Optimal XOR based (2,n)-Visual Cryptography Schemes

Feng Liu[1] and ChuanKun Wu[1]
[1]State Key Laboratory Of Information Security, Institute of Software
Chinese Academy of Sciences, Beijing 100190, China
Email: {liufeng, ckwu}@is.iscas.ac.cn

October 26, 2010

Abstract

A $(2, n)$-Visual Cryptography Scheme (VCS) is a kind of secret sharing scheme, where n participants share a secret image, and any two of them can recover the secret image visually without any cryptographic knowledge and computation devices, but any one of them cannot get any information about the secret image other than the size of the secret image. This paper studies the $(2, n) - VCS_{XOR}$, and shows the smallest (optimal) pixel expansion of such schemes, and the largest possible contrast for the $(2, n) - VCS_{XOR}$ given its optimal pixel expansion. It also shows the largest (optimal) contrast of the $(2, n) - VCS_{XOR}$, and the smallest possible pixel expansion of such schemes given their optimal contrast. The results of this paper show that the $(2, n) - VCS_{XOR}$ can achieve smaller pixel expansion and larger contrast than that of $(2, n) - VCS_{OR}$. It also shows that the construction of the basis matrix of optimal contrast $(2, n) - VCS_{XOR}$ is equivalent to the construction of binary codes when they reach the maximum capability, and the construction of a specific class of optimal contrast $(2, n) - VCS_{XOR}$ for $n = 2^k - 1$ is given.
Keywords: Secret sharing, Visual cryptography scheme, Coding theory

1 Introduction

The basic principle of Visual Cryptography Scheme (VCS) was first introduced by Naor and Shamir. The idea of the visual cryptography model proposed in [22] is to split an image into two random shares (printed on transparencies) which separately reveal no information about the original secret image other than the size of the secret image. The image is composed of black and white pixels. The original image can be reconstructed visually by superimposing the two shares. The underlying operation of such scheme is *OR*. Similar model of visual cryptography with different underlying operation has been proposed. Such as the *XOR* operation studied in [3, 16, 18, 30, 31], examples of the visual cryptography system under the *XOR* operation can be found in [16, 32, 36]. Besides, the XOR based VCS can be applied on some state of the art displays, such as multi-layer display [23]. In this paper, we denote VCS_{XOR} and VCS_{OR} as VCS under XOR and OR operations respectively. A simple 2 out of 2 VCS_{XOR} is shown in Figure 1: denote $\oplus$ as the *XOR* operation, we have $(d) = (b) \oplus (c)$ in Figure 1.

VCS seems quite primitive, however some of its properties make VCS quite useful. From a practical viewpoint, first, complex encryption techniques may not convince the users for better security, instead the users may feel more worries about those complex techniques they do not understand. For many users, seeing is believing. Second, traditional cryptography highly relies on complex computations, the attackers can not recover the plaintexts in a reasonable time without knowing the key. Hence, for the traditional cryptography, computation devices are necessary for decrypting ciphertexts. However, the computation devices are usually vulnerable to trojan horses and virus. Another possibility of leaking secrets comes from users' incorrect operations. To avoid

Figure 1: A 2 out of 2 VCS_{XOR} where (a) is the original image, (b) and (c) are the shares, (d) is the recovered image from (b) and (c).

this, it is usually required that the users know some professional cryptographic knowledge, which is not realistic for ordinary people in many circumstances. As we have already mentioned, VCS outputs a secret image on decrypting, and the users can see the decrypted image directly. Furthermore, the decryption of VCS does not rely on any computation devices and does not require the users to know any cryptographic knowledge. From the above viewpoint, VCS shows some advantages against the traditional cryptography. Many applications of VCS have been proposed by now [12, 14, 21, 25, 29, 38]. Besides, recently, many copyright protection schemes which take VCS as building blocks are proposed, for example [5, 6, 13, 17, 19, 35]. Although some of these copyright protection schemes take the *OR* based VCS as building blocks, it is clear that, if we change the *OR* based VCS to the *XOR* based ones, then the copyright schemes are still valid and can be significantly simplified.

VCS's are mainly characterized by two parameters: the pixel expansion, which is the number of sub-pixels each pixel of the original secret image is encoded into, and the contrast, which measures the clearness of the recovered image. To improve the quality of the recovered image, many schemes have been proposed in [2, 9, 22], but the drawbacks of those schemes are the large value of pixel expansion and that the participants have to take many shares with them. Recent studies show that VCS_{XOR} often has advantages on pixel expansion and contrast properties compared with VCS_{OR}, see examples in [18, 31]. In this paper, we focus on optimization of pixel expansion and contrast for VCS_{XOR}.

So far three ways have been found to realize the *XOR* based visual cryptography scheme. The first was proposed in [3, 30, 31], which realized the *XOR* operation by making use of the polarization property of light where two liquid crystal displays are needed. The second was proposed in [16], which realized the *XOR* operation by using a Mach-Zehnder Interferometer. And the third method, proposed in [33], needs a copy machine with the reversing function. By investigating the above three ways of realizing *XOR* based VCS, it is easy to find, that the decoding method of these three ways becomes more complicated when decoding more shares. Particularly, the first and the second methods need k Mach-Zehnder Interferometers or liquid crystal displays to decode the secret image for the $(k, n) - VCS_{XOR}$, and will inevitably make the cryptography system complicated and cause many difficulties, such as aligning the pixels and signal attenuation. For the third method, it will need many reversing copies to decode the secret image, see examples in [7, 33]. In other words, the *XOR* based VCS is most practical for the $(2, n)$ case. In this paper, we only consider the $(2, n) - VCS_{XOR}$.

Many studies in the literature also focused on $(2, n) - VCS$. Blundo et al. [2, 4] studies the contrast and pixel expansion bounds for the $(2, n) - VCS$ only under the *OR* operation. Santis [27] considers the contrast and pixel expansion bounds for $(2, n) - VCS$ under the combination function f, however, their pixel expansion bound $n < \binom{m}{\lfloor m/2 \rfloor}$ can be improved, and they do not give any explicit constructions for the $(2, n) - VCS$ with regard to the optimal pixel expansion and the optimal contrast. Biham [3] gives a simple construction of the $(2, n) - VCS_{XOR}$ and Tuyls et al. [30, 31] presents an simple equivalence relationship between the construction of the $(2, n) -$

VCS_{XOR} and the binary code. However neither of them has given deep discussions on how to construct optimal $(2,n)-VCS_{XOR}$ with regard to the pixel expansion or contrast.

The construction of schemes with both optimal contrast and optimal pixel expansion seems impossible. So, in this paper we construct VCS with optimal pixel expansion and optimal contrast respectively. Without confusion, we sometimes refer to the largest contrast as the optimal contrast, and smallest pixel expansion as the optimal pixel expansion. Compared to the studies in the literature, the contributions of this paper can be reflected from the following three aspects:

- We construct the $(2,n)-VCS_{XOR}$ with the optimal pixel expansion $\lceil \log_2 n \rceil$. We also study the contrast property of such schemes, and prove that, the largest possible contrast of the optimal pixel expansion $(2,n)-VCS_{XOR}$ is $\frac{1}{\lceil \log_2 n \rceil}$, and the largest average contrast of such schemes is $\frac{2\lfloor n/2 \rfloor \lceil n/2 \rceil}{n(n-1)}$.

- We prove that the optimal contrast of $(2,n)-VCS_{XOR}$ is $\frac{2\lfloor n/2 \rfloor \lceil n/2 \rceil}{n(n-1)}$, which is twice better than the optimal contrast for the $(2,n)-VCS_{OR}$. Furthermore we show the smallest possible pixel expansion of the optimal contrast scheme that can be achieved and show how to construct such schemes. The pixel expansion bound of our scheme is proved to be optimal while the bound in [27] is not optimal.

- We further study the relationship between the optimal contrast $(2,n)-VCS_{XOR}$ and the binary code. We find, that for odd n, the rows of the basis matrix of the optimal contrast $(2,n+1)-VCS_{XOR}$ are equivalent to the $(m, \frac{n+1}{2n}m)$ binary code which reaches its maximum capacity, and the rows of the basis matrix of the optimal contrast $(2,n)-VCS_{XOR}$ are equivalent to the $(m, \frac{(n+1)m}{2n}, \frac{(n\pm 1)m}{2n})$ constant weight code which reaches its maximum capacity, hence this result enables us to use the known construction of maximum capacity binary codes to construct the optimal contrast $(2,n)-VCS_{XOR}$. In addition, we also give a construction of optimal contrast $(2,n)-VCS_{XOR}$ for $n=2^k-1$, by using the technique of m-sequences.

The rest of this paper is organized as follows: Sec. 2 gives some definitions of VCS, and in Sec. 3, we study the schemes with smallest (optimal) pixel expansion, in Sec. 4, we study the schemes with largest (optimal) contrast, in Sec. 5, we study the relationship between the construction of optimal contrast VCS and that of binary codes with maximum capacity. The paper is then concluded in Sec. 6.

2 Preliminaries

In this section, we will give some definitions about visual cryptography under the operation $\bullet$, which can be the *OR* operation as discussed in [22] or the *XOR* operation as discussed in [3, 16, 30, 31]. We will restrict ourselves to images only consisting of black and white pixels and encode one pixel at a time, where we denote by 1 for a black pixel and 0 for a white pixel. In order to share a complete image, the scheme has to be applied to all the pixels in the image.

The $(2,n)-VCS_{XOR}$ is a special case of the $(k,n)-VCS_{XOR}$. By a $(k,n)-VCS_{XOR}$ we mean a scheme in which a secret pixel (black or white) is divided into n shares which are distributed to the n participants. Any subgroup of k out of these n participants, can reconstruct the secret but any subgroup consisting of less than k participants does not have any information other than the size about the secret image.

For a vector $v \in GF^m(2)$, we denote by $w(v)$ the number of 1's in the vector v (i.e. $w(v)$ is the Hamming weight of v). A (k,n)-VCS, denoted by (C_0, C_1), consists of two collections of $n \times m$ binary share matrices C_0 and C_1. To share a white (resp. black) pixel, a dealer (the one who sets

up the system) randomly chooses one of the matrices in C_0 (*resp.* C_1) and distributes its rows (shares) to the n participants of the scheme. For convenience, we call a column (resp. row) of a boolean matrix with an even number of 1's *even column (resp. row)* and otherwise *odd column (resp. row).*

More precisely, we give a formal definition of (k, n)-VCS as follows.

Definition 1 ([31]) *Let k, n, m, l and h be nonnegative integers satisfying $2 \leq k \leq n$ and $0 \leq l < h \leq m$. The two collections of $n \times m$ share matrices (C_0, C_1) constitute a threshold Visual Cryptography scheme $(k, n) - VCS$ if the following conditions are satisfied:*

1. *(Contrast) For any $s \in C_0$, the "$\bullet$" operation of any k out of n rows of s satisfies $w(v) \leq l$.*
2. *(Contrast) For any $s \in C_1$, the "$\bullet$" operation of any k out of n rows of s satisfies $w(v) \geq h$.*
3. *(Security) For any $i_1 < i_2 < \cdots < i_t$ in $\{1, 2, \cdots, n\}$ with $t < k$, the two collections of $t \times m$ matrices D_j for $j \in \{0, 1\}$, obtained by restricting each $n \times m$ matrix in C_j to rows $i_1, i_2, \cdots i_t$, they are indistinguishable in the sense that they contain the same matrices with the same frequencies.*

In the above definition,

1. v is the resulting vector of the "$\bullet$" operation over the restricted k out of the n rows.
2. h and l are the thresholds of the scheme, h is called *darkness level* and l is called the *whiteness level*.
3. m is called the pixel expansion of the scheme.
4. Define $\alpha = \frac{h-l}{m}$ as the contrast of *VCS*. For underlying operations *OR* and *XOR* we use the notations α_{OR} and α_{XOR} respectively, if necessary.

We notice that the definitions of VCS under *OR* and *XOR* operation are quite similar. Actually when we do the summation of vectors we mean *OR* and *XOR* operation on them respectively, unless we point out explicitly.

The definition of the *average contrast* was already given in [3, 15, 24]. Here we adopt the same definition, i.e. $\bar{\alpha} = \frac{\bar{h}-\bar{l}}{m}$, where $\bar{h}$ is the average value of darkness level in collection C_1 and $\bar{l}$ is the average value of the whiteness level in collection C_0. For the $(2, n) - VCS$, we can calculate the average contrast as follows: Formally, denote r_i, r_j as two rows of an $n \times m$ binary matrix M in C_1 (resp. C_0), and $\bar{h}_M$ (resp. $\bar{l}_M$) be the average value of darkness level (resp. whiteness level) of M, defined as: $\bar{h}_M = \frac{\sum_{1 \leq i < j \leq n} w(r_i \oplus r_j)}{\binom{n}{2}}$ and $\bar{h} = \frac{\sum_{M \in C_1} \bar{h}_M}{|C_1|}$ (resp, $\bar{l}_M = \frac{\sum_{1 \leq i < j \leq n} w(r_i \oplus r_j)}{\binom{n}{2}}$ and $\bar{l} = \frac{\sum_{M \in C_0} \bar{l}_M}{|C_0|}$). Note that, the difference between $\bar{h}_M$ and $\bar{l}_M$ is that, they are computed from the different collections C_1 or C_0 respectively. At this time, we can calculate the average contrast by using the formula $\bar{\alpha} = \frac{\bar{h}-\bar{l}}{m}$.

The average contrast is used to evaluate the clearness of the recovered secret image in an overall viewpoint. But it has the disadvantage in reflecting the clearness of the details in the recovered secret image, i.e. the average contrast is suitable as a criterion of the clearness for the secret images drawn with fairly thick lines (see discussions in [37]). The average contrast is important for the VCS's, especially when their share matrices have different values of $w(r_i \oplus r_j)$ where $1 \leq i < j \leq n$. For such share matrices, the traditional definition of contrast only reflect the smallest (resp. largest) value of the $w(r_i \oplus r_j)$ in the collections C_1 (resp. C_0), while the average contrast reflect the values of $w(r_i \oplus r_j)$ from an overall viewpoint. So for the scheme in Example 1 of Section 3, when the

secret image is drawn with fairly thick lines, the recovered secret image will look like an image with contrast $\frac{2}{3}$, rather than $\frac{1}{2}$.

Note that the pixel expansion satisfies $m \geq 1$ and the contrast and average contrast satisfy $0 < \alpha, \bar{\alpha} \leq 1$. In general, we are interested in schemes with m being as small as possible and with the contrast α and the average contrast $\bar{\alpha}$ being as large as possible.

As stated in Definition 1, the first two conditions ensure that the participants will be able to distinguish the black and white pixels, and the third condition ensures the security of the scheme. In fact, for a VCS with $\alpha = 0$ and $\bar{\alpha} > 0$, the participants can still see the decrypted secret image. However, we do not consider this case in this paper.

To simplify the discussion, all of our constructions in this paper will be based on basis matrix as defined in Definition 2. And since we only consider the $(2, n) - VCS_{XOR}$ in this paper, the following definition of basis matrix is only for $(2, n) - VCS_{XOR}$, and hence has a few differences from the general one of Definition 1. One will find that the Definition 2 will simplifies the discussions significantly on analyzing and constructing optimal $(2, n) - VCS_{XOR}$.

Definition 2 (Basis matrix of $(2, n) - VCS_{XOR}$) *Let n, m and h be positive integers satisfying $0 < h \leq m$. An $n \times m$ binary matrix M is called a basis matrix for a $(2, n) - VCS_{XOR}$, if it satisfies the following contrast condition: the weight of the XOR (denoted by $\oplus$) of any 2 of n rows in M satisfies: $w(j_{i_1} \oplus j_{i_2}) \geq h$, where j_i $(i = 1, \cdots, n)$ is a row of M and $h \geq 1$.*

By using the basis matrix M presented in Definition 2, one can realize an $(2, n) - VCS_{XOR}$ construction under the Definition 1 as follows: Define $M(i)$ be the $n \times m$ matrix obtained by a cyclic shift on the rows of M over i positions, denote by C_1 the collection $C_1 = \{M(0), M(1), \cdots, M(n-1)\}$. Define $A(\mathbf{r})$ be the $n \times m$ matrix for which each row equals $\mathbf{r}$, and denote by C_0 the collection $C_0 = \{A(j_1), A(j_2), \cdots, A(j_n)\}$, where $j_1, j_2, \cdots, j_n$ are the n rows of M.

Note that in the above definition, the value of the whiteness level $l = 0$, and the contrast $\alpha_{XOR} = h/m$. This approach of the construction of $(2, n) - VCS_{XOR}$ will have small memory requirements (it keeps only a basis matrix) and it is efficient (to choose a matrix in C_1 or C_0) as it only needs to cyclicly shift the rows of the basis matrix, or choose a row from M and generate $A(\mathbf{r})$).

We note that some kinds of sub-matrices always exist in the basis matrix of VCS_{XOR}. For example, the sub-matrices $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$ or $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ (i.e. the sub-matrix which consists of a 1 and a 0) always exist in any basis matrix of the $(2, n) - VCS_{XOR}$ since they cause of the contrast of the VCS_{XOR}, because the $\oplus$ of the two rows of them is 1, recall that the other patterns $\begin{bmatrix} 0 \\ 0 \end{bmatrix}$ and $\begin{bmatrix} 1 \\ 1 \end{bmatrix}$ do not contribute to the value of $w(v)$ in the Definition 1. In this paper, these kinds of sub-matrices are called *unavoidable patterns*. Note that, the definition of the unavoidable pattern under the *XOR* operation is different to the definition in [2, 4], where the two patterns $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$ and $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ are called unavoidable patterns respectively, but, here and hereafter, we call the two patterns together as the unavoidable patterns under the *XOR* operation. i.e. the basis matrix of the Definition 2 contains at least one of the two patterns. For an example of the unavoidable patterns, see in Example 1.

Furthermore, it is easy to verify that any share matrix in the collection C_1 of Definition 1 for a $(2, n) - VCS_{XOR}$ can be a basis matrix of Definition 2 (i.e. given any collections (C_0, C_1) of a $(2, n) - VCS_{XOR}$ of Definition 1, we can construct a basis matrix $(2, n) - VCS_{XOR}$ under the Definition 2, which have the same pixel expansion and an equal or larger contrast), which implies there does not exist a $(2, n) - VCS_{XOR}$ under Definition 1 that has smaller pixel expansion or larger contrast. And because we study the optimal schemes (smallest pixel expansion and largest contrast) of $(2, n) - VCS_{XOR}$, so in this paper, we can study the $(2, n) - VCS_{XOR}$ only based on the basis matrix defined in the Definition 2.

3 $(2,n)-VCS_{XOR}$ with optimal pixel expansion

In this section, we show that the optimal pixel expansion of $(2,n)-VCS_{XOR}$ is $\lceil \log_2 n \rceil$. We also study the contrast property of such schemes, and prove that, the largest possible contrast of the optimal pixel expansion $(2,n)-VCS_{XOR}$ is $\frac{1}{\lceil \log_2 n \rceil}$, and the largest average contrast of such a scheme is $\frac{2\lfloor n/2 \rfloor \lceil n/2 \rceil}{n(n-1)}$. And give a concrete construction of $(2,n)-VCS_{XOR}$ that has largest possible contrast and average contrast given the optimal pixel expansion. It can be easily verified that the bounds here are far better than the one in [27], and the constructions are better than the ones in [31] with regard to the pixel expansion.

3.1 Optimal pixel expansion of $(2,n)-VCS_{XOR}$

The following theorem shows the optimal pixel expansion of $(2,n)-VCS_{XOR}$. Here and hereafter, we denote $\lceil x \rceil$ as the smallest integer larger than or equal to x, and denote m^* as the optimal pixel expansion of $(2,n)-VCS_{XOR}$.

Theorem 1 *The optimal pixel expansion of* $(2,n)-VCS_{XOR}$ *is* $m^* = \lceil \log_2 n \rceil$.

Proof: Assume that there exists a $(2,n)-VCS_{XOR}$ with pixel expansion $m < \lceil \log_2 n \rceil$, and denote M as the basis matrix for a black secret pixel, then there must exist two identical rows in the basis matrix. And the weight of the vector of the sum of the two identical rows is 0, which is in contradiction with the contrast condition of M. Hence we must have that $m^* \geq \lceil \log_2 n \rceil$.

Let the n rows of M be arbitrary n different vectors of length $\lceil \log_2 n \rceil$, then the Hamming weight of any two of the n rows will be no less than 1, according to the Definition 2, we get to know that M is a basis matrix of the $(2,n)-VCS_{XOR}$ with $h=1$, hence the contrast $\alpha_{XOR} = h/m \geq \frac{1}{\lceil \log_2 n \rceil}$. □

To make thing clearer, we give the following example:

Example 1 *A basis matrix of a* $(2,3)-VCS_{XOR}$ *can be:*

$$M = \begin{bmatrix} 00 \\ 01 \\ 11 \end{bmatrix}$$

and hence:

$$C_1 = \left\{ \begin{bmatrix} 00 \\ 01 \\ 11 \end{bmatrix}, \begin{bmatrix} 01 \\ 11 \\ 00 \end{bmatrix}, \begin{bmatrix} 11 \\ 00 \\ 01 \end{bmatrix} \right\} \text{ and } C_0 = \left\{ \begin{bmatrix} 00 \\ 00 \\ 00 \end{bmatrix}, \begin{bmatrix} 01 \\ 01 \\ 01 \end{bmatrix}, \begin{bmatrix} 11 \\ 11 \\ 11 \end{bmatrix} \right\}$$

the contrast of this scheme is $\alpha_{XOR} = 1/2$ *and the average contrast of this scheme is* $\alpha_{XOR} = 2/3$.

3.2 Largest possible contrast of $(2,n)-VCS_{XOR}$ given optimal pixel expansion and constructions

Given a $(2,n)-VCS_{XOR}$ with optimal pixel expansion, its largest possible contrast should be no larger than the optimal contrast of $(2,n)-VCS_{XOR}$ without the optimal pixel expansion constraint. The following theorem shows the largest possible contrast of the optimal pixel expansion $(2,n)-VCS_{XOR}$.

Theorem 2 *The largest possible contrast of the* $(2,n)-VCS_{XOR}$ *given the optimal pixel expansion is* $\alpha_p^* = \frac{1}{\lceil \log_2 n \rceil}$.

Proof: Denote $m^* = \lceil \log_2 n \rceil$ as the smallest pixel expansion of the $(2,n) - VCS_{XOR}$. We have that $\log_2 n \leq m^* < \log_2 n + 1$, i.e. $2^{m^*-1} < n \leq 2^{m^*}$. Assuming that there exists a $(2,n) - VCS_{XOR}$ with optimal pixel expansion that has contrast $\alpha_p^* \geq \frac{2}{m^*}$, i.e. $\alpha_p^* \cdot m^* \geq 2$, this means that at least 2 positions are different for any pair of rows of the share matrix in the collection C_1 of a $(2,n) - VCS_{XOR}$. Hence, such pair of rows which have only 1 position being different can not both appear as rows of the share matrix. For the collection of all the vectors of length m, by adding the vector $\underbrace{0 \cdots 0}_{m-1}1$ to them, we have that each vector corresponds to a vector which has only 1 position being different from it. Hence the 2^{m^*} vectors are divided into 2^{m^*-1} groups of vectors with each group contains two vectors. In order to form a share matrix in the collection C_1 of a $(2,n) - VCS_{XOR}$, only one of the two vectors can be chosen in each group, hence, there are only 2^{m^*-1} vectors at most to form the share matrix. Because the number of rows of a $(2,n) - VCS_{XOR}$ satisfies: $2^{m^*-1} < n \leq 2^{m^*}$, i.e. there are not enough vectors, say n vectors, to form a $(2,n) - VCS_{XOR}$. Hence, we reach a contradiction. This contradiction means $\alpha_p^* < \frac{2}{m^*}$ (i.e. $\alpha_p^* \cdot m^* < 2$), because $\alpha_p^* \cdot m^*$ is integer and $\alpha_p^* \geq \frac{1}{m^*}$ (recall that the Definition 2 requires $h \geq 1$), hence the largest possible contrast of the $(2,n) - VCS_{XOR}$ given the optimal pixel expansion $m^* = \lceil \log_2 n \rceil$ is $\alpha_p^* = \frac{1}{\lceil \log_2 n \rceil}$. □

The following Example 2 will make the above proof clearer.

Example 2 *Take the $(2,3) - VCS_{XOR}$ as an example, we have $m^* = 2$. Assume that there exists a share matrix M in the collection C_1 of a $(2,3) - VCS_{XOR}$ with contrast $\alpha_{XOR} > 1/2$, i.e. the hamming distance of arbitrary two rows of M is at least 2. Because $(00) \oplus (01) = (01)$, $(01) \oplus (01) = (00)$, $(10) \oplus (01) = (11)$, $(11) \oplus (01) = (10)$, we know that the four vectors $\{(00), (01), (10), (11)\}$ can be divided into two groups $\{(00), (01)\}, \{(10), (11)\}$, and the vectors (00) and (01) can not both appear in M. Similarly, we have the vector (10) and (11) can not both appear in M either, so we have only $2^{2-1} = 2$ vectors to form M which is not enough since at least $n = 3$ vectors are needed. Hence such share matrix M does not exist, and hence such VCS does not exist.*

The largest possible contrast of a $(2,n) - VCS_{XOR}$ is affected by its pixel expansion constraint. However the average contrast is not. We show below that even a $(2,n) - VCS_{XOR}$ has optimal pixel expansion, its average contrast can reach its maximum value.

Theorem 3 *There exists a $(2,n) - VCS_{XOR}$ with the optimal pixel expansion $m^* = \lceil \log_2 n \rceil$ and the largest average contrast $\bar{\alpha}_{XOR} = \frac{2\lfloor n/2 \rfloor \lceil n/2 \rceil}{n(n-1)}$, and it is achieved if and only if all the rows of the basis matrix are different vectors and all the columns of the basis matrix have Hamming weight $\lfloor n/2 \rfloor$ or $\lceil n/2 \rceil$.*

Proof: Firstly, we prove the sufficiency: denote M as a matrix satisfies, all the rows are different vectors and all the columns have weight $\lfloor n/2 \rfloor$ or $\lceil n/2 \rceil$. According to the Definition 2, we get to know that M is a basis matrix of the $(2,n) - VCS_{XOR}$. And because all the columns have weight $\lfloor n/2 \rfloor$ or $\lceil n/2 \rceil$, we get to know that, the total number of the patterns $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$ and $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ in M is $\lfloor n/2 \rfloor \lceil n/2 \rceil \cdot m^*$, hence the average contrast is $\bar{\alpha}_{XOR} = \frac{\lfloor n/2 \rfloor \lceil n/2 \rceil \cdot m^*}{\binom{n}{2} \cdot m^*} = \frac{2\lfloor n/2 \rfloor \lceil n/2 \rceil}{n(n-1)}$. Assume that there are t 1's in one column of M, then the number of the patterns $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$ or $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ reaches its maximum when $t = \lfloor n/2 \rfloor$ or $\lceil n/2 \rceil$, and hence the value $\frac{2\lfloor n/2 \rfloor \lceil n/2 \rceil}{n(n-1)}$ is the largest possible average contrast. And it is not affected by the pixel expansion.

Then we prove the necessity: denote M as a share matrix of the $(2,n) - VCS_{XOR}$ with the optimal pixel expansion $m^* = \lceil \log_2 n \rceil$ and the largest average contrast $\bar{\alpha}_{XOR} = \frac{2\lfloor n/2 \rfloor \lceil n/2 \rceil}{n(n-1)}$. According to the Definition 2, we get to know that all the rows of M are different vectors. Denote

the total number of the patterns $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$ or $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ in M as s, hence the average contrast will be $\bar{\alpha}_{XOR} = \frac{s}{\binom{n}{2}m^*}$, obviously, the average contrast $\bar{\alpha}_{XOR}$ reach its maximum when s reach its maximum, since s reaches its maximum when if all the columns have Hamming weight $\lfloor n/2 \rfloor$ or $\lceil n/2 \rceil$, the necessity follows. □

At this point, we give a concrete construction of $(2,n) - VCS_{XOR}$ that has largest possible contrast and average contrast given the optimal pixel expansion.

Construction 1 *Let M' be the $2^{\lceil \log_2 n \rceil} \times \lceil \log_2 n \rceil$ matrix that its rows contain all the vectors of length $\lceil \log_2 n \rceil$. Denote a row vector of M' as $r = (l_1, l_2, \cdots, l_{\lceil \log_2 n \rceil})$ where $l_1, l_2, \cdots, l_{\lceil \log_2 n \rceil} \in \{0,1\}$, and denote its complementary row vector as $\bar{r} = (1-l_1, 1-l_2, \cdots, 1-l_{\lceil \log_2 n \rceil})$. r and $\bar{r}$ are called a complementary row vector pair. For an even n, choose $(2^{\lceil \log_2 n \rceil} - n)/2$ complementary row vector pairs randomly, and for an odd n, choose $(2^{\lceil \log_2 n \rceil} - (n+1))/2$ complementary row vector pairs and another row vector randomly. Remove these rows from M', then the resulting $n \times \lceil \log_2 n \rceil$ matrix, denoted by M, is a basis matrix of $(2,n)-VCS_{XOR}$ with optimal pixel expansion $m^* = \lceil \log_2 n \rceil$, optimal contrast $\alpha_p^* = \frac{1}{\lceil \log_2 n \rceil}$ and largest average contrast $\bar{\alpha}_{XOR} = \frac{2\lfloor n/2 \rfloor \lceil n/2 \rceil}{n(n-1)}$.*

Proof: The pixel expansion and contrast properties are easy to be verified. We only prove the average contrast property.

Note that since M' only contains all the row vectors of length $\lceil \log_2 n \rceil$, then each column of M' contains $2^{\lceil \log_2 n \rceil - 1}$ 1's. And each column of a complementary row vector pair contains a 1. Hence after removing columns, for an even n, each column of M has $2^{\lceil \log_2 n \rceil - 1} - (2^{\lceil \log_2 n \rceil} - n)/2 = n/2$ 1's left. And for an odd n, note that we remove $(2^{\lceil \log_2 n \rceil} - (n-1))/2$ complementary row vector pairs and another row vector. Hence, the number of 1's in a column of M should be either $2^{\lceil \log_2 n \rceil - 1} - (2^{\lceil \log_2 n \rceil} - (n+1))/2 = (n+1)/2 = \lceil n/2 \rceil$ or $2^{\lceil \log_2 n \rceil - 1} - (2^{\lceil \log_2 n \rceil} - (n+1))/2 - 1 = (n-1)/2 = \lfloor n/2 \rfloor$. Then we have that all the rows of M are different vectors and all the columns of M have Hamming weight $\lfloor n/2 \rfloor$ or $\lceil n/2 \rceil$. According to Theorem 3, we have the scheme has largest average contrast $\bar{\alpha}_{XOR} = \frac{2\lfloor n/2 \rfloor \lceil n/2 \rceil}{n(n-1)}$. □

The Example 1 makes the above discussions clearer.

4 $(2,n) - VCS_{XOR}$ with optimal contrast

In this section, we will discuss the $(2,n) - VCS_{XOR}$ with the optimal contrast (not average contrast any more). We will first construct $(2,n) - VCS_{XOR}$ with optimal contrast $\alpha^*_{XOR} = \frac{2\lfloor n/2 \rfloor \lceil n/2 \rceil}{n(n-1)}$, which is twice of that of $(2,n) - VCS_{OR}$. And then we show the smallest possible pixel expansion of the $(2,n) - VCS_{XOR}$ given the optimal contrast, we will give explicit constructions for such schemes. The result of Theorem 7 shows the smallest possible pixel expansion of the optimal contrast $(2,n) - VCS_{XOR}$ is smaller than that of $(2,n) - VCS_{OR}$ in some cases.

4.1 Optimal contrast of $(2,n) - VCS_{XOR}$ and some structural properties

The following theorem shows the optimal contrast of the $(2,n) - VCS_{XOR}$.

Theorem 4 *The contrast for a $(2,n) - VCS_{XOR}$ satisfies $\alpha_{XOR} \leq \frac{2\lfloor n/2 \rfloor \lceil n/2 \rceil}{n(n-1)}$, and equality holds if and only if all the columns have weight $\lfloor n/2 \rfloor$ or $\lceil n/2 \rceil$ and the Hamming weight of the sum of any two rows of the basis matrix is exactly $\frac{2\lfloor n/2 \rfloor \lceil n/2 \rceil}{n(n-1)} \cdot m$, where m is the pixel expansion of the scheme.*

Proof: Denote M as the basis matrix of the $(2,n)-VCS_{XOR}$, and α_{XOR} as the contrast, the contrast of M is caused by the unavoidable patterns $\begin{bmatrix}0\\1\end{bmatrix}$ or $\begin{bmatrix}1\\0\end{bmatrix}$ in matrix M, because there are at most $\lfloor n/2\rfloor\cdot\lceil n/2\rceil$ unavoidable patterns $\begin{bmatrix}0\\1\end{bmatrix}$ or $\begin{bmatrix}1\\0\end{bmatrix}$ in each column of M, hence there are at most $m\cdot\lfloor n/2\rfloor\cdot\lceil n/2\rceil$ unavoidable patterns in M. Therefore we have: $\binom{n}{2}\cdot\alpha_{XOR}\cdot m\le m\cdot\lfloor n/2\rfloor\cdot\lceil n/2\rceil$, i.e. $\alpha_{XOR}\le\frac{2\lfloor n/2\rfloor\lceil n/2\rceil}{n(n-1)}$, and the equality holds if all the columns have weight $\lfloor n/2\rfloor$ or $\lceil n/2\rceil$.

And when the contrast of M is the largest contrast $\frac{2\lfloor n/2\rfloor\lceil n/2\rceil}{n(n-1)}$, then the Hamming weight of the sum of any two rows of M is at least $\frac{2\lfloor n/2\rfloor\lceil n/2\rceil}{n(n-1)}\cdot m$. Hence we get to know the Hamming weight of the sum of any two rows of the share basis matrix is exactly $\frac{2\lfloor n/2\rfloor\lceil n/2\rceil}{n(n-1)}\cdot m$, otherwise, the total number of the unavoidable patterns $\begin{bmatrix}0\\1\end{bmatrix}$ or $\begin{bmatrix}1\\0\end{bmatrix}$ in matrix M will be more than $m\cdot\lfloor n/2\rfloor\cdot\lceil n/2\rceil$, which is impossible. On the other hand, when the Hamming weight of the sum of any two rows of the share basis matrix is exactly $\frac{2\lfloor n/2\rfloor\lceil n/2\rceil}{n(n-1)}\cdot m$ the contrast of the scheme is $\frac{2\lfloor n/2\rfloor\lceil n/2\rceil}{n(n-1)}$.

Such schemes always exist, a simple construction can be: taking all the different vectors with $\lfloor n/2\rfloor$ 1's as the columns of the basis matrix M of the $(2,n)-VCS_{XOR}$, then this scheme will have the largest contrast $\alpha_{XOR}=\frac{2\lfloor n/2\rfloor\lceil n/2\rceil}{n(n-1)}$ and pixel expansion $m=\binom{n}{\lfloor n/2\rfloor}$. □

The optimal contrast $(2,n)-VCS_{OR}$ has already been studied in [4]. The following lemma shows the optimal contrast of $(2,n)-VCS_{OR}$ and a structural property of such scheme.

Lemma 1 (Property 2 of Lemma 4.3 in [4]) *For any pair of distinct rows of the basis matrix M of the $(2,n)-VCS_{OR}$ with optimal contrast for the black secret pixel, the unavoidable pattern $\begin{bmatrix}0\\1\end{bmatrix}$ (resp. $\begin{bmatrix}1\\0\end{bmatrix}$) appears exactly $\alpha^*_{OR}\cdot m$ times, where $\alpha^*_{OR}=\frac{\lfloor n/2\rfloor\lceil n/2\rceil}{n(n-1)}$.*

From Lemma 1, it is clear that the optimal contrasts of $(2,n)-VCS_{XOR}$ and $(2,n)-VCS_{OR}$ satisfy $\alpha^*_{XOR}=2\alpha^*_{OR}$, the reason is that the unavoidable patterns $\begin{bmatrix}0\\1\end{bmatrix}$ and $\begin{bmatrix}1\\0\end{bmatrix}$ both contribute to the contrast in $(2,n)-VCS_{XOR}$, but only one of them contributes to the contrast in $(2,n)-VCS_{OR}$. Furthermore, we have the following theorem which reveals the relationship between the optimal contrast of $(2,n)-VCS_{XOR}$ and $(2,n)-VCS_{OR}$.

Theorem 5 *The basis matrix of a optimal contrast $(2,n)-VCS_{OR}$ for the black secret pixel is also a basis matrix of a optimal contrast $(2,n)-VCS_{XOR}$. Hence the smallest pixel expansion for the optimal contrast $(2,n)-VCS_{XOR}$ is no larger than that of optimal contrast $(2,n)-VCS_{OR}$.*

Proof: Denote M as the basis matrix of the $(2,n)-VCS_{OR}$ with the smallest pixel expansion and contrast $\alpha^*_{OR}=\frac{\lfloor n/2\rfloor\lceil n/2\rceil}{n(n-1)}$. By Lemma 1, we know that the pattern $\begin{bmatrix}0\\1\end{bmatrix}$ (*resp.* $\begin{bmatrix}1\\0\end{bmatrix}$) appears exactly $\alpha^*_{OR}\cdot m$ times, hence the contrast of M under the *XOR* operation is $\alpha^*_{XOR}=2\alpha^*_{OR}=\frac{2\lfloor n/2\rfloor\lceil n/2\rceil}{n(n-1)}$. Hence M is the basis matrix of a optimal contrast $(2,n)-VCS_{XOR}$. And the smallest possible pixel expansion for the optimal contrast $(2,n)-VCS_{XOR}$ is no larger than that of the optimal contrast $(2,n)-VCS_{OR}$. □

We then turn to discuss the lower bounds of the pixel expansion of $(2,n)-VCS_{XOR}$ given the optimal contrast, and such bounds for the $(2,n)-VCS_{OR}$ has been studied in [4] by the following lemma.

Lemma 2 (Theorem 4.9 in [4]) *Denote m as the pixel expansion of $(2,n)-VCS_{OR}$ with optimal contrast, then the following equations hold:*

$$m \geq \begin{cases} 2n-2 & if\ \ n\ \ is\ even \\ n & if\ \ n \equiv 3\ mod\ 4 \\ 2n & if\ \ n \equiv 1\ mod\ 4 \end{cases}$$

the equality holds if the Hadamard Matrix Conjecture is true. (The Hadamard Matrix Conjecture says that Hadamard matrices exist for all orders divisible by four.)

By Theorem 5 and Lemma 2, and assuming the Hadamard Matrix Conjecture holds, we have the following corollary:

Corollary 1 *Assuming the Hadamard Matrix Conjecture holds, the smallest possible pixel expansion m_c^* of the $(2,n) - VCS_{XOR}$ given the optimal contrast are smaller than that of the optimal contrast $(2,n) - VCS_{OR}$, i.e.*

$$m_c^* \leq \begin{cases} 2n-2 & if\ n\ is\ even \\ n & if\ n \equiv 3\ mod\ 4 \\ 2n & if\ n \equiv 1\ mod\ 4 \end{cases}$$

The following structural properties are satisfied by a $(2,n) - VCS_{XOR}$.

Lemma 3 (Structural properties) *Denote M as the basis matrix of a $(2,n) - VCS_{XOR}$ with contrast α_{XOR}.*

1. *Let s be a column vector of M, and $\bar{s}$ be the complementary vector of s. Denote $M^{'}$ as the matrix in which we replace the column s by $\bar{s}$, then $M^{'}$ is also a basis matrix of a $(2,n) - VCS_{XOR}$ with contrast α_{XOR}. Hence if there exists a basis matrix of $(2,n) - VCS_{XOR}$ with optimal contrast α_{XOR}^*, then there must exist a basis matrix of $(2,n) - VCS_{XOR}$ with all the columns have constant weight $\lfloor n/2 \rfloor$ (resp. $\lceil n/2 \rceil$) and optimal contrast α_{XOR}^*.*
2. *Denote $r_1, r_2, \cdots, r_n$ as the row vectors of M, then the matrix $M^{'}$ formed by the row vectors $r_1 + r, r_2 + r, \cdots, r_n + r$, where r is an arbitrary vector of length m, is also a basis matrix of a $(2,n) - VCS_{XOR}$ with contrast α_{XOR}. Hence there exist a basis matrix of a $(2,n) - VCS_{XOR}$ with one of its rows is the zero vector.*

Proof: Property 1: denote a and b as the ith and jth entries of s, denote $l_1, \cdots, l_n$ as the row vectors of the basis matrix M, and $l_1^{'}, \cdots, l_n^{'}$ as the row vectors of the matrix $M^{'}$, and because $a \oplus b = \bar{a} \oplus \bar{b}$, we get to know that by replacing some columns of M with their complementary vectors does not affect the Hamming weight of the "$\oplus$" operation of the two rows of M, i.e. $l_i \oplus l_j = l_i^{'} \oplus l_j^{'}$ where $i, j \in \{1, 2, \cdots n\}$, hence the matrix $M^{'}$ is also a basis matrix of a $(2,n) - VCS_{XOR}$ with contrast α_{XOR}. And for the optimal contrast $(2,n) - VCS_{XOR}$, replace all the column vectors with hamming weight $\lfloor n/2 \rfloor$(resp. $\lceil n/2 \rceil$, but not simultaneously) by its complementary vectors, the lemma follows.

Property 2: denote $r_1^{'}, \cdots, r_n^{'}$ as the row vectors of the matrix $M^{'}$, where $r_k^{'} = r_k \oplus r$ and $r_s^{'} = r_s \oplus r$, $k, s \in \{1, 2, \cdots n\}$, hence we have $r_k^{'} \oplus r_s^{'} = (r_k \oplus r) \oplus (r_s \oplus r) = r_k \oplus r_s$. The lemma follows.

The relationship of the two properties are as follows: by adding the m length vector $r = (0 \cdots 010 \cdots 0)$, where 1 is at the ith entry of r, is equivalent to replace the ith column of basis matrix with its complementary vector. □

Example 3 *The basis matrix M of a $(2,3) - VCS_{XOR}$ with contrast 2/3 is*

$$M = \begin{bmatrix} 001 \\ 010 \\ 100 \end{bmatrix}$$

Let s be the third column vector of M, i.e. $s = (100)^T$, and $\bar{s} = (011)^T$, replace the third column s of M by $\bar{s}$, we get:

$$M' = \begin{bmatrix} 000 \\ 011 \\ 101 \end{bmatrix}$$

it is easy to verify that M' is a basis matrix of another $(2,3) - VCS_{XOR}$ with the same contrast 2/3. Actually by adding the first row $r = (001)$ of M to the second and the third rows of M, we can also get the matrix M', And the first row of M' is the zero vector.

4.2 Smallest possible pixel expansion of the $(2,n) - VCS_{XOR}$ given optimal contrast and constructions

When a $(2,n) - VCS_{XOR}$ has the optimal contrast, it may have different pixel expansion properties. In this case, the smallest possible pixel expansion may be larger than in the general case without the optimal contrast constraint. In this section we show the smallest possible pixel expansion of the $(2,n) - VCS_{XOR}$ given its optimal contrast.

First we consider the case when the number of rows of the basis matrix is odd, i.e. the number of participants is odd.

Lemma 4 *For an odd n (≥ 3), if there exist a $(2,n) - VCS_{XOR}$ with optimal contrast α^*_{XOR}, and denote its pixel expansion as m, then we have $n|m$.*

Proof: Since n is odd, we have the optimal contrast $\alpha^*_{XOR} = \frac{2\lfloor n/2 \rfloor \lceil n/2 \rceil}{n(n-1)} = \frac{n+1}{2n}$, because $\alpha^*_{XOR} \cdot m$ is an integer (See Theorem 4), so we get $n|m$. □

Lemma 4 implies that $m \geq n$.

Lemma 5 *For a $(2,n) - VCS_{XOR}$ with $n \equiv 1 \ mod \ 4$ and optimal contrast $\alpha^*_{XOR} = \frac{n+1}{2n}$, the pixel expansion of such scheme satisfies $m \neq n$.*

Proof: For the case $n \equiv 1 \ mod \ 4$, since $n \neq 1$, we have $n \geq 5$. Assuming that there exists a matrix M, where M is the basis matrix of the $(2,n) - VCS_{XOR}$ with optimal contrast $\alpha^*_{XOR} = \frac{n+1}{2n}$ and pixel expansion $m = n$. Then we know that, there must exist two odd or two even rows in M since $n \geq 5$.

We consider stacking two shares (rows). Denote l_k and l_s as two odd rows(resp. even rows), then the weight of the sum of them will be $w(l_k \oplus l_s) = w(l_k) + w(l_s) - 2t$, where t is the number of the entries at which both l_k and l_s have value 1, hence $w(l_k \oplus l_s)$ is even. Because the weight of the sum of any pair of rows in M is $\alpha^*_{XOR} \cdot m = \frac{(n+1)}{2n} \cdot n = \frac{n+1}{2}$, which is odd, this results in a contradiction. This contradiction means that the Lemma 5 holds. □

Then we get the smallest pixel expansion for the case $n \equiv 1 \ mod \ 4$ as follows.

Corollary 2 *For $n \equiv 1 \ mod \ 4$, the smallest pixel expansion m^*_c of a $(2,n) - VCS_{XOR}$ given optimal contrast is $2n$.*

Proof: Lemma 4 and Lemma 5 states that $m_c^* \geq 2n$ and by combining the result of Corollary 1 we get to know $m_c^* = 2n$. □

In order to describe the construction of the $(2,n)-VCS$ more clearly, we introduce some basic results of the from the combinatorial mathematics. A (v,k,λ)-BIBD (Balanced Incomplete Block Design [8]) is a pair $(X,\mathcal{B})$, where X is a set of v elements (called points) and $\mathcal{B}$ is a collection of subsets of X (called blocks), such that each block contains exactly k points and each pair of points is a subset of exactly λ blocks. In a (v,k,λ)-BIBD, each point occurs in exactly $r = \lambda(v-1)/(k-1)$ blocks, and the total number of blocks is $b = vr/k = \lambda(v^2-v)/(k^2-k)$. The number r is called the *replication number* of the BIBD.

The following Lemma 6 provides the constructions for optimal contrast $(2,n)-VCS_{OR}$ by using BIBD.

Lemma 6

1. *(Theorem 4.7 of [4]) Assuming that $n \equiv 3 \bmod 4$ and there exists a $(2,n)-VCS_{OR}$ with pixel expansion m and contrast $\alpha_{OR}^* = \frac{\lfloor n/2 \rfloor \lceil n/2 \rceil}{n(n-1)}$. Then $m \geq n$ and $m = n$ if and only if there exists a $(n, \frac{n-1}{2}, \frac{n-3}{4})$-BIBD (or, equivalently, a Hadamard matrix of order n+1).*
2. *(Theorem 4.8 of [4]) Assuming that $n \equiv 1 \bmod 4$ and there exists a $(2,n)-VCS_{OR}$ with pixel expansion m and contrast $\alpha_{OR}^* = \frac{\lfloor n/2 \rfloor \lceil n/2 \rceil}{n(n-1)}$. Then $m \geq 2n$ and $m = 2n$ if and only if there exists a $(n, \frac{n-1}{2}, \frac{n-3}{2})$-BIBD or an $(n+1, \frac{n+1}{2}, \frac{n-1}{2})$-BIBD.*

By combining the Theorem 5 and the Lemma 6, for an odd n, it is clear that there exist $(2,n)-VCS_{XOR}$ with optimal contrast $\alpha_{XOR}^* = \frac{2\lfloor n/2 \rfloor \lceil n/2 \rceil}{n(n-1)} = \frac{n+1}{2n}$ if the Hadamard Matrix Conjecture holds. And the construction of the $(2,n)-VCS_{XOR}$ can be converted to the construction of the point-block incidence matrix of the corresponding BIBD, more details of such construction can be found in [4].

Second we consider the case when the number of rows of the basis matrix is even, i.e. there are even number of participants $n+1$ where n is odd.

Lemma 7 *Denote by m_c^* the smallest possible pixel expansion for a $(2,n)-VCS_{XOR}$ with odd n given the optimal contrast $\alpha_{XOR}^* = \frac{2\lfloor n/2 \rfloor \lceil n/2 \rceil}{n(n-1)} = \frac{n+1}{2n}$, then the smallest possible pixel expansion for a $(2,n+1)-VCS_{XOR}$ given the optimal contrast $\alpha_{XOR}^* = \frac{2\lfloor (n+1)/2 \rfloor \lceil (n+1)/2 \rceil}{n(n+1)} = \frac{n+1}{2n}$ is at least m_c^*.*

Proof: Reduction to absurdity.

Assuming that there exist a $(2,n+1)-VCS_{XOR}$ with optimal contrast $\alpha_{XOR}^* = \frac{n+1}{2n}$ and pixel expansion $m_c^{*'} (< m_c^*)$, and denote the basis matrix of this scheme is M', then the first n rows of M' constitute a $(2,n)-VCS_{XOR}$ with the same optimal contrast $\alpha_{XOR}^* = \frac{n+1}{2n}$ and pixel expansion $m_c^{*'}$, which is in contradiction with that m_c^* is the smallest possible pixel expansion for the $(2,n)-VCS_{XOR}$. □

The following lemma is the most important lemma of this paper which is required in our following discussions.

Lemma 8 *Denote M as an $n \times m$ binary matrix which satisfies:*

1. *n is odd*
2. *the minimum Hamming distance of any two rows of M is $\frac{(n+1)m}{2n}$*

3. each column of M has the same hamming weight $\frac{n-1}{2}$ (or respectively $\frac{n+1}{2}$)

then the rows of M all have the same hamming weight $\frac{(n-1)m}{2n}$ (or respectively $\frac{(n+1)m}{2n}$)

Proof: First we consider the equidistant binary code, assume that the rows of M are equidistant binary code with parameters: code length m, cardinality n, distance d, and the number k of 1's in each column. If a row has the Hamming weight w, then by counting the sum of distances to the remaining $n-1$ rows we have:

$$d(n-1) = w(n-k) + (m-w)k \tag{1}$$

hence we have:

$$d(n-1) - mk = (n-2k)w \tag{2}$$

Since n is odd, i.e. $n - 2k \neq 0$, the parameter w is determined uniquely from the equation (2).

Then we consider the general binary code (not limited to equidistant binary code) with the minimum Hamming distance d, then the equation (1) should be:

$$d(n-1) \leq w(n-k) + (m-w)k \tag{3}$$

Since $d = \frac{(n+1)m}{2n}$ and $k = \frac{n-1}{2}$ (for $k = \frac{n+1}{2}$ we reach the same conclusion), substitute for the d and k in inequality (3), then we have:

$$w \geq \frac{d(n-1) - mk}{(n-2k)} = \frac{(n-1)m}{2n} \tag{4}$$

Denote w_i as the Hamming weight of the ith row of M, $i = 0, 1, \cdots, n-1$, then, the total number of 1's in M is: (calculated by adding the rows)

$$\sum_{i=0}^{n-1} w_i \geq \frac{(n-1)m}{2} \tag{5}$$

and (calculated by adding the columns)

$$km = \frac{(n-1)m}{2} \tag{6}$$

combine the inequalities (4), (5) and equation (6), we have that $w = \frac{(n-1)m}{2n}$, hence the lemma follows. □

Theorem 6 *For an odd n, there exists a $(2,n)-VCS_{XOR}$ with the optimal contrast $\alpha^*_{XOR} = \frac{(n+1)}{2n}$ and pixel expansion m if and only if there exists a $(2,n+1)-VCS_{XOR}$ with optimal contrast same as $\alpha^*_{XOR} = \frac{(n+1)}{2n}$ and the same pixel expansion m.*

Proof: Because $\frac{2\lfloor n/2 \rfloor \lceil n/2 \rceil}{n(n-1)} = \frac{n+1}{2n} = \frac{2\lfloor (n+1)/2 \rfloor \lceil (n+1)/2 \rceil}{n(n+1)}$ we get to know that the optimal contrast of the $(2,n) - VCS_{XOR}$ and the $(2,n+1) - VCS_{XOR}$ are the same. So one just takes the first n rows of the basis matrix of the $(2,n+1) - VCS_{XOR}$ as the basis matrix of the $(2,n) - VCS_{XOR}$, the sufficiency of Theorem 6 follows.

According to property 1 of Lemma 3, we transform the basis matrix M into M' satisfying all the columns of M' have the same Hamming weight. Then according to Lemma 8, we have that the rows of M' have constant Hamming weight $\frac{(n-1)m}{2n}$ (or $\frac{(n+1)m}{2n}$), by adding an all 1 row if the Hamming weight of the rows of M' is $\frac{(n-1)m}{2n}$ (or adding an all 0 row if the Hamming weight of the rows of M' is $\frac{(n+1)m}{2n}$), one gets a $(2,n+1) - VCS_{XOR}$ with optimal contrast. □

Note that in the above discussions, it has been assumed that the Hadamard Matrix Conjecture holds. By making the same assumption, we further have:

Theorem 7 *The smallest possible pixel expansion m_c^* of $(2,n)-VCS_{XOR}$ given the optimal contrast $\alpha^*_{XOR} = \frac{2\lfloor n/2 \rfloor \lceil n/2 \rceil}{n(n-1)}$ is as follows:*

$$m_c^* = \begin{cases} 1 & if\ n = 2 \\ n & if\ n \equiv 3\ mod\ 4 \\ n-1 & if n \equiv 0\ mod\ 4 \\ 2n & if\ n \equiv 1\ mod\ 4 \\ 2n-2 & if\ n \equiv 2\ mod\ 4\ and\ n \neq 2 \end{cases}$$

Proof: The smallest pixel expansion for the case $n = 2$ can be shown as the basis matrix of the $(2,n)-VCS_{XOR}$: $M = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$, which has the pixel expansion $m_c^* = 1$ and optimal contrast $\alpha^*_{XOR} = 1$.

The smallest possible pixel expansion for the case $n \equiv 3\ mod\ 4$ and $n \equiv 0\ mod\ 4$ can be concluded from the Theorem 5, Corollary 1, Lemma 4, 6 and Theorem 6.

The smallest possible pixel expansion for the case $n \equiv 1\ mod\ 4$ and $n \equiv 2\ mod\ 4$ can be concluded from the Corollary 2, Lemma 6 and Theorem 6. □

Theorem 7 shows the smallest possible pixel expansion of the scheme given the optimal contrast, which are much smaller than the ones under the *OR* operation for the cases $n = 2$ and $n \equiv 0\ mod\ 4$. One can find a more clear comparison in Table 1.

	OR	XOR
$n = 2$	2	**1**
$n \equiv 3\ mod\ 4$	n	n
$n \equiv 0\ mod\ 4$	$2n-2$	**n-1**
$n \equiv 1\ mod\ 4$	$2n$	$2n$
$n \equiv 2\ mod\ 4$	$2n-2$	$2n-2$

Table 1: Comparison on the smallest pixel expansions of $(2,n)-VCS_{XOR}$ and $(2,n)-VCS_{OR}$ given optimal contrasts.

At this point, we summarize the constructions of optimal contrast $(2,n)-VCS_{XOR}$ with smallest pixel expansion as follows.

Construction 2 *For $n = 2$, let the basis matrix $M = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$, it is clear that its contrast is optimal and its pixel expansion is 1.*

We omit the constructions for the cases of $n \equiv 3\ mod\ 4$, $n \equiv 1\ mod\ 4$ and $n \equiv 2\ mod\ 4$ as they are the same as that in [4].

For the case $n \equiv 0\ mod\ 4$, we first apply Blundo's construction in [4] to generate the basis matrix, denoted by M', of the black secret pixels for the case $n-1 \equiv 3\ mod\ 4$. We have the pixel expansion of M' is $n-1$. Then we apply properties 1 of Lemma 3 to transform M' into M'' that satisfies all the columns of M'' has constant Hamming weight. We have each row of M'' has constant Hamming weight $(n-2)/2$ or $n/2$. By adding an all 1 row if the Hamming weight of M'' is $(n-2)/2$, or adding an all 0 row if the Hamming weight of M'' is $n/2$. Denote the resulting matrix as M, then M is the basis matrix of $(2,n)-VCS_{XOR}$ with optimal contrast and pixel expansion $n-1$ for the case $n \equiv 0\ mod\ 4$.

To make the Construction 2 more clear, we give an example for the case $n \equiv 0\ mod\ 4$.

Example 4 *Let $n = 4$. By applying Blundo's construction in [4] for $(2,3)-VCS_{OR}$, we get a basis matrix for the black secret pixel $M' = \begin{bmatrix} 100 \\ 010 \\ 001 \end{bmatrix}$, then by adding an all 1 row, we have $M = \begin{bmatrix} 111 \\ 100 \\ 010 \\ 001 \end{bmatrix}$, which is a basis matrix for $(2,4) - VCS_{XOR}$ with optimal contrast $2/3$ and pixel expansion 3.*

We also can transform $M' = \begin{bmatrix} 100 \\ 010 \\ 001 \end{bmatrix}$ into a matrix $\begin{bmatrix} 011 \\ 101 \\ 110 \end{bmatrix}$, and by adding an all 0 row, we have $M = \begin{bmatrix} 000 \\ 011 \\ 101 \\ 110 \end{bmatrix}$, which is also a basis matrix for $(2,4) - VCS_{XOR}$ with optimal contrast $2/3$ and pixel expansion 3.

5 Relationship with the constructions of optimal contrast $(2,n) - VCS_{XOR}$ and binary codes with maximum capacity

Tuyls et al. [31] present a simple equivalence relationship between the $(2,n) - VCS_{XOR}$ and the binary code. In this section, we further study the relationship between them, especially when the VCS has optimal contrast. And find that for odd n, the rows of the basis matrix of the optimal contrast $(2,n+1)-VCS_{XOR}$ is equivalent to the $(m, \frac{n+1}{2n}m)$ binary code which reaches its maximum capacity, and the rows of the basis matrix of the optimal contrast $(2,n)-VCS_{XOR}$ is equivalent to the $(m, \frac{(n+1)m}{2n}, \frac{(n\pm1)m}{2n})$ constant weight code which reaches its maximum capacity, hence we can use the known constructions of maximum capacity binary codes to construct the optimal contrast $(2,n) - VCS_{XOR}$. In addition, we give a construction of optimal contrast $(2,n) - VCS_{XOR}$ for $n = 2^k - 1$ is given, by using the technique of m-sequence.

Denote an $n \times m$ binary matrix M as the basis matrix of a $(2,n) - VCS_{XOR}$ with contrast α and the pixel expansion m. According to the first condition of Definition 1, the rows of M comprise an $(m, m\alpha)$ binary code, where m is the length of the codes and $m\alpha$ is the minimum Hamming distance. Hence by constructing an $(m, m\alpha)$ binary code with n codewords (if exists), we can construct a $(2,n) - VCS_{XOR}$ with contrast α and the pixel expansion m.

Denote $A(m,d)$ as the maximum number of codewords in any (linear or nonlinear) binary code of length m and minimum Hamming distance d. and $A(m,d,w)$ as the maximum number of codewords in any binary code of length m, constant weight w and minimum Hamming distance d. The two notations $A(m,d)$ and $A(m,d,w)$ are widely used in coding theory [1, 20, 26, 28, 34].

In order to make use of some results from coding theory, we hereby interpret some of the previous results in this paper with respect to $A(m,d)$ and $A(m,d,w)$.

First, we consider $(2,n)-VCS_{XOR}$ with smallest pixel expansion: The following two equations are from [26],

$$A(m,1) = 2^m \text{ and } A(m,2) = 2^{m-1}$$

And it is obvious that if $d_1 \leq d_2$, then $A(m,d_1) \geq A(m,d_2)$, simply because the codewords of (m,d_2) can be the codewords of (m,d_1). Therefore, alternative proofs of two of the theorems in section 3 (Theorems 1 and 2) can be as follows:

Proof of Theorem 1: For the binary code of length m, in order to form the basis matrix of a $(2,n) - VCS_{XOR}$, it should have at least n codewords, and the Hamming distance of any pair of the codewords should be at least 1 according to Definition 2, i.e. $A(m,1) \geq n$, which implies: $2^m \geq n$, i.e. $m \geq \log_2 n$. Since m is an integer, we have $m \geq \lceil \log_2 n \rceil$. Because all the m-length

binary codewords comprise a $(m, 1)$ binary code with 2^m ($\geq n$) codewords, hence the smallest pixel expansion of a $(2, n) - VCS_{XOR}$ is $\lceil \log_2 n \rceil$. □

Proof of Theorem 2: In order to prove that there does not exist such a $(2, n) - VCS_{XOR}$ that has smallest pixel expansion and the contrast is larger than $\alpha = \frac{1}{\lceil \log_2 n \rceil}$, we only need to show that there are not enough codewords to form the basis matrix with any two rows having Hamming distance larger than 1 and with the codeword length being $\lceil \log_2 n \rceil$, i.e. we need to show that $A(\lceil \log_2 n \rceil, 2) < n$. This holds true, because $A(\lceil \log_2 n \rceil, 2) = 2^{\lceil \log_2 n \rceil - 1} < 2^{1+\log_2 n - 1} = n$, and hence the theorem follows. □

Second, we discuss the $(2, n) - VCS_{XOR}$ with optimal contrast: We call that a (m, d) binary code reaches its *maximum capacity* if it has $A(m, d)$ codewords, and for binary constant weight code (m, d, w), it reaches its *maximum capacity* if it has $A(m, d, w)$ codewords. The construction of binary code with maximum capacity has been widely studied and one can find some of the constructions in [1, 20, 26, 28, 34]. The following lemmas will be needed in the proof of Theorems 8 and 9 as introduced below:

Lemma 9 *(Plotkin's Bound [20, 34]) Provided certain Hadamard matrices of order n' or less exist, then*

$A(n', 2\delta) = 2\lfloor \frac{2\delta}{4\delta - n'} \rfloor$ *if* $2\delta \leq n' < 4\delta$

$A(4\delta, 2\delta) = 8\delta$

$A(n', 2\delta) = 1$ *if* $n' < 2\delta$

Where here and hereafter $\lfloor x \rfloor$ denotes the largest integer no larger than x.

Lemma 10 *(Johnson's Bound [28])define d=2u, if $n'u > w(n' - w)$ then*

$A(n', d, w) \leq \lfloor \frac{n'u}{n'u - w(n' - w)} \rfloor$

The following Theorem 8 shows that, for an odd n, the rows of the basis matrices of the $(2, n+1) - VCS_{XOR}$ with optimal contrast form a special binary code with maximum capacity.

Theorem 8 *For an odd n, there exists a basis matrix for the $(2, n+1) - VCS_{XOR}$ with optimal contrast $\alpha = \frac{n+1}{2n}$ if and only if there exists a $(m, \alpha m)$ binary code which reaches its maximum capacity, where m is the pixel expansion of the $(2, n+1) - VCS_{XOR}$.*

Proof: First, for the necessity. Since the n rows of the basis matrices of the $(2, n+1) - VCS_{XOR}$ with optimal contrast α are a $(m, \alpha m)$ binary code, we only need to prove that it reaches its maximum capacity. Because $\alpha = \frac{n+1}{2n} < 1$ and $2\alpha = \frac{n+1}{n} > 1$, we have $\alpha m \leq m < 2\alpha m$, According to Theorem 7, we have that, αm is always even, hence:

$$A(m, \alpha m) = 2\lfloor \frac{\alpha m}{2\alpha m - m} \rfloor = 2\lfloor \frac{\frac{(n+1)m}{2n}}{\frac{(n+1)m}{n} - m} \rfloor = n + 1$$

Hence, the $n+1$ rows of the basis matrix of the $(2, n+1) - VCS_{XOR}$ with optimal contrast are a $(m, \alpha m)$ binary code which reaches its maximum capacity.

And the sufficiency is trivial, since $A(m, \frac{n+1}{2n}m) = n + 1$. □

At this point, to construct a $(2, n+1) - VCS_{XOR}$, we only need to construct a $(m, \alpha m)$ binary code which reaches its maximum capacity, and such construction with $m \leq 28$ can be found in [1].

According to Lemma 3, given the $n+1$ rows of the basis matrix of the $(2, n+1) - VCS_{XOR}$, and by adding the first row to all the $n+1$ rows, one gets that, the newly generated 2-nd,3-rd,$\cdots$,n-th,$(n+1)$-th rows are all have constant weight $\frac{(n+1)m}{2n}$ and the Hamming distance between them

is $\frac{(n+1)m}{2n}$, meanwhile, the complement of the 2-nd,3-rd,$\cdots$,n-th,$(n+1)$-th rows all have constant weight $\frac{(n-1)m}{2n}$ and the Hamming distance between them is $\frac{(n+1)m}{2n}$ too. We give the following theorem to show the relationship between the $(m, \frac{(n+1)m}{2n}, \frac{(n\pm1)m}{2n})$ constant weight code and the rows of the basis matrix of the optimal contrast $(2,n) - VCS_{XOR}$:

Theorem 9 *For odd n, there exist basis matrices for the $(2,n) - VCS_{XOR}$ with optimal contrast $\alpha = \frac{n+1}{2n}$ if and only if there exists a $(m, \frac{(n+1)m}{2n}, \frac{(n\pm1)m}{2n})$ binary constant weight code which reaches its maximum capacity, where m is the pixel expansion of the $(2,n) - VCS_{XOR}$.*

Proof: First, for the necessity. According to property 1 of Lemma 3, we transform the basis matrix, denoted as M, of the optimal contrast $(2,n)-VCS_{XOR}$ into M' satisfying all the columns of M' have the same Hamming weight. Then according to Lemma 8, we have that the rows of M' have constant Hamming weight $\frac{(n-1)m}{2n}$ (or $\frac{(n+1)m}{2n}$). Hence the rows of M' comprise a $(m, \frac{(n+1)m}{2n}, \frac{(n\pm1)m}{2n})$ binary constant weight code, and we only have to prove that it reaches its maximum capacity.

Let $n^{'} = m$, $u = \frac{(n+1)m}{4n}$,$w = \frac{(n\pm1)m}{2n}$, then $n^{'}u - w(n^{'} - w) = m\frac{(n+1)m}{4n} - \frac{(n\pm1)m}{2n}(m - \frac{(n\pm1)m}{2n}) = \frac{(n+1)m^2}{4n^2} > 0$, i.e. $n^{'}u > w(n^{'} - w)$, so according to Johnson's Bound, we have $A(n^{'}, d, w) \leq \frac{n^{'}u}{n^{'}u - w(n^{'}-w)}$, hence, $A(m, \frac{(n+1)m}{2n}, \frac{(n\pm1)m}{2n}) \leq \frac{m\frac{(n+1)m}{4n}}{m\frac{(n+1)m}{4n} - \frac{(n\pm1)m}{2n}(m - \frac{(n\pm1)m}{2n})} = n$, hence the theorem follows.

And the sufficiency is trivial, since $A(m, \frac{(n+1)m}{2n}, \frac{(n\pm1)m}{2n}) = n$. □

At this point, we get to know that, for an odd n, the construction of a $(2,n) - VCS_{XOR}$ with optimal contrast $\alpha = \frac{n+1}{2n}$ can be converted into the construction of an $(m, \frac{(n+1)m}{2n}, \frac{(n\pm1)m}{2n})$ binary constant weight code which reaches its maximum capacity, and the construction of such binary constant weight codes have been studied in [1, 10, 28].

Particularly, for $n = 2^k - 1$, where k is a positive integer, the construction of $(2,n) - VCS_{XOR}$ and $(2,n+1) - VCS_{XOR}$ can be realized via m-sequence (maximum length sequence), which is a kind of periodic bit sequences generated using linear feedback shift registers and has maximum length [11]. For any of such n, there exists an m-sequence which has period n and in each period, there are 2^{k-1} 1's. Any cyclic shift of such a sequence is also an m-sequence, and the *XOR* of an m-sequence and its shift is also an m-sequence (Theorem 15.3.11 in [39]). So let M be the matrix where all its rows are all the possible cyclic shifts of an m-sequence in one period. Then the rows of M form a binary constant weight code which is also linear. Moreover, M is an $n \times n$ matrix with each rows (as well as columns) having 2^{k-1} 1's. By adding the all-zero vector as a new row to the matrix M, it makes a new $(2,n+1) - VCS_{XOR}$ basis matrix. Hence we have the following theorem:

Theorem 10 *For $n = 2^k - 1$, there exists an m-sequence r which has period n, and the n m-sequences r_i, where $i = 0, 1, \cdots, n-1$ are generated by cyclic shift i bits of r, form a basis matrix of $(2,n) - VCS_{XOR}$, and this VCS has optimal contrast $\alpha = \frac{n+1}{2n}$, where k is a positive integer.*

Proof: Since any m-sequence has Hamming weight $w(r_i) = 2^{k-1}$, and the *XOR* of any two m-sequences is also an m-sequence, so the Hamming distance between any two m-sequences is 2^{k-1}. Because in such a VCS with the optimal contrast, the Hamming distance between any two rows is $\alpha \cdot n = \frac{n+1}{2} = 2^{k-1}$, hence the n m-sequences r_i $i = 0, 1, \cdots, n-1$ form a basis matrix of $(2,n) - VCS_{XOR}$ with optimal contrast. □

6 Conclusions

In this paper, we studied the optimal $(2,n)-VCS_{XOR}$, and have given some new results about the optimal pixel expansion of such schemes and the largest possible contrast for schemes given the optimal pixel expansion. We also studied the optimal contrast of the $(2,n)-VCS_{XOR}$, and the smallest possible pixel expansion of such schemes given the optimal contrast. The results of this paper show the properties of the $(2,n)-VCS_{XOR}$ have some advantages over the $(2,n)-VCS_{OR}$ in the sense of larger contrast and smaller pixel expansion.

It is noted that in the construction of the $(2,n)-VCS_{XOR}$ with the largest contrast and the smallest possible pixel expansion, the Hadamard Matrix Conjecture is assumed to hold. The same assumption was made in [4] as well.

We have shown that, the construction of the basis matrix of optimal contrast $(2,n)-VCS_{XOR}$ is equivalent to the construction of binary codes with specific parameters, which reaches its maximum capacity, hence we can use the known constructions of maximum capacity binary code (constant weight or not constant weight) to construct optimal contrast $(2,n)-VCS_{XOR}$, meanwhile we also give a construction of $(2,n)-VCS_{XOR}$ with optimal contrast for $n=2^k-1$, by using the technique of the m-sequence.

7 Acknowledgements

The paper was first submitted in 2006, and has been reviewed for several times. During the reviewing procedure, many anonymous reviewers' comments are very valuable. We thank a lot to these anonymous reviewers. This work was supported by China national 973 project No. 2007CB311202, NSFC grants No. 60903210 and China national 863 project No.2009AA01Z414.

References

[1] N.J.A.Sloane A.E.Brouwer, James B.Shearer and Warren D.Smith. A new table of constant weight codes. In *IEEE Transactions on Information Theory*, volume 36, No.6, pages 1334–1380, 1990.

[2] G. Ateniese, C. Blundo, A. De Santis, and D.R. Stinson. Visual cryptography for general access structures. In *Information and Computation*, volume 129, pages 86–106, 1996.

[3] E. Biham and A. Itzkovitz. Visual cryptography with polarization. In *the Dagstuhl seminar on Cryptography, September 1997, and in the RUMP session of CRYPTO'98*, 1997.

[4] C. Blundo, A. De Santis, and D.R. Stinson. On the contrast in visual cryptography schemes. In *Journal of Cryptology*, volume 12(4), pages 261–289, 1999.

[5] C.C. Chang and J.C. Chuang. An image intellectual property protection scheme for gray-level images using visual secret sharing strategy. In *Pattern Recognition Letters*, volume 23, pages 931–941, 2002.

[6] T.H. Chen and D.S. Tsai. Owner-customer right protection mechanism using a watermarking scheme and a watermarking protocol. In *Pattern Recognition*, volume 39, pages 1530–1541, 2006.

[7] S. Cimato, A. De Santis, A.L. Ferrara, and B. Masucci. Ideal contrast visual cryptography schemes with reversing. In *Information Processing Letters*, volume 93, pages 199–206, 2005.

[8] J. H. Dinitz and D. R. Stinson. *Ch. 1 in Contemporary Design Theory: A Collection of Surveys*. New York: Wiley, 1992.

[9] S. Droste. New results on visual cryptography. In *CRYPTO '96, Springer-Verlag LNCS*, volume 1109, pages 401–415, 1996.

[10] A.Vardy E.Agrell and K.Zeger. A table of upper bounds for binary codes. In *IEEE Transactions on Information Theory*, volume 47, no. 7, pages 3004–3006, 2001.

[11] S. Golomb. *Shift Register Sequences*. San Francisco, HoldenCDay, 1967.

[12] L.W. Hawkes, A. Yasinsac, and C. Cline. An application of visual cryptography to financial documents. In *Master thesis of Security and Assurance in Information Technology Laboratory, Computer Science Department, Florida State University*, 1997.

[13] C.S. Hsu and Y.C. Hou. Copyright protection scheme for digital images using visual cryptography and sampling methods. In *Optical Engineering*, volume 44(7), pages 077003.1–077003.10, 2005.

[14] H. Kuwakado, M. Morii, and H. Tanaka. Visual cryptographic protocols using the trusted initializer. In *7th International Conference on Information and Communications Security, ICICS 2005*, volume LNCS 3783, pages 112–122, 2005.

[15] H. Kuwakado and H. Tanaka. Size-reduced visual secret sharing scheme. In *IEICE Transactions on Fundamentals*, volume E87-A. No.5, pages 1193–1197, 2004.

[16] S.S. Lee, J.C. Na, S.W. Sohn, C. Park, D.H. Seo, and S.J. Kim. Visual cryptography based on an interferometric encryption technique. In *ETRI Journal*, volume 24,5, pages 373–380, 2002.

[17] F. Liu and C.K. Wu. A robust visual cryptography based watermarking scheme for multiple cover images and multiple owners. In *to appear in IET Information Security*, 2010.

[18] F. Liu, C.K. Wu, and X.J. Lin. Step construction of visual cryptography schemes. In *IEEE Transactions on Information Forensics & Security*, volume 5, No. 1, pages 27–38, 2010.

[19] D.C. Lou, H.K. Tso, and J.L. Liu. A copyright protection scheme for digital images using visual cryptography technique. In *Computer Standards & Interfaces*, volume 29, pages 125–131, 2007.

[20] M.Plotkin. Binary codes with specified minimum distances. In *IEEE Transactions on Information Theory*, volume IT-6, pages 445–450, 1960.

[21] M. Naor and B. Pinkas. Visual authentication and identification. In *Crypto '97, Springer-Verlag LNCS*, volume 1294, pages 322–336, 1997.

[22] M. Naor and A. Shamir. Visual cryptography. In *EUROCRYPT '94, Springer-Verlag Berlin*, volume LNCS 950, pages 1–12, 1995.

[23] PureDepth. Puredepth multi-layer display. In *Retrieved from http://www.puredepth.com*, 15 March 2006.

[24] Ito. R, Kuwakado. H, and Tanaka. H. Image size invariant visual cryptography. In *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Science*, volume E82-A.No.10, pages 2172–2177, 1999.

[25] P.S. Revenkar, A. Anjum, and W. Z. Gandhare. Secure iris authentication using visual cryptography. In *(IJCSIS) International Journal of Computer Science and Information Security*, volume 7, Number 3, pages 217–221, 2010.

[26] R.W.Hamming. Error detecting and error correcting codes. In *Bell System Technology Journal*, volume 29, pages 147–160, 1950.

[27] A. De Santis. On visual cryptography schemes. In *Proceedings of the Information Theory Workshop 1998, IEEE*, pages 154–155, 1998.

[28] S.Johnson. A new upper bound for error correction codes. In *IRE Transactions*, volume IT-8, pages 203–207, 1962.

[29] S. Sudharsanan. Shared key encryption of jpeg color images. In *IEEE Transactions on Consumer Electronics*, volume 51, No.4, pages 1204–1211, 2005.

[30] P. Tuyls, H.D.L. Hollmann, H.H.V. Lint, and L. Tolhuizen. A polarisation based visual crypto system and its secret sharing schemes. available at http://eprint.iacr.org, 2002.

[31] P. Tuyls, H.D.L. Hollmann, J.H.van Lint, and L. Tolhuizen. Xor-based visual cryptography schemes. In *Designs Codes and Cryptography*, volume 37, pages 169–186, 2005.

[32] P. Tuyls, T. Kevenaar, G.J. Schrijen, T. Staring, and M.V. Dijk. Security displays enabling secure communications. In *First International Conference on Pervasive Computing, Boppard Germany, Berlin Springer LNCS*, volume 2802, pages 271–284, 2004.

[33] D.Q. Viet and K. Kurosawa. Almost ideal contrast visual cryptography with reversing. In *Topics in Cryptology - CT-RSA*, pages 353–365, 2004.

[34] V.I.Levenshtein. The application of hadamard matrixes to a problem in coding. In *Problems of Cybernetics*, volume 5, pages 166–184, 1964.

[35] F.H. Wang, K.K. Yen, L.C.Jain, and J.S. Pan. Multiuser-based shadow watermark extraction system. In *Information Sciences*, volume 177, pages 2522–2532, 2007.

[36] Patent with International Application No.: PCT/IB2003/000261. *Secure Visual Message Communication Method And Device*. 2003.

[37] C.N. Yang. New visual secret sharing schemes using probabilistic method. In *Pattern Recognition Letters*, volume 25, pages 481–494, 2004.

[38] C.N. Yang, T.S. Chen, and M.H. Ching. Embed additional private information into two-dimensional bar codes by the visual secret sharing scheme. In *Integrated Computer-Aided Engineering*, volume 13, Number 2, pages 189–199, 2006.

[39] Y.X.Yang and X.D.Lin. *Coding and Cryptography (in Chinese)*. Posts and Telecom Press, 1992.