Information security has become a major issue as information technology is ruling the world. Cryptography using mathematical techniques is providing information security but requires complex algorithms, intensive mathematical computations and efficient computational resources. To avoid such intensive and complex algorithms a new scheme known as Visual cryptography (VC) was introduced by Naor and Shamir [1]. This technique allows Visual information (pictures, text, etc) to be encrypted in such a way, that their decryption can be performed by the human visual system, without any complex cryptographic algorithms. In this technique an image is encrypted into shares such that stacking a sufficient number of shares reveals the secret image. This paper proposes three modes for visual cryptography for gray-level and color images (basic 2 out of n, 3 out of n and extended modes). We have also proposed the general access structure visual cryptography. Our model not only retain the advantages of black-and-white visual cryptography, but also have the backward compatibility with the previous results in black-and-white visual cryptography, such as the k out of n threshold scheme, and can be applied to gray-level and color images easily.

**Keywords:** Secret Sharing; Visual Cryptography.

1. INTRODUCTION

A Naor and Shamir [1] proposed visual cryptography, in 1994. The elegance of their approach is that it can recover a secret image without any computation. It exploits the human visual system to read the secret message from some overlapping shares, thus overcoming the disadvantage of complex computations. It makes use of the human vision system to perform the pixel-wise OR logical operation on the superimposed pixels of the shares. When the pixels are small enough and packed in high density, the human vision system will average out the colors of surrounding pixels and produce a smoothed mental image in a human’s mind.

The Visual Cryptography scheme proposed by Naor and Shamir has become as a basic model and has been applied to many applications. Besides the obvious applications to information hiding, there are many applications such as visual authentication and identification [2], watermarking [3-4], copyright protection [5], general access structures [6] and print & scan applications [7] etc.

Naor and Shamir proposed method is based on the concept of secret sharing, we first discuss about secret sharing using the analogy given below. Every bank has a vault that must be opened by a secret key, by any two out of three of its senior employees. As a procedure the bank does not want to trust any of them individually. Hence, they would like to design a system such that any two of the three senior employees can open the vault together. This problem can be viewed as two out or three secret sharing problem and represented as secret sharing scheme. In general, a (k, n) secret sharing scheme is a method to share a secret s among n participants such that the following properties should hold:

- Any k or more participants together can compute the secret s.
- Any k-1 participants gain no information about s.

Here is an example of a (2, 2) secret sharing scheme. Assume that the secret K is a binary sequence of length m, i.e. K = (k_1, k_2, ..., k_m). The two shares, s_1 and s_2 can be constructed as follow. The first share is chosen to be a random binary sequence of length m, say s_1 = (s_{11}, s_{12}, ..., s_{1m}). Then, we can compute the second share by doing “exclusive-or” on K and s_1.

\[ s_2 = k_i \oplus s_{1i}, \quad i = 1, ..., m \quad (1) \]

For example, assume that m = 2, k = (0, 1). Then the two shares can be constructed as follow:

- \( s_1 = (0, 0) \), then \( s_2 = s_1 \oplus K = (0, 1) \)
- \( s_1 = (0, 1) \), then \( s_2 = s_1 \oplus K = (0, 0) \)
- \( s_1 = (1, 0) \), then \( s_2 = s_1 \oplus K = (1, 1) \)
- \( s_1 = (1, 1) \), then \( s_2 = s_1 \oplus K = (1, 0) \).

However, looking only at one share, say s_1, any four values of K are possible. In other words, it gains no information about K if another share s_2 is unknown.
We know that every piece of information (images/data) is stored as a bit string or a number on a computer. Suppose two parties are going to share a secret bit string 1011. The two shares are generated as follows (see Figure 2 below):

1. To generate the first bit of the two shares, we flip a coin. If the result of the coin flipping is a head, then the first bit of the first share is 0; if the result of the coin flipping is a tail, then the first bit of the first share is a 1.

2. Now generate the first bit of the second share. If the result of the previous coin flipping was a head, then we copy the first bit of the secret. Else, if result of the previous coin flipping was a tail, then we flip the first bit of the secret and use that. (Note: in fact, what we have simply done is to make the first bit of the second share equal to the XOR of the first bit of the first share and the first bit of the secret.)

3. We repeat this random process for each bit of the secret.

Suppose for our example where the secret bit string is 1011, we flip the coin 4 times and get the sequence head, tail, tail, and head. Then the bits of our first share would simply be 0110. As a result, the bits of the second share would be 1101 (the XOR of 0110 and 1011). (see Figure 1 below).

Now we need to show that this scheme satisfies the two properties mentioned earlier. First, it is easy to see that the secret can be reconstructed from the two shares using bit-wise XOR. Second, we also need to show that the secret cannot be recovered with less than two shares. We know that the first share is generated through coin flipping. Obviously, it is random and has nothing to do with the secret. As for the second share, it is the result of a random transformation, based on coin flipping, of the secret. It should also be random.

Now consider a simple (2, 2)-VC scheme using pixels as shown in Figure 2. Each pixel p from a secret binary image is encoded into m black and white sub pixels in each share. If p is a white (or) black pixel, one of the six columns is selected randomly with equal probability, replacing p. Regardless of the value of the pixel p, it is replaced by a set of four sub pixels, two of them black and two white. Now the sub pixel set gives no clue about the original value of p. When two sub pixels from two white p pixels are superimposed, the decrypted sub pixels have two white and two black pixels. On the other hand, a decrypted sub pixel having four black pixels indicates that the sub pixel came from two black p pixels.

![Figure 1: Dividing the secret into two shares](image)

2. LITERATURE SURVEY

In [1], Naor and Shamir introduced VCS and proposed several constructions, where the generic one supports k out-of-n threshold setting for black-and-white images. Their scheme does not support images of arbitrary number of colors. Based on the work of Noar and Shamir, there have been many other schemes proposed [8-17]. A VCS which has less pixel expansion when compared to [1] was proposed by Adhikari et al. [10]. In [18], Yang proposed another one which achieves no pixel expansion but their scheme only supports black-and-white images. Chen et al. proposed a model which extended the results to gray-scale images and proposed a gray-scale VCS [19] with no pixel expansion. However, their scheme does not support the general k-out-of-n threshold setting. In addition, it also needs to perform block averaging (i.e. preprocessing) on the original image before carrying out the secret sharing. Another gray-scale VCS without pixel expansion was proposed by Chan et. al [20]. Their scheme also needs preprocessing by dithering and adjusting the gray level of the original image. Their model as not supports the general k-out-of-n threshold setting. Hou’s schemes [21] are considered to be the first set of color VCS’. For color VCS, we can refer [21-26]. All the schemes in [21] have the pixel expansion of 4 and do not support the general k-out-of-n threshold setting and dithering is required for preprocessing the original image. Yang and Chen proposed a VCS for color images based upon an additive color mixing method [26]. In their scheme, each pixel is expanded by a factor of...
three. Hou and Tu proposed a new color VCS [27]. The scheme also supports k-out-of-n threshold setting with no pixel expansion. Dithering is still required for preprocessing the original image before secret sharing. Shyu proposed an efficient c-color \((k, n)\)-threshold visual secret sharing scheme [28] and has further improved the pixel expansion to maintain good visual quality of the revealed secret image. In [29] Wu et al. Proposed a probabilistic technique for achieving no pixel expansion and generically converts any k-out-of-n threshold visual cryptography scheme for black-and-white images into one which supports color images. In his paper Dastanian [30] proposed a new visual cryptography scheme, that can transmit the two secret image with the use of two shares. With stacking two shares, secret image I appears and with stacking one of the shares with 90 degrees rotation in clockwise on other share appears the secret image II. Zhou et al. [31] used halftoning methods to produce good quality halftone shares in VC. Myodo [32] proposed a method to generate meaningful halftone images using threshold arrays. Wang et al. [33] produced halftone shares showing meaningful images by using error diffusion techniques. This scheme generates more pleasing halftone shares owing to errors diffused to neighbor pixels.

In [34] Chen and Wu proposed a \((2,2)\)-threshold visual secret sharing scheme for two secret images. The first secret image is decrypted by only stacking two share images. The second secret image is decrypted also by stacking two share images and one share image rotated. To overcome the angle restriction of Chen and Wu's scheme, Hsu et al [35] proposed another scheme to hide two secret images in two share images with arbitrary rotating angles. Their scheme rolls up the share images to become rings so that it becomes easy to rotate the share images at any desired angle. Feng and et al proposed the scheme to hide m secrets and to reveal the secrets by stacking the share images at \(m\) aliquot angles, respectively. Tzung-Her Chen et al [36] anticipated a multi-secrets visual cryptography which is extended from traditional VSS implemented to generate share images macro block by macro block in such a way that multiple secret images are turned into only two share images and decode all the secrets one by one by, stacking two of share images in a way of shifting. This scheme can be used for multiple binary, grey and colour secret images with pixel expansion of 4. Daoshun Wang et al [37] provided general construction for extended VC schemes using matrix extension algorithm. A general construction method for single or multiple and binary, greyscale, colour secret images using matrix extension utilizing meaningful shares was suggested. Using matrix extension algorithm any existing VCS with random-looking shares can be easily modified to utilize meaningful shares.

3. **OUR IMPLEMENTATION OF VISUAL SECRET SHARING (VSS) SCHEMES**

We have developed our application using java and implemented the following different modes.

3.1. **Basic \((2,n)\) Mode**

First we implemented with black and white images in basic \((2,n)\) mode which is further extended in to \((2,2),(2,3),(2,4),(2,5)\) modes. The basic \((2,2)\) model is implemented as proposed by Naor and Shamir. For displaying a white pixel, the sequence of the sub pixels on the first and on the second transparency are same. Overlaying the two transparencies leads to 2 black and 2 white sub pixels. For displaying a black sub pixel the sequences of the sub pixels are different, so that we get 4 black sub pixels by overlaying the transparencies. In \((2,3),(2,4)\) and \((2,5)\) scheme we can generated various \(3\) of transparencies, whereas always any 2 participants can decode the secret image.

![Figure 3: Basic 2 Out of 5. Top Left to Right: Secret Image, Share1,2. Bottom: Share 3, 4, 5](image)

![Figure 4: Overlaying of Shares [1 & 2], [1,2&3], [3,4&5], [1,2,3&4], [2,3,4&5], [1,2,3,4&5]](image)

3.2. **Basic \((3,n)\) Mode**

Next we have implemented with black and white images in basic \((3,n)\) mode which is further extended in to \((3,3),(3,4)\) and \((3,5)\). In \((3,3)\) scheme we can generate 3 transparencies, whereas always all 3 participants are needed to decode. In remaining schemes we can generate a various number of transparencies \(4\), whereas always any 3 participants can decode the image.
We have also implemented using some random key. It generates a random transparency serving as a key and then encrypts the right and the left image with a simple 2 out of 2 scheme. By overlaying the transparencies without the key we get a symmetrical difference and can achieve a lot of information about the two encrypted pictures. To overcome this problem we should use the random key once only such as a one-time-pad.

### 3.3. Extended Modes

After implementation of basic black and white images we have extended our application by implementing 2 out of 2 (gray scale images, color images, by using some random key and also implemented general access structure. When using gray images in this scheme original picture is taken and for each pixel is decided which luminance it has and we achieved 4 different greyscales (white, light grey, dark grey, black).

While implementing VSS using color images the original picture is taken and for each pixel it is decided which elementary color (red, green, blue or black) it has. Each pixel contains 1 red, 1 green, 1 blue and 3 black sub pixels. By overlaying the transparencies the black color dominates all others. For displaying a concrete color (for example red) all sub pixels except the red one are overlayed with an black sub pixel. The red pixel is overlayed with a red subpixel. So we achieved 5 black and a red sub pixel, and for the human visual system it appears as a (dark) red pixel.

Lastly we have also implemented 2 out of 3 general access structures, with this scheme we can generate 3 transparencies, and we can specify which group(s) of participants are allowed to decode.
4. CONCLUSION

In this paper we have presented new constructions of VSS schemes. We have developed an application which extended traditional black & white visual cryptography schemes. We first proposed a technique for grayscale and color visual cryptography using 2 out of n, 3 out of n and extended modes. We have also successfully implemented Visual Cryptography using General access structure and using Random key. Experimental results show that our scheme is simple, more efficient, and can provide one of the best reconstructed images in quality.

REFERENCES


