Visual Cryptography Comparative Parameters and Research Areas

Jyoti Rao,
Research scholar of JJTU , Rajasthan , India
jyoti.aswale@gmail.com
, Dr. Vikram Patil
Research guide at JJTU , Rajasthan , India & Principal K.B.P. College of Engg.,Satara Maharashtra

Abstract— Visual cryptography is a technique of information security which is simpler and easy to decrypt by human visual system without any computational aid. Visual cryptography uses simple algorithm unlike the complex, computationally intensive algorithms used in other techniques of traditional cryptography. VC encrypts secret image into shares such that stacking the minimum desired no. of shares reconstructs the secret image. Shares are usually presented in transparencies. In this survey, we will summarize the latest developments of VCS since its inception, the main research work in this area, the current problems and possible solutions for them. Directions for future VC work along with its applications will also be studied.

Index Terms— Cheating Prevention,Halftoning, Multiple secrete sharing, Pixel Expansion, Visual Cryptogrpahy, Visual Secret sharing, Staking.

1 INTRODUCTION

Even though the computer technology is so advanced and the effort of making every system to be computerized and automated is being done, thus security becomes a core issue. Still using computer to decrypt information does not make sense in some situations. For example at highly influential event security guard checks for a badge of an invitee or a secret agent decrypts an urgent secret at some place where no electronic devices are available In these situations human visual system is most convenient and easy to available tool to do checking and secret recovery.

Secret sharing using visual cryptography is different from typical cryptographic secret sharing scheme. VSS allows each party to keep portion of secret and provides a way to know at least part of secret. Encryption using multiple keys is a possible solution. However this solution requires a large number of keys resulting into troublesome management of no. of keys.

Visual cryptography is a desirable scheme as it indicates both the idea of perfect secrecy and very simple mechanism to decrypt secret. Visual cryptography uses the idea of hiding secret into shares so as while decrypting it uses the idea of superimposing transparencies which allows construction of original secret image.

This survey is organized as follows: Section 2 details the traditional visual cryptography scheme and elaborates on the current work still being done in this area, specifically the most recent improvements. In general, these schemes primarily deal with binary images and noisy random shares. Extended forms of VC are also discussed within this section which attempt to remove the suspicion of encryption within the shares. Section 3 elaborates the VCS using random grid and probabilistic VCS is explained well. Section 4 focuses on half toning, grayscale and color visual cryptography. Section 5 gives insights into work done under multiple secret sharing in VCS. Section 6 concentrates on cheating prevention within VC along with cheating immune VC schemes. These schemes attempt to have some type of authentication or verification method which gives some clue as to the real hidden secret within a given set of shares. Performance measurements of various visual cryptography schemes are analyzed in Section 7 and the summary and future work are discussed within Section 8, along with the final conclusion.

A. Traditional Visual cryptography:

In 1994, Naor and Shamir proposed the basic model of visual cryptography scheme which can decode concealed image into number of shares without any cryptographic complex computation. When the k shares are stacked together, the human eyes do the decryption without any knowledge of cryptography and without performing any computations whatsoever. This is advantage of visual cryptography over the other popular conditionally secure cryptographic schemes. It assumes that the image is a collection of black and white pixels, each pixel is handled individually and it should be taken into account that the white pixel represents the transparent color. One disadvantage of this is that the decryption process is lossy, so affects contrast. The relative difference in Hamming weight between the representation of white and black pixels signify the loss in contrast of the recovered secret. The encryption problem is expressed as a k out of n secret sharing problem. Given the image, n transparencies are generated so that the original image is visible if and only if any k of them are stacked together otherwise image remains. [1]

B. Extended visual cryptography schemes

Ateniese et al. proposed a technique based on an access structure which contains two types of sets, a qualified access structure Γ_{Qual} and a forbidden access structure Γ_{Forb} in a set of n

participants. The technique encodes the participants in that, if any set, which is a member of the qualified access structure, are superimposed, then only the secret message is revealed. The proposed scheme has two techniques to construct visual cryptography schemes for general access structures.[2].

The pixel expansion problem that occurred in previous VCS scheme using general access structure was solved by the new algorithm proposed by Lee and Chiu [2]. The extended VC algorithm for GAS which adds a meaningful cover image in each share does not generate noisy pixels. This approach consists of two phases. In the first phase, based on a given access structure, meaningless shares are constructed using an optimization technique. In the second phase, cover images are added in each share directly by a stamping algorithm. It formulates the construction problem of VCS for general access structures as a mathematical optimization problem such that the problem can be solved by optimization techniques. Authors have developed a hybrid method for EVCS constructions. By adopting the proposed stamping algorithm, all existing VC schemes can be modified to form their extended VC schemes without redesigning codebooks. The advantage of EVCS is the modularity. Each phase in the encryption procedure is less coherent, so it can be individually designed and also can be replaced separately. The second advantage is the first phase of the proposed algorithm: this phase is applicable not only to the extended VC schemes but also to the conventional VC schemes. The third advantage is that because the density of the cover images is adjustable, it is very helpful for modifying the display quality of the cover images. [3].

C. Size invariant VCS

The first paper based on image size invariant VCS proposed by Ito et al. removes the need of pixel expansion. This scheme uses (k,n) scheme where m i.e. number of sub pixels in shared secret equals to one. The structure of this scheme is described by a Boolean n-vector $V=[v_1,\ldots,v_n]$ where v_i denotes the color of the pixel[0- white, 1[black]. The original secret is reconstructed using traditional ORing method. As in (k,n) scheme it also uses n ×m matrices[4].

The aspect ratio invariant scheme proposed by Yang and Chen has reduced the number of pixel expansions to a great extent. This scheme results into size of shares closer to the original share with aspect ratio without introducing distortion [5]. Yang and Chen further generalized the research work in aspect ratio invariant scheme to resolve the problem of pixel arrangement However, resizing the black-and-white image will lose the informative information of pixel. Thus, the proposed ARIVCS is based on image filtering and resizing. The trivial solution has the same performance like the existing ARIVCS, and meantime does not require dummy pixels and the mapping pattern [6].

D. Quality evaluation

A possible option for improving the efficiency of VC is to use the XOR operation. This method will not allow stacking of the shares on transparencies but it will improve the overall share quality. Threshold Visual Secret Sharing schemes associated to XOR-based VC systems is investigated in this paper. Hollmann et al. shown that *n* out of *n* schemes with optimal resolution and contrast exist, and that *(2,n)* schemes are equivalent to binary codes. It can be seen that these schemes have much better resolution than their OR-based counterparts. Secondly, Hollmann et al provided two explicit constructions for general *k* out of *n* schemes. Finally, they derive bounds on the contrast and resolution of XOR-based schemes. It follows from these bounds that for $k<n$, the contrast must be smaller than one. Moreover, the bounds imply that XOR-based *k* out of *n* schemes for even *k* are fundamentally different from those for odd *k*. The scheme has properties, such as, good resolution and high contrast. The scheme can be applied to color images as well. [7]

E. Random-grid and Probabilistic VCS:

To deal with size invariant schemes and the problem of pixel expansion the probabilistic VCS is proposed in which frequency of white pixels is used to show the contrast of reconstructed secret. The scheme is non-expansible [i.e. Size of secret pixel is same as that of original secret] can be easily constructed using traditional VCS. In PVCS, the frequency of white pixels in a white area of the reconstructed image should be higher than that in a black area. [8]

Another secure VCS is random grid (RG), which was originally introduced by Kafri and Keren in Ref. [9]as a solution for sharing a binary secret image into two noise-like random grids. When superimposing two random grids, only two stacked white pixels will let the light through it, while other stacked results yielding a black pixel stops the light.[9]

Many researchers further worked on random-grid technologies introducing new techniques like (2,n)-RG, (n,n)-RG, the 2-secrecy level (2, 3) incremental RG (IRG), and (k,n)-RG.[10,11,12,13]

F. Halftone, grey-scale and color VCS:

Z. Zhou, G. R. Arce, and G. Di Crescenzo introduced halftone visual cryptography. The method that uses the density of the net dots to simulate the gray level is called "Halftone". The halftone visual cryptography is proposed to achieve visual cryptography via half toning. Based on the blue-noise dithering principles, the proposed method utilizes the void and cluster algorithm to encode a secret binary image into halftone shares (images) carrying significant visual information. The simulation shows that the visual quality of the obtained halftone shares is observably better. Every pixel of the transformed halftone image has only two possible color levels (black or white). Because human eyes cannot identify too tiny printed dots and, when viewing a dot, tend to cover its nearby dots, we can simulate deferent gray levels through the density of printed dots, even though the transformed image actually has only two colors—black and white. [14]

For introducing efficiency within color VCS Shyu proposed this scheme [15].The proposed scheme follows Yang and Laih's[16] color model. The model considers the human visual system's effect on color combinations out of a set of color sub-pixels. This means that the set of stacked color sub-pixels would look like a specific color in original secret image. As with many other visual cryptography schemes, pixel expansion is an issue. However Shyu's scheme has a pixel expansion

of $(log_2 c)$ which is superior to many other color visual cryptography schemes especially when c, the number of colors in the secret image becomes large. An area for improvement however would be in the examination of the difference between the reconstructed color pixels and the original secret pixels. Having high quality color VC shares would further improve on the current schemes examined within this survey, this includes adding a lot of potential for visual authentication and identification.[15]

G. Multiple secret sharing :

Wu and Chen introduced the sharing of two secret image using two shares. The two secrets were hidden in a way that first secret can be reconstructed by stacking two shares while second secret can be reconstructed by rotating first share anticlockwise by angle of θ. The value of θ can be 90°, 180° or 270°[17]. Wu and Chang refined the idea of Wu and Chen by encoding shares in circular form to remove restriction of θ as to be 90°, 180° or 270°[18].

S J Shyu et al [19] were first to advise the multiple secrets sharing in visual cryptography. This scheme encodes a set of $n \geq 2$ secrets into two circle shares. The n secrets can be obtained one by one by stacking the first share and the rotated second shares with n different rotation angles.

Tzung-Her Chen et al [20] invented a multi-secrets visual cryptography which is extended from traditional visual secret sharing. The codebook of traditional VCS is implemented to generate shares macro block by macro block in such a way that multiple secret images are turned into only two shares and decrypts all the secrets one by one by stacking any two shares in a way of shifting. This scheme can be used for multiple binary, gray and color secret images with pixel expansion value m=4.

H. Cheating immune VCS:

Hu and Tzeng recognized cheating problem in VC and extended VC. They considered the attacks of malicious parties who may deviate from the scheme in any way. They presented three cheating methods and applied them on attacking existent VC or extended VC schemes. They improved one cheat-preventing scheme. They proposed a generic method that has property of cheating prevention. [21]

Based on a trusty third party, a co-cheating prevention visual cryptography scheme (CCPVCS) is proposed by Bin et al. The pixel expansion is small and the recovered secret image is good for viewing. Through a peculiar verification share and n optional verification shares, the truth of several shares can be detected simultaneously. However, the number of verification shares which kept by the third party is large .[22]

Chen, Horng and Tsai proposed (n, n) threshold visual cryptography scheme for cheating prevention to improve the generic transformation for cheating prevention scheme (GTCP). The cheating problem in the GTCP is analyzed, and presented the cheating method that applied it to attack on the GTCP. Then constructed the matrices for cheating prevention with following features: (a) each participant can't gain any useful information from his shares, (b) each pixel has the same number of black and white sub pixels in the secret share and in the verification share, (c) one's verification image will be recovered by stacking of his verification share and the secret share, (d) the secret image can be revealed by stacking all the secret shares [23]. Furthur , Yu-Chi Chen, Gwoboa Horng and Du-Shiau Tsai proposed an (n, n) VCS for cheating prevention, in which each participant holds his own private verification image, to improve the GTCP. This scheme is implemented by constructing four matrices, two ones are used for sharing the secret image and the two others are used for sharing the verification image.[24]

C.H. Lin proposed a new cheating–preventing scheme to benefit from a combination of two general VC codebooks. With the hybrid codebook, the verification images are skillfully hidden in the shares to check whether the intended share is fake. In such a way the cheating attack in VSS can be detected.[25]

II. PERFORMANCE ANALYSIS OF VCS :

Various parameters are recommended by researchers to evaluate the performance of visual cryptography schemes. Those are pixel expansion, contrast, accuracy, computational complexity and average light transmission. The following table can be referenced for comparison of various VCS so far by evaluating performance measures.

III. CONCLUSION:

In this paper following are identified and has scope of research yet much work have already done : 1) Contrast improvement ,2) Share size improvement, 3) pixel expansion , 4) Ability of sharing single/ multiple secret images , 5)Efficiency, 6) Security.

This paper has tried to include most of the work done in above areas mentioned and performance evaluation of fewer schemes is carried out.

More schemes providing optimum contrast and less pixel expansion for both single and multiple secret sharing scheme should be developed.

The security is also an important area where scope enabling less pixel expansion along with maintaining contrast and cheating prevention facility can be researched further with novel less complex schemes.

Sr. no	Author	Year	Number of secret images	Pixel expansion	Quality of reconstructed image	Construction complexity	Image format	Type of share generated
1	Naor and Shamir	1994	1	4	Low contrast	No	binary	random
2	Wu and Chen	1998	2	4	Average contrast	No	binary	random
3	Hsu et al	2004	2	4	Average contrast	No	binary	random
4.	S. J. Shyu et al	2007	n(n>=2)	2n	Average contrast	No	binary	random
5.	S.J.Shyu	2006	1	$(log_2 c)$	Average contrast	No	Color	random
6	C.N. Yang	2004	(k,n)	1	Average contrast	No	binary	random
7	Kafri and Keren	1987	2	1	Average light transmission	No	binary	random
8	Hu and Tzeng	2006	(k,n)	2 × 2 + 2	Average contrast	No	binary	random
9	D.S. Tsai, T.H. Chen, and G. Horng	2007	()	2×2	Average contrast	Yes	binary	random
10	Chih-Hung Lin et al.	2014	(2,3)and (2,2) Hybrid codebook	2× 2	Average contrast	No	binary	random

REFERENCES:

1. Naor, M., Shamir, A.: Visual cryptography. In: De Santis, A. (ed.) EUROCRYPT1994. LNCS, vol. 950, pp. 1–12. Springer, Heidelberg (1994).

2. Ateniese, G., Blundo, C., De Santis, A., Stinson, D.R.: Visual cryptography for general access structures. Information and Computation 129(2), 86–106 (1996).

3. KH Lee, PL Chiu.: An Extended Visual Cryptography Algorithm for General Access Structures. IEEE Transactions on Information Forensics and Security vol. 7, no. 1, (2012).

4. Ito, R., Kuwakado, H., Tanaka, H.: Image size invariant visual cryptography. IEICE Transactions E82-A(10), 2172–2177 (1999).

5. Yang, C.N., Chen, T.S.: Aspect ratio invariant visual secret sharing schemes with minimum pixel expansion. Pattern Recognition Letters 26(2), 193–206 (2005).

6. Ching-Nung Yang, Pin-Wei Chen, Hsiang-Wen Shih, Cheonshik Kim, Aspect ratio invariant visual cryptography by image filtering and resizing, Personal Ubiquitous Comput. 17(5)(2013)843–850

7. .Tuyls, P., Hollmann, H.D.L.,van Lint, J.H., Tolhuizen, L.M.G.M.:XOR-based visual cryptography schemes. Designs, Codes and Cryptography 37(1), 169–186(2005).

8. Yang, C.N.: New visual secret sharing schemes using probabilistic method. Pattern Recognition Letters 25(4), 481–494 (2004).

9. O. Kafri, E. Keren, Encryption of pictures and shapes by random grids, Opt. Lett. 12 (1987) 377–379.

10. T.H. Chen, K.H. Tsao, Visual secret sharing by random grids revisited, Pattern Recogn. 42 (2009) 2203–2217.

11. T.H. Chen, K.H. Tsao, Threshold visual secret sharing by random grids, J. Syst. Softw. (2011) 1197–1208.
12. S.J. Shyu, Image encryption by multiple random grids, Pattern Recogn. (2009) 1582–1596.

13. R.Z. Wang, Y.C. Lan, Y.K. Lee, S.Y. Huang, S.J. Shyu, L.T. Chia, Incrementing visual cryptography using random grids, Opt. Commun. (2010)4242–4249.

14. Z. Zhou, G. R. Arce, and G. Di Crescenzo, "Halftone visual cryptography," IEEE Trans. Image Process., vol. 15, no. 8, pp. 2441-2453, Aug. 2006. (Pubitemid 44089115).

15. Shyu, S.J., Huang, S.Y., Lee, Y.K.,Wang, R.Z., Chen, K.: Sharing multiple secrets in visual cryptography. Pattern Recognition 40(12), 3633–3651 (2007).

16. Yang, C.N., Laih, C.S.: New colored visual secret sharing schemes. Designs, Codes and Cryptography 20(3), 325–336 (2000).

17. Wu, C., Chen, L.: A study on visual cryptography. Master's thesis, Institute of Computer and Information Science, National Chiao Tung University, Taiwan, R.O.C. (1998).

18. Hsu, H.C., Chen, T.S., Lin, Y.H.: The ringed shadow image technology of visual cryptography by applying diverse rotating angles to hide the secret sharing. Networking, Sensing and Control 2, 996–1001 (2004).

19. S. J. Shyu, S. Y. Huanga,Y. K. Lee, R. Z. Wang, and K. Chen, "Sharing multiple secrets in visual cryptography", Pattern Recognition, Vol. 40, Issue 12, pp. 3633 - 3651, 2007.

20. Tzung-Her Chen, Kai-Hsiang Tsao, and Kuo-Chen Wei, "Multi-Secrets Visual Secret Sharing", Proceedings of APCC2008, IEICE, 2008.

21. Hu, C.M., Tzeng W.G.: Cheating prevention in visual cryptography. IEEE Transactions on Image Processing 16(1), 36–45 (2007).

22. Bin YU, Jin-Yuan LU, Li-Guo FANG.: A Co-cheating Prevention Visual Cryptography Scheme. Third International Conference on Information and Computing (ICIC), Vol.4, 157 – 160 (2010).

23. Qin Chen, Wen-Fang Pengo Min Zhang, Yi-Ping Chu. : An (n, n) threshold Visual Cryptography Scheme for Cheating prevention. Third IEEE International Conference on Computer Science and Information Technology (ICCSIT), Vol. 8, 587 – 592(2010).

24. Yu-Chi Chen, Student Member, IEEE, Gwoboa Horng, and Du-Shiau Tsai "Comment on Cheating Prevention in Visual Cryptography" IEEE Transactions on Image Processing, Vol. 21, No. 7, July 2012.

25. Chih-Hung Lin et al. : Multi-factor cheating prevention in visual secret sharing by hybrid codebooks. Vis. Commun. Image R. 25 (2014) 1543–1557.

26. D.S. Tsai, T.H. Chen, and G. Horng. A cheating prevention scheme for binary visual cryptography with homogeneous secret images, Pattern Recognition, Vol. 40 No. 8, 2007, pp. 2356-2366.

27. Weir, Jonathan, and WeiQi Yan. "A comprehensive study of visual cryptography." *Transactions on data hiding and multimedia security V*. Springer Berlin Heidelberg, 2010. 70-105.