VISUAL CRYPTOGRAPHY - MULTILEVEL PROTECTION SCHEME FOR VISULATION OF NETWORK SECURITY PROTECTION

Ms.Monali P.Umbrekar Mr.Nandkishor O.Kadu

Abstract- **Visual Cryptography is a technique, which is used to concel the secret image into transparencies(which will vary with the user) and these transparencies are distributed to the intended recipients. In Extended Visual Cryptography Scheme, the transparencies are embedded into the meaningful images so that the intended recipient will have a transparency, which is a meaningful image. Without much computation, only the qualified set of participants can reveal the secret image by simple stacking transparencies. The tool can be used in both ways, to encrypt the secret image into transparencies and also to decrypt the embedded images. Simple steps and operations perform encryption and decryption of images. Halftone algorithm is used to divide the secret image into transparencies with the help of dither matrix. Dither matrix stores the information of all pixels in the secret image. Using this tool, user can send encrypted image that are in the format of GIF and PNG. The encrypted transprencies cn be saved in the mchine and can be sent to the intended person by other means. Experimental results reveal that the tool works with gray – scale image in the format of.png and.gif**

A)BACKGROUND AND RATIONALE :--

I) Visual Cryptography Scheme For Secret Hiding.

ii)Halftone Visual Cryptography Via Error Diffusion.

iii)Sharing Multiple Secrets Using Visual Cryptography.

iv)An Extended Visual Cryptography Algorithm For General Access Structure.

v)Embedded Extended Visual Cryptography.

B) OBJECTIVES

C) IMPLEMENTATION OF EVCS MECHANISM

i)Halftone technique using dither matrix

ii) Halftone process for each pixel

iii)Embedding Process

iv) The Embedding Process

D) SYSTEM DESIGN :--

Visual Cryptography is a general encryption techniques to hide information in images ina such a way that it can be decrypted by the human vision if the correct key image is used. The technique was proposed by Naor and Shamir in 1994. Visual Cryptography uses two tranparent images. One image contain random pixels and the other image contains the secret information. It is impossible to retrieve the secret information from one of the images. Both transparent images or layers are required to reveal the information.

KEYWORDS :--Visual Cryptography, Pixels-Encryption, Contrast Secret Images, Secret Sharing.

I. INTRODUCTION

Cryptography is the science of information security. The main objective of Cryptography is information hiding.

Cryptography probably began in or around 2000 BC in EGYPT, where hierographics were used to decorate the tombs of decreased rulers and kings

A Wax is a tablet made of wood and covered with a layer of wax. It was used as a reusable and portable writing surface in the 1400BC.

The first known use of a modern cipher was introduced by Julius Coesar (100BC to 44BC), who did not trust his messangers when communicating with his governers.

Failure is success if we learn from it. Idloxoh Iv Vxffhvv li zh ohcug iurp lw.

For proving secure communication in terms of exchange of information many different methods such as Visual Cryptography, Stagnography have been developed. Sometime it is not enough to keep the message secret, it may also require to confidentiality and authenticity of the message. To keep information secure, two different approaches are used congaing cryptography and steganography. Cryptography methods try to encrypt information such that one cannot original information but in stenography the aim is to deny the existence of a secret message. In Stagnography, a text or message is hidden through a media file(eg.Picture* such that no one can guess that this file contains any other type of this file contains any other type of information. Stagnography is the art of hiding information such that hackers do not suspicious to decrypt or investigate the file. Therefore Cryptography is not the best solution for secure communication, it is only part of the solution.The performance of Stangnography can be enhanced by combining it with Visual Cryptography.

Visual Cryptography is new type of cryptographic scheme, which can decode canceled images without any cryptographic computations. The scheme is perfectly secure and very easy to implement.

Visual Cryptography is the art of encrypting information such as handwritten text, images etc. in such way that the decryption is possible without any mathematical computations and human visual system is sufficient to decrypt the information. The cryptography scheme is given by the following setup. A secret images consists of a collection of black and white pixels. Here each pixels is treated independently. To encode the secret image, we spilt the original image into a modified version (refer as shares)such that each pixel in a share new subdivided into n black and n white sub-pixels. To decode the image, a subset S of those n shares are picked and copied on separate transprencies.

First form of Visual Cryptography is also known as secret sharing. The simplest form of visual cryptography seprates a secret into two parts so that either par by itself conveys no information. When these two parts are combined together by means of superimposition, the original secret can be revaled. These parts are called as shares.

There are several advantages of Visual Cryptography. It is simple to use and no mathematical computations are required to reveal the secret. Secondly, the individuals who do not have knowledge of Cryptography are indirectly getting involved in decryption. The major drawback of this secheme is that visually blind people cannot make use of this technique.

A secure and an efficient communication of confidential and sensitive information is the initial concern in communication and network storage system. It is also important for any data not to be tamper. Now a days much multimedia information is transmitted in large amount over internet. Especially while using images, secrecy is a major challenge. Because of this advancement in the network application securing image become wide area to keep attention.

Visual Cryptography is a cryptographic technique which allows visual information (Pictures, Text, etc.) to be encrypted in such a way that decryption becomes the job of the person to decrypt via sight reading. One of the best –known technique has been credited to Moni Naor and Adi Shamir, who developed in 1994. They demsonstrate visual secret sharing scheme, where an image was broken up into n shares so that only someone with all n shares could decrypt the image, while any n-1 shares revealed no information about the original image. Each share was printed on a separate transparency, and decryption was performed by overlapping the shares. When all n-shares were overlaid, the original image would appear. There are several generation at the basic scheme including k-out of-n visual cryptography.

Using similar idea, transparency can be used to implement a one-time-pad encryption, where one transparency is a shared random pad, and another transparency acts as the expansion of space requirement in visual cryptography. The efficiency of visual cryptography can be increased to 100%. Visual Cryptography can be used to protect biometric templates in which decryption does not require any complex computations

RELATED WORK –

A)K out of K Visual Cryptography :--

Original secret is divided into K-number of shares and for reconstruction of the secret all K shares are necessary. It is not so popular because managing K numbers of shares, all K shares is difficult task and it also increase time complexity to compute shares.

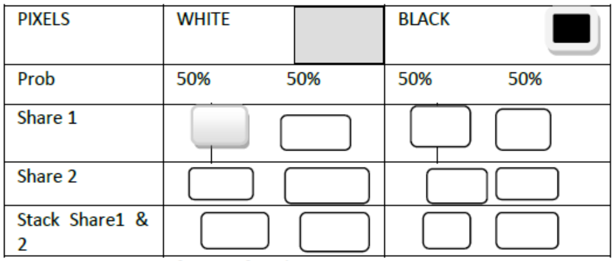
B)K out of N Visual Cryptography :--

In this scheme allows dividing a secret into a K number of shares. The secret can be revaled from any N number of shares among K. Major problem associated with scheme is that the user needs to maintain many shares which may result into loss of shares. More number of shares means more memory consumption.

The application of this scheme is found with banking system. For Joint accounts, three shares are generated. One is kept with bank's server, second is delivered to the one customer for the joint account and third share is delivered to the second customer. Hence, therefore both customers are able to access the account.

A) 2 out of 2 Visual Cryptography Scheme :--

The secret image is divided into two shares. This is simplest kind of visual cryptography. The major application of this scheme is found with remote voting system that uses 2 out of 2 secret sharing scheme for authentication purpose. To reveal the original image, these two shares are required to stacked together. Fig.(1) represents the division of black and white pixels in this scheme as follows.



PIXELS	WHITE		BLACK	
Prob	50%	50%	50%	50%
Share 1				
Share 2				
Stack Share1 & 2				

Fig. 1 Basic concept of 2 out of 2 scheme.

Following fig.2 Visual Cryptography example we create two shares (Share 1 and Share 2) of Secret Message "WIKIPEDIA". For getting back original secret message we overlapped this two shares.

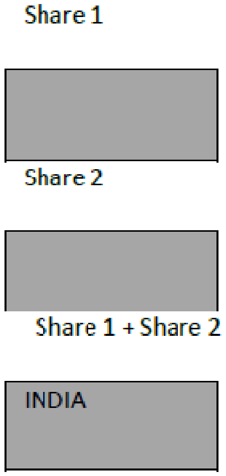


Fig.2 Visual Cryptography Example

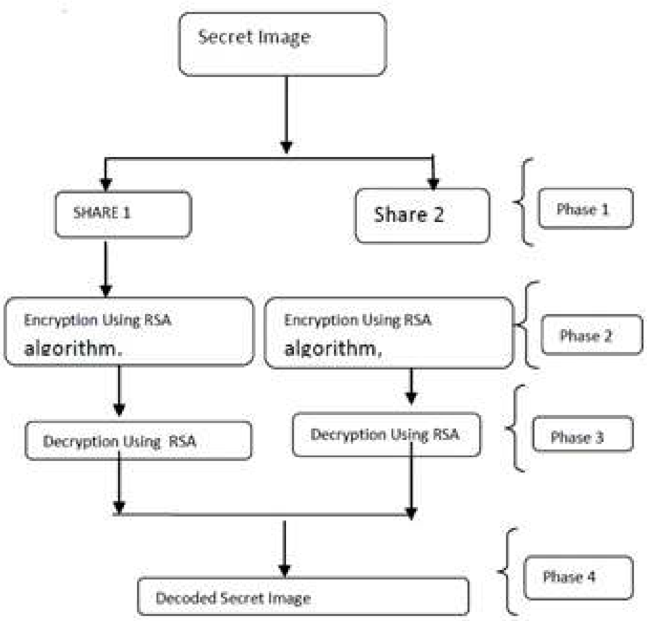
ADVANTAGES OF VISUAL CRYPTOGRAPHY APPLICATIONS ARE :-

1)Simple to implement
2)Encryptions don't require any NP- Hard problem dependency.
3) Description algorithm is not needed. Human vision is enough to decrypt the secret image. So that a person without any Cryptographic.
4) Knowledge can decrypt the image.
5) We can send Cipher text that through Fax or E-mail.
6) Infinite computations power can't predict the message.

EXISTING SYSTEM :--

The existing scheme generates the VC shares using basic Visual Cryptography model and then encrypt both shares. Using RSA algorithm of public key cryptography. So that the secret shares will be more secure and shares are more protected from the malicious users who may later the bit sequence to create the fake shares. During the decryption phase, secret shares are extracted by RSA decryption algorithm and stacked to reveal the secret image. Existing methodology is shown in Fig.3

Fig.3 Existing System Methodology



LIMITATIONS OF EXISTING SYSTEM :-

Existing scheme have the following limitations.
i)Existing scheme is only valid for binary images.
ii)Encrypted

PROPOSED SYSTEM :--

The proposed system consists of 6 modules.
1) Image Conversion
2) Share Generation
3)Blowfish
4) Encryption
5) Decryption
6) Visual Cryptography Decryption

1)Image conversion :--

A color input image is the input image. Input image is divided into three channel images namely red channel, green channel, alpha channel, And on each of the channel images half toning is applied.

A halftone image is made up of a series of dots rather than a continuous tone. These dots can be different sizes, different colors, and rarely even different shapes. Larger dots are used to represent darker, more dense areas of the image, and smaller dots are used for lighter areas. Color half toning generates a halftone pattern for each of these links. When these patterns are printed over each other, the human viewer will observe a color that depends on the amount of the color links.

2) Share Generation :--

Steps for share generation processor :--
1)Consider the input secret image as the RGB model color image.
2)The input image is now fed to the error diffiusion process that uses Floyed – Steinberg algorithm to diffuse the image.
3)Repeat step 2 until every pixel in the image is decomposed. The standard sixteen named color codes.
4)According to the traditional method for Naor and Shamir's black and white VC schemes, expand each pixel into 2*2 blocks arrays.
5)This step results in generation of two shares(transparencies) of the secret image.
6)Finally, the stacked image is produced by combining the two shares that are generated .

3)Blowfish :-- Bruce Schneier designed Blowfish in 1993 as a fast, free different to existing encryption algorithm. Since it has been analyze considerably, and it is slowly fast acceptance as a strong encryption algorithm. Blowfish algorithm has many advantages. It is suitable and efficient for hardware implementation and no authorization is required.

Blowfish algorithm include table lookup, addition and XOR. Blowfish is a cipher based on fiestel rounds, and the plan of the F – function used amounts to a generalization of the principle used in DES to provide the same security with greater speed and efficiency in software.

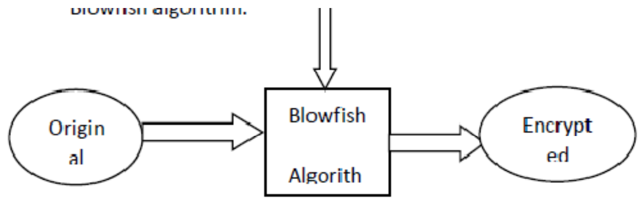
Blowfish is a 64- bit block cipher and is optional as a alternate for DES. Blowfish is a fast and free algorithm and can encrypt data on 32-bit microprocessor. Implementation of blowfish algorithm which is strongest and fastest in data processing store evaluate to other algorithm. Blowfish algorithm is really secured because it has longer key length 32 to 448 bit (more no .of key size)

Algorithm	Created By	Key Size	Block Size
Blowfish	Bruce Schneier 1993	32 – 448 bit	64 bit

Steps in the Algorithm :--
1)Input the input secret image as the RGB model color image.
2)Input to the original image.
3)Create the key value having 32 – 448 bits.
4)Encrypt the image using Blowfish algorithm.

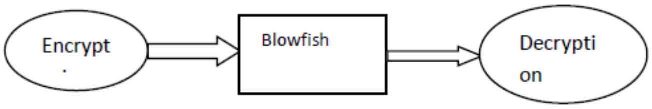
5)Decrypt the encrypted image using the same key.
6)End.

4)Encryption Process :--
Original image and encryption key are input to the encryption process. The bit stream of the original image is separated into blocks length of Blowfish algorithm.

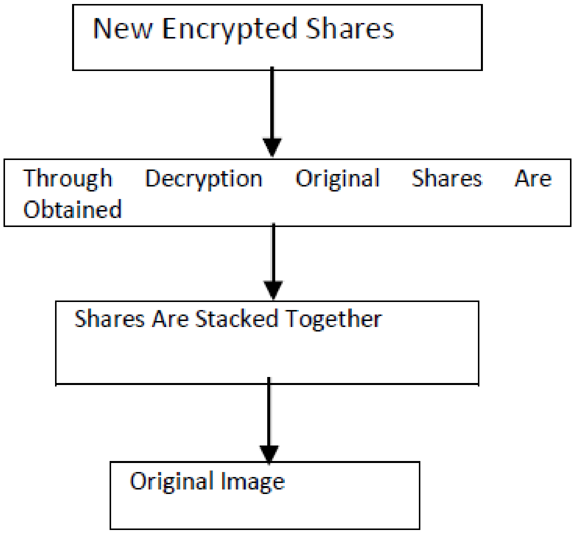


Share decryption requires the same key that is used to encrypt the share. Share decryption also uses the same algorithm which is used for share encryption is given as the inputs.

5)Decryption Process :--
The encrypted image is divided into the same block length of blowfish algorithm top of bottom. The blocks are subjected to decryption function. The same encryption key is used to decrypt the image by reversing the function of sub keys is reversed.



Visual Cryptographic decryption will be performed. We can decrypt the original image by applying binary XOR operation on both decrypted shares of each channel image and finally concatenate all these to obtain the original image.The methodology of the proposed system is shown in the fig.4.1 & fig 4.2


New Encrypted Shares
Through Decryption Original Shares Are Obtained
Shares Are Stacked Together
Original Image

Share decryption requires the same key is used to encrypt the share. Share decryption also uses the same algorithm which is used for share encryption except that the encrypted share is given as the input.

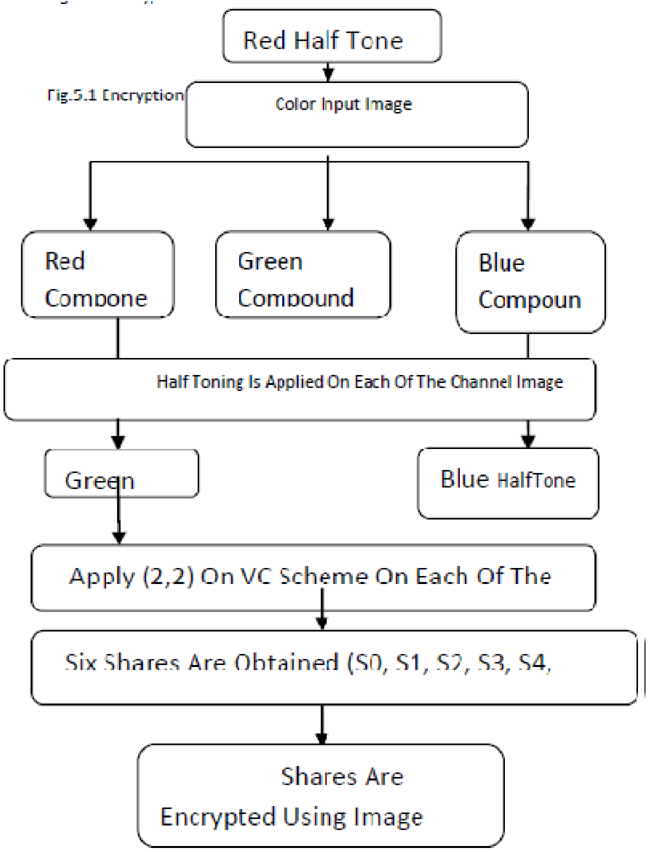


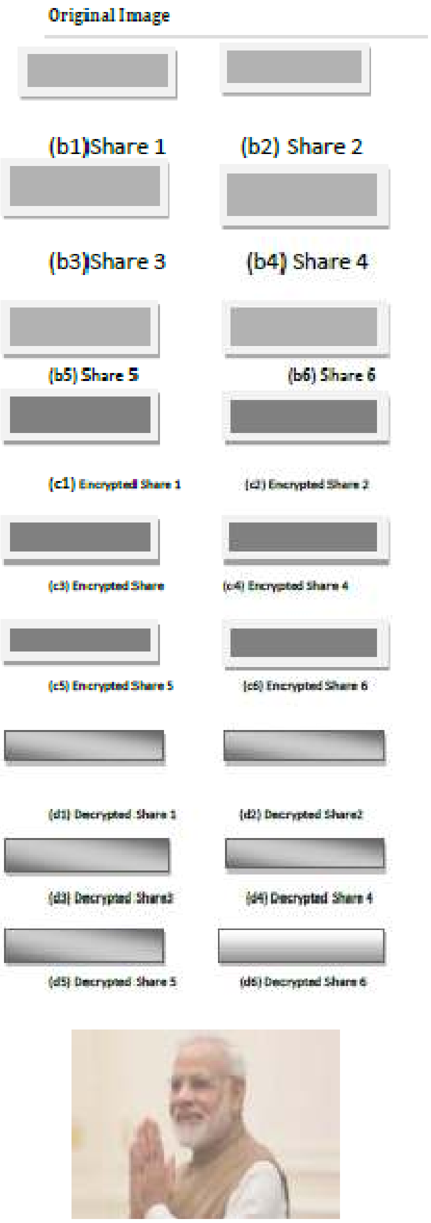
Fig.5.1 Encryption
Red Half Tone
Color Input Image
Red Compone
Green Compound
Blue Compoun
Half Toning Is Applied On Each Of The Channel Image
Green
Blue HalfTone
Apply (2,2) On VC Scheme On Each Of The
Six Shares Are Obtained (S0, S1, S2, S3, S4,
Shares Are Encrypted Using Image

Evaluation of Results :--
This scheme has been implemented in METLAB – 7 (R 2010 a). To run this scheme minimum hardware configuration is required with no extra specifications. The experiments have been run in Windows 8.
To test the performance of this scheme number of experiments has been conducted with varying image sizes, types but every time secret color image is retrieved and the time taken to encrypt the shares is less than that of existing system.
Results of same experiments are shown in the following figures.
Results of proposed scheme - Color Image
Chart – 1. Shows the size of decrypted images for the existing and proposed scheme.
14

Acknowledgement :-
Our first and sincere appreciation goes to Dr.A.D.Gawand (Prof.& HOD - EXTC Dept.), Dr.A.P.Thakare (Prof.-EXTC Dept.), Dr.N.N.Kasat(Prof.- EXTC Dept.), Dr.P.D.Gawande(Prof.EXTCDept.),&Mrs.Manisha Gawande(Kitukle)- Asst.Prof.EXTC Dept.),for all that we have learned from them and for their continuous help and support in all stages of the work. We would also thanks for the technical support.

REFERENCES

1.M.Naor and A.Shamir, "Visual Cryptography", Proceedings of Advances in Cryptography: Eurocrypt94, Lecture notes in Computer science, Vol.950, pp.1 -12, 1995.
2.Shankar. K., and P. Eswaran, " A secure visual secret share (VSS) creation scheme is visual cryptography using elliptic curve cryptography with optimization technique". Australian Journal of Basic & Applied Science 9.36(2015): 150 -163.
3.Shankar. K, and P. Eswaran, "Sharing a secret image with encapsulated shares in visual cryptography". Procedia Computer Science 70(2015): 462-468.
4.Shankar.K., and P.Eswaran, "RGB- Based Secure Share Creatiion in Visual Cryptography Using Optimal Elliptic Curve Cryptography Technique". Journal of Circuits, Systems and Computers 25.11(2016): 1650138.
5.L.N.Pandey and Neeraj Shukla, " Visual Cryptography Schemes using Compressed Random Shares", in International Journalof Advance Research in Computer Science and Management Studies, Volume 1, Issue 4, September 2013, pp:62-66.
6. Shankar.K., and P.Eswaran, " RGB Based multiple visual cryptography with aid of elliptic curve cryptography". China Communication 14.2(2017): 118-130.
.Kulvinder Kaur, Vineetha Khemchandani, , "Securing Visual Cryptographic shares using Public Key Encryption". 3rd International Advance Computing Conference, 2013.
8.Young –Chang Hou., "Visual Cryptography for color image, Pattern Recognition, 36:1619-1629, August 2002.
9.Manika Sharma, Rekha Saraswat, "Secure Visual Cryptography Technique for Color Images Using RSA Algorithm, International Journal of Engineering and Innovative Technology, Volume 2, Issue 10, April 2013.
10.InKoo Kang, Member , IEEE Gonzalo R.Arce, Fellow, IEEE, and Heung-Kyu Lee, Member, IEEE, "Color Extended Visual Cryptography Using Error Diffusion", IEEE Transactions on image processing, Vol.20, no.1, January 2011.
11.Nakajima M. and Yamaguchi.Y.," Extended Visual Cryptography for Natural Images, WSCG02(2002),303-310.
12.R.Verheul and H.C.A.Van Tilorg," Constructions and properities of k out of n visual secret schemes, Designs, Codes and Cryptography, Vol.11, No.2(1997)pp 179-196.
13.Y.C.Hou, " Visual Cryptography for color Images", Pattern Recognit., Vol.36, No.7, pp.1619-1629, 2003.
14.T.Hofmeister, M.Krause, and H.U.Simon, " Contrast optimal k out of n secret sharing scheme in visual cryptography, " Theory of Computer Science, Vol.240, No.2, pp. 471 -485, June.



(e) Retrived IMAGE

Fig – 6.1 :Results of proposed sche

THE COMPARISONS OF THE EXISTING AND PROPOSED WORK AS SHOWN IN THE Table 1

Algorithm	Complexity	Security	No.of Share Generation	Image Relieved if color image is given as input
Naor & Shamir (Basic 2*2	Medium	Increase	2	Binary
Kour & Khemc Handanils Scheme	More Complex	Increase	2	Binary
Proposed	Medium	Increase	6	Color Halftone

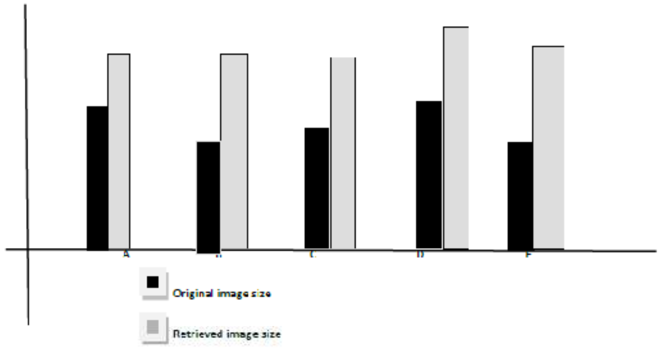


Chart – 1 . Comparison based size of decrypted images.

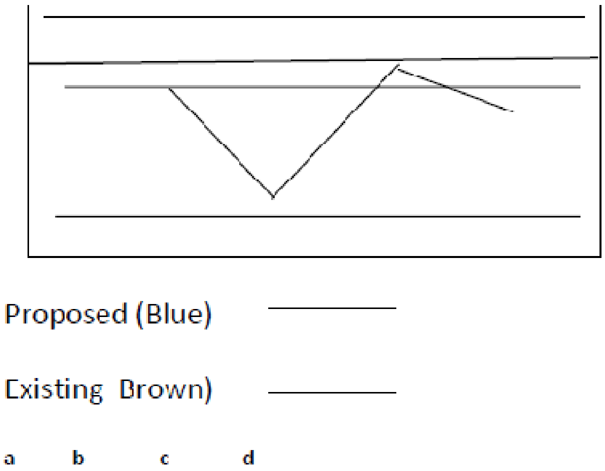


Fig.6.2 Comparasion based on entropy value

CONCLUSION :--

An effective method for field of Visual – Cryptography. In my work visual cryptography shares are again encrypted using encryption algorithm for proving the double security of secret document. Existing schemes are valid only to binary and gray – level images. But in my work when a color image is given as input, the retrieved images was color halftone image.

ADVANTAGES :--

1)Color images are retrieved.
2)Complexity is less.
3)Double Security.

FUTURE WORK :--

It has been observed that there are many possible enhancement and extensions exists as the visual quality and size of revealed image. The major areas of future scope are :
1)Indore to improve the quality of decrypted images, inverse halftonecan be applied.
2)Size of Images.

ACKNOWLEDGEMENT :--

First of all I am very much thankful to Shree.Jadishbhau M.Gupta,
President – SIPNA SHIKSHAN PRASARAK MANDAL and Dr.Gajanan P.Dhok – Officiating Principal, SIPNA College of Engg.& Tech., AMRAVATI for encouraging us and providing all the necessary infrastructure and
facilities. Our first and sincere appreciation goes to Dr.A.D.Gawand (Prof.& HOD -
EXTC Dept.), Dr.A.P.Thakare (Prof.-EXTC Dept.), Dr.N.N.Kasat(Prof.- EXTC Dept.),Dr.P.D.Gawande(Prof.EXTCDept.),&Mrs.Manisha Gawande(Kitukle)- Asst.Prof.EXTC Dept.),for all that we have learned from them and for their continuous help and support in all stages of the work. We would also thanks for the technical support.

REFERENCES

1)M.Naor and A.Shamir, “Visual Cryptography”, Proceedings of Advances in Cryptography: Eurocrypt94, Lecture notes in Computer science, Vol.950, pp.1 -12, 1995.
2)Shankar. K., and P. Eswaran, “ A secure visual secret share (VSS) creation scheme is visual cryptography using elliptic curve cryptography with optimization technique”. Australian Journal of Basic & Applied Science 9.36(2015): 150 -163.
3)Shankar. K, and P. Eswaran, “Sharing a secret image with encapsulated shares in visual cryptography”. Procedia Computer Science 70(2015): 462-468.
4)Shankar.K., and P.Eswaran, “RGB- Based Secure Share Creatiion in Visual Cryptography Using Optimal Elliptic Curve Cryptography Technique”. Journal of Circuits, Systems and Computers 25.11(2016): 1650138.
4)L.N.Pandey and Neeraj Shukla, “ Visual Cryptography Schemes using Compressed Random Shares”, in International Journalof Advance Research in Computer Science and Management Studies, Volume 1, Issue 4, September 2013, pp:62-66.
5) Shankar.K., and P.Eswaran, “ RGB Based multiple visual cryptography with aid of elliptic curve cryptography”. China Communication 14.2(2017): 118-130.
6)Kulvinder Kaur, Vineetha Khemchandani, , “Securing Visual Cryptographic shares using Public Key Encryption”. 3rd International Advance Computing Conference, 2013.
7)Young –Chang Hou., “Visual Cryptography for color image, Pattern Recognition, 36:1619-1629, August 2002.
8)Manika Sharma, Rekha Saraswat, “Secure Visual Cryptography Technique for Color Images Using RSA Algorithm, International Journal of
Engineering and Innovative Technology, Volume 2, Issue 10, April 2013.
9)InKoo Kang, Member , IEEE Gonzalo R.Arce, Fellow, IEEE, and Heung- Kyu Lee, Member, IEEE, “Color Extended Visual Cryptography Using Error Diffusion”, IEEE Transactions on image processing, Vol.20, no.1, January 2011.

10)Nakajima M. and Yamaguchi.Y.," Extended Visual Cryptography for Natural Images, WSCG02(2002),303-310.

11)R.Verheul and H.C.A.Van Tilorg," Constructions and properities of k out of n visual secret schemes, Designs, Codes and Cryptography, Vol.11, No.2(1997)pp 179-196.

12)Y.C.Hou, " Visual Cryptography for color Images", Pattern Recognit., Vol.36, No.7, pp.1619-1629, 2003.

13)T.Hofmeister, M.Krause, and H.U.Simon, " Contrast optimal k out of n secret sharing scheme in visual cryptography, " Theory of Computer
Science, Vol.240, No.2, pp. 471 -485, June.2000