Secret Sharing based Visual Cryptography Scheme for color preservation using RGB Color Space

Mr. Praveen Chouksey
M.Tech Scholar
LNCT JABALPUR
Department of Computer Science & Engineering
cvru111@gmail.com

Mr.Reetesh.Rai
professor
LNCT JABALPUR

Department of computer science & Engineering
reeteshrai16@gmail.com

Abstract—

Visual cryptography scheme is one of the most secure techniques for privacy protection, that allow the encryption of secret image or data by transferring it into the secure share and such a scheme is able to recover the secret image or data without any computation devices. In today's era security of that transmitted data is most important problem because network technology is greatly advanced and lot's of information is transmitted via the internet. Visual cryptography scheme allow encoding the original message to hide its meaning and decode it to reveal the original message. Also encoding of information in the number of shares and distributed to number of participants, which decrypt information without any cryptographic knowledge. The shares are sent through different communication channels from sender to receiver so that the probability of getting sufficient shares by the intruder minimized. But the shares may arise suspicion to the hacker's mind that passed information is secret. We can encrypt original image using a key to provide more security to this scheme. This makes visual
cryptography scheme a completely secure scheme. Visual cryptography scheme is a cryptographic technique which allows visual information (e.g. printed text, handwritten notes, and picture) to be encrypted in such a way that the decryption can be performed by the human visual system, without the aid of computers. There are various measures on which performance of visual cryptography scheme depends, such as pixel expansion, contrast, security, accuracy, computational complexity, share generated is meaningful or meaningless, type of secret images(either binary or color) and number of secret images(either single or multiple) encrypted by the scheme.

Keywords—
VisualCryptography,Encryption,Decryption,Shares,Extended Visual Cryptography

I. Introduction

Today, more and more digital documents are transmitted and exchanged on internet. It has created an environment that the digital information is easy to distribute, duplicate and modify. Image security becomes a very important issue for image transmission over the internet or wireless network. Visual Cryptography has made the security of information easier. Cryptography includes a set of techniques to achieve confidentiality when transmitting or storing data. Cryptography can be categorized into three different scheme s: symmetric cryptography, asymmetric cryptography and secret sharing. The traditional symmetric and asymmetric cryptography transform a given message to a random looking string of characters with the aid of a secret or public key. The resulting cipher text is supposed to reveal no information on plain text. The decryption of transforming the cipher text back to plain text is employed using the same or different secret key. In contrast to symmetric and asymmetric cryptography, secret sharing is based on the distribution of the secret information over several parties. Only if the required subset of parties put their information together the secret is revealed. The disadvantage of traditional symmetric and asymmetric cryptographic schemes is that they require complex operational steps for the encryption as well as for decryption of information. For average and inexperienced users, these schemes are rarely convenient to employ [2]. In 1994 Moni Naor and Adi Shamir [1] 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. The new scheme requires no complex mathematical operations but only the human visual system for the deciphering of a given printed material. The concept relies on transparencies which exhibit a white noise when each transparency is considered separately. The transparencies consist of randomly located white and black pixels. When stacking these transparencies together, the secret image is revealed. The decryption is executed by the human visual system and only the ownership of all transparencies can reveal the secret. The shares generated by the above method are meaningless and look like random dots. With such appearance, they make easy for the attackers to look into shares; whether or not the secrets can be easily cracked open, the looks of the meaningless shares are already revealing the existence of secrets to attackers. When the shares produced are meaningful images, then the attackers cannot find the secret image. A visual cryptography that reveals the target image by stacking meaningful images is Extended Visual Cryptography (EVC)[2] .

II. DIFFERENT VISUAL CRYPTOGRAPHY SCHEME

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

In 2012, J. Ida Christy and Dr. V. Seenivasagam Praposed Extended Visual Cryptographic Scheme Using Back Propagation Network. In these Scheme inputs taken for the proposed method are two cover images and one secret image. All the three images are of the same size. The outputs produced out of the encoding process are two shares that look like the two cover images. The secret image is hidden in the two shares. The size of the output images is also the same. When the two shares are overlapped, we get the secret image. There are four main steps in the proposed method. In the first step, the three images are resized to half of their size. Then the three images are transformed to color halftone images. In the second step some useful pixels are extracted. The third step is encoding where the secret image is encoded in the two shares. The last step is the decoding procedure where the secret image can be obtained by overlapping the two shares. The block diagram is shown in the Fig.1

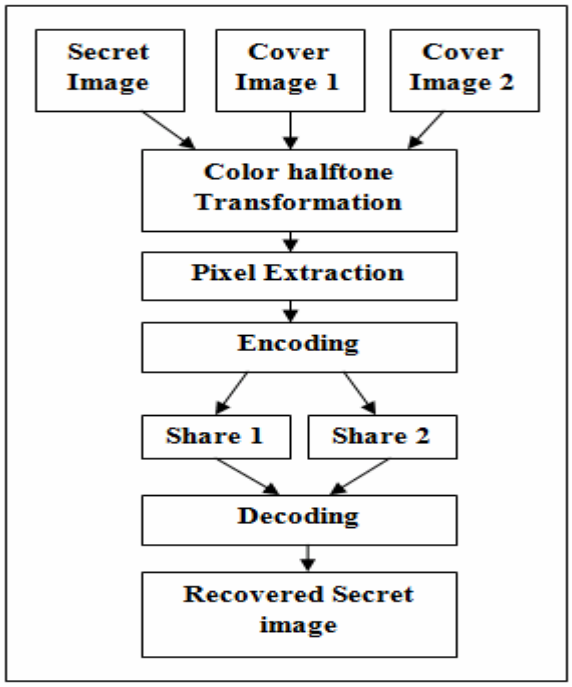


Fig 1. Block Diagram of Extended Visual Cryptography

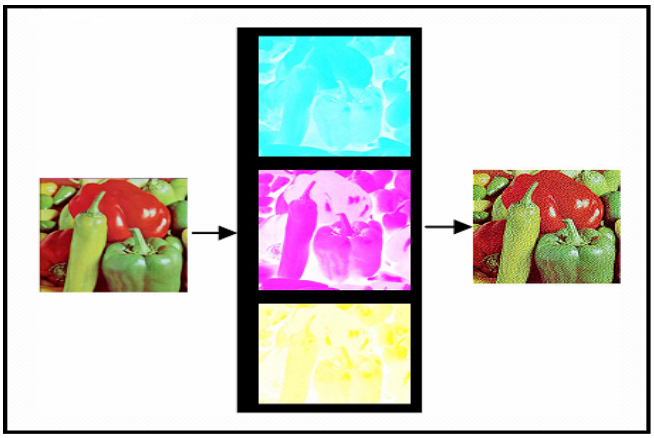


Fig 2. Color Halftone Transformation

B. *Visual Cryptography system using Cover Image share embedded security algorithm (CISEA) [3].*

In 2011,Himanshu Sharma, Neeraj Kumar proposed Visual Cryptography system using Cover Image share embedded security algorithm.
Following three phases of proposed algorithm:

PHASE 1: First phase of the algorithm is marked by the basic visual cryptography scheme. We will consider any visual cryptography model which may operate on binary images. So firstly consider the secret image I that is converted into the halftone image S by using any Halftoning technique such as ordered dithering, error diffusion [4],[5]. Later we will generate the shares S1 and S2 from the binary image. Each share is generated as a result of this phase is meaningless if we consider the share independently.

PHASE 2: Second phase is marked by the generation of embedded images with the help of compliment images of the cover image. Let the cover image be C and its complimented images are C1 and C2. Then four embedded images X11, X12, X21, X22 are generated which are to be transmitted to the destination through transmission channel. These shares can be generated by simply embedding the shares S1 and S2 over the compliments of cover image i.e. C1 and C2.

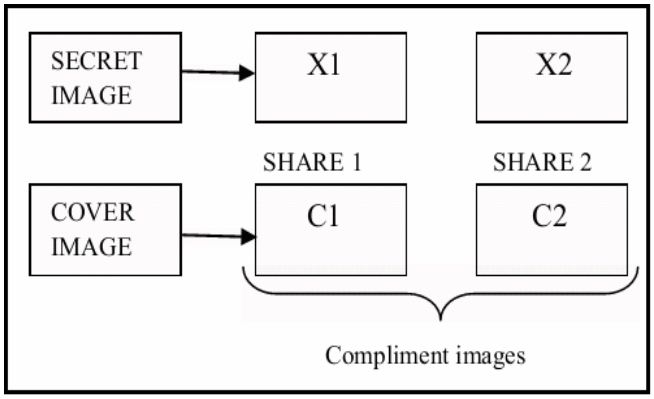


Fig 3. Proposed scheme structure

X11= EMBEDDED(S1,C1) X12= EMBEDDED(S1,C2)

X21= EMBEDDED(S2,C1) X22= EMBEDDED(S2,C2)

Watermarking scheme provide the additional security over basic visual cryptography scheme. Our proposed algorithm provides one more layer of security due to generation of compliments of cover image over which the shares can be embedded on it. The result of this phase is the new image having some information extract from cover image and some hidden information extract from secret image.

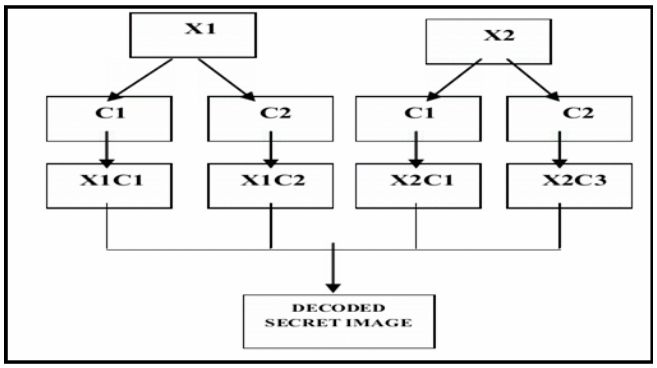


Fig. 4: Proposed scheme structure

C. Constant Aspect Ratio based (2, 2) Visual Cryptography through Meaningful Shares (CARVCMS) [6].

In this technique is a (2, 2) visual cryptographic scheme where secret will be revealed directly by stacking two meaningful shares in an arbitrary order but with proper alignment. According to the proposed algorithm, the generated shares are meaningful and the aspect ratio and the dimensions of the shares are identical with that of the secret image which ensure optimal space requirement. The main advantage of the proposed scheme is that the decrypted secret is identical with respect to the aspect ratio and image dimension of the source image.

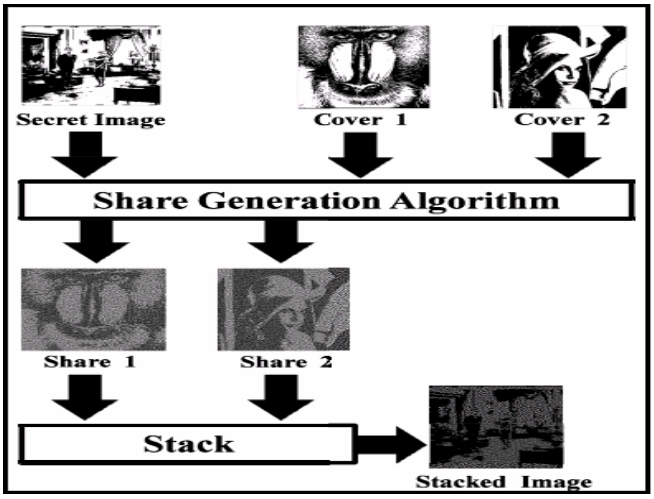


Figure 5: Schematic diagram of CARVCMS Algorithm

1) THE SHARE GENERATION ALGORITHM

Input: The secret image of size m× n and two cover Images of size m× n.

Output: Two meaningful shares of size m

Step 1. Repeat for each block of size 2 × 2 of secret image denoted by B_S and cover images denoted by C_{S1} and C_{S2} where all blocks are position wise identical.

Step 2. If B_S is a white block then C_{S1} and C_{S2} are replaced by any one of the combinations a along with their permutations.

Step 3. If B_S is a black block then C_{S1} and C_{S2} are replaced by any one of the combinations a permutation.

Step 4. Stop.

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

There are three steps in this algorithm:

1) Color Halftone Transformation
2) Encoding and Generation of Shares
3) Decryption

Each of these steps is explained in detail below:

1) Color Halftone Transformation

The sender inputs four cover images and one secret image CA, CB, CC, CD and SI respectively. Each image is of size NxN pixels. In this step the five color images CA, CB, CC, CD and SI are transformed into respective halftone images IA, IB, IC, ID and IS. The size of the halftoned images is also NxN pixels. Each input image is decomposed into three constituent planes red, green and blue. Then the halftone technique is applied to each of these planes. By combining these three halftoned planes, a color halftone image is

generated. Halftoning is performed using error diffusion. The error diffusion algorithm uses Jarvis filter.

2) Encoding and Generation of Shares

A Key Table and two types of Coding Tables—Cover Table (CT) and Secret Table (ST) are used to encode the secret image into the cover images. These encoded cover images are meaningful shares and can be transmitted securely. The sender has the option to select two (or more) of the four shares generated for transmission. The secret image is obtained when the receiver stacks the shares. The steps used in encoding are:

1) Key Generation
2) Cover Images Encoding
3) Secret Image Encoding
4) Generation Of Shares

3) Decryption

In the decryption process, we stack two or more shares along with the Key Image to reconstruct the secret image. Figure 6 shows an example of decryption with blocks from two shares, Share1 and Share2 and the corresponding block from the Key Image. The block of the stacked image produced contains two sub pixels of the same color as the pixel of the secret image and the other two sub pixels are black. Since two sub pixels out of four in each block will always be of the same color as the pixel of the secret image, 50% of the secret image is retained in the final reconstructed image.

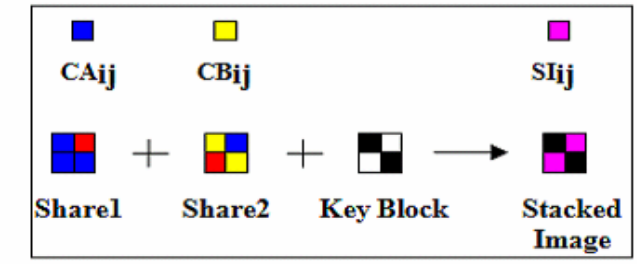


Fig 6.Example of Decryption

E. A Verifiable Visual Cryptography Scheme Based on XOR Algorithm [8].

The scheme in this paper is based on XOR algorithm and shift operations. The result produces a kind of verifiable and modified (k, n, h, l, m)-VCS [8]. K is the minimal number of share images, from which secret images can recover; n is the total number of secret share images; m is the number of pixels in a share images; his the number of used white sub-pixels per pixel in the share images=m-h, m>h>l0.

They proposed a verifiable visual cryptography scheme which based on XOR algorithm. Through using XOR algorithm with the share images of participates and the validation image, they can judge the share images are true or false without any other information to ensure the correctness of the secret image recovery. The process of recovery and judgment are both simple and the recovery of secret image and verifiable image are clear and without any pixel expansion. This scheme is able to indicate the correctness and truth of one single share image and improve the function of anti-deception.

F. Securing Visual Cryptographic Shares using Public Key Encryption [10].

The proposed 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 protected from the malicious adversaries who may alter the bit sequences to create the fake shares. During the decryption phase, secret shares are extracted by RSA decryption algorithm & stacked to reveal the secret image. As shown in Fig. 7, complete scheme is divided into following four phases:

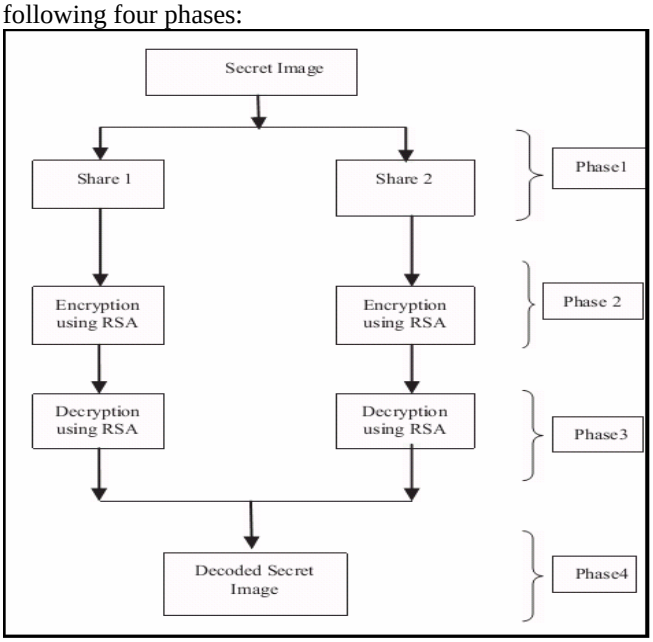


Fig.7 Methodology of the Proposed Scheme

1) PHASE-1 Generating shares of secret image:

In this phase Visual Cryptography Encryption is implemented. It consists of generation of shares from secret image using VC (2, 2) scheme. The secret image is first converted into a binary image then each pixel in the secret image is broken into 8 sub pixels, 4 pixels in each share by selecting the random pixel encoding scheme out of three given in Fig. 8.

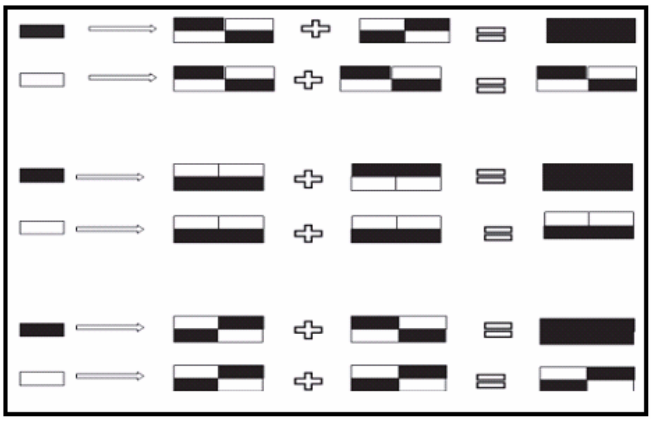


Fig. 8. Pixel encoding schemes

2) PHASE-2 Encrypting the generated Shares:
This is the second phase of our approach which will encrypt shares generated from the first phase. We have used RSA for encryption in this step. First we have generated the key for RSA and then performed the encryption. Results of this phase are encrypted shares.

3) PHASE-3 Decrypting the Shares using RSA:
This process takes place at the destination of the document/image/text. We again convert the encrypted shares in their actual form using RSA decryption algorithm, which were encrypted at the sender end.

4) PHASE-4 Visual Cryptographic decryption:
In this phase Visual Cryptographic decryption is performed. We have decrypted the original secret image by applying the binary XOR operation on both decrypted shares.

III. LITERATURE SURVEY

In the year 2010, Monisha Sharma[35], "Image encryption techniques using chaotic schemes: a review" have presented a technique using chaotic schemes for data hiding. Their techniques basically provide security functions as well as visual check, which might be applicable in some applications.To deal with the technical challenges, the two major image security technologies are under use: (a) Image encryption techniques to provide end-to-end security when distributing digital content over a variety of distributions systems, and (b) Watermarking techniques as a tool to achieve copyright protection, ownership trace, and authentication. They have done the current research efforts in image encryption techniques based on chaotic schemes are discussed.

In the year 2011, I-Jen Lai and Wen-Hsiang Tsai[26] "Secret-Fragment-Visible Mosaic Image–A New Computer Art and Its Application to Information Hiding" have presented a technique of information hiding which consist of secret image is first divided into rectangular shaped small fragments(tile images) and then for creating mosaic image they are fix to its next target image selected from a database. Secret key selects randomly some blocks of mosaic images to embed the information of tile image.A hacker without the key cannot retrieve the secret information as the key can reconstruct the secret image by retrieving the embedded information.

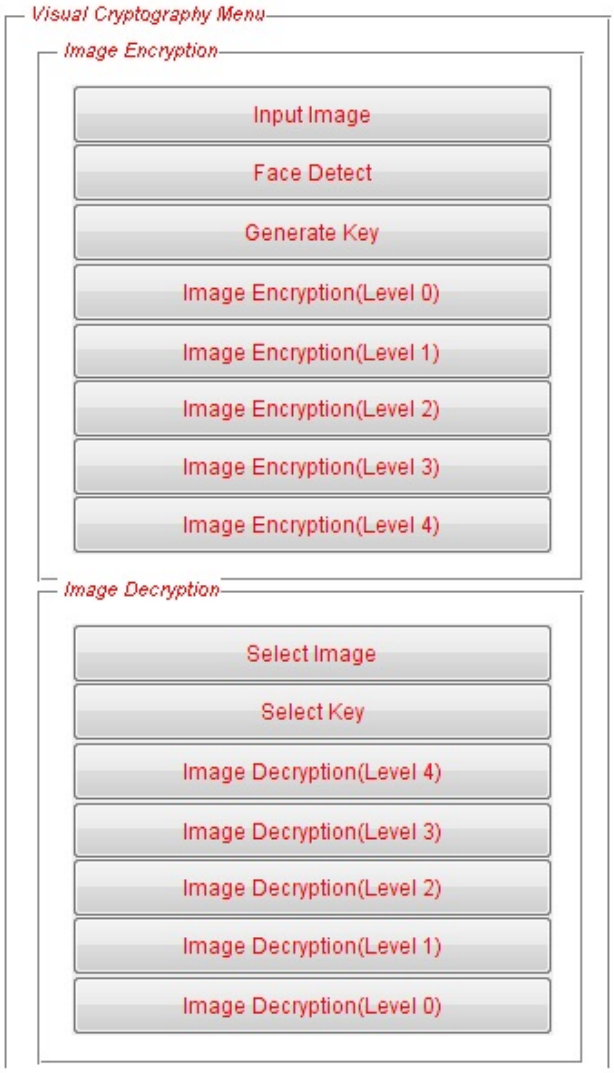
In the year 2012, Jagdeep Verma, Dr.Vineeta Khemchandani [37] "A Visual Cryptographic Technique to Secure Image Shares" proposed scheme will add the merits of both visual cryptography as well as Invisible and Blind watermarking techniques, where they will generate the secret shares using basic visual cryptography model and then they will watermark these shares into some host image using invisible and blind watermarking. The decryption is done by stacking of the shares after the secret shares have been extracted by a simple watermark extraction method. The proposed watermarking scheme do not need the original image or any of its characteristics for the extraction of watermark, and hence the proposed scheme is blind.

In the year 2013, Anuprita U. Mande and Manish N. Tibdewa[38] " Parameter Evaluation and Review of Various Error-Diffusion Half toning algorithms used in Color Visual Cryptography" have presented a technique for data hiding used in color video cryptography. They introduced an error diffusion technique for generating halftone shares which are more pleasant to human eyes. From the review of Color visual cryptography schemes, it is seen that half toning of images is achieved by various methods in different schemes. In this paper, they will take a review of all these methods. At the same time they will compare all these methods and

will adopt the one which will give us the best result with respect to color visual cryptography.

In the year 2014, Ya-Lin Lee and Wen-Hsiang Tsai [39] “A New Secure Image Transmission Technique via Secret-Fragment-Visible Mosaic Images by Nearly Reversible Color Transformations” have proposed a new scheme for secure image transmission which converts a secret image into a meaningful mosaic image with the same size and looking like a preselected target image. Secret key controls transformation process and that secret image is only recover by that key without any loss from mosaic image. The proposed method is extended by Lai and Tsai , in which a new type of computer art image, called secret-fragment-visible mosaic image, was introduced. The mosaic image is the output of rearrangement of the fragments of a secret image in disguise of another image called the target image preselected from a database.

GUI OF IMPLEMENTATION



METHODOLOGY

Algorithm of proposed methodology:-

Below are the steps used in our proposed maethod:

Step 1:- First we input an image.

Step 2:- Then we detect the input image by following

Then we load the image.

Detect the loaded image successfully.

Step 3:- After image loaded successfully we start encryption.

Step 4:- For encryption we need to generate key.

Step 5:- Pattern key genereated and adopted randomly.

Step 6:- At 0 level encryption input image would divided into three shares red, green and blue.

Step7:- At level 1 encryption every share images (i.e. R,G,B) again would divided into 8 shares.

Step 8:- At level 2 every 8 divided shares (i.e. R,G,B) again would divided into 3 shares.

Step 9:- At level 3 the new three shares combined into one encrypted form red ,green and blue.

Step 10:- At level 4 red share,green share and blue share again combined and form single encrypted image.

Decrypt

Step 1:- First we need to input the decrypted image for decryption.

Step 2:- Then we detect the encrypt input image by following:

Then we load the image.

Detect the loaded image successfully.

Step 3:- After image loaded successfully we start decryption.

Step 4:- For decryption we need to generate key

Step 5:- At level 0 the encrypted image created at level 4 of encryption process separated into red share, green share and blue 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.

IV. RESULT ANALYSIS

V. CONCLUSION

Visual Cryptography is an exciting era of research where exists a lot of scope.There exists various scope of enhancement in visual cryptography system. Our future work is to develop quantitative analysis of this algorithm in the terms of quality, contrast, reliability and clarity of the final decoded secret image that is directly decrypted by human visual system without using any decryption algorithm .So that human save money and time .One more enhanced this algorithm is also possible with our visual cryptography system make compatible with color images.

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] Tzung-Her Chen, Kai-Hsiang Tsao, and Kuo-Chen Wei, “Multiple-Image Encryption By Rotating Random Grids”, Eighth International Conference on Intelligent Systems Design and Applications, pp. 252-256 , 2008.

[12]Tzung-Her Chen, Kai-Hsiang Tsao, and Kuo-Chen Wei, “Multi-Secrets Visual Secret Sharing”, Proceedings of APCC2008, IEICE, 2008.

[13] E. Verheul and 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.

[14] C. Yang and C. Laih, “New Colored Visual Secret Sharing Schemes”, Designs, Codes and cryptography, 20, pp. 325–335, 2000.

[15] C. Chang, C. Tsai, and T. Chen. “A New Scheme For Sharing Secret Color Images In Computer Network”, Proceedings of International Conference on Parallel and Distributed Systems, pp. 21–27,July 2000.

[16] Chin-Chen Chang , Tai-Xing Yu , “Sharing A Secret Gray Image In Multiple Images”, Proceedings of the First International Symposium on Cyber Worlds (CW.02), 2002.

[17] R.Youmaran, A. Adler, A. Miri , “An Improved Visual Cryptography Scheme For Secret Hiding”, 23rd Biennial Symposium on Communications, pp. 340-343,2006.

[18] S.J. Shyu, “Efficient Visual Secret Sharing Scheme For Color Images”, Pattern Recognition 39 (5) ,pp. 866– 880, 2006.

[19] Du-Shiau Tsai, Gwoboa Horng, Tzung-Her Chen, Yao-TeHuang, “ANovel Secret Image Sharing Scheme For True-Color Images With

Size Constraint", Information Sciences 179 3247–3254 Elsevier, 2009.

[20] F. Liu, C.K. Wu, X.J. Lin , "Color Visual Cryptography Schemes" 2008.

[21] Zhengxin Fu, Bin Yu "Research on Rotation Visual Cryptography Scheme" International Symposium on Information Engineering and Electronic Commerce, 2009.

[22] Pallavi Vijay Chavan, R.S. Mangrulkar "Encrypting Informative Color Image using Color Visual Cryptography", Third International Conference on Emerging Trends in Engineering and Technology, 978-0-7695-4246-1/10 $26.00 © 2010 IEEE DOI 10.1109/ICETET.2010.94

[23] Roberto De Prisco and Alfredo De Santis, "Using Colors to Improve Visual Cryptography for Black and White Images," ICITS 2011, LNCS 6673, pp. 182-201, 2011.

[24] Gopi Krishnan S I, Loganathan D., "Color Image Cryptography Scheme Based on Visual Cryptography" Proceedings of 2011 International Conference on Signal Processing, Communication, Computing and Networking Technologies (ICSCCN 2011).

[25] Meera Kamath, Arpita Parab, Aarti Salyankar, Surekha Dholay, "Extended Visual Cryptography for Color Images Using Coding Tables" International Conference on Communication, Information & Computing Technology (ICCICT), Oct. 19-20, 2012.

[26] Chun-Yuan Hsiao, Hao-Ji Wang, "Enhancing Image Quality in Visual Cryptography with Colors", 2012 IEEE, International Conference on Information Security and Intelligence Control (ISIC), Page(s): 103 – 106, 2012.

[27] Yuanfeng Liu, Zhongmin Wang; "Halftone Visual Cryptography With Color Shares", International Conference on Granular Computing (GrC), pp. 746-749, IEEE, 2012.

[28] Shyong Jian Shyu, Hung-Wei Jiang; "General Constructions for Threshold Multiple-Secret Visual Cryptographic Schemes" IEEE Transactions on Information Forensics and Security, Volume: 8 , Issue: 5,pp: 733 – 743, 2013.

[29] Young-Chang Hou, Shih-Chieh Wei, and Chia-Yin Lin; "Random-grid-based Visual Cryptography Schemes" IEEE Transactions on Circuits and Systems for Video Technology, Issue: 99, 2013.

[30] Shyong Jian Shyu,"Visual Cryptograms of Random Grids for General Access Structures" IEEE Transactions on Circuits and Systems for Video Technology, Volume: 23 , Issue: 3 pp: 414 – 424, 2013.