

Visual cryptography is a secret-sharing scheme that uses the human visual system to perform the computations. In this article, we will present some background on traditional secret-sharing schemes, then explain visual schemes, describing some of the basic construction techniques used.

Traditional secret sharing

Suppose a bank vault must be opened every day. Although the bank employs three senior tellers, management does not want to entrust any individual with the combination. Hence, bank management would like a vault-access system that requires any two of the three senior tellers. This problem can be solved using a two-out-of-three threshold scheme.

Invented independently in 1979 by G.R. Blakley and A. Shamir, a t -out-of- n threshold scheme shares secret K among a set n participants in such a way that:

- Any t participants can compute the value of K , and
- No group of $t-1$ (or fewer) participants can compute any information about the value of K .

The secret is chosen by a special participant, D , called the "dealer." When D wants to share the secret K among the n participants, he gives each participant some partial information called a "share." The shares should be distributed in a secure manner, so no participant knows the share given to another participant. The security of the scheme should be unconditional, not depending on any computational assumption.

At a later time, a subset of participants, say B , pool their shares in an attempt to compute the secret K . If $|B| \geq t$, then they should be able to compute the value of K from the shares they collectively hold. If $|B| < t$, then they should not be able to compute K , or any information about K .

Here is a simple way to construct a two-out-of-two threshold scheme. In this example, the secret is a binary string of length m , as are each of the two shares. Suppose $K=(k_1, \dots, k_m)$ is the secret chosen by D . D will construct the two shares as follows: The first share is chosen to be a random binary string of length m , say $s_1=(x_1, \dots, x_m)$. The second share is constructed as $s_2=(y_1, \dots, y_m)$, where $y_i=k_i-x_i \bmod 2=k_i+x_i \bmod 2$ for $1 \leq i \leq m$. Given the two shares s_1 and

s_2 , K is computed by taking the modulo 2 sum of the strings s_1 and s_2 . (This is the same as computing the Exclusive-OR of two binary vectors.) However, neither s_1 nor s_2 gives any clue to the value of K .

For example, suppose that $m=2$, $s_1=(0,1)$ and $s_2=(1,1)$. Then the secret is $K=(0+1 \bmod 2, 1+1 \bmod 2)=(1,0)$. However, looking only at s_1 , say, any of the four values of K is possible:

- if $s_2=(0,0)$, then $K=(0,1)$
- if $s_2=(0,1)$, then $K=(0,0)$
- if $s_2=(1,0)$, then $K=(1,1)$
- if $s_2=(1,1)$, then $K=(1,0)$

A similar situation applies if only the share s_2 is known.

In his 1979 paper, "How to Share a Secret," Shamir showed how to construct a t -out-of- n threshold scheme for any integers t and n such that $2 \leq t \leq n$. His solution is based on polynomial interpolation over finite fields.

In their 1987 paper, "Secret Sharing Scheme Realizing General Access Structure," Ito, Saito and Nishizeki introduced the idea of secret sharing for general access structures. An access structure consists of all the subsets of participants who are supposed to be able to reconstruct the secret. For example, suppose you have four participants—1, 2, 3 and 4. And, you want a secret that can be computed by participant 4 together with any one of the other three participants (1, 2 or 3). Ito, Saito and Nishizeki showed how to construct a secret sharing scheme for any access structure.

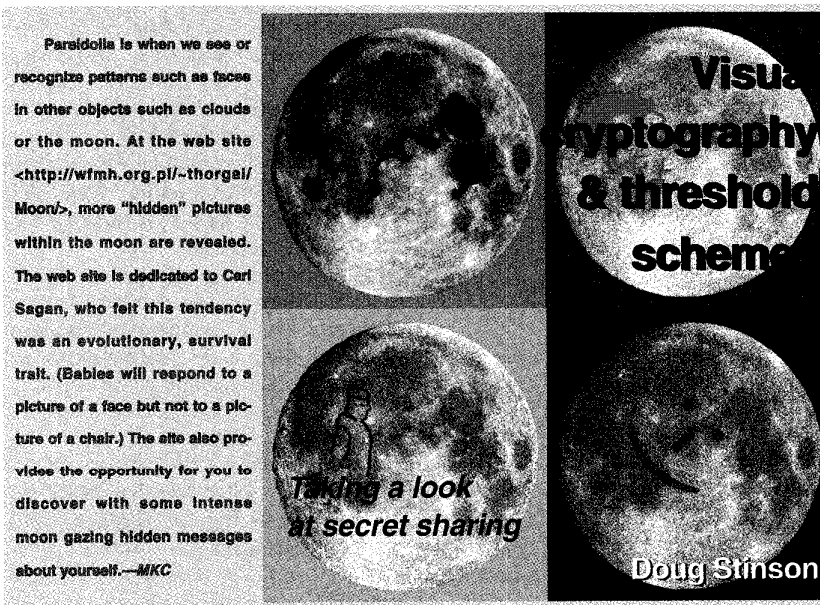
Aside from the obvious application

to access control, threshold schemes (and secret sharing schemes for general access structures) have found many applications. Various types of cryptographic protocols include: secure multiparty computations (cryptographic voting schemes, for instance), key escrow/key recovery schemes, threshold cryptography (group signature schemes, for example) and electronic cash.

A two-out-of-two visual-threshold scheme

The secret in a threshold scheme can be any type of data. For example, it might be an image I , comprised of black and white pixels. The secret image I could be encoded as a binary string $K=K(I)$, where 0 represents a white pixel and 1 represents a black pixel. Shares for K could be constructed using any convenient secret sharing scheme. K would later be reconstructed, using the appropriate algorithm for the secret sharing scheme. The resulting binary string could then be converted back into the image I . Of course, these operations would most likely be performed by a computer.

Naor and Shamir asked the following question: Is it possible to devise a secret sharing scheme in which the secret is an image I that can be reconstructed visually by superimposing a subset of the shares? Each share would consist of a transparency, made up of black and white pixels. (Actually, it would be more accurate to say "transparent" rather than "white.") In a t -out-

















pixel		s_1	s_2	s_2
	$p=5$			
	$p=5$			
	$p=5$			
	$p=5$			

Fig. 1 A two-out-of-two visual-threshold scheme

of- n scheme, there would be n transparencies, and if any t of them are superimposed, the secret image I should magically appear. However, examination of most $t-1$ shares should reveal no information about I .

The difference between a visual-threshold scheme and a traditional-threshold scheme is in how the secret is reconstructed. A traditional-threshold scheme typically involves computations in a finite field; in a visual-threshold scheme, the computation is performed by the human visual system. The security condition is the same in the two types of schemes.

At first glance, it might seem impossible to construct a visual-threshold scheme that satisfies all the necessary requirements. Suppose that a particular pixel P on a share s_i is black. Whenever a set of shares (including s_i) is superimposed, the result must be black. This means that, in the secret image I , the pixel P must be black. In other words, you have obtained some information about the secret image I by examining one of the shares. But the security condition does not allow this!

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

Example 1: Matrices that correspond to the two-out-of-two scheme in Fig. 1.

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

Example 2: A two-out-of-three scheme with pixel expansion $m=3$

Naor and Shamir found an elegant way around this impasse. They constructed a two-out-of-two visual-threshold scheme. Figure 1 illustrates the scheme by specifying the algorithm for encoding one pixel. (This algorithm is to be applied for every pixel P in the image I to construct the two shares.) A pixel P is split into two subpixels in each of the two shares.

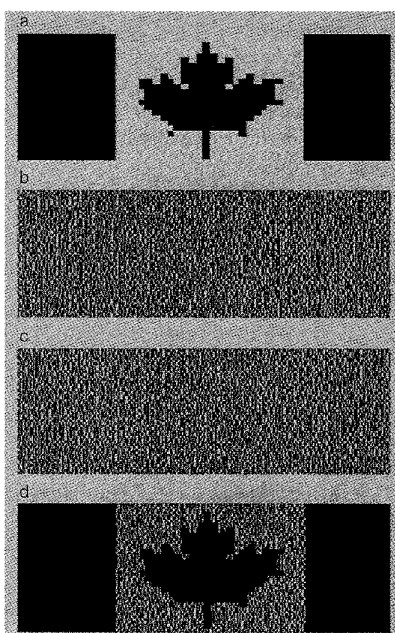


Fig. 2 The original image, two shares, and the reconstructed image: a) original image; b) share s_1 ; c) share s_2 ; d) s_1+s_2

If the given pixel P is white, then D flips a coin and randomly chooses one of the first two rows of Fig. 1. If the given pixel P is black, then D flips a coin and randomly chooses one of the last two rows of Fig. 1. Then the pixel P is encrypted as two subpixels in each of the two shares, as determined by the chosen row in Fig. 1.

Let's convince ourselves that the scheme works as desired. First, consider the security condition. Suppose you turn your attention to a pixel P in the share s_1 . One of the two subpixels in P is black and the other is white. Moreover, each of the two possibilities—black-white and white-black—is equally likely to occur. This is independent of whether the corresponding pixel in the secret image I is black or white. Thus, the share s_1 gives no clue as to whether the pixel is black or white.

The same argument applies to the share s_2 . Since all the pixels in I were encrypted using independent random coin flips, there is no information to be gained by looking at any group of pixels on a share, either. This demonstrates the security of the scheme.

Now consider what happens when you superimpose the two shares (see the last column of Fig. 1). Consider one pixel P in the image I . If P is black, then you get two black subpixels when you superimpose the two shares. If P is

white, then you get one black subpixel and one white subpixel when you superimpose the two shares. Thus, the reconstructed pixel (consisting of two subpixels) has a gray level of one if P is black, and a gray level of one-half if P is white. There will be a 50 percent loss of contrast in the reconstructed image, although it should still be visible.

Figure 2 is a Canadian flag encrypted into two shares, then reconstructed using this method. The method works quite well, despite the 50 percent loss of contrast in the reconstructed image. More complicated images may be difficult to recognize when the two shares are superimposed. This is due partly to the 50 percent loss of contrast, and partly to two nonmathematical reasons: Transparencies are floppy, hard to align precisely and move around easily. Also, when the transparencies are created, either by photocopying an image or using a laser printer, the heat produced in the printing process actually distorts the plastic in the transparencies. This makes them even more difficult to align correctly.

In general, it is best to use simple images that are made up of a relatively small number of pixels, each of which is relatively large. (The images in Fig. 2 were reduced to fit on this page.) Experimentation is the best way to get a feel for which images are suitable for using this algorithm.

Two-out-of- n visual-threshold schemes

Since it is hard enough to align two shares correctly, we will not discuss the general problem of constructing t -out-of- n visual-threshold schemes. Discussion will be restricted to the case $t=2$, an approach to use for constructing two-out-of- n schemes, and the practical limitations of these schemes.

Each pixel P in a secret image I will be encrypted as some number, m , of subpixels in each of the n shares. The number m is called the pixel expansion of the scheme; in the two-out-of-two scheme, you have $m=2$.

For convenience, a black pixel or subpixel is represented by "1," and a white pixel or subpixel by "0." Then the encryption of a pixel into m subpixels can be represented by a binary m -tuple. We will use two $n \times m$ binary matrices, named M_0 and M_1 , to describe the scheme. Given a pixel P , $P=0$ or 1 , the matrix M_P is used to determine the encryption of P on each of the n shares by applying the algorithm

Input:	$P = 0 \text{ or } 1$
1.	Choose a random permutation σ of $\{1, \dots, m\}$.
2.	Construct N_P by permuting the columns of M_P using the permutation σ .
3.	For $1 \leq i \leq n$, take row i of N_P to be m subpixels of P on the share s_i .

Fig. 3 The Encrypt_Pixel algorithm

Encrypt_Pixel in Fig. 3.

Observe that the two-out-of-two scheme in Fig. 1 corresponds to the matrices M_0 and M_1 presented in Example 1. M_0 and M_1 for a two-out-of-three scheme with pixel expansion $m=3$ are in Example 2, while Example 3 presents a two-out-of-four scheme with pixel expansion $m=6$.

Let's now turn to the encryption procedure, using the two-out-of-three scheme. In general, there are $m!$ permutations of $\{1, \dots, m\}$. In the case $m=3$, there are six permutations of $\{1, 2, 3\}$; see Example 4.

You can choose a random permutation of $\{1, 2, 3\}$ by rolling a regular six-sided die. Suppose that you want to encrypt the pixel $P=1$, and you roll a "4." Then $\sigma = \sigma_4 = (2, 3, 1)$. You proceed to construct N_1 by taking column two of M_1 , then column three, and then column one (see Example 5a). Thus, the pixel P will be encoded (as in Example 5b).

For this approach to yield a scheme that satisfies the security condition and that yields a visible image when two shares are superimposed, M_0 and M_1 must satisfy two conditions. First, to define some notation, let $wt(x)$ denote the number of 1s in a binary vector. For two binary vectors x and y , define $x \text{ OR } y$ to be the binary vector obtained by taking the binary "or" of the vectors x and y . (Recall that $0 \text{ OR } 0 = 0$, $0 \text{ OR } 1 = 1$, $1 \text{ OR } 0 = 1$ and $1 \text{ OR } 1 = 1$.)

Let $1 \leq w \leq m$ be an integer. M_0 will be the $n \times m$ matrix in which every row consists of w 1s followed by $m-w$ 0s. Now, suppose that γ is a real number such that $0 < \gamma < 1$, and suppose that M_1 satisfies the two conditions in Example 6. If these two properties are satisfied, then we will say that the pair of matrices M_0 and M_1 comprise a two-out-of- n visual-threshold scheme with pixel expansion m and relative contrast γ .

To understand what is going on here, you have to

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

Example 3: A two-out-of-four scheme with pixel expansion $m=6$

$$\sigma_1 = (1, 2, 3) \quad \sigma_2 = (1, 3, 2) \quad \sigma_3 = (2, 1, 3) \\ \sigma_4 = (2, 3, 1) \quad \sigma_5 = (3, 1, 2) \quad \sigma_6 = (3, 2, 1)$$

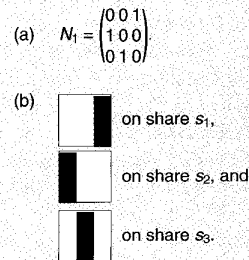
Example 4: Six permutations of $\{1, 2, 3\}$

examine the security and contrast provided by the scheme. First, look at a pixel P in a share s_i . P was obtained by means of a random permutation of a row of M_0 or M_1 . But all rows of M_0 and M_1 have the same weight, w . When you begin with any vector x of weight w , and apply a random permutation to the coordinates of x , the result is a random binary vector of weight w . (For instance, any vector of weight w is equally likely to be produced as a result of this process.) Hence, any pixel in any share consists of a random combination of w black subpixels and $m-w$ white subpixels. Again, this is independent of whether the pixel in the secret image was black or white. Thus, the security condition is achieved.

Now consider what happens when you superimpose a pixel from two shares, say pixel P_i from share s_i and the corresponding pixel P_j from share s_j . Let P denote the corresponding pixel in the secret image I . When you superimpose P_i and P_j , the number of black subpixels (out of the m subpixels) in the result is given by $wt(P_i \text{ OR } P_j)$.

Recall that P_i and P_j were obtained by applying the same permutation to rows i and j of M_P . Hence, you have $wt(P_i \text{ OR } P_j) = wt(M_P[i] \text{ OR } M_P[j])$ for all $1 \leq i < j \leq n$. Hence, if $P=0$, then $wt(P_i \text{ OR } P_j) = w$, whereas if $P=1$, then $wt(P_i \text{ OR } P_j) \geq w + \gamma m$.

A reconstructed white pixel is w/m black and a reconstructed black pixel is (at least) $(w + \gamma m)/m$ black. The difference between black and white reconstructed pixels is (at least) γm of the m subpixels. The fraction γ is therefore a measure of the relative



Example 5: a) Constructing N_1 by taking column two of M_1 , then column three, and then column one; b) the encoded pixel P

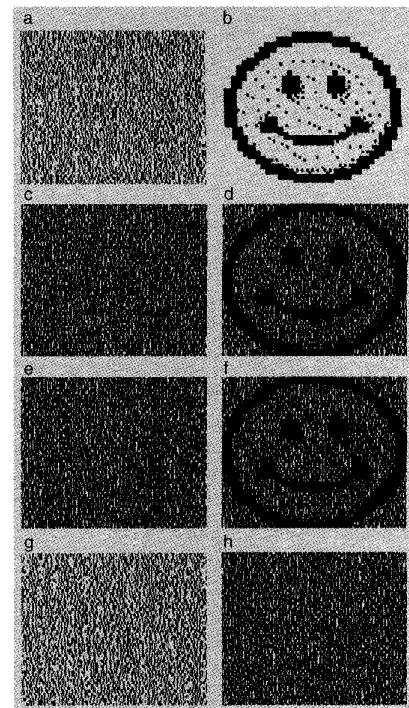


Fig. 4 The original, four shares and some reconstructed images: a) share s_1 ; b) original image; c) share s_2 ; d) s_1+s_2 ; e) s_3 ; f) s_3+s_4 ; g) share s_4 ; h) s_1+s_3

contrast.

In the two-out-of-two scheme, you have $m=2$, $w=2$ and $\gamma=1/2$. This agrees with the earlier statement that there was a 50 percent loss of contrast. In the two-out-of-three scheme, you have $m=3$, $w=3$ and $\gamma=1/3$; and in the two-out-of-four scheme, you have $m=6$, $w=3$ and $\gamma=1/3$. Observe that the two-out-of-four scheme achieves the same relative contrast as the two-out-of-three scheme, but it requires a larger pixel expansion to do so.

At this point, you might wonder about the quality of the schemes we have presented. A bound on the relative contrast helps answer this question. Blundo, De Santis and Stinson showed that in any two-out-of- n visual-threshold scheme, it holds that $\gamma \leq \gamma^*(n)$, where

$$\gamma^*(n) = \frac{\lfloor n/2 \rfloor \lceil n/2 \rceil}{n(n-1)}$$

A similar result was shown by Hofmeister, Krause and Simon.

It is not hard to compute that $\gamma^*=1/2$ and $\gamma^*(3)=\gamma^*(4)=1/3$. Thus, the three schemes presented all achieve optimal contrast.

If you examine the behavior of the function $\gamma^*(n)$, you see that $\gamma^*(n) > 1/4$ for all $n \geq 2$, and $\lim_{n \rightarrow \infty} \gamma^*(n) = 1/4$. This raises the question of whether schemes

security	$\text{wt}(M_i[j]) = w$ for $1 \leq j \leq n$, where $M_i[j]$ denotes the i th row of M ($1 \leq i \leq n$)
contrast	$\text{wt}(M_i[j] \text{ OR } M_j[i]) \geq w + \gamma n$ for $1 \leq i < j \leq n$

Example 6: If these two properties are satisfied, then the matrices M_0 and M_1 comprise a two-out-of- n visual-threshold scheme.

can be constructed for all $n \geq 2$ that achieve relative contrast $\gamma^*(n)$. This is, in fact, possible, as is shown by Blundo, De Santis and Stinson. Since the relative contrast of these schemes is always at least $1/4$, the loss of contrast is at most 75 percent. Thus, the reconstructed images should be visible, at least for relatively simple images.

There are various ways to construct optimal contrast schemes. However, in addition to wanting the contrast to be as high as possible, you also want the pixel expansion, m , to be as small as possible. This is due to practical considerations of implementing the schemes: If m is too big, then the subpixels become very small and the transparencies will be difficult to align.

Constructions for optimal contrast/minimum pixel expansion schemes are given by Blundo, De Santis and Stinson, and by Hofmeister, Krause and Simon, respectively. They depend on the existence of certain combinatorial designs derived from Hadamard matrices. Hadamard matrices have been extensively studied for many engineering applications, such as signal processing. There is a large body of knowledge on Hadamard matrices, which you can apply to the construction of visual-threshold schemes.

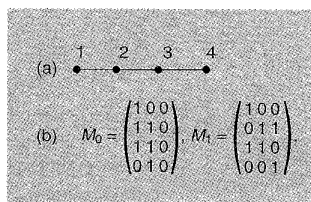
Here is one example of a particularly simple construction that can be derived by this approach. Suppose that $n \equiv 3 \pmod 4$ is prime. Here is how to construct a two-out-of- n visual-threshold scheme having optimal relative contrast $\gamma^*(n)$ and optimal pixel expansion $m=n$. Define

$$Q(n) = \{i^2 \pmod n : 1 \leq i \leq (n-1)/2\}.$$

$Q(n)$ is called the set of *quadratic residues* modulo n . You will construct an $n \times n$ matrix M_1 , labeling the rows and columns by the elements of Z_n , namely,

0	1	0	1	1	1	0	0	0	1	0
0	0	1	0	1	1	1	0	0	0	1
1	0	0	1	0	1	1	1	0	0	0
0	1	0	0	1	0	1	1	1	0	0
0	0	1	0	0	1	0	1	1	1	0
0	0	0	1	0	0	1	0	1	1	1
1	0	0	0	1	0	0	1	0	1	1
1	1	0	0	0	1	0	0	1	0	1
1	1	1	0	0	0	1	0	0	1	0
0	1	1	1	0	0	0	1	0	0	1
1	0	1	1	1	0	0	0	1	0	0

Example 7: Matrix M_1



Example 8: a) Graph on four vertices; b) matrices M_0 and M_1 presented by Ateniese, Blundo, De Santis and Stinson.

$0, \dots, n-1$. The entry in row i and column j of M_1 is defined to be 1 if $j-i$

mod $n \in Q(n)$, and 0 otherwise.

For example, let $n=11$. You compute $1^2=1 \equiv 1 \pmod{11}$, $2^2=4 \equiv 4 \pmod{11}$,

$3^2=9 \equiv 9 \pmod{11}$, $4^2=16 \equiv 5 \pmod{11}$, and

$5^2=25 \equiv 3 \pmod{11}$.

Hence, $Q(11) = \{1, 3, 4, 5, 9\}$. Then the matrix M_1 is as shown in Example 7.

You can verify that every row of M_1 has weight five and the “or” of any two distinct rows has weight eight. Thus, you have constructed a two-out-of-11 scheme with $m=11$, $w=5$ and $\gamma=\gamma^*(11)=3/11$. In general, if $n \equiv 3 \pmod 4$ is prime, then this construction will yield a two-out-of- n scheme with $m=n$, $w=(n-1)/2$ and $\gamma=\gamma^*(n)=(n+1)/4n$.

Visual cryptography for graph-access structures

In a two-out-of- n scheme, the secret is reconstructed by superimposing any two transparencies. Earlier the idea of secret sharing for general-access structures was mentioned. This idea can be pursued for visual-secret sharing schemes, as well. Since you want to avoid having to stack more than two transparencies at a time, let’s consider access structures defined by a graph.

Suppose G is a graph defined on n vertices. Thus G consists of n vertices, some of which are joined by edges. You are interested in constructing a scheme where the superposition of shares s_i and s_j reveals the secret image if and only if ij is an edge of G . The graph is just a convenient way of recording which pairs of shares are supposed to reveal the secret.

As an example, consider the graph on four vertices presented in Example 8a. Here, you want to find a scheme in which the secret is revealed by superimposing shares s_1 and s_2 ; s_2 and s_3 ; or s_3 and s_4 . However, no information about the secret should be obtainable from shares s_1 and s_3 ; s_1 and s_4 ; or s_2 and s_4 . The matrices M_0 and M_1 for such a scheme were presented by Ateniese, Blundo, De Santis and Stinson (see Example 8b).

In this scheme, we have pixel expansion $m=3$ and contrast $\gamma=1/3$. Observe that, unlike the threshold schemes we constructed earlier, not all rows of M_0 and M_1 have the same weight: Rows one and four have weight one, and rows two and three have weight two. This means that shares s_2 and s_3 will be darker than shares s_1 and s_4 . Figure 4 presents an example of shares and reconstructed images using this scheme.

Read more about it

* Ateniese, G., Blundo, C., De Santis, A. and Stinson, D.R., “Visual Cryptography for General Access Structures,” *Information and Computation* 129, pp. 86-106, 1996.

* Blundo, C., De Santis, A. and Stinson, D.R., “On the Contrast in Visual Cryptography schemes,” *Theory of Cryptography Library*, report 96-13, <ftp://theory.lcs.mit.edu/pub/tryptol/96-13.ps>.

* Droste, S., “New Results on Visual Cryptography,” *Advances in Cryptology: CRYPTO ‘96*, N. Kobitz, ed., Lecture Notes in Computer Science 1109, pp. 401-415, 1996.

* Hofmeister, T., Krause, M. and Simon, H.U., “Contrast-Optimal k out of n Secret Sharing Schemes in Visual Cryptography,” *COCOON ‘97*, T. Jiang and D.T. Lee, eds., Lecture Notes in Computer Science 1276, 1997.

* Naor, M. and Pinkas, B., “Visual Authentication and Identification,” *Advances in Cryptology: CRYPTO ‘97*, B. Kaliski, Jr., ed., Lecture Notes in Computer Science 1294, pp. 322-336, 1997.

* Naor, M. and Shamir, A., “Visual Cryptography II: Improving the Contrast via the Cover Base,” *Theory of Cryptography Library*, report 96-07, <ftp://theory.lcs.mit.edu/pub/tryptol/96-07.ps>.

* Stinson, D.R., *Cryptography Theory and Practice*, CRC Press Inc., 1995.

* Verheul, E.R. and van Tilborg, H.C.A., “Constructions and Properties of k out of n Visual Secret Sharing Schemes,” *Designs, Codes and Cryptography* 11, pp.179-196, 1997.

About the author

Dr. Doug Stinson is a Professor of computer science at the University of Nebraska, Lincoln, and author of *Cryptography Theory and Practice* (CRC Press, 1995). He can be contacted by e-mail at <stinson@bibd.unl.edu>.

Reprinted courtesy of Dr. Dobb’s Journal (<http://www.ddj.com>) © 1998.