Multi-pixel Encryption Visual Cryptography*

Teng Guo[1,2], Feng Liu[1], and ChuanKun Wu[1]

[1] State Key Laboratory of Information Security
Institute of Software, Chinese Academy of Sciences, Beijing 100190, China
[2] Graduate University of Chinese Academy of Sciences, Beijing 100190, China
{guoteng,liufeng,ckwu}@is.iscas.ac.cn

Abstract. A visual cryptography scheme (VCS) is a secret sharing method, for which the secret can be decoded by human eyes without needing any cryptography knowledge nor any computation. In their pioneer work, Naor and Shamir mentioned that encrypting a block of pixels simultaneously may result in better result. Inspired by that idea, we first define multi-pixel encryption visual cryptography scheme (ME-VCS), which encrypts a block of t $(1 \leq t)$ pixels at a time. Then we give an upper bound of the overall contrast of ME-VCS. We also give a lower bound of the pixel expansion of (n, n, t)-ME-VCS. At last, we built a contrast-optimal ME-VCS from a contrast-optimal VCS and built an optimal (n, n, t)-ME-VCS from an optimal (n, n)-VCS.

Keywords: Visual cryptography, Multi-pixel encryption, Contrast-optimal, ME-VCS.

1 Introduction

In [13], Naor and Shamir first presented a formal definition of k out of n threshold visual cryptography scheme, denoted as (k, n)-VCS for short. In a (k, n)-VCS, the original secret image is split into n shares, where the stacking of any k shares can reveal the content of the secret image but any less than k shares should provide no information about the secret image, except the size of it. In [1], Ateniese et al. extended the model of Naor and Shamir to general access structure. A general access structure is a specification of qualified participant sets Γ_{Qual} and forbidden participant sets Γ_{Forb}. Any participant set $X \in \Gamma_{Qual}$ can reveal the secret by stacking their shares, but any participant set $Y \in \Gamma_{Forb}$ cannot obtain any information of the secret image, except the size of it.

In [13], Naor and Shamir also mentioned in the footnote that encrypting a block of pixels simultaneously may result in better result. Afterwards, many studies have been spent to multi-pixel encryption. In [9], Hou proposed a method, which encrypts a block of two pixels at a time. However, this method is probabilistic and it is for 2 out of 2 threshold structure only. In [14], Du extended Hou's method to general access structure, but the proposed method is still probabilistic. In [3], Chen proposed a multiple-level (k, k) secret sharing scheme, which

* This work was supported by NSFC No.60903210.

C.-K. Wu, M. Yung, and D. Lin (Eds.): Inscrypt 2011, LNCS 7537, pp. 86–92, 2012.

encrypts a block of pixels at a time. This method combined with two techniques (histogram width-equalization and histogram depth-equalization) can deal with gray-level images, however it is not perfect secure (in an information-theoretic sense). Other studies on multi-pixel encryption can be found in [2,11,12]. However, they are all probabilistic and not proved to be optimal.

In the model of Naor and Shamir, we encode a pixel at a time, and we can recover the original secret image exactly (recover every pixel of the original secret image). In this sense, the model of Naor and Shamir is also known as deterministic VCS. In this paper, we refer deterministic VCS encoding a pixel at a time (the model of Naor and Shamir) as VCS. We first extend the model of Naor and Shamir (denoted as VCS) to the multi-pixel encryption model (denoted as ME-VCS), for which the model of Naor and Shamir is a special case of the proposed multi-pixel encryption model. Then we give an upper bound of the overall contrast of ME-VCS. For (n, n, t)-ME-VCS, we also give a lower bound of the pixel expansion. At last, we build a contrast-optimal ME-VCS from a contrast-optimal VCS and build an optimal (n, n, t)-ME-VCS from an optimal (n, n)-VCS.

This paper is organized as follows. In Section 2, we give some preliminaries of VCS and ME-VCS. In Section 3, we give an upper bound of the overall contrast of ME-VCS and a lower bound of the pixel expansion of (n, n, t)-ME-VCS. The paper is concluded in Section 4.

2 The Multi-pixel Encryption Model

In this section, we first give the definition of VCS. Then we give the definition of ME-VCS.

Let X be a subset of $\{1, 2, \cdots, n\}$ and let $|X|$ be the cardinality of X. For any $n \times m$ Boolean matrix M, let $M[X]$ denote the matrix M constrained to rows in X, then $M[X]$ is a $|X| \times m$ matrix. We denote by $H(M[X])$ the Hamming weight of the *OR* result of rows of $M[X]$. Let C_0 and C_1 be two collections of $n \times m$ Boolean matrices, we define $C_0[X] = \{M[X] : M \in C_0\}$, $C_1[X] = \{M[X] : M \in C_1\}$.

In a VCS with n participants, we share one pixel at a time. The pixel is either white or black. If the pixel to be shared is white (resp. black), we randomly choose a share matrix from C_0 (resp. C_1) and distribute its j-th $(0 \le j \le n)$ row to share j. Let $'0'$ denote a white pixel and let $'1'$ denote a black pixel. A VCS for an access structure Γ is defined as follows:

Definition 1 (VCS [13,1,7,8,10]). *Let $(\Gamma_{Qual}, \Gamma_{Forb}, n)$ be an access structure on a set of n participants. The two collections of $n \times m$ Boolean matrices (C_0, C_1) constitute a visual cryptography scheme $(\{\Gamma_{Qual}, \Gamma_{Forb}\}, n)$-VCS if the following conditions are satisfied:*

1. *(Contrast) For any participant set $X \in \Gamma_{Qual}$, we denote $l_X = \max_{M \in C_0[X]} H(M)$, and denote $h_X = \min_{M \in C_1[X]} H(M)$. It holds that $0 \le l_X < h_X \le m$.*

2. (*Security*) *For any participant set $Y \in \Gamma_{Forb}$, $C_0[Y]$ and $C_1[Y]$ contain the same matrices with the same frequencies.*

h_X (resp. l_X) is the minimum (resp. maximum) Hamming weight of the stacked patterns of a black (resp. white) pixel restricted to qualified set X. The contrast of qualified set X is defined as $\alpha_X = \frac{h_X - l_X}{m}$, and the contrast of the scheme is defined as $\alpha = \min\limits_{X \in \Gamma_{Qual}} \{\alpha_X\}$. The pixel expansion of the scheme is m. The contrast is expected to be as large as possible. The pixel expansion is expected to be as small as possible. When the contrast reaches its maximum, the VCS is contrast-optimal. When the pixel expansion reaches its minimum, the VCS is pixel-expansion-optimal. When the VCS is both contrast-optimal and pixel-expansion-optimal, we say that the VCS is optimal.

Remark: In this paper, VCS means deterministic VCS encoding a pixel at a time, for which the original secret image can be reconstructed exactly. All the results are for deterministic VCS too.

If the two collections of $n \times m$ Boolean matrices (C_0, C_1) can be obtained by permuting the columns of the corresponding $n \times m$ matrix (S_0 for C_0, and S_1 for C_1) in all possible ways, we will call the two $n \times m$ matrices the basis matrices [1]. In this case, the size of the collections (C_0, C_1) is the same (both equal to $m!$). The algorithm for the VCS based on basis matrices has small memory requirement (it keeps only the basis matrices S_0 and S_1, instead of two collections of matrices (C_0, C_1)), and it is efficient (to choose a matrix in C_0 (resp. C_1), it only generate a permutation of the columns of S_0 (resp. S_1)).

In multi-pixel encryption visual cryptography scheme (ME-VCS) with n participants, we share a block of t ($t \geq 1$) pixels at a time. We denote the t pixels as an encryption block. Obviously, the Hamming weights of all possible encryption blocks may be $0, 1, \ldots, t$. There are $t+1$ encryption collections $(C_0, C_1, \ldots, C_t)$, for which C_i $(0 \leq i \leq t)$ is for encryption blocks of Hamming weight i. To share an encryption block of Hamming weight i $(0 \leq i \leq t)$, we randomly choose a share matrix from C_i, and distribute the j-th $(0 \leq j \leq n)$ row to share j. A ME-VCS for an access structure Γ is defined as follows:

Definition 2 (ME-VCS). *Let $(\Gamma_{Qual}, \Gamma_{Forb}, n)$ be an access structure on a set of n participants. The $t+1$ collections of $n \times m$ Boolean matrices $(C_0, C_1, \ldots, C_t)$ constitute a multi-pixel encryption visual cryptography scheme $(\{\Gamma_{Qual}, \Gamma_{Forb}\}, n, t)$-ME-VCS if the following conditions are satisfied:*

1. (*Contrast*) *For any participant set $X \in \Gamma_{Qual}$, we denote $l_i^X = \min\limits_{M \in C_i[X]} H(M)$ $(0 \leq i \leq t)$, and denote $h_i^X = \max\limits_{M \in C_i[X]} H(M)$. It holds that $0 \leq h_0^X < l_1^X \leq h_1^X < l_2^X \leq h_2^X < l_3^X \leq \ldots \leq h_{t-1}^X < l_t^X \leq m$.*
2. (*Security*) *For any participant set $Y \in \Gamma_{Forb}$, $C_0[Y]$, $C_1[Y]$, ..., and $C_t[Y]$ contain the same matrices with the same frequencies.*

l_i^X $(0 \leq i \leq t)$ is the minimum Hamming weight of the stacked patterns of encryption blocks of Hamming weight i restricted to qualified set X. h_i^X

$(0 \leq i \leq t)$ is the maximum Hamming weight of the stacked patterns of an encryption block of Hamming weight i restricted to qualified set X. The contrast of qualified set X between encryption blocks of Hamming weight i $(0 \leq i \leq t-1)$ and those of Hamming weight $i+1$ is defined as $\alpha_i^X = \frac{l_{i+1}^X - h_i^X}{m}$, and the overall contrast of qualified set X is defined as $\alpha_X = \sum_{i=0}^{t-1} \alpha_i^X$. The overall contrast of the scheme is defined as $\alpha = \min_{X \in \Gamma_{Qual}} \alpha_X$. The pixel expansion of the scheme is m. The overall contrast is expected to be as large as possible. Because all possible Hamming weights of encryption blocks are evenly ranging from 0 to t, $\forall$ X $\in \Gamma_{Qual}$, the contrasts α_i^X $(0 \leq i \leq t-1)$ are expected to be equal. When the overall contrast reaches its maximum, and $\forall\ X \in \Gamma_{Qual}$, the contrasts α_i^X $(0 \leq i \leq t-1)$ are equal, the ME-VCS is contrast-optimal. The pixel expansion is expected to be as small as possible. When the pixel expansion reaches its minimum, the ME-VCS is pixel-expansion-optimal. When a ME-VCS is both contrast-optimal and pixel-expansion-optimal, we say that the ME-VCS is optimal.

Remark: If the size of encryption blocks is one, the definition of ME-VCS coincides with that of VCS. In other words, a $(\{\Gamma_{Qual}, \Gamma_{Forb}\}, n, 1)$-ME-VCS is the same as a $(\{\Gamma_{Qual}, \Gamma_{Forb}\}, n)$-VCS. The model of Naor and Shamir is a special case of the proposed ME-VCS. The concept of basis matrices in VCS can easily be applied to ME-VCS. When $(\Gamma_{Qual}, \Gamma_{Forb})$ represents a (k, n) threshold structure, for convenience, we can simply write $(\{\Gamma_{Qual}, \Gamma_{Forb}\}, n, t)$-ME-VCS as (k, n, t)-ME-VCS.

3 Multi-pixel Encryption Visual Cryptography Scheme

In this section, we first give an upper bound of the overall contrast of ME-VCS. Then we give a lower bound of the pixel expansion of (n, n, t)-ME-VCS. At last, we build a contrast-optimal ME-VCS from a contrast-optimal VCS and build an optimal (n, n, t)-ME-VCS from an optimal (n, n)-VCS.

Theorem 1. *We denote the contrast of a contrast-optimal $(\{\Gamma_{Qual}, \Gamma_{Forb}\}, n)$-VCS as α^*. We denote the overall contrast of a contrast-optimal $(\{\Gamma_{Qual}, \Gamma_{Forb}\}, n, t)$-ME-VCS as α_{me}. Then we must have that $\alpha_{me} \leq \alpha^*$.*

Proof: Let $(C_0, C_1, \ldots, C_t)$ be the $t+1$ collections of Boolean matrices of a contrast-optimal $(\{\Gamma_{Qual}, \Gamma_{Forb}\}, n, t)$-ME-VCS. It is easy to see that C_0 and C_t constitute a $(\{\Gamma_{Qual}, \Gamma_{Forb}\}, n)$-VCS.

In the following, we calculate the contrast of the $(\{\Gamma_{Qual}, \Gamma_{Forb}\}, n)$-VCS constructed from C_0 and C_t. Let l_i^X $(0 \leq i \leq t)$ be the minimum Hamming weights of the stacked patterns of a share matrix from C_i restricted to qualified set X. Let h_i^X $(0 \leq i \leq t)$ be the maximum Hamming weights of the stacked patterns of a share matrix from C_i restricted to qualified set X. The contrasts of the $(\{\Gamma_{Qual}, \Gamma_{Forb}\}, n, t)$-ME-VCS restricted to qualified set X are $\alpha_i^X = \frac{l_{i+1}^X - h_i^X}{m}$

$(0 \leq i \leq t-1)$. The contrast of the above $(\{\Gamma_{Qual}, \Gamma_{Forb}\}, n)$-VCS restricted to qualified set X is $\alpha_X = \frac{l_t^X - h_0^X}{m}$. Since $l_i^X \leq h_i^X$ $(0 \leq i \leq t)$, we get that $\sum_{i=0}^{t-1} \alpha_i^X \leq \alpha_X$. From the definition of overall contrast of ME-VCS, we get that $\alpha_{me} = \min_{X \in \Gamma_{Qual}} \sum_{i=0}^{t-1} \alpha_i^X$. The contrast of the above $(\{\Gamma_{Qual}, \Gamma_{Forb}\}, n)$-VCS constructed from C_0 and C_t is $\alpha = \min_{X \in \Gamma_{Qual}} \alpha_X$. Thus it holds that $\alpha_{me} \leq \alpha$. Since α^* is the optimal (maximal) contrast for $(\{\Gamma_{Qual}, \Gamma_{Forb}\}, n)$-VCS, it results that $\alpha_{me} \leq \alpha \leq \alpha^*$. □

In the following, we give a lower bound of the pixel expansion of (n, n, t)-ME-VCS as follows.

Theorem 2. *In an (n, n, t)-ME-VCS, we denote its pixel expansion as m, then we have that $m \geq t \times 2^{n-1}$.*

Proof: It is known that the contrast of (n, n)-VCS is upper bounded by $\frac{1}{2^{n-1}}$ (see [13]). In an (n, n, t)-ME-VCS, we denote its overall contrast as α_{me}. Because there is only one qualified set in (n, n, t)-ME-VCS, the overall contrast of the scheme equals to the overall contrast restricted to the qualified set. We will not distinguish them in the following discussion. We denote the contrast of the scheme between encryption blocks of Hamming weight i $(0 \leq i \leq t-1)$ and those of Hamming weight $i+1$ as α_i. From the definition of overall contrast, we know that $\alpha_{me} = \sum_{i=0}^{t-1} \alpha_i$. From Theorem 1, we know that $\alpha_{me} \leq \frac{1}{2^{n-1}}$. Thus it holds that $\sum_{i=0}^{t-1} \alpha_i \leq \frac{1}{2^{n-1}}$. Let $\alpha = \min_{i=0}^{t-1} \{\alpha_i\}$. Since $\alpha \leq \frac{1}{t} \times \sum_{i=0}^{t-1} \alpha_i \leq \frac{1}{t \times 2^{n-1}}$, we have that $\frac{1}{\alpha} \geq t \times 2^{n-1}$. Since the difference between the minimal Hamming weight of recovered patterns of encryption blocks of Hamming weight $i+1$ $(0 \leq i \leq t-1)$ and the maximal Hamming weight of those of Hamming weight i is at least one, we have that $\alpha \times m \geq 1$. Thus it holds that $m \geq \frac{1}{\alpha} \geq t \times 2^{n-1}$. □

In the following, we will build a contrast-optimal ME-VCS from a contrast-optimal VCS. Our method is similar to the hybrid technique widely used in complexity theory and theoretical cryptography, see chap. 3 in [5], chap. 2 in [6] and [4]. Let M_0 and M_1 be the basis matrices of a contrast-optimal $(\{\Gamma_{Qual}, \Gamma_{Forb}\}, n)$-VCS with contrast α^* and pixel expansion m. The following $t+1$ basis matrices G_i $(0 \leq i \leq t)$ define a contrast-optimal $(\{\Gamma_{Qual}, \Gamma_{Forb}\}, n, t)$-ME-VCS.

$$G_i = \underbrace{M_0 \circ \ldots \circ M_0}_{t-i} \circ \underbrace{M_1 \circ \ldots \circ M_1}_{i} \qquad (0 \leq i \leq t).$$

Theorem 3. *The above G_i ($0 \leq i \leq t$) define a contrast-optimal ($\{\Gamma_{Qual}, \Gamma_{Forb}\}, n, t$)-ME-VCS.*

Proof: The Hamming weight of the stacked pattern of M_0 restricted to qualified set X is denoted as w_0^X. The Hamming weight of the stacked pattern of M_1 restricted to qualified set X is denoted as w_1^X. The contrast of the $(\{\Gamma_{Qual}, \Gamma_{Forb}\}, n)$-VCS restricted to qualified set X is $\alpha_X = \frac{w_1^X - w_0^X}{m}$. The contrast of the $(\{\Gamma_{Qual}, \Gamma_{Forb}\}, n)$-VCS is $\alpha^* = \min_{X \in \Gamma_{Qual}} \alpha_X$.

The Hamming weight of the stacked pattern of G_i restricted to qualified set X is denoted as l_i^X $(0 \leq i \leq t)$. From the construction of G_i, we know that $l_i^X = w_0^X \times (t-i) + w_1^X \times i$ $(0 \leq i \leq t)$. So the contrast of qualified set X between encryption blocks of Hamming weight i $(0 \leq i \leq t-1)$ and those of Hamming weight $i+1$ is $\alpha_i^X = \frac{l_{i+1}^X - l_i^X}{m \times t} = \frac{w_1^X - w_0^X}{m \times t} = \frac{\alpha_X}{t} > 0$. The contrast condition of the ME-VCS is satisfied. The overall contrast of qualified set X is $\alpha_X^{me} = \sum_{i=0}^{t-1} \alpha_i^X = t \times (\frac{\alpha_X}{t}) = \alpha_X$. The overall contrast of the scheme is $\alpha = \min_{X \in \Gamma_{Qual}} \alpha_X^{me} = \min_{X \in \Gamma_{Qual}} \alpha_X = \alpha^*$. From Theorem 1, we know that the overall contrast reaches its maximum value. Besides, $\forall\ X \in \Gamma_{Qual}$, the contrasts α_i^X $(0 \leq i \leq t-1)$ are equal up. Thus the $(\{\Gamma_{Qual}, \Gamma_{Forb}\}, n, t)$-ME-VCS is contrast-optimal. The security condition follows from the security of the $(\{\Gamma_{Qual}, \Gamma_{Forb}\}, n)$-VCS. Thus the conclusion holds. □

The construction of an optimal (n, n)-VCS can be found in [13]. In the following, we prove that the above construction builds an optimal (n, n, t)-ME-VCS from an optimal (n, n)-VCS.

Theorem 4. *Let M_0 and M_1 be the basis matrices of an optimal (n, n)-VCS, then the above G_i ($0 \leq i \leq t$) define an optimal (n, n, t)-ME-VCS.*

Proof: From Theorem 3, we know that the above (n, n, t)-ME-VCS is contrast-optimal. From the construction of G_i $(0 \leq i \leq t)$, we know that the pixel expansion of the above (n, n, t)-ME-VCS is $t \times 2^{n-1}$. From Theorem 2, we know that the above (n, n, t)-ME-VCS is pixel-expansion-optimal. Thus the conclusion holds. □

4 Conclusions

We first extended the model of Naor and Shamir (denoted as VCS) to the multi-pixel encryption model (denoted as ME-VCS), for which the model of Naor and Shamir is a special case of the proposed multi-pixel encryption model. Then we give an upper bound of the overall contrast of ME-VCS. We also give a lower bound of the pixel expansion of (n, n, t)-ME-VCS. At last, we built a contrast-optimal ME-VCS from a contrast-optimal VCS and built an optimal (n, n, t)-ME-VCS from an optimal (n, n)-VCS.

Acknowledgements. This work was supported by NSFC No.60903210.

References

1. Ateniese, G., Blundo, C., De Santis, A., Stinson, D.R.: Visual cryptography for general access structures. Information and Computation 129, 86–106 (1996)
2. Chang, C.Y.: Visual cryptography for color images. MS thesis, National Central University, Taiwan (2000)
3. Chen, Y.F., Chan, Y.K., Huang, C.C., Tsai, M.H., Chu, Y.P.: A multiple-level visual secret-sharing scheme without image size expansion. Information Sciences 177, 4696–4710 (2007)
4. Goldreich, O.: A note on computational indistinguishability (1989), `http://www.wisdom.weizmann.ac.il/~oded/PS/iplnote.ps`
5. Goldreich, O.: Foundations of cryptography: Basic tools, vol. 1, p. 392. Cambridge University Press (2001)
6. Goldwasser, S., Bellare, M.: Lecture notes on cryptography, (2008), `http://cseweb.ucsd.edu/~mihir/papers/gb.pdf`
7. Hofmeister, T., Krause, M., Simon, H.U.: Contrast-Optimal k Out of n Secret Sharing Schemes in Visual Cryptography. In: Jiang, T., Lee, D.T. (eds.) COCOON 1997. LNCS, vol. 1276, pp. 176–185. Springer, Heidelberg (1997)
8. Hofmeister, T., Krause, M., Simon, H.U.: Contrast-optimal k out of n secret sharing schemes in visual cryptography. Theoretical Computer Science 240(2), 471–485 (2000)
9. Hou, Y.C., Tu, C.F.: Visual cryptography techniques for color images without pixel expansion. Journal of Information, Technology and Society 1, 95–110 (2004) (in Chinese)
10. Krause, M., Simon, H.U.: Determining the optimal contrast for secret sharing schemes in visual cryptography. Combinatorics, Probability & Computing 12(3), 285–299 (2003)
11. Lin, C.H.: Visual cryptography for color images with image size invariable shares. MS thesis, National Central University, Taiwan (2002)
12. Liu, F., Wu, C.K., Lin, X.J.: Color visual cryptography schemes. IET Information Security 2(4), 151–165 (2008)
13. Naor, M., Shamir, A.: Visual Cryptography. In: De Santis, A. (ed.) EUROCRYPT 1994. LNCS, vol. 950, pp. 1–12. Springer, Heidelberg (1995)
14. Tu, S.F.: On the design of protection scheme for digital images and documents based on visual secret sharing and steganography. PhD thesis, National Central University, Taiwan (2005)