International Journal of Engineering Applied Sciences and Technology, 2019
Vol. 4, Issue 3, ISSN No. 2455-2143, Pages 353-358
Published Online July 2019 in IJEAST (http://www.ijeast.com)

A COLOR IMAGE STEGANOGRAPHY USING 7TH BIT PIXEL INDICATOR & GALOIS FIELDARITHMETIC

Pooja.V, Ganavi. M, Sowmya. D, Hiriyanna.G.S
Department of Computer Science and Engineering,
JNN College and Engineering, Shimoga

Abstract— As the web has become the medium for transmitting delicate data, the transmitted message's safety has become the top concern. Image steganography has emerged as an eminent information hiding instrument that guarantees data transmission safety. The image coding technique is used in this scheme to conceal the data along a pixel chosen and on the next value of the pixel chosen. Two parts of the message can be concealed on each pixel based on a mixture of these two values. Galois field theory is also used to build Galois picture for efficient transmission. There is nothing revealed by individual stego and Galois pictures. The Galois field of exponential reverse operation is used to disclose the hidden picture.

Keywords— Cover image, Secret image, Stego image, Galois image, Galois field arithmetic.

I. INTRODUCTION

Steganography implies hiding within the cover medium one piece of information. Hiding a document, information, picture, and video is a practice. The concept Steganography merge the Greek term steganos means “covered, hidden, or shielded” with the Greek tern “writing”. Johannes Trithemius first used the word Steganography in 1499. Many distinct transportercase formats can be used, but due to their frequency, digital pictures are the popular. There is a wide range of Steganography methods available to hide hidden data in pictures. Different apps have varying Steganography demands.

It is possible to apply Steganography methods to pictures, a video or an audio. Steganography is typically written in terms involves marking, but it is also prevalent to use it within pictures. Steganography protects against pirating copyrighted products and helps in unauthorized viewing at any level[20].

Steganography can be used to hide nearly any form of digital content, including text, picture, video or audio content. The concealed information can be concealed within nearly any other form of digital content. The information to be hidden by Steganography – known as hidden text – is often encrypted before being inserted into the text file or data stream of the innocuous looking cover. If not encrypted, to improve the trouble of identifying the secret information, the hidden text is frequently processed in some manner.

Steganography involves watermarking that hides data about copyright in a watermark by overlapping documents that the bare eye can not readily notice. This avoids fraudulent behavior and provides additional protection for media protected by copyright.

Sometimes Steganography is used when encryption is not allowed. Or, more frequently, in addition to encryption, Steganography is used. An encrypted document conceal data involves Steganography, so hidden message is not seen even if the encrypted document is decoded.

Digital watermarking is also a variant of Steganography – where one used to insert a cryptographic signature into a watermark in a document to render it digitally binding and falsified protected. The other important region of Steganography is the marking of copyright, where the message to insert is defined as to claim right for the publication of the file.

For the guarantee of data confidentiality, both Steganography and encryption are defined. Thus, the primary distinction between them, however, is that anyone can view both sides communicate in undisclosed with encryption. Steganography embeds a hidden message and no one can see in the best scenario that both sides communicate in undisclosed. It make

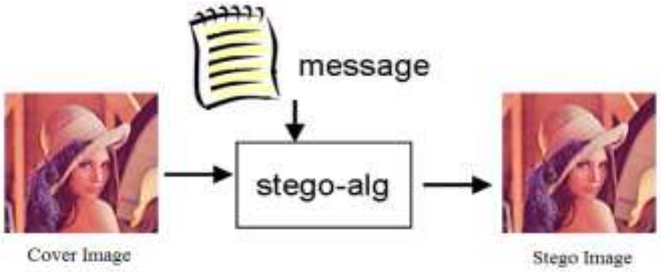


Fig 1.1: Example for Steganography

Steganography suitable for certain functions, such copyright marking, for which encryption is not. Involving encrypt copyright data to a document may simple for extraction, but encrypting in the content of the document itself may discourage simple identification and removal of it. Example for steganography is shown in the fig 1.1.

The objective of steganalysis is to locate suspected packages, determine whether or not they have an encoded payload and retrieve that payload if necessary.

Attacked information involves a data (although that information is encrypted), In general, steganalysis begins with a stack of suspected information files, and small data of documents, has a payload. Steganalyst can be generally the forensic statistician and this set of data must begin to decrease records to the subgroup most probable to have been changed.

II. PROPOSED ALGORITHM

This nominated practical technique of visual cryptography consisting of two algorithms, such as visual secret sharing and recovery algorithms based on Galois field. Fig 2.1 defines the overview of project work. First, cover picture is given as an input from the user. The user needs to select the Secret Image as well, for embedding process. Inside the cover picture, the secret picture is hidden to get the Stego picture. Here, for the hiding process, to get the Stego Image, 7th bit Pixel Indicator algorithm is used. Then Galois field arithmetic is applied to image of Stego to get the image of Galois, heighten the security of the stego images. Now these Galois images are dispatched to the participant to make the secure image transmission.

To the reconstruct the secret image, the participant read the Galois image and apply the Galois field theory's exponential reverse, on authenticating the secret key. The secret key is generated with the help of random key generation function. For the retrieved galois image, the extraction of 7th bit pixel indicator Steganography method is applied and then the secret image is extracted. This nominated job also effectively recovers cover pictures without any data being lost.

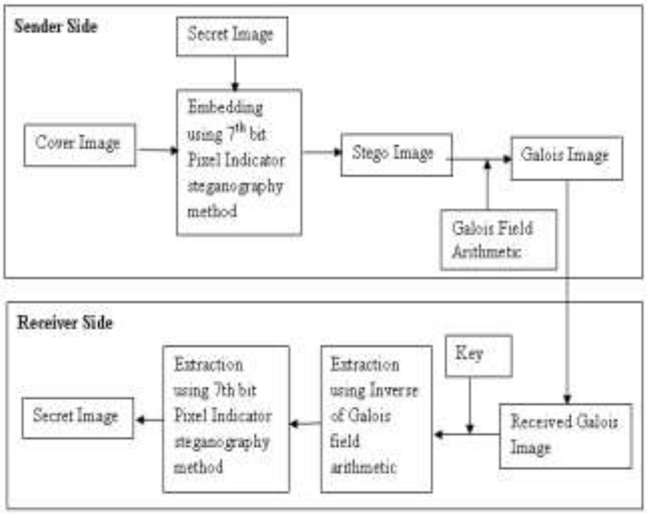

Sender Side
Secret Image
Cover Image
Embedding using 7th bit Pixel Indicator steganography method
Stego Image
Galois Image
Galois Field Arithmetic
Receiver Side
Key
Secret Image
Extraction using 7th bit Pixel Indicator steganography method
Extraction using Inverse of Galois field arithmetic
Received Galois Image

Fig 3.1: Color Secret Visual Sharing system for Embedding and Extraction

2.1 7th bit Pixel Indicator algorithm

Sender as well as the receiver is known to send the duration of the secret message. A function which is implemented at the pixel's 7th bit of an picture, that produces the short-term variable called (pixel+1) based on 7th bit of an picture. At chosen pixel, 1 bit in secret message will be concealed and second bit is placed on the value of (pixel+1). 7th bit of pixel chosen and the 7thbit of (pixel+1)is in use to hide, also to extract data. Two parts of the message can be concealed on each pixel based on a mixture of these two values.

Let the receiver and the sender knows duration of the information. Let I is the cover image of R*C pixels, S the secret N-bit message, x the pixel value of I, and s the hidden information bit, the picture matrix is defined in (2.1), and S is defined in (2.2).

$$I = \{xij|\ 1<=i<=R,\ 1<=j<=C,\ xijE\ \{0,1,\ldots,255\}\} \qquad (2.1)$$

$$S = \{sN|\ 1<=N<=n,\ sNE\ \ \{0,1\}\} \qquad (2.2)$$

Let S is concealed text, Y is the cover media, K is stego key that is in use of the insert and for extraction of information, E and D respectively defines the embedding and extraction algorithms, and Y′ defines as the stego document.A method of embedding can be provided by the below equation:

$$Y^1= EK\ (S,Y) \qquad (2.3)$$

The embedding process embedding algorithm is explained in the embedding process steps. The inverse process is performed at the other end and the information is extracted using the extraction process which is explained in the extraction process steps. The information is differentiated from the cover picture by (2.4).

$$X = DK\ (Y^1) \qquad (2.4)$$

2.2 Galois Field Arithmetic

A finite set has a finite field identified as a field, defines product, summation, difference and division and complies with arithmetic laws defined as field axioms.

The components number in the finite field is defined in their sequence or, at times, their differences. If the q sequence is a prime power pk is a finite field in q sequence. Inpk order field, summing p duplications of different component will anytime result in null, i.e., the field feature is p.

If all the q command areas are isomorphic. Furthermore, there can be no two distinct finite subfields with the same order in a field. Thus it is possible to recognize the finite fields in similar sequence and those were clearly declared as Fq or GF(q), the letters GF defines "Galois field."

2.3 System Design

2.3.1 Embedding using 7th bit Pixel Indicator Steganography method

In order to send the secret information, Steganography defines very vital role in which Image Steganography will be one among them. Here, in the proposed method, the user selects the original cover and secret picture. The secret picture is been hidden inside the cover image. For hiding process, 7th bit Pixel Indicator algorithm is used.

Each pixel of the initial image was accessed. These each pixels is converted into the 8 bit binary. The 7thbinary bits of the pixel and also 7thbinary bit of the (pixel+1) binary bits is been considered. The secret image is also converted into binary bits, the first 2 bits of the secret image is hidden inside the combination of 7thbinary bit of pixel and the 7thbinary bit of the (pixel+1) bits. And the process continues. Like this, to get the stego image, every bits of the The secret picture in the cover picture is concealed.

2.3.2 Galois field arithmetic

Stego image generated on hiding the secret picture inside the original picture is collected and read. Then for the stego image Galois field arithmetic is applied to be able to get the Galois Image. Then the user may select the number of bits they wanted to shift on applying galois field. On selecting and shifting the bits, the XOR operation is done between those pixels. The new generated resultant pixel is stored for the new image and the process continues. This generated image is the Galois image. For embedding the image, two methods is applied to heighten the security of the image.

2.4 Flowchart for Embedding and Extraction Process

The cover picture and secret image is being selected by the user. The embedding process using 7th bit pixel indicator Steganography method is used in the formation of the stego picture. For galois field, stego image is given as the input. Galois field arithmetic method is applied for the stego images to get the galois images. Fig 3.2 defines the flowchart of embedding process. Two level of embedding is done to heighten the security the secret information.

a) Algorithm for Embedding Process

Step 1: The user has to select the original cover and secret pictures.

Step 2: The images will be given as input for transmission.

The length of secret image is calculated and is transmitted into binary bits. From the help of 7th bit of the pixel, the pixel+1 value is calculated. The first two pixel bits of a hidden picture is embedded inside the 7th bit of pixel and 7th bit of pixel+1 value of the original picture. The method remains to obtain the stego picture for all the pixels of an picture.

Step 3: The stego image is given as input for the next phase.

Here the user can shift the number of bits for the transformation of the stego picture. The XOR operation is performed between the bits of the original pixel value and the shifted bits. The XORed bits is been considered as the pixel of the galois picture. The Galois picture is created in order to get one more level as security for the secret image

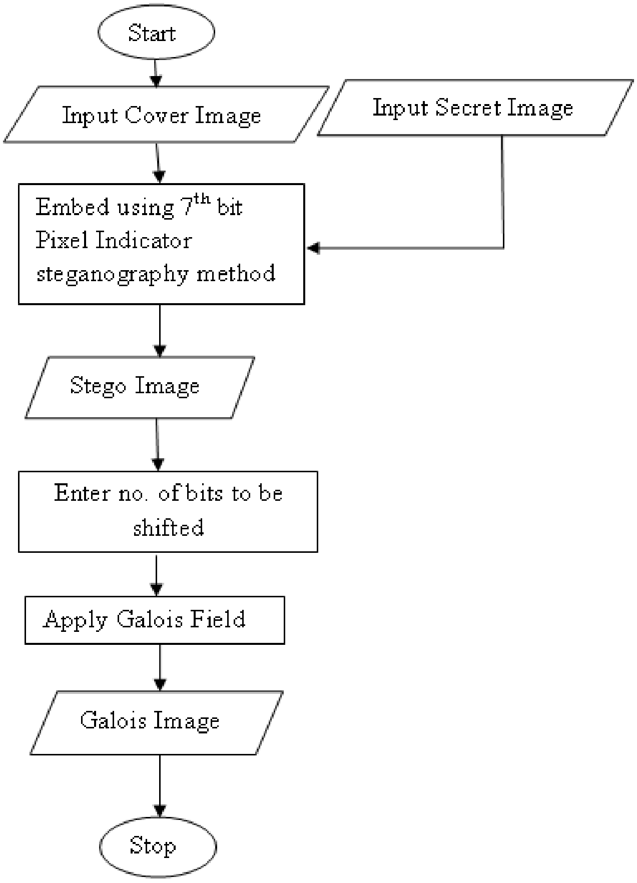

Start
Input Cover Image
Input Secret Image
Embed using 7th bit Pixel Indicator steganography method
Stego Image
Enter no. of bits to be shifted
Apply Galois Field
Galois Image
Stop

Fig 3.2: Flow chart of Embedding phase

The generated galois image in the transmitting process will be given as input in extraction process to receive the secret information. After reading the galois image, the secret has to be entered by the user which is generated through mail. This secret key is generated randomly using random generation function and is displayed to the given mail of the receiver. Only if authenticated, the inverse of galois field arithmetic is applied. After reversing the galois process, the retrieval process of 7th bit pixel indicator Steganography method is applied and the hidden data is received. If secret code is unauthenticated, the procedure is stopped. Flowchart for Extraction process is shown in fig 3.3.

b) Algorithm for Extraction Process:

Step 1: The galois picture is given as the input for the extraction process.

Step 2: After reading the galois image, the authentication process takes place.

The secret key will be generated randomly using random generation function, for the authentication of the secret information. If authenticated, move to Step 3, otherwise end the procedure.

Step 3: After authentication of the secret information, the inverse of galois field is performed for the galois picture. The stego picture is being extracted for the next stage retrieval process.

Step 4: For the extracted stego image, the retrieval process of 7th bit pixel indicator Steganography method is performed. At last, the secret picture is extracted.

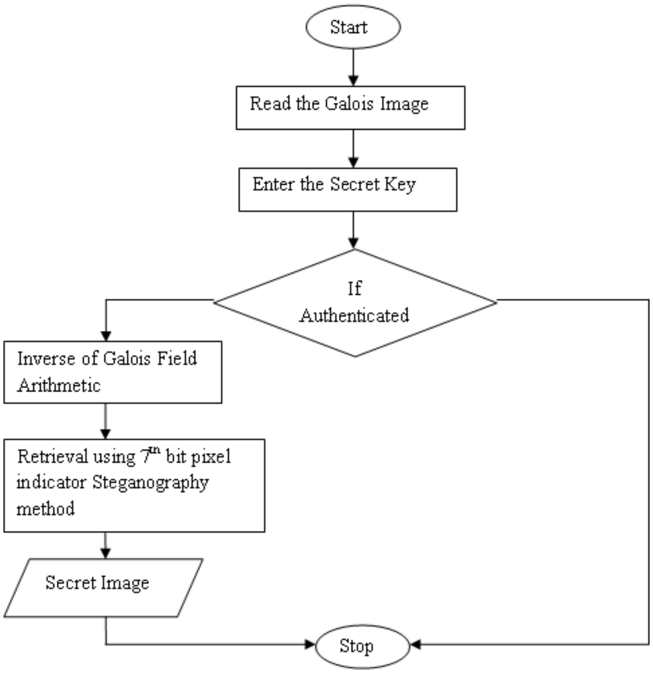

Start
Read the Galois Image
Enter the Secret Key
If Authenticated
Inverse of Galois Field Arithmetic
Retrieval using 7th bit pixel indicator Steganography method
Secret Image
Stop

Fig 3.2: Flow chart of Extraction phase

III. EXPERIMENT AND RESULTS

3.1 Results

The secret images are hidden inside the cover images to be able to get security and confidentiality for the hidden data. When the secret image is concealed in the cover image, the stego image is generated. For this stego image produced after embedding, a mathematical function is applied to obtain the

Galois image, which is used in turn to extract the hidden data. For the hiding of secret information inside the cover medium, 7th bit pixel indicator algorithm is used, that will generate the stego image. And to provide one more level of security, Galois field arithmetic is applied for the stego images to produce Galois image. These Galois image is given as the input in the Extraction process for the extraction of secret information.

Fig 3.1: Cover Image

Fig 3.2: Secret Image

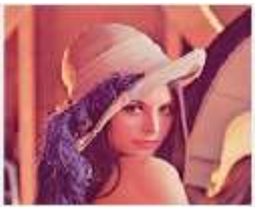
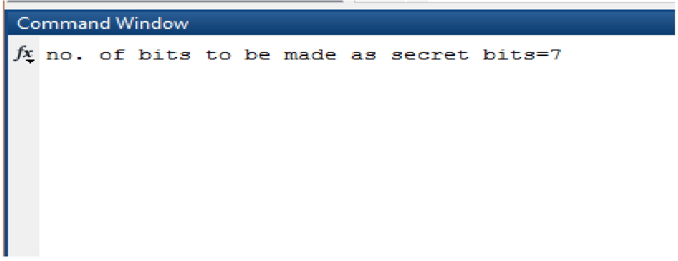


Fig 3.3: Stego Image

The initial cover picture and the secret picture are shown by the user as the input, as shown in fig 3.1 and fig 3.2. The Stego picture is produced by using the 7th bit Pixel Indicator algorithm to hide the data into the original picture, as shown in fig 3.3. The picture of stego is identical to the picture of the cover, but the only shift in the pixel values is between the original cover picture and the stego picture.



```
fx no. of bits to be made as secret bits=7
```

Fig 3.4: Snapshot of entering secret bits for the Galois field

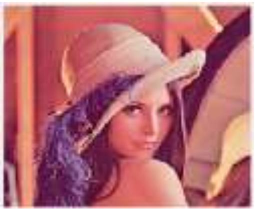
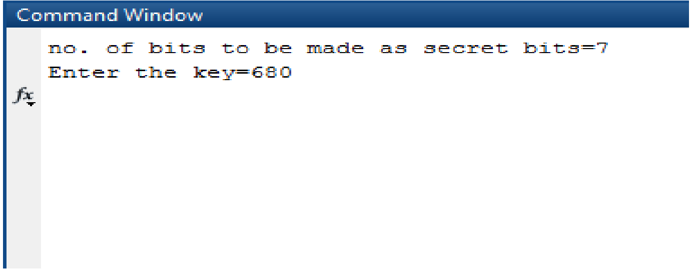


Fig 3.5: Galois Image

After hiding the hidden picture within the cover picture, the stego picture produced is taken as the input for a further conversion stage stage. For the stego image, galois field arithmetic is applied in which, the user must pick the amount of bits they would like to change as shown in fig 3.4. On selecting the bits, the performance of XOR operation is donefor the original and the shifted bits, the resultant bits is considered as the pixel value. And the process continues for all the pixels to get the Galois Image as shown in fig 3.5. These two layers of embedding is used to heighten the security of the secret image.



```
no. of bits to be made as secret bits=7
Enter the key=680
fx
```

Fig 3.6: Snapshot of entering secret key for extraction

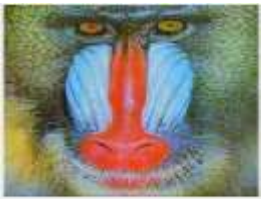


Fig 3.7: Extracted Secret Image

In the extraction phase, the secret key has to be generated by one or the other way. Here, the secret key is generated through Email. For extraction, the Galois image is given as the input. Then the user has to enter the secret key generated randomly using random generation function through mail as shown in fig 3.6. If authenticated, the stego picture is extracted from galois picture and then from the extracted stego picture, the secret picture is obtained using the 7th bit pixel indicator method Steganography as in fig 3.7. If the secret key is unauthenticated, the unauthenticated message box is shown.

3.2 Analysis Phase

Analysis is the method of breaking a complicated subject or substance into smaller components in order to obtain a better knowledge of it. The method was used in the research of mathematics and logic, although assessment as a formal idea is a comparatively latest development.

1. Peak signal-to-noise ratio(PSNR)

Usually higher PSNR indicates a greaterclarity reconstruction. PSNR is very important because it involves image processing and is used as a standard model for assessing different kinds of image quality evaluation methods. Using the embedding algorithm, the galois field is implemented to get galois picture after hiding the data in the original picture. Performance analysis is shown in table 3.1

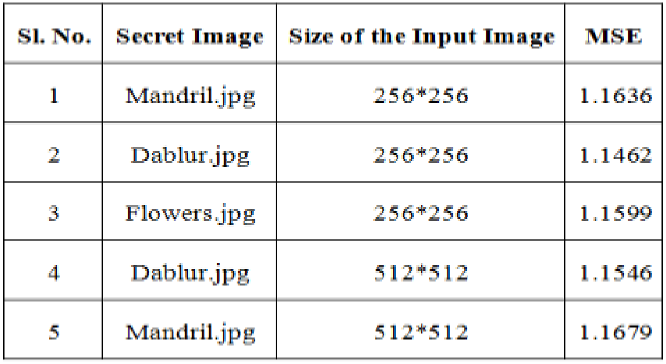
Table 3.1 Performance analysis for PSNR values

Sl. No.	Secret Image	Size of the Input Image	PSNR(in dB)
1	Mandril.jpg	256*256	52.2778
2	Dablur.jpg	256*256	52.3436
3	Flowers.jpg	256*256	52.2918
4	Dablur.jpg	512*512	58.3322
5	Mandril.jpg	512*512	58.2824

2. Mean Square Error(MSE)

A larger MSE means that the data values are frequently distributed over their main moment (mean), otherwise a reduced MSE will imply. The primary priority is the low MSE. Using the transmitting algorithm to hide the data inside the original picture, the galois field is implemented to obtain galois picture. Performance analysis is shown in table 3.2

Table 3.2 Performance analysis for MSE value

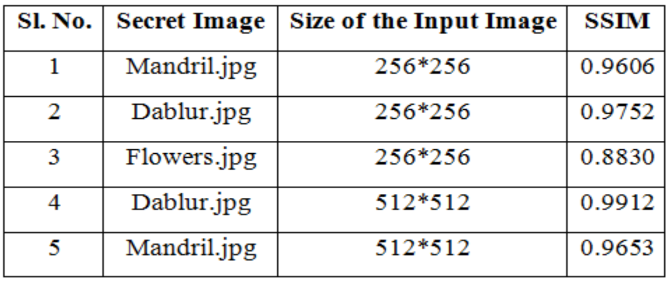


Sl. No.	Secret Image	Size of the Input Image	MSE
1	Mandril.jpg	256*256	1.1636
2	Dablur.jpg	256*256	1.1462
3	Flowers.jpg	256*256	1.1599
4	Dablur.jpg	512*512	1.1546
5	Mandril.jpg	512*512	1.1679

3. Structural Similarities(SSIM)

Using the embedding algorithm, the galois field is implemented to get galois picture after hiding the data inside the original picture.If value is near to 1 the SSIM sets values between (-1 to 1) which means that the test images are more the same. Performance analysis is shown in table 3.3

Table 3.3 Performance analysis for SSIM values

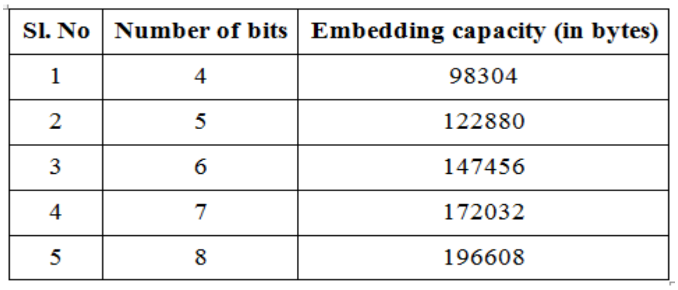


Sl. No.	Secret Image	Size of the Input Image	SSIM
1	Mandril.jpg	256*256	0.9606
2	Dablur.jpg	256*256	0.9752
3	Flowers.jpg	256*256	0.8830
4	Dablur.jpg	512*512	0.9912
5	Mandril.jpg	512*512	0.9653

4. Embedding Capacity

Using the embedding algorithm, the galois field is implemented to get galois picture after hiding the data inside the original picture. For the original cover picture "Lena.jpg" and the hidden data "Mandril.jpg," the embedding capability can be measured. The ability of embedding rises in bytes as the amount of bits rises by moving the bits for galois field purposes. Performance analysis is shown in table 3.4

Table 3.4 Performance analysis for PSNR values



Sl. No	Number of bits	Embedding capacity (in bytes)
1	4	98304
2	5	122880
3	6	147456
4	7	172032
5	8	196608

5. Histogram

Using the embedding algorithm, the galois field is implemented to get galois picture after embedding the secret picture in the cover picture. Fig 3.8 and fig 3.9 show the histogram for the proposed work of the original image and galois image respectively. The left portion of the picture indicates the initial picture and the galois picture, and the correct part of the picture displays the corresponding picture graph.

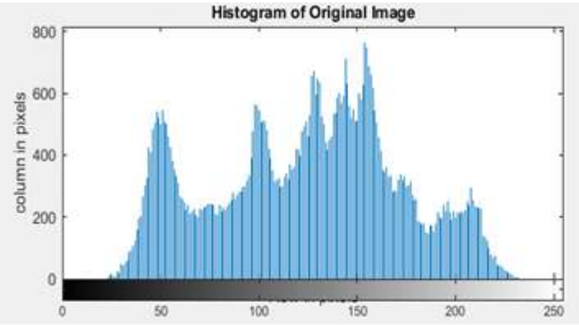


Fig 3.8: Histogram of Original Image

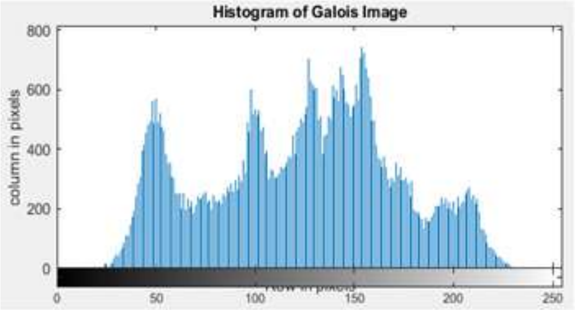


Fig 3.9: Histogram of Galois Image

IV. CONCLUSION

One of the primary requirements of steganography shall send a secret signal within the picture of the carrier without having a major difference to the initial picture. Better method for Embedding and Extraction has been proposed in this method, which provides confidentiality to images with less computation work. In the method, the 7th bit Pixel indicator algorithm is used to generate the Stego images. For those Stego images, Galois field arithmetic is been applied to get the Galois image. Here, two levels of embedding are performed to make the hidden picture more secure. For the extraction phase, Inverse of Galois field arithmetic is been used for the Galois image to extract the secret image. Embedding is achieved on different images and the calculation of quality parameters such as PSNR, MSE, SSIM, Embedding Capacity, and Pixel Correlation is illustrated with tables. It is found from the performance analysis that this technique has less MSE values and high PSNR for the color images.

This proposed method can be extended to construct more number of shadow images and participants in future. This project can be improved by combining compression and also improved to withstand different types of steganography attacks.

ACKNOWLEDGEMENT

This research was supported by the department of Computer Science & Engineering, JNNCE, Shimoga. We thank our guide Mrs.Ganavi.M who provided insight and expertise that greatly assisted the research of this paper and for comments that greatly improved the manuscript.

V. REFERENCES

[1] Ramandeep kaur Brar and Ankit Sharma, January 2018, “A Review on Steganography”, International Journal of Computer and Information Technology, Volume 07 – Issue 01, pp 45-48.

[2] Ankur Gupta, Jan-March 2018, “Image Steganography and Data Security Approaches: A Review”, International Journal of Research and Analytical Reviews, volume 5, issue 1, pp 1-5.

[3] Danny Adiyan Z.1, Tito Waluyo Purboyo2 and RatnaAstuti Nugrahaeni3, 2018, “Implementation of Secure Steganography on Jpeg Image Using LSB Method”, International Journal of Applied Engineering Research, Volume 13, Number 1, pp. 442-448.

[4] K. Joshi and R. Yadav, August 2016, “New approach toward data hiding using XOR for image steganography” in Proceedings of the Ninth International Conference on Contemporary Computing (IC3), pp. 1–6.

[5] M. Khan, S. Muhammad, M. Irfan, R. Seungmin, and B. W. Sung, 2015, “A Novel Magic LSB Substitution Method (M-LSBSM) Using Multilevel Encryption and Achromatic Component of an Image”, pp 1-27.

[6] K. Joshi and R. Yadav, December 2015, “A new LSB-S image Steganography method blend with cryptography for secret communication” in Proceedings of the 1ird International Conference on Image Information Processing (ICIIP), pp. 86–90.

[7] K. H. Jung, 2015, “Dual image based reversible data hiding method using neighboring pixel value differencing” Imaging ScienceJournal, vol. 63, no. 7, pp. 398–407.

[8] F. A. Jassim, 2013, “A novel steganography algorithm for hiding text in image using five modulus method”, Volume 72– No.17, pp 39-44.

[9] S. Atawneh and P. Sumari, 2013, “Hybrid and blind steganographic method for digital images based on DWT and chaotic map” Journal of Communications, vol. 8, no. 11, pp. 690–699.

[10] S. Rajagopalan, H.N. Upadhyay, J.B. Balaguru Rayappan and R. Amirtharajan, 2014, “Galois Field Proficient Product for Secure Image Encryption on FPGA”, published in Research Journal of Information Technology, Volume 6 (4), pp 308-324.

[11] Amirtharajan, R., K.M. Ashfaaq, A.K. Infant and J.B.B. Rayappan, 2013. “High performance pixel indicator for color image Steganography”. Res. J. Inform. Technol., pp 277-290.

[12] Amirtharajan, R., P.S. Priya and J.B.B. Rayappan, 2013. “Pixel indicated user indicator: A muxed stego”. Res. J. Inform. Technol., pp 73-86.

[13] S. Batra and R. Rishi, 2010 “Insertion of message in 6th, 7th and 8th bit of pixel values and its retrieval in case intruder changes the least significant bit of image pixels,” International Journal of Security and Its Applications, vol. 4, no. 3, pp. 1–10.

[14] K. Bailey and K. Curran, 2006, “An evaluation of image based steganography methods,” Multimedia Tools and Applications, vol. 30, no. 1, pp. 55–88.