An Image Database Security Using Multilayer Multi Share Visual Cryptography: A Review

Apurva A. Mohod[1], Prof. Komal B.Bijwe[2]

[1]Department of Computer Science and Engineering, P.R. Pote Engg/Sant. Gadage Baba Amravati University, India.

[2]Department of Computer Science and Engineering, P.R. Pote Engg/Sant. Gadage Baba Amravati University, India.

ABSTRACT

In the present world when whole web is coming closer from text data to multimedia data, the majority of security concerns about the protection of this multimedia data. An Image which covers the highest percentage of the multimedia data, its protection is very important. These might include Commercial Secrets, Military Secrets and Information of individuals. It can be achieved by a technique known as Visual cryptography. By using this technique visual information (e.g. printed text and picture) is encrypted in such a way that the decryption can be performed by the human visual system, without the aid of computers. The visual secret sharing scheme divide the secret image into two or more images which are called shares. The secret image can be recovered in very simple way by stacking the shares together without any complex computation involved. The intent of this review paper is to study various techniques used for visual cryptography and also given some general introduction about it.

Keywords:-Security, Visual Cryptography, Visual Secret Share, Multi shares, half-tone.

1. INTRODUCTION

Maintaining the secrecy and confidentiality of images is a vibrant area of research, different approaches being followed for this purpose, one of them is cryptography .Cryptography is the science of keeping private information whether communicated over secured or unsecured channel from unauthorized access, of ensuring data confidentiality, integrity and authentication, and other tasks.[1] The basic theme of cryptography contains plain text and cipher text. Sender encrypts (convert plain text into cipher text) the message using the secret key and then sends it to the receiver. The receiver decrypts (convert cipher text into plain text) the message to get the secret information. Similar to cryptography, Visual Cryptography (VC) is a technique which encrypts the image and converts it into unreadable format with the help of key by decrypting the image we get original secret image. Encryption is the process of transforming the image into some other image using an algorithm so that any unauthorized person cannot recognize it. Visual cryptography is extended up to secret sharing [2]. Visual secret sharing encrypt a secret image into transparent shares such that stacking a sufficient number of shares reveals the secret image without any computation[3]. It is a obtain by secret sharing scheme [4] given by Adi Shamir in 1979[5]in which they showed how to divide data D into n pieces in such a way that D is easily reconstructable from any k pieces, but even complete knowledge of k – 1 pieces reveals absolutely no information about D . Visual cryptography is a class of technique to embed a hidden secret image in a set of binary share images [6].The effective and secure protections of sensitive information are primary concerns in commercial, medical and military systems. It is also important for any information process to ensure data is not being altered. Encryption methods are popular approaches to ensure the secrecy and integrity of the protected information. However, one of the important vulnerabilities of encryption techniques is the single-point-failure. For example, secret information is impossible to recover if the decryption key is lost or the encrypted content is corrupted during the transmission. To address these problems, in particular for large information content items such as secret images (satellite images, medical images), an image secret sharing scheme is a good alternative to remedy these types of vulnerabilities[7]. In 1994, Moni Naor & Adi Shamir shows a new concept using images called ”Visual Cryptography”.[8]In which they consider the problem of encrypting written material in perfectly secure way which can be decoded by the human visual system. The basic model consist of printed page of cipher text and a printed transparency(secret key).The original clear text is revealed by placing the transparency with the key over the page of cipher text, even though each of them is indistinguishable from random noise. Because of its simplicity it was easy to perform computation [9]. Although the Visual Secret sharing scheme was an innovative and secure solution to image sharing, it suffered from two main drawbacks. First, every pixel of an image was represented by more than one pixel in a given share. This is known as pixel expansion. Second, the recovered image suffers from low contrast. Further, each image is split into share images of higher size, resulting in high memory requirement. To address these issues, many researchers have given solutions that deal with one or more aspects of the Visual Secret Sharing issues [10].

.

2. LITERATURE SURVEY

Visual cryptography was originally invented and pioneered by Moni Naor and Adi Shamir [8] in 1994 at the Eurocrypt conference. The (k, n) Visual Cryptography Scheme can decode the concealed images without any cryptographic computations. It contain black and white pixel only and it was for sharing single secret. The secret image is divided into exactly two random shares i.e. Share1 and Share2. To reveal the original image, both shares are required to be stacked. They use complementary matrices to share a black pixel and identical matrices to share a white pixel. When two shares are superimposed, if two white pixels overlap, the resultant pixel will be white and if a black pixel in one share overlaps with either a white or black pixel in another share, the resultant pixel will be black. This implies that the superimposition of the shares represents the Boolean OR function. In Visual Cryptography Scheme, all n shares have equal importance. It may compromise the security of system. To overcome this problem, G. Ateniese, C. Blundo, A. DeSantis, and D. R. Stinson give a general access structure [11] in 1996. In which given set of n shares is divided into two subsets namely qualified and forbidden subset of shares as per the importance of shares. Any k shares from qualified subset of shares can reveal secret information, but less than k shares from qualified subset of shares can not reveal any secret information. Even k or more shares from forbidden set can’t reveal secret information. The system was more secure and pixel expansion log n.It is also for sharing the single secret having black and white pixel only. Until year 1997 visual cryptography schemes were applicable to only black and white images. First gray colored visual cryptography scheme was developed by Verheul and Van Tilborg [12] for sharing single secret. Colored secret images can be shared with the concept of arcs or MDS codes. In colorful visual cryptography one pixel is transformed into m sub pixels, and each subpixel is divided into c color regions. In every sub pixel, there is exactly one color region colored, and all the other color regions are black. The color of one pixel depends on the interrelations between the stacking of sub pixels. For a colored visual cryptography scheme with c colors, the pixel expansion m is c× 3.The share generated were meaningless. In 2000 Ching-Nung Yang and Chi-Sung Laih [13] ,presented new constructions of colored Visual secret sharing schemes. The construction methods are based on the modification and extension of the black & white Visual Secret Sharing schemes and get much better block length than the Verheul-Van Tilborg scheme[12].They improve the pixel expansion from c x 3 to c x 2. This scheme was also developed for sharing a single secret and shares generated were meaningless. Nakajima, M. and Yamaguchi, Y.[14],developed Extended visual cryptography scheme (EVS) in 2002. An EVC provide technique to create meaningful shares instead of random shares of traditional visual cryptography and help to avoid the possible problems, which may arise by noise-like shares in traditional visual cryptography. It showed a method to improve the image quality of the output by enhancing the image contrast beyond the constraints given by the previous studies. The method enables the contrast enhancement by extending the concept of error and by performing half toning and encryption simultaneously. This paper also describes the method to improve the quality of the output images. Visual Cryptography Scheme for Grey images by dithering technique was given by Chang-Chou Lin, Wen-Hsiang Tsai[15]in 2003. Instead of using gray sub pixels directly to construct shares, a dithering technique is used .The overall effect of the proposed method is the achievement of visual encryption and decryption functions for gray-level images. Extension of visual cryptography for binary to gray-level ones is useful for wider applications. An input gray-level image is first converted into an approximate binary image by dithering technique, and a visual cryptography method for binary images is then applied to the resulting dither image. This scheme possesses the advantages of inheriting any developed cryptographic technique for binary images and having less increase of image size in ordinary situations. The decoded images can reveal most details of original images. Most visual cryptographic methods utilize the technique of pixel expansion, because of which the size of the shares to be much larger than that of the secret image. This situation is more critical for grey-level and chromatic images. In 2005 Young-Chang Hou and Shu-Fen Tu[16],propose a multi-pixel encoding method for grey-level and chromatic images without pixel expansion. They have utilized two n × r basis matrices to simultaneously encrypt r successive white or black pixels each time. The probability of these r pixels being colored black depends on the ratio of blacks in the basis matrices. The experimental results show that the shares are not only the same size as the secret image, but also attain the requirement of security. Also the superimposed images have good visual effect. In 2006 Zhi Zhou, Gonzalo R. Arce, and Giovanni Di Crescenzo[17],suggested a novel technique named halftone visual cryptography to achieve visual cryptography via halftoning. It simulates continuous tone imagery through the use of dots, which may vary either in size, in shape or in spacing.It is Based on the blue-noise dithering principles, the proposed method utilizes the void and cluster algorithm to encode a secret binary image into n halftone shares carrying significant visual information. The visual quality of obtained halftone shares is observably better than any available visual cryptography method known to date. It maintains good contrast and security and increases quality of the shares.

In 2007 Shyong Jian Shyua, Yeuan-Kuen Leea,Shih-Yu Huanga Ran-ZanWangb and Kun Chena[18] were first researchers to advise the multiple secrets sharing in visual cryptography. This scheme encodes a set of n>=2 secrets into two circle shares such that none of any single share leaks the secrets. The n secrets can be revealed one by one by stacking the first share and the rotated second shares with different rotation angles. This technique was developed for sharing multiple secret in black and white visual cryptography scheme. This is the first true result which shows the sharing ability in visual cryptography up to any general number of multiple secrets in two circle shares. In 2008 Hsien-

Chu Wu, Hao-Cheng Wang and Rui-Wen Yu [19] proposed a color visual cryptography scheme producing meaningful shares .The scheme uses halftone technique, secret coding table and cover coding table to generate two meaningful shares without increasing the security risks on the secret image. The secret image can be decrypted by stacking the two meaningful shares together. This scheme is perfectly applicable and achieves a high security level they extend a single pixel into a 2×4 block. However, the size of the share remains the same as what happens in the 2×2 pixel expansion case. Also a considerable part of the storage space can be saved. A new reversible visual secret sharing method proposed in 2009 by Wen-Pinn Fang [20]. Without doing any computation, if we stack two transparencies directly, a secret image will appear. Again stack two transparencies but reversing one of transparencies, another secret image will unveil. Different from traditional reversible visual cryptography, the method has advantages and also will not have pixel expansion .They had used Random grid method. Besides, the same idea can be extended to complex style visual cryptography. It was for sharing multiple secret having black and white image .Rezvan Dastanian and Hadi Shahriar Shahhoseini 2011[21] proposed Multi Secret Sharing Scheme for encrypting two Secret Images into two Shares. By stacking two shares, first secret image appears and with stacking one of the shares with 90 degrees rotation in clockwise on other share appears the second secret image. At first, based on halftone technology secret images are transformed secret to binary images then dealer divides secret image1 to two shares, share a and share b, and secret image2 is also divided into two shares, share a’, share b’. To make share A, dealer stacks share a’ with 90 degrees rotation in counterclockwise on share A and for share B, share b stacking on share b’. Dealer distributes share A and B between two participants and for decryption with present two participants, by stacking share A and B, secret image I appears and stacking share A on share B with 90 degrees rotation in clockwise reveal secret image II. Anantha Kumar Kondra and Smt. U. V. Ratna Kumari[22] in 2012 Developed an Improved (8, 8) Color Visual Cryptography Scheme Using Floyd Error Diffusion solution which helps to identify the error in the shares and to verify the authentication. Using CRC algorithm, Color VC scheme and error diffusion method generates the quality shares and diffuses the errors and provides the security from threats like modification, fabrication, interception and shows the good results compared to the previous schemes and increases the security level. Error diffusion is used to construct the shares such that the noise introduced by the preset pixels is diffused away to neighbors when encrypted shares are generated. It is obvious that there is a tradeoff between contrast of encryption shares and the decryption share; however, reorganization of the colorful secret messages having even low contrast. In 2013 N. Askari, H.M. Heys, and C.R. Moloney[23] proposed An EVC Scheme Without Pixel Expansion For Halftone Images which contain method for processing halftone images that improves the quality of the share images. The size of the share images and the recovered image is the same as for the original halftone secret image. In this scheme the grey scale image is converted to halftone image and simple block replacement and balanced blocked replacement method are applied on it. The scheme maintains the perfect security of the original extended visual cryptography approach. By using an intelligent pre-processing of halftone images based on the characteristics of the original secret image, they have produce good quality images in the shares and the recovered image. In 2014 Shubhra Dixit, Deepak Kumar Jain and Ankita Saxena[9]proposed an approach for secret sharing using randomized VSS in which they propose new visual cryptography algorithm for gray scale image using randomization and pixel reversal approach. (2, 2) randomize visual cryptography in practice where the shares are generated based on pixel reversal, random reduction in original pixel and subtractions of the original pixel with previous shares pixel. The original secret image is divided in such a way that after OR operation of qualified shares we reveals the secret image. In the (3, 3) visual secret sharing scheme shares are generated based on pixel reversal, random reduction in original pixel and subtractions of the original pixel with previous shares pixel and storing the final value of the share pixel after reversal into the shares in round robin fashion. The result of the three shares and after OR operation using stacking of all these qualified shares the original secret reveal.

2.1 TABLE

S.No.	Year	Author	Schemes And methodology	Advantages
1	1994	Moni Naor and Adi Shamir[8]	(k,n) Visual Cryptography Scheme by Boolean OR function	First visual cryptography scheme, secure and easy to implement.
2	1996	G. Ateniese, C. Blundo, A. DeSantis, and D. R. Stinson[11]	General access structure scheme using forbidden and qualified shares	It is more secure than scheme proposed in [7] and pixel expansion is reduced to log n.
3	1997	Verheul and Van Tilborg [12]	Gray colored visual cryptography scheme using arcs or MDS codes	First Visual cryptography technique performed on colour images.

4	2000	Ching-Nung,Yang and Chi-Sung Laih [13] ,	New construction of colored VSS scheme using modification and extension of black and white pixel	Much better block length than Verheul-Van Tilborg scheme. Pixel expansion is c x 2
5	2002	Nakajima, M. and Yamaguchi, Y.[14]	Extended visual cryptography scheme for natural images	The shares generated are meaningful and improve the quality of output image.
6	2003	Chang -Chou Lin, Wen-Hsiang Tsai[15]	Visual Cryptography Scheme for Gray images by dithering technique	It inheriting any developed cryptographic technique for binary images and having less increase of image size given in [3].
7	2005	Young-Chang Hou and Shu-Fen Tu[16]	Visual Cryptographic Technique for Chromatic Images using MPEM	It provide grey-level and chromatic images cryptography without pixel expansion
8	2006	Zhou, Gonzalo R. Arce, and Giovanni Di Crescenzo[17]	Halftone visual cryptography using void and cluster algorithm to encode a secret binary image into n halftone shares.	The visual quality obtained better than available method. It maintains good contrast and security and increases quality of the shares.
9	2007	Shyong Jian Shyua, et al [18]	Multiple secrets sharing scheme	The first true result that discusses the sharing ability in visual cryptography of multiple secrets in two circle shares.
10	2008	Hsien-Chu Wu, Hao-Cheng Wang and Rui-Wen Yu[19]	Colour visual cryptography scheme using halftone technique, secret coding table and cover coding table	It generates meaningful shares without increasing the security risks on the secret image. It is for colour images.
11	2009	Wen-Pinn Fang[20]	Reversible visual secret sharing scheme using random grid method	Non-expansion visual secret sharing method with reversible property.
12	2011	Rezvan Dastanian and Hadi Shahriar Shahhoseini [21]	Multi Secret Sharing Scheme for Encrypting Two Secret Images into Two Shares using halftone technique	Two secret images are encrypted using this scheme hence storage capacity and bandwidth required is less.
13	2012	Anantha Kumar Kondra and Smt. U. V. Ratna Kumari[22]	(8,8)Colour Visual Cryptography Scheme Using Floyd Error Diffusion	An encryption method to construct colour EVC scheme for visual quality improvement and it provide more security having meaningful 8 shares.
14	2013	N. Askari, H.M. Heys, and C.R. Moloney[23]	EVC scheme without pixel expansion using an intelligent pre-processing of halftone images ,SBR and BBR	It produces good quality images in the shares and the recovered image used for biometric security
15	2014	Shubhra Dixit, Deepak Kumar Jain,Ankita Saxena[9]	VC using randomised Visual Secret Sharing and pixel reversal approach.	The results are better and the size of the retrieve image is the same as the original image

3. PROPOSED METHODOLOGY

Proposed methodology has been divided into 2 phases.

3.1 IMAGE ENCRYPTION

In this phase, an image will be encrypted in five steps. In the first step an input image will be selected. The selected image must be RGB Image. In second step red, green and blue channels are separated from an input image. After each channel is further encrypted into 8 shares in third step. This encryption will depend on key Used. As each channel is divided into 8 shares total 24 shares are obtained. These 8 shares of an each channel then further compress to 3 shares. As compression is performed on each channel output of 9 shares is obtained at step four. Compress these 9 shares to 3 Shares and finally compress 3 shares to one final encrypted image.

3.2 IMAGE DECRYPTION

Proposed image decryption method work exactly opposite as that of the encryption phase. In first step select an encrypted image. It must be RGB Image. After that separate red, green and blue channels from an encrypted Image. Create 3 Shares from each channel. From these 3 shares 9 encrypted images will be obtained as an output .In step 4 creates 8 shares from previous 9 shares for each channel. From 8 shares each of step 4, Create 3 Shares (i.e red, green and Blue each).Finally Compress last step images to plain Image (Decrypted Image).

4. CONCLUSION AND FUTURE SCOPE

Currently, many new schemes are introducing in the field of Visual Cryptography. Some of the schemes are discussed in this paper. The concept of secret sharing was given by Moni Naor and Adi Shamir and many techniques were implemented by extending that concept. Every methodology has advantages and disadvantages regarding pixel expansion, complexity, number of share generated, type of share generated. In future this technique can be implemented for 3dimensional images.

REFERENCES

[1] Quist-Aphetsi kester, Laurent nana,Anca Christine Pascu,,"A Novel Cryptographic Encryption Technique of Video Images using Quantum Cryptography for satellite Communication,"978-1 -4799-3067-8/13 ©2013 IEEE.

[2] Roberto De Prisco and Alfredo De Santis,"On the Relation of Random Grid and Deterministic Visual Cryptography, " Transactions On Information Forensics And Security, Vol. 9, No. 4, April 2014 IEEE.

[3] Biswapati lana, Madhumita Mallick, Partha Chowdhuri, Shyamal Kumar Mondal,"Cheating Prevention in Visual Cryptography using Steganographic Scheme," 978-1-4799-2900-9/14/$31.00 ©2014 IEEE.

[4] K Ching-Nung Yang and Dao-Shun Wang, "Property Analysis of XOR-Based Visual Cryptography," Transactions On Circuits And Systems For Video Technology, Vol. 24, No. 2, February 2014 IEEE.

[5] Adi Shamir,"How to share a secret,"ACM N0014-76-C-0366, vol. 22, Novembber 1979.

[6] Ming Sun Fu, Oscar C. Au, " Joint Visual Cryptographyand Watermarking," 0-7803-8603-5/04©2004 IEEE.

[7] Vinay Rishiwal and Ashutosh Gupta, "An Efficient Secret Image Sharing Scheme," World Applied Programming, Vol (2), Issue (1), January 2012. 42-48.

[8] Naor, M. and Shamir, A.,"Visual cryptography,"In Proc. Eurocrypt 94, Perugia, Italy, May 912, LNCS 950, pp. 112.,2010, Springer Verlag.

[9] Shubhra Dixit,Deepak Kumar Jain, and Ankita Saxena, "An Approach for Secret Sharing Using Randomised Visual Secret Sharing," 2014 Fourth International Conference on Communication Systems and Network Technologies 978-1-4799-3070-8/14 $31.00 © 2014 IEEE.

[10] Subhash Chand Bunker, Mayur Barasa and Aparajita Ojha, Linear Equation Based Visual Secret Sharing Scheme," 978-1-4799-2572-8/14/$31.00c 2014 IEEE .

[11] Giuseppe Ateniese ,Carlo Blundo and Alfredo De Santis, Visual Cryptography for General Access Structures, information and computation 129, 86106 (1996), article no. 0076.

[12] 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.

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

[14] Mizuho Nakajima and Yasushi Yamaguchi, "Extended Visual Cryptography For Natural Images," Journal of WSCG. v10 i2. 303-310,2002.

[15] Chang-Chou Lin and Wen-Hsiang Tsai, "Visual cryptography for gray-level images by dithering techniques," 0167-8655/03/$ - see front matter 2003 Elsevier Science B.V.

[16] Young-Chang Hou and Shu-Fen 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, May 2005.

[17] Z. Zhou, G. R Arce, and G. Di Crescenzo, "Halftone Visual Cryptography," in Proc. of IEEE International Conference on Image Processing,Barcelona, Spain, VOL. 15, NO. 8, August 2006.

[18] Shyong Jian Shyu,Shih-Yu Huang, Yeuan-Kuen Lee, Ran-ZanWang, Kun Chen, "Sharing multiple secrets in visual cryptography," doi:10.1016/j.patcog.2007.03.012_ 0031-3203/$30.00 _ 2007.

[19] Hsien-ChuWu,Hao-Cheng Wang, and Rui-Wen Yu,"Color Visual Cryptography Scheme Using Meaningful Shares," Eighth International Conference on Intelligent Systems Design and Applications, 978-0-7695-3382-7/08 $25.00 © 2008 IEEE.

[20] Wen-Pinn Fang, "Non-expansion Visual Secret Sharing in Reversible Style". IJCSNS, VOL.9 No.2, February 2009

[21] Rezvan Dastanian and Hadi Shahriar Shahhoseini," Multi Secret Sharing Scheme for Encrypting Two Secret Images intoTwo Shares," 2011 International Conference on Information and Electronics Engineering IPCSIT vol.6 (2011) IACSIT Press, Singapore.

[22] Anantha Kumar Kondra, Smt. U. V. Ratna Kumari, "An Improved (8, 8) Colour Visual Cryptography Scheme Using Floyd Error Diffusion," IJERA ISSN: 2248-9622 Vol. 2, Issue 5, September- October 2012, pp.1090-1096

[23] N. Askari, H.M. Heys, and C.R. Moloney" An Extended Visual Cryptography Scheme Without Pixel Expansion For Halftone Images," 26th Annual IEEE Canadian Conference On Electrical And Computer Engineering Year 2013 .

AUTHOR

Apurva A. Mohod Received Bachelor of Engineering in Information Technology from SGB Amravati university & Pursuing Master of Engineering in Computer Science and Engineering from P.R.Pote(Patil) College of Engineering and Management, Amravati.

Prof. Komal B. Bijawe Received Master of Engineering in Computer Science and Engineering from SGB Amravati University. Working as assistant professor in P.R.Pote(Patil) College of Engineering and Management, Amravati.