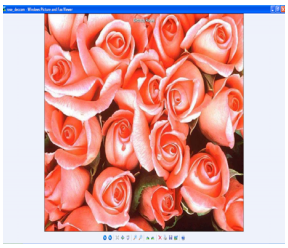

Fig.3c Decrypted Image

Fig.3 Encryption and Decryption process

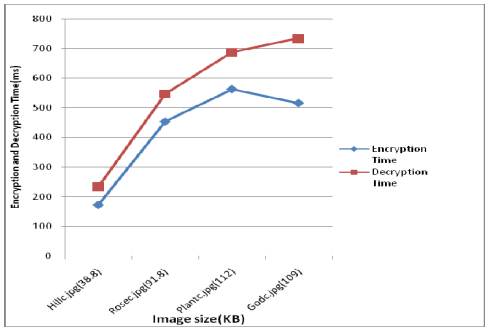

Fig.5. Encryption and Decryption of image file after compression

The sample output of encryption and decryption time of image file using compression are presented in Fig.6. Finally the execution time of both the compressed and uncompressed image files are compared using the four selected images. The corresponding graph is represented in fig 7. The uncompressed files needs more execution time than the compressed files. In the first two cases of files, there is no much difference in file size. The time taken for encryption and decryption towards these files is one and the same. In the rest of cases, where the size of the files are larger, the crypt time taken by the uncompressed file is comparatively higher than the compressed file.

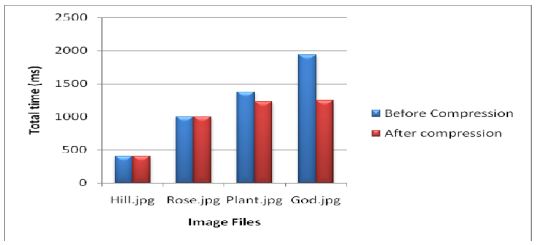

Fig.7. Comparison of execution time between compressed and uncompressed files.

4.2. Results and Discussion

The proposed methodology image encryption and decryption using MR is implemented in Java. When the file size is increased, the encryption and decryption time will also increases. It takes additional time to generate magic rectangle and image compression during initial stage. The size of the file is reduced by the compression technique. Hence additional

time is not warranted for encryption and decryption process. The data communication security is enhanced due to the randomness of the value of magic rectangle. The cipher text format of the image also plays important role in improving the security. The existing concept of image encryption and decryption used only the RGB color value and symmetric algorithms. In the proposed Algorithm, both asymmetric algorithm and MR are used for image encryption.

The proposed algorithm contains the following features.

1. Increases the randomness of the cipher text value.
2. Cipher text is in the form of numerical value instead of image
3. No much differences in Encryption and decryption process time.
4. Increases the complexity of initial activity such as image to number conversion using magic rectangle.
5. To construct the magic rectangle from any starting value and ending value
6. To apply Magic rectangle concept in any type of file such as text file, image file, audio file and video file.
7. To overcome the attacks in RSA algorithm.

V. CONCLUSION

The proposed work introduces an additional level of security using singly even magic rectangle. It enhances the randomness of the calculated value in the cipher text. In the existing work, the same cipher text value is repeated and the cipher text is in the format of image only. In Magic rectangle, there is no repetition of values. Even though the repetition of same value takes place, it assigns different value for each occurrence. There are several parameters used to construct the magic rectangle such as seed value, row sum, column sum and the Min_{start} and Max_{start} values. Hence it is difficult to identify the type of the original message whether text or image file, since the cipher text is in the format of numerals instead of image. It will be more helpful to increase the efficiency and security of the algorithm. The future improvement needed in the proposed work is to reduce the additional time needed for construction of magic rectangle and compression of images.

References

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

[2]. Gopinath Ganapathy, and K.Mani , " Add-On Security Model for publickey 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]. Quist-Aphetsi Kester," Image Encryption based on the RGB PIXEL Transposition and Shuffling", International Journal of Computer Network and Information Security, 2013, Vol 7, Pages:43-50.

[4]. Musheer Ahmad, M. Shamsher Alam," A New Algorithm of Encryption and Decryption of Images Using Chaotic Mapping", International Journal on Computer Science and Engineering, Vol.2(1), 2009, 46-50.

[5]. Varsha Bhatt, Gajendra Singh Chandel,"Implementaion of new advance image Encryption Algorithm to enhance the security of Multimedia Component" International Journal of Advanced Technology & Engineering Research (IJATER), ISSN No: 2250-3536 Volume 2, Issue 4, July 2012.

[6]. Hiral Rathod, Mahendra Singh Sisodia, Sanjay Kumar Sharma," Design and Implementation of Image Encryption Algorithm by using Block Based Symmetric Transformation Algorithm (Hyper image Encryption Algorithm)", International Journal of Computer Technology and Electronics Engineering (IJCTEE) Volume 1, Issue 3, ISSN 2249-6343.

[7]. Manoj. B, Manjula N Harihar," Image Encryption and Decryption using AES", International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-1, Issue-5, June 2012.

[8]. Mohammad Ali Bani Younes and Aman Jantan, "Image Encryption Using Block-Based Transformation Algorithm", IAENG International Journal of Computer Science, 35:1, IJCS_35_1_03, 19 February 2008.

[9]. Naresh Reddy, Rakesh Nayak ,S. Baboo, " Analysis and Performance Characteristics of Cryptosystem using Image Files", International Journal of Computer Applications (0975 – 8887) Volume 51– No.22, August 2012

[10]. Adam Rogers and Peter Loly ,"The inertial properties of Squares and Cubes", Nov-2004,pp.1-3

[11]. Mohammad Zaidul Karim and Nargis Akter, " Optimum Partition Parameter of Divide-And-Conquer Algorithm for solving closest-PairProblem", International Journal of Computer Science & Information Technology (IJCSIT) Vol 3, No 5,Oct 2011.

[12]. D.I.George Amalarethinam, J.Sai geetha, ," Enhancing Security Level for Public Key Cryptosystem Using MRGA", World Congress on Computing and Communication Technologies (WCCCT),2014 Pages 98-102.ISBN:978-1-4799-2876-7.

[13]. B.Schenier. "Applied Cryptography", John Wiley & Sons Inc, New York, Second Edition,1996.

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

[15]. Ashish Agarwala, R Saravanan," A Public Key Cryptosystem Based on Number Theory" 978-1-4673-0255-2, IEEE2012.