A Survey on Perceived Visual Quality and Secured Visual Cryptography Schemes

D. Madhavi
Assistant Professor
VR Siddhartha Engineering
College, Kanuru, Vijayawada

A. Vasu Devasastry
M-Tech Scholar
VR Siddhartha Engineering
College, Kanuru, Vijayawada

ABSTRACT
VC, EVCS and Color EVCS are the three techniques used for Visual Cryptography Schemes. Visual Cryptography Scheme (VCS) is one of the techniques used to encrypt the image by dividing the original image into transparencies called Shares. A set of qualified participants is able to recover the secret image. An Extended Visual Cryptography Scheme (EVCS) is a kind of VCS which consists of embedded random shares realized by embedding shares into covering shares. Color Visual Cryptography (VC) encrypts a color secret image into n color halftone image shares. Different methods for VC have different algorithms to provide cryptography for images. Two of the main areas of research in visual cryptography have been on improving the visual quality of the recovered image and the security of encrypted transparency shares. Generally, Visual Cryptography suffers from the deterioration of the image quality and security. Many authors are proposed different algorithms for these parameters. This paper describes the trade-off between the image quality and the security is discussed by comparing these VC schemes.

General Terms
Visual Cryptography, Security, Quality.

Keywords
VCS (Visual Cryptography Scheme), EVCS (Extended Visual Cryptography Scheme), Color EVCS, DEGGA (Data Embedding Technique for Grayscale Image using Genetic Algorithm)

1. DESCRIPTION
Visual Cryptography (VC) is a type of secret sharing scheme introduced by Nair and Shamir [1] [10], which serves as a basic model and has been applied to many applications. Generally, applications of information hiding are a lot, apart from those there are many other applications of VC, which includes general access structures, copyright protection, and watermarking, visual authentication, print and scan applications etc.

Generally, In VC scheme the process of dividing the image into transparencies is called shares, which are used for encryption technique. The decryption process is done through by selecting the stack of set of qualified transparencies. In Embedded Extended Visual Cryptography, the DEGGA algorithm is used for encryption process. Whereas, in the Color EVCS uses Visual information pixel (VIP) synchronization for encryption process. It uses pseudo random numbers and error diffusion method for better security and image quality respectively. This paper describes among these three methods which one gives the best visual cryptography method for providing security and good image quality.

Initially, the VC scheme [11] is applied only to binary image shares later it is extended to gray scale share images. Many authors are proposed generalizations to the gray scale image shares and invented Extended Embedded VC scheme for Color images. Working on color images in VC scheme does not stopped just by invention of Color EVCS it also extends to 2-out-of-2 or 2-out-of-secure Color VC scheme [9], which uses a lattice structure to define the mixing result of arbitrary two colors and further extended too many colors. All of these VC schemes for color images produce random pattern shares. The author's researches on VC and EVC schemes and Color EVC Schemes are as follows [15] from the Figure 1 and Figure 2 respectively.

AUTHOR		INVENTION
Blonde	----- >	VC schemes with general structures for grayscale share images
Attendees	----- >	EVC scheme in which shares contain not only the meaningful images
Wang	----- >	Generalized the Attendee's scheme using concatenation of basis metrices and the extended matrices collection to achieve more simpler deviation of basis matrices
Nakajima	----- >	Extended EVC to a scheme with natural grayscale images to improve the image quality
Zhou	----- >	Used Halftoning methods to produce good quality halftone shares in VC
Fu	----- >	Generated Halftone shares that carry visual information by using VC and watermarking methods
Myodo	----- >	Proposed a method to generate meaningful Halftone images using threashold arrays
Wang	----- >	Produced Halftone shares showing meaningful images by using error diffusion techniques. This scheme generates more pleasing Halftone shares owing to errors diffused to neighbor pixels.

Figure 1: Different methods of VC and EVC generations

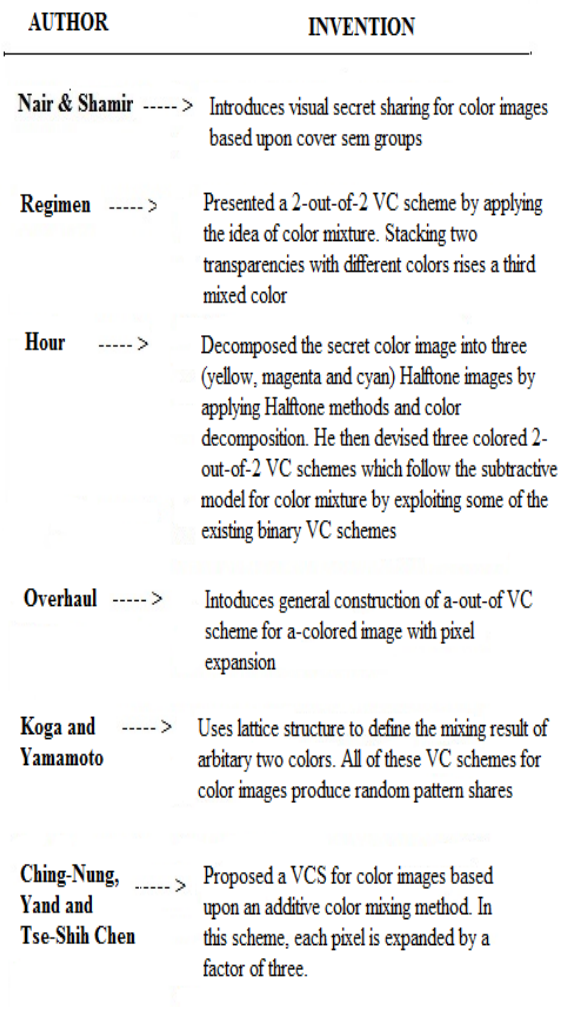

Figure 2: Different methods of Color VCS generations

VC and EEVCS schemes show good results for black and white or gray scale images. However, they are not sufficient to be applied directly to color shares due to different color structures. VIP synchronization and error diffusion used to attain a color visual cryptography encryption method that produces shares with high visual quality. VIP synchronization retains the positions of pixels carrying visual information of original images throughout the color channels and error diffusion generates shares pleasant to human eyes. Comparisons with previous approaches shows how the superior performance of the new method.

In a-out-of-scheme of VC, a secret binary image is cryptographically encoded into shares of random binary patterns. The shares are Xeroxed onto transparencies, respectively, and distributed amongst participants, one for each participant. No participant knows the share given to another participant. Any or many participants can visually reveal the secret image by superimposing any transparencies together.

Visual Cryptography for gray-level images by dithering technique [14] through Halftoning algorithm [6] and logical OR operations to generate meaningful shares. EEVCS uses DEGGA algorithm [3] which embedded large amount of information to enhance a layer of security through mutation (mutual XOR). For Color EVCS, there are different methods of VC [15] [7] [12] and uses XOR operation [8].

In the EEVCS technology, the receiver identifies an image, which is not the correct image that is, while transmitting image the sender will encrypt the image into two or more transparencies of the same image. The encrypted images are in the format of GIF or PNG. The encrypted transparencies can be saved in the machine and can be sent to the intended participant.

Keeping secret is always an important issue in many applications in the fields of Visual Cryptography [13] [2]. Two major approaches to this aim are information hiding and secret sharing. Visual cryptography provides these two.

Relation of secure and perceived visual quality of various Visual Cryptographic schemes are shown in Table 1.

Table 1: Comparisons of Image Security and Quality in VC, EVC and Color EVC Schemes.

Technique	Algorithm	Security	Image Quality
VCS	Halftoning	low	medium
EVCS	DEGGA	Medium	low
Color EVCS	VIP (multipixel)	high	high

The traditional VCS algorithm gives a best quality of images after decryption but due to color inconsistency across color channels, the EVCS produce shares with low visibility which leads to low image quality to human perception. Whereas modern techniques that are applied to Color Extended Visual Cryptography give high quality of decrypted images by using randomly generated shares using VIP.

The relation between the keys, shares, random numbers in VC, EVCS and Color EVCS respectively and security are shown in the below graph, as Figure 3.

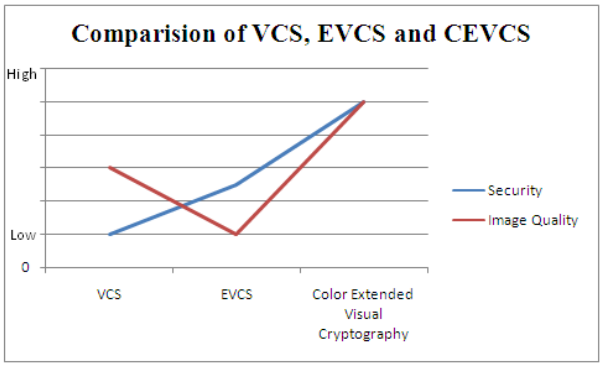

Figure 3: Relationship of VCS, EVCS and Color EVC Schemes

Peak Signal-to-Noise Ration (PSNR) [6] [4] [5], is an engineering term for the ration between the maximum possible power of signal and the power of computing noise that affect the fidelity of its representation. Because many signals have a wide dynamic range and it is usually expressed in terms of logarithmic decibel scale.

Consider the two parameters security and image quality, as the number of shares, keys and random numbers are increased the security in VCS, EVCS and Color EVCS respectively.

2. CONCULSION

The shares generated in VC, EEVC and Color EVC schemes are meaningful transparency shares, and the stack of qualified subset of shares will recover the secret image quality without the aid of computers. Each method follows their own approaches for encryption and decryption processes to provide security and image quality. The relation between Security and Image quality is based on the number of random shares and the PSNR ration of corrupting the noise that affects the quality of reconstructed image shares. The results of this paper are based on the observations on the implementation of all the three VC techniques. Security and perceived image quality are better in Color EVCS when compared to Gray level VCS and Embedded Extended VCS.

3. REFERENCES

[1] M. Naor, A. Shamir, 1994. "Visual Cryptography". Lecture Notes in Computer Science, Vol. 950, pp. 1-12. http://link.springer.com/chapter/10.1007%2FBFb0053419

[2] Jim Cai, 2003. A Short Survey on Visual Cryptography Schemes. Technical Paper. CiteSeerx, Penn State University, doi: 10.1.1.85.3060. http://www.cs.toronto.edu/~jcai/paper.pdf

[3] J.K Mandal, A. Khamuri, 2011. A Data Embedding Technique for Gray scale Image using Genetic Algorithm (DEGGA). IEEE sponsored International Conference on Communication, Computing and Security, Proceedings by Excel India Publishers. ISBN-978-93-80697-505, NIT Rourkela, 7-9 January 2011, pp. 19-22, (SP_2011_2001). http://jkmandal.com/pdf/DEGGA.pdf

[4] Nakajima, M. and Yamaguchi, Y., 2002. Extended Visual Cryptography for Natural Images, WSCG02, 303. http://wscg.zcu.cz/wscg2002/papers_2002/a73.pdf

[5] Anuprita Mande, Manish Tibdewal, 2013. "A Fast Encryption Algorithm for Color Extended Visual Cryptography" International Journal of Emerging Technology and Advanced Engineering. ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 4, April 2013. http://www.ijetae.com/files/Volume3Issue4/IJETAE_0413_64.pdf

[6] T. Rajitha, P. Pradeep Kumar, V. Laxmi, 2012. Construction of Extended Visual Cryptography Scheme for Secret Sharing. International Journal of Computer Science and Network (IJCSN) Volume 1, Issue 4 (August 2012), ISSN 2277-5420. http://ijcsn.org/IJCSN-2012/1-4/IJCSN-2012-1-4-56.pdf

[7] Mohsen Heidarinejad, K. N. Plataniotis, Edward S. Rogers. 2007. A Karnaugh Map Based {2, 2} Visual Cryptographic Scheme for Color Images. Technical Paper. University of Toronto. April 3, 2007.

[8] Wang Dao-Shun, Zhang Lei, Ma Ning and Huang Lian-Sheng. Secret Color Images Sharing Schemes based on XOR operation. Technical Paper. Tsinghua University, Beijing, 100084, China. http://eprint.iacr.org/2005/372.pdf

[9] H. Koga, H. Yamamoto, 1998. Proposal of a Lattice-based Visual Secret Sharing Scheme for Color and Gray Scale Images. IEICE Transaction on Fundamentals, Vol. E81-A (6):1262-1369. http://hirosuke.it.k.u-tokyo.ac.jp/files/abst/pdfs/E81-A-6-1262.pdf

[10] Adi Shamir, 1979 "How to share a secret". Computer Communications. ACM, vol. 22, no.11, pp. 612-613, doi:10.1145/359168.359176. http://www.iacr.org/archive/asiacrypt2001/22480554.pdf

[11] M. Naor, A. Shamir, in: M. Lomas, ed., Visual Cryptography II: Improving the Contrast via the Cover Base, Presented at Seurity in Communication Networks, AmalE, Italy, September 16-17, 1996. Lecture Notes in Computer Science, Vol. 1189, Springer, Berlin, 1997, pp.197-202. Available also at Theory of Cryptography Library, Report 96-07. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.21.4631&rep=rep1&type=pdf

[12] Sozan Abdulla, 2010. "New Visual Cryptography Algorithm for Colored Image". Journal of Computing, Vol. 2, Issue 4 (21-25), April 2010, ISSN: 2151-9617. http://arxiv.org/ftp/arxiv/papers/1004/1004.4445.pdf

[13] L. W. Hawkes, A. Yasinsac, C. Cline, 2000. An Application of Visual Cryptography to Financial Documents. Technical Paper. Security and Assurance in Information technology Laboratory, Florida State University, Tallahassee, FL 32306-4530. http://websrv.cs.fsu.edu/research/reports/TR-001001.pdf

[14] Chang-Chou Lin, Wen-Hsiang Tsai, 2003. Visual Cryptography for Gray-level Images by Dithering Techniques, Pattern Recognition Letters 24 (2003) 349-358. ELSEVIER. Available at Computer Science Web, powered by SCIENCE DIRECT. http://www.cis.nctu.edu.tw/~whtsai/Journal%20Paper%20PDFs/Lin_&_Tsai_PRL_2003.pdf

[15] Young-Chang Hou, 2003. Visual Cryptography for Color Images. Technical report. Pattern recognition 36 (2003) 1619-1629. Journal of the Pattern recognition society, PERGAMON. Published by ELSEVIER. http://csis.bits-pilani.ac.in/faculty/murali/netsec-10/seminar/refs/muralikrishna3.pdf