2012

Enhancing the perceived visual quality of a size invariant visual cryptography scheme

Yang-Wai Chow
University of Wollongong, caseyc@uow.edu.au

Willy Susilo
University of Wollongong, wsusilo@uow.edu.au

Duncan S Wong
Hong Kong University

Publication Details

Chow, Y., Susilo, W. & Wong, D. (2012). Enhancing the perceived visual quality of a size invariant visual cryptography scheme. Lecture Notes in Computer Science, 7618 (2012), 10-21.

Enhancing the perceived visual quality of a size invariant visual cryptography scheme

Abstract
Two of the main areas of research in visual cryptography have been on improving the visual quality of the recovered image and in reducing the pixel expansion of the shares. This paper addresses both of these visual cryptography issues. First, a method to enhance the perceived visual quality of the recovered image using various image filtering techniques is presented. In particular, these image filtering techniques are used to enhance the local and global contrasts of a grayscale image. Second, a multi-pixel block size invariant visual cryptography scheme that maintains the relative density of local neighboring pixels is proposed. This method encrypts blocks of pixels based on whether the total number of black pixels within the respective blocks is above or below a certain threshold. In conjunction, these approaches effectively improve on the perceived visual quality of a recovered visual cryptography image.

Keywords
scheme, cryptography, invariant, size, quality, perceived, enhancing, visual

Disciplines
Physical Sciences and Mathematics

Publication Details
Chow, Y., Susilo, W. & Wong, D. (2012). Enhancing the perceived visual quality of a size invariant visual cryptography scheme. Lecture Notes in Computer Science, 7618 (2012), 10-21.

Enhancing the Perceived Visual Quality of a Size Invariant Visual Cryptography Scheme

Yang-Wai Chow[1], Willy Susilo[2⋆] and Duncan S. Wong[3]

[1] Advanced Multimedia Research Laboratory
[2] Centre for Computer and Information Security Research
School of Computer Science and Software Engineering, University of Wollongong, Australia
{caseyc, wsusilo}@uow.edu.au,
[3] Department of Computer Science, City University of Hong Kong, Hong Kong
duncan@cityu.edu.hk

Abstract. Two of the main areas of research in visual cryptography have been on improving the visual quality of the recovered image and in reducing the pixel expansion of the shares. This paper addresses both of these visual cryptography issues. First, a method to enhance the perceived visual quality of the recovered image using various image filtering techniques is presented. In particular, these image filtering techniques are used to enhance the local and global contrasts of a grayscale image. Second, a multi-pixel block size invariant visual cryptography scheme that maintains the relative density of local neighboring pixels is proposed. This method encrypts blocks of pixels based on whether the total number of black pixels within the respective blocks is above or below a certain threshold. In conjunction, these approaches effectively improve on the perceived visual quality of a recovered visual cryptography image.

Keywords: Visual cryptography, visual quality, image filtering, size invariant, multi-pixel encoding

1 Introduction

A visual secret sharing scheme known as visual cryptography was introduced by Naor and Shamir [11] as a means of using images to conceal information. The concealed information can be decrypted by the human visual system without any need of a computer to perform decryption computations. As such, this scheme can even be decrypted by individuals who have no knowledge of cryptography.

In the k-out-of-n Visual Cryptography Scheme (VCS) originally proposed by Naor and Shamir, a secret image is assumed to consist of a collection of black and white pixels. The secret image is used to create a set of n shares, each to be printed on a separate transparency. Individually, the shares look like random black and white pixels that reveal no information about the secret image, other than the image size. When a threshold number of shares, k, or more are stacked together, the human visual system averages the black and white pixel contributions of the superimposed shares to recover the hidden information. White is usually treated as transparent in order to allow colors (i.e. black) of the other shares to pass through it when superimposed. Stacking any $k-1$, or less, shares together does not reveal any information that can be used to recover the secret image, hence a (k, n)-VCS.

Since the introduction of visual cryptography, many researchers have proposed a variety of different VCSs over the years. One of the main drawbacks of traditional VCSs is the pixel expansion. In traditional VCSs, each pixel in the original secret image is represented using m pixels in each of the resulting shares. The parameter m is known as the pixel expansion, because the recovered image will be m times larger than the secret image [3]. Pixel expansion typically increases with the number of created shares, in some cases this increase is exponential. Large pixel expansion has a number of drawbacks in terms of the quality of the recovered image and the complexity of the VCS [4]. Furthermore, it makes it inconvenient for carrying shares and wastes storage space [6].

⋆ This work is supported by ARC Future Fellowship FT0991397.

Therefore, one of the main areas of research has been in reducing the pixel expansion. A number of researchers have proposed techniques for dealing with the pixel expansion problem in order to develop VCSs with no pixel expansion [2, 3, 6, 7, 10, 12–14]. In these size invariant VCSs, shares have the same size as the original secret image, thus $m = 1$.

In conjunction with reducing the pixel expansion, another commonly researched area has been in improving the visual quality of VCSs. Splitting the secret image into multiple shares in visual cryptography has the effect of reducing the contrast in the recovered image. Since visual cryptography relies on the human visual system to average the black and white pixel contributions of superimposed shares, the perceived visual quality of the recovered image is an extremely important issue. In general, the lower the overall contrast in the recovered image, the lower the perceived visual quality, as it becomes harder for the human mind to form a mental image of the secret image.

The issue of visual quality is even more vital in the case of size invariant VCSs, because in order to preserve the size, some information from the secret image is definitely lost. Unlike the traditional VCS, which is called deterministic because reconstruction of a secret pixel is guaranteed, size invariant VCSs give no absolute guarantee on the correct reconstruction of the original pixels. As such, it is not possible to recover the exact secret image from the shares. For the guarantee of a correct reconstruction, a certain pixel expansion must be paid in a deterministic scheme [4].

Our Contribution. This paper addresses both the issue of visual quality and the pixel expansion concern in visual cryptography. For grayscale images, we show that the perceived visual quality of the recovered image can be improved by using image filtering techniques prior to encrypting the secret image. It should be noted that other grayscale image VCSs can potentially benefit from the implementation of similar image filtering techniques. In addition, we also propose a size invariant VCS that maintains the relative density of local neighboring pixels in the recovered image. This is because unlike VCSs which encrypt individual pixels separately, in our proposed VCS we encrypt a block of multiple pixels based on the density of black pixels within the entire block. Together, these methods have the overall effect of enhancing the perceived visual quality of the recovered image.

2 Preliminaries

This section presents a brief background in relation to VCSs, including the (k, n)-VCS construction as defined by Naor and Shamir [11] and how it can be used for grayscale images.

2.1 Fundamentals of VCSs

In general, a (k, n)-VCS encrypts a secret image into n shares. Each share contains a collection of black and white pixels that do not reveal any information about the secret image. The secret image can only be recovered by stacking together k or more shares. The human visual system averages the black and white pixel contributions of the superimposed shares to recover the hidden information. No information is revealed if less than k shares are stacked together.

The resulting structure can be described by two collections of $n \times m$ binary matrices, C_0 and C_1, where each row in these matrices represents the black and white subpixel configuration that are used to encrypt one share. Since each pixel in the secret image is encrypted in each share as m subpixels, this represents the pixel expansion. A square is usually a good choice for the subpixel configuration because it maintains the aspect ratio. To encrypt a white pixel in the secret image, one of the matrices in C_0 is randomly selected, whereas to encrypt a black pixel, one of the matrices in C_1 is randomly selected.

Stacking shares together has the effect of 'OR'ing the m subpixels of the respective matrix rows. The gray-level of the stacked shares is proportional to the Hamming weight $H(V)$ of the 'OR'ed binary vector V of length m. This gray-level is interpreted by the human visual system as black if $H(V) \geq d$ and as white if $H(V) < d - \alpha m$ for some fixed threshold $1 \leq d \leq m$ and relative difference $\alpha > 0$ [11].

(a) (b) (c)

Fig. 1. Example of Naor-Shamir (2, 2)-VCS applied to a grayscale image by first dithering the image. (a) The secret grayscale image; (b) Dithered image; (c) Recovered image, with a pixel expansion of $m = 4$.

Definition 1. *Let* k, n, m *and* d *be non-negative integers which satisfy* $2 \leq k \leq n$ *and* $1 \leq d \leq m$. *Two collections of* n×m *binary matrices,* C_0 *and* C_1, *constitute a* (k, n)-VCS *if the following conditions are satisfied:*

1. *For any* S *in* C_0, *the 'OR' operation of any* k *of the* n *rows satisfies* $H(V) < d - \alpha m$.
2. *For any* S *in* C_1, *the 'OR' operation of any* k *of the* n *rows satisfies* $H(V) \geq d$.
3. *For any subset* $\{i_1, i_2, ..., i_q\}$ *of* $\{1, 2, ..., n\}$ *with* $q < k$, *the two collections of* q×m *matrices* D_t *for* $t \in \{1, 0\}$ *obtained by restricting each* n×m *matrix in* C_t *(where* $t = 0, 1$*) to row* i_1, i_2, ..., i_q *are indistinguishable in the sense that they contain the same matrices with the same frequencies.*

The first two conditions are known as the contrast and the third condition as the security [11]. Ateniese et al. [1] showed how general access structures can be constructed for a (k, n)-VCS. A (2, 2)-VCS can be represented by the following two collections of binary matrices, known as the basis matrices of a VCS:

$$C_0 = \{\text{all matrices obtained by permutating the columns of } \begin{bmatrix} 0\,0\,1\,1 \\ 0\,0\,1\,1 \end{bmatrix}\}$$

$$C_1 = \{\text{all matrices obtained by permutating the columns of } \begin{bmatrix} 0\,0\,1\,1 \\ 1\,1\,0\,0 \end{bmatrix}\}$$

2.2 VCSs for Grayscale Images

Since the secret image in the original VCS is assumed to consist of black and white pixels, for grayscale images the secret image can first be converted to an image containing only black and white pixels through a techniques known as dithering [9]. Dithering is a technique commonly used in printing applications to create an illusion of color depth in images with a limited color palette. Colors not available in the palette are approximated by a diffusion of colored pixels from within the available palette. The basic principle of the diffusion is to pack pixels with a higher density to represent darker colors and to distribute the pixels sparsely to represent lighter colors [8].

In a dithered image, the human eye perceives the diffusion as a mixture of colors within it. This means that for grayscale images, the human visual system perceives different gray levels from the distribution of black and white pixels. Figure 1 depicts this process for a (2, 2)-VCS. The secret image, which is a 256-level grayscale image, is shown in Figure 1(a). Figure 1(b) shows the same image after Floyd-Steinberg dithering [5]. Note that the Floyd-Steinberg dithering technique was used for all dithered images in this paper. The dithered image can then be encrypted into two shares using the basis matrices presented in the previous section. An example of the recovered image obtained by stacking the two resulting shares together is shown in Figure 1(c). The original secret image size was 512×512, whereas the shares and recovered image sizes are 1024×1024, hence this gives a pixel expansion of $m = 4$.

3 Related Work

The VCS defined in the previous section is referred to as a deterministic VCS, because reconstruction of the secret pixels is guaranteed. A probabilistic visual cryptography scheme (probVCS) was presented by Yang [14], where each pixel in the original image is represented using a single pixel in the image that is reconstructed from the shares, thus giving rise to a scheme with no pixel expansion. A similar size invariant VCS was previously proposed by Ito et al. [7].

The main characteristic of the probabilistic scheme is that there is no guarantee that each pixel in the recovered image accurately represents the actual pixel from the original secret image. This is because a black pixel in the original secret image may be incorrectly represented, with a certain probability, as a white pixel in the reconstructed image, and vice versa. This presents a trade off between pixel expansion and the accuracy of the recovered image. Cimato et al. [3] generalized Yang's [14] model and showed that it is possible to trade pixel expansion for the probability of a good reconstruction.

Chen et al. [2] proposed a method that maps a block of pixels in the original grayscale secret image into a block of the same size in each share. They presented two techniques based on histogram width-equalization and histogram depth-equalization to generate corresponding share blocks with multiple levels, each containing different black and white pixel densities, rather than just two levels as implemented in traditional visual cryptography. However, their method is only able to handle the special case of a (n, n)-VCS. Wu et al. [13] in turn developed a histogram approach for color images, which provides a tunable feature that allows the user to control the quality of the recovered image.

Hou and Tu [6] introduced a VCS based on a method of encoding multiple pixels simultaneously. In their approach, a number of successive white or black pixels are taken as a unit of encryption. The probability that these pixels will be encrypted as black pixels depends on the ratio of black pixels in the basis matrices. However, Liu et al. [10] suggested that the method proposed in Hou and Tu [6] has a security defect, where a participant may see the contour of the secret image only by viewing the image of his/her own share. In their paper, they proposed two other multi-pixel VCS encryption methods that attempt to improve the visual quality by reducing the variance in the recovered image. They argue that a smaller variance gives rise to better visual quality especially in terms of the evenness of the pixel distribution in the recovered image. They further suggest that since black pixels can be recovered perfectly, to obtain good visual quality for the recovered image the secret image should have a black background. Therefore, they suggest thresholding a grayscale image into a black and white image first before applying the multi-pixel VCS. Ito et al. [7] have previously made a similar observation for encrypting color images, where white pixels can perfectly be recovered.

4 Image Filtering

In view of the fact that the aim of visual cryptography is for the human visual system to decrypt the superimposed shares, it is conceivable that the perceived visual quality of the recovered image can be improved by performing image filtering prior to encryption. Yang and Chen [15] observed that since the contrast of a recovered image is poor, it is possible to prioritize certain 'more important' pixels during the encryption. They proposed a size reduced VCS, in which they performed edge detection on the secret image to identify important pixels, as these edge pixels give the most meaningful information about the image. Once identified, the important pixels and less important pixels are given different pixel expansions during encryption. As such, the size of the resulting shares is smaller than that of the traditional size expanded VCSs.

Instead of performing edge detection, we propose a method to enhance the perceive edges by passing the secret image through a sharpening filter. This has the effect of increasing the local contrast at discontinuities in the image, which have distinct gray-levels, hence making it easier to perceive edges in the image. To the human visual system, the resulting image appears sharper. For this we apply a Laplacian operator using a 3×3 kernel. Figure 2(a) shows the image produced by

(a) (b) (c)

Fig. 2. Example of how the perceived visual quality of a VCS can be improved using an image sharpening technique. (a) Image after sharpening; (b) Dithered image; (c) Recovered image.

applying this sharpening filter to the secret image previously shown in Figure 1(a). The dithered image, after sharpening, is shown in Figure 2(b). This image was then encrypted using the Naor-Shamir (2, 2)-VCS into two separate shares, and the image recovered by superimposing the two shares is shown in Figure 2(c). By comparing this recovered image with the image in Figure 1(c), one can see an improvement in the perceived visual quality of the resulting image.

In addition to an image sharpening filter, which increases the local contrast at discontinuities, the global contrast of the secret image can also be enhanced using histogram equalization. In general, a grayscale image has 256 possible intensity values. An image histogram can be constructed to represent the intensity distribution of the pixels in an image over these values. Histogram equalization is a technique that can be used to spread the image intensity to cover the full $0-255$ range of values. For images that do not cover the full range of values, histogram equalization effectively increases the global contrast of an image.

The complete overall process taken to enhance the perceived visual quality of the resulting recovered image is listed as follows:

1. Perform histogram equalization
2. Pass the resulting image through a sharpening filter
3. Dither the image produced from the previous step
4. Apply a VCS

This full process is illustrated in Figure 3. Figure 3(a) shows the secret image along with its corresponding histogram. In a histogram the horizontal axis represents the intensity values and the vertical axis represents the number of pixels for each intensity value. Histogram equalization is performed on the secret image and the resulting image, and its histogram, are shown in Figure 3(b). One can observe the enhancement in the global image contrast. The image is then passed through a sharpening filter, resulting in the image shown in Figure 3(c). This image is then dithered to get an image with only black and white pixels, shown in Figure 3(d). The dithered image was then encrypted using the Naor-Shamir (2, 2)-VCS, and Figure 3(e) shows the image recovered by superimposing the two shares.

One can see a difference in the visual quality of the recovered image by comparing the images shown in Figure 1(c), Figure 2(c) and Figure 3(e). The details in the image can be perceived more clearly in the recovered image obtained using the described image filtering techniques. Admittedly, passing the secret image through these image filters effectively modifies the original image. Nevertheless, since the primary goal of visual cryptography is for the human visual system to be able to perceive the recovered image, enhancing the visual quality in this manner certainly achieves that objective.

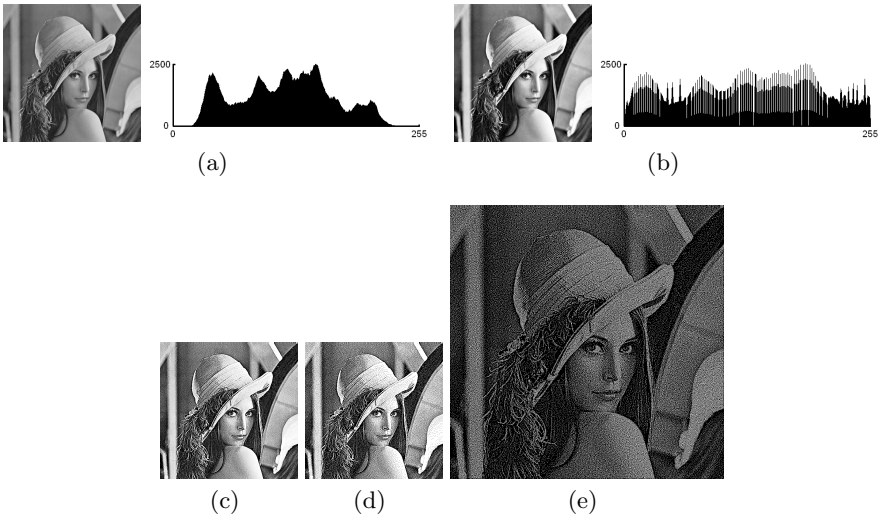

Fig. 3. Enhancing the perceived visual quality of a VCS via image filtering techniques. (a) Secret image and its corresponding histogram; (b) Image resulting from histogram equalization and its histogram; (c) Image produced after passing it through a sharpening filter; (d) Dithered image; (e) Recovered image.

5 Block Threshold Visual Cryptography

In this section, we propose a VCS that encrypts blocks containing multiple pixels. The aim of this approach is to preserve the relative density of local neighboring pixels in a recovered image. Probabilistic VCSs produce shares with no pixel expansion by encrypting individual pixels as either black or white in a probabilistic manner. However, since each pixel is treated independently, there is no guarantee that density of pixels within small areas in the recovered image is accurate. As such, the recovered image looks rather noisy. By proposing a scheme that encrypts blocks of pixels based on the density of the pixels within the block, this maintains the relative density of pixels within the block, thereby improving the perceived visual quality of the recovered image.

The proposed VCS is built from the same basis matrices, C_0 and C_1, as the traditional (k, n)-VCS. However, instead of performing encryption on a per pixel basis, in this scheme encryption is performed by taking a multi-pixel block as a unit of encryption. The block size contains the same number of pixels, m, as in the traditional (k, n)-VCS. If the total number of black pixels within the block is greater than a certain threshold, the corresponding block of pixels in the shares are encrypted using the pixel configuration representing a black pixel block, which is randomly chosen from the collection of C_1 matrices with equal frequencies. On the other hand, if the total number of black pixels within the block is less than, or equal to, the threshold, then the corresponding block of pixels in the shares are encrypted using the pixel configuration representing a white pixel block, which is randomly chosen from the collection of C_0 matrices with equal frequencies. The adopted threshold for determining whether a block should be encrypted as a white or black pixel block, is half the total number of pixels within the block, i.e. $\frac{m}{2}$. We will refer to this as the Block Threshold Visual Cryptography Scheme (BTVCS) and is defined as follows:

Construction. (k, n)-BTVCS. *Let* k, n, m *and* t *be non-negative integers which satisfy* $2 \leq \mathrm{k} \leq \mathrm{n}$ *and* $0 \leq \mathrm{t} \leq \mathrm{m}$. *Let* C_0 *and* C_1 *be two collections of* n×m *basis matrices corresponding to white and black pixel configurations for a traditional* (k, n)-VCS*, with* n *being the number of shares and* m *being the pixel expansion. For each block of* p×q *pixels in the secret image, where the number of pixels in* p×q *is equal to* m*, let* t *be the total number of black pixels within the block. If* $\mathrm{t} \leq \frac{m}{2}$*, encrypt the corresponding block in the* n *shares as a 'white' pixel block by randomly selecting a matrix from* C_0*. Otherwise, encrypt the corresponding block in the* n *shares as a 'black' pixel block by randomly selecting a matrix from* C_1*.*

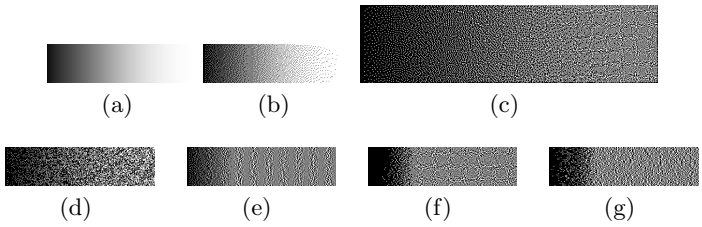

Fig. 4. Results of various (2, 2)-VCSs on a gradient image. (a) Gradient image; (b) Dithered gradient image; (c) The traditional VCS with pixel expansion; (d) probVCS; (e) BTVCS with block dimensions of 1x2; (f) BTVCS with block dimensions of 2x2; (f) BTVCS with block dimensions of 1x4.

Since BTVCS is built from the same basis matrices as the traditional VCS, the contrast and security conditions are also the same. In a sense, BTVCS can be seen as the image being reconstructed using large pixels (i.e. the pixel configuration obtained from the basis matrices used to represent white and black pixel blocks) as its basic building components. From an image processing point of view, this is somewhat similar to reducing the resolution of an image whilst maintaining its image size. The relative perceived density of the local neighboring pixels is maintained, whilst the image resolution is reduced.

The dimensions of the block of pixels, $p \times q$, should ideally be as close to a square as possible given the number of pixels m. For example, for at (2, 2)-BTVCS the pixel configurations can take the form of a 1×2 block using the following collections of basis matrices, where $m = 2$:

$C_0 = \{\text{all matrices obtained by permutating the columns of } \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}\}$

$C_1 = \{\text{all matrices obtained by permutating the columns of } \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\}$

A (2, 2)-BTVCS can also be constructed using the pixel configurations obtained from the collections of basis matrices previously presented in Section 2.1, where $m = 4$. In this case, the block pixel configuration can either be a 2×2 or a 1×4 pixel block. However, using the dimensions of 2×2 will produce better visual results as shown in the section to follow.

6 Results and Discussions

To illustrate the end result of performing encryption using different VCSs, Figure 4 shows comparisons between the resulting recovered images for a gradient image obtained by applying various VCSs. The gradient image, where the gray-levels smoothly transition from black to white, is shown in Figure 4(a) with its corresponding dithered image shown in Figure 4(b). Figure 4(c) shows the result of Naor and Shamir's traditional (2, 2)-VCS which has pixel expansion. Figure 4(d) in turn shows Yang's [14] size invariant (2, 2)-probVCS. Figures 4(e), 4(f) and 4(g) were obtained using (2, 2)-BTVCS with block dimensions of 1×2, 2×2 and 1×4 respectively.

From the figures, it can be seen that Naor and Shamir's traditional VCS and Yang's probVCS are better at capturing the overall range of intensity values. However, the former has pixel expansion and the later gives the appearance of more noise as compared to the BTVCS approach. BTVCS with block size of $m = 4$ gives rise to higher contrasting regions compared to with $m = 2$. Also, in comparing BTVCS with pixel blocks of 2×2 and 1×4, it can be seen that for the 1×4 case there are some undesirable streaks of white in the darker areas. This is because if m pixels are encrypted in a single row, there will be cases where all the black (resp. white) pixels are all located on one side of the block. This effect becomes more prominent with increasing block sizes. Hence, the reason why block pixel dimensions $p \times q$, should ideally be as close to a square as possible.

Figure 5 shows the results of the size invariant schemes on the secret image that was previously shown in Figure 1(a). Figure 5(a) shows recovered images resulting from the (2, 2)-BTVCS with

block dimensions of 1×2. Figure 5(b) in turn shows recovered images resulting from the (2, 2)-BTVCS with block dimensions of 2×2. This is followed by Figure 5(c) which shows recovered images resulting from the (2, 2)-BTVCS with block dimensions of 1×4. Finally, Figure 5(d) shows recovered images resulting from Yang's [14] (2, 2)-probVCS.

In general, it can be seen from the recovered images that the perceived visual quality is improved when the secret image is enhanced using the image filtering techniques, as the details in the image can be seen more clearly. In addition, the overall density of pixels in the recovered images using BTVCS are more evenly distributed and give rise to a better visual appearance, compared to the random pixel density of probVCS, which appears to be rather noisy. Similar observations that encrypting multiple pixels produce more evenly distributed pixels in recovered image have also been made in the multi-pixel schemes proposed by Hou and Tu [6] and Liu et al. [10]. Of the different BTVCS block dimensions, using a block size of $m = 4$ results in recovered images with higher contrast between light and dark regions. Also, ideally the dimensions should form a block that is as close to a square as possible. Otherwise, undesirable white stretches may occur in the darker regions.

7 Conclusion

This paper addresses the issue of visual quality in the recovered image and the problem of pixel expansion in the resulting shares, which are two major concerns in visual cryptography. We show that before performing dithering, the local and global contrasts of the image can first be enhanced to improve the resulting recovered visual cryptography image. In addition, we proposed a size invariant VCS that encrypts pixel blocks using a thresholding approach to maintain the local density of pixels in the recovered image. Since the goal of visual cryptography is for the human visual system to decrypt the hidden information, these image filtering techniques together with our size invariant VCS successfully enhances the resulting visual quality of the recovered image.

References

1. G. Ateniese, C. Blundo, A. D. Santis, and D. R. Stinson. Visual cryptography for general access structures. *Inf. Comput.*, 129(2):86–106, 1996.
2. Y.-F. Chen, Y.-K. Chan, C.-C. Huang, M.-H. Tsai, and Y.-P. Chu. A multiple-level visual secret-sharing scheme without image size expansion. *Inf. Sci.*, 177(21):4696–4710, 2007.
3. S. Cimato, R. D. Prisco, and A. D. Santis. Probabilistic visual cryptography schemes. *Comput. J.*, 49(1):97–107, 2006.
4. S. Cimato and C. Yang. *Visual cryptography and secret image sharing.* Digital Imaging and Computer Vision Series. Taylor & Francis, 2011.
5. R. W. Floyd and L. Steinberg. An adaptive algorithm for spatial greyscale. *Proceedings of the Society of Information Display*, 17:75–77, 1976.
6. Y.-C. Hou and S.-F. Tu. A visual cryptographic technicque for chromatic images using multi-pixel encoding method. *Journal of Research and Practice in Information Technology*, 37(2), 2005.
7. R. Ito, H. Kuwakado, and H. Tanaka. Image size invariant visual cryptography. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, 82(10):2172–2177, 1999.
8. B. W. Leung, F. Y. Ng, and D. S. Wong. On the security of a visual cryptography scheme for color images. *Pattern Recognition*, 42(5):929–940, 2009.
9. C.-C. Lin and W.-H. Tsai. Visual cryptography for gray-level images by dithering techniques. *Pattern Recognition Letters*, 24(1-3):349–358, 2003.
10. F. Liu, T. Guo, C. K. Wu, and L. Qian. Improving the visual quality of size invariant visual cryptography scheme. *J. Visual Communication and Image Representation*, 23(2):331–342, 2012.
11. M. Naor and A. Shamir. Visual cryptography. In *EUROCRYPT*, pages 1–12, 1994.
12. S. J. Shyu. Image encryption by random grids. *Pattern Recognition*, 40(3):1014–1031, 2007.
13. X. Wu, D. S. Wong, and Q. Li. Threshold visual cryptography scheme for color images with no pixel expansion. In *Proceedings of the Second Symposium International Computer Science and Computation Technology*, pages 310–315, 2009.

Fig. 5. Recovered images resulting from different techniques. Left image: with dithering only. Center image: with sharpening and dithering. Right image: with histogram equalization, sharpening and dithering. (a) (2, 2)-BTVCS with block dimensions of 1x2; (b) (2, 2)-BTVCS with block dimensions of 2x2; (c) (2, 2)-BTVCS with block dimensions of 1x4; (d) (2, 2)-probVCS.

14. C.-N. Yang. New visual secret sharing schemes using probabilistic method. *Pattern Recognition Letters*, 25(4):481–494, 2004.
15. C.-N. Yang and T.-S. Chen. Visual secret sharing scheme: Improving the contrast of a recovered image via different pixel expansions. In A. C. Campilho and M. S. Kamel, editors, *ICIAR (1)*, volume 4141 of *Lecture Notes in Computer Science*, pages 468–479. Springer, 2006.