International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 05 | May-2016 www.irjet.net p-ISSN: 2395-0072

An Enhance Color Visual Cryptography Scheme

Miss Arpana jaiswal
M.Tech Scholar
C.V.R.U.

Mr. Praveen Chouksey
Asst.Professor(se)
C.V.R.U.

Abstract

Visual Cryptography is one of the important encryption techniques to hide the secret image into two or more images which are called shares. The shares are very safe because separately they reveal nothing about the secret image. The original secret image can be obtained by simply stacking all the shares together without any complex computation involved. Visual Cryptography has made the security of information easier and better than other cryptography techniques used in secret writing.

Keywords: Color Visual Cryptography, Data hiding, Encryption, Decryption

I. INTRODUCTION

In this Digital world internet is the strongest medium to exchange and transmit digital document and data. Internet is an environment through which we can easily distribute, duplicate and modify digital information. Security must be provided to the image during its transmission over the internet because of hackers. That's why security becomes an important thing for today networking. For security of image we have an important technology which is called Visual Cryptography.

Visual cryptography is a secure, easy, simple and effective cryptographic technique used for secret image sharing. Secret image sharing is the important subject in the field of communication techniques, information security and production. However we can provide security in many other ways like transmitting with password, image hiding, watermarking technique, authentication and identification. But the main drawback of these methods is that the secret images can be protected in single information carrier.

The method of protecting confidential information by hackers is called cryptography It uses mathematical computation to encrypt secret information and then to decrypt the encrypted one it uses secret key for this. That's why we can also use the cryptography to encrypt the images but it has two disadvantages:

1. The traditional cryptosystems requires a lot of time to encrypt the image data because of image size is much greater than of text.
2. Also, the decrypted text must be equal to the original text, but the decrypted image should not necessarily be equal to the original image because of the characteristics of human perception.

To overcome this problem, Visual cryptography scheme for secret sharing was introduced by Naor and shamir[3] In 1994, Moni Naor and Adi Shamir [3] combined the two mechanisms : secret sharing and traditional cryptography. They introduced a new concept named Visual Cryptography for the encryption and decryption of printed materials such as images or text.

In this scheme the secret image is split up into number of shares and transmits to the number of participants. In Visual cryptography, visual information (Image, text, etc) gets encrypted in such a way that the decryption can be performed by the simply human vision without any computer operation [1].

II. Different Visual Cryptography Scheme

A). Extended Visual Cryptographic Scheme Using Back Propagation Network [2].

EVC Scheme by J. Ida Christy and Dr. V. Seenivasagam In 2012, Using Back Propagation Network. In EVC scheme two cover images and one secret image taken as inputs of systems. The size should be same of this three images. After the process of encoding two shares are produced as outputs, these shares are treated as two cover images. The output image must be same in size as a input image. the secret information hidden on this output images. We can get the secret image iff shares are stacked together.

Steps=

1st resized the images to half of their size and transformed in color halftone images.

2nd useful pixels are extracted.

3rd secret image is encrypted into two shares.

4th after stacking this share we got the original image this process called decryption

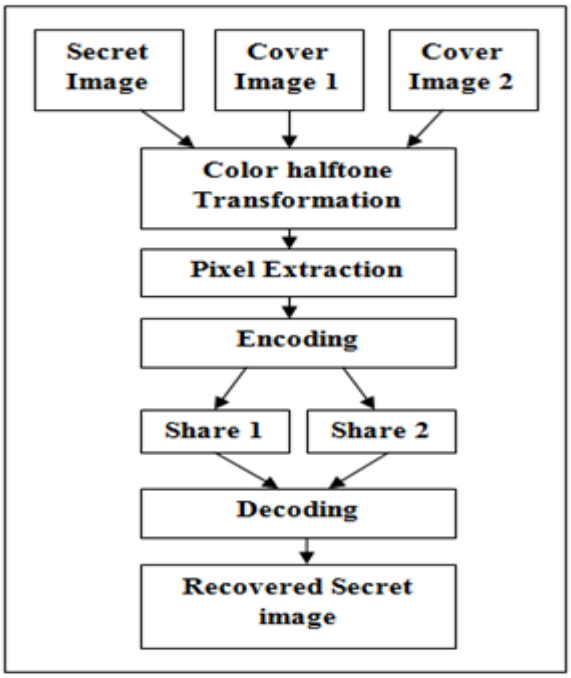


Fig 1.4: working process of EVC

B).VCS by Cover Image share embedded security algorithm (CISESA) [3].

This Visual Cryptography system proposed by Himanshu Sharma, Neeraj Kumar In 2011, they used Cover Image share embedded security algorithm.

This system has following three steps for the encryption and decryption-

STEPS 1: 1st steps started by the basic VCS. Here we are using any visual cryptography model which can be operating on binary images. In this method the original image I is transformed in halftone image S by Half toning method such as ordered dithering, error diffusion [4],[5]. After that shares Sa and Sb are generated by the binary image.

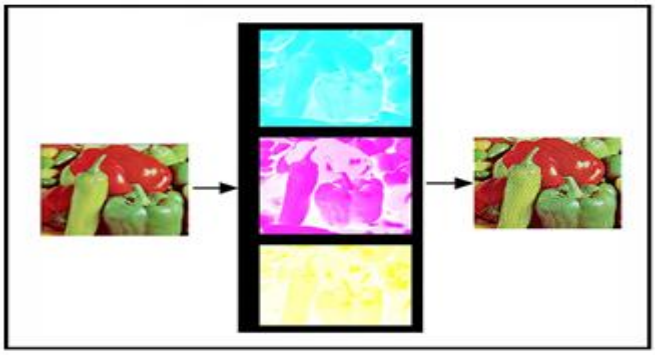


Fig 1.5. Color Halftone Transformation

STEP 2: Second step of the algorithm must be used to generate the embedded images with the help of cover image. here we will taking cover image as C and its complimented images as Ca and Cb. Then four embedded images Zaa, Zab, Zba, Zbb generated and transmitted to the destination through transmission channel.

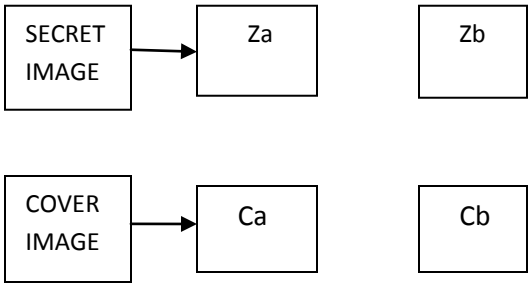


Fig 1.6. Procedure

Zaa= EMBEDDED(Sa,Ca)

Zab= EMBEDDED(Sa,Cb)

Zba= EMBEDDED(Sb,Ca)

Zbb= EMBEDDED(Sb,Cb)

STEP 3: Watermarking is a method of providing the extra security on basic VCS, extra security provided by the compliments of cover image in which the shares can be embedded. The decoded image can be revealed by simply stacking all this 4 shares.

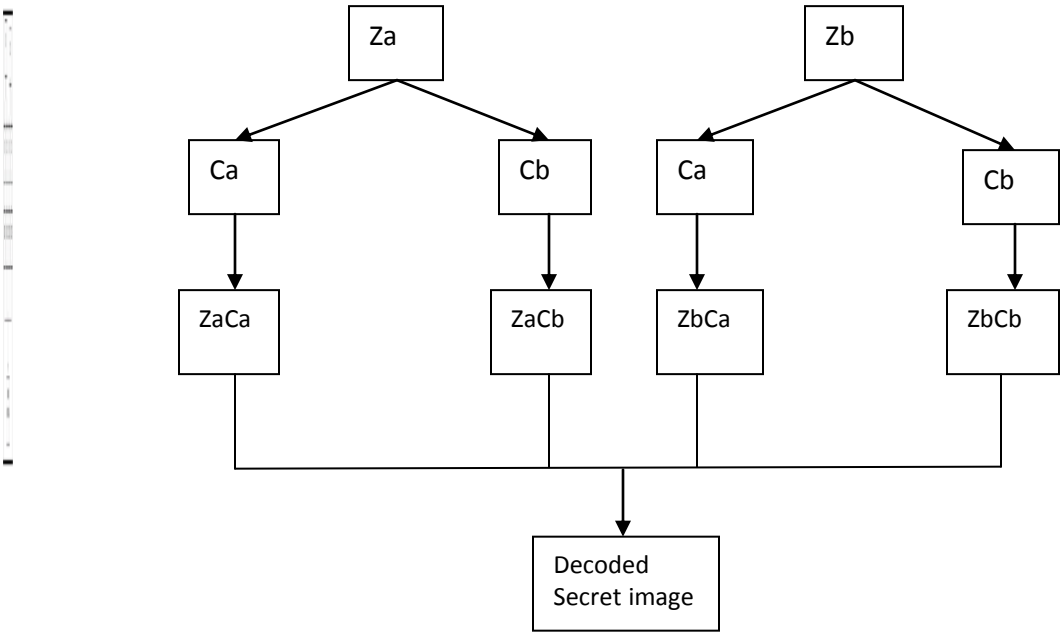


Fig. 1.6 (a) : Procedure

C). CAR (2, 2) (Constant Aspect Ratio) with Meaningful Shares (CARVCMS) [6].

In this scheme original secret information divide into exactly 2 shares. No one can reveal the secret information if they have only one shares. In this scheme one shares acts as a cipher text and other one act as secret key. Both the shares merged together to reconstructs the original image. In this the generated shares must be meaningful and the share's aspect ratio and should be identically dimensioned with the original secret image. This is the main advantages of this proposed system.

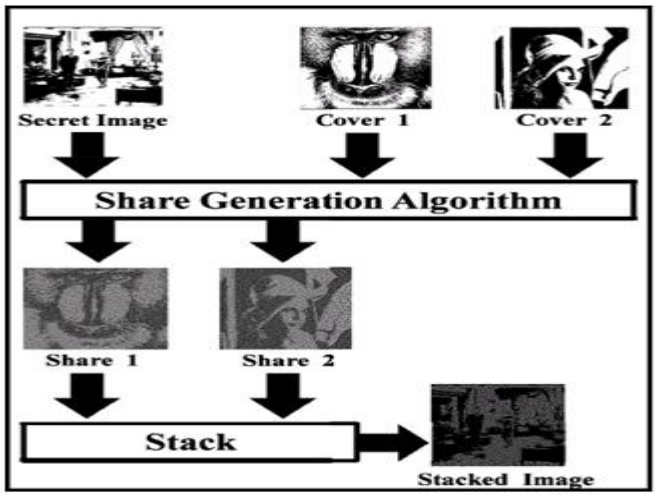


Fig 1.7: CARVCMS structure

D). Extended Visual Cryptography for Color Images Using Coding Tables [7].

This algorithm has 3 steps:

1) Image Transformation (by Color Halftone)

2) Encoding

3) Decoding

Image Transformation (by Color Halftone)
The sender takes Ca, Cb, Cc, Cd as four cover images and Si as secret input image. Size of all image is NxN pixels. All the five input image Ca, Cb, Cc, Cd and Si transformed into Ia, Ib, Ic, Id and Is (halftone images) of size NxN pixels . Images are extracted into RGB planes for this process. Now halftone technique is applied in this RGB planes. Now to get a color halftone image we must be combined these three halftone planes. Half toning is performed using error diffusion.

Encoding and Generation of Shares
In this step we use a 3 tables namely Key Table, Cover Table (CT) and Secret Table (ST)) for generating shares. In this method shares which are generated must be meaningfull.When the receiver stacks all the shares then only secret image is revealed.

Decryption
In decryption process stack out two or more shares with the Key Image to reconstruct the secret image. In the Figure 1.8 we saw Share1 and Share2 and one Key block. Here the block of the stacked image contains four pixels in which 2 sub pixels must be same in color and other 2 sub pixels must be black.

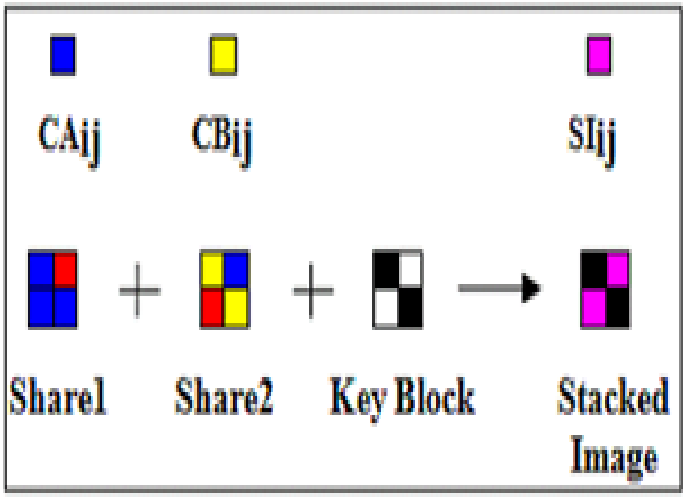


Fig 1.8:Decryption process

E). VCS Based on XOR Algorithm

The XOR algorithm and shift operations are the main operations of this visual cryptography scheme. The verifiable and modified (k, n, h, l, m)-VCS [9] result must be produced. where K is the minimal number of share images which is required to reveal the secret image; the total number of secret share images is n ;the share images must have m no of pixels; h is the number of white sub-pixels per pixel used in the share images=m-h, m>h>l0.

The recovery and judgment are very simple process on this scheme. There is no any pixel expansion on secret image and verifiable image both is very clear and identical. This scheme improves the function of anti-deception.

F). VCS with Public Key Encryption [10].

Public Key Cryptography is used to encrypt both shares through which the secret shares becomes more secure and shares are protected .In the decryption phase, RSA decryption algorithm is used to extract secret share & stacked this shares to reconstruct the secret image. Fig.1.9,shows all the four phases of this scheme:

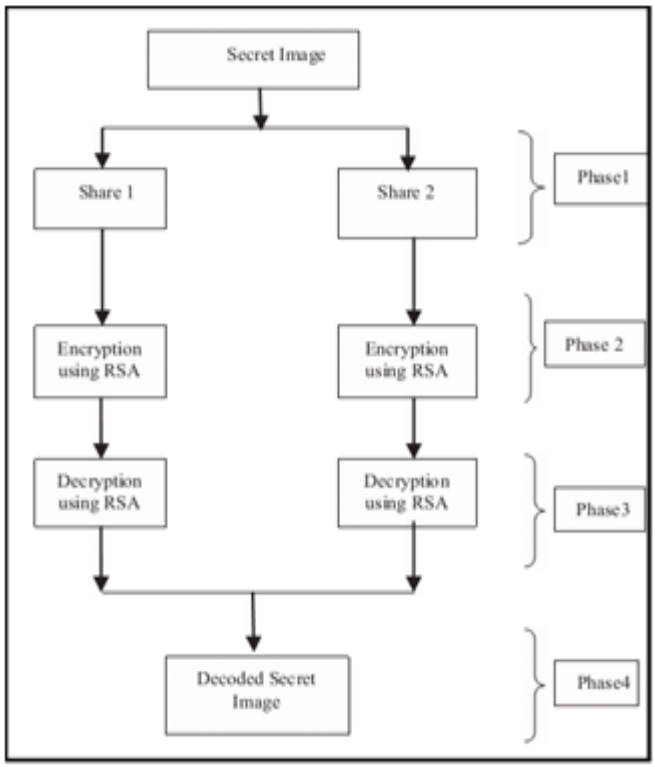


Fig 1.9:structure of this scheme

1)PHASE-1Share generation:

Here shares generated by using VCS (2, 2). Firstly secret image is transformed in a binary image then every pixels divided in 8 sub pixels, Fig. 1.9(a) explained how randomly 4 pixels are selected.

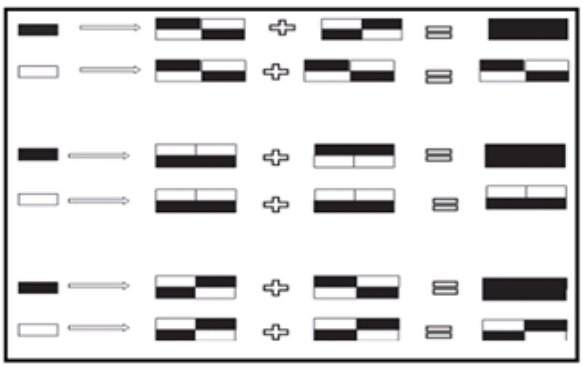


Fig 1.9(a): encoding

2) PHASE-2 Encryption:

Here we used RSA algorithm for encryption. For this should generated the key first for RSA and then after we can follow the encryption process. We got encrypted shares as result of this phase.

3) PHASE-3 Decryption using RSA:

In this phase decryption is done, for decryption RSA decryption algorithm is used to convert the encrypted shares in their actual form, the sender is responsible for this.

4) PHASE-4 Final decryption process :

Here VCS decryption performed. In which XOR is a main operation .Here we have decrypted shares which is generated on phase 3 now in this phase XOR operation performed on the shares to generate secret image back.

III Literature Survey

In the year 1995, MoniNaor and Adi Shamir [13] "Visual cryptography" proposed the basic model of visual cryptography. where a secret image divided into n shares through which those person are only capable to reveal the secret image that have all this n shares, while someone having n-1 shares can not reveal the secret image.

In (2,2) VCS scheme each secret image is divided into two shares and this two share must be needed to reconstruct the image, only one share cannot be used to reconstruct the image. Decryption process is very simple for this we just print Each share on transparencies, and after that we just stack this transparencies and the secret image can be revealed and can be easily visualized by the naked eye without any kind of complex computation [13].

The basic VCS model extended into a (k, n) VCS [13] to enhance the property, In (k, n) VCS, original image divided into n shares and distributed to the participants through transmission media. In the (k,n) VCS model where k is a minimum no of shares required to decrypt the secret image and n is the total number of shares obtained by the visual cryptographic scheme. It gives flexibility to user, if users lost some shares but they have atleast k shares they can be revealed the original image. all n shares in this scheme have equal importance to reconstruct the image.

In the year 1996, G. Ateniese , C. Blundo , A. DeSantis , and D. R. Stinson [14] "Visual Cryptography for general access structures" proposed extended (k, n) visual cryptography model to overcome the problem in basic (k, n) visual cryptography scheme .In general access structure scheme, as per the importance of shares, the given set of n shares is split into the two subsets as qualified and for bidden subset of shares.

In the year 1997, E. Verheuland H. V. Tilborg, [15] proposed color VCS. In this VCS one pixel distributed into m sub pixels then it is split into c color regions.
In the year 1998, C.C. Wu, L.H. Chen [16] proposed a VCS which shares two secret images in 2 shares. All the above scheme secretly convert only one secret image on shares but in this VCS two secret images can be transformed into two shares, namely S1 and S2.
In the year2002,Young-Chang Hou[17] "Visual cryptography for color images" proposed a Technique for color images visual cryptography which has three methods for visual cryptography of gray-level and color images based on past studies in black and white visual cryptography, the halftone technology method, and the color decomposition method. This technique provides backward comp ability with the old results.
In the year 2003, Z. Zhou, G.R Arce, and G. Di Crescenzo, [18] uses a reprographic technique which is half toning technique to generate shares. A halftone shares can be generated By using halftone cells with an appropriate size. Half toning technique is used to maintain good contrast, security and increases quality of the shares of secret image.
Chang-Chou Lin, Wen-Hsiang Tsai [19]. In this gray image transformed in binary image by es a dithering technique. Previous techniques are only suitable for binary images this techniques extend the features of previous VCS.
In the year 2003, Bert W. Leung, Felix Y. Ng [20]. Hou generated a four-share visual cryptography scheme. In this scheme secret image splits into four shares, the black mask and the other three shares. No one can reveal the secret information if they have not the black mask even they have all the other three shares.
In the year 2005, Jin, W. Q. Yan, and M. S. Kankanhalli [21] proposed a VCS scheme which is a extended method of basic (k,n) scheme there is no needed of at least k shares If have one or more share then we can starts the revealing of the secret image. Quality depends in the no of shares received.as many as shares received the quality of recovered image improves.
Wang, R.Z.[Ran-Zan], [22] generated a VCS for splitting multiple secret level in a single image.
In the year 2007, S. J. Shyu, S. Y. Huanga,Y. K. Lee, R. Z. Wang, andK. Chen [23] generated a visual cryptography scheme to share multiple secrets in visual cryptography, By the help of this scheme we can secured multiple secret image at the same time.
In basicVCS, shares are a noise because the random patterns. Hackers interested on this Noise-like shares because hacker may suspect that some data may be revealed by these noise-like images. Through which security issues obtained. And noise –like shares are not easy to manage bcs all shares looking same.
Nakajima, M. and Yamaguchi, Y., [**24**]. Proposed an extended visual cryptography (EVC) which creates meaningful shares rather than meaningless shares of basic VCS.
In the year 2008, F. Liu, C.K. Wu, X.J. Lin, [25] proposed a approach for colored VCS.
 In first approach, In the shares colors of the secret image can be printed directly. Working process is similar to the traditional visual cryptography model. The main disadvantages are large pixel expansion and low quality image (decoded ones).
 The second approach reduces pixel expansion but due to half toning techniques quality of image was disturbed. RGB components method is used. RGB for additive model & CYN for subtractive model. Then to every color channels black and white images are assigned of basic VCS
 In third approach, this approach ensures much better quality of image.

In the year 2008, Haibo Zhang, Visual Cryptography for General Access Structure Using Pixel-block Aware Encoding Multi-pixel In visual cryptography encoding is an emerging method for that more than on pixel can be encoded for each encoding run. Nevertheless, The encoding length is invariable that's why its encoding

efficiency is still low and very small for each run. This paper based on pixel-block aware encoding. In this the secret image must be scanned by zigzag and perceives a pixel block with as many pixels as possible. The proposed scheme has benefits in encoding efficiency over single pixel encoding and other known multi-pixel encoding methods.

In the year 2009,Abhishek Parakh and SubhashKak [25] "A Recursive Threshold Visual Cryptography Scheme developed a technique to overcome the limitation of (k, n) visual secret sharing scheme.

In the year 2011,I-Jen Lai and Wen-Hsiang Tsai[26] in this secret image is firstly split into tile images and then generating mosaic image. In this scheme randomly selects the Secret key. Without the key A hacker or un authorized person cannot retrieve the secret information.

In the year 2012,JagdeepVerma, Dr. Vineeta Khemchandani[27] this scheme merge all advantages of visual cryptography and Invisible watermarking techniques.

In the year 2014,Ya-Lin Lee and Wen -Hsiang Tsai [28] in this techniques meaningful mosaic image are generated with the same size and looking like a target image. The transformation process control by Secret key .The proposed method is extended by Lai and Tsai ,that introduced secret-fragment-visible mosaic image.

In the year 2014, Bharanivendhan N et al.[29] VCS with GAS Algorithm the previous approach suffers with security problems because at decoding side no complex computations is required you just stack all the share and secret image revealed. In this proposed system two phases are presented. 1st phase start with generation of the four meaningless shares. then 2nd phase started, in this cover images are embedded to each shares.

In the year 2015, Prof. Sujit Ahirrao1 , Tusharkumar Sakariya2, Abhijeet Bhokare3, [30]
In (k, n) visual cryptography scheme, original image divided into n shares and distributed to the participants through transmission media. In the (k,n) VCS model where k is a minimum no of shares required to decrypt the secret image and n is the total number of shares obtained by the visual cryptographic scheme. It gives flexibility to user, if users lost some shares but they have at least k shares they can be revealed the original image.

IV OBJECTIVES -

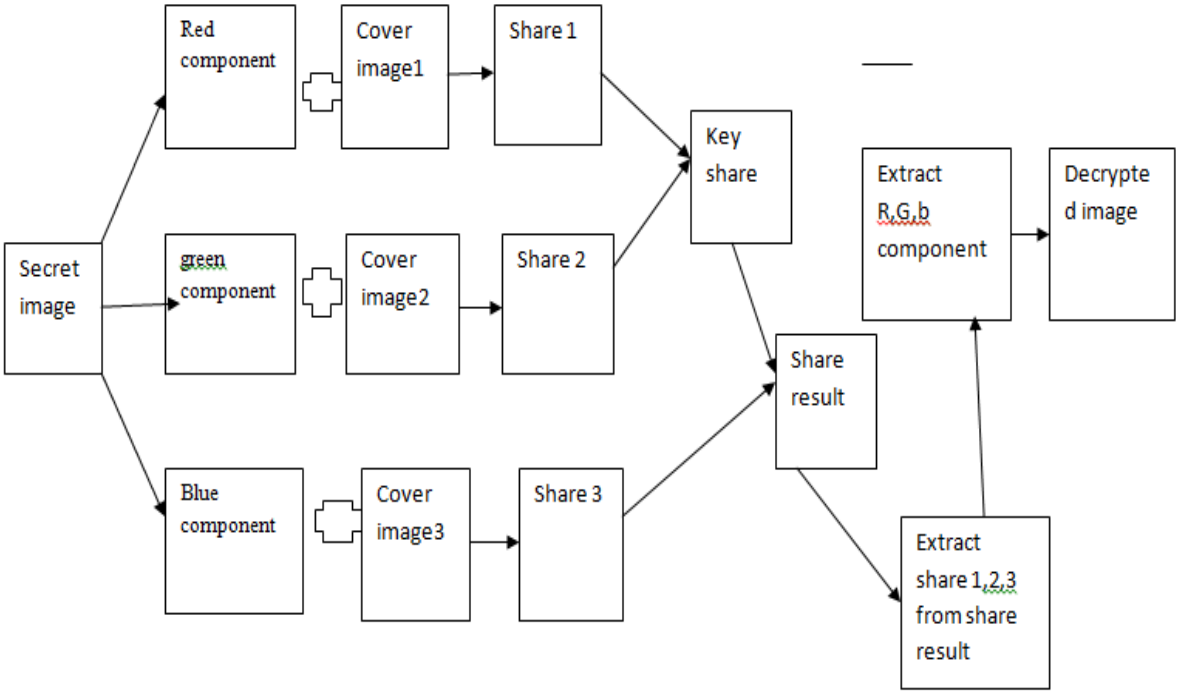
Objective of this project is to hide the original image information from an intruder or an unwanted user. For this the original image converted into the shares and shares will be transmitted to the authenticate receiver over the communication network, the receiver recalculate the secret image by the help of those shares when only they receive all the shares and this is called the decryption process.

Objective-1.To hide original image,2. To enhance the picture quality, 3. To reduce noise, 4. For security of image. Different types of losses occurs like: Color loss, Contrast loss, Noisy image, Pixel expansion

V PROBLEM STATEMENT-

In existing visual cryptography scheme, the sender will send their shares to the target receiver. The decoder will then stack over all the shares images to reconstruct the original image. Guarantee is a main issue presented here because the share can be hacked by hacker or can be lost during transmission. This is the problem statement of vcs system to address these kind of reliability problems, The decoder must be ensure whether the shared images brought to the target place are fake. Because of this, in our work, we proposed wavelet method to secure data. Other problem is that, in most of the proposed algorithms the decrypted

image quality is not good here we are trying to improve the quality of decrypted image. And here we are trying to provide the extra security to the systems.



BLOCK DIAGRAM OF WHOLE PROCESS

VI GUI OF IMPLEMENTATION

VII. METHODOLOGY

Algorithm:-

Step 1:- In this step we firstly input an image.
Step 2:- Then we load the image. Detect the loaded image successfully.
Step 3:- After this step we can start the encryption process.
Step 4:- For encryption we need to generate key.
Step 5:- Pattern key generated and adopted randomly.
Step 6:- At 0 level encryption input image should be divided into red, green and blue shares.
Step7:- At level 1 encryption R, G, B share images again would divided into 8 shares.
Step 8:- At level 2 every 8 shares again divided into 3 shares.
Step 9:- At level 3 the new three shares will be combined into one encrypted form R,G,B.
Step 10:- At level 4 R, G, B. share again combined and form single encrypted image

Decrypt

Step 1:- For decryption Firstly we input the decrypted image.
Step 2:- Then by following step we detect the encrypt input image.
Step 3:- After image loaded successfully we start decryption.
Step 4:- We need to generate a key for decryption process
Step 5:- At level 0 the encrypted image separated into R,G,B. share.
Step 6:- Decrypt the encrypted image of level 3 of encryption process.
Step7:- Decrypt the encrypted image of level 2 of encryption process.
Step 8:- Decrypt the encrypted image of level 1 of encryption process.
Step9:- Decrypt the encrypted image of level 0 of encryption process.

VIII. CONCLUSION:

Visual Cryptography is an exciting era of research where exists a lot of scope. Existing systems motivates us to improve the security of image for send over the network as well as secure sharing of key over the network. There is scope to automate the process of encryption for saving time and improve the quality of shares. Work can be done to improve quality of decrypted image at receiver side. Pixel expansion is problem in various existing systems. Work can be done in n pixel expansion problem. Some technique can be made to improve the quality of resultant image and also to reduce the power consumption.

In this we provided a detailed security visual cryptography algorithm for color image. The original secret image is color image and the adversary has acquired three of the R, G and B shares. Our results suggest that the security of the scheme depends critically on the color composition and distribution of the original secret image.

IX. REFERENCES

[1] M. Naor and A. Shamir, "Visual cryptography," Advances in Cry ptology - EUROCRYPT'94, pp. 1-12, 1995.
[2] J. Ida Christy and Dr. V. Seenivasagam, "Construction of Color Extended Visual Cryptographic Scheme Using Back Propagation Network for Color Images", 20 12 International Conference on Computing, Electronics and Electrical Technologies [IC CEET] 978- 1-4673 -02 1 0-41 1 2©20 12 IEEE.
[3] Himanshu Sharma , Neeraj Kumar, Govind Kumar Jha," Enhancement of security in Visual Cryptography system using Cover Image share embedded security algorithm (CISEA)", 978-1-4577-1386-611©2011 IEEE
[4] Zhongmin Wang and Gonzalo R. Arce, "Halftone visual cryptography through error diffusion", ISBN 1-4244-0481-9/06 © 2006 IEEE, pp.109-112.
[5] Digital Image Processing Laboratory: Image Halftoning" April 30, 2006. Purdue University.
[6] J. K. Mandal and Subhankar Ghatak, "Constant Aspect Ratio based (2, 2) Visual Cryptography through Meaningful Shares (CARVCMS)".
[7] Meera Kamath, Arpita Parab, "Extended Visual Cryptography for Color Images Using Coding Tables", 2012 International Conference on Communication, Information & Computing Technology (ICCICT), Oct. 19-20, Mumbai, India 978-1-4577-2078-9/12 ©2011 IEEE.
[8] Bin Yu, Xiaohui Xu, Liguo Fang, "Multi-secret sharing threshed visual cryptography," CIS Workshops 2007, Harbin, 2007: 815-818.
[9] Yanyan Han and Haocong Dong, "A Verifiable Visual Cryptography Scheme Based on XOR Algorithm", 978-1-4673-2101-3/12/$31.00 ©2012IEEE.
[10] Kulvinder Kaur and Vineeta Khemchandani "Securing Visual Cryptographic Shares using Public Key Encryption", 978-1-4673-4529-3/12/$31.00c 2012 IEEE.
[11] Shamir, A. 1979. How to Share a Secret. Communications of the ACM. 22: 612-613.
[12] Blakely, G. R. 1979. Safeguarding Cryptographic Keys. Proceedings of the National Computer Conference, American Federation of Information Processing Societies Proceedings. 48: 313-317.
[13] Moni Naor and Adi Shamir, "Visual cryptography". In Proceedings of Advances in Cryptology, EUROCRYPT 94, Lecture Notes in Computer Science, 1995, (950):pp. 1-12.
[14] G. Ateniese, C. Blundo, A. DeSantis, and D. R. Stinson, "Visual cryptography for general access structures", Proc.ICAL96,Springer, Berlin,1996,pp.416-428.

[15] E. Verheuland H. V. Tilborg, "Constructions And Properties Of K Out Of N Visual Secret Sharing Schemes."Designs, Codes and Cryptography, 11(2), pp.179–196, 1997.
[16] C.C. Wu, L.H. Chen, "A Study On Visual Cryptography", Master Thesis, Institute of Computer and Information Science, National Chiao Tung University, Taiwan, R.O.C., 1998.
[17] Young-ChangHou" Visual cryptography for color images" Pattern Recognition 36 (2002) .
[18] Z. Zhou, G. R Arce, and G. Di Crescenzo, "Halftone Visual Cryptography," in Proc. of IEEE International Conference on Image Processing, Barcelona, Spain,Sept 2003, vol. 1, pp. 521–52
[19] Chang-Chou Lin, Wen-Hsiang Tsai, "Visual cryptography for graylevel images by dithering techniques", Pattern Recognition Letters, v.24 n.1-3.
[20] Bert W. Leung, Felix Y. Ng, and Duncan S. Wong Bert W. Leung, Felix Y. Ng, and Duncan S. Wong . On the Security of a Visual Cryptography Scheme for Color images In Pattern Recognition, vol. 36, 2003, Hou proposed a four-share visual cryptography scheme for color images.
[21] . Jin, W. Q. Yan, and M. S. Kankanhalli, "Progressive color visual cryptography," J. Electron. Imag., vol. 14, no. 3, pp. 1–13, 2005.
[22] Wang, R.Z.[Ran-Zan], "Region Incrementing Visual Cryptography", SPLetters(16), No. 8, August 2009, pp. 659-662.
[23] S. J. Shyu, S. Y. Huanga,Y. K. Lee, R. Z. Wang, andK. Chen, "Sharing multiple secrets in visual cryptography", Pattern Recognition, Vol. 40, Issue 12, pp. 3633 - 3651, 2007.
[24] Nakajima, M. and Yamaguchi, Y., "Extended visual cryptography for natural images" Journal of WSCG. v10 i2. 303-310.
[25] F. Liu, C.K. Wu, X.J. Lin, "Colour Visual Cryptography Schemes", IET Information Security, vol. 2,No. 4, pp 151-165, 2008.
[26] I-Jen Lai and Wen-Hsiang Tsai "A Recursive Threshold Visual Cryptography Scheme", CoRR abs/0902.2487: (2009).
[27] Jagdeep Verma, Dr.Vineeta Khemchandani," A Visual Cryptographic Technique to Secure Image Shares", International Journal of Engineering Research and Applications (IJERA) Vol. 2, Issue 1,Jan-Feb 2012.
[28] Ya-Lin Lee and Wen-Hsiang Tsai," A New Secure Image Transmission Technique via Secret-Fragment-Visible Mosaic Images by Nearly Reversible Color Transformations", IEEE transaction on circuits and system for video technology, vol. 24, no. 4, April 2014.
[29] Bharanivendhan N " Visual Cryptography Schemes for Secret Image Sharing using GASAlgorithm" International Journal of Computer Applications (0975 – 8887) Volume 92 – No.8, April 2014.
[30] Prof. Sujit Ahirrao1, Tusharkumar Sakariya2, Abhijeet Bhokare3, VISUAL CRYPTOGRAPHY SCHEME FOR COLOR International Journal of Advanced Technology in Engineering and Science Volume No.03, Issue No. 02, February 2015,