Chapter 37
Visual Cryptography Based on Optical Image Projection

Rita Palivonaite, Algiment Aleksa and Minvydas Ragulskis

Abstract A visual cryptography scheme based on optical image projection is proposed in this paper. Initially the secret image is split into two shares. Then, such digital images are constructed in share's planes that their projections in the projection screen would correspond to each of the appropriate shares. Geometrical parameters describing the location of shares' planes and focus points of projectors are additional security parameters of the encoded image. Direct overlapping of the reconstructed shares does not leak any information on the encrypted image. The original image can be interpreted by a naked eye when appropriate projectors are placed at predefined locations of the geometrical setup.

37.1 Introduction

Visual cryptography is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that the decryption can be performed by the human visual system, without the aid of computers. Visual cryptography was pioneered by Naor and Shamir in 1994 [1]. They demonstrated a

R. Palivonaite (✉) · A. Aleksa · M. Ragulskis
Research Group for Mathematical and Numerical Analysis of Dynamical Systems, Department of Mathematical Research in Systems, Kaunas University of Technology, Studentu 50-222, LT-51638 Kaunas, Lithuania
e-mail: rita.palivonaite@ktu.lt

A. Aleksa
e-mail: algiment.aleksa@ktu.lt

M. Ragulskis
e-mail: minvydas.ragulskis@ktu.lt

K. Elleithy and T. Sobh (eds.), *Innovations and Advances in Computer, Information, Systems Sciences, and Engineering*, Lecture Notes in Electrical Engineering 152,
DOI: 10.1007/978-1-4614-3535-8_37,

visual secret sharing scheme, where an image was broken up into n shares so that only someone with all n shares could decrypt the image, while any $n-1$ shares revealed no information about the original image. Each share was printed on a separate transparency, and decryption was performed by overlaying the shares. When all n shares were overlaid, the original image would appear.

Since 1994, many advances in visual cryptography have been done. Extended visual cryptography is presented in [2]. Four—share visual cryptography scheme for color images is proposed in [3]. A Visual Cryptography (VC)-based system for sharing multiple secret images is developed in [4]. Visual cryptography schemes are defined and analyzed for grey level images whose pixels have g grey levels ranging from 0 to 1 are presented in [5]. Colored visual cryptography without color darkening is proposed in [6]. Cheating prevention in visual cryptography is developed in [7]. Visual cryptography schemes with optimal pixel expansion are introduced in [8]. Image encryption by random grids is presented in [9]. A new method of producing multicolored share images based on visual cryptography is proposed in [10]. A novel technique named halftone visual cryptography is proposed to achieve visual cryptography via halftoning [11]. Colored visual cryptography scheme based on additive color mixing is presented in [12].The best pixel expansion of various models of visual cryptography schemes is investigated in [13]. A new definition of the contrast of the visual cryptography is proposed in [14]. General construction of extended visual cryptography schemes is proposed in [15]. A high contrast and capacity efficient visual cryptography scheme for the encryption of multiple secret images is introduced in [16]. Image encryption by multiple random grids is presented [17].

We propose a modification of the classical visual cryptography scheme when each share has to be projected on the screen. We exploit the principle of the projection moiré technique [18] when an image projected on to the projection plane undergoes non-affine transformations (if only the projection angle is not perpendicular to the projection plane). The proposed method requires n projectors (if the original image is broken into n shares). Each of the projectors must project its share on the screen at the predefined geometrical location (projection angles for each projector can be different). Without loss of generality we will describe the method when the original image is broken into 2 shares only.

Each share is constructed in such a way that its projection (at strictly predefined geometrical parameters of the projector) would result into a projected image of a share which can be used to visualize the original secret image. Someone who has all shares can decrypt the secret image only if he knows how to project all these shares. Direct overlaying of n transparent shares (or projection of at least one of the shares at a wrong angle) would not leak any information about the secret image. Such an encryption technique can be considered as a visual cryptography scheme with additional security protection.

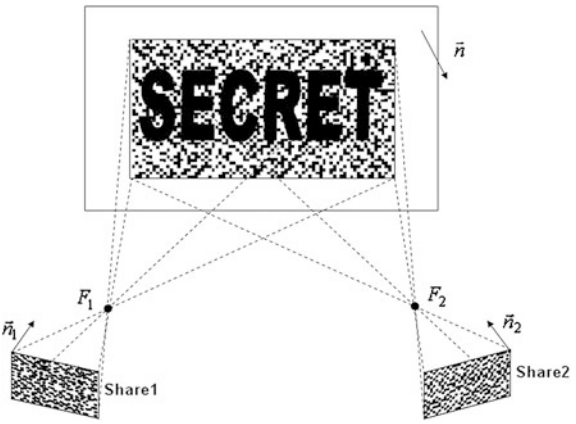

Fig. 37.1 A schematic diagram illustrating the principle of visual cryptography based on the projection technique

37.2 Description of the Projection Technique

As mentioned previously, we will use 2 shares to illustrate the proposed visual cryptography method based on projection techniques. The basic principle of the method is illustrated in Fig. 37.1. Two shares are projected on the projection plane; every share is located at a different position in the 3D space. Coordinates of focal points and the geometrical location of each share determine unique locations of each of projectors. The secret image appears on the projection plane when both shares are projected appropriately. It should be noted that Fig. 37.1 is only a schematic diagram. We do not show geometrical deformations of the projected rectangular images; exact geometrical locations of the projection plane and two shares are determined not only by their normal vectors. In fact, one has to solve an inverse problem of an image construction. One has to construct a share given a structure of the projected share and geometrical parameters of the projector.

Initially we assume that the equation of the projection plane is $z = 0$; $n = (0; 0; 1)$. As mentioned previously, a projected image on the projection plane must form a matrix of dots (it is assumed that a pixel is smaller object than a dot). Since we consider a classical visual cryptography scheme, every element of the projected matrix can be described as

$$\boldsymbol{M}_1(i, j) \in \{0; 1\}; \quad i = 1, 2, \ldots, r_1; \quad j = 1, 2, \ldots, r_2 \tag{37.1}$$

where $\boldsymbol{M}_1$ is the projection of the Share 1; r_1 and r_2 define the resolution of the visual cryptography scheme. The numerical value 0 corresponds to the black color; 1 corresponds to the white color (all intermediate values would correspond to appropriate grayscale colors). Similarly, both shares are also represented as matrixes of dots.

Lets assume that the origin of the 3D frame is a point $O(0; 0; 0)$; coordinates of the focus point are $F_1(f_x; f_y; f_z)$; $n_1 = (n_x; n_y; n_z)$; the equation of the first share's

plane is $n_x x + n_y y + n_z z = p$ (p is such that the focus point is between the share and the projection plane).

The first step is the selection of a local 2D frame in the share's plane. This is necessary because a share needs not only to be placed in a correct plane, but also rotated around its normal vector up to a correct angle. Initially, the origin of the 2D local frame O_1 is set as an intersection point between the line F_1O and the share's plane: $O_1\left(-t_O \cdot f_x + f_x; -t_O \cdot f_y + f_y; -t_O \cdot f_z + f_z\right)$, where $t_O = \frac{p - n_x f_x - n_y f_y - n_z f_z}{-n_x f_x - n_y f_y - n_z f_z}$. Next, images of points $A(1;0;0)$ and $B(0;1;0)$ are computed in the share's plane and denoted as A_1 and B_1. Then, base vectors of the local 2D frame in the share's plane are denoted as:

$$\mathbf{i}_1 = \frac{\mathbf{O_1A_1}}{|\mathbf{O_1A_1}|}; \mathbf{j}_1 = \frac{\mathbf{O_1B_1}}{|\mathbf{O_1B_1}|} \tag{37.2}$$

Elementary transformations yield:

$$\begin{aligned} i_1 &= \frac{\left(t_A(1-f_x) + t_O f_x; -t_A f_y + t_O f_y; -t_A f_z + t_O f_z\right)}{\sqrt{\left(t_A(1-f_x) + t_O f_x\right)^2 + \left(-t_A f_y + t_O f_y\right)^2 + \left(-t_A f_z + t_O f_z\right)^2}}; \\ j_1 &= \frac{\left(-t_B f_x + t_O f_x; t_B\left(1-f_y\right) + t_O f_y; -t_B f_z + t_O f_z\right)}{\sqrt{\left(-t_B f_x + t_O f_x\right)^2 + \left(t_B\left(1-f_y\right) + t_O f_y\right)^2 + \left(-t_B f_z + t_O f_z\right)^2}}; \end{aligned} \tag{37.3}$$

where,

$$t_A = \frac{p - n_x f_x - n_y f_y - n_z f_z}{n_x(1-f_x) - n_y f_y - n_z f_z};$$
$$t_B = \frac{p - n_x f_x - n_y f_y - n_z f_z}{-n_x f_x + n_y\left(1-f_y\right) - n_z f_z}$$

It can be noted that vectors $\mathbf{i}_1$ and $\mathbf{j}_1$ are not necessarily orthogonal. The next step is the construction of an image of a dot from the projection plane in the share's plane. In general, computation of coordinates of an image point in a 2D local frame in the share's plane involves solution of a linear algebraic system of equations. Let coordinates of a point in the projection plane are $C(x;y;0)$. Then, coordinates of its image point in the share's plane are $C_1(t_C(x-f_x) + f_x; t_C\left(y-f_y\right) + f_y; -t_C f_z + f_z)$ where $t_C = \frac{p - n_x f_x - n_y f_y - n_z f_z}{n_x(x-f_x) + n_y\left(y-f_y\right) - n_z f_z}$. Now, a vector $\mathbf{O_1C_1}$ has to be expressed in a linear combination of base vectors $\mathbf{i}_1$ and $\mathbf{j}_1$:

$$\mathbf{O_1C_1} = c_x \cdot \mathbf{i}_1 + c_y \cdot \mathrm{j}_1 \tag{37.4}$$

where c_x and c_y are 2D coordinates of the point C_1 in the share's plane. It can be noted that Eq. (37.4) produces 3 linear algebraic equations. One of these equations can be omitted (or used as a criterion for checking if the point C_1 is exactly mapped on the share's plane). Other two equations can be used for determination of c_x and c_y (we omit details for brevity):

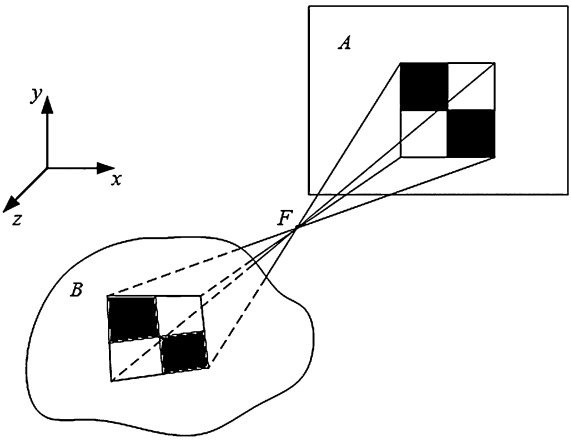

Fig. 37.2 A schematic diagram representing of the construction of the images in the share plane; *A* stands for the projection plane; *F* is the focus point; *B* is the share plane. Note that only one share plane is shown

$$\begin{cases} i_x c_x + j_x c_y = t_C(x - f_x) + t_O f_x; \\ i_y c_x + j_y c_y = t_C(y - f_y) + t_O f_y. \end{cases} \tag{37.5}$$

Reconstruction of a point's local coordinates in the second share's plane is analogous to the procedure described above. As mentioned previously, a dot can be comprised from many pixels (this is determined by the resolution of the projected image). A schematic diagram of the image computation process is presented in Fig. 37.2. A set of four black and white dots in the projection plane *A* is shown at the top of Fig. 37.2; the corresponding image in projected through the focus point *F* into the share plane *B*. Note that only one share plane is illustrated in Fig. 37.2; the splitting rule is a standard random scheme used in classical visual cryptography [1].

37.3 The Construction of Images in the Share Plane

The construction of digital image in the share plane is not a straightforward task simply due to fact that the image in the share plane *B* is skewed in respect of the orthogonal matrix of pixels in the share image (Fig. 37.2). It is clear that the proposed system of visual cryptography will not work if the size of a pixel in the share plane is comparable to the size of a projected dot in the projection plane.

The algorithm for the computation of grayscale levels of pixels in the share plane is illustrated in Fig. 37.3. The shape of the inclined grid of dots in the share plane is illustrated in Fig. 37.3a. Note that the projected grid in the projection plane is rectangular and corresponds to the position of pre-defined dots (Fig. 37.2). The size of pixels in the share plane is illustrated by the dashed grid in Fig. 37.3a. The computational procedure for the reconstruction of the grayscale level at the pixel in the *i*th row and the *j*th column in the share plane is explained in Fig. 37.3b.

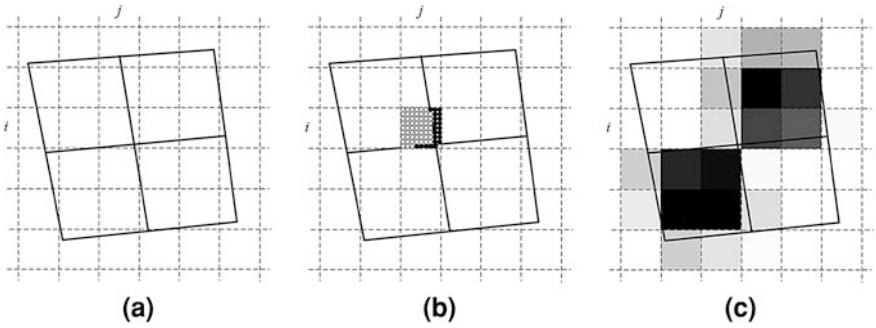

Fig. 37.3 A schematic diagram representing of the reconstruction of the grayscale levels of pixels in the share plane; the size of pixels in the share plane is denoted by dashed grid. The inclined grid corresponding to the projected image in the projected plane is shown in (**a**). The algorithm for the computation of the grayscale level at the $i-j$th pixel is illustrated in (**b**). The reconstructed image in the share plane is shown in (**c**). Note that only one share plane is shown

We cover the surface of the $i-j$th pixel in the share plane by a rectangular matrix of points. Every point of this matrix is projected to the projection plane.

A point is marked by an empty circle in Fig. 37.3b if the coordinates of the projected point in the projection plane correspond to a white dot. Analogously, a point is marked by a black circle if the projected point is located inside a black dot in the projection plane.

Now, the grayscale level g_{ij} at the $i-j$th pixel is computed according to the equation:

$$g_{ij} = \text{round}\left(255\frac{w_{ij}}{n}\right) \tag{37.6}$$

where w_{ij} is the number of white points and n is the total number of points in the area occupied by the $i-j$th pixel in the share plane.

The reconstructed grayscale digital image is shown in Fig. 37.3c. It is clear that the quality of the projected image is directly related to the size of a pixel in the share plane.

The effect of the pixel size in the share plane to the quality of the image in both share planes is illustrated in Fig. 37.4. We show the digital images in the share plane (left columns in Fig. 37.4) and the projected images to the projection plane (right columns in Fig. 37.4). The quality of digital images in the share plane depends on the ratio between the size of the dot in the projection plane and the size of the pixel in the share plane; *A* stands for the ratio 2:1; *B* stands for the ratio 5:1; *C*—10:1; *D*—20:1 and *E*—50:1.

It is clear that it is pointless to discuss a visual cryptography scheme based on projected images if one cannot reproduce a realistic image in the projection plane. Our computations show that at least 50×50 pixels in the share plane should correspond to one dot in the projection plane. Moreover, the quality of the

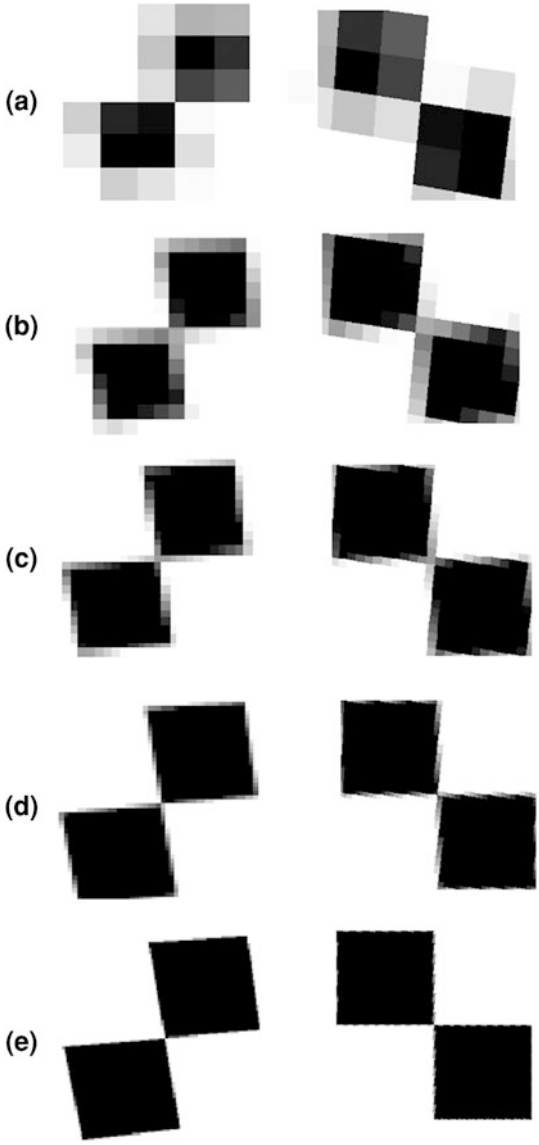

Fig. 37.4 The quality of digital image in the share plane depends on the ratio between the size of the dot in the projection plane and the size of the pixel in the share plane. The left column shows the image in the share plane; the right column—the projected image in the projection plane. The angle of projection $s = 0.01$

projected image depends of the geometrical set-up. The more inclined is the angle of the projection the higher must be the ratio between the size of the dot in the projection plane and the size of the pixel in the share plane.

It is possible to assess the quality of the projected image by comparing the original image (Fig. 37.2a) and the projected image (images in the right column in Fig. 37.4). We use root mean square error estimate (RMSE) and plot these errors as a function from the angle of projection s (Fig. 37.5).

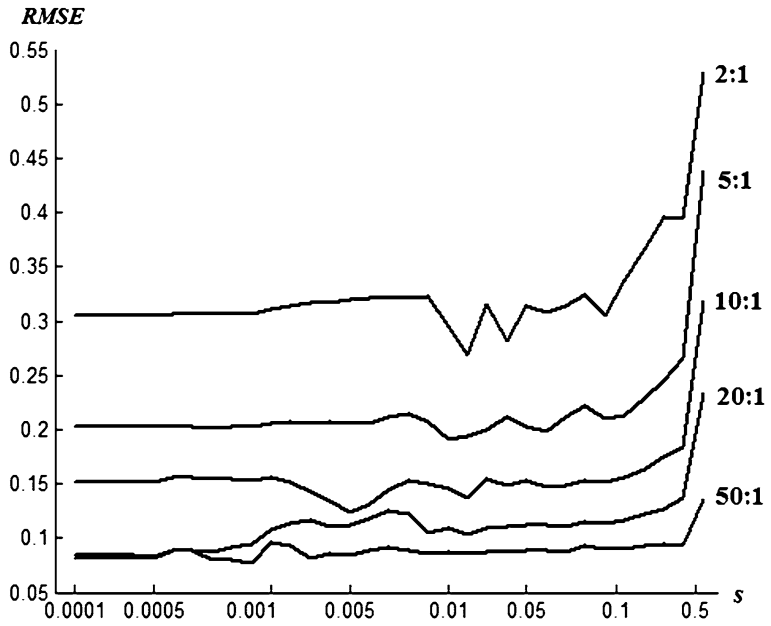

Fig. 37.5 The relationship among the ratio between the size of the dot in the projection plane and the size of the pixel in the share plane, the angle of projection s and the RMSE of the projected image

It can be seen that RMSE errors depend both on the ratio between the sizes of dots but also on the projection angle s. The general recommendation is to select larger dots in the projection plane if the projection angle is rather inclined.

37.4 Computational Experiments

Initially we use a classical cryptography scheme to split a digital image (three letters KTU) into two shares. Both shares are shown in Fig. 37.6a and Fig. 37.6b. Direct geometrical superposition yields an image which can be interpreted by a naked eye (Fig. 37.6c). It can be noted that inaccurate superposition of two shares prevents visual interpretation of the encoded image.

The next step is the construction of such digital images in shares' planes that their projected images would coincide with original shares shown in Fig. 37.6a and Fig. 37.6b. This is an inverse problem of image construction described in the previous section.

Following parameters of the geometrical setup were selected for computational experiments: $F_1 = (0; 0; 10)$; $F_2 = (0; 4; 10)$; $n_1 = (-s; s; -1)$; $n_2 = (s; -s; -1)$; distance between the plane of the share 1 and F_1 is equal to 10; distance between the plane of the share 2 and F_2 is also equal to 10; the width of the secret image is

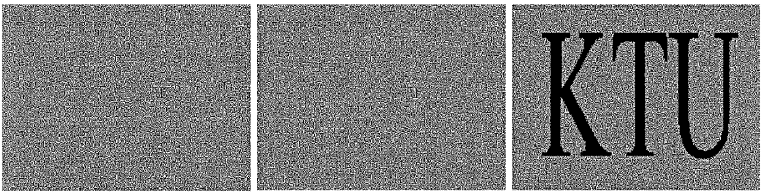

Fig. 37.6 Illustration of a classical visual cryptography: **a**, **b** show two shares in the projection plane; **c** exact geometrical superposition of both shares in the projection plane produces the secret image

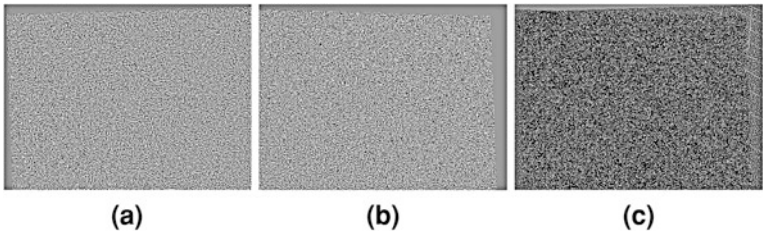

Fig. 37.7 Reconstructed images of share 1 (**a**) and share 2 (**b**); direct geometrical superposition of share 1 and share 2 does not reveal the secret image (**c**)

4 units; the height is 3 units. Reconstructed images of share 1 and share 2 at $s = 0.1$ are shown in Fig. 37.7a, b.

As mentioned previously, projections of share 1 and share 2 in the projection plane should correspond to digital images in Fig. 37.6a, b. But nonlinear transformations occurring during the process of projection and described in the previous section cause the appearance of parasitic moiré patterns in the superposed image in the projection plane (Fig. 37.8a, b).

Reconstructed images of shares in their planes can be considered as a next security level in a visual cryptography scheme. Direct superposition of these shares prevents visual interpretation of the encrypted image, which becomes observable only when shares' planes become almost parallel to the projection plane (Fig. 37.9c).

37.5 Concluding Remarks

A classical visual cryptography scheme is extended by introducing projection effects which distort original shares when they are projected on the surface of a projection plane. Such extensions can be considered as a next step in the security level of the image encryption. Both shares are constructed in such a way that their

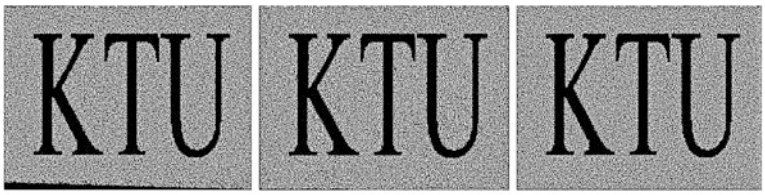

Fig. 37.8 Projected and superposed images of share 1 and share 2 in the projection plane; normal vectors of the shares' planes are $n_1 = (-s; s; -1)$; $n_2 = (s; -s; -1)$; **a** at $s = 0.1$; **b** at $s = 0.01$; **c** at $s = 0.0001$

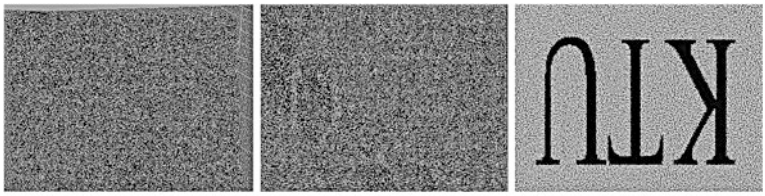

Fig. 37.9 Direct geometrical superposition of share 1 and share 2; **a** at $s = 0.1$; **b** at $s = 0.01$; **c** at $s = 0.0001$

projections would coincide with the original shares of the encoded image (at strictly defined geometrical parameters of the projection scheme). Distortions occurring during the construction of both shares damage the allocation of appropriate pixels and thus direct overlapping of both shares cannot leak any information about the encoded image.

We have used a simplified geometrical projection scheme. In practice (if a CCD projector is used to project an image on the screen) one should take care of distortions caused by non-ideal lenses. Also one should consider the effect of the depth of the projection's focus on the screen, especially if the projection angle is high and the projector is far from the screen.

The proposed image sharing scheme is still a visual cryptography scheme. Computational algorithms are necessary to construct the shares, but visualization does not require a computer; this is a completely visual process. But one needs to place two projectors with high accuracy in reference to the projection screen, instead of simply overlapping two shares.

Finally, it can be noted that the proposed scheme can be extended to an n shares scheme, halftone or even color visual projection cryptography schemes.

References

1. Naor M, Shamir A (1995) Visual cryptography. LNCS 950:1–12
2. Nakajima M, Yamaguchi Y (2002) Extended visual cryptography. In: Conference Proceedings 10th international conference on computer graphics, visualization and computer vision, vols I and II, University of West, Bohemia pp 303–310
3. Leung BW, Ng FY, Wong DS (2009) On the security of a visual cryptography scheme for color images. Pattern Recogn 42(5):929–940
4. Chen SK (2007) A visual cryptography based system for sharing multiple secret images. In: Proceedings of the 7th WSEAS international conference on signal processing, computational geometry and artificial vision (ISCGAV'-07) pp 113–118
5. Blundo C, De Santis A, Naor M (2000) Visual cryptography for grey level images. Inform Process Lett 75(6):255–259
6. Cimato S, De Prisco R, De Santis A (2007) Colored visual cryptography without color darkening. Theoret Comput Sci 374(1–3):261–276
7. Hu SM, Tzeng WG (2007) Cheating prevention in visual cryptography. IEEE Trans Image Process 16(1):36–45
8. Blundo C, Climato S, De Santis A (2006) Visual cryptography schemes with optimal pixel expansion. Theoret Comput Sci 369(1):169–182
9. Shyu SH (2007) Image encryption by random grids. Pattern Recogn 40(3):1014–1031
10. Wu HC, Wang HC, Tsai CS (2006) Multiple image sharing based on colour visual cryptography. Imaging Sci J 54(3):164–177
11. Shou Z, Arce GR, Di Crescenzo G (2006) Halftone visual cryptography. IEEE Trans Image Process 15(8):2441–2453
12. Yang CN, Chen TS (2008) Colored visual cryptography scheme based on additive color mixing. Pattern Recogn 41(10):3114–3129
13. Hajiabolhassan H, Cheraghi A (2010) Bounds for visual cryptography schemes. Discret Appl Math 158(6):659–665
14. Liu F,Wu CK, Lin XJ () A new definition of the contrast of visual cryptography scheme. Inform Process Lett 110(7):241–246
15. Wang D, Yi F, Li X (2009) On general construction for extended visual cryptography schemes. Pattern Recogn 42(11):3071–3082
16. Lee KH, Chiu PL (2011) A high contrast and capacity efficient visual cryptography scheme for the encryption of multiple secret images. Optics Commun 284(12):2730–2741
17. Shyu SJ (2009) Image encryption by multiple random grids. Pattern Recogn 42(7):1582–1596
18. Kobayashi AS (1993) Handbook on experimental mechanics, 2nd edn. Bethel, SEM