International Journal of Information and Computation Technology.
ISSN 0974-2239 Volume 3, Number 5 (2013), pp. 459-464

http://www. irphouse.com /ijict.htm

Visual Cryptography for Black and White Images

Maneesh Kumar[1] and Sourav Mukhopadhyay[2]

Department of Mathematics
[1]Delhi University, [2]IIT Kharagpur

Abstract

A visual cryptography scheme is a method to encode a secret image SI into shadowimages called shares such that, certain qualified subsets of shares enable the “visual"recovery of the secret image. The “visual" recovery consists of xeroxing the shares ontotransparencies, and then stacking them. The shares of a qualified set will reveal the secretimage without any cryptographic computation. Here, we analyze the construction of k outof n visual cryptography schemes for black and white images(In such a scheme any kshares out of n will reveal the secret image, but any k -1 shares give no information aboutthe image).The important parameters of a scheme are its contrast, i.e., the clarity of thedecoded image, and the number of pixels needed to encode one pixel of the originalimage. We discuss some methods of construction of (2, n)-schemes having optimalrelative contrast using Hadamard matrices and some combinatorial block designs. Westudy the construction of an efficient (3, n)-scheme. We also study the construction of (3,n)-schemes using 3 designs and (t, n)-schemes using t-designs.Some constructions for the general (k, k) and (k, n) schemes are also discussed.

Keywords: Hadamard Matrices, BIBDs, PBD.

1. Introduction

A secret sharing scheme permits a secret to be shared among a set P of n participants insuch a way that only qualified subsets of P can recover the secret, and any non-qualified subset has absolutely no information on the secret. In other words, a nonqualified subsetknows only that the secret is chosen from a prespecified set (which we assume is publicknowledge), and they cannot compute any further information regarding the value of thesecret.In 1979, Shamir [6] and Blakley [1] introduced the concept of a *threshold scheme*A. (k, n) threshold scheme is a method whereby n pieces of information of the secret key$K$, called *shares* are distributed to n participants so that the secret key cannot bereconstructed from the knowledge of fewer than k shares.In 1994, Naor and Shamir (1995) proposed a new type of cryptographic scheme,which can decode secret images without any cryptographic computations. The basicmodel consists of a printed page of cipher text (which can be sent by mail or faxed) and aprinted transparency (which serves as a secret key). Each one of them isindistinguishable, but placing the transparency with the key over the page with the ciphertext can reveal the original text. The remarkable feature of this scheme is that the secretcan be decoded directly by the human visual system; hence it can be called visualcryptography scheme. This basic model can be extended into the k out of n secret sharingproblem; that is, given a secret message, one can generate n transparencies (so-calledshares), and the original message is visible if at least k of them are stacked together buttotally invisible or unanalyzable if fewer than k transparencies are stacked together.A VCS is mainly applied to a binary image containing a collection of black andwhite pixels, each of which is handled separately. Each pixel of the binary image isencoded into m black and white sub pixels, which are printed in close proximity to eachother so that the human visual system averages their individual black/white contributions.Figure1.1 is an illustration of (2, 2)-threshold VCS. The encryption rules specify that apixel is encoded into two sub pixels composing of one black and one white on each share.

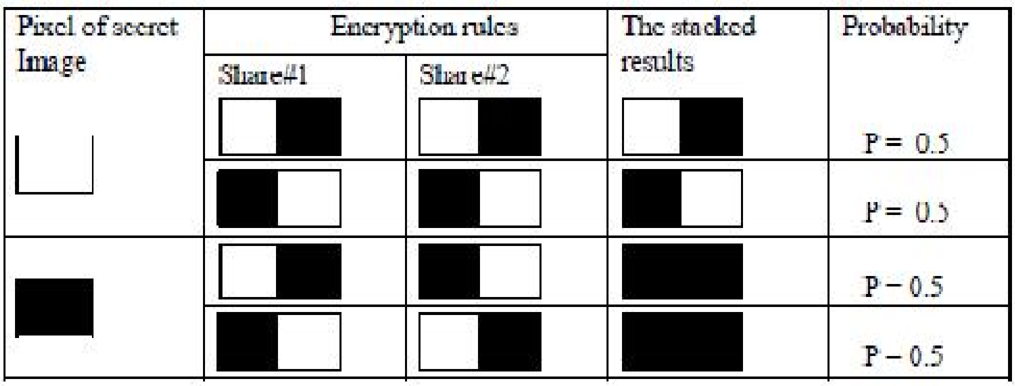

Figure 1.1: An (2, 2)-threshold VCS.

2. (2, N) - Threshold VCS

In this chapter, we consider only (2, n)-threshold VCSs for black and white images. In[2], Naor and Shamir first proposed a (2, n)-threshold VCS for black and white images.They constructed the 2 out of n visual secret sharing scheme by considering the two $n \times n$basis matrices S_0 and S_1 given as follows.

$$S^0 = \begin{bmatrix} 1 & 0 & 0 & . & . & 0 \\ 1 & 0 & 0 & . & . & 0 \\ . & . & . & & & . \\ . & . & . & . & & . \\ . & . & . & . & . & . \\ 1 & 0 & 0 & . & . & 0 \end{bmatrix} \qquad S^1 = \begin{bmatrix} 1 & 0 & 0 & . & . & 0 \\ 1 & 0 & 0 & . & . & 0 \\ . & . & . & & & . \\ . & . & . & . & & . \\ . & . & . & & . & . \\ 1 & 0 & 0 & . & . & 0 \end{bmatrix}$$

S_0 is a Boolean matrix whose first column comprises of 1's and whose remaining entriesare 0' s. S_1 is simply the identity matrix of dimension n.When we encrypt a white pixel, we apply a random permutation to the columns ofS_0 to obtain matrix T. We then distribute row i of T to participant i. To encrypt a blackpixel, we apply permutation to S_1. A single share of a black or white pixel consists of arandomly placed black sub pixel and n -1 white sub pixels. Two shares of a white pixelhave a combined Hamming weight of 1, whereas any two of a black pixel have a combined Hamming weight of 2, which looks darker. The visual difference between thetwo cases becomes clearer as we stack additional transparencies.

3. An Example Implementation of a (2, 2)-Threshold VCS

The basis matrices used here are

$$S^0 = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix} \quad \text{And} \quad S^1 = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}$$

IITKGP

Figure 3.1: Original image.

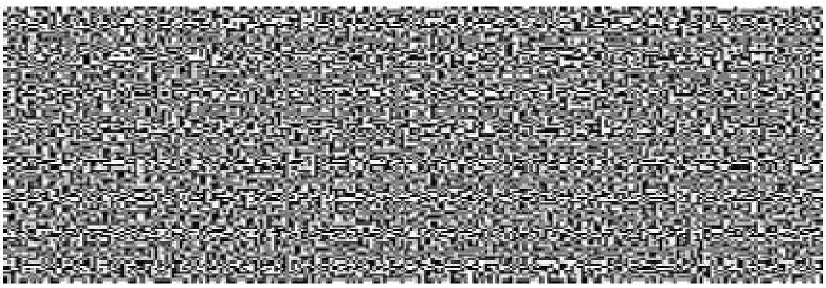

Figure 3.2: Share 1.

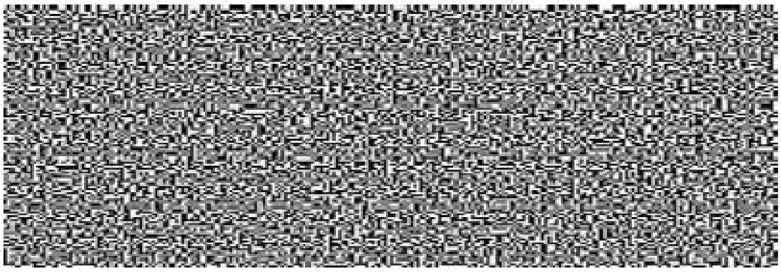

Figure 3.3: Share 2

Figure 3.4: Superimposition of Share 1 and Share 2.

4. A Construction of (3, *N*)-Threshold VCS

The following scheme gives a 3 out of n scheme for an arbitrary $n \geq 3$. Let B be a black $n\times (n- 2)$ matrix which contains only 1' s, and let I be the $n \times n$ identity matrix whichcontains 1's on the diagonal and 0's,elsewhere. Then S_1 is the $n \times (2n- 2)$ matrix obtainedby concatenating B and I. And S_0 is the complement of the matrix S_1.

5. Construction OF (*K*, *K*)-threshold VCS

In [2], a k out of k visual cryptography scheme with pixel expansion 2^{k-1} is described.Theauthors proved that the construction is optimal in that any k out of k scheme must useat least 2^{k-1} pixels.The basis matrices are constructed as follows. S_1 is the $k \times 2^{k-1}$ matrix whosecolumns are all boolean n-vectors having an odd number of `1's, and $S_0$ is the $k \times 2^{k-1}$matrix whose columns are all boolean $n$-vectors having an even number of `1's.

6. Construction of (*K*, *N*)-threshold VCS When *K* Divides *N*

In this section, we describe a construction for (k, n)-threshold VCS which is given in [5],for the case when $k | n$. The result is generalized in the next section to any k and n, $n \geq k$.They make use of an initial matrix which is defined below.

Let n, l, k be integers such that k ▪ n. An initial matrix *IM* (*n, l, k*) *in an n*× *lmatrix whose entries are elements of a ground set A* = *{a*1, *a*2……. *ak }, in which the setof columns is equal to the set of vectors in which each element of A appearsk/ntimes.*

7. Construction of (*K, N*) VCS for any Value of *K* and *N*

In the previous section we had seen a construction for a (*k, n*)-threshold VCS when *k* ln.To realize a (k, n)-threshold VCS for any values of the parameters k and n we canconstruct, using the previous technique, a (k ,n0)-threshold VCS, where n0 ≥n is amultiple of k, and then consider only the first n rows of the basis matrices of this scheme.The scheme obtained in this way is a (k, n)-threshold VCS having the same parameters asthe (k, n0)-threshold VCS. The following theorem states the existence of a (k, n)-thresholdVCS for any value of k and n.

8. Conclusion

Visual Cryptography can be used to share a secret message among *k* participants, suchthat any *k* -1 participants can get no information about the secret message. In suchschemes, only *k* or more shares can reveal the secret.We presented the model of (*k, n*)-threshold Visual Cryptography Scheme. Westudied techniques to construct (2, *n*)-threshold VCS using Hadamard matrices and combinatorial structures such as BIBDs, PBDs. The techniques described give thresholdvisual cryptography schemes which are optimal with respect to relative contrast. Anefficient (3, *n*)-threshold VCS was discussed. A new construction of (3, *n*)-threshold VCSusing 3-design and (*t, n*)-threshold VCS using *t*-design was also discussed. Someconstructions for general (*k, k*) and (*k, n*) schemes were studied.We implemented the schemes and it was observed 3-designs gives better relativecontrast and also observed that (*k, n*) secret sharing schemes are efficient for smallervalues of *k*. This is because, for large *k*, pixel expansion becomes too large and also the contrast of the reconstructed image is poor.For future, two Multi-pixel Encoding Methods based on the visual cryptographyscheme can be proposed. The main purpose of the proposed method is to solve theproblem of pixel expansion and generate smooth-looking decoded images. For each time,we simultaneously encode *m* pixels, called an encryption sequence, on the secret imageinto *m* pixels on the share. Hence the size of the decoded image is the same as that of the secret image.Thus the proposed method holds immense potential in becoming a better sharing technique in visual cryptography scheme by efficiently using the memory space during decoding process.

References

[1] Blakley G. R, Safeguarding cryptographic keys, *AFIPS 1979, National ComputerConference*, Vol. 48, 313-317, 1979.

[2] Naor M. and Shamir A., Visual cryptography, Eurocrypt' (1994) Lecture Notes inComputer Science, Vol. 950, Springer-Verlag, pp. 1- 12.

[3] Hofmeister T., Krause M., and Simon H. (2000), Contrast optimal k out of n secretsharing schemes in visual cryptography, Theoretical Computer Science, Vol. 240, pp.471- 485.

[4] Bose, R. C. and Manvel, B. (1984), Introduction to Combinatorial Theory. New York:Wiley.

[5] Blundo C., De Santis A. and Stinson D. R. (1999), On the contrast in visualcryptography Schemes, Journal of Cryptology, Vol. 12, No. 4, 261- 289.

[6] Shamir A. (1979), How to share a secret, Communication of the ACM, Vol. 22, No.11, pp. 612- 613.

[7] Ateniese, G., Blundo, C., De Santis, A., and Stinson, D. R. (1996b), “Visualcryptography for general access structures,” Information and Computation, Vol. 129No.2, pp. 86-106.