VISUAL CRYPTOGRAPHY FOR PRINT AND SCAN APPLICATIONS

Wei-Qi Yan, Duo Jin, Mohan S Kankanhalli

School of Computing
National University of Singapore
Singapore 117543

ABSTRACT

Visual cryptography is not much in use in spite of possessing several advantages. One of the reasons for this is the difficulty of use in practice. The shares of visual cryptography are printed on transparencies which need to be superimposed. However, it is not very easy to do precise superposition due to the fine resolution as well as printing noise. Furthermore, many visual cryptography applications need to print shares on paper in which case scanning of the share is necessary. The print and scan process can introduce noise as well which can make the alignment difficult. In this paper, we consider the problem of precise alignment of printed and scanned visual cryptography shares. Due to the vulnerabilities in the spatial domain, we have developed a frequency domain alignment scheme. We employ the Walsh transform to embed marks in both of the shares so as to find the alignment position of these shares. Our experimental results show that our technique can be useful in print and scan applications.

1. INTRODUCTION

Visual cryptography (VC) is basically a secret sharing scheme extended for images [1] and its distinguishing characteristic is the ability of secret restoration without the use of computation. Figure 1 is an example of the use of visual cryptography.

The two top images figure 1(a) and figure 1(b), share 1 and share2 are two randomly generated images which carry the secret information. If we print the two shares on transparencies and superimpose them, we can clearly see the secret as shown in figure 1(c).
Briefly speaking, the VC technique technique is for binary images where α is the secret image, γ is a randomly generated share while β is the other share such that:

$$\alpha_i + \beta_i = \gamma_i, \;\; i = 0, 1, 2, \ldots, n$$

Thus without β and γ, α cannot be deduced at all [2]. This scheme provides perfect security with simplicity [1]. Visual cryptography possesses these characteristics:

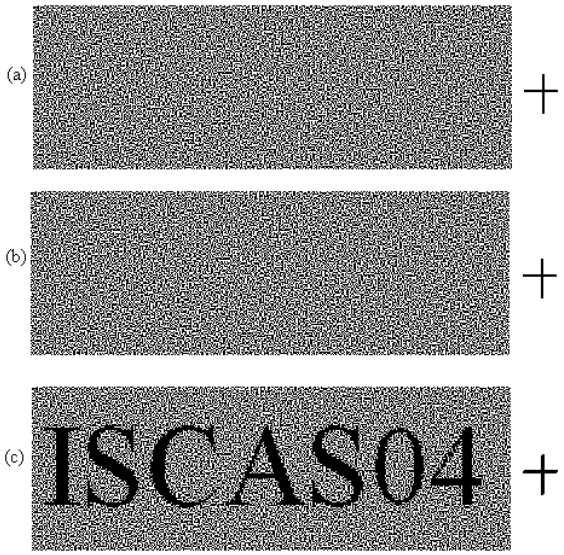

Fig. 1. Cross Alignment for Visual Cryptography

- Perfect security
- Decryption (secret restoration) without the aid of a computing device
- Robustness against lossy compression and distortion due to its binary attribute.

However, the shortcomings of visual cryptography are as salient as its merits. There are three main drawbacks in visual cryptography:

- It results in a loss of resolution. The restored secret image has a resolution lower than that of the original secret image.
- Its original formulation is restricted to binary images. For color images, some additional processing such as halftoning and color-separation are required.
- The superposition of two shares is not easy to perform unless some special alignment marks are provided.

The manual alignment procedure can be tedious especially for high resolution images.

The first two shortcomings have been discussed in literature earlier [3] [4] [5] [6]. We will focus on the third problem in this paper. The shares of VC printed on transparencies are very difficult to be overlapped with proper alignment even if we ignore the printing errors. A wide variety of applications of visual cryptography would require the printing of the shares on paper like that of documents, checks, tickets or cards [7] [8]. In such cases, scanning of the printed shares is inevitable for restoring the secret. The scanned shares (with printing, handling and scanning errors) have to be superimposed in order to reconstruct the secret image which could be some photo, code or other such important information.

In this paper, we concentrate on the print and scan applications of visual cryptography. i.e. to obtain the precise position of scanned shares which requires rotation and alignment correction. Putting alignment marks in the spatial domain is extremely vulnerable to cropping and editing. Therefore, we use the Walsh transform domain to embed perceptually invisible alignment marks. We show that the Walsh transform helps in recovering the marks inspite of noise and we can precisely align the scanned shares to recover the secret.

2. BACKGROUND

In order to carry out the superposition, initially a spatial tag is marked beside the shares. In figure 1, we put a cross beside each share. For restoring the secret, the two crosses need to be precisely overlapped. If this is done, the secret image will be revealed. Another solution to this problem is by utilizing the extended visual cryptography scheme [9]. This scheme shares a secret by using two protection images **B** and **C**. The procedure of visual cryptography is performed as: **A** = **B'** + **C'** where the secret **A** is divided into two shares **B'** and **C'**. On these shares **B'** and **C'**, images **B** and **C** are also visible. During restoration, images **B** and **C** are aligned to make them disappear (by cancelling) revealing the secret in the process. An example of this technique is shown in figure 2, figure 2(a) and figure 2(b) are shares, figure 2(c) is the reconstructed image.

Actually, figure 1 and figure 2 belong to the same class of techniques since they both work in the spatial domain. The problem with this class is that the alignment marks are visible to an attacker and thus can be easily removed by cropping or localized image alteration. We therefore explore the alternative idea of using marks in the frequency domain. In particular, we consider the use of the discrete Walsh transform, which is useful for pulse signals and is distinct from the discrete Fourier transform **(DFT)**, discrete cosine transform **(DCT)** and discrete wavelet transform **(DWT)**. Walsh functions are a complete set of orthogonal functions

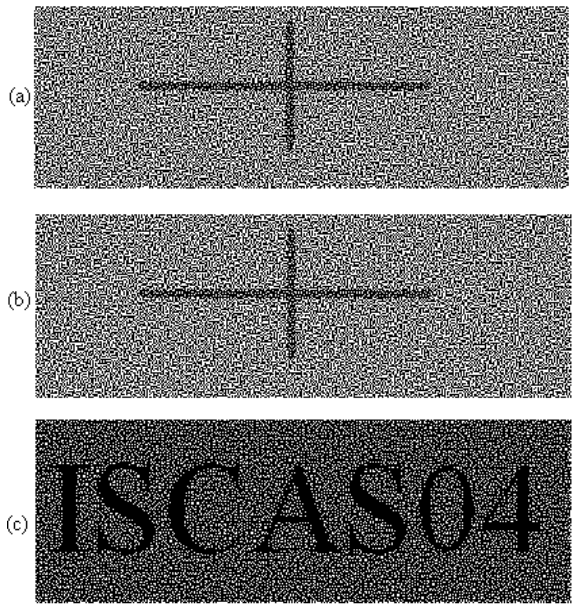

Fig. 2. Cross Alignment by Using Extended Visual Cryptography

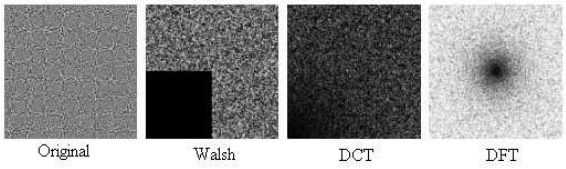

Fig. 3. The original shares and their transformations

with the the value being only -1 and 1. We use the 2D discrete Walsh transform:

$$W_{xy}(u,v) = \frac{1}{N_x}\frac{1}{N_y}\sum_{y=0}^{N_y-1}\sum_{x=0}^{N_x-1} f(x,y)\cdot(-1)^{\alpha} \qquad (1)$$

The inverse transform is given by:

$$f(x,y) = \sum_{v=0}^{N_y-1}\sum_{u=0}^{N_x-1} W_{xy}(u,v)\cdot(-1)^{\alpha} \qquad (2)$$

where $\alpha = \sum_{r=0}^{p_x-1} x_r u_r + \sum_{s=0}^{p_y-1} y_s v_s$, $f(x,y)$ is a pixel of the image, (x,y) is its position. $W_{xy}(u,v)$ represents the transform coefficients, $N_x = 2^{P_x}$, $N_y = 2^{P_y}$, (P_x and P_y are positive integers), x_r, u_r, y_s and v_s are either 0 or 1 (i.e. one bit of x, u, y and v respectively).

Unlike the Walsh transform, transforms like **DFT**, **DCT** and **DWT** are mainly used for continuous tone color images. The results of applying these three transformations to a VC share is shown figure 3. In figure 3, the left image is a VC share. The subsequent images show the result of applying

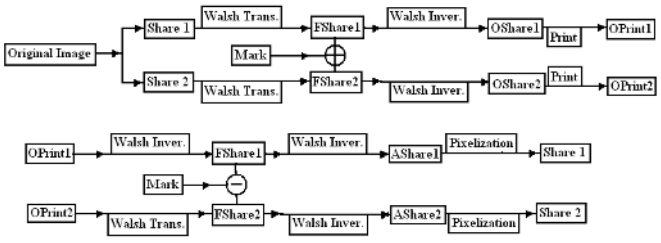

Fig. 4. Flowchart of Process for Print and Scan VC

the Walsh, **DCT** and the **DFT** transforms. The differences are quite apparent. Note that the bottom-left rectangle of the image for the Walsh transform is totally dark. This information can exploited in removing noise by filtering the coefficients in this quadrant. The overview of our print and scan scheme for the superposition of VC shares is shown in the flowchart of figure 4. The basic idea is to introduce some alignment marks in the Walsh transform domain.

3. OUR WORK

In this section, we will describe our contributions. During encryption, as shown in figure 4, we apply the Walsh transform on the shares. Then we embed marks in the high frequency coefficients of the transform. Then the inverse transform is applied to obtain the new shares with hidden marks that are printed on paper to be transmitted via public channels.

During the process of decryption, we scan the paper image and extract the marks by performing the Walsh transform to obtain the approximate alignment for shares superimposition. We then fine-tune the alignment by performing rotation and translation. The rotation is done by using:

$$\begin{bmatrix} x\prime \\ y\prime \end{bmatrix} = \begin{bmatrix} \cos(\alpha) & -\sin(\alpha) \\ \sin(\alpha) & \cos(\alpha) \end{bmatrix} \cdot \begin{bmatrix} x \\ y \end{bmatrix} \qquad (3)$$

The rotation adjustment in increments of angle α is done as shown in figure 5. The translation adjustment by $\triangle x$ and $\triangle y$ is done as shown in figure 6. The criteria for finding the best alignment position is that the superimposed image should have the least number of black pixels if we perform the XOR operation between them. This is because the XOR operation allows for perfect restoration of the secret image [3]. Our algorithm can thus be described as follows:

4. RESULTS

In this section, we will provide the results for visual cryptography. Figure 7 shows a share and the mark in the Walsh

input : Scanned Shares
output : Revealed Secret

1: Scan the two printed shares;
2: Do initial alignment by aligning Walsh transform domain marks;
3: Do final alignment by minimizing black pixels (after XOR) using shifts & rotates;
4: Reveal the secret;

Algorithm 1: Alignment of the VC Shares

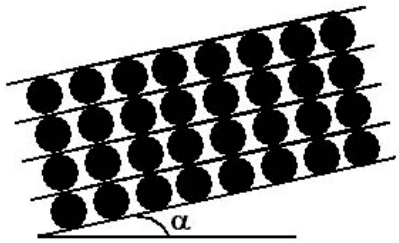

Fig. 5. Adjustment of Visual Cryptography Shares

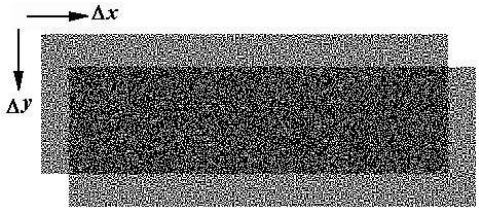

Fig. 6. The Shift Operation to the Overlapping Shares

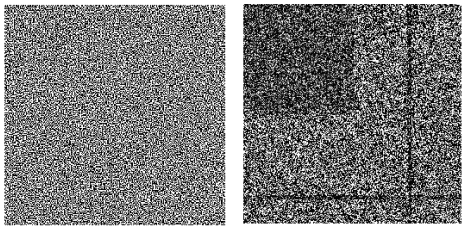

Fig. 7. Marked VC Share in Walsh Transform Domain

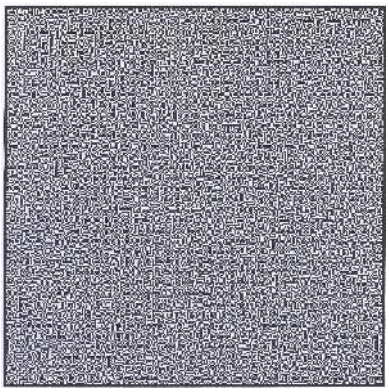

Fig. 8. The Scanned Watermarked VC Shares

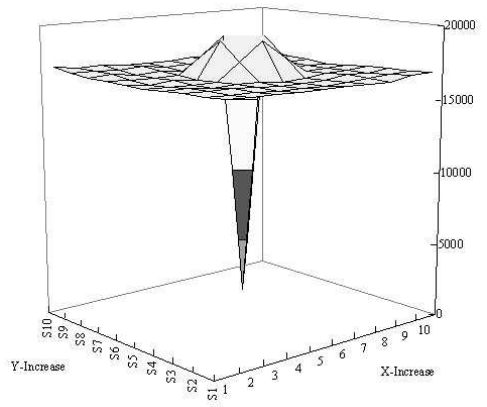

Fig. 9. Number of Black Pixels at Various Alignments

transform domain. The mark is in the form of a cross. In the implementation, we print the image by using the default setting of the Lexmark T622 PS3 printer at 1200dpi and scan the share image at 300dpi resolution. Figure 8 is an example of a scanned marked share. Figure 9 shows the minimization of black pixels when the correct alignment is obtained. The revealed secret after performing the XOR operation is shown in figure 10.

SOC/NUS

Fig. 10. Secret Image Revealed by the XOR operation

5. CONCLUSION

In this paper, we have tried to solve the practical problem associated with the use of visual cryptography. Many VC applications involve printing the share on the paper channel. If this is the case, then a print and scan technique needs to be developed for recovering the secret image. However, precise alignment at high resolutions is then a problem. We therefore propose the use of the Walsh transform to embed alignment marks in the transform domain. These marks are used as guides to precisely align the shares automatically. Our experimental results point to the viability of the use of VC for print and scan applications. Our future work will focus on the applications of visual cryptography on the 2D bar code.

6. REFERENCES

[1] M. Naor and A. Shamir, "Visual cryptography," in *Proc. of Advances in Cryptology*. 1995, vol. 950, pp. 1–12, Springer-Verlag.

[2] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, Nov 1979.

[3] D. Jin, "Progressive color visual cryptography," Masters degree thesis, School of Computing, National University of Singapore, Singapore, July 2003.

[4] Y.C. Hou, C.Y. Chang, and F. Lin, "Visual cryptography for color images based on color decomposition," in *Proc. of 5th Conference on Information Management*, Taipei, Nov 1999, pp. 584–591.

[5] Y.C. Hou, C.Y. Chang, and SF Tu, "Visual cryptography for color images based on halftone technology," in *Proc. of International Conference on Information Systems, Analysis and Synthesis,World Multiconference on Systemics, Cybernetics and Informatics*, 2001.

[6] Young-Chang Hou, "Visual cryptography for color images," *Pattern Recognition*, vol. 36, pp. 1619–1629, 2003.

[7] B.S. Zhu, J.K. Wu, and M.S. Kankanhalli, "Print signatures for document authentication," in *Proc. of ACM Conference on Computer and Communications Security*, October 2003, pp. 145–153.

[8] N. Degara-Quintela and F. Perez-Gonzalez, "Visible encryption: using paper as a secure channel, security and watermarking of multimedia contents," in *Proc. of SPIE'03*, 2003, vol. 5020.

[9] G. Ateniese, C. Blundo, A. De Santis, and D. Stinson, "Extended schemes for visual cryptography," *Theoretical Computer Science*, vol. 250, pp. 143–161, 2001.