A Survey Report on Visual Cryptography and Secret Fragment Visible Mosaic Images

Rucha R. Raut[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 as the information world progresses and data become more and more valuable, security concern is the major issue and protection of that data, which comes from text data to multimedia data. Multimedia data includes high percentage of images so its protection is very important. The protection of this multimedia data is done by visual cryptography and secret fragment visible mosaic images. There are so many different skilful techniques design to conduct for protection of this confidential image data from unauthorized access. In this paper, I had done the literature survey on existing work which used different techniques for image hiding from 2001 to 2014 and also given general introduction about visual cryptography and secret fragment visible mosaic images
Keywords:-Visual cryptography, Mosaic images, watermarking, halftone images

1.INTRODUCTION

Visual cryptography was mainly introduced for the problem of secret sharing. Secret sharing is one of the major problems to be considered in cryptography. Secret sharing is one type of key establishment protocols. [1]-[2].Visual Cryptography was pioneered by Moni Naor and Adi Shamir in 1994. They proposed visual secret sharing scheme, where an image is divided into n shares so that only someone with all n shares could decrypt the image, while someone with any n-1 shares can retrieve no information about the original image. Each share is printed on a different transparency and decryption is performed by overlaying the shares when all n shares are overlaid, the original image gets visible [3]. The main objective of data hiding is to communicate securely in such a way that the secret message is not visible to the observer. That is unauthorised person should not be able to identify in any sense between target image and secret image. For the data hiding visual cryptography and secret fragment visible mosaic images plays a very important role. Mosaic is a different type of art manufactured by generating small pieces of any materials, such as stone, glass, tile, etc. First target image is selected; the given secret image is then divided into rectangular tiles, which then are fit into similar blocks in the target image. Next, the colour characteristic of each tile image is transformed to be that of the corresponding block in the target image, resulting in a secret mosaic image which looks like the selected target image [4].Genetic algorithms (GAs) are search methods based on principles of natural selection and genetics [5]. It is useful for the application of covert communication or secure keeping of secret images. There is another technique discovered lαβcolor space in the context of understanding the human visual system, and to humans knowledge, lαβ space has never been applied otherwise or compared to other color spaces[6].A watermarking has been defined as the practice of embedding identification information in an image, audio, video or other digital media element to provide privacy protection from vulnebarities[7].For generation of shares two basic principles used namely, error diffusion and pixel synchronization. Error diffusion is a simple but necessary algorithm for image halftone generation. The quantization error at each pixel is altered and fed back to future inputs. The error filter is designed in a way that the low frequency difference between the input and output image is minimized and subsequently it produces pleasing halftone images for human vision. Synchronizing the visual information pixels across the color channels increases visual contrast of shares [8]. For visual cryptography, the use of digital half toning is for the purpose of converting a greyscale image into a monochrome image. Once we have a binary image, then the original visual cryptography technique can be established [9].Given that the direct binary search method can achieve significantly better output halftone image quality than error diffusion. The secret image can be clearly decrypted without showing any interference with the share images [10].In this paper we proposed a survey report on different data hiding techniques for visual cryptography and mosaic images.

2. LITERATURE SURVEY

Chin Chen chang, Min- Shian Hwang, and Tung Shou Chen[11] have proposed a fast encryption algorithm for image cryptosystems in 2001. Vector Quantization, cryptography and other number theorem is the main platform for this cryptosystems.VQ is an useful technique to low bit rate image compression. In VQ first decomposition of images into vectors takes place and then vector by vector then are sequentially encoded Young-Chang Hou[12] have presented a technique for visual cryptography of color images in 2002 which consist of three methods for visual cryptography of gray-level and color images based on past studies in black and white visual cryptography, the halftone technology method, and the color decomposition method. His technique gives us backward compability with the ols results in black and white VS along with advantages of black and white VS which is very helpful visual system to decrypt secret image without computation like t out of n threshold scheme which can be applied to gray level and colourful images. Soo-Chang Pei and Jing-Ming Guo [13] have developed a hybrid method of combing noise balanced error diffusion (NBEDE) data hiding and kernel altered error diffusion (KAEDE) watermarking into one or more error diffusion images in 2003. The hybrid model is extended up to color images; in which large amount of information is embedded and has maintained good quality of result. It also proposed pixel based data hiding with noise balanced error diffusion along with block based digital watermarking technique with KAEDE and at last watermarking for error diffused images and hybrid data hiding takes place.   Sabu M Thampi[14] have presented a information hiding technique in 2004 in which a brief history of steganography is explained along with techniques that were used to hide secret information. Textual , audio and image based information hiding techniques like Least Significant bit(LSB) insertion technique in which embed the information in graphical image file, masking and filtering techniques in which by making an image in a manner similar to paper watermarks and transformation techniques which is done by using discrete cosine transformation or wavelet transform. to hide information in significant areas of image. Clemens Fruhwirth[15] have presented a technique in 2005 in which he investigates the state of the art in hard disk cryptography. As the choice of the cipher mode is necessary for the security of hard disk data, they discuss the recent cipher mode developments at two   standardization bodies, NIST and IEEE. CBC analysis is also done by Clemens Fruhwirth. It includes mainly (1) efficient algorithms for series of multiplications in a Galois field (2) password based security analysis cryptography with respect to low entropy attacks and (3) TKS1, a design template for secure key management.. After that they solve the difficulties arising from magnetic storage by using a technique such as anti-forensic information splitter.   Zhicheng Ni, Yun-Qing Shi, Nirwan Ansari, and Wei Su [16] have proposed a new data hiding technique in 2006, i.e. reversible data embedding technique, which can embed a large amount of data (5–80 kb for a 512 512 8 grayscale image) the PSNR of the marked image versus the original image is guaranteed to be higher than 48 dB which kept a large percentage of visual quality for all natural images. For embedding of data it uses the zero or the smallest point of the histogram and slightly modifies the pixel grayscale values. All types of image are based on this technique. Dinu Coltuc and Jean-Marc Chassery[17]have presented a data hiding technique in 2007 like RCM, a modified version that allows robustness against cropping. It also is investigates the control of distortions introduced by the watermarking. It also analysed the mathematical complexity of the RCM watermarking, and a very low cost implementation is proposed. Finally, the RCM scheme is compared with Tian's difference expansion scheme with respect to the bit-rate hiding capacity and to the mathematical complexity. It is shown that the RCM scheme provides almost similar embedding bit-rates when compared to the difference expansion approach, but it has a considerably lower mathematical complexity. Yongjian Hu,Heung-Kyu Lee, Kaiying Chen, and Jianwei Li [18]have presented a algorithm based on integer Haar wavelet transform in 2008, propose an algorithm that selects expandable differences under the same selection threshold in two difference images and embeds the payload in two orthogonal embedding directions. Furthermore, no matter in which difference image, our algorithm can always give priority to the use of small differences, which improves image quality. Algorithm does not have the original layer embedding capacity limit. The algorithm performance is smooth and varies gradually with the change of payloads. InKoo Kang, Gonzalo R. Arce and Heung-Kyu-Lee [19] have proposed a new data hiding method in 2009, a color VC encryption method which leads to meaningful shares and is free of the previously mentioned limitations error diffusion and pixel synchronization basic principles used in the generation of shares. Error diffusion is a simple but basic algorithm for image halftone generation. In this technique the quantization error at each pixel is filtered and fed back to future input. for VS. Monisha Sharma[20], have presented a technique using chaotic schemes for data hiding in 2010.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. I-Jen Lai and Wen-Hsiang Tsai[21]have presented a technique of information hiding in 2011 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 t he key can reconstruct

International Journal of Application or Innovation in Engineering & Management (IJAIEM)
Web Site: www.ijaiem.org Email: editor@ijaiem.org

Volume 3, Issue 10, October 2014   **ISSN 2319 - 4847**

the secret image by retrieving the embedded information. Jagdeep Verma, Dr.Vineeta Khemchandani [22] proposed scheme will add the merits of both visual cryptography as well as Invisible and Blind watermarking techniques in 2012, where we will generate the secret shares using basic visual cryptography model and then we 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 Anuprita U. Mande and Manish N. Tibdewa[23] have presented a technique in 2013 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, we will take a review of all these methods. At the same time we will compare all these methods and will adopt the one which will give us the best result with respect to color visual cryptography.   Ya-Lin Lee and Wen-Hsiang Tsai [24] have proposed a new scheme in 2014 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.

2.1 TABLE

Sr.No	Year	Author	Proposed Work
1	2001	Chin-Chen,Min Shian Hwang,Tung Shou Chen	Vector Quantization method achieved a low bit rate image compression.
2	2002	Young Chang hou Hou	Gives backward compability with previous results in black and white VS to decrypt the image
3	2003	Soo Chang Pei Jing Ming Guo	Combine WBEDE $ KAEDE in which large amount of information is embedded & maintain good quality of results.
4	2004	Sabu M Thampi	Used LSB insertion discrete cosine transform technique to hide image
5	2005	Clemens Fruhwrth	They proposed efficient algorithm for series of multiplication in a Galois field along with password based security analysis and TKS1.
6	2006	Zbicheng Ni,YunQing , Ansari,Weisu	Embed a large amount of data using zero or smallest point of the histogram.
7	2007	Dihu Coltuc & Jean Marc Chassery	Used data hiding technique like RCM having lower mathematical complexity
8	2008	Yongjian Hu,Heung Kyu lee,Kaiying Chen Jianwei	Proposed algorithm which improve image quality by using Haar wavelet transform by reversible data hiding
9	2009	Inkoo Kang, Gonzalo R. Arce ,Heung Kyu lee	In this, quantization error at each pixel is filtered and fed back to the future input for VS by using Matrices construction with VIP synchronization algo.
10	2010	Monisha Sharma	They provide security function as well as visual check by using chaotic schemes.

International Journal of Application or Innovation in Engineering & Management (IJAIEM)
Web Site: www.ijaiem.org Email: editor@ijaiem.org

Volume 3, Issue 10, October 2014   **ISSN 2319 - 4847**

11	2011	I-Jen Lai ,Wen Hsiang Tsai	Create a secret fragment visible mosaic image by fragmentation technique to better data security by Mosaic Image Creation Algorithm.
12	2012	Jagdeep Varma,Dr.Vineeta Khemchandani	Add the merits of both VC & blind watermarking by avoiding any feature from original image.
13	2013	Anupita u.Mande,Manish N. Tibdewel	They introduce color error diffusion technique for generating halftone shares which are more pleasant to human eyes
14	2014	Ya Lin Bee , Wen Hsiang tsai	They converts secret image into a meaningful mosaic image with the same size by reversible color transformation.

3. PROPOSED METHODOLOGY

Proposed methodology has been divided into 2 phases.

3.1 Mosaic Image Creation

In this first phase, Shamir secret sharing algorithm is used by which a secret is divided into parts, giving each participants its own unique part, some of the parts or all of them are needed in order to reconstruct the secret counting on all participants to combine together, the secret might be impractical and therefore sometimes the threshold scheme is used. Now fitting the tile images of the secret image into the target blocks of a preselected target image. After this transforming the color characteristic of each tile image in the secret image to become that of the corresponding target block in the target image and rotating each tile image into a direction with the minimum RMSE value with respect to its corresponding target block. After the rotation embedding relevant information into the created mosaic image for future recovery of the secret image. In this way we get the output secret fragment visible mosaic image.

3.2 Secret Image Recovery

In this second phase, extracting the embedded information for secret image recovery from the mosaic image, and recovering the secret image using the extracted information by secret image recovery algorithm. In this phase result will be calculated and optimize if required result is in the form of delay and accuracy

4. CONCLUSION AND FUTURE SCOPE

In today's world where nothing is secure, the security of images is very important. In this paper I have surveyed different image hiding techniques in the span of 14years (2001- 2014).   I conclude that all techniques are good for data hiding and have their own advantages and disadvantages and give a security so that no one can access the image which is in the open network. Good mosaic image creation results are guaranteed only when the database is large in size so that the selected target image can be sufficiently similar to the input secret image. In future it may be may be directed to allowing users to select target images from a smaller sized database or even freely without using a database, as well as to developing more information hiding applications using the proposed secret-fragment-visible mosaic images.

REFERENCES

[1] Er. Supriya Kinger, "Efficient Visual Cryptography", Journal of emerging technologies in web intelligence, vol. 2, no. 2, may 2010

[2] Musaab R. Abdulrazzaq ,"Visual Cryptography Vs Bit Level Secret Sharing For Image Encryption" Eng. & Tech. Journal, Vol.28, No.7, 2010

[3] Moni Naor and Adi Shamir, "Visual cryptography", Springer veriag,1998.

[4] Nitin Kumar Agrawal, Neeraj Pandey& Ashish Arya," Data Hiding System with Mosaic Image for Protected Communication", International Journal of Computer Trends and Technology (IJCTT) ,volume 4 Issue 5,May 2013

[5] Nithya Francis &Naveen ," Secret Fragment Visible Mosaic Image Using Genetic Algorithm", International Journal of   Advanced Trends in Computer Science and Engineering   (IJATCSE), Vol.2 , No.5, Pages :64-69 (2013) Special Issue of ICCECT 2013 - Held during September 20, 2013

[6] Erik Reinhard, Michael Ashikhmin, Bruce Gooch and Peter Shirley"color transform between images" IEEE 0272-1716/01/$10.00 © 2001

[7] Jitendra Saturwar,Dr.D.N.Chaudhari" Digital Watermarking Scheme For Secret Images Using Visual Cryptography" International Journal of Scientific & Engineering Research, 6 ISSN 2229-5518 Volume 4, Issue 6, June-2013

[8] InKoo Kang, Gonzalo R. Arce and Heung-Kyu Lee "Color extended visual cryptography using error diffusion" 978-1-4244-2354-5/09/$25.00 ©2009 IEEE.

[9] Abhinav Paliwal , Ashish Patnaik and Kritika Vaid" Half toning visual cryptograpy for sharing secret image" IJARES Volume 1 Issue 1 Jan 2014

[10] Zhongmin Wang†, Gonzalo R. Arce† and Giovanni Di Crescenzo" Halftone visual cryptography via direct binary search" 14th European Signal Processing Conference (EUSIPCO 2006), Florence, Italy, September 4-8, 2006.

[11] Chin chen Chang,Min Shian Hwang and Tung Shou Chen," A new image encryption algorithm for image cryptosystems",the journal of system and software 58(2001

[12] Young-ChangHou" Visual cryptography for color images" Pattern Recognition 36 (2002) .

[13] Soo-Chang Peiand and Jing-Ming Guo" Hybrid Pixel-Based Data Hiding and Block-Based Watermarking for Error-   Diffused Halftone Images", IEEE transactions on circuits and system for video technology, vol. 13, no. 8, august 2003.

[14] SabuM.Thamp,"Information Hiding Techniques: A Tutorial Review", ISTE-STTP on Network Security & Cryptography , LBSCE2004.

[15] Clemens Fruhwirth, New Methods in Hard Disk Encryption, Institute for Computer Languages Theory and Logic Group Vienna University of Technology, July 18,2005

[16] Zhicheng Ni, Yun-Qing Shi, Nirwan Ansari, and Wei Su," Reversible Data Hiding", IEEE   transactions on circuits and   system for vedio technology, vol. 16, no. 3, march 2006

[17] Dinu Coltuc and Jean-Marc Chassery," Very Fast Watermarking by Reversible Contrast Mapping", IEEE signal processing letters, vol. 14, no. 4, april 2007

[18] Yongjian Hu, Member, IEEE, Heung-Kyu Lee, Kaiying Chen, and Jianwei Li," Difference Expansion Based Reversible Data Hiding Using Two Embedding Directions", IEEE transactions on multimedia, vol. 10, no. 8, december 2008

[19] InKoo Kang, Gonzalo R. Arce and Heung-Kyu-Lee," color extended visual cryptography using error diffusion", 978-1-4244-2354-5/09/$25.00 ©2009 IEEE

[20] Monisha Sharma," Image encryption techniques using chaotic schemes: a review", International Journal of Engineering Science and Technology Vol. 2(6), 2010, 2359-2363

[21] I-Jen Lai and Wen-Hsiang Tsai,"] Secret-Fragment-Visible Mosaic Image–A New Computer Art and Its Application to Information Hiding", IEEE transactions on information forensics and security, vol. 6, no. 3, September 2011.

[22] Jagdeep Verma, Dr.Vineeta Khemchandani," A Visual Cryptographic Technique to Secure Image Shares", International Journal of Engineering Research and Applications (IJERA) Vol. 2, Issue 1,Jan-Feb 2012

[23] Anuprita U. Mande and Manish N. Tibdewal," Parameter Evaluation and Review of Various Error-Diffusion Half toning algorithms used in Color Visual Cryptography", International Journal of Engineering and Innovative Technology (IJEIT) Volume2,Issue8,February2013

[24] Ya-Lin Lee and Wen-Hsiang Tsai," A New Secure Image Transmission Technique via Secret-Fragment-Visible Mosaic Images by Nearly Reversible Color Transformations", IEEE transaction on circuits and system for video technology, vol. 24, no. 4, April 2014

AUTHOR

Rucha R. Raut 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.