

A SHORT SURVEY ON VISUAL CRYPTOGRAPHY SCHEMES

JIM CAI

ABSTRACT. Visual Cryptography Scheme (VCS) is an encryption method that uses combinatorial techniques to encode secret written materials. The idea is to convert the written material into an image and encode this image into n shadow images. The decoding only requires only selecting some subset of these n images, making transparencies of them, and stacking them on top of each other. In this survey paper, we will provide the readers an overview of the basic VCS constructions, as well as several extended work in the area. In addition, we also review several state-of-art applications that take full advantage of such simple yet secure scheme.

1. INTRODUCTION

Suppose 4 intelligent thieves have deposited their loot in a Swiss bank account ¹. These thieves obviously do not trust each other. In particular, they do not want a single member of themselves to withdraw the money and fled. However, they assume that withdrawing money by two members of the group is not considered a conspiracy, rather it is considered to have received "authorizations". Therefore, they decided to encode the bank code (with a trusted computer) into 4 partitions so that any two or more partitions can be used to reconstruct the code. Since the thieves's representatives will not have a computer with them to decode the bank code when they come to withdraw the money, they want to be able to decode visually: each thief gets a transparency. The transparency should yield no information about the bank code (even implicitly). However, by taking any two transparencies, stacking them together and aligning them, the secret number should "pop out". How can this be done?

The solution is proposed in 1994 by Naor and Shamir [1] who introduced a simple but perfectly secure way that allows secret sharing without any cryptographic computation, which they termed as Visual Cryptography Scheme (VCS). The simplest Visual Cryptography Scheme is given by the following setup. A secret image consists of a collection of black and white pixels where each pixel is treated independently. To encode the secret, we split the original image into n modified versions (referred as shares) such that each pixel in a share now subdivides into m black and white sub-pixels. To decode the image, we simply pick a subset S of those n shares and Xerox each of them onto a transparency. If S is a "qualified" subset, then stacking all these transparencies will allow visual recovery of the secret. Figure 1 provides an example of such construction. Suppose the secret image "IC" is divided into 4 shares, which is denoted by $\wp = \{1,2,3,4\}$, and that the qualified sets are all subsets of \wp containing at least one of the three sets $\{1,2\}$, $\{2,3\}$ or $\{3,4\}$. Then the qualified sets are exactly the following:

$$\Gamma_{Qual} = \{\{1, 2\}, \{2, 3\}, \{3, 4\}, \{1, 2, 3\}, \{1, 2, 4\}, \{1, 3, 4\}, \{2, 3, 4\}, \{1, 2, 3, 4\}\}$$

Along with this basic setup, Naor and Shamir also proposed (k,n) threshold model as its extension. This extended scheme is constructed such that any k shares can be stacked together to reveal the original secret, but any $k-1$ shares gain no information about it. It is not hard for the readers to verify that the scenario described at the beginning of the paper is an instance of $(2,4)$ -threshold VCS.

The rest of the paper is structured as follows. In section 2 we will introduce the construction of (k,n) -threshold VCS along with some parameters used to describe the model.

¹This is a summary of a story taken from www.wisdom.weizmann.ac.il/~naor/PUZZLES/visual.html

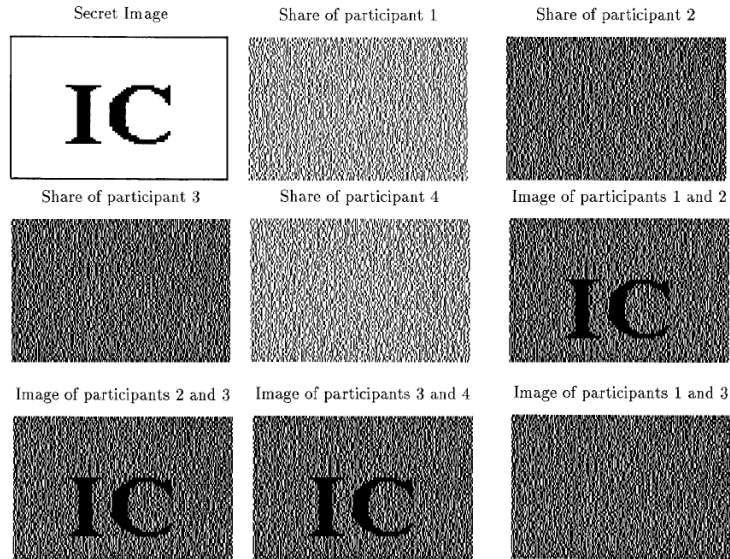


FIGURE 1. Different shares overlaying

In section 3 we review several extension of visual cryptography research that includes VC for general access structure, contrast optimization and the concept of randomness. We briefly introduce some applications of VCS in section 4 and conclude our paper in section 5.

2. THE MODEL

In this section we formally define VCS model, as well as (k,n) -threshold VCS scheme that was proposed by Naor and Sharmir [1].

Definition 2.0.1. Hamming weight: The number of non-zero symbols in a symbol sequence. In a binary representation, Hamming weight is the number of "1" bits in the binary sequence.

Definition 2.0.2. OR-ed k -vector: Given a $j \times k$ matrix, it is the k -vector where each tuple consists of the result of performing boolean OR operation on its corresponding $j \times 1$ column vector.

Definition 2.0.3. An VCS scheme is a 6-tuple (n, m, S, V, α, d) . It assumes that each pixel appears in n versions called shares, one for each transparency. Each share is a collection of m black and white subpixels. The resulting structure can be described by an $n \times m$ Boolean Matrix $S=[S_{ij}]$ where $S_{ij} = 1$ iff the j th sub-pixel in the i th share is black. Therefore, the grey level of the combined share, obtained by stacking the transparencies, is proportional to the Hamming weight $H(V)$ of the OR-ed m -vector V . This grey level is usually interpreted 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 $\alpha > 0$. αm , the difference between the minimum $H(V)$ value of a black pixel and the maximum allowed $H(V)$ value for a white pixel is called the contrast of a VCS scheme.

Definition 2.0.4. VCS Schemes where a subset is qualified if and only if its cardinality is k are called (k,n) -threshold visual cryptography schemes. A construction to (k,n) -threshold VCS consists of two collections of $n \times m$ Boolean matrices ζ_0 and ζ_1 , each of size r . To construct a white pixel, we randomly choose one of the matrices in ζ_0 , and to share a black pixel, we randomly chooses a matrices in ζ_1 . The chosen matrix will define the color of the m sub-pixels in each one of the n transparencies. Meanwhile, the solution is considered valid if the following three conditions are met:

- (1) For any matrix S in ζ_0 , the "or" operation on any k 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 of the n rows satisfies $H(V) \geq d$
- (3) For any subset $\{i_1, i_2, \dots, i_q\}$ of $\{1, 2, \dots, n\}$ 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, \dots, i_q are indistinguishable in the sense that they contains exactly the same matrices with the same frequencies. In other words, any $q \times n$ matrices $S^0 \in B_0$ and $S^1 \in B_1$ are identical up to a column permutation.

Condition (1) and (2) defines the contrast of a VCS. Condition (3) states the security property of (k, n) -threshold VCS. Should we have not been given k shares of the secret image, we cannot gain any hint in deciding the color of our pixel, regardless of the amount of computation resource we have on hand.

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

$$\zeta_0 = \left\{ \text{all matrices obtained by permuting the columns of } \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix} \right\}$$

$$\zeta_1 = \left\{ \text{all matrices obtained by permuting the columns of } \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix} \right\}$$

In order to encode a white pixel, the dealer needs to randomly choose one matrix from ζ_0 to construct the sub-pixels in three shares accordingly. Meanwhile, to encode a black pixel, the dealer needs to randomly pick one matrix from ζ_1 . It is not hard to verify that this construction will yield a relative contrast of 0.25. That is, the encoding of a black pixel needs all 4 black sub-pixels where a white pixel needs 3 black sub-pixels and 1 white sub-pixel. Therefore, when the three shares stack together, the result is either dark grey, which we use to represent white, or completely black, which we use to represent black. Readers can verify the security property of $(3, 3)$ threshold VCS by taking any two rows from any $S^0 \in \zeta_0$ and $S^1 \in \zeta_1$ 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 2.0.5. *In any (k, k) -threshold VCS scheme construction, $m \geq 2^{k-1}$ and $\alpha = 1/2^{k-1}$.*

Theorem 2.0.6. *There exists a (k, n) -threshold VCS scheme with $m = n^k \cdot 2^{k-1}$ and $\alpha = (2e)^{-k} / \sqrt{2\pi k}$.*

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. In [3] the authors show a more optimal (k, n) VCS construction with a smaller m . Interested readers can consult [1][3] for their details.

3. EXTENSIONS

Because VCS construction is simple and secure with no extra burden in decoding process, it quickly became a popular research area for cryptographers and mathematicians, where most of the extended work are dedicated to generalization and optimization of VCS. In this section, we will explore several representative work over the years.

3.1. VCS for general access structure. When Naor and Shamir propose VCS, they only discussed construction of (k, n) -threshold scheme where a subset $X \in \wp$ is a qualified set if and only if $|X| = k$. Ateniese et al [3] generalizes this definition by introducing the

concept of access structure. An access structure refers to specifications of qualified and forbidden subsets of participants, and is denoted by $\{\Gamma_{Qual}, \Gamma_{Forb}\}$. Let $X = \{i_1, i_2, \dots, i_p\}$, $x \in \Gamma_{Qual}$ if and only if for any $M \in \zeta_0$, the "or" operation of rows i_1, i_2, \dots, i_p satisfies $H(V) \leq t_x - \alpha \cdot m$.

As we can see, this model associate a possibly different threshold t_x with each set $X \in \Gamma_{Qual}$ and therefore considered a more generalized VCS model than the one Naor and Shamir proposed.

3.2. Optimizations. The optimality of VCS is determined mostly by its pixel expansion m and the relative contrast α . Pixel expansion m represents the loss in resolution from the original image to the decoded one. Therefore m needs to be as small as possible. In addition, m also needs to be in the form of n^2 where $n \in N$ in order to preserve the aspect ratio of the original image. On the other hand, the relative contrast α needs to be as large as possible to ensure visibility[1]. In the scope of this paper, we will only explore works related to contrast optimization. Works related to deriving lower bound of pixel expansion m can be found in [7], [8] etc.

The research on contrast optimization was motivated by the problem of extra greying effect introduced to decoded image. This occurs because the decoded image is not an exact reproduction of the original image, but an expansion of the original, with extra black pixels. The black pixels in the original image will remain black if $d=m$. However, the white pixels will become grey, due to the blackness introduced by the black sub-pixels, which resulted in loss of contrast to the entire image.

It is not hard to show that a (2,2) threshold schemes have the best possible relative contrast $\alpha = 1/2$. To further improve this contrast, Naor and Shamir extended their 1994 work by introducing the "Cover" semi-group Operation.[2] There are a few changes in this new model. First of all, instead of considering only binary colors, the new model would consist of two "opaque" colors (say, red and yellow) and the third "transparent" one. When overlaying together, the top opaque color will always dominate. Secondly, instead of having two shares I and II, there are now $2c$ sheets marked I1, I2,...Ic, II1, II2,...IIc. Each sheet contains red,yellow and transparent pixels. When overlaying, we also make sure that II1 is placed on top of I1, I2 is placed on top of II1, etc. Formally:

Definition 3.2.1. A solution to (2,2) threshold VCS using the Cover semi-group consists of:

- (1) Two distributions D_R and D_Y on $c \times m$ matrices where m is the number of sub-pixels used to encode one pixel in the original image. Each entry of D_R and D_Y is an element from $\{R,Y,T\}$, which stands for red, yellow and Transparent respectively.
- (2) A partition of $\{1\dots c\}$ into 2 subsets S_1 and S_2 .

The upper bound for relative contrast α obtained in this cover semi-group construction is $1 - \frac{1}{c}$ for (2,2) threshold VCS. Unfortunately, the construction cannot be extended to (k,n) threshold VCS.

3.3. VCS randomness. Recall that any VCS would consist of two collections of matrices ζ_0 and ζ_1 . When encoding a pixel, depending on the color of the pixel, we need to randomly pick a matrix from one of the collections. In other words, if we number all the candidate matrices as $1,2,\dots,|\zeta_t|$, the encoding algorithm should generate a secret key k , where k represents the index of the matrix that we have used to encode this pixel. Blundo et al[4] formalizes this idea of randomness behind VCS as the follows:

Definition 3.3.1. The randomness of a VCS represents the number of random binary bits per pixel required to share a secret image among the participants. Formally, let the randomness of a VCS be denoted \mathfrak{R} , then $\mathfrak{R}(\zeta_0, \zeta_1) = \log(\min\{|\zeta_0|, |\zeta_1|\})$.

Note that given an arbitrary VCS, we can always find another VCS that have same m , α and equal sized ζ_1 and ζ_2 . This proof is shown in [3]. Therefore it is safe to assume

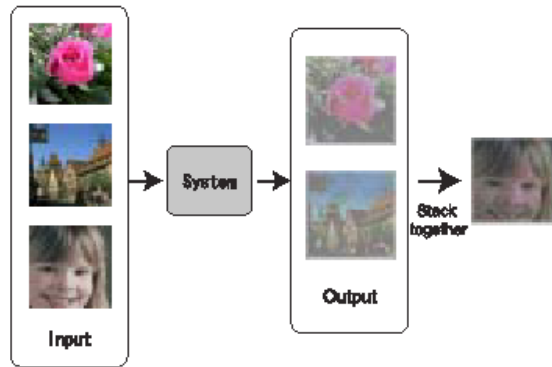


FIGURE 2. Hide secret in natural images

$\zeta_0 = \zeta_1 = r$ w.o.l.g. It turns out that r is the only variable that impacts the randomness \mathfrak{R} . We further know that virtually all constructions of ζ_0 and ζ_1 for (k,n) -threshold VCS consists of basis matrices $S^0 \in \zeta_0$ and $S^1 \in \zeta_1$ together with all of their permutations, each of which satisfy contrast and security conditions outlined in section 1. Recall that each matrix is $n \times m$ where m is the pixel expansion. Hence it follows that the randomness of such threshold VCS can also be expressed as $\log(m!)$. This lower bound is further improved in [9] for (k,k) -threshold VCS.

3.4. Secret Encoding With Natural Images. Now we know that given a secret message, we can always encode it into sets of n images, each containing no information about the secret. However, it would be more useful to conceal the existence of the secret message. In other words, the shares given to participants in the scheme should not look as a random bunch of pixels, but they should be innocent looking images (an house, a dog, a tree, etc). The solution is addressed in [1] [8] and [10]. The basic idea behind is to represent the hidden image by controlling the way opaque sub-pixels in natural images are stacked together. A class of VCS constructions are developed in [10] to hide images in the multi-color natural images. We conclude this section by showing you a working example of this work in the figure below.

4. APPLICATIONS

Visual Cryptography Schemes can decode concealed images based purely on human visual systems, without any aid from cryptographic computation. This nice property gives birth to a wide range of encryption applications. In this section, we will discuss how VCS is used in applications such as E-Voting system, financial documents and copyright protections.

4.1. Electronic-Balloting System. Nowadays, most of the voting are managed with computer systems. These voting machines expected voters to trust them, without giving proof that they recorded each vote correctly. One way to solve this problem is to issue receipts to voters to ensure them their votes are counted. However, this could improperly influence the voters, which produces coercion or vote selling problems. To solve this dilemma, Chaum [6] proposed a secret-Ballot Receipts system that is based on $(2,2)$ -threshold binary VCS. It generates an encrypted receipt to every voter which allows her to verify the election outcome - even if all election computers and records were compromised. At the polling station, you will receive a double-layer receipt that prints your voting decision. You will be asked to give one of the layer to the poll worker who will destroy it immediately with a paper shredder. The remaining one layer will now become unreadable. To make sure that your vote is not altered or deleted, you could querying the serial number on your receipt on the election Web site. This will return a posted receipt that

looks identical to yours in hand. Notice that you do not need any software to verify this: simply print the posted receipt and overlaying it with your original receipt. There are two security advantages of this system. First of all, a receipt that is not properly posted can act as a physical evidence of the failure of the election system. Secondly, voters are ensured that their vote is correctly recorded at the polling station, but after surrendering a layer of the receipt, no one can decode it unless he somehow know the decryption algorithm and obtained all secret keys, which are typically held by different trustee. Thirdly, even if all election computers were compromised, there are only limited ways that the system could alter the voting. For example, the system could print a wrong layer and hope that the voter will choose another one. However, the chances that it would go undetected is $1/2$ for one vote, and hence $(1/2)^{10}$ for 10 ballots, which is considered negligible for a voting population of, say 30,000 people.

4.2. Encrypting financial documents. The VCS principle can also be applied in transmitting confidential financial documents over Internet. VCRYPT is an example of this type of system being proposed by Hawkes et al [?]. VCRYPT can encode the original drawing document with a specified (k,n) VCS, then send each of the encoded n shares separately through Emails or Ftp to the recipient. The decoding only requires bitwise "OR" operation on all shares in the specified directory, and needs no extra effort of cryptographic computation. Any malicious attacker who intercepts only m of n shares where $m < k$ will not be able to gain any information about the financial document. Moreover, it is impossible to alter the content of the document unless all shares are intercepted, altered and re-inject into the network.

Financial documents often contain a lot of digits. Therefore, after applying VCS, we will expect that the greying effect will prevent us from recognizing the "fuzzy" digits in decoded documents. To work around this problem, VCRYPT proposed a post filtering process to return the decoded image precisely to its original form. It evaluates every set of m sub-pixels against the encoding threshold and display the final pixel as black if the number of black sub-pixels is above the threshold and white otherwise.

5. CONCLUSION

In this paper, we briefly review the literature of visual cryptography schemes as special instances of secret sharing methods among participants. We also described different constructions that generalize and optimize VCS. Among various advantages of VCS, we emphasize the property that VCS decoding relies purely on human visual system, which leads to a lot of interesting applications in private and public sectors of our society.

REFERENCES

1. M. Naor and A. Shamir, Visual cryptography, in "Advances in Cryptology – EUROCRYPT '94", A. De Santis, ed., Lecture Notes in Computer Science 950 (1995), 1-12.
2. M. Naor and A. Shamir, Visual cryptography II: improving the contrast via the cover base, in "Security Protocols", M. Lomas, ed., Lecture Notes in Computer Science 1189 (1997), 197-202.
3. G. Ateniese, C. Blundo, A. De Santis and D. R. Stinson, Visual cryptography for general access structures, Information and Computation 129 (1996), 86-106.
4. C. Blundo, A. Giorgia Gaggia and D. R. Stinson, On the dealer's randomness required in secret sharing schemes, Designs, Codes and Cryptography 11 (1997), 107-122.
5. W. Hawkes, A. Yasinsac, C. Cline, An Application of Visual Cryptography to Financial Documents, technical report TR001001, Florida State University (2000).
6. D Chaum, Secret-ballot receipts: True voter-verifiable elections, IEEE Security and Privacy, 2004, 38-47.
7. A.Klein, M. Wessler, Extended Visual Cryptography Schemes.
8. G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, Extended Schemes for Visual Cryptography Theoretical Computer Science.
9. A. Bonis and A.Santis, Randomness in secret sharing and visual cryptography schemes, Theor. Comput. Sci. 314 (2004), 351-374.
10. Nakajima, M. and Yamaguchi, Y., Extended Visual Cryptography for Natural Images, WSCG02, 2002, 303.

DEPARTMENT OF COMPUTER SCIENCE, UNIVERSITY OF TORONTO
E-mail address: jcai@cs.toronto.edu