An Advancement To The Security Level Through Galois Field In The Existing Password Based Technique Of Hiding Classified Information In Images

Mita Kosode, Suresh Gawande

Abstract: In this paper we are using the existing passcode based approach of hiding classified information in images with addition of the Galois field theory,which is advancing the security level to make this combination method extremely difficult to intercept and useful for open channel communication while maintaining the losses and high speed transmission.

Index Terms: Galois field, interception, stegnography.

1 introduction

Galois Field refers to a field in which there exists finitely many elements. It is particularly useful in translating computer data as they are represented in binary forms. Galois operations match those of regular maths. Addition, multiplication and logarithms are common Galois operations. Using the multiplication property of the Galois field an algorithm can be implemented to design an encoder. Mathematically 4 bit multiplication results in the 8 bit of the result but the Galois technique multiplication will result 4 bit resultant for 4 bit multiplication. As for the case of n bit multiplication it will result in n bit result.[13] In the information age, sharing and transfer of data has increased tremendously and usually the information exchange is done using open channels which can make it vulnerable to interception. The threat of an intruder accessing secret information has been a continuing concern for data communication experts [1]. Steganography (SG) is one of many techniques used to overcome this threat. It is a technique in which communication between two parties is done in a covert fashion using a cover object. SG is a very old practice for secret communication and can be traced back to techniques like invisible ink and microdots used by spies [2]. In general, the embedding operation in SG requires a digital medium to carry the data. Images and multimedia components, such as video and audio files, are widely used and exchanged through the internet. Such mediums are the best cover media to hide messages. Digital images are the most widespread cover files used for SG, due to their high embedding efficiency and the insensitivity of the human visual system (HVS) [3]. It is not necessary that the cover and message have a homogeneous structure. For example, it is possible to embed a recording of an audio stream message inside a digital image [4]. The simplest steganographic techniques embed the bits of the message directly into the least significant bit (LSB) plane of the cover image in a deterministic sequence [5, 6]. Different steganographic techniques focus on a variety of requirements such as robustness, tamper resistance, imperceptibility, security and capacity [7-10]. Our technique is focused on providing high security and high speed operation while maintaining imperceptibility. We are using here Galois Encoder to provide high operational speed while maintaining the security intensively. The 2BC (two bit code) technique is the basic steganography technique we are using with the Galois Operation. Galois field arithmetic has received considerable attention in recent years due to their application in public-key cryptography schemes and error correcting codes.[12] We are here using the 2BC(two bit code) and Galois Field algorithm to achieve the goal of the maximum reception of the original message signal while maintaining the losses and enhancing the speed of operation. Different steganographic techniques focus on a variety of requirements such as robustness, tamper resistance, imperceptibility, security and capacity. Our embedding technique is focused on providing security while maintaining imperceptibility. Our method can work in any transform domain, but we are illustrating the ideas in the spatial domain for convenience. The rest of the paper is divided among the following sections: section 2 explains the existing passcode based technique which involves the matching process and the embedding techniques, section 3 describes the Galois operation, section 4 and 5 explains the data transmission and retrieval process using the Galois Encoder and decoder, section 6 contains simulation result and section 7 summarizes the Conclusion.

2 PASSWORD BASED EMBEDDING TECHNIQUE

Matching Process and Embedding Technique Let M (i, j) be a randomly selected pixel from the cover image C, where i

- *Mita Kosode is currently pursuing masters degree program in Digital Communication in Bhabha Engineering Research Institute,Bhopal,India .*
  E-mail: mitakosode@gmail.com
- *Prof. Suresh Gawande is HOD of Electronics Communication engineering in Bhabha Engineering Research Institute, Bhopal, India.*
  E-mail: suresh.gawande@rediffmail.com

and j represent the row and column of thepixel. Let Xk denote the bit positions of M (i, j) with Xk = 8, 7, 6, and 5 representing the higher nibble as shown in Fig. 1. Let 'B' be the data of size 'L' bits to be embedded whose nth bit is Bn. Then, the matching process and generation of 2BC is done using the following steps.

Step 1: Scan the bit positions Xk (8, 7, 6 and 5) in the randomly selected M (i, j) pixel and match with nth bit of data Bn.
Step 2: Generate the 2BC associated with the matching position with 00, 01, 10 and 11 representing positions 5, 6, 7, and 8, respectively.
Step 3: If no match occurs, then all the bits in higher nibble are the same and they are different than the data bit. In such a special case of "no match", assume that a matching happened in the 5th position. While decoding, the receiver side will check for this special case and complement the bit obtained in position 5 to get the data bit.
Step 4: Repeat step 1 and 2 for all the bits (n ≤ L) of the data Bn.

The Embedding Technique for 2BC
Let 'S' be the password of length 'T' characters. The password could be of any length and any combination of characters like lower case letters, upper case letters, and special characters. The choice of password doesn't affect the performance of the algorithm. It is used to enhance the security of the algorithm by one more level. This password is converted into a binary code and is used for storing one of the bits of the 2BC. It is repeated until all bits are embedded. Let E (i, j) be another randomly selected pixel from the cover image. The lower nibble of E will be used to hide the 2BC's obtained from the matching positions of M, in different positions as shown in Fig. 2 based on a password. If the password bit is '0', then the first bit of 2BC is saved in position 1, else it is saved in position 2. The second bit of 2BC can be saved using the technique described below. Save the second bit in a specific order. For example, the first 10 bits are hidden in position 1 or 2, whichever, is available after embedding the first bit of the 2BC, the next five bits are hidden in position 3 and next bit is hidden in position 4. Repeat the same pattern until all bits are embedded. By using this approach, the PSNR value can be controlled to some degree.

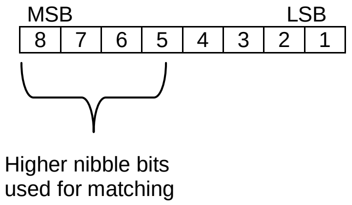


***Fig.1 :** Representation of the image pixel 'M' used for matching*

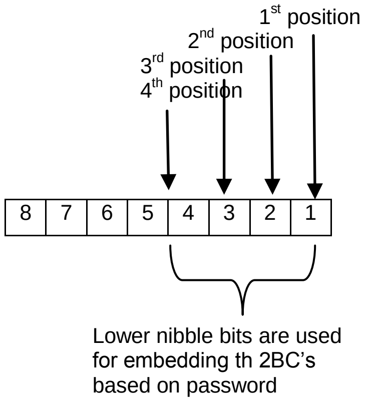


***Fig. 2.** Representation of the image pixel 'E' used for embedding the 2BC based on password.*

The mean squared error between the cover image and the stego-image is used as the measure to assess the relative perceptibility due to the embedded data [5]. The Mean Square Error (MSE) is given by,

$$\mathrm{MSE} = \sum_{i=1}^{L}\sum_{j=1}^{W}\left(f_{i,j} - g_{i,j}\right)^2 \qquad (1)$$

Where L and W are number of rows and columns respectively in the image, fi,j is the pixel value of the cover image and gi,j is the pixel value of the stego-image. The PSNR can be calculated using MSE as

$$\mathrm{PSNR} = 10log_{10}\left(\frac{P^2}{MSE}\right), \qquad (2)$$

Where P is the peak signal value of the cover image (for 8-bit images, P = 255). Say, we want the PSNR of the image to be around a specific value (50 dB). Since the value of 'P' is constant to be '255'. To obtain the required PSNR we can play with the MSE. This MSE is dependent on the change in the pixel values. The value to which the intensity of the pixel can change depends upon in which position the data is embedded as shown in Fig. 3. Hence to obtain the required PSNR we can decide how many bits and in which position they must be changed. In this way the PSNR can be controlled to some degree using the third technique.[12]

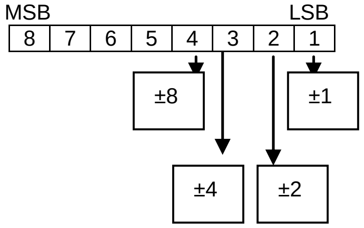


***Fig. 3.** Image Bit Error Effects*

3 GALOIS OPERATION

Using the multiplication property of the Galois field an algorithm can be implemented to design an encoder. A Galois field multiplication method enables for an arithmetical operations including addition a deduction a multiplication and a multiplier utilizing the multiplication method. The message signal is taken in form of the multiplicand that denotes 4 bit of data. Galois algorithm is implemented on the multiplicand using the generator key irreducible polynomial and a 4 bit multiplier key. Mathematically 4 bit multiplication results in the 8 bit of the result but the Galois technique multiplication will result 4 bit resultant for 4 bit multiplication. As for the case of n bit multiplication it will result in n bit result. The flowchart of Galois field algorithm describes the encoding technique using the shift and adds method. Operands will cover all combination of four binary bits and unlike standard multiplication the result will be four bit. In order to design four bit of Galois encoder the pre-requisite information is taken as message signal. The message signal is represented as the multiplicand the private key is taken as the irreducible polynomial based on NIST recommended specifications for cryptographic applications. The message bit is taken as input B, multiplier bit is taken input Ai .The irreducible polynomial and multiplicand remain static. The structure is able to multiply when the operands are all loaded.[13]

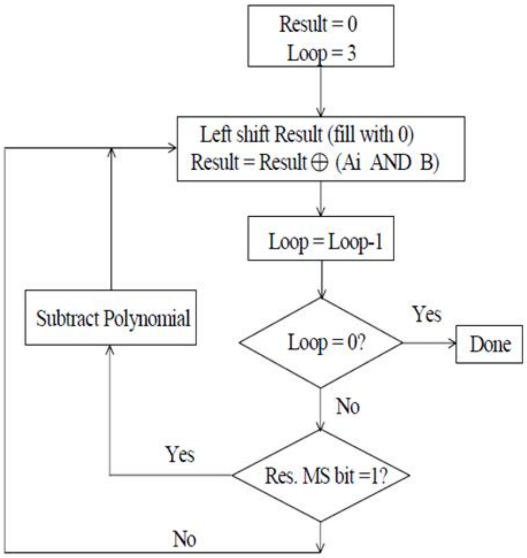


***Fig. 4:** Algorithm for GF (2m) Multiplication(Shift and Add Technique)*

Operation of the 4-bit multiplier brings as the MSB of the multiplier is under ANDing process with static multiplicand bit and resultant is EX-OR with current result register, which must initialize to 0. As multiplier bits shift, the result accumulates in “R” result. If R (3) is a 1, that means the current partial result is overflowing the 4-bit register and we must subtract a copy of the irreducible polynomial. Note that “subtraction” is also the EX-OR operation. This accomplishes the overall “modulo an irreducible polynomial” correction process. Figure 4 depicts the Galois operation. Algorithm Implemented[13]

Result =0000, Multiplicand=1111, original data Multiplier=1111 [Private Key], Irreducible polynomial [private key] =‘10011’

STEP1: 0000 XOR 1 AND (1111) = 1111 [Result] [A (3)] [Multiplicand] MSB High append step result with 0.

STEP2: 11110 xor 1 (1111) = 11110 XOR 01111 = 10001 Result is 5 Bit subtract polynomial to get 4bit result 10001-10011=00010

STEP3: 00010 xor 1(1111) = 00010 xor 01111=01011

STEP4: 1011+1(1111) =10110 xor 01111=11001(MSB 1 append 0 to result)

Result is 5 Bit subtract polynomial 11001-10011=1010
Final Result =1010
15* 15 = 10

Thus 4 bit of multiplication yields 4 bit of result.

4 DATA TRANSMISSION

At the transmitting end the data signal is first embedded in to the image using the passcode based technique then at the next stage it is then encoded via a Galois Encoder and transmitted. The flowchart for embedding the data at the transmitter side including the matching process and the generation and embedding of the 2BC is shown in Fig. 5.

GALOIS ENCODER

The Galois encoder is used at the transmitting end to encrypt the message using GF (2m) algorithm. On receiving the original Message signal the Galois algorithm implemented on the FPGA encodes the message using the private key the irreducible polynomial and multiplier. The irreducible polynomial is NIST based is 10011 $=x^4+x+1$. The 4 bit multiplication yields 4 bit of encrypted data.[13]

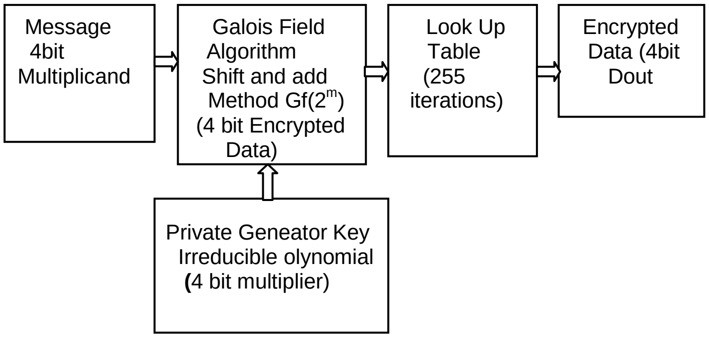

Message 4bit Multiplicand
Galois Field Algorithm Shift and add Method Gf(2^m) (4 bit Encrypted Data)
Look Up Table (255 iterations)
Encrypted Data (4bit Dout
Private Geneator Key Irreducible olynomial (4 bit multiplier)

***Fig. 6.** Block diagram for Galois Transmitter*

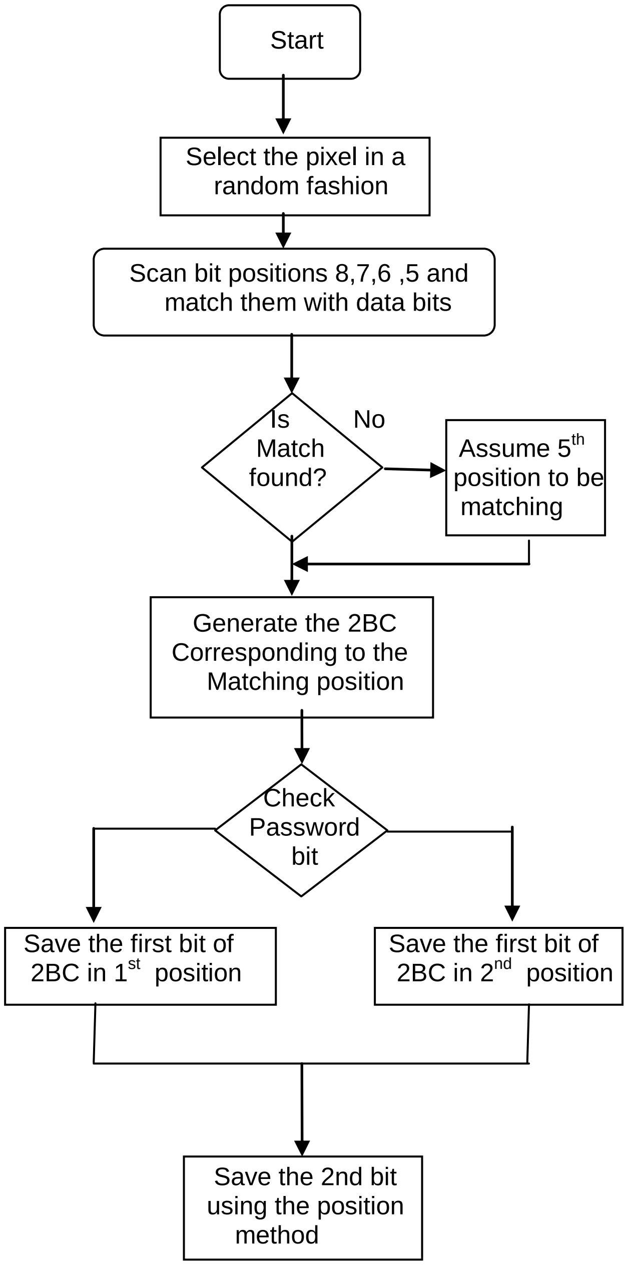
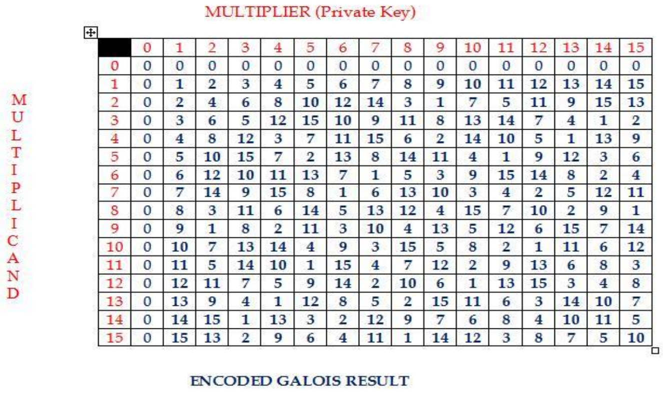

Start
Select the pixel in a random fashion
Scan bit positions 8,7,6 ,5 and match them with data bits
Is Match found?
No
Assume 5th position to be matching
Generate the 2BC Corresponding to the Matching position
Check Password bit
Save the first bit of 2BC in 1st position
Save the first bit of 2BC in 2nd position
Save the 2nd bit using the position method

Fig. 5. *Flowchart for embedding the data.*



MULTIPLIER (Private Key)

MULTIPLICAND

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
2	0	2	4	6	8	10	12	14	3	1	7	5	11	9	15	13
3	0	3	6	5	12	15	10	9	11	8	13	14	7	4	1	2
4	0	4	8	12	3	7	11	15	6	2	14	10	5	1	13	9
5	0	5	10	15	7	2	13	8	14	11	4	1	9	12	3	6
6	0	6	12	10	11	13	7	1	5	3	9	15	14	8	2	4
7	0	7	14	9	15	8	1	6	13	10	3	4	2	5	12	11
8	0	8	3	11	6	14	5	13	12	4	15	7	10	2	9	1
9	0	9	1	8	2	11	3	10	4	13	5	12	6	15	7	14
10	0	10	7	13	14	4	9	3	15	5	8	2	1	11	6	12
11	0	11	5	14	10	1	15	4	7	12	2	9	13	6	8	3
12	0	12	11	7	5	9	14	2	10	6	1	13	15	3	4	8
13	0	13	9	4	1	12	8	5	2	15	11	6	3	14	10	7
14	0	14	15	1	13	3	2	12	9	7	6	8	4	10	11	5
15	0	15	13	2	9	6	4	11	1	14	12	3	8	7	5	10

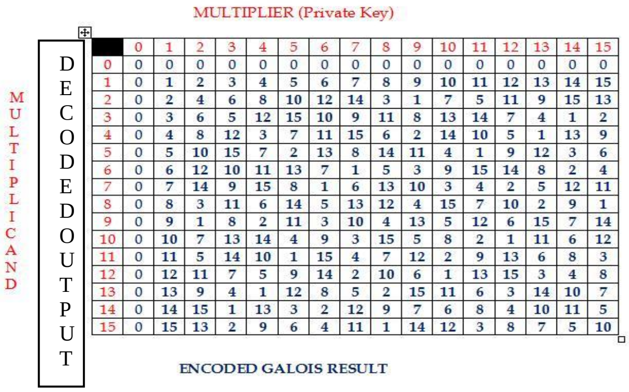
ENCODED GALOIS RESULT

Fig 7: *Look up table for Galois Encoder*

6. DATA RETRIEVAL

GALOIS DECODER

The 4 bit of the encrypted data D out is to be hatched for retrieving the original data. Multiplier is taken as the private key to decode the data at the receiver end. Look up table is created at Rx end that use the private key for identification of the original bit message data. Look up table consist of 225 iteration generated by the Galois field algorithm. The result & private key retrieves original data. If there is error in private key then the original message cannot be retrieved.[13]



MULTIPLIER (Private Key)

MULTIPLICAND

DECODED OUTPUT

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
2	0	2	4	6	8	10	12	14	3	1	7	5	11	9	15	13
3	0	3	6	5	12	15	10	9	11	8	13	14	7	4	1	2
4	0	4	8	12	3	7	11	15	6	2	14	10	5	1	13	9
5	0	5	10	15	7	2	13	8	14	11	4	1	9	12	3	6
6	0	6	12	10	11	13	7	1	5	3	9	15	14	8	2	4
7	0	7	14	9	15	8	1	6	13	10	3	4	2	5	12	11
8	0	8	3	11	6	14	5	13	12	4	15	7	10	2	9	1
9	0	9	1	8	2	11	3	10	4	13	5	12	6	15	7	14
10	0	10	7	13	14	4	9	3	15	5	8	2	1	11	6	12
11	0	11	5	14	10	1	15	4	7	12	2	9	13	6	8	3
12	0	12	11	7	5	9	14	2	10	6	1	13	15	3	4	8
13	0	13	9	4	1	12	8	5	2	15	11	6	3	14	10	7
14	0	14	15	1	13	3	2	12	9	7	6	8	4	10	11	5
15	0	15	13	2	9	6	4	11	1	14	12	3	8	7	5	10

ENCODED GALOIS RESULT

Figure 8: *Look up table for Galois Decoder*

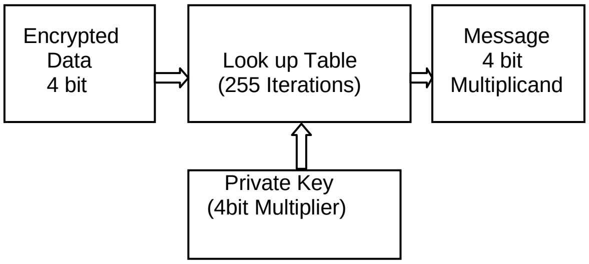

Encrypted Data 4 bit
Look up Table (255 Iterations)
Message 4 bit Multiplicand
Private Key (4bit Multiplier)

Fig. 9. *Block diagram for Galois Receiver*

The Galois encoder generates the encrypted data that can be used for transmitting the Galois encrypted message. At the receiver 4 bit of encrypted data is decoded using the Galois decoder .Multiplier as private key & look up table at the Rx end is used for decryption of the original message signal. The same pseudo random algorithms used at the Galois transmitter side are used at the Galois receiver side to find the M and E, which are the pixels used for matching the data and embedding the 2BCs based on password. The location where the first bit of the 2BC is embedded in E can be obtained from the password. Then, depending on the technique used to embed the second bit of the 2BC, the second bit can be read directly, read from position 3, or read from different positions in a particular order according to techniques 1, 2and 3, respectively. The extracted bits are then combined to obtain the different 2BCs. The data bits are extracted from the M pixels based on the locations obtained from the 2BC's. When the location is '5', the receiver will check if the bits in locations 8, 7, 6 and 5 are the same. If they are the same, then this case corresponds to a "no match" and hence the complement of the bit in position 5 is taken as the data bit, else the same bit is taken.[12] The flow chart for data retrieval at the receiver side is shown in Fig. 5.

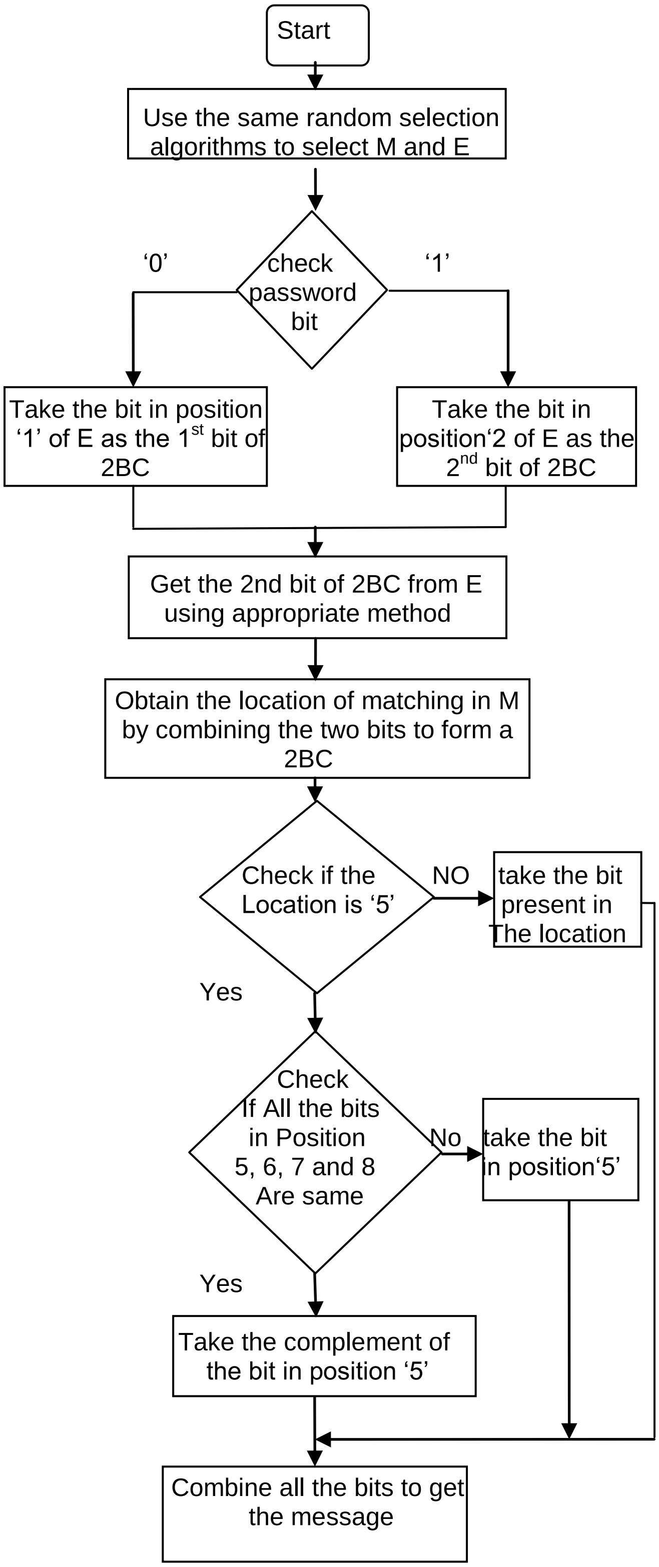

Start
Use the same random selection algorithms to select M and E
'0'
check password bit
'1'
Take the bit in position '1' of E as the 1st bit of 2BC
Take the bit in position'2 of E as the 2nd bit of 2BC
Get the 2nd bit of 2BC from E using appropriate method
Obtain the location of matching in M by combining the two bits to form a 2BC
Check if the Location is '5'
NO
take the bit present in The location
Yes
Check If All the bits in Position 5, 6, 7 and 8 Are same
No
take the bit in position'5'
Yes
Take the complement of the bit in position '5'
Combine all the bits to get the message

***Fig. 10.** Flowchart for decoding the data.*

5 SIMULATION RESULTS

The proposed data hiding techniques were implemented in MATLAB® (Mathworks, Inc., version 2007Ra) using various IEEE standard images for different number of ASCII characters. Tables 1-2 indicate the PSNR values for various Stego-images of size 256 x 256 using the proposed techniques, calculated for 1500 characters. We conducted further experiments with the Lena image using more characters. Table 2 indicates the PSNR values for the Lena image calculated for up to 1997 characters using the three suggested techniques. Thus, using the proposed method, up to 1997 characters (or 15,976 bits) have been embedded in a 256 x 256 pixel image. This shows that, 12.5% of the image pixels are used to embed 15,976 bits and yet the perceptual quality of the stego-image is still high. The PSNR of the third method can be controlled depending on number of bits being stored in various positions. Considering a minimum of 34 dB PSNR threshold for stego-image perceptual quality [11] It is clear from the obtained PSNR values that the proposed technique can generate stego-images with good perceptual quality. For qualitative assessment, , Figures 11(a), 11(b) show the Baboon image before and after steganography using the proposed technique for 500 characters. Figures 12(a) and 12(b) show the Lena image using the proposed technique, for 1997 ASCII characters.

PSNR VALUES IN dB FOR BABOON IMAGE

No of Characters	MSE	PSNR(dB)	Total Time (sec)
500	0.3141	53.16	3.532
800	0.5165	51.0	1.240
1200	0.7889	49.16	5.991

PSNR VALUES IN dB FOR BABOON IMAGE

No of Characters	MSE	PSNR(dB)	Total Time (sec)
500	0.2908	53.49	1.526
800	0.4833	51.28	1.851
1500	0.9201	48.49	1.710
1997	1.2461	47.17	1.806

6 CONCLUSION

A new steganography method for hiding classified data based on matching of bit values and Galois field multiplication property has been presented. The most important feature of this method is the extreme difficulty to which a third party would encounter in trying to intercept the hidden data. This difficulty arises from the two random algorithms used to select the matching and embedding pixels, the fact that the data bits are not hidden directly, and the use of password and the Galois password. In the proposed algorithm, an eavesdropper can destroy the message by low-bit reverse attack due to LSB weakness but cannot interpret the message. Simulation results on the IEEE standard Lena image with hiding 500 text characters indicate that the demonstrated embedding techniques can achieve PSNR of up to 53.5 dB. Lastly, the reported method has significant potential to serve as an effective means for secure transmission using open channel communications.

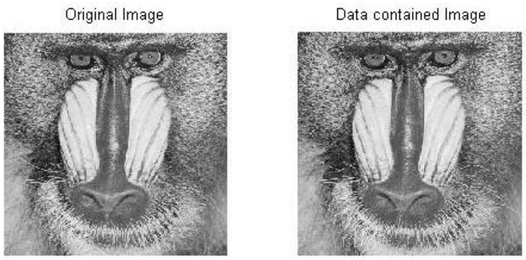


Fig. 11(a) *Baboon Image: original image* ***11(b)*** *Baboon Image: data contained image*

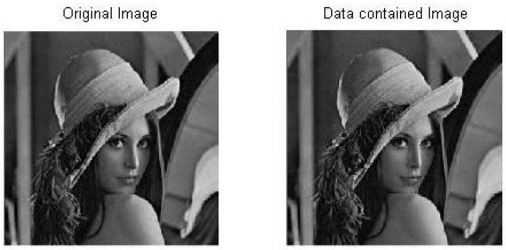


Fig. 12(a) *Lena Image: original image* ***12(b)*** *Lena Image: data contained image*

7 REFERENCES

[1] P. Marwaha and P. Marwaha, “Visual cryptographic steganography in images”, Proc. Int. Conf. on Computing Communication and Networking Technologies, Karur, India, July 29-31, 2010, pp. 1-6.

[2] D. Kahn, Information Hiding: First International Workshop, R.J. Anderson, Editor, Cambridge, UK: Springer-Verlag, 1996, vol. 1174, Lecture Notes in Computer Science, pp. 1-5.

[3] A. Almohammad and G. Ghinea, “Image steganography and chrominance components”, Proc. IEEE Int. Conf.on Computer andInformation Technology, Bradford, UK, June 29 2010-July 1 2010, pp. 996-1001.

[4] E. T.Lin and E. J. Delp, “A review of data hiding in digital images”, CERIAS Tech. Report, no.149, 2001.

[5] J. Fridrich, M. Goljan, and R. Du, “Detecting LSB steganography in color and gray-scale images”, IEEE Multimedia Special Issue on Security, vol.8, no.4, pp.22-28, Oct-Dec 2001.

[6] H. Mathkour, G.M.R. Assassa, A. Al Muharib, and I. Kiady, “A novel approach for hiding messages in images”, Proc. Int. Conf. on Signal Acquisition and Processing, Kuala Lumpur, Malaysia, April 3-5, 2009, pp. 89-93.

[7] S. Dumitrescu, X. Wu, and Z. Wang, “Detection of LSB steganography via sample pair analysis”, IEEE Trans. on Signal Processing, vol.51, no.7, pp.1995-2007, 2003.

[8] X. Luo, B. Liu, and F. Liu, “Detecting LSB steganography based on dynamic masks”, Proc. of the Int. Conf. on Intelligent Systems Design and Applications, Wroclaw, Poland, Sept. 8-10, 2005, pp.251- 255.

[9] T. Zhang, Y. Zhang, X. Ping, and M. Song, “Detection of LSB steganography based on image smoothness”, Proc. IEEE Int.Conf. on Multimedia and Expo., Toronto, Canada, July 9-12 2006, pp.1377- 1380.

[10] S. Sarreshtedari, M.Ghotbi, and S.Ghaemmaghami, “One-third probability embedding: Less detectable LSB steganography”, Proc. IEEE Int.Conf.on Multimedia and Expo.,New York, NY, June 28 2009-July 3 2009, pp.1002-1005.

[11] D. Artz, “Digital steganography: Hiding data within data”, IEEE Internet Computing, vol.5, no.3, pp. 75-80, May-June 2001.

[12] [Vijay Devabhaktuni, Vishwanath Ullagaddi, Brent D. Cameron, Firas Hassan, and Douglas Nims “A New Passcode Based Approach for HidingClassified Information in Images” 45th Southeastern Symposium on System Theory Baylor University, Waco, TX, USA, March 11, 2013

[13] Dr.Ravi Shankar Mishra, Puran Gour and Mohd Abdullah “Design & Implementation of 4 Bit Galois Encoder and Decoder on FPGA” International Journal of Engineering Science and Technology (IJEST), Vol. 3 No. 7 July 2011.