International Research Journal of Advanced Engineering and Science
ISSN (Online): 2455-9024

Modulus Approach of Image Steganography

Kirti
Department of Computer Science and Engineering, University Institute of Engineering and Technology, Rohtak, India

Abstract**—** *Steganograhy sends message by concealing it so that intruder can't detect the presence of message. It is an art of hiding information in digital media. It ensures that communication between two parties remain secure. Cryptography is another approach used to hide data. After cryptography, steganography came in existence. Steganography and cryptography both are using for the secure the communication. But their way of working is different. Cryptography encodes the message but steganography hides the presence of the message. This modern era need secure communication. For this various security aspects or various techniques are there. There are two types of the steganography one is spatial and the other is frequency domain. This method belongs to spatial domain. In this method image metrix with modulus approach is used to hide data..6*6 image matrix with modulus of 3 is use. Window size is select according to remainder. New approach of modulus method is introducing in this paper. In this paper steganography with cryptography is combine. In this R.S.A. algorithm and modulus approach is combining and trying to make a secure communication.*

Keywords**—** *Steganography, Cryptography, F.M.M., R.S.A.*

I. INTRODUCTION

As we know for the secure communication steganography is used from the last decades. Cryptography is also used to hide data for many years but some time it fails in secure communication [1, 2]. Steganography was used back in ancient Greek centuries when the message was tattooed on the messengers shaved heads. Hairs then grows to hide the message. Their head will be shaved when they reach the recipient of the message .Another steganography method that was used during those days is tablet wax. In order to hide the message, the tablet was erased by wax and text was etched on and then again covered it by wax and appeared blank upon inspections.

But now a day's steganography used to communicate. Both are used for secure communication but difference between them is, cryptography hides the data but steganography hides the existence of the data. So that intruder doesn't get any indication of existence of data. Steganography hides the data in any media like image, audio, video etc but cryptography scrambled data. Both of them are consider as the more secure way to communicate, if both of them are combine data become more secure. Both are used to protect the data from intruder with their own way. Two other similar techniques are there- Watermarking and Fingerprinting. These are used to protect the copyrighting data.

Transmission of data should not be detectable by any third party. More secure information like military data, business data these are more sensitive information that should be confidential and not be detectable by the any intruder. Steganography use various methods to hide the data like L.S.B, Interpolation, F.M.M and many more.

This paper discuss about the modulus approach combine with cryptography so that the data become more secure.

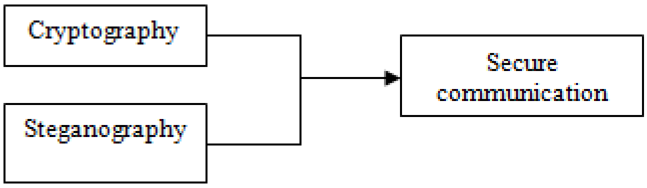

Fig. 1.

II. LITRATURE SURVEY

Shaveta Mahajan, Arpinder Singh "A Review of Methods and Approach for Secure Stegnography",. in this various method used for the steganography was introduced and there overview is given [3]. Firas A. Jassim," A Novel Steganography Algorithm for hiding Text in Image using FMM" [4].To achieve good quality of image, after applying steganography. It uses ST-FMM which provide higher PSNR value than other FMM method. Firas A. Jassim," Hiding Image in Image using FMM" [5]. In this method 4*4 window size has been implemented to hide image. For each 4*4 window inside the cover image, a number from 1 to 4 could be embedded secretly from the stego image. Chaithra H, Manjula Y, M Z Kurian, Dr. K.B. Shivakumar, Nuthan A C." Hiding Technique using FMM, Visual Cryptography and Genetic algorithm" [6] In this paper, a novel method for steganography based on Visual Cryptography and FMM has been proposed. The security features of the steganography are highly optimized using genetic algorithm. The major merit of proposed method is to increase the embedding capacity and secure the information. Praneeta Dehare, Padma Bonde" Hiding Image in Image by using FMM with LSB Substitution in Image Steganography" [7] The embedding of images done by using two algorithms, first algorithm called five modulus methods and second is LSB substitution technique. In embedding process, secret image apportioned into two parts. The first part have size of 75% of secret image that uses FMM algorithm and rest of the 25% of secret image uses LSB substitution to hide into cover image. To provide more security a private stego-key is also used with FMM algorithm so that detection of secret image from the cover image becomes more difficult for any unauthorized recipients. Firas a. Jassim, hind e. Qassim "Five modulus method for image Compression",. This paper demonstrates the potential of the FMM based image compression technique. The advantage of this method is the high PSNR although it's low compression ratio. This method is appropriate for bi-level images.

III. PROPOSED METHOD

This method works in two steps:-

1) Cyptography
2) Steganography

In this we use R.S.A. to hide the data .R.S.A is considered as the most secure algorithm till now. In step 2 we use modulus function to hide the data .The common idea behind this method is correlated pixels of image .This method uses the **ASCII vales of alphabets**. So that if data is hide in it, it should not be visible to the third party.

This method uses the window size. Window size is select according to the mode value. It depends on the new range of the values and secondly on the remainder means values that are not divisible by the number. Suppose if we choose mod 3.

Than distinct values 0-83 and the remainder 0, 1 and 2. According to above calculation window size 6 is used.

So, in the proposed method we use R.S.A. and modulus of 3 with window size 6.

A. *Insertion Algorithm*

Firstly use R.S.A. algorithm to hide data.

Steps of R.S.A.:-

1) In this we have to choose two prime no. M,N.
2) Now multiply both the no's K= M*N.
3) For the public key L= (M-1)*(N-1).
4) Private Key: (D*E) mod (M-1)*(N-1) =1.
5) CT=PT^E mod (M-1)*(N-1).
6) PT=CT^D mod (M-1)*(N-1).

Here CT means cipher text which is encrypted data and PT means plain text means original data that is to be transmitted. D, E are the keys of decryption and encryption.

In first step using this algorithm we encrypt the data.

Now data is encrypted to hide in the image we use this formula.

Alphabet/Digit value= (location+ (reminder-1) ×F^2) + (startingindex-1).

This formula is used previous [12] papers of the modulus approach.

Algorithm:- F = size of matrix=6*6
A = empty matrix=6*6
S= starting index=32
r= remainder

Steps of insertion:-

```
Step 1  Select an image of 256*256.
Step 2  M= Enter message which is to be hide.
Step 3  Calcuate the length of message.
            x=length (M)
        where M is message.
Step 4  if    x%3==0
                Do nothing
        else y =  3-x%3
                x= x+y;
    Append y alphabets append at end of x.
Step 5  Repeat until x>0
          for m=1:6
           for n=1:6
     a)  F(m,n) = Generate 6*6 sub matrix from 256*256
         matrix.(every time new next matrix is to generate)
     b)  Repeat for 3 alphabets of x
                x[i]=1;
                 r=2;
           Repeat  unil r>=0
          Repeat until Alphabets value=location+(r-1)*$F^2$+(S-1)
             r=r-1;
              Return location , r ;
     c)  Store values of location[e] and r[e] in form of linear
         array of 3 so that there values can be further use.
     d)  Now check every pixel should be modulus of 3,
         expect pixel in which data is to hide.
             A=F%3; (from here remainders of matrix are
         known)
             F=F-A; (As remainders are subtracted from sub
         matrix , from here K become new matrix which is
         completely divisible by 3)
     e)  For every pixel of 6*6 sub matrix expect  location
                Repeat for e=1:3
        K (location) = K(location)+r[e];(As remainder and
         location   are already stored)
                  end
         From here new 6*6 sub matrix in which data is
         present.
Step 6   x=x-3; (Here length of message is reduced by 3)
         M(1,i)=i+2; (New 3 characters are select)
Step7    go to step5
Step 8   Perform 5(d) for all remaining sub matrix
Step 9   Combine all sub matrix.
```

Flow chart

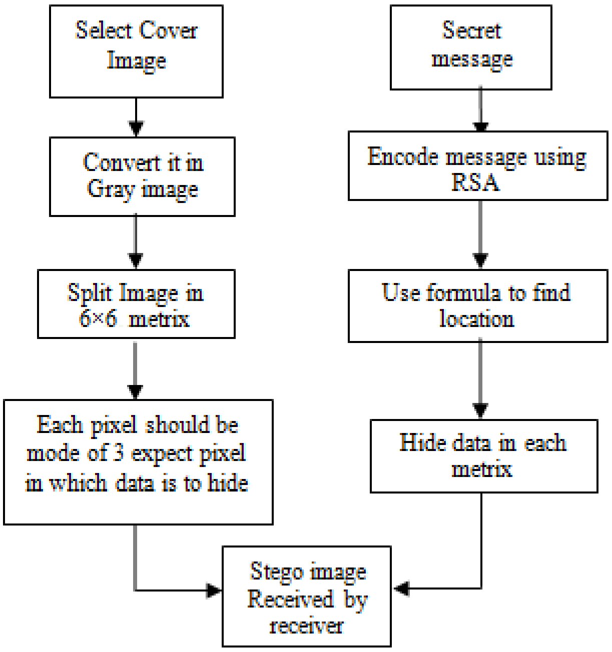
Select Cover Image
Secret message
Convert it in Gray image
Encode message using RSA
Split Image in 6×6 metrix
Use formula to find location
Each pixel should be mode of 3 expect pixel in which data is to hide
Hide data in each metrix
Stego image Received by receiver

Fig. 2. Flow chart of insertion.

B. *Extraction Algorithm*

a[n]= array of n alphabets
F = size of matrix=36
S= starting index=32
r= remainder

```
Step 1   Read pixels of stego image(256*256) .

Step 2 Repeat until all 6*6 sub matrix of stego image are not
       traversed
    a) for each sub matrix traverse all the pixels.
          For i=1:6
           For j=1:6
       If pixel(i,j)%3==0
          No Data
    b) Else
       Data is present
        r=pixel%3
       for n=a:b
       a=1,b=3;
       $a[n]=location+(r-1)F^2+(S-1)$
Step3     a=b+1;b=b+3; go to step 2
Step4    Show a[n]
Step 5   Use R.S.A to decode data.
```

Eg. Suppose " Cab" is data which is to hide . Now firstly use R.S.A. to encrypt the data.

From the first step of R.S.A choose two numbers suppose nos are 5,7

K=35

L=24

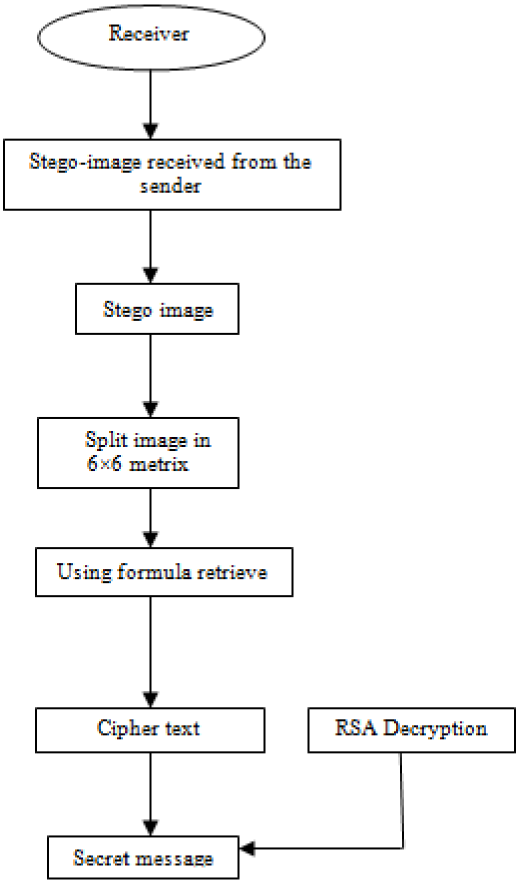

Fig. 3. Flow chart of extraction.

Private Key: (D*E) mod (M-1)*(N-1) =1, using this formula suppose the values of the D, E are 29 or 9.

For the cipher text

$CT=PT^E$ mod (M-1)*(N-1), this formula is used.

Suppose C= $(67)^9$mod 35=55 (67 is ASCII value of C)

a= $(97)^9$mod 35=61

b= $(98)^9$ mod 35=62

Now the encrypted ASCII values are = 55, 45, 67.

To hide or retrieve data in image we use this formula:-

Alphabet /Digit value= (location+ (reminder-1) × F^2) + (starting index-1)

C=24+ (1-1)36+31=55 Firstly divide image in 6×6 metrix. values of remainder vary from 0-2 for each location of sub matrix. By checking the locations from formula insert data at those locations. From this table at the location 24 data is to hide. Location which is not divisible by 3 contains data.

TABLE 1. Before insertion of data.

36	76	67	68	44	50
56	118	110	199	200	203
61	125	128	203	128	43
56	136	137	121	154	86
62	145	154	221	158	73
61	154	179	239	152	74

TABLE 2. After insertion of data.

36	78	69	69	45	**50**
54	117	111	201	201	204
60	126	129	204	129	45
57	138	138	120	156	87
63	147	156	222	159	75
60	156	180	**239**	**152**	75

a =30+ (1-1)36+31=61

b = 31+ (1-1)36+31=62

At the retrieval end pixels of matrix which is non divisible by 3 contain data. Locations and remainders (using mod remainders are obtain) are already known at retrieval end. Putting values in same formula data can be retrieve Core of this method is that every pixel value in the window metrix should be divisible by 3 expect one pixel where value is hide. Now at the other end using this formula we get the encrypted data .After retrieval of encrypted data using this formula decryption is done.

$$PT=CT^D\ (M-1)*(N-1)$$

$PT=(55)^{29}$mod35=67

$PT=(61)^{29}$mod35=97

$PT=(62)^{29}$mod35=98

Retrieve values are =67, 97, 98

Now after checking its ASCII values data is ”Cab”.

Novelty: -

This method become more secure than other methods because of using R.S.A. as data encrypted before it is hiding in image. If any intruder guess about the locations but due to encryption it is difficult to guess about the original data. In this more distinct values are present. Human eyes can’t detect the any change in the image as modulus of 3 is used and maximum change pixel value is 2. It can hide more data than previous modulus method. As in previous method only one character can be hide [12]. But in this with in one matrix 3 character can hide. This method can hide 43*43*3 data.

$\frac{256}{6}$ = 43 blocks =43*3= 129 characters

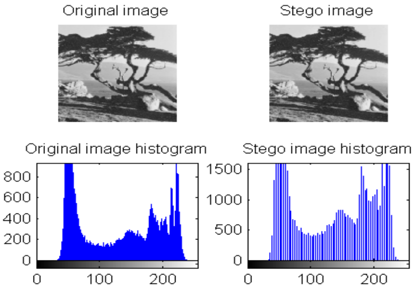

Fig. 4. (1 kb data).

Experiments Result:-

TABLE 3. 256*256 image set (1 kb data)

Image name	PSNR	MSE	MAXERR
Tree	46.38	0.098	2
Couple	40.25	0.096	2
Girl1	45.79	0.093	2
Girl2	45.87	0.097	2

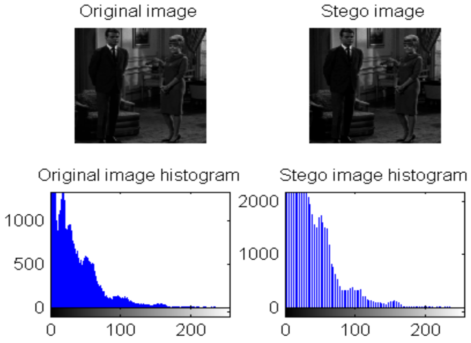

Fig. 5.

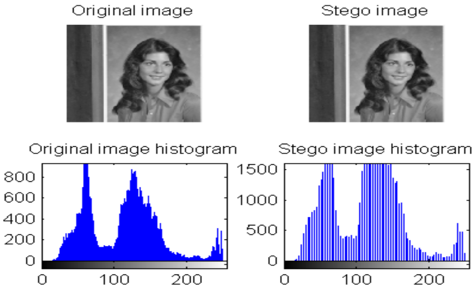

Fig. 6.

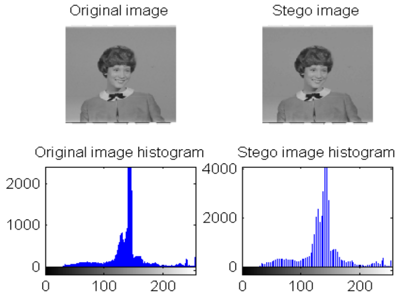

Fig. 7.

TABLE 4. 256*256 image set (2kb data).

IMAGENAME	PSNR	MSE	MAXERR
Tree	40.38	1.002	2
Couple	40.05	1.001	2
Girl1	43.09	0.096	2
Girl2	45.07	0.097	2

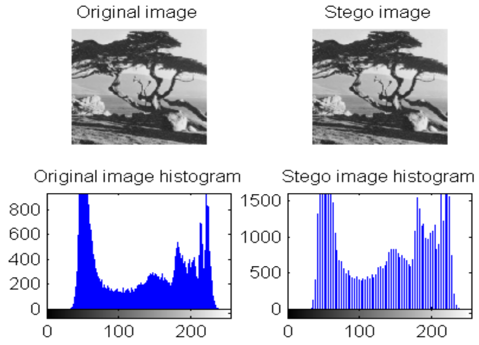

Fig. 8. (2 kb data).

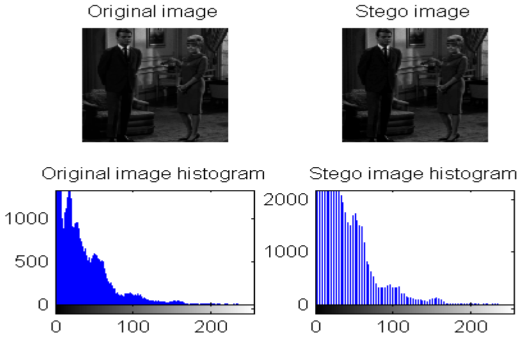

Fig. 9.

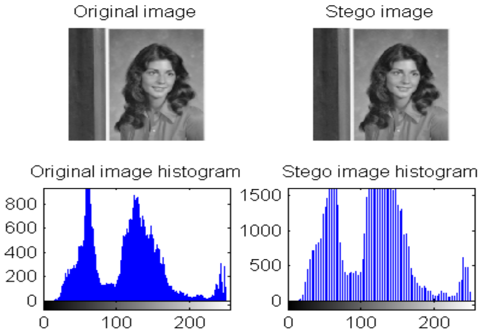

Fig. 10.

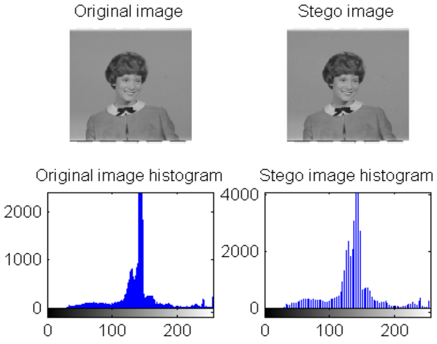

Fig. 11.

TABLE 5. Comparison of the proposed scheme with other algorithms based on PSNR (dB) with 4kb data same dimensions (256×256).

Image name	Classic LSB	SCC Method	PIT	FMM	Proposed Method
Baboon	57.42	48.27	47.80	44.58	45.93
Lena	49.58	49.89	44.07	46.13	45.94
Peppers	58.66	50.03	50.10	45.76	45.91
House	47.79	53.39	53.84	67.53	41.88

IV. CONCLUSION

Steganography make communication more secure. This method consists of combination of both steganography and cryptography. As cryptography is their before steganography. Only difference between both of them is that one encrypts data and one hides the existence of data. So, in this data is encrypted as well as existence of data is also hide to provide more secure communication. This method is more secure than other methods because of using R.S.A.to encrypt data before hiding in image. If any intruder guess about the locations but due to encryption it is difficult to guess about the original data. In this more distinct values are present. Human eyes can't detect the any change in the image as modulus of 3 is used and maximum change pixel value is 2. In this method 0, 1, 2 are remainder by using these remainders window size is selected. Decryption key is present at the end of the message metrix. It can hide more data than previous modulus method as 3 alphabets or digits are hiding with in one metrix. In previous method 100 values with in one block can hide. As in previous method only one character can be hide [12]. But in this with in one matrix 3 character can hide and than more 100 values can hide.

REFERENCES

[1] S. U. Maheswari and D. J. Hemanth, "Different methodology for image steganography-based data hiding: Review paper," *International Journal of Information and Communication Technology*, vol. 7, issue 4/5, pp. 521-536, 2015.

[2] B. Saha and S.Sharma "Steganographic techniques of data hiding using digital images," *Defence Science Journal*, vol. 62, issue 1, pp.11-18, 2012.

[3] S. Mahajan and A. Singh, "A review of methods and approach for secure stegnography," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 2, issue 10, pp. 67-70, 2012.

[4] F. A. Jassim, "A novel steganography algorithm for hiding text in image using FMM," *International Journal of Computer Applications*, vol. 72, no. 17, pp. 39-44, 2013.

[5] F. A. Jassim, "Hiding image in image using FMM," *Journal of Computing*, vol. 5, issue 2, 2151-9617, 2013.

[6] Chaithra H., Manjula Y., M. Z. Kurian, Dr. K. B. Shivakumar, and Nuthan A. C., "Hiding technique using FMM, visual cryptography and genetic algorithm," *International Journal for Research and Development in Engineering (IJRDE)*, vol. 2, issue 3, pp. 10-15, 2014.

[7] P. Dehare and P. Bonde, "Hiding image in image by using FMM with LSB substitution in image steganography," *International Journal of Advance Research in Computer Science and Management Studies*, vol. 2, issue 11, pp. 455-459, 2014.

[8] G. Chugh, R. Yadav, and R. Saini, "A new image steganographic approach based on mod factor for RGB images," *International Journal of Signal Processing, Image Processing and Pattern Recognition*, vol. 7, no. 3, pp. 27-44, 2014.

[9] F. A. Jassim and H. E. Qassim, "Five modulus method for image Compression," *Signal & Image Processing: An International Journal (SIPIJ)*, vol. 3, no. 5, pp. 19-28, 2012.

[10] S. Siddul, N. Surve, A. Vartale, and Prof. M. R. Wanjre, "Image steganography using LSB substitution and five modulus technique," *International Journal of Computer Science Information and Engg., Technologies*, issue 4, vol. 1, series 3, pp. 1-3, 2014.

[11] F. A. Jassim, "Five modulus method for image compression," *Signals and Image Processing: An International Journal (SIPIJ)*, vol. 3, no. 5 pp. 19-28, 2012.

[12] F. A. Jassim, "Hiding two binary images in grayscale BMP image via five modulus method," *Research Journal of Applied Sciences, Engineering and Technology*, vol. 7, issue 20, pp. 4235-4243, 2014.

[13] S. Mahajan and A. Singh, "A review of methods and approach for secure stegnography," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 2, issue 10, pp. 67-70, 2012.

[14] C. P. Sumathi, T. Santanam, and G. Umamaheswari, "A study of various steganographic techniques used for information hiding," *International Journal of Computer Science & Engineering Survey (IJCSES)*, vol. 4, no. 6, pp. 9-25, 2013.

[15] H. Wang and S. Wang, "Cyber warfare: Steganography vs Steganalysis," *Communications of the ACM*, vol. 47, no. 10, pp. 76-82, 2004.

[16] E. T. Lin and E. J. Delp, "A review of data hiding in digital images," in *Proceedings of the Image Processing, Image Quality, and Image Capture Conference*, Georgia, pp. 274-278, 1999.

[17] S. Channalli and A. Jadhav, "Steganography an art of hiding data," *International Journal on Computer Science and Engineering*, vol. 1, no. 3, pp. 137-141, 2009.

[18] M. Jokay and T. Moravcik, "Image-Based jpeg steganography," *Tatra Mt. Math. Publ.*, vol. 45, pp. 65–74, 2010.