International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
www.ijcsjournal.com Volume 4, Issue 1, No 2, 2016. ISSN: 2348-6600
Reference ID: IJCS-114 PAGE NO: 660-665.

A Survey of Various Visual Cryptography Techniques

Azmat Khan[#1], Danish Ali[*2]

[#]*Department of Computer Science & Engineering*
S.A.M.C.E.T

[1]azmat.aini@gmail.com
[3]danishalibpl@gmail.com

Abstract— **Visual cryptography is a entirely secure method to save from harm secrets and is differentiated by its original decryption process. A visual cryptography method is a process to divide a secret image into a set of shares so that a number of authorized shares can right of entry to the secret while other unauthorized shares cannot reveal out any secret information. In recent times, visual cryptography or its perception is fundamentally assumed to protect the rational possessions rights for digital images. On the other hand, some of the schemes do not assure the security conditions of visual cryptography; thus they cannot be used to protect the copyright of the images. Additionally, many techniques are not appropriate for gray-level or color watermarks.**

***Index Terms*— Security, Visual Cryptography, half tone images, embedding, extraction, dithering matrix.**

I. INTRODUCTION

Visual cryptography is a very secure and distinctive way to protect secrets [1], [2]. Contrasting conventional cryptographic methods, it uses human eyes to get better the secret without any difficult decryption algorithms and to give support of computers. Therefore, when computers or any other decryption devices are not existing, visual cryptography methods can be very useful.

In the learning of visual cryptography, pixel expansion and contrast are two most important concerns. The method of pixel expansion has been for the most part assumed to construct visual cryptography methods. On the other hand, pixel expansion cans consequence in many difficulties such as the trouble of image distortion, the prerequisite of more storage space, and the complexity in taking shares. Consequently, some techniques were suggested to manage with the difficulties of pixel expansion. Many of these techniques put together the probability perception with the convenient methods to keep away from pixel expansion. In such methods, the contrast is the same with that provided by the underlying schemes. Although some schemes can provide the best contrast for some access structures, there are still many other schemes cannot provide the best contrast. Unlike traditional cryptographic schemes, visual cryptography uses human eyes to decrypt the secret without any complex decryption algorithms and the aid of computers.

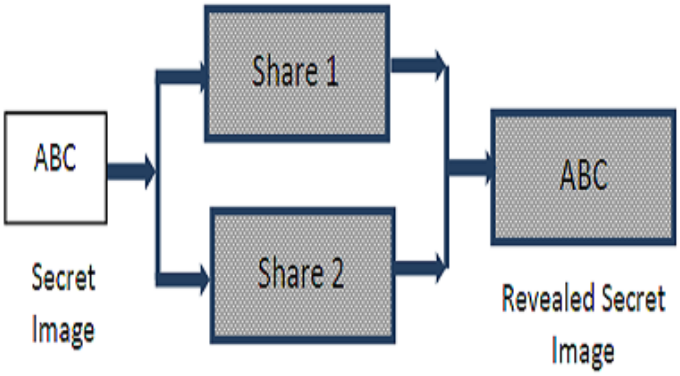

Figure 1: Traditional Way of Visual Cryptography

Usually, the decryption of the secret image consists of printing more than k shares onto transparences and superimposing these transparences on the whole; subsequently, applicants can recognize the get bettered secret from the stacked image with their observes.

Visual cryptography which make available a very powerful method by which one top secret can be allocated into two or more pieces known as shares. The top secret whose text format subject matter to encryption using substitution cipher and the consequential encrypted text were embedded into the image. When the shares on transparencies are place over accurately mutually the original secret can be determined without computer contribution.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
www.ijcsjournal.com Volume 4, Issue 1, No 2, 2016. ISSN: 2348-6600
Reference ID: IJCS-114 PAGE NO: 660-665.

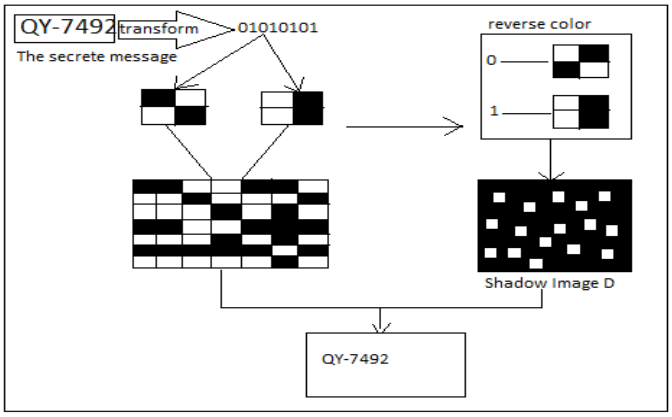

Figure 2: Sharing of Secret Image.

In figure a secret image that has to be sent is divided into shares. When these two shares are stacked together and put into a Human Visual System the consequential image is make known. In the visual secret sharing representation, a secret picture must be shared among n applicants. The image is partitioned into n shares so that if m transparencies i.e. shares are placed together the photograph is able to be seen. When there is smaller amount m transparencies it is invisible. This makes sure that the top secret image is viewed as a set of black and white pixels with each pixel being handled separately.

The traditional visual cryptography schemes employ pixel expansion. In pixel expansion, each share is m times the size of the secret image. Thus, it can lead to the difficulty in carrying these shares and consumption of more storage space. That is, the reconstructed image is identical to the original image. In order to provide perfect secrecy and the maximum clarity of the recovered secret illustrations, most investigators use the conception of pixel expansion, which was first introduced by Naor and Shamir [1] to design their visual cryptography methods. Specifically, each pixel of the binary secret image is encoded into m subpixels on each contribute to, where m is called the constraint of pixel expansion of the method. By analyzing any block of m subpixels of the forbidden set of shares, one cannot distinguish which color was used in the secret pixel.

By observing the working principles of visual cryptography, we can easily find that the recovered secret images are not identical to the original ones. For example, in the well-know 2-out-of-2 visual cryptography scheme, the contrast of the recovered binary secret images is only a half of the original secret images. This phenomenon is unavoidable in all visual cryptography schemes and is called contrast loss in this paper. If the secret image to be encrypted is a gray-level image with a narrow dynamic range in it gray scales, the phenomenon of contrast loss can be a serious problem because the recovered image may be difficult to be identified. Thus, it is an important issue to improve the contrast of the recovered gray-level images. However, few researches are about this issue. Recently, many researchers applied visual cryptography based applications or its concept to copyright protection for digital images are proposed, such as authentication, human identification, copyright protection and watermarking, mobile ticket validation, electronic cash, visual signature checking, computer generated hologram, …, [3, 4] etc. Some of the methods can fully employ the visual decryption ability of visual cryptography, and the others can guarantee the host image against modification.

II. Theoretical Background

Cryptography is the art of sending and receiving encrypted messages that can be decrypted only by the sender or the recipient. Encryption and decryption are achieved by using mathematical algorithms in such a way that no one but the intended recipient can decrypt and read the message. Visual cryptography is commenced by Noar and Shamir [2]. It is another form of cryptography in which secret communication is done in the form of representations. This can be second-hand to save from harm the biometric templates in which the decryption doesn't require any complex computations; it is done by human visual method. By means of this visual cryptography the biometric data capture from the authorized user. Visual cryptography is the technique using in the latest technology to transmit the secret information in images i.e., called secret image. Secret image sharing is the important subject in the field of communication technology, information security and production. However security can be introduced in many ways like transmitting password, image hiding, watermarking technique, authentication and identification. But the drawback of these methods is that the secret images can be protected in single information transporter. If it missing formerly, the information transporter is either damaged or destroyed. A traditional VCS takes the secret image as input and number of shares as output, it satisfies two conditions 1) secret images can be recover by any qualified subset of shares; 2) any forbidden subset of shares cannot gain any information about the secret image. The various researchers have also needs an understanding of the underlying concepts of Visual Cryptography and how they are used to generate shares of binary images. In recent times, Visual Cryptography has been

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
www.ijcsjournal.com Volume 4, Issue 1, No 2, 2016. ISSN: 2348-6600
Reference ID: IJCS-114 PAGE NO: 660-665.

making bigger to accommodate shares of gray and color images, supplementary make bigger its competence and resourcefulness.

III. Various Visual Cryptography Methods

A.) Visual cryptography for gray level images : Previous efforts in visual cryptography were restricted to binary images which is insufficient in real time applications. Chang- ChouLin, Wen-HsiangTsai [5] proposed visual cryptography for gray level images by dithering methods. In place of using gray sub pixels in a straight line to build shares, a dithering method is used to translate gray level images into approximate binary representations. Then continue livening visual cryptography systems for binary images are applied to accomplish the work of generating shares. The consequence of this system is unmoving reasonable in the characteristics of enlarge in relative size and decoded image quality, even when the number of gray levels in the original image still reaches 256.

B.) Visual cryptography for general access structures: In (k,n) Basic model any "k" shares will decode the secret image which reduces security level. To defeat this concern the fundamental representation is extended to general access structures by G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson [6],where an access structure is a specification of all qualified and forbidden subsets of "n" shares. Any subset of "k" or more qualified shares can decrypt the secret image but no information can be obtained by stacking lesser number of qualified shares or by stacking disqualified shares. Construction of scheme is still satisfactory in the aspects of increase in relative size and decoded image superiority, even when the amount of gray levels in the original image still reaches 256.

C.) Halftone Visual Cryptography: The meaningful shares generated in extended visual cryptography proposed by Mizuho NAKAJIMA and Yasushi YAMAGUCHI [7] was of poor quality which again increases the suspicion of data encryption. Zhi Zhou, Gonzalo R. Arce, and Giovanni Di Crescenzo proposed halftone visual cryptography which increases the quality of the consequential shares. In halftone visual cryptography a top secret binary pixel "P" is encoded into an array of Q1 x Q2 ("m" in basic model) subpixels, referred to as halftone cell, in each of the "n" shares. By using halftone cells with a suitable size, visually satisfying halftone shares can be acquired. Also preserves distinguish and security.

D.) Recursive Threshold visual cryptography: The (k,n) visual cryptography explained in section I needs "k" shares to reconstruct the secret image. Each share consists at most [1/k] bits of secrets. This approach suffers from inefficiency in terms of number of bits of secret conveyed per bit of shares. Recursive threshold visual cryptography proposed by Abhishek Parakh and SubhasKak eliminates this problem by hiding of smaller secrets in shares of larger secrets with secret sizes replication at every step. When Recursive threshold visual cryptography is used in network request, network consignment is diminished.

E.) Visual cryptography for color images: The researches in visual cryptography leads to the degradation in the quality of the decoded binary images, which creates it inappropriate for defense of color image .F.Liu,C.K. Wu X.J. Lin proposed a new approach on visual cryptography for colored images. They proposed three approaches as follows:

- The first approach to realize color VCS is to print the colors in the secret image on the shares directly similar to basic representation. It uses larger pixel development which decreases the superiority of the decoded color image.
- The second approach converts a color image into black and white images on the three color channels (red, green, blue or consistently cyan, magenta, yellow), in that order, and then be appropriate the black and white VCS to every one of the color guides. This results in decrease of pixel expansion but reduces the quality of the image due to halftone process.
- The third approach utilizes the binary representation of the color of a pixel and encrypts the secret image at the bit level. This consequences in enhanced excellence but necessitates devices for decryption.

F.) Regional incrementing Visual Cryptography: VC schemes mentioned above usually process the content of an image as a single/secret i.e. all of the pixels in the secret image are shared using a

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
www.ijcsjournal.com Volume 4, Issue 1, No 2, 2016. ISSN: 2348-6600
Reference ID: IJCS-114 PAGE NO: 660-665.

single encoding rule. This type of sharing policy reveals either the entire image or nothing, and hence limits the secrets in an image to have the same secrecy property. Ran-Zan Wang [8] proposed Region Incrementing Visual cryptography for sharing visual secrets in multiple secrecy level in a single image. The "n" level RIVC method, an image S is allocated to various regions associated with secret levels, and predetermined to shares with the subsequent features:

- Each share cannot obtain any of the secrets in S,
- Any t (2<t<n+1) shares can be used to reveal (t-1) levels of secrets.
- The number and locations of not-yet revealed secrets are unknown to users,
- All secrets in S can be disclosed when all of the (n+1) shares are available.

G.) Segment based visual cryptography: The VC Methods mentioned above is based on pixels in the input image. The disadvantage of pixel based visual cryptography is loss in contrast of the reconstructed image which is directly proportional to pixel expansion "m". A New approach proposed by Bernd Borchert [2] was based on segments which takes pixels as the smallest unit to be encrypted .The advantage of segment based over pixel is that it may be easier for the human eye to recognize the representations. The messages consists of numbers can be determined by segment based visual cryptography using seven segment demonstrate.

H.) Extended visual cryptography for natural images: All of the VC methods suffer from a severe limitation, which hinders the objectives of VC. The limitation lies in the fact that all shares are inherently random patterns carrying no visual information, increasing the feeling of data encryption. Mizuho NAKAJIMA and Yasushi YAMAGUCHI [7] proposed extended visual cryptography for natural images constructs meaningful binary descriptions as shares. This will decrease the cryptanalysts to imagine secrets from an entity shares. While the previous researches basically handle only binary descriptions, [7] begins the extended visual cryptography method suitable for natural images.

I.) Progressive visual cryptography: In traditional Color Visual Cryptography, loss of difference formulates VCS realistic only when an overview of visual cryptography superiority is not a problem, which is sensibly unusual. The purpose of digital halftoning techniques results in some downgrading of the original image quality due to its inherently lossy nature and it is not possible to recover the original image from its halftone version. Duo Jin Wei-Qi Ya n,Mohan S, Kankanhalli[9] proposed a new encoding method that enables us to transform gray-scale and color images into monochrome ones without loss of any information. Incorporating this new encoding scheme into visual cryptography technique allows perfect recovery of the secret grayscale or color image.

IV. Literature Survery

Wang et al. have discussed Halftone visual cryptography (HVC) [10] enlarges the area of visual cryptography by the addition of digital halftoning techniques. The proper halftoned patterns of the dithering matrix of the gray-levels 0…9 is as shown in the figure 2.

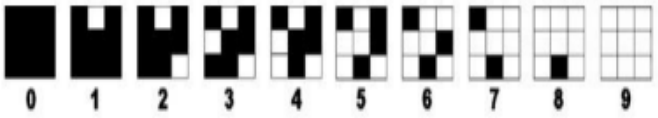

Figure 3: Halftoned patterns of the dithering matrix of the gray-levels 0…9 [10].

In particular, in visual secret sharing methods, a secret picture can be programmed into halftone shares taking meaningful visual information. Error diffusion has low complexity and provides halftone shares with good image feature. A recreated secret image, get hold of by stacking experienced shares mutually, does not experience from annoyed interference of share pictures. To overcome this problem, three methods are developed to make the reconstructed image immune to the interference from the share images. The first method employs a complementary halftone image pair. The second method deliberately introduces homogeneously distributed black pixels into each share, which has the advantage that complementary image pairs are not needed. The third method exploits the fact that the half toning of the grayscale images alone may generate a sufficient number of black pixels to satisfy the contrast condition of image decoding. The Half toning

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
www.ijcsjournal.com Volume 4, Issue 1, No 2, 2016. ISSN: 2348-6600
Reference ID: IJCS-114 PAGE NO: 660-665.

process for each pixel is done using the Algorithm. A black pixel is deliberately introduced only when a sufficient number of black pixels have not yet been generated. Consequently, balancing shares are also not necessitated. With fewer constraints on error diffusion, the third method has the potential to obtain shares showing natural images with fine details. The drawback in that the requirement of a complementary pair is removed and all the shares are generated to carry the natural images.

Author Tsai et al [11] describes the k-out-of-n visual secret sharing scheme (VSSS) propose a binary secret picture, is instructed into n shares called transparencies. Each share consists of black and white pixels, in the form of noise and has dimension bigger than that of the secret representation. The binary secret picture can be decoded by using the visual method all the way through superimposing any k of n transparencies without performing any cryptographic computation. To overcome the above problem, this system takes three pictures as an input and generates two images which correspond to two of the three input images. The third image is rebuilder by printing the two output images onto transparencies and stacking them mutually. While the earlier investigates essentially switch only binary images, but this establishes the extended visual cryptography scheme suitable for natural images. Advantage is to extend the schemes and encoded n shares as meaningful. Disadvantage of this technique is in practice, meaningless shares, however, might invite the adversary attention and to manage numerous increasing transparencies belonging to different secrets is also a problem.

N. Askari, H.M. Heys, and C.R. Moloney proposed in 'Extended Visual Cryptography Scheme with Preprocessing Halftone Images' two methods Simple Block Replacement (SBR) and Balanced Block Replacement (BBR). Straightforward approach and Very effective for unprocessed binary secret images which have large number of all white and black blocks these are some advantages of this SBR and BBR methods. The disadvantages of these methods are unfortunate contrast, being gloomier than the original image, reasons the thrashing of many very well features in the representations. The Balanced Block Replacement method uses the concept of candidate block 'CB' which consists of block of two white and two black pixels. It improves the visual quality of the processed image. The BBR method tries to keep the local ratio of black to white pixels in the processed image close to the local ratio of black to white pixels in the original halftone secret image. The algorithm used for BBR method is as follows: a) the secret image is processed into halftone picture, b) split the image into four have common characteristics clusters each restraining four secret block, c) compute no. of black pixels for each cluster and save in a template, d) leaving only black, white or candidate block other blocks are converted into black pixels, e) turned the candidate block into black or white block, based on the minimum difference among the threshold and no. of black pixels, f) Repeat the step (e) for remaining clusters and get the final processed image[12].

The halftone technique is used to produce binary images for processing gray-level and color secret images. In color visual secret sharing scheme the general k-out-of-n threshold setting and dithering is required for preprocessing the original image. In 2005, Hou and Tu developed new color VC technique using multi-pixel encoding method [13]. This scheme also supports k-out-of-n threshold setting with no pixel expansion. Dithering is still required for preprocessing the original image before secret sharing. The k-out-of-n threshold VCS for color images in this scheme supports original images of any number of color levels. It is assume that without any loss the color of the original image is represented by the conventional 24-bit color primitives, R (red), G (green) and B (blue), each has 256 levels (i.e. 8-bits). For each pixel of the original secret image, the color quality is represented by three bytes of values; and each byte specifies the intensity of the corresponding color primitive: R, G and B. The scheme is divided into four parts Histogram Generation, Color Quality Determination, Grouping, and Share Creation. In the Histogram Generation three histograms representing the intensity distribution of R, G and B color primitives of the original image are first generated. In the histogram for R (resp.G or B), the horizontal axis represents the intensity of R (resp. G or B) ranging from 0 to 255; and the vertical axis represents the number of pixels of each intensity value. In the Color Quality Determination the user choose the number of intensity levels that the reconstructed secret image will have. The user is to determine this intensity level with the purpose of maximizing the quality of the reconstructed image. In Grouping for each color primitive histogram is created with the boundary color intensity between every pair of adjacent groups. At last in the Share Creation the secret shares are created which are of same size as that of original color secret image [13].

V. Conclusion

In this paper we review various visual cryptography secret sharing methods exclusive of pixel expansion are deliberate

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
www.ijcsjournal.com Volume 4, Issue 1, No 2, 2016. ISSN: 2348-6600
Reference ID: IJCS-114 PAGE NO: 660-665.

and their concert is estimated on the basis of quality of modernized secret image. Mainly of the methods complain to bring about the high contrast of the make known secret image. To make known the secret image no other piece of equipments were required, just two share images are loaded and the original secret image is get bettered. The share images in this method are insignificant so authenticated to the safety measures regulation of visual cryptography secret sharing system.

REFERENCES

[1] M. Naor, A. Shamir, "Visual cryptography", in: A. De Santis (Ed.), Advances in Cryptology: Eurpocrypt'94, Lecture Notes in Computer Science, vol. 950, pp. 1–12, 1995.

[2] M. Naor and A. Shamir "Visual cryptography 2: Improving the contrast via the cover base," 1996, a preliminary version appears in "Security Protocols", M. Lomas ed. Vol. 1189 of Lecture Notes in Computer Sciencee, Springer-Verlag, Berlin, pp.197-202, 1997.

[3] Chang, C. C., Chuang, J. C., "An image intellectual property protection scheme for gray-level images using visual secret sharing strategy," Pattern Recognition Letters, Vol. 23, pp. 931−941, 2002.

[4] Chen, C. T. and Lu, T. C."A mobile ticket validation by VSS tech with time-stamp," Proceedings of the 2004 IEEE International Conference on e-Technology, e-Commerce and e-Service, Taipei, Taiwan, pp. 267−270, 2004.

[5] Zhou, G. R. Arce, and G. Di Crescenzo, "Halftone Visual Cryptography," IEEE transactions on Image Processing, 2006.

[6] M. Naor and B. Pinkas, "Visual authentication and identification," Crypto97, LNCS, vol. 1294, pp. 322–340, 1997.

[7] A. Bonnis and A. Santis, "Randomness in secret sharing and visual cryptography schemes," Theory. Computer. Science, 314, pp 351- 374, 2004.

[8] R. Hwang, "A digital Image Copyright Protection Scheme Based on Visual Cryptography," Tambang Journal of science and Engineering, vol.3, No.2, pp. 97-106, 2000.

[9] E.Myodo, S. Sakazawa, Andy. Takishima, "Visual cryptography based on void-and-cluster half toning technique," in Proc. IEEE ICIP, Atlanta, GA, Oct., 2006.

[10] Z. M. Wang, G. R. Arce, and G.Di Crescenzo, "Halftone visual cryptography via error diffusion," IEEE Trans. Inf. Forensics Security, vol.4, no. 3, pp. 383–396, 2009.

[11] D. S. Tsai, T. Chenc, and G. Horng, "On generating meaningful shares in visual secret sharing scheme," Image Sci. J., vol. 56, pp. 49-55, 2008.

[12] N. Askari, H.M. Heys, and C.R. Moloney "An extended visual cryptography scheme without pixel expansion for halftone images", 26th IEEE Canadian Conference of Electrical and Computer Engineering (CCECE) 978-1-4799-0033, 2013.

[13] Y.C. Hou and S. F. Tu, "A visual cryptographic technique for chromatic images using multi-pixel encoding method," Journal of Research and Practice in Information Technology, vol. 37, no. 2, pp. 179–191, 2005.