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

Feng Liu and Chuankun Wu

SKLOIS, IIE, CAS

2014-10-02

Contents

- Introduction
- Preliminaries
- $(2,n)-VCS_{XOR}$ with optimal pixel expansion
- $(2,n)-VCS_{XOR}$ with largest contrast given optimal pixel expansion
- $(2,n)-VCS_{XOR}$ with optimal contrast
- $(2,n)-VCS_{XOR}$ with smallest pixel expansion given optimal contrast
- Equivalence between $(2,n)-VCS_{XOR}$ and binary code

Introduction

- Why XOR?
  - Semi-group VS. GF(2)
  - Better visual quality and smaller pixel expansion
- How to realize XOR based VCS?
  - Mach-Zehnder Interferometer [Lee2002]
  - Polarization property of liquid crystal displays [Tuyls2002,PCT2003]
  - Copy machine with the reversing function [Viet2004]
- Why $(2,n)-VCS_{XOR}$?
  - For(k,n)–VCS_{XOR} ,many Mach-Zehnder Interferometers or liquid crystal displays or reversing copies make the decoding system complicated.

Contents

- Introduction
- Preliminaries
- $(2,n)-VCS_{XOR}$ with optimal pixel expansion
- $(2,n)-VCS_{XOR}$ with largest contrast given optimal pixel expansion
- $(2,n)-VCS_{XOR}$ with optimal contrast
- $(2,n)-VCS_{XOR}$ with smallest pixel expansion given optimal contrast
- Equivalence between $(2,n)-VCS_{XOR}$ and binary code

Formal definition of $(k, n) - VCS$

- **Definition 1.** Let k, n, m, l and h be non-negative integers satisfying $2 \leq k \leq n$ and $0 \leq l < h \leq m$. The two sets of $n \times m$ Boolean share matrices (C_0, C_1) constitute a (k, n)-VCS if the following properties are satisfied:
- 1. (Contrast) For any $s \in C_0$, the "●" operation of any k out of the n rows of s, is a vector v that, satisfies $w(v) \leq l$.
- 2. (Contrast) For any $s \in C_1$, the "●" operation of any k out of the n rows of s, is a vector v that, satisfies $w(v) \geq h$.
- 3. (Security) For any $i_1 < i_2 < \ldots < i_t$ in {1, 2,…, n} with $t < k$, the two collections of $t \times m$ matrices D_0 and D_1 obtained by restricting each $n \times m$ matrix in $C_0$and $C_1$to rows $i_1, i_2, \ldots, i_t$, are indistinguishable in the sense that they contain the same matrices with the same frequencies.

Basis matrix of $(2, n) - VCS_{XOR}$

- **Definition 2.** 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 out of n rows in M satisfies: $w(j_{i_1} \oplus j_{i_2}) \geq h$, where j_i $(i = 1, \dots, n)$ is a row of M and $h \geq 1$.
- **Boolean share matrices (C_0, C_1)**

  $C_0 = \{A(j_1), \dots, A(j_n)\}$. $j_1, \dots, j_n$ are the n rows of M

  $C_1 = \{M(0), M(1), M(2), \dots, M(n-1)\}$

  - A(r) is the $n \times m$ matrix for which each row equals to r
  - M(i) is the $n \times m$ matrix obtained by cyclicaly shift the rows of M over i positions.

$(2,3) - \boldsymbol{VCS_{XOR}}$

$$M = \begin{Bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{Bmatrix}$$

$\boldsymbol{C_0}$

$$\begin{Bmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{Bmatrix}$$

$$\begin{Bmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \end{Bmatrix}$$

$$\begin{Bmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{Bmatrix}$$

$\boldsymbol{C_1}$

$$\begin{Bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{Bmatrix}$$

$$\begin{Bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{Bmatrix}$$

$$\begin{Bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{Bmatrix}$$

Average contrast for $(2, n) - VCS_{XOR}$

- **The contrast is** $\alpha = \frac{h-l}{m} = \frac{h-0}{m} = \frac{h}{m}$,
- **Average contrast is** $\bar{\alpha} = \frac{\bar{h}-\bar{l}}{m}$,

$\bar{h}$(resp. $\bar{l}$) is the average value of darkness level in collection C_1(resp. C_0)

- $\bar{h} = \frac{\sum_{M \in C_1} \bar{h}_M}{|C_1|}, \bar{h}_M = \frac{\sum_{1 \le i < j \le n} w(r_i \oplus r_j)}{\binom{n}{2}}$

$\bar{l} = \frac{\sum_{M \in C_0} \bar{l}_M}{|C_0|}$, $\bar{l}_M = \frac{\sum_{1 \le i < j \le n} w(r_i \oplus r_j)}{\binom{n}{2}}$

$\bar{h}_M$(resp. $\bar{l}_M$) is the average value of darkness level of M

Contents

- Introduction
- Preliminaries
- $(2,n)-VCS_{XOR}$ with optimal pixel expansion
- $(2,n)-VCS_{XOR}$ with largest contrast given optimal pixel expansion
- $(2,n)-VCS_{XOR}$ with optimal contrast
- $(2,n)-VCS_{XOR}$ with smallest pixel expansion given optimal contrast
- Equivalence between $(2,n)-VCS_{XOR}$ and binary code

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

Proof: Assume that there exists a the $(2, n) - VCS_{XOR}$ 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 $m \geq \lceil \log_2 n \rceil$.

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

- **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 $\overline{\alpha}_{XOR} = \frac{2\lfloor n/2 \rfloor \lceil n/2 \rceil}{n(n-1)}$, 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* $\lceil n/2 \rceil$

Construction: $n = 5, m^* = 3, \alpha = \frac{1}{3}, \overline{\alpha}_{XOR} = \frac{3}{5}$

- $M' = \begin{bmatrix} 0\,0\,0 \\ 0\,0\,1 \\ 0\,1\,0 \\ 1\,0\,0 \\ 0\,1\,1 \\ 1\,0\,1 \\ 1\,1\,0 \\ 1\,1\,1 \end{bmatrix}$

Remove one complementary row vector pairs randomly

$\{0\,0\,1\}$
$\{1\,1\,0\}$

$M'' = \begin{bmatrix} 000 \\ 010 \\ 100 \\ 011 \\ 101 \\ 111 \end{bmatrix}$

Remove one row randomly

$\{0\,1\,1\}$

$M = \begin{bmatrix} 000 \\ 010 \\ 100 \\ 101 \\ 111 \end{bmatrix}$

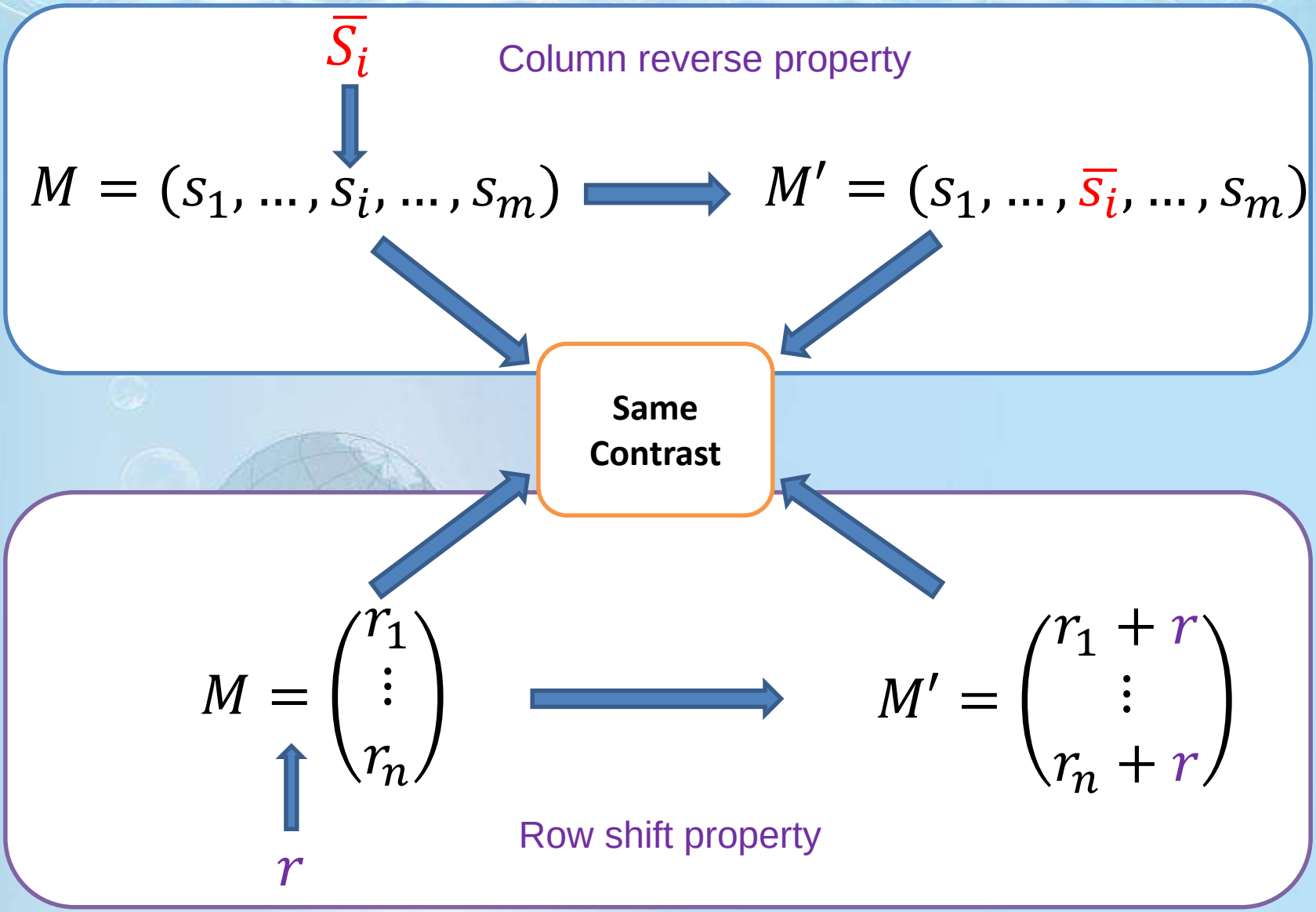
Contents

- Introduction
- Preliminaries
- $(2,n)-VCS_{XOR}$ with optimal pixel expansion
- $(2,n)-VCS_{XOR}$ with largest contrast given optimal pixel expansion
- $(2,n)-VCS_{XOR}$ with optimal contrast
- $(2,n)-VCS_{XOR}$ with smallest pixel expansion given optimal contrast
- Equivalence between $(2,n)-VCS_{XOR}$ and binary code

Optimal contrast of $(2, n) - VCS_{XOR}$

- **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 $\oplus$ 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: Consider when the unavoidable patterns $\binom{0}{1}$ and $\binom{1}{0}$ reach its maximum
- **Theorem 5.** The basis matrix of an optimal contrast $(2, n) - VCS_{OR}$ for the black secret pixel is also the basis matrix of an 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: The proof follows directly from property 2 of Lemma 4.3 in [Blundo1999], which pointed out that each unavoidable pattern $\binom{0}{1}$ and $\binom{1}{0}$ appears $\frac{\lfloor n/2 \rfloor \lceil n/2 \rceil}{n(n-1)} \cdot m$ times for optimal OR based VCS.
  - [Blundo1999] also proved that $\alpha_{OR} \leq \frac{\lfloor n/2 \rfloor \lceil n/2 \rceil}{n(n-1)}$,

Structural properties of $(2, n) - VCS_{XOR}$



Bounds for the pixel expansion when n is odd (given optimal contrast)

- **Lemma 1.** For an odd n (≥ 3), if there exists a $(2, n) - VCS_{XOR}$ with the optimal contrast α^*_{XOR} and denote its pixel expansion as m, then we have $n|m$.
- **Lemma 2.** For a $(2, n) - VCS_{XOR}$ with $n \equiv 1\ mod\ 4$ and optimal contrast $\alpha^*_{XOR} = \frac{2\lfloor n/2 \rfloor \lceil n/2 \rceil}{n(n-1)} = \frac{n+1}{2n}$, the pixel expansion of such scheme satisfies $m \neq n$.
- **Corollary 1.** For $n \equiv 1\ mod\ 4$, the smallest pixel expansion m_c^* of a $(2, n) - VCS_{XOR}$ given optimal contrast is $2n$.

Deduce from odd n to even (The most important lemma of this paper)

- **Lemma 3.** 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

   $\frac{n-1}{2}$ $(or\ resp. \frac{n+1}{2})$

then all the rows of M will also have the same hamming weight

$\frac{(n-1)m}{2n}$ $(or\ resp. \frac{(n+1)m}{2n})$

Proof :

For an equidistant binary code (rows of M) with parameters: code length m, cardinality n (odd number), distance d, and each column has k 1's. If a row of M has the hamming weight w, we note that its sum of distances with the remaining n-1 rows, will equal to the number of unavoidable patterns in M:

$$d(n-1) = w(n-k) + (m-w)k \qquad (1)$$

Hence:

$$d(n-1) - mk = (n-2k)w \qquad (2)$$

Consider a general binary code with the minimum Hamming distance d, then the equation (1) will be changed as follows:

$$d(n-1) \leq w(n-k) + (m-w)k \qquad (3)$$

Since $d = \frac{(n+1)m}{2n}$ and $k = \frac{n-1}{2}$, substitute them in (3), we have:

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

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: (by adding all rows)

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

meanwhile, by adding all columns:

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

combine (4), (5), and (6),we have

$$w = \frac{(n-1)m}{2n}$$

$(2,n)-VCS_{XOR}$ and $(2,n+1)-VCS_{XOR}$

- **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:***
- Note that: $\frac{2\lfloor n/2\rfloor\lceil n/2\rceil}{n(n-1)}=\frac{n+1}{2n}=\frac{2\lfloor (n+1)/2\rfloor\lceil (n+1)/2\rceil}{n(n+1)}$, the sufficiency is easy.
- Necessity: transform M into M' with constant weight of columns using column reverse property. And according Lemma 3, the rows will have constant weight of $\frac{(n-1)m}{2n}$ $(or\ resp.\ \frac{(n+1)m}{2n})$, by adding an all 1 row (resp. 0), we generate a $(2,n+1)-VCS_{XOR}$ with optimal contrast $\frac{n+1}{2n}$.

Constructions for even number rows

- For $n = 2$. $M = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$
- When n is even, take $n = 4$ as an example.

Basis Matrix for $(2,3)$ – $VCSXOR$

$$M' = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{bmatrix}$$

Adjust columns

$$M'' = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Add all 1 row

$$M = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Adjust columns

$$M'' = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}$$

Add all 0 row

$$M = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}$$

Basis Matrix for $(2,4)$ –

Constructions for the smallest pixel expansion $(2,n)-VCS_{XOR}$ given optimal contrast

1. **(Theorem 4.7 of [Blundo1999])** Assuming that $n \equiv 3\ mod\ 4$ 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 $\left(n, \frac{n-1}{2}, \frac{n-3}{4}\right) - BIBD$ (or equivalently, a Hadamard matrix of order n+1).

2. **(Theorem 4.8 of [Blundo1999])** Assuming that $n \equiv 1\ mod\ 4$ 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 $\left(n, \frac{n-1}{2}, \frac{n-3}{2}\right) - BIBD$ or an $\left(n+1, \frac{n+1}{2}, \frac{n-1}{2}\right) - BIBD$.

The smallest possible pixel expansion of $(2, n) - VCS_{XOR}$ given the optimal contrast

Theorem 7:

	OR	XOR
$n = 2$	**2**	**1**
$n \equiv 3 \, mod \, 4$	n	n
$n \equiv 0 \, mod \, 4$	$\boldsymbol{2n-2}$	$\boldsymbol{n-1}$
$n \equiv 1 \, mod \, 4$	$2n$	$2n$
$n \equiv 2 \, mod \, 4$	$2n-2$	$2n-2$

Contents

- Introduction
- Preliminaries
- $(2,n)-VCS_{XOR}$ with optimal pixel expansion
- $(2,n)-VCS_{XOR}$ with largest contrast given optimal pixel expansion
- $(2,n)-VCS_{XOR}$ with optimal contrast
- $(2,n)-VCS_{XOR}$ with smallest pixel expansion given optimal contrast
- Equivalence between $(2,n)-VCS_{XOR}$ and binary code

$(2,n)-VCS_{XOR}$ and binary code

	Odd n		
Optimal contrast $\alpha^*_{XOR}=\frac{n+1}{2n}$	$(2,n+1)-VCS_{XOR}$	$(\mathrm{m},\alpha^*_{XOR}\mathrm{m})$ binary code	Equivalent
	$(2,n)-VCS_{XOR}$	$(\mathrm{m},\frac{(n+1)m}{2n},\frac{(n\pm1)m}{2n})$ binary constant weight code	
	$(2,n)-VCS_{XOR}$	$n=2^k-1$ n period m-sequence	

Thank you very much!

Full version available at:
http://www.fengliu.net.cn
http://eprint.org