Visual Cryptography II: Improving the Contrast Via the Cover Base*

Moni Naor † Adi Shamir ‡

Abstract

In Eurocrypt'94 we proposed a a new type of cryptographic scheme, which can *decode* concealed images without any cryptographic computations, by placing two transparencies on top of each other and using the decoder's (human) visual systems. One of the drawback of that proposal was a loss in contrast: a black pixel is translated in the reconstruction into a black region, but a white pixel is translated into a grey region (half black and half white). In this paper we propose am alternative model for reconstruction with a different set of operation (which we call the "Cover" semi-group) is proposed. In this model we are able to obtain a better contrast than is possible in the previous one.

We prove tight bounds on the contrast as a function of the complexity of the scheme. We also show that for constracting k-out-n secret sharing schemes when $n \geq k \geq 3$ the new method is not applicable.

---

*Part of this work was done while the authors where visiting the Newton Institute, Cambridge.

†Dept. of Applied Mathematics and Computer Science, Weizmann Institute of Science, Rehovot 76100, Israel. E-mail: naor@wisdom.weizmann.ac.il. Research supported by an Alon Fellowship and a grant from the Israel Science Foundation administered by the Israeli Academy of Sciences.

‡Dept. of Applied Mathematics and Computer Science, Weizmann Institute of Science, Rehovot 76100, Israel. E-mail: shamir@wisdom.weizmann.ac.il.

1 Introduction

In Eurocrypt'94 [2] we considered the problem of encrypting images (printed text, handwritten notes, pictures, etc.) in a perfectly secure way which can be *decoded* directly by the human visual system. The basic model consists of "splitting" the image into two transparencies I and II (one can be considered as the ciphertext (which can be sent by mail or faxed) and the other one as the secret key). The original cleartext is revealed by placing the transparency with the key over the one with the ciphertext, even though each one of them is indistinguishable from random noise. The system is similar to a one time pad in the sense that each page of ciphertext is decrypted with a different transparency. Due to its simplicity, the system can be used by anyone without any knowledge of cryptography and without performing any cryptographic computations.

The main drawback of the above scheme is that there is loss in contrast and resolution: each pixel in the original image is mapped into several subpixels in both transparency I and II. The distribution in each transparency of the color of these subpixels is independent of the color of the original pixel. In case the original pixel is black, then the combination of the subpixels of the two transparencies yields a completely black region. However, in case the original pixel is white, then the combination of the two transparencies yields a region where half the pixels are white and half are black. The difference between the grey level of a black pixel and white pixels is called the *contrast*.

Note the distinction of this model from the usual one-time-pad: the underlying algebraic structure is the "Or" semi-group rather than a group (commonly known as the Xor group). In particular, the visual effect of a black subpixel in one of the transparencies cannot be undone by the colour of that subpixel in other transparencies which are laid over it. This monotonicity rules out common encryption techniques which add random noise to the cleartext during the encryption process, and subtracts the same noise from the ciphertext during the decryption process.

It is not hard to show that in the above model and in case the encoding is done pixel by pixel then the best possible contrast we can obtain is $1/2$ [1]. The goal of this paper is to suggest a different model allowing us to do Visual Cryptography with a much better contrast.

The new model contains several important changes from the previous one: in the new model there will be two "opaque" colours and a completely transparent one (which can even be implemented as a hole, or cutout). Suppose that the original image consists of two colours, say red and yellow[2]. We use the "Cover" semi-group on {Red, Yellow, Transparent} where the top opaque color wins:

[1]In the Eurocrypt'94 paper we showed that the contrast can be at most $1/2^{k-1}$ in case we are doing k-out-of-k secret sharing.

[2]Any two colours will do of course. We choose red and yellow so as do avoid confusion with the black and white colours of [2].

top / bottom	R	Y	T
R	R	Y	R
Y	R	Y	Y
T	R	Y	T

Unlike the "Or" semi-group, the "Cover" semi-group is non-commutative and hence the order on which the transparencies are stacked is significant. The second change is that instead of I and II being a single transparency each, they are now c sheets marked $1, 2, \ldots, c$. Each sheet contains red, yellow and transparent pixels. The reconstruction is done by merging the sheets of I and II, i.e. for $1 \leq i \leq c$ put the ith sheet of II on top of the ith sheet of I and the $(i+1)$th sheet of I on top of the ith sheet of II. We assume that the sheets align perfectly, i.e. we can label all the pixels in the sheets in the range $1, \ldots, m$ and when the sheets are placed on top of each other all the jth pixels in all the sheets are in the same position. Figure 1 demonstrates the merging with $c = 4$.

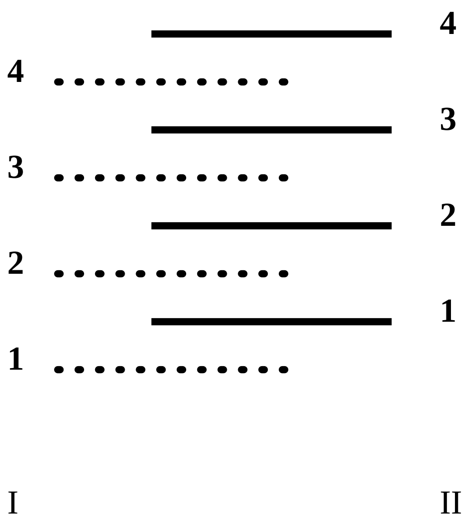

Figure 1: Merging with $c = 4$

In this model we are able to obtain a much better contrast, roughly $1 - 1/c$ where c is both the number of sheets and the number of subpixels each pixel in the original image is mapped to. The contrast is defined to be the difference between the fraction of red pixels in a reconstructed red and the fraction of non-yellow pixels in a reconstructed yellow. Note that if the reconstructed region contains a transparent pixel, then it counts "against" both red and yellow original pixels.

We present two constructions: the first one (Section 2) requires both I and II to have c sheets each and obtains a contrast of $1 - 1/c$. The sheets I and II get are monochromatic, i.e. I gets red/transparent sheets and II gets yellow/transparent sheets. The second construction (Section 3) requires the two users to get c sheets *between* them while achieving a $1 - 1/c$ contrast. However, each user's sheets must contain red, yellow and transparent pixels. In Section 4 we prove that these constructions are optimal with respect to the number of sheets used as a function of the contrast.

In the Eurocrypt'94 paper (as well as in [1]) this basic model was extended into a visual variant of the k-out-of-n secret sharing problem: given a written message, we would like to generate n transparencies so that the original message is visible if any k (or more) of them are stacked together, but totally invisible if fewer than k transparencies are stacked together (or analyzed by any other method). The original encryption problem can be considered as a 2 out of 2 secret sharing problem. In Section 5 we show that the new model is not applicable to general k-out-of-n secret sharing: for $n \geq k \geq 3$ no scheme can have a non-trivial contrast. For the 2-out-n problem we can get some improvement over the Or semi-group. We show a tight bound of $1/2$ for the contrast in this case.

2 The Monochromatic Construction

We describe our scheme as a 2-out-of-2 perfectly secure secret sharing scheme which is equivalent to a perfectly secure encryption method where one party may be the one-time-pad and the other the ciphertext. As in [2], we map each pixel separately. Each pixel in the original image is mapped into c subpixels (it is best when the c subpixels can be arranged in a square, but it is not necessary; any other method of tiling is acceptable). User I gets c sheets indexed 1 through c. In each of those sheets, one of the subpixels is red and the other $c-1$ subpixels are transparent. Similarly for II, in each sheet one subpixel is yellow and the other $c-1$ subpixels are transparent. The way the sheets of I and II are merged is by starting from sheet number 1 of I and putting sheet number 1 of II on top of it, then sheet number 2 of I and so on.

The order in which the subpixels of I are coloured red constitutes a permutation π on $\{1, \ldots c\}$ (i.e. on the ith sheet pixel $\pi(i)$ is red) and the order in which the the subpixels of II are coloured yellow constitutes a permutation σ.

The permutations π and σ are chosen according to the following method: π is chosen uniformly at random from the set of all permutations on c elements[3]. If the original pixel is yellow let $\sigma = \pi$ and if the original pixel is red let $\sigma(i) = \pi(i+1)$ for $1 \leq i \leq c-1$ and $\sigma(c) = \pi(1)$, i.e. σ is a shift of π.

Claim 2.1 *If $\pi = \sigma$ then all the red subpixels are covered by yellow subpixels.*

Claim 2.2 *If $\sigma(i) = \pi(i+1)$ for $1 \leq i \leq c-1$ and $\sigma(c) = \pi(1)$ then all the yellow pixels, except $\sigma(c)$ are covered by red ones.*

Finally, in order to make sure that no partial information is leaked we have

Claim 2.3 *Both π and σ are distributed uniformly at random over the set of permutation on $\{1, \ldots c\}$ regardless of the colour of the original pixel.*

Proof: As constructed π is a random permutation and hence is independent of the colour of the pixel. σ is either equal to π or is a cyclic shift of it. In both cases its distribution is uniform over the set of permutation on $\{1 \ldots c\}$. $\square$

[3] As we shall see, π can be chosen from a smaller set, that of cyclic permutations.

Since the information I and II each gets is a collection of random permutations corresponding to each of the pixels of the original image, this is a *perfectly secure* 2-out-of-2 secret sharing scheme.

Note that sheet 1 of I is useless, i.e. the pixel $\pi(1)$ will always be covered by either the one in $\sigma(1)$ (in case the original pixel is yellow) or by $\sigma(c)$ (in case the original subpixel is red). Therefore we really have $2c-1$ sheets altogether.

Note also that there is no need to choose π from the set of *all* permutations on c elements. It suffices to choose it from the set of all cyclic shifts on c elements, since σ would be then also distributed uniformly over the cyclic shifts.

3 The Bichromatic Construction

We now describe an improved scheme that requires roughly half the total number of sheets in order to get the same contrast. Let c be an even number. As above, each pixel in the original image is mapped into c pixels. The two parties share between them c sheets altogether labeled 1 through c where party I gets all the odd numbered sheets and II gets all the even ones. The reconstruction is as before, by merging the sheets of I and II.

The scheme for splitting one pixel is as follows: let $C \in \{R, Y\}$ be the color of the pixel shared and $\bar{C}$ the other color. Choose a permutation π on $\{1 \ldots c\}$ uniformly at random. On the ith sheet let pixel $\pi(i)$ be coloured C and pixel $\pi(i+1)$ be coloured $\bar{C}$ and all the rest of the pixels are transparent. To complete the description, at sheet c, make the pixel coloured R transparent as well (this pixel is either $\pi(c)$ or $\pi(1)$).

Claim 3.1 *IF $C = Y$ then in the reconstructed region only pixels coloured Y are visible and if $C = R$ the $c-1$ pixels are R and one is Y.*

Proof: First note that each position $1 \le j \le c$ is transparent in all but at most two sheets. If $C = Y$, then for sheet $1 \le i \le c-1$ the pixel coloured R (which is $\pi(i+1)$) is covered by the pixel coloured Y in sheet $i+1$ (which has $\pi(i+1)$ coloured Y). The top sheet has only a Y pixel so no R pixel is left uncovered. Finally note that position j is coloured Y in sheet $\pi^{-1}(j)$, so all the visible pixels are Y. If $C = R$, then for sheet $1 \le i \le c-1$ the pixel coloured Y (which is $\pi(i+1)$) is covered by the pixel coloured R in sheet $i+1$ (which has $\pi(i+1)$ coloured R). As for the top sheet, it has pixel $\pi(1)$ coloured Y and this will remain Y since it is left uncovered. Note that no pixel is transparent, since position j is coloured R in sheet $\pi^{-1}(j)$, so no visible pixel is transparent, one is Y and $c-1$ are R. $\Box$

Claim 3.2 *The bichromatic scheme is perfectly secure.*

Proof: Given the odd sheets (those I receives) there are two candidates for π: one assuming the shared pixel is Y, denoted π_Y, and one assuming it is R, denoted π_R. If the the jth pixel of sheet i is Y then $\pi_Y(i) = j$ and if the kth pixel is R then $\pi_Y(i+1) = k$. Note that this completely specifies π_Y and there are no contradiction since all odd sheets have a pixel coloured Y and one coloured R and since I gets only the odd sheets each $\pi(i)$ is defined once. Similarly for odd $1 \le i \le c-1$ we have that $\pi_R(i) = j$ if the jth pixel at sheet i is R and $\pi_R(i+1) = k$ if the k pixel at sheet i is Y.

We claim that no matter how the original pixel is coloured, the distributions of π_R and π_Y are uniform over the permutations of $\{1 \ldots c\}$: If the original pixel is coloured $C \in \{R, Y\}$, then $\pi_C = \pi$, which is distributed uniformly, and $\pi_{\bar{C}}$ is a shift by one position of π, which is also distributed uniformly. Therefore the distribution of the sheets I receives is independent of C.

As for the sheets II receives, suppose that in the generations we hadn't erased the pixel coloured R on sheet c. Now the information II receives is similar to the information I gets, which we have just argued. But since we have only erased (fixed) information, II cannot gain anything from it, so the distribution of the sheets II receives is independent of C. □

4 Lower bound on the number of sheets

A natural issue to consider at this point is whether the solutions of Section 2 & 3 can be improved. The most important factor seems to be the total number of transparencies used, since it implies technical problems of alignment and fading of the lower colors. We show however that in order get a contrast of $1 - \alpha$ one needs $1/\alpha$ transparencies (between I and II) which is what our second construction achieves.

Our lower bound is applicable to any method that works on each pixel individually. I.e. each pixel in the original image is mapped into several pixels in the sheets distributed to the two parties. In order to show the lower bound we consider one particular pixel position in the region corresponding to a pixel in the original image and analyze the probability that it is correct. Before we continue, we give precise definition of a 2-out-2 secret sharing scheme.

Definition 4.1 *A solution to the* 2*-out-of-*2 *visual secret sharing scheme using the Cover semi-group consists of:*

- *Two distributions D_R and D_Y on $c \times m$ matrices where each entry is an element from $\{R, Y, T\}$.*
- *A partition of $\{1..c\}$ into two subsets S_I and S_{II}.*

The parameter c is the number of sheets, m is the resolution and the two subsets are the sheets that each party receives. To share a yellow pixel, the dealer samples from D_Y and to share a red pixel the dealer samples from D_R. The ith sheet is assigned the ith row of the matrix generated (where each column is mapped to some predetermined location on the sheets). Party I receives the sheets in S_I and Party II receives the sheets in S_{II}. The solution is considered valid if the following conditions are met:

Security: For both S_I and S_{II} the induced distribution on the rows in S_I or S_{II} is identical in D_Y and D_R.

Contrast: For every matrix M produced by D_Y, if the cover operation is performed on the columns of M (i.e. for each column separately perform the cover operation from 1 *to* c*), then the number of Y pixels is at least d_1. For every matrix M produced by D_R the, if the cover operation is performed on the columns of M then the number of R pixels is at least d_2. The* contrast *is the value $\frac{d_1}{m} - \frac{m-d_2}{m} = \frac{d_1+d_2}{m} - 1$.*

To prove the lower bound fix any column and consider the probability that it reconstructs the correct color. We will prove an lower bound δ on the sum of P_Y and P_R where P_C is the probability that the column does *not* reconstruct C when the distribution is D_C for $C \in \{R, Y\}$. Taking $1-\delta$ yields the desired result for the contrast, since if we sum over all the columns the probabilities of an incorrect reconstruction we get that $(m-d_1)+(m-d_2) \geq \delta \cdot m$ which implies that $\frac{d_1+d_2}{m} - 1 \geq 1 - \delta$.

For simplicity assume that the scheme is monochromatic, i.e for every pixel there is a $C \in \{R, Y\}$ such that the ith sheet is either coloured C or is transparent. It can easily be seen that this can at most double the number of sheets - simply split each sheet into two, one containing the red pixel and the other the yellow one (preserving the transparent ones)[4]. Also we can assume w.l.o.g. that for each party at most one sheet is opaque, since there is no point in giving one party two opaque sheets when it is clear that the bottom one will not influence the outcome.

Let $A_i(C)$ be the event that pixel i is opaque given that the original pixel is C. From the security requirement we have that $P_i = \text{Prob}[A_i(R)] = \text{Prob}[A_i(Y)]$ is well defined, since otherwise it would be possible to guess the colour of the original pixel with probability better than $1/2$ based on the ith sheet alone.

For sheets i and j belonging to two different parties and such that i is below j let $A_{ij}(C)$ be the event that pixel i and j are opaque given that the original pixel is C. If sheet i is either transparent or coloured C then let $P_{ij} = \text{Prob}[A_{ij}(\bar{C})]$. The events $A_{ij}(C)$ and $A_{ik}(C)$ are disjoint for $1 \leq i < j < k \leq c$ and the events $A_{ki}(C)$ and $A_{ji}(C)$ are disjoint for $1 \leq k < j < i \leq c$. Therefore, for all $1 \leq i < c$ we must have

$$P_i \geq \sum_{j=i+1}^{c} P_{ij}$$

and for all $1 < i \leq c$ we must have

$$P_i \geq \sum_{k=1}^{i-1} P_{ki}$$

.

The quantity $P_i - \sum_{j=i+1}^{c} P_{ij}$ is the probability that the ith sheet is the top colour and the original pixel is of the other colour. In other words, it is the loss in contrast contributed by the ith sheet. We are interested in the minimum possible value of

$$\sum_{i=1}^{c} \left(P_i - \sum_{j=i+1}^{c} P_{ij} \right) = P_Y + P_R. \tag{1}$$

From the assumption that for each party at most one sheet is opaque we have have that $\sum_{i=1}^{c} P_i \leq 2$. By adding at most one additional sheet (i.e. increase c by 1) we can make $\sum_{i=1}^{c} P_i = 2$ without changing the contrast. Hence to bound (1) from below is equivalent to searching for $\rho = \max \sum_{i=1}^{c-1} \sum_{j=i+1}^{c} P_{ij}$ subject to the same constraints (and taking $2 - \rho$).

[4] Actually we can do slightly better: if we start with a bichromatic scheme with c' sheets we can construct a monochromatic scheme with the same contrast using $c = 2c' - 1$ sheets. Do not split the top sheet, simply turn the yellow pixel into a red one. This makes the reconstruction redder for both an original yellow and an original red, i.e. whatever the yellow losses the red gains.

Claim 4.1 *Consider the linear program*

$$\max \sum_{i=1}^{c} \sum_{j=i+1}^{c} P_{ij}$$

s.t

$$\sum_{j=i+1}^{c} P_{ij} - P_i \leq 0 \quad 1 \leq i < c \tag{2}$$

$$\sum_{k=1}^{i-1} P_{ki} - P_i \leq 0 \quad 1 < i \leq c \tag{3}$$

and

$$\sum_{i=1}^{c} P_i \leq 2 \tag{4}$$

Then the optimal value ρ *is* $2 - \frac{2}{c}$ *and is obtained when for all* $1 \leq i \leq c$ *we have* $P_i = \frac{2}{c}$ *and* $P_{i,i+1} = \frac{2}{c}$ *and all the rest are* 0.

Proof: Consider the dual linear program. We have $2c-1$ variables: $U_1, \ldots U_{c-1}$ corresponding to inequalities (2), $L_2, \ldots L_c$ corresponding to inequalities (3) and S corresponding to inequality (4). The dual program is

$$\min 2 \cdot S$$

s.t.

$$U_i + L_j \geq 1 \quad 1 \leq i < j \leq c \tag{5}$$

$$-U_i - L_i + S \geq 0 \quad 1 \leq i \leq c \tag{6}$$

A solution to the above program is $U_i = \frac{c-i}{c}, L_i = \frac{i-1}{c}$ and $S = \frac{c-1}{c}$. To see that (5) holds, note that

$$U_i + L_j = \frac{c-i}{c} + \frac{j-1}{c} = \frac{c+j-i-1}{c} \geq 1$$

since $j \geq i+1$. As for (6), $U_i + L_i = \frac{c-i}{c} + \frac{i-1}{c} = \frac{c-1}{c} = S$. For this solution the value of the target function is $2 \cdot S = 2 - \frac{2}{c}$ and is equal to the one proposed in the claim. By duality they are both optimal. □

From the claim we have that (1) is at least $\frac{2}{c}$ and therefore we can conclude:

Theorem 4.1 *In any 2-out-of-2 secret sharing scheme that uses c sheets we must have:*

- *If the scheme is monochromatic, then the contrast can be at most* $1 - \frac{2}{c+1}$ *(the scheme in Section 2 matches this bound).*
- *If the scheme is bichromatic, then the contrast can be at most* $1 - \frac{1}{c}$ *(the scheme in Section 3 matches this bound).*

5 On k-out-of-n schemes

We now discuss the applicability of the Cover semi-group to k-out-of-n secret sharing schemes and show that in general it is not the appropriate tool, no matter how many sheets are used.

Definition 5.1 *A solution to the k-out-of-n visual secret sharing scheme using the Cover semi-group consists of:*

- *Two distributions D_R and D_Y on $c \times m$ matrices where each entry is an element from $\{R, Y, T\}$.*
- *A partition of $\{1..c\}$ into n subsets $S_1, S_2, \ldots S_n$.*

The parameter c is the number of sheets, m is the resolution and the subsets are the sheets that each party receives. To share a yellow pixel, the dealer samples from D_Y and to share a red pixel the dealer samples from D_R. The ith sheet is assigned the ith row of the matrix generated (where each column is mapped to some predetermined location on the sheets). Party j gets the sheets in S_j. For a subset $T \subset \{1, \ldots, n\}$ of parties M_T be the submatrix of M whose rows are those in $\bigcup_{j \in T} S_j$. The solution is considered valid if the following conditions are met:

Security: For any $j_1, j_2, \ldots j_{k-1} \in \{1, \ldots, n\}$ the induced distribution on the rows in $\bigcup_{i=1}^{k-1} S_{j_i}$ is identical in D_Y and D_R.

Contrast: For every subset $T \subset \{1, \ldots, n\}$ of k different parties, for every matrix M produced by D_Y, if the cover operation is performed on the columns of M_T then the number of Y pixels is at least d_1. For every matrix M produced by D_R the, if the cover operation is performed on the columns of M_T then the number of R pixels is at least d_2. The contrast *is the value $\frac{d_1}{m} - \frac{m-d_2}{m} = \frac{d_1+d_2}{m} - 1$.*

Consider the case of a 3-out-of-3 secret sharing scheme. We claim that there is no scheme using the Cover semi-group that has contrast better than 0. As in Section 4 we concentrate on one pixel position. We can also assume w.l.o.g. that in each party *exactly* one sheets is opaque and the rest are transparent. (There is no point in having more than one opaque colour and by adding an extra layer we can have the property that exactly one sheet is opaque.)

Given a realization of the method, i.e. a column in the matrix M, all that matters is the relative order the colours. Consider all the combinations that yield a top yellow colour:

Y	Y	Y	Y
R	R	Y	Y
R	Y	Y	R

For any of these combinations, if two parties (out of the three) are chosen at random, then with probability at least 2/3 the top colour is yellow. Similarly, the combinations that have a red on the top have the property that if two parties (out of the three) are chosen at random, then with probability at least $2/3$ the top colour is red. Since two parties should gain no information about the pixel shared it follows that the probability of having one of the above combinations is the same whether the original pixel is red or yellow. Therefore the probability of having a yellow in the reconstruction is the independent of the original colour and the contrast is 0.

Given a k-out-of-n secret sharing scheme for $n \geq k \geq 3$, we can turn it into a a 3-out-of-3 secret sharing scheme by considering the first three parties and giving the party 3 the sheets of parties $3, \ldots k$. Therefore we can conclude:

Theorem 5.1 *There are no k-out-of-n secret sharing schemes using the Cover semi-group with contrast better than 0 for any $n \geq k \geq 3$.*

What remains to be checked is the case of 2-out-of-n secret sharing. We claim that the contrast cannot be better than $1/2$ in this case and that this is achievable for any n. Consider any pixel position and examine the n-dimensional vector where the jth entry corresponds to the colour the jth party received. From the security property it follows that the distribution on the number of occurrences of each colour is independent of the original colour, since this distribution can be checked by picking a random party and examining its colour. For a given realization, suppose that two parties are picked at random. If there are a entries coloured yellow and $n-a$ entries coloured red, then in case the original is red the probability of picking the wrong colour is at least $\frac{a^2}{n^2}$ and in case the original is yellow the probability is at least $\frac{(n-a)^2}{n^2}$. However, $\frac{a^2}{n^2} + \frac{(n-a)^2}{n^2}$ is at least $1/2$ and we get that for at least one pair out of the n parties the contrast is at most $1/2$.

We know that in the Or semi-group the best contrast for a 2-out-of-n scheme is $1/4$. Therefore it is of interest to see that we can do better in the Cover semi-group and approach the above bound. To see how to approach a contrast of $1/2$ we will adopt the scheme of Section 2. The number of sheets each party gets is $2c$ where the $(2i-1)$th sheet corresponds to the the ith red sheet and the $2i$th sheet corresponds to the the ith yellow sheet. Given the sheets of two parties j_1 and j_2, to reconstruct the image merge the two collections starting, say, with the lower numbered party. For each pixel in the original image we run n independent copies of the scheme of Section 2, i.e. each pixel is mapped into $c \cdot n$ pixels altogether. For $1 \leq j, k \leq n$, party j receives for the kth copy the following: if $\langle k, j \rangle = 0$, then the share of party I and if $\langle k, j \rangle = 1$ the share of party II where $\langle k, j \rangle$ is the inner product over $GF[2]$ of the bit vector representations of j and k.

Since each copy is perfectly secure there is no problem with respect to the security. Regarding the contrast, the key property that we are interested is that for any pair of parties j_1 and j_2 in exactly a quarter of the copies both parties play the same role. Therefore if the original pixel is $C \in \{R, Y\}$, then in a quarter of the copies both opaque pixels are C, in a quarter they are $\bar{C}$ and in half one is C and the other is $\bar{C}$. The fraction of correct pixels if therefore $3/4 - 1/c$ and the resulting contrast is $1/2 - 1/c$. To summarize:

Theorem 5.2 *In every 2-out-of-n secret sharing schemes using the Cover semi-group the contrast is at most $1/2$ for any $n \geq 3$. For any $\epsilon > 0$ and there exist 2-out-of-n secret sharing schemes using the Cover semi-group with contrast at least $1/2 - \epsilon$.*

Remark: In the above scheme we used pair-wise independence between the different copies. We can obtain a similar contrast by using pair-wise small-bias probability spaces (as suggested in [2]) and this requires the number of pixels to be only $O(c \log n)$.

6 Open Problems

We have shown the inapplicability of the Cover semi-group for k-out-of-n secret sharing schemes. This leaves the possibility of secret sharing scheme over other access structures, as was considered in [1]. Note, however, that from the impossibility of 3-out-of-3 secret sharing it follows that the DNF representation of the access structure cannot contain a disjunction of three different variables.

Another problem is whether we can encrypt images composed out of more than two colours while preserving the colors more or less intact[5].

Another problem is that of visual *authentication*: can one party be convinced that the message received was indeed sent by someone who knows a common key. The test should be visual (and simple to verify by a human!).

References

[1] Giuseppe Ateniese, Carlo Blundo, Alfredo De Santis, Douglas R. Stinson, *Visual Cryptography for General Access Structures*, ECCC Report TR96-012, accepted on Feb 12, 1996 (to appear, ICALP 96).

[2] M. Naor and A. Shamir, *Visual Cryptography*, Advances in Cryptology – Eurocrypt'94 Proceeding, LNCS vol. 950, Springer-Verlag, 1995, pp. 1–12.

[5] Using the methods of this paper we can get a contrast of almost $(k-1)/2\binom{k}{2} \approx 1/k$ for k colors.