International Journal of Signal Processing, Image Processing and Pattern
Vol. 2, No.1, March, 2009

An Efficient Probability-based *t* out of *n* Secret Image Sharing Scheme

Chi-Chen Chang[1], Yu-Zheng Wang[2] and Chi-Shiang Chan[3]

[1]*Department of Information Engineering and Computer Science, Feng Chia University,Taichung, Taiwan 40724, R. O. C.*
E-mail: ccc@cs.ccu.edu.tw

[2] *Department of Computer Science and Information Engineering, National Chung Cheng University,Chiayi, Taiwan 621, R. O. C.*
E-mail: wyc92@cs.ccu.edu.tw

[3] *Department of Information Science and Applications, Asia University, Wufeng, Taiwan 41354, R. O. C.*
E-mail: CSChan@asia.edu.tw

Abstract

Noar and Shamir presented the concept of visual cryptography. Many researches following it go down the same track: to expand the secret pixels to blocks. As a result, the size of the secret image becomes larger, and the quality of the expanded secret image becomes worse. In order to prevent the pixels from expanding, Yang has proposed his probability-based visual secret sharing scheme, where the concept of probability is employed to pick out pixels from the black or white sets. In this paper, we shall propose a new scheme that is a modified version of Yang's scheme. Our experimental results show that we can obtain better recovered image quality with high contrast.

1. Introduction

In the realm of image-hiding techniques, there exists a special topic of research called visual cryptography [4], which can be traced back to Noar and Shamir in 1994. The main feature of visual cryptography is that the hidden message can be revealed by overlaying transparencies together, where the transparencies appear to be composed of nothing but random dots. This means people can simply use their eyes to decode the information directly once the transparencies are stacked up together.

A common trick Noar and Shamir's method and its successors play [2, 3] is that the secret pixels must be expanded into blocks. It goes without saying that the expanded image becomes bigger than the original binary image. Moreover, the expanded image may become significantly different from the original binary image. In order to prevent the binary image from expanding, Yang proposed his visual sharing scheme with a probabilistic method [6]. Following Yang's method, the secret binary image can be distributed to certain number of camouflage transparencies. After stacking the transparencies, the secret image can be visually revealed. The size of the secret image is the same as that of the original binary image. Moreover, the recovered secret image is more similar to the original binary image.

Although visual cryptography has become a focus of research in the field of secret image protection, there are still some practicality problems left unsolved. For one thing, the camouflage image must be printed on transparencies so that the transparencies can be stacked together to reveal the secret image. However, it is usually not a very convenient thing to carry transparencies around. If the camouflage images were printed on paper or stored in the cell phone, then it would not cause too much trouble. Nevertheless, nothing can be revealed when camouflage images printed on paper are stacked together, and nor can they be stacked together to reveal the secret image on the screen of a cell phone. Another drawback is that the camouflage transparencies must be stacked and aligned with extreme precision. When the camouflage transparencies are not put together exactly in position, the secret image cannot be revealed. Finally, when the scheme is applied on the computer, the stacking action is simulated by using the OR-ed operator. That is, if there exists any pixel whose color is black, the final color of the stacked pixel will also be black.

In this paper, instead of the OR-ed operator, we decide to use the MODULE operator. Moreover, the camouflage images are stored in a low computation device (such as cell phone or PDA). When a certain number of persons want to work together and recover the secret image, they just show their cell phones and transmit the camouflage images to each other by using infrared rays. By using the MODULE operator, our method can give better image quality than Yang's method, which our experimental results will demonstrate later.

The rest of this paper is organized as follows. To begin with, we shall review Yang's method in Section 2. Then, we will continue to present our method in Section 3. In Section 4, we shall offer our experimental results to demonstrate the effectiveness of our new method. Finally, the conclusions will be given in Section 5.

2. Related Works

In this section, we will briefly review the visual sharing scheme with a probabilistic method developed by Yang [6]. In the remaining parts of this paper, we shall refer to this probabilistic visual sharing scheme as **PVSS**.

PVSS mainly works by applying different white pixel appearance probabilities in white areas and black areas to form different degrees of darkness. The white pixel appearance probability in a white area is greater than that in the black area, and that is why we can distinguish a white area from a black area. Here, we use $\mathbf{P_w}$ to denote the appearance probability of white pixel in the white area, and $\mathbf{P_b}$ to denote the appearance probability of white pixel in the black area.

Since the (t, n) **PVSS** scheme functions on the basis of the appearance probability of white pixel in the "white area" and "black area", the (t, n) **PVSS** scheme uses two sets, the white set $\mathbf{S_w}$ and the black set $\mathbf{S_b}$. The white set, as well as the black set, is composed of a collection of $n\times1$ matrices. Here we define an $n\times1$ matrix as $\mathbf{A}=[\mathbf{a}_i]$, where $\mathbf{a}_i=1$ indicates that the pixel in the i-th shadow is a black pixel, and $\mathbf{a}_i=0$ means that the pixel in the i-th shadow is a white pixel.

Yang's **PVSS** scheme also provides a transferred function **T(•)**. This transferred function can easily construct the (t, n) **PVSS** scheme from conventional (t, n) **VSS** schemes [1, 5]. In a conventional **VSS** scheme, two Boolean matrices, namely a white

matrix and a black matrix, are typically used. To form a **PVSS** scheme, the white matrix and black matrix of the conventional **VSS** scheme can be directly transferred to the white set and black set of the **PVSS** scheme, respectively. The method here is to transform an $m \times n$ matrix to a set of "m" $n \times 1$ column matrices.

Then, let us see how the **PVSS** scheme works. First, the construction steps are as follows.

Input: A binary secret image **I**

Output: n shadow images

Step 1. Take a pixel $\mathbf{g}_x$ from the secret image **I**, where x denotes the current position. If the pixel $\mathbf{g}_x$ is a white pixel ($\mathbf{g}_x = 0$), an $n \times 1$ matrix **A** is randomly picked out from the white set $\mathbf{S_w}$. If the pixel $\mathbf{g}_x$ is a black pixel ($\mathbf{g}_x = 1$), the $n \times 1$ matrix **A** is picked out from the black set $\mathbf{S_b}$.

Step 2. For every column value $\mathbf{c}_i$ in the matrix A, where $1 \le i \le n$, if $\mathbf{c}_i$ is 0, the pixel at the same position x in the i-th shadow image is represented by a white pixel. If $\mathbf{c}_i$ is 1, the pixel is represented by a black pixel. This way, the same position x of n shadow images can be constructed.

Step 3. Repeat Step 2 and Step 3 until all pixels have been processed.

Finally, let us observe how the **PVSS** scheme recovers the sharing secret image. When shadow images i_1, i_2… i_r are to be stacked together, where $1 \le r \le n$, Yang's scheme uses a so-called stacking operation to put together the shadow images. This stacking operation is executed by OR-ed operations, and it can be represented by $U(V) = i_1 \vee i_2 \vee \ldots \vee i_r$. Here V is a column vector $i_1, i_2, \ldots, i_r$ and "$\vee$" denotes the OR-ed operation. Then, the secret image can be recovered according to the above-mentioned stacking method.

3. The Proposed Method

In this section, we shall present our method. The details of our proposed scheme are as follows.

3.1. Constructed method

Assume that we have a secret image **I**, which is made up of a collection of black and white pixels, and we have a construction composed of two sets, the white set $\mathbf{S_w}$ and the black set $\mathbf{S_b}$. Different (t, n) thresholds have different constructions. The construction method is as follows.

First, there is raster scanning done to image **I**. For each pixel, we judge the color of this pixel. If the color is white, it means that we must use the white set to construct the color of the pixel in the same position for n shadow images. If the color is black, we use the black set to construct the n shadow images. The trick here is that we randomly choose one matrix $\mathbf{A} = [\mathbf{a}_i]$, where $1 \le i \le n$, from the white set (or black set), and then

the pixel color for these n shadow images is decided according to each column value $\mathbf{a}_i$ of matrix $\mathbf{A}$. Say, if $\mathbf{a}_i = 1$, the pixel in the i-th shadow will come out to be black. Otherwise, if $\mathbf{a}_i = 0$, the pixel in the i-th shadow will turn out to be white. An example is shown in Figure 1.

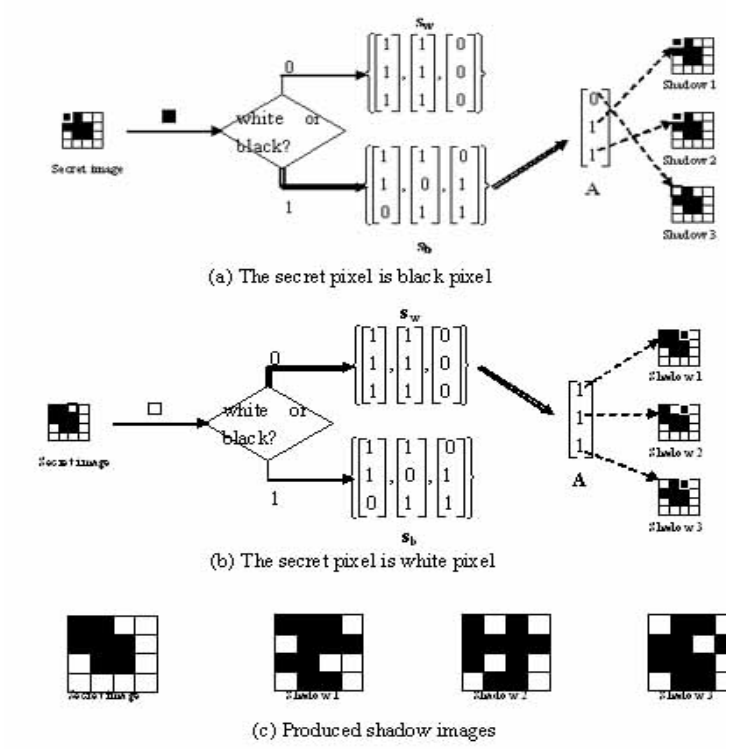

Figure 1 The sketchy flowchart of constructed method

As Figure 1(a) reveals, when the sharing secret pixel is black, we randomly choose one matrix $\mathbf{A}$ from the black set $\mathbf{S_b}$, and then we randomly pick out one column value to represent a pixel of one shadow image. After that, we choose the second column value to represent a pixel of shadow 1, choose the third column value to represent a pixel of shadow 2, and choose the first column value to represent a pixel of shadow 3. The result of the construction is shown in Figure 1(c).

3.2. Stacked method

We use raster scanning on every shadow image to recover the secret image. For each pixel in the same position in every shadow image, we recover the secret pixel in the secret image in the same position by using our proposed stacking operation D(•). This stacking operation is executed by modular operations as follows,

$$D(V') = \begin{cases} (s_1 + s_2 + ... + s_r) \bmod 2 & if \quad r = t. \\ (s_1 + s_2 + ... + s_r) \bmod (2 + r - t) & r > t. \end{cases} \tag{1}$$

Here V' is the r-tuple column vector, where $1 \leq r \leq n$, which contains $s_1, s_2, \ldots, s_r$. These $s_1, s_2, \ldots, s_r$ denote the values of the pixels in each shadow image i, where $1 \leq i \leq r$. If a pixel in the shadow image i is white, the value s_i is 0. If the pixel is black, s_i is 1.

In our stacking operation, we first determine whether the number of stacked shadow images is greater than or equal to t. If the number of stacked shadow images is equal to t, we adopt the modulus of 2. Otherwise, in case the number of stacked shadow images is greater than the value t, we adopt the modulus of $(2 + r - t)$. Then, we add up all the shadow images we want to stack and obtain the value D(V') after the modulus. If the value D(V') is equal to zero, it means that the pixel of the recovered secret image is white; otherwise, if the value D(V') isn't equal to zero, then the pixel is colored black. The flowchart of the stacking process is shown in Figure 2.

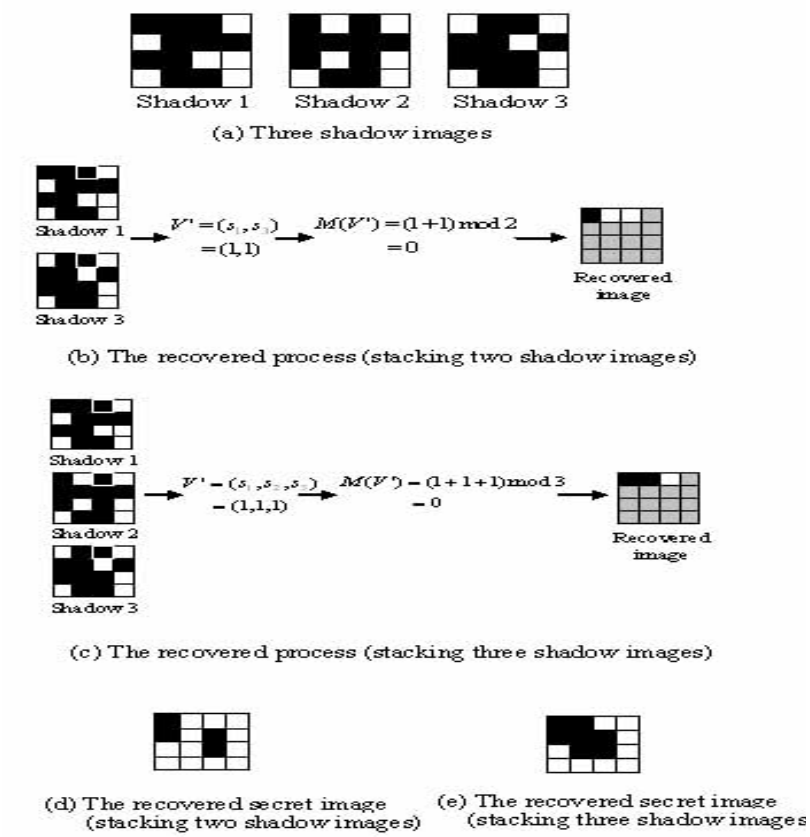

Figure 2. Our stacked method

Example: Going on with the above example, we would like to recover the secret image of the (2, 3) threshold. That is, we have n=3 and t=2 here. There are three shadow images, which are shown in Fig 5(a), and the recovery process is illustrated in Figs. 3(b)-(c). Figs. 3(d)-(e) show the results of our stacking operation.

4. Experimental results

In this section, we shall present our experimental results and show how effectively and efficiently our modular operation can produce shadows and recover the recovered

image. Figure 3 shows the original binary image, the 512 × 512 Lena image, and the 300 × 200 CCU image we want to share. The following are our experimental results on the (2, 3) threshold schemes.

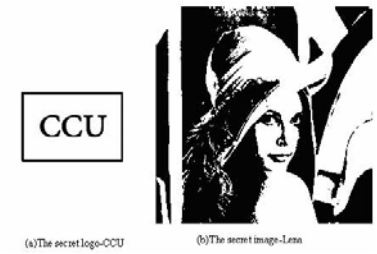

Figure 3. The original secret image

The experimental results of our (2, 3) threshold scheme are shown in Figure 4 and Figure 5. Figure 4 shows the shadow images produced by our proposed method and **PVSS** for the CCU logo. Figure 5 shows the shadow images produced by our proposed method and **PVSS** for the Lena image.

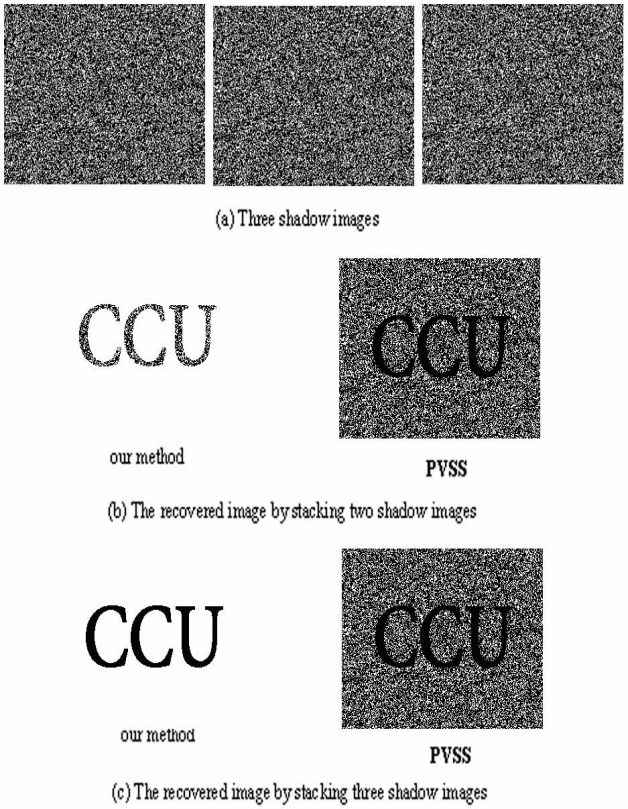

Figure 4. The experimental results of CCU for (2, 3) threshold scheme

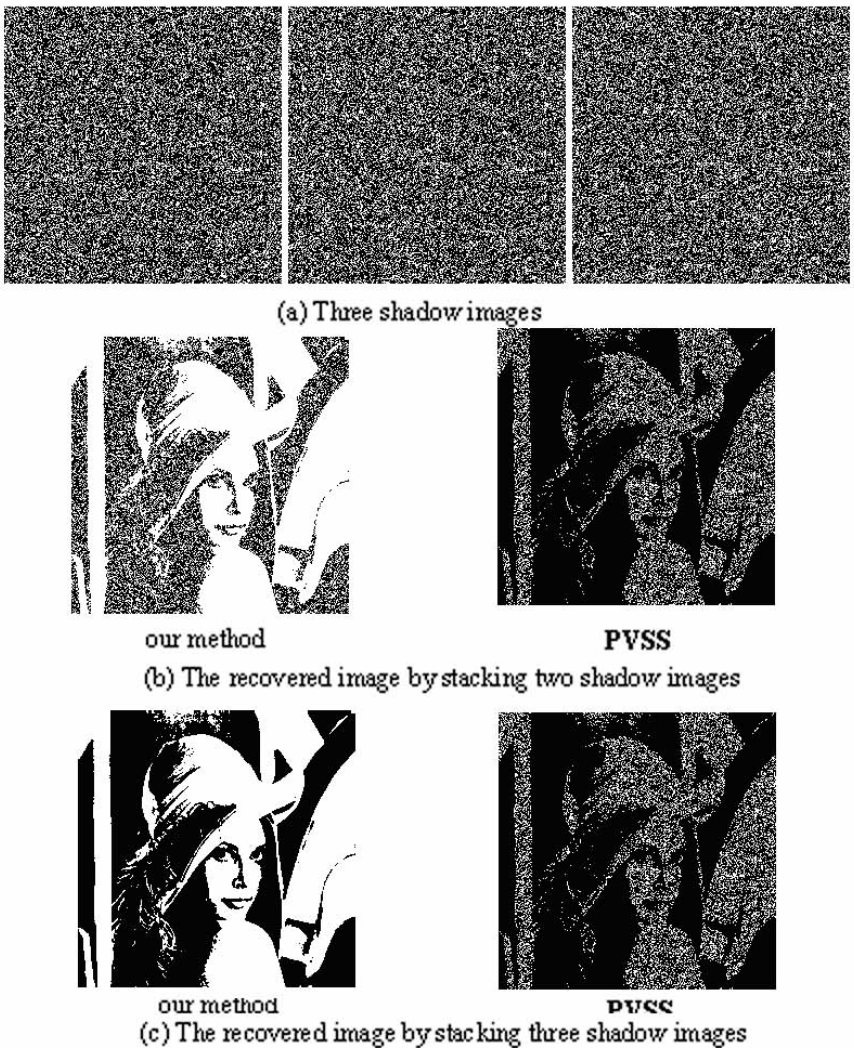

Figure 5. The experimental results of Lina for (2, 3) threshold scheme

The experimental results with our proposed stacking method are shown in the above-mentioned figures. As for the security of our proposed method, it will be discussed in the next section.

5. Conclusions

In this paper, we have presented a new (t, n) threshold scheme. The design of our new scheme is based on the framework of the **PVSS** scheme, and only simple operations are used in the stacking process to obtain better image quality. Our experimental results seem good. As we can conclude that our proposed scheme is indeed applicable to modern mobile devices.

References

[1] S. Droste, "New results on visual cryptography, " *Eurocrypt'96*, *Lecture Notes in Computer Science*, vol. 1109, 1996, pp. 401-415

[2] Y. C. Hou, "Visual cryptography for color images," *Pattern Recognition,* vol. 36, no. 7, 2003, pp. 1619-1629.

[3] R. J. Hwang and C. C. Chang, "Hiding a picture in two pictures," *Optical Engineering*, vol. 40, no. 3, 2001, pp. 342-351.

[4] M. Naor and A. Shamir, " Visual cryptography, " *Eurocrypt'94*, *Lecture Notes in Computer Science*, Springer-Verlag, 1994, pp.1-12.

[5] E. R. Verheul and H.C.A.Van Tilborg, " Constructions and properties of *k* out of *n* visual secret sharing schemes, " *Designs, Codes and Cryptography*, vol. 11, no. 2, 1997, pp.179-196.

[6] C. N. Yang, "New visual secret sharing schemes using probabilistic method, " *Pattern Recognition Letters*, vol. 25, 2004, pp.481-494.

Chin-Chen Chang received his BS degree in applied mathematics in 1977 and his MS degree in computer and decision sciences in 1979, both from the National Tsing Hua University, Hsinchu, Taiwan. He received his Ph.D in computer engineering in 1982 from the National Chiao Tung University, Hsinchu, Taiwan. During the academic years of 1980-1983, he was on the faculty of the Department of Computer Engineering at the National Chiao Tung University. From 1983-1989, he was on the faculty of the Institute of Applied Mathematics, National Chung Hsing University, Taichung, Taiwan. From 1989 to 2004, he has worked as a professor in the Institute of Computer Science and Information Engineering at National Chung Cheng University, Chiayi, Taiwan. Since 2005, he has worked as a professor in the Department of Information Engineering and Computer Science at Feng Chia University, Taichung, Taiwan. Dr. Chang is a Fellow of IEEE, a Fellow of IEE and a member of the Chinese Language Computer Society, the Chinese Institute of Engineers of the Republic of China, and the Phi Tau Phi Society of the Republic of China. His research interests include computer cryptography, data engineering, and image compression.

Yu-Zheng Wang received the BS degree in computer science and information engineering from National Dong Hwa University, Hualien, Taiwan, Republic of China, in 2003 and the MS degree in computer science and information engineering in 2005 from National Chung Cheng University, Chiayi, Taiwan. His current research interests include steganography, watermarking, image processing, and video.

Chin-Chen Chang received his BS degree in Computer Science in 1999 from the National Cheng Chi University, Taipei, Taiwan and the MS degree in Computer Science and Information Engineering in 2001 from the National Chung Cheng University, ChiaYi, Taiwan. He received his Ph.D in Computer Science and Information Engineering in 2005 from the National Chung Cheng University, ChiaYi, Taiwan. Since 2007, he has worked as a assistant professor in the Department of Information Science and Application at Asia University, Wufeng, Taiwan.His Research fields are image hiding and image compression.