Almost Ideal Contrast Visual Cryptography with Reversing *

Duong Quang Viet[1] and Kaoru Kurosawa[2]

Department of Information and Networks Systems,
[1]National Institute of Information and Communications Technology,
4–2–1 Nukui-Kitamachi, Koganei, Tokyo 184-8795, Japan
viet@nict.go.jp

[2] Department of Computer and Information Sciences,
Ibaraki University
4–12–1 Nakanarusawa, Hitachi, Ibaraki 316-8511, Japan
kurosawa@cis.ibaraki.ac.jp

Abstract

A drawback of visual cryptography schemes (VCS) is much loss of contrast in the reconstructed image. This paper shows a new paradigm of VCS in which the original image is almost perfectly reconstructed. A very simple non-cryptographic operation is assumed, reversing black and white, which many copy machines have these days. We first show a (k, n)-VCS with *reversing* such that white pixels are almost perfectly reconstructed in addition to the perfect reconstruction of black pixels. The proposed scheme is fully compatible with traditional VCS in the following sense: Even if we do not have a copy machine as described above, we can reconstruct the secret image I exactly in the same way as in the underlying VCS. In other words, we use a copy machine as a hedge to obtain better contrast.

We next show how to convert a perfect *black* (k, n)-VCS (with reversing) into a perfect *white* (k, n)-VCS with reversing. Thirdly, we show a perfect black VCS for any monotone access structure. Finally, we show applications of our idea to colored VCS and grey level VCS, respectively.

Keywords: Visual cryptography, reversing, ideal contrast, perfect black

*A preliminary version of this paper was presented at CT-RSA 2004 and appeared in *Lecture Notes in Computer Science* **2964**, pp. 353–365, Springer-Verlag, 2004.

Contents

1 Introduction

1.1 Background

The notion of visual cryptography schemes (VCS) was introduced by Naor and Shamir [10]. Since then, it has been studied by many researchers, to name a few [1, 3, 4, 5, 8, 12]. A VCS is a special kind of secret sharing scheme in which the secret is an image I, comprised of black and white pixels. The difference is in how the secret is reconstructed. While a traditional secret sharing scheme needs to use a computer or cryptographic operations, a VCS uses only the human visual system. That is, in the reconstruction phase of a VCS, the secret image is reconstructed visually by superimposing a subset of transparencies.

More precisely, a (k, n)-threshold VCS (or (k, n)-VCS for short) is a method to encode a secret image I into n transparencies, where each participant receives one transparency. In the reconstruction phase, any k participants can recover the secret image by superimposing their transparencies. However, any $k - 1$ participants have no information on I.

However, a drawback of VCSs is a much loss of contrast in the reconstructed image. In particular, no white pixel can be reconstructed perfectly. For example, in a $(2, 2)$-VCS of [10], a white pixel is translated into a grey region (half black and half white) while a black pixel is translated into a black region. That is, the contrast degrades to $1/2$. (Naor and Shamir showed an improved VCS later in [11]. However, it works only for $(2, 2)$-VCS.)

On the other hand, it is known that the reconstruction of black pixel can be perfect for any $2 \leq k \leq n$, which was shown by Blundo et al. [7, 3].

Some variants of VCS also exist. Colored VCS was proposed by Verheul and van Tilborg [12]. They gave a general construction of colored (k, n)-VCS, and it was improved by Blundo et al. [7]. A VCS for grey level images was shown by Blundo et al. in which each pixel has g grey levels ranging from 0 (white) to $g - 1$ (black) [6]. The contrast of the reconstructed image of these schemes is very poor, too.

1.2 Our contribution

In traditional VCS, no black subpixel can be made into white because transparencies are simply superimposed in the reconstruction phase. This is the essential reason of a much loss of contrast in the reconstructed image.

This paper shows a new paradigm of VCS in which the original image is almost perfectly reconstructed. A very simple non-cryptographic operation is assumed, reversing black and white, which many copy machines have these days. All the black region is reversed into white and all the white region is reversed into black by this operation. We call our scheme a (k, n)-VCS with *reversing*.

1. We first show a perfect black (k, n)-VCS with *reversing* such that white pixels are almost perfectly reconstructed in addition to the perfect

reconstruction of black pixels. The cost we have to pay is the size of shares. If the size of shares is c times larger, then the grey level of white region converges to zero exponentially.

The proposed scheme is fully compatible with traditional VCS in the following sense: Even if we do not have a copy machine as described above, we can reconstruct the secret image I exactly in the same way as in the underlying VCS. In other words, we use a copy machine as a hedge to obtain better contrast. Therefore, our scheme is very attractive.

2. We next show how to convert a perfect *black* (k, n)-VCS (with reversing) into a perfect *white* (k, n)-VCS with reversing. Perfect *white* VCSs are much more preferable than perfect *black* VCSs because the white region is much larger than the black region in usual images.

From our first result, we can obtain a perfect *white* (k, n)-VCS with reversing such that the reconstruction of black region is almost perfect in addition to the perfect reconstruction of white pixels.

3. Thirdly, we show a perfect black VCS for any monotone access structure. (Perfect black VCSs have been known only for (k, n)-threshold cases so far although VCS itself can be constructed for general access structures [1].)

This means that we can obtain a VCS with *reversing* for any monotone access structure such that the contrast is almost ideal.

Finally, we show applications of our idea to colored VCS and grey level VCS, respectively.

4. We show a scheme such that the original colored image I is almost perfectly reconstructed. It is assumed that there is a copy machine which has three functions, coloring a black pixel into red, blue and yellow, respectively.

5. We show a scheme such that the original grey level image I is almost perfectly reconstructed. It is assumed that there is a copy machine which can make a black pixel into grey level i for $1 \leq i \leq g - 1$.

2 Preliminaries

For a random variable X, $E[X]$ denotes the expected value and $\mathrm{Var}[X]$ denotes the variance. We sometimes use $+$ to express OR.

2.1 Naor-Shamir $(2,2)$-VCS

Naor and Shamir showed the first (k,n)-VCS [10]. Fig 1 illustrates their construction of $(2,2)$-VCS.

In the distribution phase, each pixel P is split into two sub-pixels in each of the two shares s_1 and s_2. If P is white, then the dealer $\mathcal{D}$ randomly chooses one of the first two rows of Fig 1. If P is black, then $\mathcal{D}$ randomly chooses one of the last two rows of Fig 1. $\mathcal{D}$ then gives s_1 to participant $\mathcal{P}_1$ and s_2 to participant $\mathcal{P}_2$.

In the reconstruction phase, the two participants superimpose s_1 and s_2. If P is black, then they get two black sub-pixels; if P is white, then they get one black sub-pixel and one white sub-pixel.

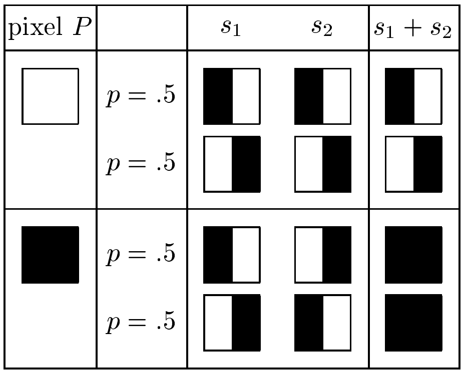

Figure 1: Naor-Shamir 2-out-of-2 visual cryptography scheme

This scheme can be expressed by a pair of basis matrices

$$M_0 = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}, \text{ and } M_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \tag{1}$$

The dealer $\mathcal{D}$ computes the encoding matrix C of a pixel P by randomly permuting the columns of M_0 if P is white and by randomly permuting the columns of M_1 if P is black. The first row is used to compute s_1 and the second row is used to compute s_2, where 0 means white and 1 means black.

2.2 Model

A (k,n)-visual cryptography scheme (VCS) consists of a distribution phase and a reconstruction phase. Let I be a secret image which consists of black and white pixels P.

In the distribution phase, a dealer $\mathcal{D}$ encodes each pixel P into n shares $s_1, \cdots, s_n$, one for each transparency. $\mathcal{D}$ then gives s_i to participant $\mathcal{P}_i$ for $i = 1, \cdots, n$.

In the reconstruction phase, any k participants $\mathcal{P}_{i_1}, \cdots, \mathcal{P}_{i_k}$ *reconstruct* I by superimposing their transparencies. That is, the reconstructed pixel is given by

$$\tilde{P} = s_{i_1} + s_{i_2} + \cdots + s_{i_k},$$

where $+$ means OR. However, any $k-1$ participants have no information on I.

Each s_i consists of m sub-pixels, where m is called the *expansion rate*. Hence s_i is described by a Boolean vector of length m

$$v_i = (c_{i,1}, \cdots, c_{i,m}),$$

where $c_{i,j} = 1$ if the j-th sub-pixel in s_i is black. Let $C = [c_{i,j}]$ be the $n \times m$ Boolean matrix which consists of $v_1, \cdots, v_n$. We say that C is the *encoding matrix* of P.

Usually, the dealer $\mathcal{D}$ computes the encoding matrix C of a pixel P from two matrices M_0 and M_1 as follows: C is obtained by randomly permuting the columns of M_0 if P is white and by randomly permuting the columns of M_1 if P is black. M_0 and M_1 are called the *basis matrices.*

$\tilde{P}$ is interpreted as black if $w_H(\tilde{P})$ is large, and as white if $w_H(\tilde{P})$ is small, where $w_H(\tilde{P})$ denotes the Hamming weight of $\tilde{P}$. We define the grey level of a pixel P as

$$\mathsf{GREY}(P) = w_H(\tilde{P})/m,$$

where P = white or black. $\mathsf{GREY}(white)$ should be close to zero and $\mathsf{GREY}(black)$ should be close to one. In Naor-Shanir $(2,2)$-VCS, the grey levels of a black pixel and a white pixel are

$$\mathsf{GREY}(black) = 1, \quad \mathsf{GREY}(white) = 1/2.$$

The *contrast* is ideal if

$$\mathsf{GREY}(white) = 0 \text{ and } \mathsf{GREY}(black) = 1.$$

2.3 Perfect Black VCS

We say that a (k,n)-VCS is *perfect black* if

$$\mathsf{GREY}(black) = 1 \text{ and } \mathsf{GREY}(white) < 1.$$

The (n,n)-VCS shown by Naor and Shamir [10] is perfect black. The expansion rate is $m = 2^{n-1}$ and they showed that it is optimum.

For any $2 \le k \le n$, Blundo et al. showed a perfect black (k,n)-VCS such that

$$\mathsf{GREY}(white) = 1 - 1/m$$

for some expansion rate m [7].

3 Basic Idea

In this section, we show a basic idea of our schemes. We present a $(2,2)$-VCS with reversing such that $\mathsf{GREY}(white) = 1/4$ in addition to $\mathsf{GREY}(black) = 1$. Since $\mathsf{GREY}(white) = 1/2$ in the Naor-Shamir $(2,2)$-VCS, the contrast is improved in our scheme.

Definition 1 *We say that an image I is reversed if all black pixels are reversed into white and all white pixels are reversed into black. We denote by $\overline{P}$ the reversed pixel of P and by $\overline{I}$ the reversed image of I.*

Our scheme is described as follows. (See Fig 2 and Fig 3.)

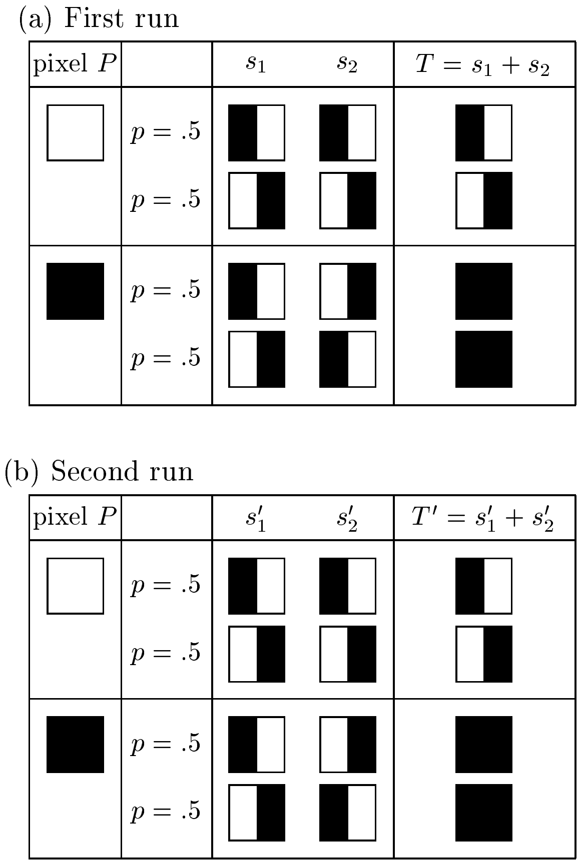

Figure 2: Proposed $(2,2)$-VCS (1)

(Distribution phase)

1. The dealer $\mathcal{D}$ runs the distribution phase of Naor-Shamir $(2,2)$-VCS twice independently. Let (s_1, s_2) denote the shares of the first run and (s_1', s_2') denote the shares of the second run.

2. Now in our scheme, the share of participant $\mathcal{P}_1$ is (s_1, s'_1), and that of participant $\mathcal{P}_2$ is (s_2, s'_2).

(Reconstruction phase)

Step 1. Two participants superimpose s_1, s_2 and obtain $T = s_1 + s_2$. Similarly, they superimpose s'_1, s'_2 and obtain $T' = s'_1 + s'_2$. They are illustrated in the last columns of Fig 2(a) and Fig 2(b).

Step 2. They next reverse T, T' and obtain $\overline{T}$ and $\overline{T'}$ as shown in Fig 3.

Step 3. The two participants superimpose $\overline{T}$, $\overline{T'}$ and obtain $\overline{T} + \overline{T'}$.

Step 4. Finally the two participants reverse $\overline{T} + \overline{T'}$ and obtain $\overline{\overline{T} + \overline{T'}}$.

The $\overline{\overline{T} + \overline{T'}}$ is the reconstructed image of our scheme.

Now as we can see from Fig 3, we obtain that $\mathsf{GREY}(black) = 1$ and

$$E[\mathsf{GREY}(white)] = (1/2) \times 0 + (1/2) \times (1/2) = 1/4.$$

We will show the reason below. Suppose that a pixel P is white. Then

1. T and T' are always black as whown in Fig 2.
2. Therefore, $\overline{T}$ and $\overline{T'}$ are always white as shown in Fig 3.
3. Therefore, $\overline{T} + \overline{T'}$ is always white.
4. Hence $\overline{\overline{T} + \overline{T'}}$ is always black.

On the other hand, suppose that a pixel P is white. Then

1. As whown in Fig 2, T and T' are grey such that a half region is black and the other half is white in each one of the four cases.
2. Therefore, $\overline{T}$ and $\overline{T'}$ are grey such that a half region is white and the other half is black in each one of the four cases as shown in Fig 3.
3. Therefore, $\overline{T}+\overline{T'}$ is black with probability 1/2 and grey (half black and half white) with probability 1/2. This is because (s_1, s_2) and (s'_1, s'_2) are generated independently and randomly.
4. Hence $\overline{\overline{T} + \overline{T'}}$ is all white with probability 1/2 and it is grey (half black and half white) with probability 1/2.

4 Proposed Scheme

In this section, we show our (k, n)-VCS with *reversing*. The reconstruction of black region is perfect and the reconstruction of white region is almost perfect. The cost we have to pay is the size of shares. If the size of shares is c times larger, then the grey level of white region converges to zero exponentially.

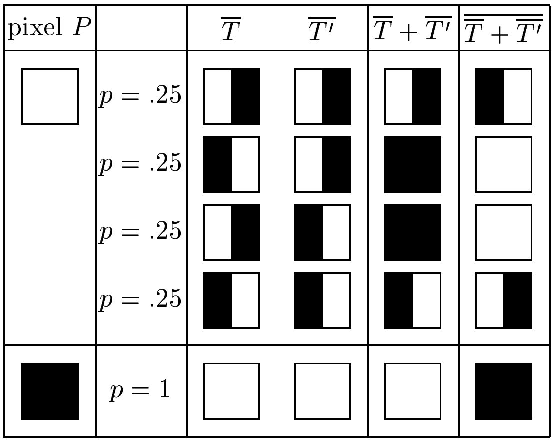

Figure 3: Proposed $(2,2)$-VCS (2)

4.1 c-Run (k,n)-VCS with Reversing

Suppose that there exists a perfect black (k,n)-VCS. (Remember that there exists a perfect black (k,n)-VCS for any $2 \le k \le n$.) We then construct a "c-run (k,n)-VCS with *reversing*" as follows in which the underlying (k,n)-VCS is run c times independently.

Let P a secret pixel to be distributed.

(Distribution phase)

1. The dealer $\mathcal{D}$ runs the distribution phase of the underlying perfect black (k,n)-VCS c times independently. Let $(s_{1,i},\cdots,s_{n,i})$ be the set of shares in the i-th run for $i=1,\cdots,c$.

2. In our scheme, the share of participant $\mathcal{P}_j$ is $(s_{j,1},\cdots,s_{j,c})$.

(Reconstruction phase) Any k participants, say $\mathcal{P}_{j_1},\cdots,\mathcal{P}_{j_k}$, reconstruct P as follow.

1. For $i=1,\cdots,c$, they superimpose their shares and obtain

$$T_i = s_{j_1,i}+\cdots+s_{j_k,i}$$

2. They reverse T_i and obtain $\overline{T}_i$ for $i=1,\cdots,c$.

3. They superimpose $\overline{T}_1,\cdots,\overline{T}_c$ and obtain $U=\overline{T}_1+\cdots+\overline{T}_c$.

4. We reverse U and obtain $\tilde{P}$, where

$$\tilde{P}=\overline{U}=\overline{\overline{T}_1+\cdots+\overline{T}_c}.$$

(See Fig.4.)

It is clear that any $k-1$ participants have no information on P from the property of the original (k,n)-VCS.

$$\begin{array}{lcl} & & n \text{ transparencies} \\ & \nearrow & \\ \text{secret pixel } P & \vdots & \\ & \searrow & \\ & & n \text{ transparencies} \end{array}$$

(Distribution phase)

$$\begin{array}{lcl} \text{stack } k \text{ sheets } T_1 \to \text{reverse } \overline{T}_1 & & \\ & \searrow & \\ & & U = \overline{T}_1 + \cdots + \overline{T}_c \to \text{reverse } \overline{U} \\ & \nearrow & \\ \text{stack } k \text{ sheets } T_c \to \text{reverse } \overline{T}_c & & \end{array}$$

(Reconstruction phase)

Figure 4: Proposed VCS

4.2 Contrast

It is easy to see that $\mathsf{GREY}(black) = 1$ because the original VCS is perfect black. We now show that both $E[\mathsf{GREY}(white)]$ and $\mathrm{Var}[\mathsf{GREY}(white)]$ converge to zero.

Theorem 1 *Suppose that* $\mathsf{GREY}(white) = q < 1$ *in the original perfect black VCS. Then in our c-run VCS with reversing,*

(1) $E[\mathsf{GREY}(white)] = q^c$.

(2) $\mathrm{Var}[\mathsf{GREY}(white)] \leq q^c(1 - q^c)$.

Proof. (1) Let P be a white pixel. Each T_i is described by a Boolean vector of length m

$$A_i = (a_{i,1}, \cdots, a_{i,m}),$$

where m is the expansion rate. Similarly, the reconstructed pixel $\tilde{P}$ is described by a Boolean vector

$$W = (w_1, \cdots, w_m).$$

Now since

$$w_j = \overline{\overline{a}_{1,j} + \cdots + \overline{a}_{c,j}},$$

it holds that

$$w_j = a_{1,j} \times \cdots \times a_{c,j}$$

from De Morgan's law. Therefore,

$$\begin{aligned}
E[w_H(W)] &= E[\sum_j w_j] = \sum_j E(w_j) = \sum_j E[a_{1,j} \times \cdots \times a_{c,j}] \\
&= \sum_j \Pr(a_{1,j} = \cdots = a_{c,j} = 1) \\
&= \sum_j \Pr(a_{1,j} = 1) \times \cdots \times \Pr(a_{c,j} = 1) \\
&= \sum_j q^c \\
&= mq^c.
\end{aligned}$$

Consequently, $E[\mathsf{GREY}(white)] = E[w_H(W)]/m = q^c$.

(2) It is easy to see that $(w_1 + \cdots + w_m) \leq m$ because $w_j = 0$ or $w_j = 1$. Therefore,

$$(w_1 + \cdots + w_m)^2 \leq m(w_1 + \cdots + w_m) = m \sum_{j=1}^{m} w_j$$

Hence

$$\begin{aligned}
\mathrm{Var}[w_H(W)] &= E[w_H(W)^2] - E[w_H(W)]^2 = E[(\sum_j w_j)^2] - m^2 q^{2c} \\
&\leq mE[\sum_j w_j] - m^2 q^{2c} \\
&= mE[w_H(W)] - m^2 q^{2c} \\
&= m^2 q^c (1 - q^c)
\end{aligned}$$

Consequently, $\mathrm{Var}[\mathsf{GREY}(white)] = \mathrm{Var}[w_H(W)]/m^2 \leq q^c(1 - q^c)$.

□

Therefore,

$$\lim_{c \to \infty} E[\mathsf{GREY}(white)] = 0 \text{ and } \lim_{c \to \infty} \mathrm{Var}[\mathsf{GREY}(white)] = 0.$$

This means that we can obtain asymptotically ideal contrast by letting c large.

If we use the Naor-Shamir $(2, 2)$-VCS, we obtain the following corollary.

Corollary 1 *There exists a perfect black $(2, 2)$-VCS with reversing such that*

$$\begin{aligned}
E[\mathsf{GREY}(white)] &= (1/2)^c \\
\mathrm{Var}[\mathsf{GREY}(white)] &\leq (1/2)^c \{1 - (1/2)^c\}
\end{aligned}$$

with the expansion rate $m = 2$, where c is any positive integer.

For general (k, n)-VCS, we obtain the following corollary from [7].

Corollary 2 *For any $2 \leq k \leq n$, there exists a perfect black (k,n)-VCS with reversing such that*

$$\begin{aligned} E[\mathsf{GREY}(white)] &= (1-1/m)^c \\ \mathrm{Var}[\mathsf{GREY}(white)] &\leq (1-1/m)^c\{1-(1-1/m)^c\} \end{aligned}$$

for any positive integer c, where m is the expansion rate given by [7].

4.3 Example

As an example, we present a 3-Run $(2,2)$-VCS.

(Distribution phase) The dealer $\mathcal{D}$ runs the distribution phase of Naor-Shamir $(2,2)$-VCS three times independently. Let (s_1, s_2) be the shares of the first run, (s_1', s_2') be the shares of the second run and (s_1'', s_2'') be the set of shares of the third run.

Then the share of participant $\mathcal{P}_1$ is (s_1, s_1', s_1'') and that of participant $\mathcal{P}_2$ is (s_2, s_2', s_2'').

(Reconstruction phase)

1. We superimpose s_1 and s_2, and then obtain $T = s_1 + s_2$. Similarly, we obtain $T' = s_1' + s_2'$ and $T'' = s_1'' + s_2''$.
2. We reverse T, T' and T'', and obtain $\overline{T}, \overline{T'}$ and $\overline{T''}$.
3. We superimpose $\overline{T}, \overline{T'}$, $\overline{T''}$ and obtain $U = \overline{T} + \overline{T'} + \overline{T''}$.
4. We reverse U and obtain $\tilde{P}$.

(Contrast): We can then see that $\mathsf{GREY}(black) = 1$ and

$$E[\mathsf{GREY}(white)] = (1/4) \times (1/2) + (3/4) \times 0 = 1/8.$$

5 Discussion

5.1 Compatibility

The proposed scheme is fully compatible with traditional VCS in the following sense: even if we do not have a copy machine in the reconstruction phase, we can reconstruct the secret image I exactly in the same way as in the underlying VCS.

This is done as follows. Suppose that k participants do not have a copy machine in the reconstruction phase. They just superimpose their transparencies and then obtain T_1 as the reconstructed image. (See step 1 of the proposed reconstruction phase shown in Sec.4.1.) Note that T_1 is the reconstructed image obtained by the underlying traditional (k,n)-VCS.

In other words, we use a copy machine as a hedge to obtain better contrast. Therefore, our scheme is very attractive.

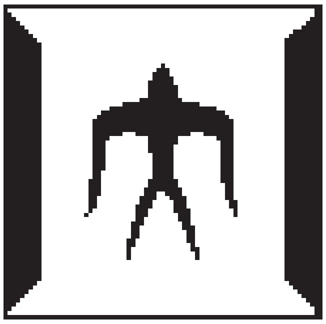

Figure 5: Original image

5.2 Complexity

The reconstruction phase of the c-run (k, n)-VCS with reversing requires $c + 1$ reversing operations and superimposing $kc - 1$ transparencies. The size of shares become c times larger than that of the original VCS.

6 Comparison

We show a comparison of $(2, 2)$-VCS (with reversing) among the Naor-Shamir scheme, our perfect black VCS with reversing and our perfect white VCS with reversing.

Fig.5 is the original image. Fig.6 is the reconstructed image by Naor-Shamir $(2, 2)$-VCS.

- Fig.7 $\sim$ Fig.9 are the reconstructed images by our perfect black $2, 3, 4$-run $(2, 2)$-VCS, respectively.
- Fig.10 $\sim$ Fig.13 are the reconstructed images by our perfect white $1, 2, 3, 4$-run $(2, 2)$-VCS, respectively.

7 Perfect White VCS

7.1 Conversion from Perfect Black VCS

We say that a (k, n)-VCS is *perfect white* if

$$\mathsf{GREY}(white) = 0 \text{ and } \mathsf{GREY}(black) > 0.$$

In usual pictures, the white region is much larger than the black region. Therefore, perfect *white* VCSs are much preferable than perfect *black* VCSs. However, no perfect white VCS has been known.

In this section, we show that a perfect *white* (k, n)-VCS with reversing is easily obtained from a perfect *black* (k, n)-VCS (with reversing).

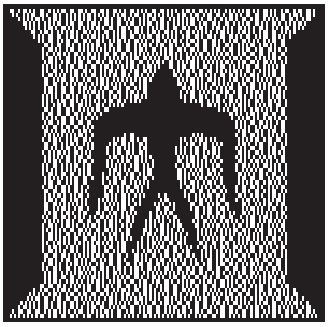

Figure 6: Naor-Shamir $(2,2)$-VCS

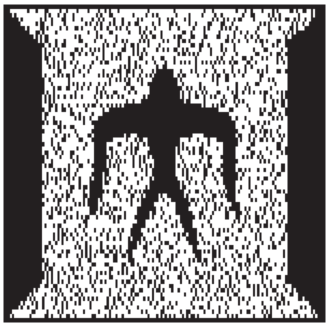

Figure 7: Proposed 2-run perfect black VCS

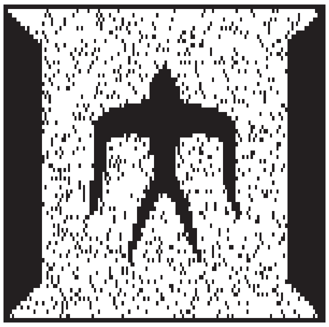

Figure 8: Proposed perfect black 3-run VCS

Figure 9: Proposed perfect black 4-run VCS

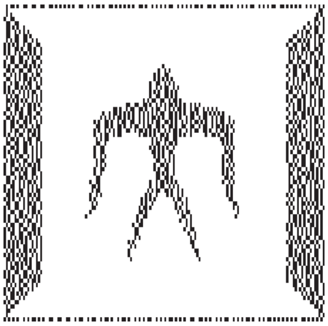

Figure 10: 1-run perfect white VCS

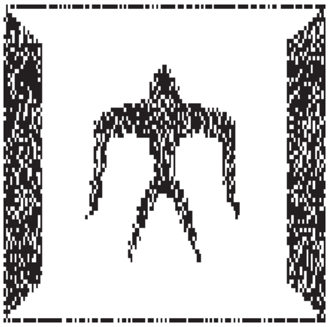

Figure 11: 2-run perfect white VCS

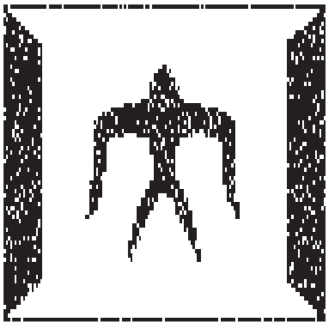

Figure 12: 3-run perfect white VCS

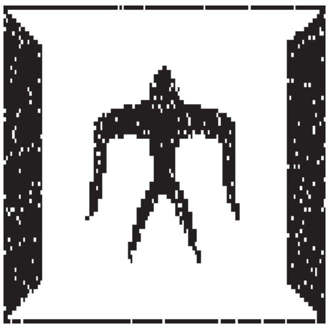

Figure 13: 4-run perfect white VCS

Theorem 2 *Suppose that there exists a perfect black (k,n)-VCS with reversing such that $E[\mathsf{GREY}(white)] = p$. Then there exists a perfect white (k,n)-VCS with reversing such that $E[\mathsf{GREY}(black)] = 1-p$.*

Proof. We describe a perfect *white* (k,n)-VCS.

In the distribution phase,

1. the dealer $\mathcal{D}$ first reverses the original image I and obtains $\overline{I}$.
2. $\mathcal{D}$ then applies the distribution phase of the perfect *black* (k,n)-VCS with reversing to $\overline{I}$.

In the reconstruction phase,

1. a qualified subset of participants apply step 1 $\sim$ step 3 of the reconstruction phase for the perfect *black* (k,n)-VCS with reversing and obtain a reconstructed image $\overline{I'}$.
2. They finally reverse $\overline{I'}$ and obtain $\overline{\overline{I'}}$.

Then it is easy to see that the above scheme is a perfect *white* (k,n)-VCS such that $E[\mathsf{GREY}(black)] = 1-p$.

□

7.2 Almost Ideal Contrast with Perfect White

We can obtain a perfect *white* (k,n)-VCS with reversing such that

$$E[\mathsf{GREY}(black)] \to 1$$

by applying Theorem 2 to our construction shown in Sec.4.1.

In this case, we can reduce the number of reversing from $c+1$ to c by terminating at step 3 of the reconstruction phase. The U of step 3 is the reconstructed image. This process is illustrated in Fig.14.

7.3 Example

As an example, we show how to convert the perfect black $(2,2)$-VCS of Sec.2.1 into a perfect white $(2,2)$-VCS with reversing. (See Fig 15.)

In the distribution phase:

1. the dealer $\mathcal{D}$ first reverses the original image I. Hence each white pixel is reversed into black and each back pixel is reversed into white.
2. $\mathcal{D}$ then applies the distribution phase of the perfect *black* $(2,2)$-VCS. Participant $\mathcal{P}_1$ obtains a share s_1 and participant $\mathcal{P}_2$ obtains a share s_2.

$$
\text{Image } I \to \text{reverse } \bar{I} \quad
\begin{array}{l}
\nearrow \; n \text{ transparencies} \\
\vdots \\
\searrow \; n \text{ transparencies}
\end{array}
$$

(Distribution phase)

$$
\begin{array}{l}
\text{stack } k \text{ sheets } T_1 \to \text{reverse } \overline{T}_1 \\
\qquad\qquad\qquad\qquad \searrow \\
\qquad\qquad\qquad\qquad\quad U = \overline{T}_1 + \cdots + \overline{T}_c \text{ (=reconstructed image)} \\
\qquad\qquad\qquad\qquad \nearrow \\
\text{stack } k \text{ sheets } T_c \to \text{reverse } \overline{T}_c
\end{array}
$$

(Reconstruction phase)

Figure 14: Perfect white VCS

In the reconstruction phase:

1. the two participants superimpose s_1 and s_2 and obtains $s_1 + s_2$.
2. They finally reverse $s_1 + s_2$ and obtain $\overline{s_1 + s_2}$.

From Fig 15, we see that a perfect white $(2,2)$-VCS is obtained such that $\mathsf{GREY}(black) = 1/2$.

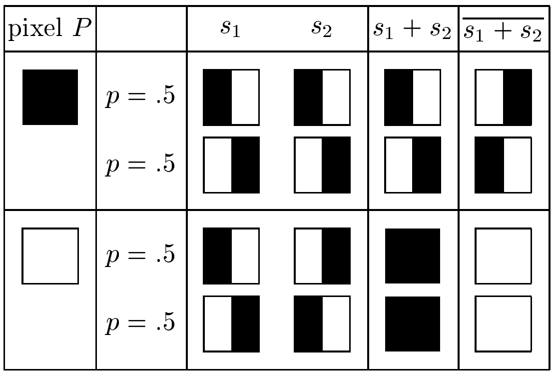

Figure 15: Perfect white 2-out-of-2 visual cryptography scheme

8 Perfect Black VCS for General Access Structure

Perfect black VCSs have been known only for (k, n)-threshold cases so far although VCS itself can be constructed for general access structures [1]. In this section, we show a perfect black VCS for any monotone access structure. This means that we can obtain a VCS with *reversing* for any monotone access structure such that the contrast is almost ideal.

8.1 Access Structure

Let $\mathcal{P} = \{1, \ldots, n\}$ be a set of participants. In a generalized secret sharing scheme, qualified subsets of $\mathcal{P}$ can recover the secret. Let

$$\Gamma \stackrel{\triangle}{=} \{A \subseteq \mathcal{P} \mid A \text{ can determine } s\}.$$

Then Γ is called an access structure and A is called an access set. However, any $B \notin \Gamma$ has no information on s.

Definition 2 *Γ is said to be monotone if*

$$A \in \Gamma, A \subseteq A' \Rightarrow A' \in \Gamma.$$

There exists a secret sharing scheme for Γ if and only if Γ is monotone [9, 2]. For an access structure Γ, define

$$\Gamma_0 \stackrel{\triangle}{=} \{A \subseteq \mathcal{P} \mid A \text{ is a minimal access set.}\}.$$

Γ_0 is called a minimal access structure.

In what follows, we assume that Γ is monotone.

8.2 General Construction

Naor and Shamir showed a perfect black (k, k)-VCS such that the expansion rate is $m = 2^{k-1}$ and $\mathsf{GREY}(white) = 1 - 1/2^{k-1}$ [10]. The basis matrices (M_k^0, M_k^1) are given as follows.

$$M_k^0 = \begin{pmatrix} | & | & & | \\ c_1 & c_2 & \cdots & c_{2^{k-1}} \\ | & | & & | \end{pmatrix} = \begin{pmatrix} -e_{k,1}- \\ \vdots \\ -e_{k,k}- \end{pmatrix}, \tag{2}$$

$$M_k^1 = \begin{pmatrix} | & | & & | \\ c'_1 & c'_2 & \cdots & c'_{2^{k-1}} \\ | & | & & | \end{pmatrix} = \begin{pmatrix} -e'_{k,1}- \\ \vdots \\ -e'_{k,k}- \end{pmatrix}, \tag{3}$$

where $\{c_1, c_2, \cdots, c_{2^{k-1}}\}$ is the set of all even weight binary vectors of lengh k and $\{c'_1, c'_2, \cdots, c'_{2^{k-1}}\}$ is the set of all odd weight binary vectors of lengh k.

Now by employing the above VCS, we show a perfect black VCS for any minimal access structure $\Gamma_0 = \{A_1, \cdots, A_t\}$.

Define $k_j = |A_j|$ and suppose that $A_j = \{j_1, \cdots, j_{k_j}\}$. A pair of basis matrices (L_0, L_1) for Γ_0 are then constructed as follows.

Construction of L_0. For $1 \le j \le t$, construct a $n \times 2^{k_j - 1}$ matrix

$$E_j = \begin{pmatrix} \vdots \\ e_{k_j,1} \\ \vdots \\ e_{k_j,k_j} \\ \vdots \end{pmatrix},$$

as follows:

- The j_uth row of E_j is the uth row of $M^0_{k_j}$ for $1 \le u \le k_j$.
- The other rows of E_j are $(1, \cdots, 1)$.

Then define

$$L_0 = (E_1, \cdots, E_t).$$

Construction of L_1. For $1 \le j \le t$, construct a $n \times 2^{k_j - 1}$ matrix

$$E'_j = \begin{pmatrix} \vdots \\ e'_{k_j,1} \\ \vdots \\ e'_{k_j,k_j} \\ \vdots \end{pmatrix},$$

as follows:

- The j_uth row of E'_j is the uth row of $M^1_{k_j}$ for $1 \le u \le k_j$.
- The other rows of E_j are $(1, \cdots, 1)$.

Then define

$$L_1 = (E'_1, \cdots, E'_t).$$

The expansion rate is $m = 2^{|A_1|-1} + \cdots + 2^{|A_t|-1}$ and $\mathsf{GREY}(white) = 1 - \frac{1}{m}$ in this VCS.

We show an example for $\Gamma_0 = \{\{1,2\},\{2,3,4\}\}$. First,

$$M^0_2 = \begin{pmatrix} 10 \\ 10 \end{pmatrix},\ M^1_2 = \begin{pmatrix} 10 \\ 01 \end{pmatrix}$$

$$M^0_3 = \begin{pmatrix} 0011 \\ 0101 \\ 0110 \end{pmatrix},\ M^1_3 = \begin{pmatrix} 0011 \\ 0101 \\ 1001 \end{pmatrix}$$

Therefore,

$$L_0 = \begin{pmatrix} 10\ 1111 \\ 10\ 0011 \\ 11\ 0101 \\ 11\ 0110 \end{pmatrix},\ L_1 = \begin{pmatrix} 10\ 1111 \\ 01\ 0011 \\ 11\ 0101 \\ 11\ 1001 \end{pmatrix}$$

The expansion rate is $m = 2^{2-1} + 2^{3-1} = 6$ and $\mathsf{GREY}(white) = 1 - 1/m = 5/6$.

Theorem 3 *The above L_0 and L_1 are a pair of basis matrices of a perfect black VCS for Γ_0 such that the expansion rate is $m = 2^{|A_1|-1} + \cdots + 2^{|A_t|-1}$ and $\mathsf{GREY}(white) = 1 - 1/m$.*

Proof. Let $\{0, 1\}$ the set of secrets. Then a secret sharing scheme is known for any $\Gamma_0 = \{A_1, \cdots, A_t\}$ as follows, where $A_j = \{j_1, \cdots, j_{k_j}\}$.

- Suppose that $s = 0$. Then for $1 \le j \le t$, the dealer $\mathcal{D}$ chooses random bits $b_{j,1}, \cdots, b_{j,k_j}$ such that

  $$0 = b_{j,1} \oplus \cdots \oplus b_{j,k_j}$$

  and gives $b_{j,u}$ to participant j_u for $1 \le u \le k_j$.

- Suppose that $s = 1$. Then for $1 \le j \le t$, $\mathcal{D}$ chooses random bits $b'_{j,1}, \cdots, b'_{j,k_j}$ such that

  $$1 = b'_{j,1} \oplus \cdots \oplus b'_{j,k_j}$$

  and gives $b'_{j,u}$ to participant j_u for $1 \le u \le k_j$.

Now in our VCS, $b_{j,u}$ is encoded to $e_{k_j,u}$ for L_0 and $b'_{j,u}$ is encoded to $e'_{k_j,u}$ for L_1. Further, (M_k^0, M_k^1) is the basis matrices of a perfect black (k,k)-VCS. Therefore, it is easy to see that L_0 and L_1 are a pair of basis matrices of a perfect black VCS for Γ_0.

It is clear that $m = 2^{|A_1|-1} + \cdots + 2^{|A_t|-1}$ and $\mathsf{GREY}(white) = 1 - 1/m$.
□

8.3 For Special Access Structure

If we apply the above construction to $\Gamma_0 = \{\{1,2\}, \{2,3\}, \{3,4\}\}$, then we obtain a VCS such that $m = 6$ and $\mathsf{GREY}(white) = 5/6$. In this subsection, we present a perfect black VCS such that $m = 4$ and $\mathsf{GREY}(white) = 3/4$.

Remember that the basis matrices of a perfect black $(2,2)$-VCS is given as follows.

$$M_0 = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} e_1 \\ e_2 \end{pmatrix}$$

$$M_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} e'_1 \\ e'_2 \end{pmatrix}$$

On the other hand, a secret sharing scheme for Γ_0 is known as follows. Let $\{0,1\}$ be the set of secrets. The dealer $\mathcal{D}$ chooses random bits $b_1, \cdots, b_4$ such that

$$\begin{aligned} s &= b_1 \oplus b_2 & (4) \\ &= b_3 \oplus b_4 & (5) \end{aligned}$$

Let

$$v_1 = b_1,\ v_2 = b_2,\ v_3 = (b_1, b_3),\ v_4 = b_4,$$

where v_i is a share of participant i.

Now we show a perfect black VCS for Γ_0. Let $d_1 = (b_1, b_2, b_1, x)^T$, where x means that eq.(4) is not used for participant 4. Let $d_2 = (x, x, b_3, b_4))^T$, where x means that eq.(5) is not used for participant 1 and participant 2. Define

$$G = (d_1, d_2) = \begin{pmatrix} b_1, & x \\ b_2, & x \\ b_1, & b_3 \\ x, & b_4 \end{pmatrix}$$

The basis matrices L_0 and L_1 for Γ_0 are then constructed as follows.
(Construction of L_0): In G,

- Substitute $e_1 = (1,0)$ into b_1 and b_3.
- Substitute $e_2 = (1,0)$ into b_2 and b_4.
- Substitute $(1,1)$ into x.

(Construction of L_1): In G,

- Substitute $e'_1 = (1,0)$ into b_1 and b_3.
- Substitute $e'_2 = (0,1)$ into b_2 and b_4.
- Substitute $(1,1)$ into x.

That is,

$$L_0 = \begin{pmatrix} 1011 \\ 1011 \\ 1010 \\ 1110 \end{pmatrix},\ L_1 = \begin{pmatrix} 1011 \\ 0111 \\ 1010 \\ 1101 \end{pmatrix}$$

It is easy to see that L_0 and L_1 are the basis matrices of a perfect black VCS for Γ_0. The expansion rate is $m = 4$ and $\mathsf{GREY}(white) = 3/4$.

9 Application to Colored VCS

Verheul and van Tilborg proposed a model for colored VCS and gave a general construction for colored (k, n)-VCS [12]. Blundo et al. improved this construction [7]. However, the contrast of the reconstructed images by these schemes is very poor.

In this section, we show that if there exists an almost ideal contrast (k, n)-VCS with reversing, then there exists a colored (k, n)-VCS with reversing such that the original image I is almost perfectly reconstructed.

9.1 Proposed Scheme

Any color is realized by mixing three primary colors, $red, blue$ and $yellow$, appropriately. The proposed colored VCS is based on this principle.

We assume that there is a color copy machine which has three coloring functions $\mathsf{Color}_{red}, \mathsf{Color}_{blue}, \mathsf{Color}_{yelow}$ as follows.

- Color_{red}: A black pixel is made into red.
- Color_{blue}: A black pixel is made into blue.
- Color_{yellow}: A black pixel is made into yellow.

(All white pixels remain white.)

Suppose that there exists an almost ideal contrast (k, n)-VCS with reversing denoted by Σ. Then the proposed scheme is described as follows. For simplicity, suppose that the secret image I consists of 7 colors which are obtained by simply mixing the primary three colors.

(Distribution Phase)

1. The dealer $\mathcal{D}$ decomposes I into three images I_{red}, I_{blue} and I_{yellow}, where I_x is the component of I of color x.

   That is, each pixel of I_x has color x or white, and I is reconstructed by stacking I_{red}, I_{blue} and I_{yellow}.

2. For each I_x, convert I_x into a black-white image I_x^B in such a way that all pixels of color x are made into black, and all white pixel remain white.

3. For each I_x^B, apply the distribution phase of Σ.

(Reconstruction Phase)

1. Apply the reconstruction phase of Σ to recover I_x^B for each color x. Let $\tilde{I}_x^B$ be the recovered image of I_x^B.

2. Apply the coloring function Color_x of the copy machine to the black-white image $\tilde{I}_x^B$ for each color x. Then we obtain a mono-color image $\tilde{I}_x$ such that all black pixels are made into color x, and all white pixel remain white.

$$
\begin{array}{ccl}
 & & I_{red} \to \text{monocolor } I^{B}_{red} \to \text{distribution phase of } \Sigma \\
 & \nearrow & \\
I & \to & I_{blue} \to \text{monocolor } I^{B}_{blue} \to \text{distribution phase of } \Sigma \\
 & \searrow & \\
 & & I_{yellow} \to \text{monocolor } I^{B}_{yellow} \to \text{distribution phase of } \Sigma
\end{array}
$$

(Distribution phase)

$$
\begin{array}{lcl}
\text{reconstruction of } \Sigma \to \tilde{I}^{B}_{red} \to \text{coloring } \tilde{I}_{red} & & \\
 & \searrow & \\
\text{reconstruction of } \Sigma \to \tilde{I}^{B}_{blue} \to \text{coloring } \tilde{I}_{blue} & \to & \text{stack} \to \text{reconstruction} \\
 & \nearrow & \\
\text{reconstruction of } \Sigma \to \tilde{I}^{B}_{yellow} \to \text{coloring } \tilde{I}_{yellow} & &
\end{array}
$$

(Reconstruction phase)

Figure 16: Proposed Colored VCS

3. Finally stack $\tilde{I}_{red}, \tilde{I}_{blue}$ and $\tilde{I}_{yellow}$.

This process is illustrated in Fig.16.

Since Σ achieves almost ideal contrast, $\tilde{I}_x$ is an almost prefect reconstruction image of I_x for each color x. Therefore, we can reconstruct I almost perfectly.

10 Application to Grey Level Images

In a grey level image, each pixel has g grey levels ranging from 0 (white) to $g-1$ (black). A VCS for grey level images was shown by Blundo et al. [6].

In this section, we show that if there exists an almost ideal contrast (k,n)-VCS with reversing, then there exists a (k,n)-VCS with reversing for grey level images such that the original image I is almost perfectly reconstructed.

We assume that there is a copy machine which can make a black pixel into grey level i for $1 \leq i \leq g-1$. Suppose that there exists an almost ideal contrast (k,n)-VCS with reversing denoted by Σ. Then the proposed scheme is described as follows.

(Distribution Phase)

1. The dealer $\mathcal{D}$ decomposes I into g images $I_0, I_1, \cdots, I_{g-1}$, where I_i is the component of I of grey level i.

   That is, each pixel of I_i has grey level i or 0, and I is reconstructed by stacking $I_0, I_1, \cdots, I_{g-1}$.

$$
\begin{array}{ccl}
 & & I_1 \to \text{monotone } I_1^B \to \text{distribution phase of } \Sigma \\
 & \nearrow & \\
I & \to & I_2 \to \text{monotone } I_2^B \to \text{distribution phase of } \Sigma \\
 & \searrow & \\
 & & I_3 \to \text{monotone } I_3^B \to \text{distribution phase of } \Sigma
\end{array}
$$

(Distribution phase)

$$
\begin{array}{lcl}
\text{reconstruction of } \Sigma \to \tilde{I}_1^B \to \text{grey leveling } \tilde{I}_1 & & \\
 & \searrow & \\
\text{reconstruction of } \Sigma \to \tilde{I}_2^B \to \text{grey leveling } \tilde{I}_2 & \to & \text{stack} \to \text{reconstruction} \\
 & \nearrow & \\
\text{reconstruction of } \Sigma \to \tilde{I}_3^B \to \text{grey leveling } \tilde{I}_3 & &
\end{array}
$$

(Reconstruction phase)

Figure 17: Proposed Grey Level VCS

2. For each I_i with $1 \leq i \leq g-1$, convert I_i into a black-white image I_i^B in such a way that all pixels of grey level i are made into black, and all white pixel remain white.

3. For each I_i^B, apply the distribution phase of Σ.

(Reconstruction Phase)

1. Apply the reconstruction phase of Σ to recover I_i^B for each grey level i. Let $\tilde{I}_i^B$ be the recovered image of I_i^B.

2. Apply the grey level function of the copy machine to each black-white image $\tilde{I}_i^B$. Then we obtain a two-level grey image $\tilde{I}_i$ such that all black pixels are made into grey level i, and all white pixel remain white.

3. Finally stack $I_0, I_1, \cdots, I_{g-1}$.

This process is illustrated in Fig.17.

Since Σ achieves almost ideal contrast, $\tilde{I}_i$ is an almost prefect reconstruction of I_i for each grey level i. Therefore, we can reconstruct I almost perfectly.

11 Conclusion

We first showed a (k,n)-VCS with *reversing* such that white pixels are almost perfectly reconstructed in addition to the perfect reconstruction of black pixels. The proposed scheme is fully compatible with traditional VCS.

We next showed how to convert a perfect *black* (k, n)-VCS (with reversing) into a perfect *white* (k, n)-VCS with reversing. Thirdly, we showed a perfect black VCS for any monotone access structure. Finally, we showed applications of our idea to colored VCS and grey level VCS, respectively.

It will be a further work to find another simple non-cryptographic operation which can achieve almost ideal contrast.

References

[1] G. Ateniese, C. Blundo, A. D. Santis and D. R. Stinson, "Visual cryptography for general access structures", in: Information and Computation, vol. 129, pp. 86–106 (1996).

[2] J. C. Benaloh and J. Leichter, "Generalized secret sharing and monotone functions", in: Proc. of Crypto'88, Lecture Notes on Computer Science, LNCS vol. 403, pp. 27–36 (1990).

[3] C. Blundo and A. De. Santis, "Visual cryptography schemes with perfect reconstruction of black pixels", in: Computer and Graphics, vol. 22, no. 4, pp. 449–455 (1998).

[4] C. Blundo, A. De. Santis and D. R. Stinson, "On the contrast in visual cryptography schemes", in: Journal of Cryptology, vol. 12, no. 4, pp. 261–289 (1999).

[5] C. Blundo, P. D'Arco, A. De. Santis and D. R. Stinson, "Contrast optimal threshold visual cryptography schemes", to appear in: SIAM Journal on Discrete Mathematics (Available from http://cacr.math.uwaterloo.ca/~dstinson/papers/COTVCS.ps).

[6] C. Blundo, A. De Santis and M. Naor, Visual cryptography for grey level images. Inf. Process. Lett. vol.75(6), pp.255-259 (2000)

[7] C. Blundo, A. De. Bonis and A. De. Santis, "Improved schemes for visual cryptography", in: Designs, Codes, and Cryptography, vol. 24, pp. 255–278 (2001).

[8] P. A. Eisen and D. R. Stinson, "Threshold Visual Cryptography Schemes With Specified Whiteness Levels of Reconstructed Pixels", in: Designs, Codes, and Cryptography, vol. 25, no. 1, pp. 15–61 (2002).

[9] M. Itoh, A. Saito and T. Nishizeki, "Multiple assignment scheme for sharing secret", in: Journal of Cryptology, vol. 6, no. 1, pp. 15–20 (1993)

[10] M. Naor and A. Shamir, "Visual cryptography", in: Proc. of Eurocrypt'94, Lecture Notes on Computer Science, LNCS vol. 950, pp. 1–12 (1995).

[11] M. Naor and A. Shamir, "Visual cryptography II: Improving the Contrast Via the Cover Base", in: Proc. of Security Protocols'96, Lecture Notes on Computer Science, LNCS vol. 1189, pp. 197–202 (1997). Full version available from http://www.wisdom.weizmann.ac.il/~naor/PAPERS/new_cov.ps.

[12] E. R. Verheul and H. C. A. van Tilborg, "Constructions and properties of k out of n visual secret sharing schemes", in: Designs, Codes, and Cryptography, vol. 11, no. 2, pp. 179–196 (1997).