Two Step Share Visual Cryptography Algorithm for Secure Visual Sharing

N. Gowdham[1], S.D. Libin Raja[2], M. Sornalakshmi[3], M. Navaneetha Krishnan[4]
[1, 2]PG Student, [3, 4]Assistant Professor
Department of Computer Science
St. Joseph College of Engineering
Sriperumbudur, India.
gowdhamn@gmail.com, visitlibin@gmail.com, sorna.jesus@gmail.com, mnksjce@gmail.com

Abstract-This paper re-examines the problem of visual secret sharing for general access structures by using visual cryptograms of random grids (VCRG). Given a binary or color secret image shared by a set of n participants with a strong access structure, we devise two effective algorithms to produce a set of VCRG so that the members in each qualified set can reconstruct the secret image by superimposing their shares, while those in any forbidden set cannot. The basic 2 out of 2 visual cryptography model consists of a secret message encoded into two transparencies, one transparency representing the cipher text and the other acting as a secret key. Both transparencies appear to be random dots when inspected individually and provide no information about the original clear text. However, by carefully aligning the transparencies, the original secret message is reproduced. The actual decoding is accomplished by the human visual system. Our algorithms do not require any extra pixel expansion, which is indispensable and grows exponentially as n increases in conventional visual cryptographic schemes.

Index Terms: -General access structures, pixel expansion, random grids, visual cryptography, visual secret sharing.

____*****____

1. INTRODUCTION

Visual secret sharing (VSS) is a way to protect a secret image among a group of participantsAn initial model of VSS was proposed by Naor and Shamir. In a (k, n)-threshold scheme, a binary secret image is encrypted into n meaningless images called shares or shadows, which are then distributed to n associated participants. When any k or more participants share their shadows, the secret image is visually revealed by printing their shares on transparencies and stacking them together.

A visual cryptography scheme for general access structures (VCS-GAS) defined by Ateniese is an extension to the threshold (k, n)-VCS It encodes P into n transparencies for the n participants in such a way that only the participants in qualified subsets of P can visually recover P by superimposing their shares, but those in forbidden subsets of P cannot acquire any information about P. A VCS-GAS is more general than a (k, n)-VCS and may be applied to different applications.

Random grid (RG) is an alternative approach to implement VSS without pixel expansion. However, reported RG-based VSS methods are threshold schemes. In this study, RG-based VSS for general access structures is presented. Secret image is encodes into n RGs while qualified set can recover the secret visually and forbidden sets cannot. The proposed scheme is a generalization of the threshold methods. Where those reported RG-based schemes can be considered as the special cases of the proposed scheme.

Experimental results are provided, demonstrating the effectiveness and advantages of the proposed scheme. Sensitive digital contents kept by only one person is easily lost or destructed. Secret sharing is a method to share the secret information among a group of participants against destruction and modification. Visual secret sharing (VSS), which is also called visual cryptography, is a novel type of secret sharing that focuses on sharing images. Advanced merit of VSS is that the decryption is completely based on human visual system without the aid of computers. The stacked result is interpreted as black when four black sub pixels are recovered. Whereas, the stacked result is interpreted as white when two black and two white sub pixels are reconstructed. An example of a 2-out-of-2 VSS scheme is demonstrated, where the original secret image is two shares generated by the construction are illustrated and the stacked result of the two shares.

In conventional VSS, a code book (all the pre-defined patterns) is required for share construction. Each pattern in the code book consists of m ≥ 2 black and white pixels, where m is referred to pixel expansion. Pixel expansion indicates that each share is m times as big as the original secret image. Transmitting and storing the shares would be further burdened by pixel expansion problem.

Based on the pioneer work of Naor and Shamir, wide studies on VSS were presented.

To relieve the concern of pixel expansion, some models different from Naor and Shamir’s have been proposed recently, including probabilistic VCS , multipixel encoding, or random grids . Most of them address the design of threshold schemes for sharing binary images. This proposed paper is to resolve the problem of visual secret sharing for general access structures using the concept of visual cryptograms of random grids. The proposed VCRG-GAS algorithms produces more accurate image and can also be extended to cope with color images

2. LITERATURE REVIEW

A. Visual Cryptographic Scheme for General Access Structures

Consider a secret image P shared by a set of n participants P = {1, 2, . . . , n}. We collect all subsets of P that are able to reveal P into a set T_{Qual} and those that are not into T_{Forb} where T_{Qual}, _Forb⊆2P. We refer to each member of _Qual as a qualified set and that of T_{Forb}as a forbidden set. The pair (T_{Qual}, T_{Forb}) is called the *access structure* of P with regard to P, in which $T_{\text{Qual}}\cap T_{\text{Forb}} = \varphi$ since it makes no sense that some subset A of P exists such that $A\in T_{\text{Qual}}$ and $A\in T_{\text{Forb}}$.

Let $w(V)$ denote the Hamming weight of a 1×m vector V.The following definition slightly modified from the original version which specifies the necessary conditions for $B0$ and $B1$ to be the basis matrices of a VCS-GAS.

Definition 1:Let (T_{Qual}, T_{Forb}) be an access structure on a set of n participants. A VCS-GAS for ($T_{Qual}l$, T_{Forb}) with relative difference α and set of thresholds $\{(X, tX)\}X\in T_{\text{Qual}}$is realized using the two $n \times m$ basis matrices $B0$ and $B1$ if the following two conditions hold.

1) If $X = \{i1, i2, . . . , ip\} \in T_{\text{Qual}}$ (i.e., if X is a qualified set), then the *or* V of rows $i1$, $i2$, . . . , ip of $B0$ satisfies $w(V) \le tX-\alpha\times m$, whereas for $B1$ it results that $w(V) \ge tX$.

2) If $X = \{i1, i2, . . . , ip\} \in T_{\text{Forb}}$ (i.e., if X is a forbidden set), then the two $p\times m$ matrices obtained by restricting $B0$ and $B1$ to rows $i1$, $i2$, . . . , ip are equal up to a column permutation.

Table I

p	probability	s_1	s_2	$s_1\otimes s_2$	h or l	α
□	1/2	□■	□■	□■	1	1/2
	1/2	■□	■□	■□		
■	1/2	□■	■□	■■	0	
	1/2	■□	□■	■■		

Basic Encoding Idea in Naor and Shamir’s Scheme

It is assumed that throughout this paper all participants are essential and all access structures discussed are strong. For instance, consider ($T0$’, $Z’M$) = ({{2, 3}, {2, 4}, {3, 4}, {1, 2,3, 4}}, {{1, 2}, {1, 3}, {1, 4}}) with respect to P’ = {1, 2, 3,4}.It should be rephrased as ($T0$, ZM) = ({{2, 3}, {2, 4}, {3,4}}, {{2}, {3}, {4}}) with respect to P = {2, 3, 4}, because participant 1 is no more essential (where no set X ⊆P_ exists such that $X \cup\{1\} \in T$Qual but X /∈TQual) so that he or she can be removed from P’(t’0 and $Z’M$, too), and the qualificationof {2, 3, 4} (after deleting 1 from {1, 2, 3, 4}) has beenguaranteed by {2, 3} (or {2, 4}, {3, 4}) owing to the strongproperty so that it is deleted from T’0.

B. Basic Models of Visual Cryptographic Scheme and Visual Cryptograms of Random Grids

The encoding idea of Naor and Shamir’s (2, 2)-VCS for each $p\in P$ into corresponding $s1\in S1$ and $s2\in S2$ can be illustrated by Table I, where both $s1$ and $s2$ are blocks of two pixels. When all pixels in P are encoded in this way, $S1$ and $S2$ become two seemingly random pictures, whereas $S = S1\otimes S2$ reveals P to our eyes where ⊗is the superimposition operation. The pixel expansion is $m(2, 2)$ VCS = 2. Let $s = s1\otimes s2$ and $s[p(0)]$ ($s[p(1)]$) be such block s whose corresponding p. The contrast of s, the relative difference between the reconstructed white ($s[p(0)]$) and black ($s[p(1)]$) blocks, is measured by $\alpha(2, 2)$ VCS = $(h-l)/m(2, 2)$ VCS = (1−0)/2 = 1/2, where $h(l)$ is the number of transparent pixels in $s[p(0)]$ ($s[p(1)]$). Inspite of a 50% loss of contrast in S, our visual perception is still able to recognize P. Regarding VCRG, we refer to a *random grid R* as a 2-D transparency consisting of all pixels with the same probability of being transparent (0) [17], [18], [20]. Let each pixel $r\in R$ be a random pixel with $Prob(r = 1) = Prob(r = 0) = 1/2$.The light transmission of r, i.e., the probability of $r = 0$, is1/2 and consequently that of R is also 1/2, denoted as

TABLE II

Encoding Pixel $p \in P$ Into Random Pixels $r1 \in R1$ and $r2 \in R2$

p	probability	r_1	r_2	$r_1\otimes r_2$	$t(r_1\otimes r_2)$	$l(r_1\otimes r_2)$
□	1/2	□	□	□	1/2	1/2
	1/2	■	■	■		
■	1/2	□	■	■	0	
	1/2	■	□	■		

$$t(r) = Prob(r = 0) = 1/2 \text{ (or } t(R) = 1/2).$$

Table II illustrates one of the three (2, 2)-VCRG encoding processes of $p\in P$ into corresponding $r1\in R1$ and $r2\in R2$.We see that there is no way to judge p = W or B from a single $r1$ or $r2$ individually. Let $r = r1\otimes r2$ and $r[p(0)]$ ($r[p(1)]$) denote such pixel r whose corresponding p is W (B). We obtain $t(r[p(0)]) = 1/2$, while $t(r[p(1)]) = 0$, as shown in

Table II. Owing to such a difference, our visual system can distinguish $r[p(0)]$ from $r[p(1)]$. As a result, both $R1$ and $R2$ are random grids with $T(R1) = T(R2) = 1/2$, whereas $R = R1 \otimes R2$ reveals P to our eyes due to $T(R[P(0)]) = 1/2$ and $T(R[P(1)]) = 0$ where $R[P(0)]$ ($R[P(1)]$) denotes the area in R correspondingto the white (black) pixels in P. Note that there is no extra pixel expansion ,i.e., $m(2, 2)$VCRG= 1.The light contrast, which measures the relative difference between the light transmissions of the transparent and opaque areas in the superimposed result R,

$$L(R) = \frac{T(R[P(0)]) - T(R[P(1)])}{1 + T(R[P(1)])}$$

where r∈R. In this (2, 2)-VCRG, L(R1⊗R2) = ((1/2)−0)/(1+0)= 1/2. Note that when two light contrasts are with the same T (R[P(0)])−T (R[P(1)]), the one with a larger T (R[P(1)]) results in a smaller L(R) since more light in T (R[(1)]) degrades our visual perception relatively.

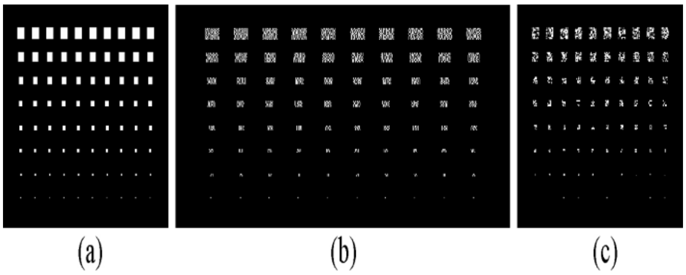


Fig. 1. Reconstruction abilities of VCS and VCRG. (a) P. (b) $S1 \otimes S2$.(c) $R1 \otimes R2$.

Fig. 1 deliberately elucidates the reconstruction abilities ofVCS and VCRG for dealing with small white regions. Fig. 1(a) is the secret image P consisting of eight kinds (10×10, 8×8,6×6, 5×5, 4×4, 3×3, 2×2, 1×1 pixels) of ten white regions. Fig. 1(b) shows $S1 \otimes S2$ by (2, 2)-VCS, which reconstructs all white and black pixels in P flawlessly with mVCS = 2.Fig. 1(c) gives $R1 \otimes R2$ by (2, 2)-VCRG with mVCRG = 1, in which about 50%1 × 1 white regions are mis-reconstructed as black [see the bottom of Fig. 1(c)]. Nevertheless, VCRG works well as long as the white regions are not too small (say, no less than 3 × 3 pixels in this case) in P. Regarding the study on the lower bound of the size of a recognizable white region in the reconstructed result for VCRG. This paper thus excludes the consideration of those secret images whose critical information is characterized by very small white regions.

3.PROPOSED METHODOLOGY

The system involves an automatic segregator of images which is a two-step process of converting any images into the required Visual cryptography formatted images.After getting the exact image, the images will be bifurcated into various shares depends on the access structure.

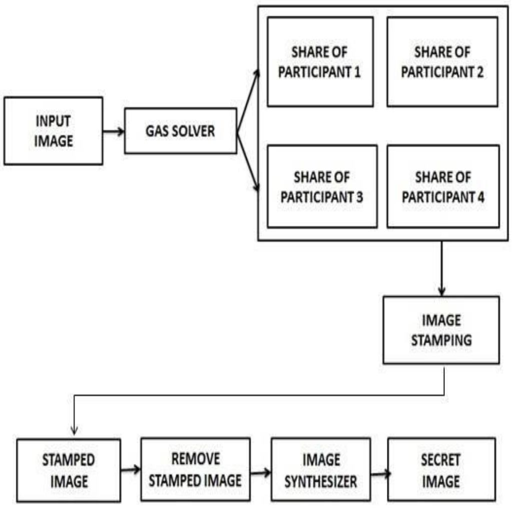


Fig 2: Architecture Diagram

The secret image which needs to be encode into N shares printed on transparencies. Option of providing decision of the number of shares to the user is the new feature introduced. The shares of the images appear random and contain no decipherable information's about the underlying secret image. Still,, if any 2 or more (Based on access structure) of the shares are stacked on top of one another the secret image becomes decipherable by the human eye.

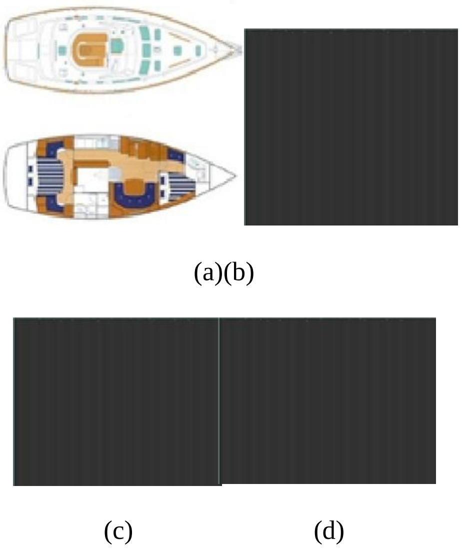
The shares were taken the shares needs to be stamped with the help of “Block-Based Transformation Algorithm”. So that, a clear picture of segregating the images based on a viewable identifiers. The system involves two step process of removing the stamp and de-ciphers the logic behind the share spread and everything will be decided based on the underlying access structure.

A) Access Structure Define Module

In this module, the user will be given a secure login and provide all the necessary details. Multiple users will be created in a hierarchical manner. So that, the owner of the data will login and an automatic bifurcation of images will happen based on the logged in users sub Childs.The information about the hierarchy needs to be given to the GAS system. Logging into this system is enable with MD5 algorithmic security.

B) Image Upload and Image subdiv Module

In this module, the images will be uploaded by the data owner. An automatic recognizer in turn our GAS will take care of analyzing the general access structure inside the system and based on that, the images will be segregated in the fore coming module. In VC scheme each pixel ‘p’ of the secret image is encrypted into a pair of sub pixels in each of the two shares. If ‘p’ is white, one of the two columns under the white pixel is selected. If p is black, one of the two columns under the black pixel is selected. In each case, the selection is performed randomly such that each column has 50% probability to be chosen. The above points is valid for the system which has only two shares. Whereas in our system, the GAS solver will identify the number of shares automatically.Based on the number of shares, the pixel will be subdivided and ready to share to the end user.



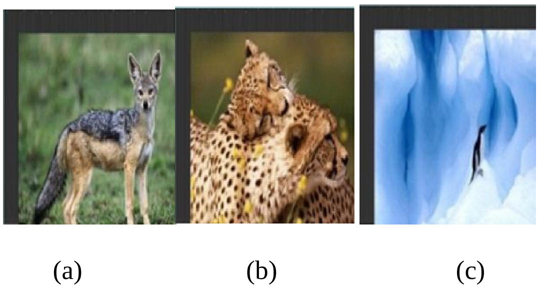
(a)(b)

(c) (d)

Fig 3: Implementation Results a)Original Image(P) b)share(s1) c)share(s2) d)share(s3)

C) Image Stamping Module

The major drawback of the system is to identify the shares if the shares get collapsed. We don't have a proper system to identify such kind of pictures. That's why, to overcome such kind of problem. We are proposing a system which has a stamping system. Our stamping system involves stamping of a picture on top of the other images. This is one of the most complex part in the system.



(a) (b) (c)

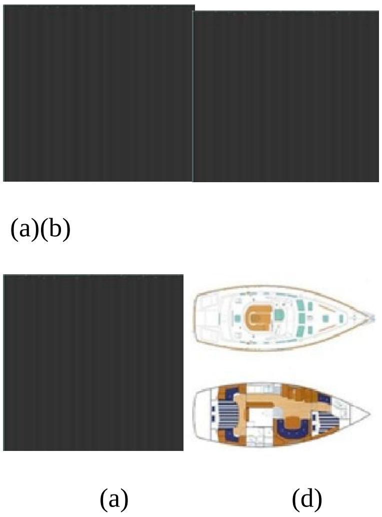
Fig 4: Stamped Images on shares

D) Image Remove Stamping Module

In this module, the stamped shares will be received from the users and then stamped image will be removed from the shares, with the help of stamped shares user can be easily identified. It checks whether the given stamped image is in valid format or not. If the image not valid it will notify the user and ask for the correct input. If the images are valid then the stamped image over the shares will be removed and original shares will be produced.

E) Image Synthesizer Module

In this module, once the valid shares were obtained from the remove stamping module. The images were validated. An automatic Image synthesize system will validate the shares. In case, if the images were not obtained from the valid set of participants. An automatic indication of forge share will be indicated to the user.



(a)(b)

(a) (d)

Fig 5: a) s1 b) s2 c) s3 d) original images obtained by stacking shares together

F) Image re-constructs Module

Once the images were given into the system without any issues. The images will be merged based on the white pixel and black pixel combination and the final images will be re-constructed. The visual cryptosystem does not require any complex decryption algorithm. Because we can easily find the secret by combining all shares.

4) RELATED WORK

Given a secret image *P* shared by a set P of *n* participants in a strong access structure (*T*Qual,TForb) with _0 and *ZM*, we introduced two novel and effective VCRG-GAS algorithms to resolve the problem of visual secret sharing for binary and color images in this paper. One was based on _0 to produce a set of (|*Qj* |, |*Qj* |)-VCRG for each *Qj*∈_0 and distribute the constituent shares according to the inclusion matrix, and the other focused on *ZM* by generating a set of (|*ZM*|, |*ZM*|)-VCRG and dispatching the universal shares according to the exclusion matrix. Their feasibility and applicability were formally proved and empirically verified. The most important contribution of our approaches was that no extra pixel expansion was required. Provided that the (*n*, *n*)-VCS would be adopted, the pixel expansion became max*Qj*∈_0 {2|*Qj*|−1} or 2|*ZM*|−1. When max*Qj*∈_0 {|*Qj*|} or |*ZM*| goes larger, the exponentially grown share size in VCS would be less attractive than the one with the same size as the secret in VCRG. For a given access structure, the light contrasts of a particular qualified set derived from the two algorithms may be different. More specifically, the T_0-based algorithm may deliver different light contrasts for different qualified sets, while the *ZM*-based algorithm gives a constant one. The light transmissions of the shares may also be different. These flexible features enrich the applications of VCS-GAS. The dealer could depend on the practical concerns to choose the one that he or she prefers most. The common core of our proposed algorithm is an (n, n)- VCRG and we adopt Algorithm to be the role throughout the paper. Undoubtedly, characterized by very small white regions. How to improve such a drawback is surely a challenging research topic. In addition, whether there exist other algorithms that could improve or maximize the light contrast in the reconstructed result is another topic worthy of further study. Furthermore, applying the VCRG approach to other subjects of great significance in visual cryptography.

5) CONCLUSION

Our method guarantees the blackness of black secret pixels for VCSs and improves the display quality of the worst-case image. The experimental results show that our approach performs better than those previously proposed in terms of the display quality of the recovered image, which includes the controllable blackness for black secret pixels and maintenance of the same aspect ratio as that of the original secret image.

6. REFERENCES

[1] S.J. Shyu, "Visual Cryptograms of Random Grids for General Access Structures, “*video technology*, vol. 23, no. 3, 2013

[2] G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, “Visualcryptography for general access structures,” *Inform. Comput.*, vol. 129,no. 2, pp. 86–106, 1996.

[3] C. Blundo, S. Cimato, and A. De Santis, “Visual cryptography schemes with optimal pixel expansion,” *Theor. Comput. Sci.*, vol. 369, nos. 1–3, pp. 169–182, 2006.

[4] C. Blundo, P. D’Arco, A. De Santis, and D. R. Stinson, “Contrast optimalthreshold visual cryptography schemes,” *SIAM J. Discrete Math.*, vol.16, no. 2, pp. 224–261, 2003.

[5] C. Blundo, A. De Santis, and D. R. Stinson, “On the contrast in visual cryptography schemes,” *J. Cryptology*, vol. 12, no. 4, pp. 261–289, 1999.

[6] M. Bose and R. Mukerjee, “Optimal (k, n) visual cryptographic schemes for general k,” *Designs Codes Cryptography*, vol. 55, no. 1, pp. 19–35, 2010.

Algorithms, or even other VCSs with a pixel expansion of 1 (by probabilistic, multipixel encoding, and so on) can also be chosen as the core.

The analyses and experiments derived from Algorithm are pertinent and applicable to other alternatives. The approach of VCRG relieves the concern of pixel expansion, yet its reconstruction ability is not flawless as VCS due to the reason that a quite small white region might be misreconstructed as black. Therefore, it is not appropriate to deal with those secret images whose critical information is

[7] S. Cimato, R. De Prisco, and A. De Santis, “Optimal colored threshold visual cryptography schemes,” *Designs Codes Cryptography*, vol. 35,no. 3, pp. 311–335, Jun. 2005.

[8] F. Liu, C. Wu, and X. Lin, “Step construction of visual cryptography schemes,” *IEEE Trans. Information Forensics Security*, vol. 5, no. 1, pp. 27–38, Mar. 2010.

[9] S. Cimato, R. De Prisco, and A. De Santis, “Probabilistic visual cryptography schemes,” *Comput. J.*, vol. 49, no. 1, pp. 97–107, 2006.

[10] Y.-C. Hou, “Visual cryptography for color images,” *Pattern Recognit.*, vol. 36, no. 7, pp. 1619–1629, 2003.

[11] T.Katoh and H. Imai, “An extended construction method for visual secret sharing schemes,” *Electron. Commun. Japan Part III FundamElectron. Sci.*, vol. 81, no. 7, pp. 55–63, 1998.

[12] F. Liu, C. Wu, and X. Lin, “Step construction of visual cryptography schemes,” *IEEE Trans. Information Forensics Security*, vol. 5, no. 1, pp. 27–38, Mar. 2010.

[13] F. Liu, C. Wu, and X. Lin, “Step construction of visual cryptography schemes,” *IEEE Trans. Information Forensics Security*, vol. 5, no. 1, pp. 27–38, Mar. 2010.

[14] S. J. Shyu and M. C. Chen, “Optimum pixel expansions for threshold visual secret sharing schemes,” *IEEE Trans. Information ForensicsSecurity*, vol. 6, no. 3, pp. 960–969, Sep. 2011.

[15] C.-N. Yang, “New visual secret sharing schemes using probabilistic method,” *Pattern Recognit. Lett.*, vol. 25, no. 4, pp. 481–494, 2004.