International Journal of Engineering Research-Online
A Peer Reviewed International Journal
Articles available online http://www.ijoer.in

Vol.3., Issue.6., 2015
(Nov.-Dec.,)

RESEARCH ARTICLE

ISSN: 2321-7758

A METHODOLOGY TO HIDE INFORMATION USING IMAGE STEGANOGRAPHY WITH GALOIS FIELD

SAJID PARVEZ ANSARI[1], Prof. NAMRATA SAHAYAM[2]

[1]Department of Electronics & Communication Engineering, Jabalpur Engineering College, Jabalpur
[2]Professor, Department of Electronics & Communication Engineering, Jabalpur Engineering College, Jabalpur

SAJID PARVEZ ANSARI

ABSTRACT

Steganography is the art of hiding the fact that communication is taking place, by hiding information in other information. Many different carrier file formats can be used, but digital images are the most popular because of their frequency on the Internet. For hiding secret information in images, there exists a large variety of steganographic techniques some are more complex than others and all of them have respective strong and weak points. Different applications have different requirements of the steganography technique used. For example, some applications may require absolute invisibility of the secret information, while others require a larger secret message to be hidden. This paper proposed a method to hide secret information in digital images with the use of the combination of steganography technique and galois field and to enhance security to the communication. Galois field arithmetic has received considerable attention in recent years due to their application in public-key cryptography schemes and error correcting codes. Using the multiplication property of the Galois field an algorithm can be implemented to design an encoder. Galois Encoder is used to provide high operational speed while maintaining the security intensively.

Keywords- Image steganography, Galois Field, Information Hiding, Encoder.

I.INTRODUCTION

Since the rise of the Internet one of the most important factors of information technology and communication has been the security of information. Cryptography was created as a technique for securing the secrecy of communication and many different methods have been developed to encrypt and decrypt data in order to keep the message secret. Unfortunately it is sometimes not enough to keep the contents of a message secret, it may also be necessary to keep the existence of the message secret. The technique used to implement this, is called steganography. Steganography is the art and science of invisible communication. This is accomplished through hiding information in other information, thus hiding the existence of the communicated information. The word steganography is derived from the Greek words “stegos” meaning “cover” and “grafia” meaning “writing” [1] defining it as “covered writing”. In image steganography the information is hidden exclusively in images.

The idea and practice of hiding information has a long history. In Histories the Greek historian Herodotus writes of a nobleman, Histaeus, who needed to communicate with his son-in-law in Greece. He shaved the head of one of his most trusted slaves and tattooed the message onto the

slave's scalp. When the slave's hair grew back the slave was dispatched with the hidden message [2]. In the Second World War the Microdot technique was developed by the Germans. Information, especially photographs, was reduced in size until it was the size of a typed period. Extremely difficult to detect, a normal cover message was sent over an insecure channel with one of the periods on the paper containing hidden information [3]. Today steganography is mostly used on computers with digital data being the carriers and networks being the high speed delivery channels.

Galois Field, named after Evariste Galois, also known as Finite field, refers to a field in which there exists finitely many elements[11]. It is particularly useful in translating computer data as they are represented in binary forms. That is, computer data consist of combination of two numbers, 0 and 1, which are the components in Galois field whose number of elements is two. Representing data as a vector in a Galois Field allows mathematical operations to scramble data easily and effectively. 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. In this paper, simplest steganographic technique used to embed the bits of the message directly into the least significant bit (LSB) plane of the cover image in a deterministic sequence. Different steganographic techniques focus on a variety of requirements such as robustness, tamper resistance, imperceptibility, security and Capacity. Our technique is focused on providing high security and high speed operation while maintaining imperceptibility[9]. 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.

II.PREVIOUS WORK

Information hiding plays a very crucial role today. It provided methods for encrypting the information so that it becomes unreadable for any unintended user[12]. Many researcher have worked in this field and studied about the different techniques that exist for data hiding and analyze the performance.

(a) Chetna, Krishan Kumar [4] proposed and explained a scheme in which encryption of the secret Information done before embedding it in the image. In this invisible watermarking is used with Stegano – graphic techniques. Which results that the time complexity of the overall process increases but at the same time the security achieved at this cost is well worth it.

(b) Vijay Devabhaktuni [5] proposed a new steganography method for hiding classified data based on matching of bit values . In which 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. Results shows that the advantage of this method is the difficulty to which a third party would encounter in trying to intercept the hidden data and get the higher PSNR values.

(c) Ajit Singh and Upasana Jauhari [6] provide the mechanism which enhance the security of data by using a crypto+stegano combination to increase the security level without knowing the fact that some secret data is sharing across networks.In this method encryption of the message is done before embedding by steganography technique. The security level of this method is better but it is slightly complex and lengthy method.

(d) Vishwa gupta, Gajendra Singh [7] presents a new block based cryptography algorithm. In this technique a random number is used for generating the initial key, where this key will use for encrypting the message using proposed encryption algorithm with the help of encryption number. Results shows that it is almost impossible to break the encryption algorithm without knowing the exact key value.

Different techniques of data hiding have different advantages and disadvantages. Where one

technique lacks in security of the data, the other lacks in time complexity. Some techniques are much complex than others.To remove these drawbacks, we use the simplest steganography technique with galois field.

III. DESIGN AND IMPLEMENTATION

A. LEAST SIGNIFICANT BIT STEGANOGRAPHY-

Least significant bit (LSB) insertion is a common, simple approach to embedding information in a cover image[10] . The least significant bit (in other words, the 8th bit) of some or all of the bytes inside an image is changed to a bit of the secret message. When using a 24-bit image, a bit of each of the red, green and blue colour components can be used, since they are each represented by a byte. In other words, one can store 3 bits in each pixel. An 800 × 600 pixel image, can thus store a total amount of 1,440,000 bits or 180,000 bytes of embedded data [8]. For example a grid for 3 pixels of a 24-bit image can be as follows:

(00101101 00011100 11011100)
(10100110 11000100 00001100)
(11010010 10101101 01100011)

When the number 200, which binary representation is 11001000, is embedded into the least significant bits of this part of the image, the resulting grid is as follows:

(00101101 00011101 11011100)
(10100110 11000101 00001100)
(11010010 10101100 01100011)

Although the number was embedded into the first 8 bytes of the grid, only the 3 underlined bits needed to be changed according to the embedded message. On average, only half of the bits in an image will need to be modified to hide a secret message using the maximum cover size [8]. Since there are 256 possible intensities of each primary colour, changing the LSB of a pixel results in small changes in the intensity of the colours. These changes cannot be perceived by the human eye - thus the message is successfully hidden. With a well-chosen image, one can even hide the message in the least as well as second to least significant bit and still not see the difference .

In the above example, consecutive bytes of the image data from the first byte to the end of the messag are used to embed the information. This approach is very easy to detect [3]. A slightly more secure system is for the sender and receiver to share a secret key that specifies only certain pixels to be changed. Should an adversary suspect that LSB steganography has been used, he has no way of knowing which pixels to target without the secret key .

B. 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[11]. 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 flow chart of Galois field algorithm is shown in fig.1. 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]

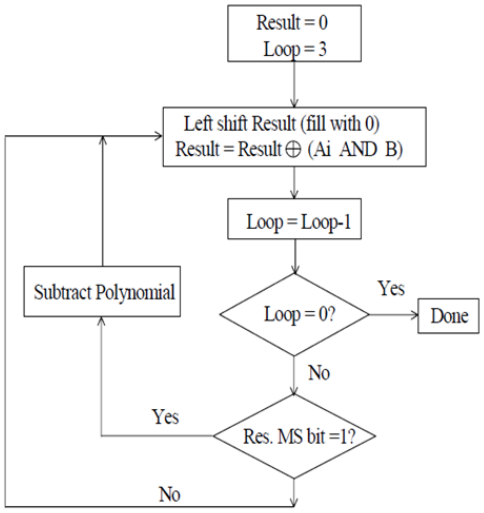

Fig. 1: Algorithm for GF Multiplication(Shift and Add Technique)

C. PROPOSED METHOD

In this paper, I proposed an Image based steganogaraphy method with the combination of Galois field theory. The Image steganography method used is a Least Significant Bits(LSB) technique. In the LSB approach, the basic idea is to replace the Least Significant Bits (LSB) of the cover image with the Bits of the messages to be hidden without destroying the property of the cover image significantly. The LSB-based technique is the most challenging one as it is difficult to differentiate between the cover-object and stego-object if few LSB bits of the cover object are replaced. After applying Image steganography method , we encode the messege with galois field by using galois look up table[13]. The galois look up table is shown in fig.3.From galois look up table ,we get new value which replace the least significant bits of the cover images. The strength of steganography can thus be amplified by combining it with Galois field. Here we describe the step by step procedure of the proposed technique which use the combination of image steganography and galois field. At first, the image to be segmented is taken as input in JPG format. The image is read by MATLAB with the help of 'imread' command and returns the image data in the array RGB (M×N×3). Next, the image is converted from RGB to grayscale image with the help of 'rgb2gray' command. After this, a random pixel of the image is selected in which the data will be encode. After selection of a random pixel, we apply LSB(Least Significant Bit) steganography technique to generate 2BC corresponding to the matching bits position of data and replaced the pixel value with the encoded value. Next, Galois field is applied to embedding the information in image. The encoded value we get from the steganography technique, is replaced by a new value which is obtained from the galois look up table. By replacing this value we get a final data contained image which is to be communicated. With the help of Galois encoder we embedded the information in cover image and send to the receiver. At receiving end, a galois decoder (which performs the reverse operation) is used to decode the information. The proposed algorithm for embedding the data is shown in fig.2

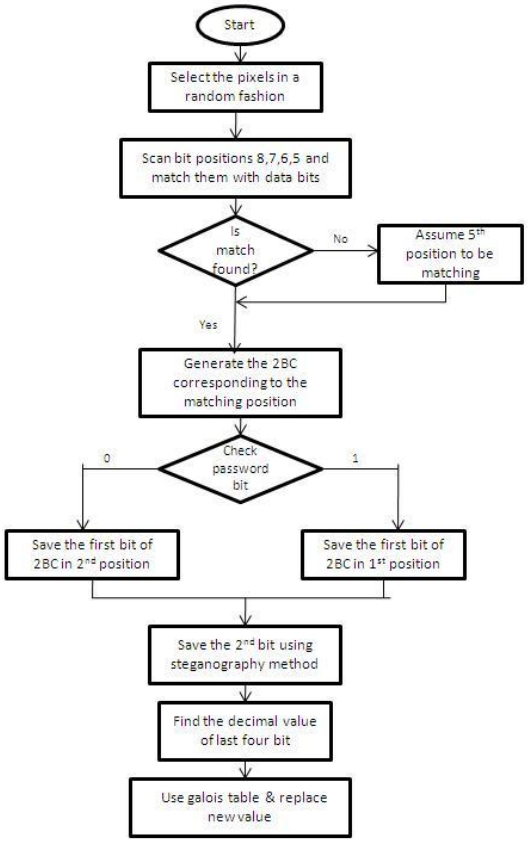

Fig. 2: Flow chart for embedding the data

MULTIPLIER (Private Key)

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

ENCODED GALOIS RESULT

Fig. 3: Look up table for embedding data

Simaulation results indicate that the demonstrated embedding techniques can achieve PSNR of min. 39.56 dB. After comparing different method with the proposed method , It has been found that the PSNR value of the image embedded by the proposed technique is slightly low but yet the quality of the stego-image is still high . It is found that the security level of the communication encoded with Galois Field is much more than the normal image based steganography . 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.

Table 1: PSNR values for various images using proposed technique

No. of characters	Lena (dB)	Pears (dB)	Peppers (dB)	Tape (dB)
800	50.78	50.29	51.49	50.91
1600	47.78	47.24	48.64	47.82
2400	45.92	45.48	46.90	46.13
3200	44.60	44.24	45.68	44.79

Table 2: PSNR values for the Lena image using the different techniques

No. of characters	4000	4800	5600	6400	7200	8000	8800	9600	10400
Technique1	60.26	59.49	58.48	58.24	57.73	57.28	56.84	56.49	56.14
Technique2	47.16	46.38	45.69	45.14	44.58	44.12	43.74	43.35	43.10
Technique3	48.81	48.03	47.37	46.74	46.33	45.80	45.34	45.02	44.70
Proposed Technique	43.65	42.80	42.22	41.68	41.15	40.69	40.27	39.91	39.56

Fig.4: Lena image using proposed method (a)before embedding (b)after embedding

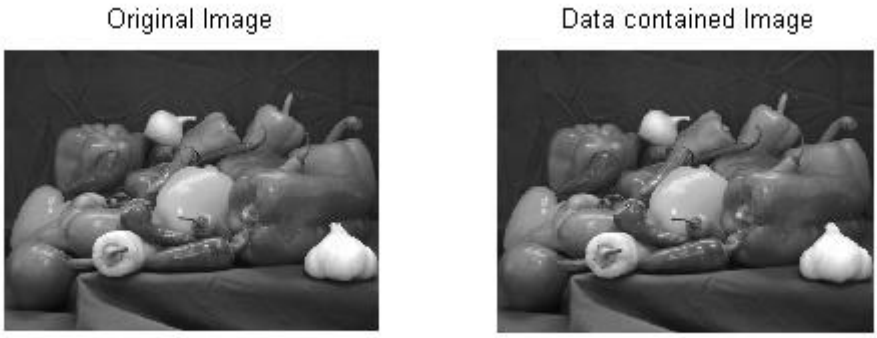

Fig.5: Peppers image using the proposed method (a)before embbeding (b)after embbeding

IV. CONCLUSION

Although only an image steganographic technique using Galois field theory is discussed in this thesis, one can see that there exists a large selection of approaches to hiding information in images. All the major image file formats have different methods of hiding messages, with different strong and weak points respectively. Where one technique lacks in payload capacity, the other lacks in robustness. For example, the patch-work approach has a very high level of robustness against most type of attacks, but can hide only a very small amount of information. Least significant bit (LSB) in both BMP and GIF makes up for this, but both approaches result in suspicious files that increase the probability of detection when in the presence of a warden. To solve this problem we use Galois field with this steganography method which reduced the probability of detection and enhance the security of communication. Thus for an agent to decide on which algorithm to use, he would have to decide on the type of application he want to use the algorithm for and if he is willing to compromise on some features to ensure the security of others.

V. REFERENCES

[1]. Moerland, T., "Steganography and Steganalysis", Leiden Institute of Advanced Computing Science,www.liacs.nl/home/tmoerl/privtech.pdf

[2]. Silman, J., "Steganography and Steganalysis: An Overview", SANS Institute, 2001

[3]. Jamil, T., "Steganography: The art of hiding information is plain sight", IEEE Potentials, 18:01, 1999

[4]. Chetna, Krishan Kumar, "Data and Information Hiding on Color Images Using Digital Watermarking" International Journal of Computer Science Trends and Technology (IJCST) – Volume 2 Issue 5, Sep-Oct 2014.

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

[6]. Ajit Singh and Upasana Jauhari "Data Security by Preprocessing the Text with Secret Hiding" , Advanced Computing: An International Journal (ACIJ), Vol.3, No.3, May 2012.

[7]. Vishwa gupta, Gajendra Singh , Ravindra Gupta, "Advance cryptography algorithm for improving data security" International Journal of Advanced Research in Computer Science and Software Engineering Volume 2, Issue 1, January 2012.

[8]. Krenn, R., "Steganography and Steganalysis", http://www.krenn.nl/univ/cry/steg/article.pdf

[9]. Saleh Saraireh "A Secure data communication system using Cryptography and Steganography" International Journal of Computer Networks & Communications (IJCNC) Vol.5, No.3, May 2013.

[10]. 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.
[11]. J.S. Milne, "Fields and Galois Theory"
[12]. Sabu M Thampi , "Information Hiding Techniques: A Tutorial Review" .
[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.