Visual Cryptography with Polarization*

Eli Biham
Computer Science Department
Technion – Israel Institute of Technology
Haifa 32000, Israel
Email: biham@cs.technion.ac.il
WWW: http://www.cs.technion.ac.il/~biham/

Ayal Itzkovitz
Computer Science Department
Technion – Israel Institute of Technology
Haifa 32000, Israel
Email: ayali@cs.technion.ac.il
WWW: http://www.cs.technion.ac.il/~ayali/

Abstract

Visual cryptography was introduced by Naor and Shamir as a way to allow fast visual sharing of graphic objects. No reconstruction device is required; instead reconstruction is performed by fitting slides together. Several schemes were suggested, which allow users to share secret pictures (and text) in an information-theoretically secure way, so that reconstruction is easy if all the shares are given, but it is impossible if one of them is missing. The drawbacks of all the existing methods are the exponentially small contrast of the deciphered picture as the number of shares increases, and the reduction in quality due to pixels' being represented by many smaller (black and white) pixels.

In this paper we propose using light polarization properties for visual cryptography, and describe new visual cryptographic schemes based on light polarization which are better than the optimal existing schemes. Then we present an ultimate scheme which does not subdivide pixels, and in which the contrast is independent of the number of shares.

*Presented in the Dagstuhl seminar on Cryptography, September 1997, and in the RUMP session of CRYPTO'98.

1 Introduction

Visual cryptography was introduced by Naor and Shamir in [13]. Visual cryptographic schemes allow to share secret data and print it on slides in such a way that reconstruction can be performed visually without any computation (neither by computer nor by humans) by fitting the slides together. When the slides are fitted together, the shared data appears instantaneously. However, one slide, or a subset of slides, cannot be used to reconstruct the secret data, nor leak any information on the secret data.

In their paper Naor and Shamir propose several types of visual cryptographic schemes: (1) A 2-out-of-2 scheme, in which two slides are required to reconstruct the secret data, while none of these two slides have any information on the secret data (and thus even a powerful computer cannot analyze a single slide and get any information on the secret data). (2) n-out-of-n schemes, in which n slides are required to reconstruct the secret data, while any subset of up to $n-1$ slides have no information on the secret data. (3) k-out-of-n schemes, in which any subset of k slides can be used to reconstruct the secret data by fitting them together, while any subset of up to $k-1$ slides do not have any information on the secret data. (4) They also propose schemes in which two different slides with two different pictures, show a third unrelated picture when fitted together.

In their 2-out-of-2 scheme they take an original picture (or a printed text viewed as a picture), and share each pixel separately. The picture is shared on two slides, in such a way that each slide contains no information on the picture, but by fitting both slides together the picture appears instantaneously. Each original pixel is represented on the two slides by two subpixels: one of them is white, and the other one is black. The choice of the white and black subpixels of each of the pixels (i.e., which of the two subpixels is the white and which is the black) of one of the two slides is chosen at random, independently of the picture (even before the picture is chosen). The choice of the white and black subpixels in the second slide is done as follows: For each white pixel in the original picture choose the order of the white and black subpixels exactly as in the corresponding pixel in the first slide, and for each black pixel in the original picture choose the order of the white and black subpixels as the complement of the corresponding pixel in the first slide. Figure 1 describes this construction. As the order of white and black subpixels is random in the first slide, it is also random in the second slide. Only the relation between the orders in the first and the second slides is not random. Thus, given only one slide, the (random) order of the white and black subpixels do not contain any information on the picture. However, when the two slides are fitted one on top of the other, an original black pixel is seen as complete black (as half of it is black in the first slide, and the second half is black in the second slide), while original white pixels are seen as half white and half black.

However, the contrast of the reconstructed picture is lower than the original, as original black pixels are shown in black, but original white pixels are shown

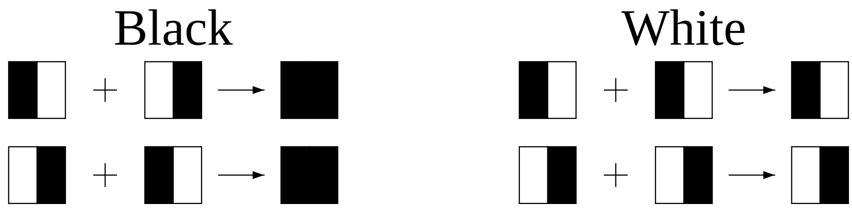

Figure 1: Naor and Shamir's 2-out-of-2 Scheme

as half white and half black. Thus, the contrast of the reconstructed picture, defined as the difference between the average gray levels of the representations of the original black and the original white pixels, is only 50%. The contrast of the n-out-of-n schemes is exponentially small 2^{-n+1}, and the contrast of the k-out-of-n schemes is even lower. Also note that the quality of the pictures might be poor, as not only the contrast is low, also the (white) pixels are not represented with uniform gray levels, but as a random mixing of white subpixels and black subpixels.

Naor and Shamir proved that their proposed schemes are optimal with respect to contrast, as it is impossible to generate secure schemes with a higher contrast.

Several other works had generalized their work and proposed other applications of visual cryptography: Naccache [11] had proposed how to share color pictures, when none of the slides contain any information on the original picture. Naor and Shamir [14] had proposed other schemes using non-transparent slides. Droste [9] had generalized the schemes in which two different pictures fitted together give a third picture. Naor and Pinkas [12] had shown how to utilize visual cryptography for authentication, and many other works [1, 2, 3, 4, 5, 6, 7, 10, 15, 16] extended visual cryptography is various directions.

In this paper we propose to utilize light polarization for visual cryptography. We present a 2-out-of-2 scheme with 100% contrast, several 2-out-of-n schemes, and for even n's an n-out-of-n scheme, all of them with a higher contrast than the corresponding optimal schemes of Naor and Shamir. Most proposed schemes have uniform gray levels, as the original pixels are not divided into several subpixels. We show reductions from our schemes with n slides to the schemes of Naor and Shamir with $n-1$ slides, and vice versa, and thus can use their proof of optimality to show that our better schemes are optimal in our model. We also show n-out-of-n schemes for odd n's, and a 3-out-of-3 scheme that supports three gray levels (white, gray, and black).

We then show that these results can also be extended to k-out-of-n schemes, and to colored schemes.

Finally, we utilize another additional feature of polarized light to present an ultimate n-out-of-n scheme with 100% contrast for any n.

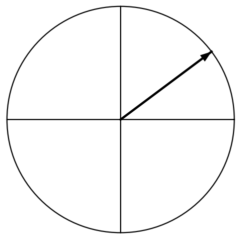

Figure 2: A Two-Dimensional Representation of a Wave of Light

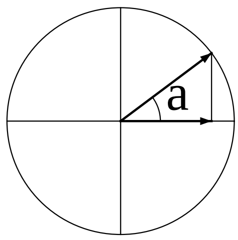

Figure 3: Projection of Light Polarization

This paper is organized as follows: In Section 2 we briefly describe the main properties of light polarization. In Section 3 we describe our 2-out-of-2 scheme based on light polarization. In Section 4 we describe 2-out-of-n schemes. In Section 5 we describe n-out-of-n schemes. In Section 6 we mention our k-out-of-n schemes, based on Naor and Shamir's reduction from n-out-of-n schemes to k-out-of-n schemes. In Section 7 we present our ultimate n-out-of-n schemes with 100% contrast. Finally, in Section 8 we summarize the paper.

2 A Short Introduction to Light Polarization

Waves of light are two dimensional, and can be represented by a two dimensional vector (see Figure 2). Devices, called *polarizers*, can project polarization on any other axis. An example of such projection on the X axis is given in Figure 3. In this figure, the original wave, which has angle α related to the X axis, is projected on the X axis. Only a fraction of $\cos^2\alpha$ (the square of the projected vector length) of the light is transfered by this polarization, and all the transfered light becomes polarized in the new direction. Once polarized, future polarizations are independent of the previous ones, and of the previous polarization directions: only the current direction affect the next polarization. Therefore, two consecutive polarization projections, the first by angle α and the second by angle β, transfer only a fraction of $\cos^2\alpha\cos^2\beta$ of the original

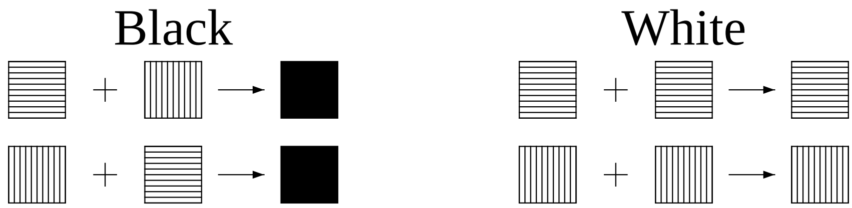

Figure 4: Our 2-out-of-2 Scheme

light, and rotate the polarization by angle $\alpha + \beta$. In particular, if $\alpha = -\beta$, the resultant polarization direction is unmodified, but only a fraction of $\cos^4 \alpha$ of the light is transferred.

Usually, the viewable light is a mixing of light polarized in all directions. Only half of the viewable light is thus transfered through a polarizer. If two polarizer are fitted together with the same projection axis, all the light transfered by the first polarizer is transmitted also by the second, as the projection angle is 0, and $\cos^2 0 = 1$. However, if two polarizers are set in orthogonal directions, no light is transfered from the second polarizer, as all the light transfered by the first one has an orthogonal direction to the projection axis of the second one.

For more information on light polarization see [8].

3 Our 2-out-of-2 Scheme

Unlike in Naor and Shamir's scheme, our 2-out-of-2 scheme does not divide the pixels into subpixels. Naor and Shamir used this division to gain different average gray levels for white and black pixels, while in each slide each pixel is still half black. Instead, we use the features of light polarization for the same purpose. Thus, we no longer need to have black (opaque) pixels or subpixels in each slide, as the distinction between white and black is done using parallel vs. orthogonal polarizers.

The construction is as follows: Each original pixel is represented by one pixel of the same size. This pixel is made of a polarizer, directed to one of two orthogonal directions, which we denote by X and $\bar{X}$. The choice of the direction (either X or $\bar{X}$) of the pixels in one of the two slides is chosen at random, independently of the picture (even before the picture is chosen). The choice of the directions in the second slide is done as follows: For each white pixel in the original picture choose the same direction as in the corresponding pixel in the first slide, and for each black pixel in the original picture choose the orthogonal direction. Figure 4 describes this construction: in the figure we assume that X is the horizontal polarization angle, and that $\bar{X}$ is vertical. Polarized results are denoted by their polarization angle, while black results (no light is transferred) are denoted by black pixels. As the polarization direction is random in the first slide, it is also random in the second slide. Only the relation between the directions in the first and the second slides (i.e., both have same direction, or either the directions are orthogonal) is not random. Thus, given only one slide, the (random) directions do not contain any information on the picture. However, when the two slides are fitted one on top of the other, an original black pixel combines two orthogonal polarization angles, and thus no light can be transferred, while original white pixels combine two same angles, and thus all the light transferred by the first slide is also transferred by the second. As each pixel is represented by only one (black or white) subpixel, the quality of the combined picture is perfect.

4 2-out-of-n Schemes

We present several different 2-out-of-n schemes. One scheme divides the pixels into subpixels, and in each subpixel the polarization angle is chosen out of two orthogonal possibilities. The other schemes use non-orthogonal polarization angles, and reach the same goal without dividing the original pixels.

4.1 A 2-out-of-n Scheme with Orthogonal Directions

This scheme divides the original pixels to $\lceil \log_2 n \rceil$ or more subpixels. We first describe it with division to $\lceil \log_2 n \rceil$ subpixels, and for simplicity assume that $n = 4$ (and $\log_2 n = 2$). In this case, each pixel is represented by two subpixels, and each subpixel can be in one of two orthogonal polarization angles X or $\bar{X}$. Obviously, there are four possible combinations of the polarization angles of both subpixels. When constructing the four slides, we choose for each original black pixel the set of all the four possible polarization angles of both subpixels to appear in the four slides in a random order. Each original white pixel is chosen with the same choice in all slides, which is chosen at random from the four possibilities. Thus, each slide is random and does not contain any information on the original picture. When any pair of the slides is fitted together, the white pixels always transfer light, while the black pixels transfer light only by some of their subpixels, or do not transfer light at all.

The contrast of this scheme is as follows: original white pixels are viewed in white (0% black) , while black pixels are viewed with either 50% black or 100% black. As these black choices are chosen at random, and as there are four possibilities for choosing a pair of slides from four slides with 50% black, and two with 100% black, the average contrast is $\frac{4 \cdot 0.5 + 2 \cdot 1}{6} = \frac{2}{3}$. This average contrast is higher than the (provably) optimal contrast of Naor and Shamir in their corresponding scheme.

For larger numbers of shares, the scheme is as follows: divide the each pixel to $l = \lceil \log_2 n \rceil$ subpixels, and select n different l-subpixel "values" out of the

2^l possible l-subpixel values, with the property that the selection is balanced for each subpixel when n is even (e.g., take all 2^l possible combinations, and discard $(2^l - n)/2$ pairs of complement combinations), or almost balanced when n is odd (e.g., discard pairs of complement combinations, and then discard a single additional combination). Then select only these combinations: for a white pixel select one combination from this list at random and use it for all slides, and for a black pixel select all these combinations in a random order. For even n's, each subpixel of a black pixel differs from exactly $n/2$ out of the $n-1$ other shares, while no difference occurs in white pixels, leading to average contrast of

$$\frac{n/2}{n-1}.$$

For odd n's, subpixels of $(n-1)/2$ shares differ from $(n+1)/2$ out of the $n-1$ other shares, while subpixels of $(n+1)/2$ shares differ from $(n-1)/2$ out of the $n-1$ other shares, leading to an average contrast of

$$\frac{n-1}{2n}\frac{(n+1)/2}{n-1} + \frac{n+1}{2n}\frac{(n-1)/2}{n-1} = \frac{(n+1)/2}{n}.$$

Note that in these schemes the contrast varies between pixels, or between the choices of the pairs of slides. Overall, this contrast is better than the (provably) optimal contrast of Naor and Shamir.

We can devise a variant of this scheme with a fixed contrast, using $\binom{n}{\lceil n/2\rceil}$ subpixels, where for white pixels the polarization of the subpixels of the first slide are selected at random, and these polarizations are also copies to all other slides. For black pixels, we view the n polarizations of each pixel in the n slides as a n-"bit" value, where each "bit" accepts one of the two orthogonal polarization angles. The $\binom{n}{\lceil n/2\rceil}$ subpixels of each pixel are selected to include all the n-"bit" value with exactly $\lceil n/2\rceil$ polarization angles in one direction and $\lfloor n/2\rfloor$ in the orthogonal direction. Clearly, for any pair of slides, there are exactly

$$\binom{n-2}{\lceil n/2\rceil - 1 \quad \lfloor n/2\rfloor - 1} + \binom{n-2}{\lceil n/2\rceil - 1 \quad \lfloor n/2\rfloor - 1}$$

subpixels whose polarization differ, thus the contrast is exactly

$$\frac{\binom{n-2}{\lceil n/2\rceil - 1 \quad \lfloor n/2\rfloor - 1} + \binom{n-2}{\lceil n/2\rceil - 1 \quad \lfloor n/2\rfloor - 1}}{\binom{n}{\lceil n/2\rceil}} = \begin{cases} \frac{n/2}{n-1}, & \text{if } n \text{ is even;} \\ \frac{(n+1)/2}{n}, & \text{if } n \text{ is odd.} \end{cases}$$

In many cases, the same fixed contrast can be achieved with fewer subpixels. We describe here only one simple example of n being a power of 2. Each pixel is divided to $n-1$ subpixels. For simplicity of description, select two orthogonal polarization directions, and denote them by 0 and 1. For the scheme to work correctly, the names of the 0 vs. 1 directions (out of two orthogonal directions) should be done at random for each subpixel (but same in all slides), i.e., not all 0 subpixels have parallel polarization angles. The slides are generated as follows: For black pixels, the first $\log_2 n$ slides are generated such that for each subpixel the selection of the values of the $\log_2 n$ slides is different, and the $n-1$ subpixels contain all the $n-1$ possible combinations, except for the all-zero combination. Then, $n-\log_2 n$ slides are generated as all the linear combinations of all possible subsets of the first $\log_2 n$ slides (including the empty subset, i.e., a slide with all subpixels being 0). For white pixels a random selection of the directions of the subpixels of the first slide are made, and all the slides are generated as copies of this selection. This construction assures that for any choice of two slides, black pixels differ by exactly $n/2$ out of the $n-1$ subpixels, and white pixels differ by zero subpixels, leading to contrast of exactly $\frac{n/2}{n-1}$.

4.2 A 2-out-of-n Scheme with non-Orthogonal Directions

In this scheme we do not divide the pixels into subpixels. Instead, we choose the polarization angles from a larger set. We choose n distinct polarization angles: X, $X+\frac{\pi}{n}$, $X+2\frac{\pi}{n}$, $X+3\frac{\pi}{n}$, $\ldots$, $X+(n-1)\frac{\pi}{n}$. When constructing the slides, we choose for each original black pixel the set of all the n possible polarization angles to appear in the n slides in a random order. Each original white pixel is chosen with the same angle in all slides, where the angle is chosen at random. Thus, each slide is random and does not contain any information on the original picture. When any pair of the slides is fitted together, the white pixels always transfer light, while the black pixels transfer $\cos^2\alpha$ of the light, where α is the difference of their angles, i.e., transfer only some of the light, or do not transfer light at all. The average contrast reached in this scheme is

$$\text{contrast} \quad = \quad \frac{1}{n-1}\sum_{i=1}^{n-1}\left(1-\cos^2\frac{i\pi}{n}\right) = \frac{1}{n-1}\sum_{i=0}^{n-1}\sin^2\frac{i\pi}{n} =$$

using $\sin^2\alpha = (1-\cos 2\alpha)/2$:

$$= \quad \frac{1}{n-1}\sum_{i=0}^{n-1}\frac{1-\cos 2i\pi/n}{2} = \frac{1}{n-1}\frac{n}{2} - \frac{1}{n-1}\frac{1}{2}\sum_{i=0}^{n-1}\cos\frac{2i\pi}{n} =$$

using $\sum_{j=0}^{n-1}\cos j\pi/n = 0$:

$$= \quad \frac{n/2}{n-1} - 0 = \frac{n/2}{n-1},$$

for both even and odd n's. This contrast is the optimal contrast possible for any selection of n polarization angles (either distinct or not, and either orthogonal or not).

Optimality is shown as follows: let $\alpha_0, \alpha_1, \ldots, \alpha_{n-1}$ be a set of n polarization angles. Then the average contrast between any pair of them is

$$\text{contrast} \quad = \quad \frac{2}{n(n-1)}\sum_{i<j}\left(1-\cos^2(\alpha_i-\alpha_j)\right) = \frac{2}{n(n-1)}\sum_{i<j}\sin^2(\alpha_i-\alpha_j) =$$

$$
\begin{aligned}
&= \frac{2}{n(n-1)} \sum_{i<j} \frac{1-\cos(2\alpha_i - 2\alpha_j)}{2} = \\
&= \frac{2}{n(n-1)} \frac{n(n-1)/2}{2} - \frac{2}{n(n-1)} \frac{1}{2} \sum_{i<j} \cos(2\alpha_i - 2\alpha_j) = \\
&= \frac{1}{2} - \frac{2}{n(n-1)} \frac{1}{2} \frac{1}{2} \sum_{i \neq j} \cos(2\alpha_i - 2\alpha_j) = \\
&= \frac{1}{2} - \frac{2}{n(n-1)} \frac{1}{2} \frac{1}{2} \left[\left(\sum_{i,j=0}^{n-1} \cos(2\alpha_i - 2\alpha_j) \right) - n \right] = \\
&= \frac{1}{2} + \frac{1}{2n(n-1)} n - \frac{1}{2n(n-1)} \sum_{i,j=0}^{n-1} \cos(2\alpha_i - 2\alpha_j) = \\
&= \frac{1}{2} + \frac{1}{2(n-1)} - \frac{1}{2n(n-1)} \Re \sum_{i,j=0}^{n-1} e^{\mathbf{i}2\alpha_i - \mathbf{i}2\alpha_j} =
\end{aligned}
$$

where $\mathbf{i}$ is the imaginary unit

$$
\begin{aligned}
&= \frac{n/2}{n-1} - \frac{1}{2n(n-1)} \Re \sum_{i,j=0}^{n-1} e^{\mathbf{i}2\alpha_i - \mathbf{i}2\alpha_j} = \\
&= \frac{n/2}{n-1} - \frac{1}{2n(n-1)} \Re \left(\sum_{i=0}^{n-1} e^{\mathbf{i}2\alpha_i} \sum_{j=0}^{n-1} e^{-\mathbf{i}2\alpha_j} \right).
\end{aligned}
$$

As the two sums are conjugates their product is real and non-negative. We can therefore conclude that for any set of polarization angles, the contrast is bounded by

$$\text{contrast} \leq \frac{n/2}{n-1}.$$

4.3 Even Better 2-out-of-n Schemes

We had just proved that we reached the optimal contrast possible in these models. We now show that the contrast of the previous scheme (with various polarization angles) can be improved considerably with very simple modifications to the schemes. We observe that the light is reduced every time it is projected. Thus, if we would only cause the light to be projected again through the same slides, we can increase the contrast. We can cause the light to be projected twice through the pair of slides using a mirror: instead of looking at the slides from one side while the source of light is at the other side, we look at the slides from the same side as the source of light, and put a mirror in the other side. A variant of this method can be used with some new slide projectors, in which the source of light is set at the upper part of the projector, while the slides are put on top of a mirror, and the light is transfered twice through the slides before it is projected on the screen. In this case, white remains white (as all the pixels have parallel polarization), but black becomes darker: if $\cos^2 \alpha$ of the light is transfered by the first projection, only $\cos^2 \alpha$ of this remaining light is transfered by the second projection. The contrast is increased by a factor of $5/4$ to $(5/8)n/(n-1)$ (for $n > 2$).

We can even cause the light to be projected more than twice without loosing any feature of our scheme by giving each party several exact copies of his slide. In this case, reconstruction is done visually by interleaving the slides. We can reach any required contrast in this way, by choosing a sufficiently large number of duplicated slides. For example, by giving two copies of each slide, the light is projected three times, the fraction of transferred light is reduced from $\cos^2 \alpha$ to $\cos^6 \alpha$, and the contrast is increased by a factor of $11/8$ to $(11/16)n/(n-1)$ for $n > 3$. In the general case, given l copies of each slide, the transferred light is reduced $l' = 2l - 1$ times to $\cos^{2l'} \alpha$, and the contrast is

$$\left(1 - \prod_{i=1}^{l'} \frac{2i-1}{2i}\right) \frac{n}{n-1} = \left(1 - \frac{1}{2^{2l'}} \binom{2l'}{l'}\right) \frac{n}{n-1}$$

if $n > l'$ (the product in this formula is the free constant of the Fourier series of $\cos^{2l'} \alpha$). For $l' \geq n$ the formula of the contrast has additional terms: for $l' = n$ it is

$$\left(1 - \frac{1}{2^{2l'}} \binom{2l'}{l'} - \frac{1}{2^{2l'-1}}\right) \frac{n}{n-1},$$

and for $l' > n$

$$\left(1 - \frac{1}{2^{2l'}} \binom{2l'}{l'} - \frac{1}{2^{2l'-1}} \sum_{i=1}^{\lfloor l'/n \rfloor} \binom{2l'}{l'+in}\right) \frac{n}{n-1}$$

(the additional terms in this formula are the coefficients of $\cos 2in\alpha$ in the Fourier series of $\cos^{2l'} \alpha$). Observe that $\frac{1}{2^{2l'}}\binom{2l'}{l'} + \frac{1}{2^{2l'-1}} \sum_{i=1}^{\lfloor l'/n \rfloor} \binom{2l'}{l'+in} \to 1/n$ when $l' \to \infty$, and thus the contrast can be as close to 1 as we wish

$$\left(1 - \frac{1}{2^{2l'}} \binom{2l'}{l'} - \frac{1}{2^{2l'-1}} \sum_{i=1}^{\lfloor l'/n \rfloor} \binom{2l'}{l'+in}\right) \frac{n}{n-1} \stackrel{l' \to \infty}{\longrightarrow} \left(1 - \frac{1}{n}\right) \frac{n}{n-1} = 1.$$

5 n-out-of-n Schemes

We divide the n-out-of-n schemes to two cases: in the simpler case n is even, and in the other n is odd.

5.1 Even n

For even $n \geq 4$ we describe a general n-out-of-n scheme, built above Naor and Shamir's optimal n-out-of-n scheme but improves their results to one additional slide.

We reduce the problem of generating an n-out-of-n scheme to the problem of generating Naor and Shamir's $(n-1)$-out-of-$(n-1)$ schemes, e.g., a 4-out-of-4 scheme in our model is constructed using Naor and Shamir's 3-out-of-3 scheme.

In Naor and Shamir's $(n-1)$-out-of-$(n-1)$ optimal scheme, each pixel is represented by 2^{n-2} subpixels. In our n-out-of-n scheme we also divide each pixel into 2^{n-2} (but we generate n slides rather than $n-1$). We first generate a "zero slide" using a randomly chosen polarization angle X in each of the 2^{n-2} subpixels. Then, we generate the other $n-1$ slides similarly to Naor and Shamir's construction, where a white subpixel is replaced by a polarization X of that subpixel, and a black subpixel is replaced by the orthogonal angle $\bar{X}$ of that subpixel. In this scheme all white pixels have an even number of slides with each polarization direction, and black pixels have an odd number of slides with each polarization direction.

We now show that (1) construction is correct, (2) any collection of n slides contains no information on the secret picture, (3) contrast is optimal.

It is easy to see that fitting slides together with the "zero slide" cause any set of originally white subpixels to remain white, and any set of originally black pixels to remain black, as this is equivalent to fitting the zero slide to each of the other slides, resulting with white (polarized) subpixels, and complete black (dark) subpixels. Therefore, fitting all n slides reconstructs the picture with the same contrast as Naor and Shamir's $(n-1)$-out-of-$(n-1)$ scheme. Their best achieved contrast is $1/2^{n-1}$ for n slides, i.e., $1/2^{n-2}$ for $n-1$ slides, thus, according to the construction, we achieve contrast $1/2^{n-2}$, which we later show as optimal.

It is clear that any subset of the slides that include the zero slide, except for the full set of slides, does not contain any information on the original picture, as this is equivalent to a subset of Naor and Shamir's slides. Due to the construction of the slides, the $n-1$ slides without the zero slide also do not contain any information. Another way to prove it uses the observation that by turning the directions of all the subpixels of any single slide by $\pi/2$, all white pixels become black, and vice versa.

We now show a reduction, constructing a n-out-of-n scheme for the Naor and Shamir model, out of any $(n+1)$-out-of-$(n+1)$ scheme (with only two orthogonal polarization directions) in our model. Using this reduction we prove the optimality of our results. Given a $(n+1)$-out-of-$(n+1)$ scheme in our model, produce a n-out-of-n scheme in the following way. Choose one of the slides (in an arbitrary way). Call it the "zero slide". For any other slide mark the subpixels that have the same polarization direction as the corresponding subpixels in the "zero slide" as white, and the subpixels which have orthogonal polarization as black. Excluding the "zero slide", we claim that the remaining n slides are a correct scheme in the Naor and Shamir model. This can be viewed as publishing one of the slides (the zero slide), and remaining with a scheme with one less slide.

From Naor and Shamir's proof of optimality and using the above reduction we conclude that our result is also optimal under our model.

5.2 Odd n

For an odd number n of slides, the above construction does not work, and in fact there is no 3-out-of-3 scheme with only two orthogonal polarization directions. However, there are 3-out-of-3 schemes with more than two polarization directions.

The best n-out-of-n scheme with an odd n we are aware of has contrast 2^{-n+1} (which is the same as the contrast in Naor and Shamir's schemes). The preparation of this scheme is equivalent to the optimal scheme of Naor and Shamir, with two differences: one is the usage of two orthogonal polarization angles instead of the white and black colors. The second difference affect only the second slide, in which the orthogonal directions are replaced by two directions with angle $\pi/4$ apart.

For each pixel generate 2^{n-1} subpixels, each with angles either 0 or $\pi/2$, except that in the second slide the angles are either 0 or $\pi/4$. For a white pixel select all combinations of the angles that have an odd number of 0's (thus an even number of $\pi/2$ and $\pi/4$). For a black pixel select all combinations of the angles that have an even number of 0's (thus an odd number of $\pi/2$ and $\pi/4$). For $n = 3$ the contrast is $1/4$, and the contrast is reduced by a factor of 4 for any two additional slides. Note that the slide with the $\pi/4$ direction can be set in some other locations, rather than only the second slide, but in many of these locations the contrast becomes smaller.

Another interesting 3-out-of-3 scheme uses three directions whose distance is $\pi/3$ apart (e.g., 0, $\pi/3$, and $2\pi/3$): in this scheme white is represented by either the same directions in all the slides with a probability of $1/3$, or either with three different directions with a probability of $2/3$. For black, two of the three slides should have the same direction, while the other one should have a different direction. In this scheme white transfers a fraction of $6/16$ of the light, black transfers $3/16$, and the contrast is $3/16 = 0.1875$.

Improvement of this scheme can be made by giving each party several copies of his slide. In this case, given many slides, black becomes almost complete dark, while white transfers about $1/3$ of the light, so the contrast becomes about $1/3$.

An interesting variant of this last 3-out-of-3 scheme (with a single copy of each slide) supports three colors: white (about 36% transparent), gray (25%) and black (about 14%). The trick is to rotate the angles of the last slide by $\pi/12$, and consider all combinations whose sum of the three angles in the three slides (modulo π) is $11\pi/12$ as white, all combinations whose sum is $3\pi/12$ as gray, and all combinations whose sum is $7\pi/12$ as black. Of course, a picture that does not contain any gray has only white and black pixels, and in this case the contrast between black and white is about 0.22.

6 k-out-of-n Scheme

Naor and Shamir describe a general and optimal transformation of k-out-of-k schemes to k-out-of-n schemes. We can use this transformation in our model as well in all schemes that have two choices for the polarization angle in each slide. As for even n's our n-out-of-n schemes have better contrast, we also get better contrast in the k-out-of-n schemes for even k's.

Note that in the case of basing a k-out-of-n scheme on our scheme with an odd n (where the contrast is the same as in the case of Naor and Shamir), the second slide of the generated k-out-of-n scheme should be set with the angles 0 and $\pi/4$, while all the rest should be set with 0 and $\pi/2$. As we do not know in advance which slide becomes the second, or whether a specific slide participates in the constructions of the k slides, we need to give two slides to each participant, one with the orthogonal angles, and one with the $\pi/4$ angles for case this participant should put the second slide in the construction.

7 The Ultimate n-out-of-n Scheme

As shown in Section 3 we succeeded in finding a perfect 2-out-of-2 scheme, so that a 100% contrast is achieved when fitting all slides together. Although we showed general n-out-of-n schemes, they did not produce perfect results. In this section we present additional properties of light polarization that can be used to provide perfect n-out-of-n schemes with no loss of contrast.

Special kinds of polarizers, called *retarders*, can change light polarization by $\pi/2$. Retarders of width $\frac{1}{4}\lambda$, where λ is the wave length, change the linear polarization, dealt in the previous sections, to circular polarization[1], and retarders of width $\frac{1}{2}\lambda$ change linear polarization to linear polarization in a possibly different angle. If the polarized light and the $\frac{1}{2}\lambda$-width retarder are set with an angle α, the transferred light is rotated by an angle 2α, and the angle between the transferred light and the retarder becomes 3α. If the angle α is set in advance to be $\pi/4$, the light polarization is rotated by $\pi/2$. Retarders have a perfect transmission, and all the light is transformed and transferred through them.

If we denote one linear-polarization angle by 1 and the orthogonal angle by 0, the $\frac{1}{2}\lambda$ retarder may be considered as complementing the angle (or XORing the angle by 1). A regular glass, film or two adjacent $\frac{1}{4}\lambda$ retarders in opposite directions can be considered as XORing by 0 (they do not change the polarization

[1]In circular polarization the angle of polarization changes with time. There is also elliptic polarization whose amplitude and angle change with time.

angle). It is also possible to take a retarder, and cut holes in it in the XOR-0 pixels.

We show now a general construction for an n-out-of-n scheme. For each pixel, let the color to be $V \in \{0, 1\}$, where 0 denotes white and 1 denotes black, choose $n-1$ random values $V_1, V_2, \ldots, V_{n-1}$ and compute $V_n = V_1 \oplus V_2 \oplus \ldots \oplus V_{n-1} \oplus V$. Generate n slides without dividing pixels into subpixels. In each pixel of slide i, if $V_i = 1$, use a XOR-1 retarder, otherwise use XOR-0 retarder. When fitted (in any order), and put between a source of polarized light, and a polarizer whose polarization angle is parallel to the angle of the polarized source, all the original white pixels transfer all the light, and the original black pixels remain dark.

It is easy to see that this solution is perfectly secure. Every subset of $n-1$ slides contain randomly selected retarders. All n slides are required to reconstruct the original picture. Also, although being general for any n, this solution does not suffer from the "scalability" problem, and each pixel is represented by only one pixel, while the contrast remain fixed at 100%. Thus, for any n-out-of-n scheme we reach the same results as for our 2-out-of-2 schemes.

8 Summary

We described new visual cryptographic schemes using light polarization. These schemes have better contrast than the schemes described in the literature in the usual models, and the last scheme we presented have a 100% contrast for any n-out-of-n scheme. We should mention that it is practically possible to implement these schemes in the current technology, either by cutting pieces of polarizer and recombine them, or by using specially designed printers. We should also note that these schemes can be also used with color pictures, as color pictures can be represented by RGB: each pixel is constructed from three subpixels with colors red, green, and blue, each of them is dealt as in our black and white construction, and only an additional (fixed and publicly known) slide adding the color to each subpixel is added as the last slide in these schemes.

It is interesting to note that some kinds of color copiers can take some polarizers, and cancel their polarization properties (by careful heating) in specified areas, thus enabling easy automation of our proposed schemes. In the case of the ultimate n-out-of-n scheme, generation of slides requires taking a retarder, and cancel the polarization in the appropriate locations. In the case of schemes with linear polarization where two or more polarization angles are required in each slide, we can generate a different slide for each polarization angle, using such a printer, and glue them together after printing.

Acknowledgments

We are pleased to acknowledge the major help of Steve Lipton and Ofer Biham in the Physical background of this research, and for Jon Green and Orr Dunkelman for useful comments.

References

[1] G. Ateniese, C. Blundo, A. De Santis, D. R. Stinson, *Constructions and Bounds for Visual Cryptography*, 23rd International Colloquium on Automata, Languages and Programming, LNCS 1099, Springer-Verlag, pp. 416–428, 1996.

[2] Giuseppe Ateniese, Carlo Blundo, Alfredo De Santis, Douglas R. Stinson, *Visual Cryptography for General Access Structures*, Information and Computation, Vol. 129, pp. 86–106, 1996.

[3] G. Ateniese, C. Blundo, A. De Santis, D. Stinson, *Extended Schemes for Visual Cryptography*, Theoretical Computer Science, Vol. 250, pp. 143–161, 2001.

[4] Giuseppe Ateniese, Carlo Blundo, Alfredo De Santis, Douglas R. Stinson, *Extended capabilities for visual cryptography*, Theoretical Computer Science, Vol. 250, No. 1–2, pp. 143–161, 2001.

[5] I. Biehl, S. Wetzel, *Traceable visual cryptography*, Information and Communications Security, Lecture Notes in Computer Science 1334, pp. 61–71, 1997.

[6] C. Blundo, P. D'Arco, A. De Santis, D. Stinson, *Contrast Optimal Threshold Visual Cryptography Schemes*, SIAM Journal on Discrete Mathematics, Vol. 16, pp. 224–261, 2003.

[7] Carlo Blundo, Alfredo De Santis, Douglas R. Stinson, *On the Contrast in Visual Cryptography Schemes*, Journal of Cryptology, Vol.12, No. 4, pp. 261–289, 1999.

[8] Max Born, Emil Wolf, *Principles of Optics: Electromagnetic Theory of Propagation, Interference and Diffraction of Light*, 7th Edition, Cambridge University Press, October 1999.

[9] Stefan Droste, *New Results on Visual Cryptography*, Lecture Notes in Computer Science, Advances in Cryptology, proceedings of CRYPTO'96, pp. 401–415, 1996.

[10] Philip A. Eisen, Douglas R. Stinson, *Threshold Visual Cryptography Schemes With Specified Whiteness Levels of Reconstructed Pixels*, Designs, Codes and Cryptography Vol. 25, pp. 15–61, 2002.

[11] David Naccache, *Color in Visual Cryptography.*

[12] Moni Naor, Benny Pinkas, *Visual Cryptography and Authentication*, Lecture Notes in Computer Science, Advances in Cryptology, proceedings of CRYPTO'97, pp. 322–336, 1997.

[13] Moni Naor, Adi Shamir, *Visual Cryptography*, Lecture Notes in Computer Science, Advances in Cryptology, proceedings of EUROCRYPT'94, pp. 1–12, 1994.

[14] Moni Naor, Adi Shamir, *Visual Cryptography II: Improving the Contrast Via the Cover Base*, Lecture Notes in Computer Science, proceedings of Security Protocols workshop, pp. 197–202, 1996.

[15] D. R. Stinson, *Visual cryptography and threshold schemes*, Dr. Dobb's Journal, pp. 36–43, April 1998.

[16] E. R. Verheul, H. C. A. van Tilborg, *Constructions and properties of k out of n visual secret sharing schemes*, Designs, Codes and Cryptography, Vol. 11, pp. 179–196, 1997.