International Journal of Computer Science and Business Informatics

IJCSBI.ORG

A Review on Various Visual Cryptography Schemes

Nagesh Soradge
Sinhgad College of Engineering,
Vadgaon. Pune, India.

Prof. K. S. Thakare
Associate Professor
Sinhgad College of Engineering,
Vadgaon. Pune, India.

ABSTRACT
Cryptography is study of transforming information in order to make it secure from unintended recipients or use. Visual Cryptography Scheme (VCS) is a cryptography method that encrypts visual information (picture, printed text, handwritten notes) such that decryption can be performed using human visual system. The idea is to convert this visual information into an image and encypher this image into *n* different shares (known as sheets). The deciphering only requires selecting some shares out of *n* shares. The intent of this review paper is to contribute the readers an overview of the basic visual cryptography scheme constructions as well as continued work in the area. In inclusion, we also review some applications that take advantage of such secure system.

Keywords
Visual cryptography scheme (VCS), Pixel expansion, Contrast, Security, Accuracy, Computational complexity

1. INTRODUCTION
Various sensitive data such as credit card information, personal health information, military maps and personally identifiable information are transmitted over the Internet. Multimedia information is also transferred over the Internet conveniently, with the advancement of technology. Therefore, the protection of the secret information has become critical research. While using secret images, hackers may get help of weak link over network to suspect the information. To solve the problem of protection of secret images, many image secret sharing schemes have been formed. A new information security technique called visual cryptography scheme was invented by Naor et al in 1994 [1]. Human visual system decode secret (handwritten notes, printed text and pictures etc.) directly without performing any computations. This scheme excludes complex computation problem in decryption and the secret images

can be reinstated by stacking operation. This property of visual cryptography is useful for less computation load requirement.

Visual cryptography was presented for the problem of secret sharing. Secret sharing is one of the early issues to be considered in cryptography. In particular, suppose 4 smart robbers have deposited their loot in a bank account. These robbers do not trust each other and they do not want a single robber of themselves to withdraw the loot and escape. However, they assume that withdrawing loot by at least two robbers is considered a loyalty. Therefore, they decided to encrypt the bank code (with a trusted machine) into 4 partitions so that at least two partitions can reconstruct the code and the partitions are distributed themselves. Since the robbers will not have a machine with them to decrypt the bank code when they want to withdraw the loot, they want to be able to decrypt visually. The partition should not yield any information about code. Nonetheless, by taking any two or more partitions, stacking them together and aligning them, the code should be constructed. The solution to above complication is given by visual cryptography scheme.

Simplest visual cryptography scheme is given by following structure. A secret image will be made up of a gathering of black and white pixels, where each pixel is served independently [1]. To encrypt the image, we split the image into n modified versions such that each pixel in a share subdivides in *m* black and white sub-pixels [1]. For deciphering the image, we pick a subgroup S of those *n* shares. If S is a "qualified" subset, then stacking all these shares will allow recovery of the image.

This paper introduces the construction of (*k*, *n*) threshold VCS along with some parameters used to describe the model. Later, this paper provides overview of various visual cryptography schemes. To meet the demand of multimedia information, gray and color image format should be enciphered by the schemes. Performance measures like security and computational complexity that affect the efficiency of visual cryptography are also discussed.

The rest of the paper is structured as follows. Section II will describe the model for the construction of (*k*, *n*) threshold VCS. Section III provides overview of black and white VCS. Section IV elaborates color VCS. Applications of VCS are included in section V. Performance of visual cryptography schemes are analyzed in section VI and conclude the paper in section VII.

2. MODEL FOR ENCRYPTION

VCS model as well as (*k*, *n*)-threshold VCS scheme that was proposed by Naor and Sharmir [1] formally defined as:

Definition 1→ *Hamming Weight*: The number of non-zero symbols in a series of symbols [1]. In a binary representation of number, Hamming weight is the number of '1' bits in the binary series.

Definition 2→ *OR-ed k-vector*: Given a j×k matrix, it is the k-vector where each and every tuple is made up of the result of executing Boolean OR operation on its analogous j×1 column vector [1].

A VCS scheme is a 6-tuple (d, α, V, S, m, n). It supposes that each pixel arises in n versions called shares and each share representing its corresponding transparency. Each share is a group of m black and white sub-pixels. This new generated structure can be described by an $n \times m$ Boolean Matrix $S = [S_{ij}]$ where $S_{ij} = 1$, iff the jth sub pixel in the ith share is black. Hence, the grey degree of the combined share which is obtained by overlapping the transparencies is proportional to the Hamming Weight $H(V)$ of the OR-ed m-vector V [1]. This grey degree is usually depicted by the visual system as black if $H(V) \geq d$ and as white if $H(V) < (d - \alpha m)$ for some fixed threshold $1 \leq d \leq m$ and relative difference $\alpha > 0$ [1]. αm is the difference between the minimum $H(V)$ estimate of a black pixel and the maximum permitted $H(V)$ estimate for a white pixel is called the contrast of a VCS scheme [1].

VCS Schemes where a subgroup is permitted if and only if its cardinality is k are called (k, n)-threshold visual cryptography schemes [1]. A formation of (k, n) - threshold VCS consists of two collections of $n \times m$ Boolean matrices ζ_0 and ζ_1, each of size r [1]. To produce a white pixel, we randomly choose one of the matrices in ζ_0 and to produce a black pixel, we randomly choose a matrix in ζ_1 [1]. The chosen matrix will define the color of the m sub-pixels in each one of the n transparencies [1]. Meantime, the solution will be correct if the following three conditions are satisfied:

1) For any matrix S in ζ_0, the "OR" operation on any k out of the n rows satisfies $H(V) \leq d - \alpha m$.
2) For any matrix S in ζ_1, the "OR" operation on any k out of the n rows satisfies $H(V) \geq d$.
3) For any subset $\{i_1, i_2 \ldots i_q\}$ of $\{1, 2 \ldots n\}$ along with $q<k$, the two collection of $q \times m$ matrices B_t obtained by restricting each $n \times m$ matrix in ζ_t (where t= {0, 1}) to rows $i_1, i_2 \ldots i_q$ are indistinguishable in the sense that they contains exactly the identical matrices with the identical frequencies [1]. In other words, any $q \times n$ matrices $S^0 \in B_0$ and $S^1 \in B_1$ are same up to a column permutation.

Condition (1) and (2) defines the contrast of a VCS and condition (3) states the security property of (*k*, *n*)-threshold VCS.

Let us consider an instance of (3, 3)-threshold VCS formation where, each pixel is divided into 4 sub-pixel (*m*=4). According to the definition, ζ_0 and ζ_1 are defined as following:

ζ_0 = {all matrices obtained by permuting the columns of $\begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}$ }

ζ_1 = {all matrices obtained by permuting the columns of $\begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}$ }

To encode a white pixel, the encoder needs to randomly choose one matrix from ζ_0 to form the sub-pixels in three shares accordingly. Meantime, to encode a black pixel the encoder needs to randomly pick one matrix from ζ_1. It is not so hard to check that this construction will yield a relative contrast of 0.25. The encoding of a black pixel needs altogether 4 black sub-pixels where a white pixel needs 3 black sub pixels and 1 white sub-pixel. Consequently, when the three shares stack together, the result is either dark grey, which we use to substitute white or completely black, which we use to substitute black. Readers can verify the security property of (3,3) threshold VCS by taking any two rows from any $S^0 \in B_0$ and $S^1 \in B_1$ and convince themselves that superposition of any two transparencies will always result in 3 white sub-pixels and 1 black sub-pixel.

The construction of arbitrary (*k*, *k*) and (*k*, *n*)-threshold VCS is out of the scope of our paper. Therefore we only state the result of such construction.

Theorem 1 → *In any (k, k)-threshold VCS scheme construction,* $m \geq 2^{k-1}$ *and* $\alpha = 1/2^{k-1}$.

Theorem 2 → *There exists a (k, n)-threshold VCS scheme with m = nk.2k-1 and* $\alpha = (2e)\text{-}k/\sqrt{2\pi k}$

Notice that the first theorem states the optimality of (*k*, *k*) scheme where the second theorem only states the existence of a (*k*, *n*) VCS with given parameters. H. C. Hsu et al [2] showed a more optimal (*k*, *n*) VCS construction with a smaller *m*.

3. GREY SCALE VISUAL CRYPTOGRAPHY

A. Sharing Only One Secret

If pixel is white, one of the upper two rows of Table 1 is selected to produce Share1 and Share2. In a similar way, if pixel is black, one of the lower two rows of Table 1 is selected to produce Share1 and Share2. Here pixel p of each share is encoded into two white and two black pixels. Whether each share alone is white or black, it does not give hint about the pixel p. Secret image is displayed only when both shares are overlapped. This encrypting scheme to share a binary image into two shares Share1 and Share2 is suggested by Naor et al [1].

Table 1. Scheme for encoding a binary pixel into two shares

Pixel	Probability	Share1	Share2	Share1 XOR Share2
	50%			
	50%			
	50%			
	50%			

To decrypt the concealed messages, embedding images can be overlapped. Balancing the performance between pixel expansion and contrast Liguo Fang [3] proposed a (2, *n*) scheme based on combination. To conceal a binary image into two meaningful shares Chin-Chen Chang et al [4] recommended spatial-domain image hiding schemes. These two secret shares are embedded into two gray level cover images [4]. Threshold visual secret sharing schemes mixed XOR and OR operation with reversing and based on binary linear error correcting code was suggested by Xiao-Qing and Tan [5]. The above schemes have disadvantage that only one set of sensitive messages can be enclosed, so to share large amounts of sensitive messages a number of shares have to be produced.

B. Sharing Many Secrets

C. C. Wu et al [6] firstly presented the visual cryptography schemes to share two secret images into two shares. They concealed two secret binary images into two arbitrary Shares A and B [6]. The first secret can be obtained by stacking the two shares and it is denoted by A ⊗ B. The second secret can be seen by first rotating A in anti clock wise direction. They designed the rotation angle Θ to be 90◦. However, it is easy to obtain that Θ can be 180 ◦ or 270◦. To control the angle restriction of scheme of C. C. Wu, Hsu et al [2] proposed a scheme to conceal two secret images into two rectangular share images with inconsistent rotating angles.

S. J. Shyu et al [7] firstly advised the two or more than two secrets sharing in visual cryptography. This scheme encrypts a set of $n \geq 2$ secrets into two circular shares. The n secrets can be recovered one after another by stacking the first share and second share is rotated with n discrete rotation angles. To encode unrestricted shapes of image and to eliminate the restriction of transparencies to be circular, a reversible visual cryptography scheme is recommended by Fang [8]. Jen-Bang Feng et al [9] proposed a visual secret sharing scheme for suppressing multiple secret images into two shares.

Tzung-Her Chen et al [10] proposed the multiple image encryption schemes by rotating random grids, without any pixel expansion. Jonathan Weir et al [11] suggested sharing multiple secrets using visual cryptography. A master key is produced for all the secrets. Correspondingly, secrets are shared using the master key and multiple shares are obtained. To provide more randomness for producing the shares, a secret sharing scheme depending on the rotation of shares is advised by Mustafa Ulutas et al [12]. This scheme produces rectangular shares, which are designed randomly. Stacking the two shares reproduces the first secret. After rotating the first share by 90° anticlockwise and stacking it with the second share regenerates the second secret.

A non-expansion reversible visual secret sharing method that does not need to define the lookup table was presented by Fang [13]. Zhengxin Fu et al [14] intended a rotation visual cryptography scheme for encryption of four secrets into two shares and recovering the reconstructed images without distortions. Rotation visual cryptography scheme construction was depending correlative matrices set and random permutation. Above mentioned all the schemes used to share the black and white secret images. To deal with colorful images researchers have been worked to share the colorful images.

4. COLORFUL VISUAL CRYPTOGRAPHY SCHEME

A. Sharing Only One Secret

Visual cryptography schemes were applied to only black and white images until the year 1997. Verheul and Van Tilborg [15] firstly developed colored VCS. With the concept of arcs colored secret images can be shared. In *c*-color VCS single pixel is translated into *m* sub pixels, and each sub pixel is split into *c* color regions. In each sub pixel, only one color region is colored, and all the other color regions are kept black. The color of one pixel depends on the combination between the stacked sub pixels. For a colored VCS with *c* colors, the pixel expansion *m* is $c \times 3$. Yang and Laih [16] improved the pixel expansion to $c \times 2$.

To share and transmit a secret color image and also to generate the meaningful share Chang and Tsai proposed color VCS [17]. For a secret color image two effective color images are chosen as cover images which are the exactly same size of the secret color image. Then according to a predefined Color Index Table, the secret color image will be concealed into two disguise images. One loss of this scheme is that extra space is required to assemble the Color Index Table.

To deal with this limitation Chin-Chen Chang et al [18] constructed a secret color image sharing scheme depending on modified visual cryptography. In this scheme size of the shares is decided; it does not change when the number of colors appearing in the secret image differs [18]. Although pixel expansion is set in this scheme, it is not suitable for true-color secret image. To share true-color image Lukac and Plataniotis [19] proposed bit-level based scheme by operating directly on bit-planes of a secret image.

S J Shyu [20] suggested a colour VCS for reducing pixel expansion which is a more efficient coloured Visual secret sharing scheme with pixel expansion of $|\log_2 c^* m|$ where *m* is the pixel expansion of the exploited binary scheme and *c* is the number of colour regions [20]. A cost effective VCS was developed by Mohsen Heidarinejad et al. [21] by considering colour image transmission over bandwidth constraint channels. The solution offers perfect reconstruction while producing shares with size smaller than that of the input image using maximum distance separable.

F. Liu et al [22] developed a colour visual cryptography scheme under the visual cryptography model of Naor et al [1] without pixel expansion. In this scheme, the increase in the number of colours of recovered secret image does

not increase pixel expansion. To increase the speed of encoding Haibo Zhang et al [23] presented a multi-pixel encoding which can encode unfixed number of pixels for each run.

B. Sharing Many Secrets

A multi-secrets visual cryptography anticipated by Tzung-Her Chen et al [24] which is enlarged from traditional visual secret sharing. This scheme can be used for multiple binary, gray and color secret images with pixel expansion of 4. The codebook of traditional visual secret sharing applied to generate share images macro block by macro block just as if multiple secret images are converted into only two share images and decode all the secrets one by one by superimposing two of share images in a way of shifting [24].

5. APPLICATIONS OF VCS

A secret-Ballot Receipts system depending on (2, 2) - threshold binary VCS was proposed by Chaum [26]. It produces an encrypted receipt to each voter which allows verifying the election result. The VCS principle can also be enforced in transferring important financial documents over Internet. VCRYPT is a sample of this type of system was presented by Hawkes et al [27]. VCRYPT can encrypt the original drawing document with a certain (k,n) VCS, then send each of the encrypted n shares independently through Emails to the recipient.

6. PERFORMANCE OF VISUAL CRYPTOGRAPHY SCHEMES

Several parameters are constructed by researchers to evaluate the performance of VCS. Naor et al [1] suggested two main parameters: pixel expansion m and contrast α. Pixel expansion m means the number of sub pixels in the generated shares which represents a pixel of the original input image. Pixel expansion represents the impairment in resolution from the original picture to the shared one. Contrast α refers to the relative difference in weight between combined shares that come from a white pixel and a black pixel in the original image.

Jung-San Lee et al [25] suggested security, accuracy and computational complexity as a performance measures. Security can be defined as if each share does not give information of the original image. Accuracy is considered to be the quality of the restructured secret image and evaluated by peak signal-to-noise ratio (PSNR) measure. Computational complexity is the total number of operators required both to produce the set of n shares and to reconstruct the original secret image.

7. CONCLUSION

In this paper, we briefly review the research of visual cryptography schemes as special cases of secret sharing methods among participants. In visual cryptography schemes the grey-scale VCS and colorful VCS both are studied according to the number of shares generated. Interesting applications are also studied. Further, formulated performance parameters of various visual cryptography schemes are evaluated.

REFERENCES

[1] Moni Naor and Adi Shamir, "Visual Cryptography", *advances in cryptology– Eurocrypt*, 1995, pp 1-12.

[2] H. C. Hsu, T.-S. Chen, Y.-H. Lin, "The Ring Shadow Image Technology Of Visual Cryptography By Applying Diverse Rotating Angles To Hide The Secret Sharing", *In Proceedings of the 2004 IEEE International Conference on Networking, Sensing & Control*, Taipei, Taiwan, March 2004, pp. 996–1001.

[3] Liguo Fang, BinYu, "Research On Pixel Expansion Of (2, n) Visual Threshold Scheme", *1st International Symposium on Pervasive Computing and Applications*, IEEE, 2006, pp. 856-860.

[4] Chin-Chen Chang, Jun-Chou Chuang, Pei-Yu Lin, "Sharing A Secret Two-Tone Image In Two Gray-Level Images", *Proceedings of the 11th International Conference on Parallel and Distributed Systems (ICPADS'05)*, 2005, pp. 300-304.

[5] Xiao-qing Tan, "Two Kinds of Ideal Contrast Visual Cryptography Schemes", *International Conference on Signal Processing Systems*, 2009, pp. 450-453.

[6] C.C. Wu, L.H. Chen, "A Study On Visual Cryptography", *Master Thesis, Institute of Computer and Information Science*, National Chiao Tung University, Taiwan, R.O.C., 1998.

[7] 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 , 2007, pp. 3633 - 3651.

[8] Wen-Pinn Fang, "Visual Cryptography In Reversible Style", *IEEE Proceeding on the Third International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIHMSP2007)*, Kaohsiung, Taiwan, R.O.C, 2007.

[9] Jen-Bang Feng, Hsien-Chu Wu, Chwei-Shyong Tsai, Ya-Fen Chang, Yen Ping Chu, "Visual Secret Sharing For Multiple Secrets", *Pattern Recognition Vol. 41*, 2008, pp. 3572 – 3581.

[10] Tzung-Her Chen, Kai-Hsiang Tsao, and Kuo-Chen Wei, "Multiple Image Encryption By Rotating Random Grids", *Eighth International Conference on Intelligent Systems Design and Applications*, 2008, pp. 252-256.

[11] Jonathan Weir, WeiQi Yan, "Sharing Multiple Secrets Using Visual Cryptography", *IEEE*, 2009, pp 509-512,.

[12] Mustafa Ulutas, Rıfat Yazıcı, Vasif V. Nabiyev, Güzin Ulutas, "(2, 2) - Secret Sharing Scheme With Improved Share Randomness", *IEEE*, 2008.

[13] Wen-Pinn Fang, "Non-Expansion Visual Secret Sharing in Reversible Style", *IJCSNS International Journal of Computer Science and Network Security*, VOL.9 No.2, February 2009, pp.204-208.

[14] Zhengxin Fu, Bin Yu, "Research on Rotation Visual Cryptography Scheme", *International Symposium on Information Engineering and Electronic Commerce*, 2009, pp 533-536.
[15] E. Verheul and H. V. Tilborg,"Constructions And Properties Of K Out Of N Visual Secret Sharing Schemes." *Designs, Codes and Cryptography*, 11(2), 1997, pp.179–196.
[16] C. Yang and C. Laih, "New Colored Visual Secret Sharing Schemes", *Designs, Codes and cryptography*, 20, 2000, pp. 325–335.
[17] C. Chang, C. Tsai, and T. Chen. "A New Scheme For Sharing Secret Color Images In Computer Network", Proceedings of International Conference on Parallel and Distributed Systems, July 2000, pp. 21–27.
[18] Chin-Chen Chang, Tai-Xing Yu, "Sharing A Secret Gray Image In Multiple Images", *Proceedings of the First International Symposium on Cyber Worlds (CW.02)*, 2002.
[19] R. Lukac, K.N. Plataniotis, "Bit-Level Based Secret Sharing For Image Encryption", *Pattern Recognition 38 (5)*, 2005, pp. 767–772.
[20] S.J. Shyu, "Efficient Visual Secret Sharing Scheme For Color Images", Pattern Recognition 39 (5), pp. 866– 880, 2006.
[21] Mohsen Heidarinejad, Amirhossein Alamdar Yazdi and Konstantinos N, Plataniotis "Algebraic Visual Cryptography Scheme For Color Images", *ICASSP*, 2008, pp. 1761-1764.
[22] F. Liu1, C.K. Wu X.J. Lin, "Colour Visual Cryptography Schemes", *IET Information Security*, vol. 2, No. 4, 2008, pp. 151-165.
[23] Haibo Zhang, Xiaofei Wang, Wanhua Cao, Youpeng Huang , "Visual Cryptography For General Access Structure By Multi-Pixel Encoding With Variable Block Size", *International Symposium on Knowledge Acquisition and Modeling*, 2008, pp. 340-344.
[24] Tzung-Her Chen, Kai-Hsiang Tsao, and Kuo-Chen Wei, "Multi-Secrets Visual Secret Sharing", *Proceedings of APCC2008, IEICE*, 2008.
[25] Jung-San Lee, T. Hoang Ngan Le, "Hybrid (2, N) Visual Secret Sharing Scheme For Color Images", 978-1- 4244-4568-4/09, *IEEE*, 2009.
[26] D Chaum, "Secret-ballot receipts: True voter-verifiable elections", *IEEE Security and Privacy*, 2004, pp.38-47.
[27] W. Hawkes, A. Yasinsac, C. Cline, An Application of Visual Cryptography to Financial Documents, technical report TR001001, Florida State University (2000).

This paper may be cited as:

Soradge, N. and Thakare, K. S., 2014. A Review on Various Visual Cryptography Schemes. *International Journal of Computer Science and Business Informatics, Vol. 12, No. 1, pp. 45-54*.