ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

Enhancement of Security in Visual Cryptography using DES Algorithm

Er. Rimsy Dua[(1)], Er. Narender Singh[(2)]

M.Tech. Student, Department of Computer Science & Engineering, GITM, Bilaspur, Haryana, India[(1)]

Assistant Professor, Department of Computer Science & Engineering, GITM, Bilaspur, Haryana, India[(2)]

ABSTRACT*:* A new technique of Visual Cryptography is used for securing the visual content such as texts or images. In the proposed scheme mentioned below, the concept of visual cryptography is extended in terms of security, meaningful shares and the grid of the final image(extracted secret image) that is formed. Here, We have successfully implemented the proposed methodology using DES (Data Encryption Standard)algorithm. The concept is enhanced by the transformation of meaningless to meaningful shares and the security is enhanced by encrypting the shares of the secret image by using DES. The tool that we have used for implementing the proposed scheme is MATLAB(short for Matrix Laboratory).A software package i.e MATLAB is used for high-performance numerical computations having high performance and visualization. MATLAB provides an interactive environment in which there are hundreds of built-in functions for technical computation, animation, graphics etc.

KEYWORDS*:*Visual Cryptography;Secret; Shares; Data Encrytion Standard; Security; Encryption; Image quality; Number of shares; Decryption

I.INTRODUCTION

In the modern era the security over the network has become an important concern as in Internet it is now very easy to find any information. It is really a big challenge to make some information fully protected from hackers. The solution of this problem is to encrypt the data so that even if the hackers steal the encrypted data, they cannot get any information from the data. Visual Cryptography is a new Cryptography technique which is used to secure the visual content such as texts or images. In Visual Cryptography the image is divided into parts called shares which are then distributed to the participants. The Decryption side just stacking the share images gets the image. The initial model developed only for the binary images or monochrome images. The authors alter it to suit for the Color Images means Gray Images and RGB/CMYK images. For the RGB/CMYK images different methods are developed based on the color decomposition techniques[11].

One of the approach to keep a secret safe is secret sharing. Visual Cryptography is the well-known approach if the secret is an image. Most of the studies discuss the concept of visual cryptography for binary images. Later on, Visual Cryptography was extended for Gray Scale Images. Another visual cryptography scheme is (k, n)-threshold scheme. This scheme was described by Naor and Shamir. In this, a secret image is encoded into n shadow images also called shares .Recovering secret image involves stacking any k of the n shares but if k-1 or less stacking shares are there then no information about the secret image can be revealed[1].

Individual shares in the layers cannot reveal any useful information to attackers because these shares are random noise. If there is limited availability of share, then it is not possible to decrypt the message or information even with the availability of the computer. Randomness is the limitation of the above method and that is without any visual information. Extended form of Visual Cryptography have been suggested which has the same drawbacks of randomness[3].

VISUAL CRYPTOGRAPHY BASIC MODEL

A type of cryptography called Visual Cryptography is that in which there is secure encryption of images just by the division of those images in a distorted image called transparent shares and for physical transmission these shares are printed on transparency sheets and transmitted to the intended user. There are many formats accepted by Visual Cryptography such as for grayscale images, black and white images and color images. The proposed method is

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

specifically done for the color visual cryptography. The white pixels of black-and-white images are taken as transparent for ensuring transparencies in the gray scale model. Typically, in the black-and-white visual cryptography, decomposition of every pixel is done in a secret image into a block of 2×2 in the two transparencies according to the rules of the basic model. There are basically two combinations of white pixels for forming the content of the block in the two transparencies depending on whether the pixel is white or black .If pixel is white, it chooses one of the two combinations and if the pixel is black, it chooses one of the other two combinations. Therefore, when two transparencies are stacked then there will be blocks corresponding to black pixels in the secret image and also corresponding to white pixels. Blocks corresponding to black pixels are full black, and corresponding to white pixels, blocks are half- black-and-half-white, which can be observed as 50% gray pixels.
There are six possible patterns for information security from which every block in a transparency can choose randomly and so we cannot identify secret image from a single transparency. Before printing, There is a transformation of the gray-level images into halftone ones , and also the transformed Halftone images are black-and-white only.

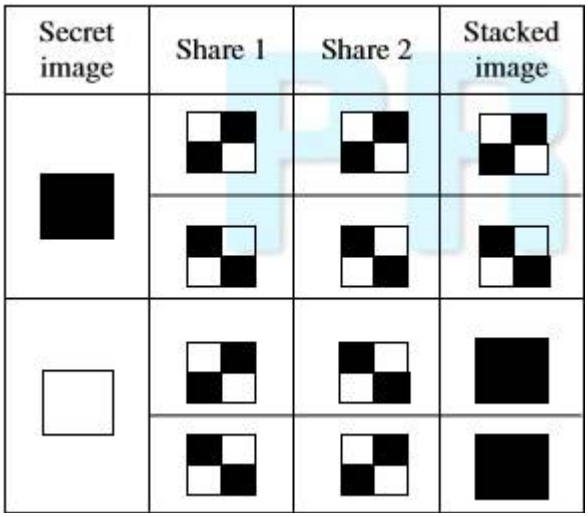

Figure 1.1: Sharing and Stacking Scheme of Black and White Pixels

This type of image format is very suitable for the traditional method to generate visual cryptography shares. Each black or white pixel in the halftone image is decomposed into a 2×2 block of the two transparencies according to the rules. In case the pixel is white, then we randomly select one combination from the former two rows as the content of the blocks in Shares 1 and 2. If there is black pixel , then one combination is randomly selected from the latter two rows as the content of the blocks in the two transparencies. This process is repeated until every pixel in the halftone image is decomposed. As a result, two transparencies of visual cryptography are there to share the secret image.
The RGB (Red, Green and Blue) color image is taken in the proposed method for the information sharing. The Floyd – Steinberg dithering algorithm is used for the manipulation of the 256 code image to low code image. Dithering is achieved using error diffusion, and the nearest neighbor pixel is taken to create the share. CMY color image format is used by the existing algorithm which is converted into eight color codes. In this method, the color code of RGB is separated into 16 standard color code formats without any reduction of the resolution. Instead of image half-toning, the dithering algorithm is used .Separate array is created and manipulated for every share by dithering. Decryption is involved for the secret image sharing and stacking. The intensity of the original image is maintained by using this method as well as 16 shares can be created and used[14].
In EVCS a secret image and original share images is taken as input and shares are generated that can satisfy the criteria given below. There can be recovery of secret image from any subset of shares. To obtain secret image, Forbidden shares can't be used. All the shares are meaningful images[6].

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

II.RELATED WORK

In [1], In visual cryptography (VC) ,most of the studies is for binary images. A good extension from binary to colors was given by Hou's method. In this study, Hou's method has been extended further so that there can be a fault-tolerant ability in new scheme. Also the secret image can still be revealed if there is a delay in one of the generated shares because of communication channel failure or by natural crash of the storage equipment, or it can be even destroyed by hackers. In the proposed scheme, a color secret image is decomposed into three shares. The secret image cannot be revealed by an individual share alone. However, if we gather any two of the three shares then secret image can be unveiled.In [2], A technique for protecting sensitive data is secret sharing , such as cryptographic keys. Literature is full of well-known secret sharing schemes such as Shamir, Asmuth- Bloom and Blakley which leads to high computational complexity during both sharing and reconstruction and also noise like shares are generated . In order to create meaningful shares, a method was proposed by Lin and Tsai that uses Steganography using the secret sharing scheme of Shamir and again that led to high computational complexity. There is a scheme that can overcome above problem and also deploys simple graphical masking method. For share generation, a simple ANDing is done and for reconstruction, a simple ORing is done on the qualified set of shares. Finally, the meaningful shares are created by using Steganography instead of noise like shares.In [3], In case of color visual cryptography methods, there is no limitation of randomness on color images. Error diffusion and pixel synchronization are the two basic methods used. One of the simple method is Error diffusion in which the there is filtering of quantization error at each pixel level and is further fed as the input to the next pixel. In this way, low frequency obtained between the input and output image is minimized which results in quality images. Color degradation is avoided with the help of pixel synchronization. An efficient color image visual cryptic filtering scheme has been presented by this proposal for improving the image quality on restored original image from visual cryptic shares. An effect called Deblurring effect is presented by the proposed color image visual cryptic filtering scheme on the non-uniform distribution of visual cryptic share pixels. After the elimination of blurring effects on the pixels, there is need to apply fourier transformation to normalize the unevenly transformed share pixels on the original restored image. As a result, the quality of restored visual cryptographic image is improved to its optimal point. In[4], In this paper , an efficient color image visual cryptic filtering scheme is proposed to improve the image quality on restored original image from visual cryptic shares. There is no limitation of randomness on color images in case of color visual cryptography methods. The two basic ideas such as error diffusion and pixel synchronization are used for error filtering of the color images and for producing meaningful color shares. A simple method of error diffusion involves the filtering of quantization error at each pixel level and that is further fed as input to the next pixel level. In this way, the low frequency obtained between the input and output image is minimized and results in giving quality images and color degradation is avoided with the help of pixel synchronization. The performance of this proposed scheme is measured in terms of PSNR value that is improved 3 times and the pixel error rate that is reduced to nearly 11% with existing gray visual cryptic filters. The proposed method completely removes the blurring noise effect when the original image is restored.In [5], In visual cryptography (VC) schemes, there is hiding of the secret image into two or more images which further allows the encoding of secret image into shares which are distributed to participants. The recovery of secret image can be done simply by stacking the shares together and that is without any complex computation. In traditional VCS, random shares were used but in case of Extended Visual Cryptography Scheme (EVCS) meaningful shares are there. In this paper, a color visual cryptography scheme is proposed that uses meaningful shares. These meaningful shares will not arouse the attention of hackers. The halftone technique, secret coding table and cover coding table is utilized by the proposed scheme, to generate two meaningful shares. Comparative analysis have demonstrated that new scheme is perfectly applicable and also high security level is achieved.In [6], Hiding of secret image into n number of shares is the main concept of Visual Cryptography and those n number of shares are further distributed to n number of participants. There is no need to know the cryptographic knowledge in order to recover the secret image from the shares due to which this scheme is very useful. This concept is called VCS i.e Visual Cryptography Scheme. In extended visual cryptography scheme, there is a generation of meaningful shares when compared with the shares of the VCS. An EVCS is proposed here by embedding the random shares (result of VCS) into covering images. There is more security in proposed EVCS as shown by empirical results and also this scheme is flexible than the EVCS found in literature.In [7], A cryptographic technique called Visual cryptography allows visual information (pictures, text, etc.) to be encrypted in such a way that decryption becomes such a mechanical operation for which there is no requirement of a computer. In color visual cryptography, a color secret message is encrypted into n color halftone image shares. Some methods for color visual cryptography failed to provide satisfaction both in terms of producing either meaningful shares or meaningless shares with low visual quality

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

and that further leads to suspicion of encryption. We propose the visual cryptography for color image for reducing the size and the distortion of decrypted image that uses visual information pixel (VIP) synchronization and dithering technique of floyd error diffusion. There is an improvement in the quality of decrypted image as compared to other dithering techniques. This proposed method has better performance as compared to previous approaches. In [8], In this method, a transparency is provided by the visual variant of the k out of n secret sharing to each one of the n user; such that any k of them can see the image by just stacking their transparency but if k-1 of them attempts to see the image then no information will be given about it. The resulting image is similar to the original image. The two important parameters to evaluate the effectiveness of a visual cryptography are pixel expansion and contrast. In this paper, To minimize the pixel expansion and increase image contrast, linear programming matrix algorithm and the halftone pattern is used. Security of an image is enhanced by the resulting scheme with minimal pixel expansion and maximum contrast.In [9], Now a days ,it has become a common practice that multimedia contents, confidential or secret data such as financial documents, military information are being distributed over the internet. Along with this, the main target of many malicious applications are financial account information and documents, secret images, etc. For secure transmission, there are three possible major common approaches. These are key encryption, steganography and visual cryptography. A new algorithm in which all the three approaches will be combined is proposed and this will overcome problems associated with these and provide additional security. A symmetric secret key is used by this scheme for the encryption of the image and then there is a generation of secret shares of cipher image by secret sharing algorithm with steganography. In [10], In this paper, a new design for friendly visual cryptography scheme is proposed. The hiding of secret will take place into two meaningful shares. The ratio of black-appearing in each block of the shares is same for the corresponding black (rep. white) secret pixel. Disclosing any information related to the secret image on each share is impossible which achieves the goal of improving security. The contours of the cover image will disappear on the stacked image by superimposing the shares, which will only reveal the secret image. According to our experimental results, the contrasts of the stacked images or shares are good which can reveal the contents of the secret images and the cover images clearly.In [11], In this paper ,a new scheme for encrypting secret message has been applied by authors where the secret message is embedded in three shares. For the reconstruction of the secret message all the three shares are to be stacked one by one. This method is fully secured as no information can be retrieved until and unless all the three shares are used together.In [12], Nowadays, There is an enhancement in security and efficiency because of dependence of each and every transmission system on internet and also the response time is reduced. This advantage of real time on internet is also being taken by Visual Cryptography and also at destination user for security purpose. In this proposed system, the main focus is to provide mechanism for information security by using visual cryptography scheme on condition that privacy, Authentication, authorization, Confidentiality, and security are maintained in VCS. We work with digital gray scale images for secret and covering image, data confidentiality can be provided using asymmetric cover image encryption and finally there is an improvement in the contrast of the recovered secret image and clear resultant image is produced.In [13],A Visual cryptography technique allows visual information (pictures, text, etc.) to be encrypted in such a way that decryption becomes such a mechanical operation for which there is no requirement of a computer. There is splitting of original image into shares and it can't be possible for unauthorized person to get the data which is hidden within that share images. The secret data can be revealed just by stacking the two shares. Similarity in size and quality of the reconstructed image to that of the original image is the highlighted issue in VC. In this, in order to improve security and to produce meaningful shares, a novel k out of k extended visual cryptography scheme (EVCS) is used. In halftone visual cryptography (VC), there is an encoding of a secret image into k halftone meaningful image shares through error diffusion algorithm of Floyd steinberg. In [14], In existing methods, there is a work for color images with 8 colors and even few of them are without halftone techniques. In this paper, a method is proposed for images with 256 colors and these are further converted to 16 standard RGB colors format. Shares are generated without compromising the resolution. The dithering algorithm of Floyd – Steinberg is used for the manipulation of the 256 color code image so as to reduce it to 16 standard colors code image. (2, 2) XOR-Based visual cryptography method employed by the proposed method is also used to generate shares. Secret image sharing and stacking is enabled by the Decryption procedure.In [15], In this paper, Double layer encryption and Double layer hiding is proposed which is supposed to give security to the secret data and the secret images. There is a usage of X- or base visual cryptography and higher LSB data hiding method. A Visual cryptography (VC) technique encrypts a secret image into n shares. Each participant holds one or more shares. The original motivation of Visual Cryptography is to securely share secret images in non-computer-aided environments. Devices with computational powers are ubiquitous. Double security and less complexity is proposed compared to existing system.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

III.SCOPE OF RESEARCH

In the proposed scheme, we have used the concept of cover image.Cover image is that image which is used for hiding secret image i.e the user will misinterpret it as original secret image but in fact it is just cover image.Here,in the proposed methodology ,it is necessary that the size of the secret and cover image must be same .Our future scope is that the size of secret image and cover image is not the mandatory requirement i.e if the size of the secret and cover image is different then still it must be possible to extract the secret image from the cover image with same quality as when the size of the secret and cover image was similar.

IV.PROPOSED METHODOLOGY AND DISCUSSION

4.1 PROPOSED WORK

Presently the generated shares are meaningless i.e. the shares do not express any meaning, There can be generation of meaningful shares by the use of cover image so that just by viewing the shares no one can guess that there is some secret data encrypted in that image. The shares can be encrypted using DES algorithm to ensure more security to shares so the present work can be improved by removing the unwanted colors from the decrypted image and extended to (4,4) cryptography scheme.

4.1.1 PROPOSED ALGORIHTM AND FLOWCHART

The proposed algorithm for our research is DES i.e Data Encryption Standard. Its proper name is Data Encryption Algorithm as this was based on Lucifer algorithm .This algorithm provides very strong encryption by using a combination of two fundamental building blocks of encryption i.e Substitution and Transposition. Two other alternative terms are linked with substitution and diffusion. These terms are Confusion and Diffusion. Confusion means to create cipher text in such a way that its plain text is not apparent .The basic tool for confusion is substitution. Diffusion means to spread the effect of change in plain text throughout the resulting cipher-text and the basic tool for diffusion is Transposition. Basically, Substitution is represented by S-Boxes and Transposition is represented by P-Boxes. Data Encryption algorithm is an iterative algorithm that uses table look ups and simple bit operations. First of all, Input to the DES is arranged in the form of 64 bit blocks. We know that this algorithm basically operates on data blocks.So the 64 bit input is divided into two halves (Left half and Right Half) each of 32 bits. Each half is scrambled independently, key is combined with one half and then the two halves are swapped. This is called 1 cycle and the process is repeated 16 times. The following are the steps of an algorithm along with its flowchart.

4.1.1.1 EXPANSION PERMUTATION

The very first step of this algorithm is Expansion Permutation.The main intent behind expansion permutation is to make intermediate halves of the cipher text comparable in size to the key and provide a longer result that can later be compressed. In this,right half is expanded from 32 to 48 bits. In this ,order of the bits is permuted and also the certain bits are repeated.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

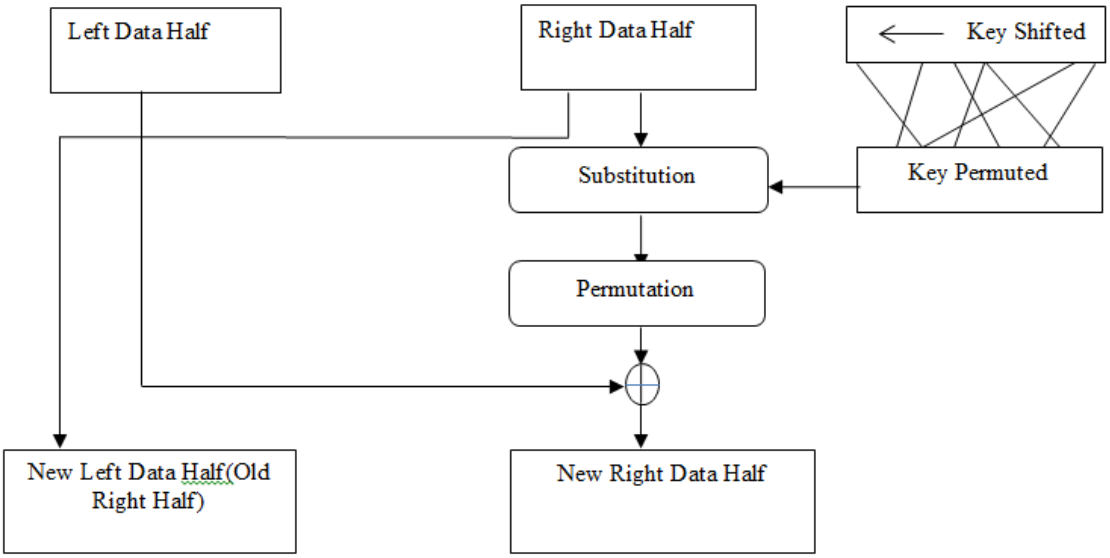

Figure 4.1 Basic Flowchart of DES

4.1.1.2 KEY TRANSFORMATION

Here the key length is of 64 bits but we will use only 56 bits as a key in our proposed algorithm by removing every 8^{th} bit (8,16,24,……..,64).This is because these 8 bits are used as parity bits and no information is carried by these parity bits in the key. This process is called Key Transformation. There is a splitting of a key into two 28 bit halves at each step in the cycle. There is a left shifting of these two halves by a specified number of bits which are then pasted together again. Out of 56 bits,48 bits are permuted to use as a key during this cycle. After key transformation,48 bit key is combined with expanded right half by using an exclusive-OR operation.

4.1.1.3 S-BOXES

S-Boxes are used to perform substitution based on a table of 4 rows and 16 columns. It is a permuted choice function in which there is a replacement of 6 bits of data by 4 bits. There are 8 S-Boxes.Here,48 bit input is divided into eight 6 bit blocks identified as $B_1,B_2,B_3.....B_8$. S-Box S_j operates on block B_j. Suppose that block B_j is 6 bits i.e $b_1, b_2, b_3, b_4, b_5, b_6$ .Bits b_1 and b_6 having a decimal value from 0 to 3 form a two bit binary number and is equal to the value of row i.e represented by r .Bits b_2, b_3, b_4, b_5 having a decimal value from 0 to 15 form a decimal number which is equal to the value of the column that is represented by c.

4.1.1.4 P-BOXES

All 32 bits of the result obtained after an S-Box Permutation are permuted by straight permutation. Here the bits will be moved to different positions and there will be 8 bits on each row. Basically, there are two types of permutations that are employed in this algorithm .One is Initial Permutation in which the 64 bits of each input block is reordered. Another is Final Permutation that is used at the conclusion of 16 substitution-permutation rounds.

4.1.1.5 COMPLETE DES

Now, all the different pieces are combined together to form complete DES.Firstly, 64 bit key is reduced to 56 bits. Then the initial permutation is carried on the 64 data bits. There are 16 cycles in which key is shifted and permuted. There is a transformation of half of the data block with the substitution and permutation functions and the result is combined with the remaining half of the data block.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

V.EXPERIMENTAL RESULTS

Figure no. 5.1 Cover Image | Figure no. 5.2 Secret Image | Figure no. 5.3 Stegnographic Image | Figure no. 5.4 Extracted Image

Figure 5.1 shows the cover image for the process of Visual Cryptography. This cover image is basically used to hide the secret message. The cover image and the secret image must be of same size. Figure 5.2 shows the secret message to be hidden. This secret message will be hidden in the cover image. The use of cover image is to misrepresent the identity of the cover image to any unauthorized person. He or she will think that the cover image they are visualizing is original image. In this way, there will be safe secret image. Figure 5.3 shows the stegnographic image in which secret message is hidden in the cover image but it is difficult to identify the secret image from the cover image by just looking at the stegnographic image.This is because Stegnographic image will show the original image in front .Figure 5.4 shows the secret message is extracted from the stegnographic image. The main focus is on enhancing the quality of the extracted image approximately equal to that of original secret image.

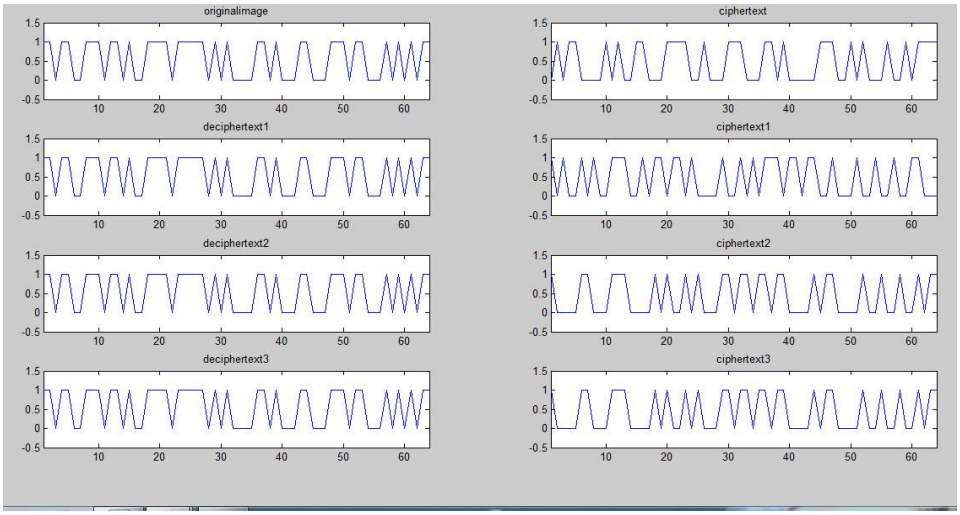

Figure no. 5.5Encoding and Decoding

This figure shows the encoding and decoding of the original image. Here, we can observe that there is a variation of different parameters due to which different cipher text are produced for the same plain text. On the other hand, same decipher text is produced at the decryption end i.e the same secret message will be retrieved after the decryption.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

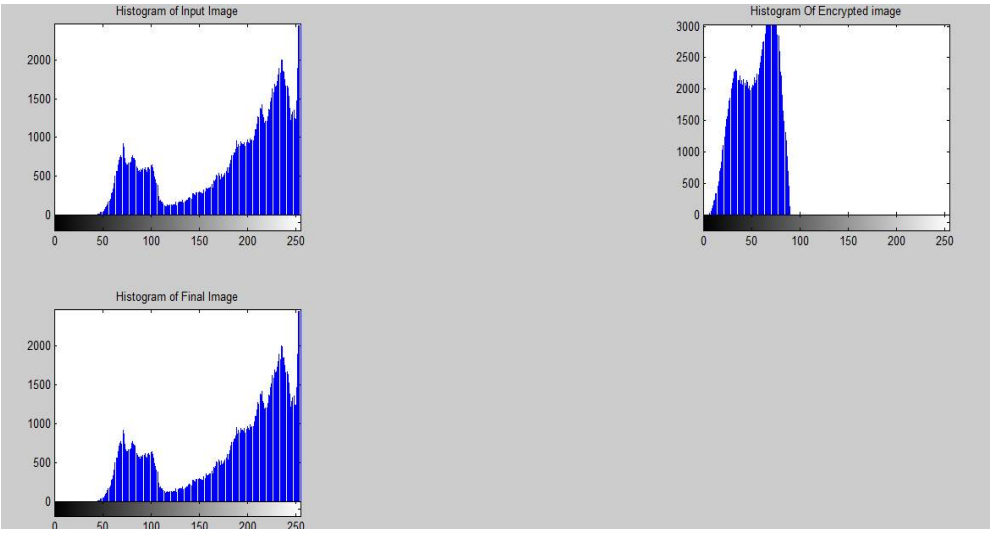

Figure no. 5.6Histogram of Final Image

This figure shows the histogram of the input image, encrypted image and the final image. It can be observed that the histogram of the input image and final image is same but that of the encrypted image is different. This is because encrypted image also contains the cover image.

VI.CONCLUSION

We have successfully implemented the proposed scheme using Data Encryption Standard algorithm.The detailed evaluation of the proposed scheme is done with the help of histogram.The histogram of the input image,encrypted image and the final image is shown in the previous chapter.From histogram,it is analysed that the histogram of the input image and final image is same but that of the encrypted image is different. This is because encrypted image also contains the cover image.

VII.ACKNOWLEDGEMENT

The process of implementation of the proposed scheme “Secured Visual Cryptography Using Meaningful Shares” was carried out at Ganpati Institute Of Technology And Management ,Bilaspur (Yamuna Nagar).All the faculty members of computer science and engineering department helped me a lot in retrieving the desired results .Also,I would like to thank head of Ganpati Group Of Institutions ,Principal and management of GITM,Bilaspur(Yamuna Nagar) for supporting me during the dissertation period.

REFERENCES

[1]. Kun-Yuan Chao* , Ja-Chen Lin,”(2, 3)-threshold visual cryptography for color images”, Proc. of the 6th WSEAS Int. Conf. on Signal Processing, Computational Geometry & Artificial Vision, Elounda, Greece, August 21-23, 2006 (pp89-94).
[2]. Prabir Kr. Naskar, Ayan Chaudhuri ,Atal Chaudhuri,” Image Secret Sharing Scheme Using a Novel Secret Sharing Technique with Steganography”, IEEE CASCOM , pp 62-65, Nov. 27, 2010.
[3]. Shiny Malar F.R, Jeya Kumar M.K,” Error Filtering Schemes for Color Images in Visual Cryptography”, International Journal of Advanced Computer Science and Applications, Vol. 2, No. 11, 2011.
[4]. Shiny Malar F.R , Jeya Kumar M.K ,” A novel algorithm for color visual cryptographic images using error filtering schemes”, International journal of computer engineering & technology (ijcet):ISSN 0976 – 6367(print) ,ISSN 0976 – 6375(online),volume 3, issue 2, pp. 323-336, july-september 2012.
[5]. Ch. Priyanka, Prof.ThaduriVenkataRamana, and T.Somashekar,” Analysis of Secret Sharing & Review on Extended Visual Cryptography Scheme”, International Journal of Engineering Inventions, ISSN: 2278-7461, ISBN: 2319-6491Volume 1, Issue 10 (November2012) PP: 43-51, 2012.
[6]. Jerripothula Sandeep, Abdul Majeed,”Embedded Extended Visual Cryptography Scheme”,IOSR Journal of Computer Engineering (IOSRJCE) : ISSN 2278-0661, ISBN: 2278-8727, pp 41-47 ,Volume 8, Issue 1 (Nov. - Dec. 2012).

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

[7]. L M Varalakshmi, Prithy R and Radhika Parameswari." Extended Visual Cryptography for Color Images and its PSNR Analysis",International Journal of Computer Applications:67(17):17-22, April 2013.
[8]. Andal devi k, ilamathi k and packialakshmi T,"A Visual Cryptography Scheme for Colour Images using Halftone Pattern", International Journal of Research in Engineering & Advanced Technology : ISSN: 2320 – 8791, Volume 2, Issue 2, Apr-May, 2014.
[9]. PoonamBidgar, NehaShahare ,"Secret Image Transmission through Image Sharing using Secret Key and LSB Embedding", International Journal of Electronics Communication and Computer Engineering Volume 5, Issue (4) July, Technovision-2014.
[10]. Young-Chang Hou, Zen-Yu Quan, and Hsin-Yin Liao, "New Designs for Friendly Visual Cryptography Scheme", International Journal of Information and Electronics Engineering, Vol. 5, No. 1, January 2015.
[11]. Sankar Das, Sandipan Chowdhury and Dibya Chakraborty,"Visual Cryptography using Three Independent Shares in Color Images", International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: 2349-2163 Issue 4, Volume 2 (April 2015).
[12]. Ritesh D.Yelane*, Dr. Nitiket. N. Mhala and Prof. B. J. Chilke,"Security Approach by Using Visual Cryptographic Technique", International Journal of Advanced Research in Computer Science and Software Engineering:ISSN: 2277 128X Volume 5, Issue 1, January 2015.
[13]. Jainthi.k, Prabhu.P ,"A novel cryptographic technique that emphasis visual quality and efficieny by floyd steinberg error diffusion method",International Journal of Research in Engineering and Technology, eISSN: 2319-1163 pISSN: 2321-7308,Volume: 04, Issue: 02 Feb-2015.
[14]. M.Karolin, Dr.T.Meyyapan,"RGB based secret sharing scheme in color visual cryptography",International Journal of Advanced Research in Computer and Communication Engineering, ISSN : 2278-1021,Vol. 4, Issue 7, July 2015.
[15]. Anuja R. Yeole*, Prof. Mahip, M. Bartere,"A X-or base image encryption and data security through higher lsb data hiding approach: a review", International Journal Of Engineering Sciences & Research Technology, ISSN: 2277-9655, February, 2016.

BIOGRAPHY

Er. Rimsy Dua is a student of M.Tech.(Computer Science) at Ganpati Institute of Technology and Management, Bilaspur, Yamunanagar, Haryana, India, affiliated to Kurukshetra University, Kurukshetra. She completed her Bachelor of Engineering (B.E) in 2014 from Ganpati Institute of Technology and Management, Bilaspur, Yamunanagar, Haryana, India, affiliated to Kurukshetra University, Kurukshetra and is pursuing Master of Technology (M.Tech.) in Computer Science from Ganpati Institute of Technology and Management, Bilaspur, Yamunanagar, Haryana, India, affiliated to Kurukshetra University, Kurukshetra .Her research interests are Security(Visual Cryptography,Graphical Password Authentication),Software Testing,Intelligent computing etc.