International Journal of Advance Engineering and Research Development
Scientific Journal of Impact Factor (SJIF): 4.72
Special Issue SIEICON-2017,April -2017
e-ISSN : 2348-4470 p-ISSN : 2348-6406

A systematic review on visual cryptography system for security of image

Shivam Upadhyay[1],Shrikant Lade[2],Ritesh Yadav[3],Sheshang Degadwala[4]
[1]*M.tech Student,CSE,RKDFIST,Bhopal*
[2]*Head of Department,CSE,RKDFIST,Bhopal*
[3]*Asst.Prof. CSE, RKDFIST,Bhopal*
[4]*Asst.Prof,CSE,SigmaInstituteofEngineering,Vadodara*

ABSTRACT-- *Visual Cryptography is a secure and unique image encryption technique which protects image based secret. In visual cryptography image is encrypted into shares and in decryption process all or some of shares are super imposed with each other to decrypt the original secret image. In this technique no complex computation is needed for decryption of secret image which is the best advantage of Visual Cryptography Scheme. In this survey paper in this proposed system (N, N) VCS is used for encryption.*

KEYWORD: *visual cryptography,Shares,Encryption*

I. INTRODUCTION

Visual cryptography is a cryptographic method which permits visual data (pictures, content and so on) to be encrypted in a manner that decryption turns into the employment of the individual to decrypt by means of sight perusing. One of the best-known systems has been credited to MoniNaor and Adi Shamir, who created it in 1994. They showed a visual secret sharing scheme, where a picture was separated into n imparts so that exclusive somebody to all n shares could decrypt the picture, while any n − 1 offers uncovered no data about the original picture. Every share was imprinted on a different straightforwardness, and decryption was performed by overlaying the shares. At the point when all n shares were overlaid, theoriginal picture would show up. Visual cryptography is an extraordinary sort of picture encryption system, in which picture is encrypted into shares utilizing simple XOR operation.

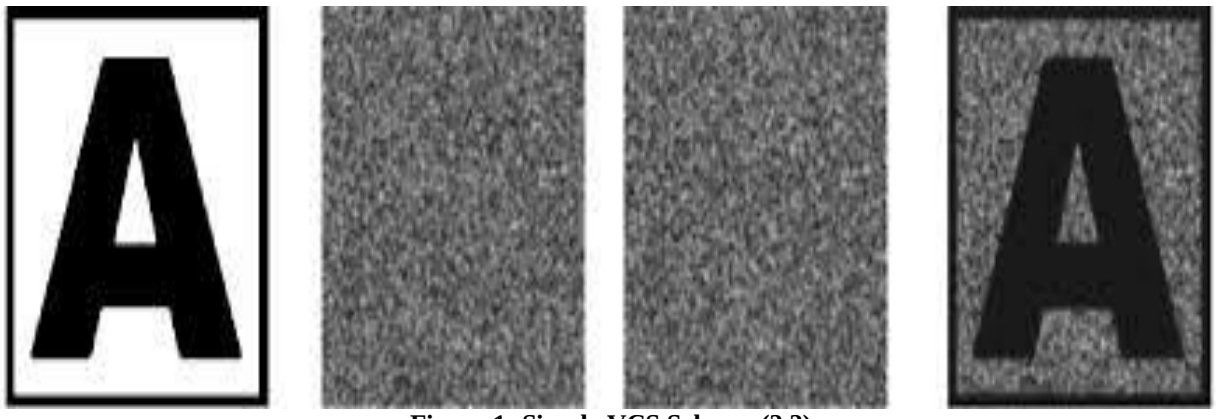

Figure 1: Simple VCS Scheme (2,2)

Visual cryptography is a picture encryption system, which conceal the picture based secret. The huge favorable position of visual cryptography is that it doesn't require any unpredictable calculation for decryption of secret however it is just performed by human eyes. In this day and age information security is essential in light of the fact that a large portion of our information is gone over web. Numerous strategies have been proposed and produced for security of our information. Secret information will be as content, picture, sound, and video and so on. Here we concentrates on security of picture based secret. Visual cryptography assumes a critical part for picture security. In this procedure picture is encoded into number of shares and at decoding side all or a portion of the shares are covered with each other to uncover the secret picture. Distinctive sorts of visual cryptography methods have been investigated which is customary visual cryptography, halftone visual cryptography, general get to structure based visual cryptography, square based dynamic visual cryptography and irregular framework based visual cryptography, and as of late created progressive visual cryptography.

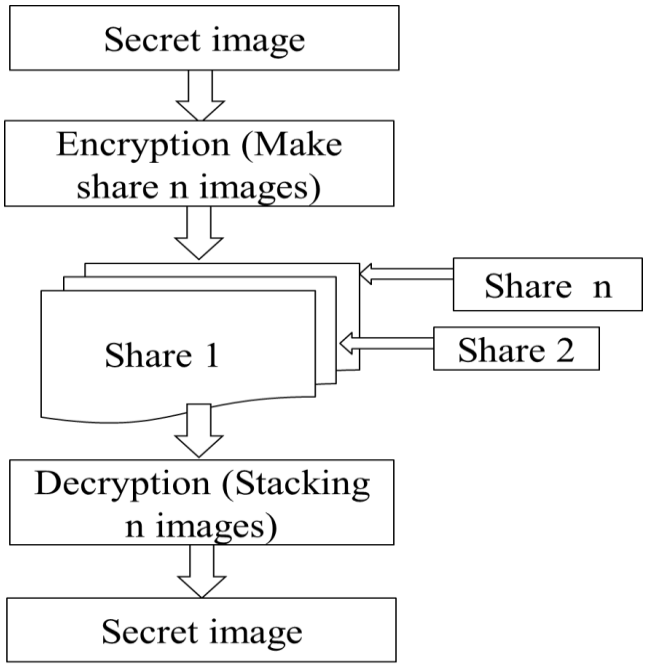

Figure 2: Flow of VCS

To keep up the privacy and secrecy of pictures is a vivacious space of examination so the Visual Cryptography arranged by Naor and Shamir could be a system that securely shares a secret picture to a few participants [9]. "Visual Cryptography is an uncommon sort of cryptographic strategy in which the decryption can perform by the human visual ability". Visual Cryptography encrypts the useful secret picture into shares with the goal that one cannot reveal the original data without other share. To decrypt the secret, all or qualified arrangement of shares are required be superimposed with each other. The encryption happens in such a way along these lines, to the point that at decryption side no mathematical equation is expected to decrypt the secret picture. The original picture which is to be encrypted is referred as secret picture. Once the encryption is finished, figures are created which is referred as shares. Share is a scramble type of unique info picture from single share anybody can't get any data about secret picture. To share the secret among gathering of n members is the central thought behind visual cryptography [10]. The secret is separated into n number of pieces, referred as shares, to share the secret. After that, these shares are conveyed among n members. Every member gives his own particular share, to reveal the originalsecret.

II. RELATED WORK

In [1], the system, the signature of a person is taken as input which is encrypted using hierarchical visual cryptography. HVC divides input signature into four resultant shares. Among four shares, any three are taken to generate key share. Remaining share is handed over to the user and the key share is placed on authentication system. Both the shares appear in scrambled format but upon superimposition, the secret is revealed.

In [2] they discuss the additions and deletions of users in a dynamic user group. To reduce the overhead of generating and distributing transparencies in user changes, this paper proposes a (t,n) VC scheme with unlimited based on the probabilistic model. The proposed scheme allows changing dynamically in order to include new transparencies without regenerating and redistributing the original transparencies. Specifically, an extended VC scheme based on basis matrices and a probabilistic model is proposed.

In [3] the system improves the security of (2, n) RGVCS by incorporating the concept of a master share. The concept of a master share is introduced in such a way that recovery of the original image is possible if and only if one among the two shares combined is the master share. Decryption using any two shares from the remaining n-1 shares other than the master (i.e. client shares) reveals nothing. XOR-based decryption is implemented here as it seems to be a perfect candidate for (2, n) schemes which enhance the image quality of the recovered secret and solving alignment problems in visual cryptographic systems.

In [4] they have proposed the new algorithms for the (2, 2) visual cryptography and (3, 3) visual secret sharing. Our proposed schemes are for gray scale image and by stacking the shares; the resultant image achieved in same size with original secret image and Its shadow Image. We used randomization and pixel reversal approach in all methods.

In [5] this paper proposes a color transfer scheme which can be incorporated into the (k, n) visual cryptography model. In encoder, a color image is encrypted into n noise-like binary share images. When any k or more than k shares are collected, a high quality colorful version of the secret image can be reconstructed with low complexity computations. The principle is

motivated to develop a color image secret sharing for output devices such as monochrome printer or fax machines. The generated share images are still binary transparencies which can be directly produced by these low cost output devices. Meanwhile, the security of a (k, n) visual cryptography model is perfectly preserved. When stacking a qualified set of transparencies, the gray level version of secret content can be revealed by human visual system. Nevertheless, the proposed paradigm is cheating immune. It also can be integrated into some emerging display technologies such as cholesteric liquid crystal display. Experimental results and related examples demonstrate the effectiveness and efficiency.

In [6]Given a secret image S, a set P of n participants and a strong access structure (LQual, LForb) a visual cryptographicscheme for general access structures (GVCS, for short) encodes S into n shares of transparencies such that the participants of eachqualified set in LQual can reveal S by superimposing their shares;whereas those of any forbidden set in LForb obtain nothing about S.Elegant GVCS constructions have been designed with smallerpixel expansions. Yet, whether the pixel expansion derived isminimized is still unknown. In this letter, we generalize andextend our recent study, in which the modeling of minimizing thepixel expansion for a (k, n) VCS into an integer linear program(ILP) was proposed, to ensure that the constraints for GVCS canbe satisfied. The pixel expansion of a GVCS can thus beminimized by solving the corresponding ILP. This is the firstresult in the literature for acquiring the optimal solution to aGVCS. The computational study demonstrates the effectiveness ofour ILP and also verifies that the best solution from previousGVCS approaches is optimal for all strong access structures of n<=4; but no more reliable for those of n>=5.

In [7] A new condition for the hierarchical threshold SIS scheme to guarantee the secrecy of the secret image when the access condition is not satisfied. SIS with the proposed condition, in which if the access condition is satisfied then the secret image is recovered in lossless manner, otherwise only pseudorandom pattern is extracted.

In [10] In visual cryptography the secret image is encrypted in to shares and at decryption side all shares are superimposed with each other so that secret is revealed. The key feature of visual cryptography is that, no difficult computation is needed at decryption side to decrypt the secret. In this paper various visual cryptographic techniques are discussed and performance analysis is done based on number of secret image, pixel expansion, image format, type of share generated.

III. DIFFERENT VISUAL CRYPTOGRAPHYS TECHNIQUES

Visual cryptography is an image encryption technique, which hide the image based secret. The big advantage of visual cryptography is that it does not require any complex computation for decryption of secret but it is performed by human visual system. In the following section the review of the different types of visual cryptography schemes are given.

A. Halftone Visual Cryptography

The review based on halftone visual cryptography is given as follows. In [5] authors have developed a general halftone visual cryptography framework, where secret image is encoded into halftone shares. This technique uses blue noise halftoning principle. The visual quality of obtained halftone shares is better than other methods. In [8] authors have proposed halftone visual cryptography construction method based on error diffusion. Pixels which carry the secret information are preset before a halftone shares are generated from gray scale image. The homogeneous and isotropic distribution of the preset pixels imposes the least noise in the error diffusion, thus leading to shares with high image quality. In [10] authors have proposed a method for processing halftone image that improve the quality of generated shares and recovered secret image, and also maintain the perfect security. In [9] authors have proposed a size invariant VSS scheme which is suitable for different distribution of image's gray values. The secret image is changed to another image then histogram of original image is generated, according to the type of the histogram shares are generated.

B. Color Visual Cryptography

The review based on color visual cryptography is given as follows. In [3] authors have proposed an effective and generalized scheme for color image hiding. In this scheme, a secret color image hides itself in two arbitrary color images, which can be constructed and then are kept by two participants, separately. The processed image is known as camouflage image. In [4] authors have proposed a method of visual cryptography for color image. This method exploits the techniques of halftone technology and color decomposition to construct three methods that can deal with both gray-level and color visual cryptography. In [8] authors have proposed a new color transfer scheme with (k,n) visual cryptography model. In encoder a color image is encrypted in to noise like binary share images, when any k or more than k shares are collected, a high quality colorful version of secret image can be reconstructed. The proposed method is a cheating immune. The reconstructed color image quality is determined by digital halftoning approach, inverse halftoning technique and printing and scanning distortion. This scheme is cheating immune and can be used as an image and video colorization. In [6] authors have proposed a secret sharing scheme for color image using Asmuth bloom technique which is further extended for accurate reconstruction of given original image. The proposed method uses quantization process to avoid loss of secret data.

C. General access structure visual cryptography

The review based on general access structure is given as follow. In [3] authors have proposed a new visual cryptography method for general access structure using optimization technique. The advantage of this method is that it

improves the visual quality of worse image; no need of codebook or basis matrices as well as it reduces the pixel expansion problem. The recovered image has better display quality then original image. In [4] authors have extended the capabilities of XORed based visual cryptography for general access structure. The advantages of this method are that no codebook is needed; decryption is done by XOR operation, no pixel expansion and perfect reconstruction of secret. In [5] authors have introduced minimization of pixel expansion using integer linear program visual cryptography for general access structure.

D. Random grid based visual cryptography

The review based on random grid based visual cryptography is given as follow. In [3] authors have shown the strict relation between deterministic and random grid based visual cryptography. The authors shown new results of (2, n), (3, n), (k, n), (n, n) threshold scheme for both deterministic and random grid based visual cryptography. In [3] authors have discussed a new random grid based non expanded visual cryptography for generation of both meaningful and noise like share. They have proposed probability allocation method for production of best contrast in share image as well as stack image. The advantage of this method is that it improved the visual quality of both share and stack images. In [5] authors have proposed a new scheme for random grid based visual cryptography. The size of revealed image is same as original secret image. The researchers have used randomization and pixel reversal approach for all methods. The proposed scheme is highly secured because of randomness. The future work is to improve contrast and reduce pixel expansion.

E. Extended visual cryptography

The review based on extended visual cryptography is given as follows. In [9] authors have proposed an extended visual cryptography for color image, which uses VIP synchronization and error diffusion for visual quality improvement. In [19] authors have proposed a new algorithm for extended embedded visual cryptography for color image using artificial bee colony algorithm. First halftoning process is applied over color image then embedding process is applied. The visual quality is increased then other methods.

F. Hierarchical visual cryptography

Hierarchical visual cryptography encrypts the secret image in to levels. In [8] authors have introduced a new concept for secret image sharing. Hierarchical visual cryptography hides the secret information into number of levels. The expansion ration is 1:4. In [9] authors have proposed design of hierarchical visual cryptography. The secret image is divided into two shares; these two shares are independently generated their own two share. In this method Generated shares are expansion less. In reference have proposed a novel idea of signature based authentication using hierarchical visual cryptography. HVC encrypts the secret in three different levels. Shares generated out of HVC are used for authentication mechanism. All shares are high contrast in nature. Signature based authentication is found to be powerful than biometric authentication as biometric patterns changes over time. Shares generated with this scheme are random in nature giving no information by visual inspection. This is expansion less scheme retaining the size of secret. Graying effect is reduced to zero due to high contrast nature of shares. In proposed a new protocol for hierarchical visual secret sharing using steganography, which maintain hierarchy and detect fake share. The PSNR value of this method is higher than other method.

IV. EXPECTED OUTCOMES

In this proposed system (N, N) visual cryptography scheme is used for security. This technique is applied on a color image. First color image is added as an input then next phase is R, G, and B component extraction. Then color shares are generated by XOR operation with Key Mask. Key mask generation algorithm is used for generating key mask. In decoding process all color shares are XOR-ed with each other and generate Master share. Master share is XOR-ed with key mask to get the recovered image. By using this method user get better security, so hacker cannot get any idea about the secret.

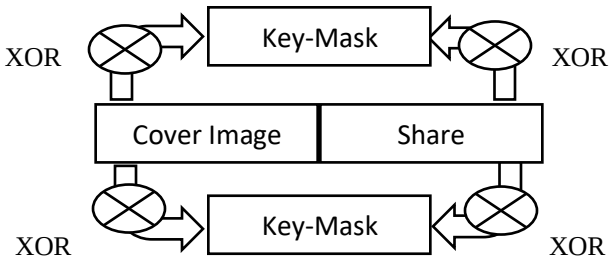

Figure 3: Flow of Proposed System

In the proposed system new shares are generated by XOR operation between Original image and Key-Mask. Key-Mask is created with the help of Key-Mask generation algorithm. At the end secret is revealed by XOR operation between new shares and Key-Mask.

CONCLUSION

Hereby it is concluded that system will provide color share VCS with novel key share approach. It will provide better security in confidential document so hacker cannot hack our important document when we will share document in secured transmission channel. And we will also improve the Mean Square Error and Peak Signal to Noise Ratio.

REFERENCES

[1] Pallavi Vijay Chavan, Dr. Mohammad Atique, Dr. Latesh Malik, "Signature Based Authentication using Contrast Enhanced Hierarchical Visual Cryptography" IEEE: Students' Conference on Electrical, Electronics and Computer Science: 2014

[2] M. Sukumar Reddy, S. Murali Mohan,"Visual Cryptography Scheme for Secret Image Retrieval" IJCSNS International Journal of Computer Science and Network Security, VOL.14 No.6, June 2014

[3] Mohamed Fathimal. P and ArockiaJansi Rani .P ,"(N, N) Secret Color Image Sharing Scheme with Dynamic Group " I. J. Computer Network and Information Security, 2015, 7, 46-52

[4] Shubhra Dixit, Deepak Kumar Jain,AnkitaSaxena, "An Approach for Secret Sharing Using Randomised Visual Secret Sharing" Fourth International Conference on Communication Systems and Network Technologies: 2014

[5] HaoLuo a, Hua Chen a, Yongheng Shang a, Zhenfei Zhao b, Yanhua Zhang b, "Color transfer in visual cryptography" Elsevier Ltd. All rights reserved: 2014

[6] ShyongJianShyu and Ming Chiang Chen," Minimizing Pixel Expansion in Visual Cryptographic Scheme for General Access Structures" , 1051-8215 (c) 2015 IEEE

[7] Angelina Espejel-Trujillo, Mariko Nakano-Miyatake, and Hector Perez-Meana," New Condition for Hierarchical Secret Image Sharing Scheme", 1550-445X/14 $31.00 © 2014 IEEE

[8] RajendraAjjipuraBasavegowda and SheshadriHolaluSeenappa,"Secret Code Authentication Using Enhanced Visual Cryptography", _ Springer India 2014

[9] Shamir A," *How to share a secret",* Communication of the ACM 22(11):612–3,1979

[10] Trupti Patel , "A Review on Different Visual Cryptography Techniques ", IJSRD - International Journal for Scientific Research & Development| Vol. 4, Issue 06, 2016

