A (2, n) and (3, n) Visual Cryptography Scheme for Black and White Images

Maneesh Kumar[1], Rahul Singh[2]

[1, 2] Department of Mathematics, University of Delhi, Delhi, India

Abstract: ***A visual cryptography scheme (VCS) is a method to encode a secret image into shadow images 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 onto transparencies, and then stacking them. The shares of a qualified set will reveal the secret image without any cryptographic computation. Here, we analyze the construction of k out of n visual cryptography schemes for black and white images(In such a scheme any k shares out of n will reveal the secret image, but any k -1 shares give no information about the image). The important parameters of a scheme are its contrast, i.e., the clarity of the decoded image, and the number of pixels needed to encode one pixel of the original image. Some methods of construction of (2, n)-schemes having optimal relative contrast using Hadamard matrices and some combinatorial block designs have been discussed. We study the construction of an efficient (3, n)-scheme. We also study the construction of (3,n)-schemes using a design.***

Keywords: Visual Cryptographic schemes, (2, n) schemes, (3, n) schemes

1. Introduction

A secret sharing scheme permits a secret to be shared among a set P of n participants in such 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 subset knows only that the secret is chosen from a pre-specified set (which we assume is public knowledge), and they cannot compute any further information regarding the value of the secret. 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 be reconstructed from the knowledge of fewer than *k* shares. In 1994, Naor [2] and Shamir (1995) proposed a new type of cryptographic scheme, which can decode secret images without any cryptographic computations. The basic model consists of a printed page of cipher text (which can be sent by mail or faxed) and a printed transparency (which serves as a secret key). The remarkable feature of this scheme is that the secret can be decoded directly by the human visual system; hence it can be called visual cryptography scheme. This basic model can be extended into the *k* out of *n* secret sharing problem; that is, given a secret message, one can generate *n* transparencies (so-called shares), and the original message is visible if at least *k* of them are stacked together but totally invisible or cannot be analyzed if fewer than *k* transparencies are stacked together. Various other literatures pertaining to this field are studied [3], [4], [5]. A VCS (visual cryptography scheme) is mainly applied to a binary image containing a collection of black and white pixels, each of which is handled separately. Each pixel of the binary image is encoded into *m* black and white sub pixels, which are printed in close proximity to each other so that the human visual system averages their individual black/white contributions. Figure 1 is an illustration of (2, 2)-threshold VCS. The encryption rules specify that a pixel is encoded into two sub pixels composing of one black and one white on each share.

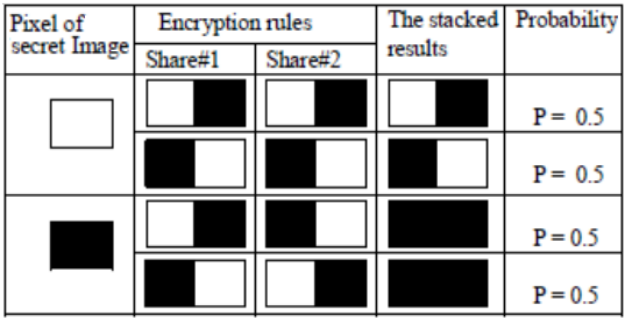


Figure 1: An (2, 2) – threshold VCS

2. Division of the Pixel

In this section, we shall review the basic visual cryptography scheme proposed by Naor and Shamir. Here a secret black and white image is divided into two grey images. In order to share a secret black and white image, the concept of their scheme is to transform one pixel into two sub-pixels and divide each sub-pixel two color regions. The sub-pixels are half white and half black.



Figure 2: Different types of pixels along with the representation

Where
(a) White pixel (b) Black pixel
(c) LB pixel (d) RB pixel

For example, Figure 2 represents four different types of pixels. The first is a white pixel, the next is a black pixel, and the last two are grey pixels. Note that in the grey pixels, the black and white portions are different. Let us call these pixels as LB and RB pixels respectively. We represent a white pixel by 00, black by 11, LB-pixel by 10 and RB-pixel by 01. They can be thought of as modified version of pixels to be used in shares.

3. Superposition of pixels

If we stack two LB pixels (or two RB pixels) we get nothing new, whereas, if we stack an LB pixel and an RB pixel, we get a black pixel. This can be shown as in Figure 1. We can see that by the representation used for pixels, the superposition of two pixels can be thought of as if a binary "OR" operation.

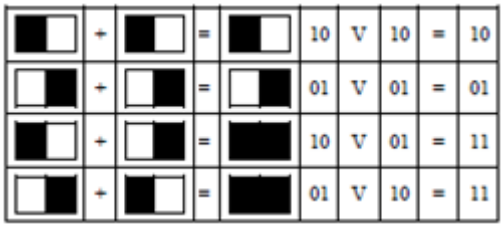


Figure 3: Superposition of two pixels

Naor and Shamir devised the following scheme, illustrated in Figure 1. The algorithm specifies how to encode a single pixel, and it would be applied for every pixel in the image to be shared. A pixel *P* is replaced by two pixels (called sub pixels) in each of the two shares. If *P* is white, then a coin toss is used to randomly choose one of the first two rows in the Figure 1. If *P* is black, then a coin toss is used to randomly choose one of the last two rows in the Figure 1. Then the pixel *P* is encrypted as two sub pixels in each of the two shares, as determined by the chosen row in the figure. Every pixel is encrypted using a new coin toss. Suppose we look at a pixel P in the first share. One of the two sub-pixels 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, independent of whether the corresponding pixel in the secret image is black or white. Thus the first share gives no clue as to whether the pixel is black or white. The same argument applies to the second share. Since all the pixels in the secret image 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.

4. (2, n) – Threshold VCS

In this section, 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* x *n* basis matrices *S*0 and *S*1 given as follows.

$$S^0=\begin{bmatrix}1&0&0&\cdots&0\\1&0&0&\cdots&0\\\vdots&\vdots&\vdots&&\vdots\\1&0&0&\cdots&0\end{bmatrix}\quad S^1=\begin{bmatrix}1&0&0&\cdots&0\\1&0&0&\cdots&0\\\vdots&\vdots&\vdots&&\vdots\\1&0&0&\cdots&0\end{bmatrix}$$

*S*0 is a Boolean matrix whose first column comprises of 1's and whose remaining entries are 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 of *S*0 to obtain matrix *T*. We then distribute row *i* of *T* to participant *i*. To encrypt a black pixel, we apply permutation to *S*1. A single share of a black or white pixel consists of a randomly placed black sub pixel and *n* -1 white sub pixels. Two shares of a white pixel have 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 the two cases becomes clearer as we stack additional transparencies.

We take the example of a (2, 4)-threshold VCS. The basis matrices in this case are given by:

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

If one examines just a single share then it is impossible to determine whether it represents a share of a black or a white pixel since single shares, whether black or white, looks alike. If two shares of black pixel are superimposed together, we obtain two black and two white sub pixels. Combining the shares of a white pixel yields only one black and three white sub pixels. Therefore, on stacking two shares, a black pixel will look darker than a white pixel.

5. An example implementation of a (2, 2) - Threshold VCS

The basis matrices used here are

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

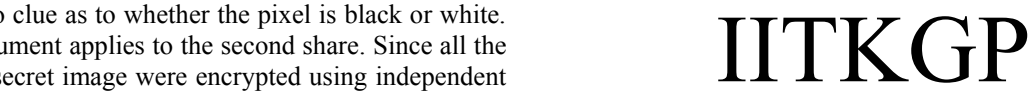


Figure 4: Original image

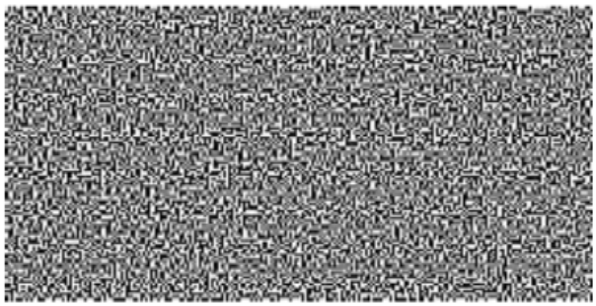


Figure 5: Share 1

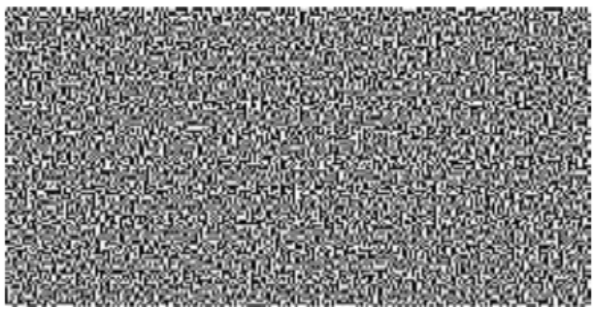


Figure 6: Share 2



Figure 7: Superimposition of Share 1 and Share 2

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

The following scheme gives a 3 out of *n* scheme for an arbitrary $n \geq 3$. If *B* be a black *n* x (*n*- 2) matrix which contains only 1' s, and if *I* be the *n* x *n* identity matrix which contains 1's on the diagonal and 0's,elsewhere, then *S*1 is the *n* x (2*n*- 2) matrix obtained by concatenating *B* and *I*. And *S*0 is the complement of the matrix *S*1. For the (3, 5)-VCS, the basis matrices are given by

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

Any single share contains an arbitrary collection of n- 1 black and n- 1 white subpixels; any pair of shares have n- 2 common black and two individual black sub pixels. But, superimposition of any three shares from S0 gives n black sub pixels, whereas any three from S1 gives n +1 black sub pixels. Note that, in this (3, n) scheme, pixel expansion is (2n - 2) and relative contrast is equal to 1 / (2n - 2).

7. An Example Implementation of (3, 3)-threshold VCS

Here we use basis matrices constructed by the method given in the previous section.

CSDP

Figure 8: Original image



Figure 9: Share 1



Figure 10: Share 2



Figure 11: Share 3



Figure 12: Superimposition of Shares 1, 2 and 3

8. Conclusions

Visual Cryptography can be used to share a secret message among *k* participants, such that any *k* -1 participants can get no information about the secret message. In such schemes, only *k* or more shares can reveal the secret. We presented the model of (2, *n*)-threshold Visual Cryptography Scheme using Hadamard matrices. The techniques described give threshold visual cryptography schemes which are optimal with respect to relative contrast. An efficient (3, *n*)-threshold VCS was discussed. For future, two Multi-pixel Encoding Methods based on the visual cryptography scheme can be proposed. The main purpose of the proposed method is to solve the problem of pixel expansion and generate smooth-looking decoded images. 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 Computer Conference*, Vol. 48, 313-317, 1979.
[2] Naor M. and Shamir A., Visual cryptography, Eurocrypt' (1994) Lecture Notes in Computer Science, Vol. 950, Springer-Verlag, pp. 1- 12.
[3] Hofmeister T., Krause M., and Simon H. (2000), Contrast optimal k out of n secret sharing 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 visual cryptography 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.

Authors Profile

Maneesh Kumar received his M. Tech Degree in Computer Science and Data Processing (CSDP), Department of Mathematics, Indian Institute of Technology, Kharagpur in 2012. He is currently working in the Department of Mathematics, University of Delhi. His research interests include techniques in visual cryptography schemes.

Rahul Singh received his M. Tech Degree in Computer Applications, Department of Mathematics, Indian Institute of Technology, Delhi in 2011. He is currently working in the Department of Mathematics, University of Delhi. His research interests include braid group cryptography.