A Visual Cryptographic Technique for Chromatic Images Using Multi-pixel Encoding Method

Young-Chang Hou
Department of Information Management
Tamkang University
151 Ying-Chuan Road, Tamshui, Taipei County 251, Taiwan, R.O.C.
TEL: +886-2-2621-5656 ext. 3514 FAX: +886-2-2620-9737
Email: ychou@mail.im.tku.edu.tw

Shu-Fen Tu
Department of Information Management
Chao Yang University of Technology
No. 168, Jifong E. Rd., Wufong Township, Taichung County 413, Taiwan, R.O.C.
TEL: +886-4-233-23000 ext. 4761
Email: ariel_tu@anet.net.tw

Visual cryptography is a secret sharing method that uses human eyes to decrypt the secret. Most visual cryptographic methods utilize the technique of pixel expansion, which causes the size of the shares to be much larger than that of the secret image. This situation is more serious for grey-level and chromatic images. In this paper, we propose a multi-pixel encoding method for grey-level and chromatic images without pixel expansion. We simultaneously encrypt \( r \) successive white or black pixels each time. The probability of these \( r \) pixels being coloured black depends on the ratio of blacks in the basis matrices. Afterward, we incorporate the techniques of colour decomposition and halftoning into the proposed scheme to handle grey-level and chromatic images. The experimental results show that the shares are not only the same size as the secret image, but also attain the requirement of security. The stacked images have good visual effect as well. Besides, our method can be easily extended to general access structure.

Keywords: Visual Secret Sharing, Halftoning, Colour Model, Information Security
ACM Classification: K.6.5 (Security and Protection)

1. INTRODUCTION
Cryptography is a method of protecting confidential information. It usually scrambles the content of the information through some mathematical computation, and the disordered content is difficult to revert to the original one within limited time and resources if the secret key is unknown. Hence cryptography can be used to avoid the secret being disclosed. Nevertheless, the drawback of the traditional cryptography is that it heavily relies on a lot of complex computation to encrypt and decrypt a secret; hence computers are essential for both encryption and decryption.

In 1994, Naor and Shamir (1995) proposed a new method applied on secret images, called visual cryptography. It’s a visual secret sharing scheme to split a secret image into \( n \) shares, which reveal...
A Visual Cryptographic Technique for Chromatic Images Using Multi-pixel Encoding Method

no information about the secret. The secret can be seen from the stacked shares with human eyes; therefore it provides a solution to decrypt secrets without computers. Initially, the scheme realized a \((k, n)\)-threshold access structure for black-and-white images, called \((k, n)\)-threshold visual secret sharing (VSS) scheme. That means that the secret image can be recovered when \(k\) out of \(n\) shares are stacked. An access structure is a rule, which defines how to share a secret. Tzeng and Hu (2002) define a general access structure in the form of \(\Gamma = (P, F, Q)\), where \(P = \{1, 2, \ldots, N\}\), \(F\) and \(Q\) are sets of subsets of \(2^P\), and \(Q \cap F = \emptyset\). \(P\) denotes the set of participants, \(F\) denotes a collection of forbidden sets, and \(Q\) denotes a collection of qualified sets. An element of a forbidden set or a qualified set represents a share held by the corresponding participant. Stacking all the shares of a forbidden set cannot reveal any information about the secret image, but stacking all the shares of a qualified set can recover the secret image. The \((k, n)\)-threshold VSS scheme mentioned above is a special case of the general access structure, and the \((2, 2)\)-threshold VSS scheme can consequently be represented as \(\Gamma = (P = \{1, 2\}, F = \{\{1\}, \{2\}\}, Q = \{\{1, 2\}\})\); therefore share 1 and share 2 cannot reveal the secret image, and only stacking share 1 and share 2 can recover the secret image. In this paper, we adopted the form \(\Gamma = (P, F, Q)\) to represent an access structure, and the term “stacked image” is used to represent the result of stacking all the shares of a forbidden set or a qualified set. Therefore, a stacked image may be composed of one or more shares. In many studies, the visual cryptography scheme, which realizes an access structure, is denoted by black and white basis matrices. There are many studies about how to design the basis matrices (Ateniese et al., 1996b; Blundo et al., 1999; Naor and Shamir, 1995; Tzeng and Hu, 2002; Verheul and van Tilborg, 1997).

Most visual cryptographic methods need to expand pixels (Ateniese et al., 1996a, 1996b, 2001; Blundo et al., 2001; Blundo and De Santis, 1998; Blundo et al., 2000; Blundo et al., 1999; Droste, 1996; Eisen and Stinson, 2002; Hofmeister et al., 2000; Hou, 2003; Naor and Shamir, 1995; Tzeng and Hu, 2002; Verheul and van Tilborg, 1997; Yang and Laih, 2000); that is, every pixel on the secret image is expanded to \(m\) sub-pixels on the shares, where \(m \geq 2\). Consequently, the share is \(m\) times the size of the secret image, and that leads to not only distortion of images but also inconvenience of carrying shares and waste of the storage space. The parameter \(m\) is called “pixel expansion”, and “\(m = 1\)” refers to the situation that the size of shares is the same as that of the secret image. A few studies have been done on this situation. Hou et al (2001) proposed a \((2, 2)\)-threshold visual cryptographic scheme without pixel expansion. For each time, an \(L \times M\) block \(B\) with \(cnt\) black pixels on the secret image is encoded to corresponding blocks \(B_1\) and \(B_2\) on the first and second shares respectively. \(B_1\) is filled with \((L \times M)/2\) blacks randomly. \((L \times M)\)-\(cnt\) pixels of \(B_2\) corresponding to the black area of \(B_1\) are filled with blacks, and \(cnt-(L \times M)/2\) pixels of \(B_2\) corresponding to white area of \(B_1\) are filled with blacks. Hence \(B_2\) also has \((L \times M)/2\) black pixels, which satisfies the security requirement. Although Hou et al’s method does not need to expand pixels, it only fits \((2, 2)\)-threshold access structure. It is impossible for the method to realize \((k, n)\)-threshold or general access structure. Moreover, the secret image has to be preprocessed to ensure the number of black pixels of a block \(B\) is more than \((L \times M)/2\).

Ito et al (1999) utilized black and white basis matrices to implement a \((k, n)\)-threshold visual secret sharing scheme without pixel expansion. When a black (resp. white) pixel is encrypted, one of the columns of the black (resp. white) basis matrix is picked randomly, and the \(i\)-th row of the column is then assigned to the \(i\)-th share. Since the corresponding rows of the black and white basis matrix have the same ratio of ‘0’ to ‘1’, each pixel on the share has the same probability of being coloured black or white, no matter what the colour of the corresponding pixel on the secret image is. Therefore it is impossible to perceive any clue about the secret image from the shares. The contrast of the stacked image depends on Eq. 1.

\[
\beta = |p_0 - p_1|
\]

(1)
In Equation 1, \( p_0 \) (resp. \( p_1 \)) denotes the probability that a white (resp. black) pixel of the secret image becomes black on the stacked image. As long as the difference between these two probabilities is large enough, human eyes can discriminate black areas from white areas on the stacked image. However, they did not mention how to apply their method to continuous-tone images. Moreover, although the whole stacked image may truly attain the contrast defined by \( \beta \), it is still possible for a small area that the distribution of black and white pixel can’t totally fulfill the values of \( p_0 \) and \( p_1 \) because the selection of the columns of the basis matrix is fully random. Thus the visual effect of the stacked image is probably poor.

In this paper, we propose another visual cryptographic method without pixel expansion, called multi-pixel encoding method (MPEM). Afterward we utilize MPEM incorporated halftoning and colour model to share a secret grey-level and chromatic image. The experimental results show that the shares are secure enough, and the stacked images have better visual effects compared to Ito et al’s method. With appropriate basis matrices, our method can be easily extended to realize any access structure.

2. THE MULTI-PIXEL ENCODING METHOD

2.1 The Proposed Scheme

To attain the aim of not expanding the pixel, we propose that MPEM encrypt multiple pixels of the secret image simultaneously. Let \( M_0 \) and \( M_1 \) be the two \( n \times r \) basis matrices corresponding to white and black pixels, respectively. We simultaneously take \( r \) successive white (resp. black) pixels as a unit of encryption. The set of positions of these \( r \) white (resp. black) pixels is called “a white (resp. black) encryption sequence”. The steps of encryption are as follows:

1. Take \( r \) successive white (resp. black) pixels, which have not been encrypted yet, from the secret image sequentially. Record the positions of the \( r \) pixels as \((p_1, p_2, \ldots, p_r)\).
2. Permute the columns of \( M_0 \) (resp. \( M_1 \)) randomly.
3. Fill in the pixels in the positions \( p_1, p_2, \ldots, p_r \) of the \( i \)-th share with the \( r \) colours of the \( i \)-th row of the permuted matrix, respectively.
4. Repeat step (1) to step (3) until every white (resp. black) pixel is encrypted.

Take a \((2, 2)\)-threshold visual secret sharing scheme for example to compare the MPEM with the traditional method (i.e. Naor and Shamir’s method). The two basis matrices for white and black pixels are as follows:

\[
M_0 = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}, \quad M_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}
\]  

(2)
Suppose Figure 1(a) is the secret black-and-white image. In Naor and Shamir’s method, when encoded a black (resp. white) pixel, the columns of $M_1$ (resp. $M_0$) are randomly permuted, and the two pixels of each row of the permuted matrix are distributed to each share. Hence, each pixel is encoded into two sub-pixels on each share. Observing Figure 1(b), we can see that the size of the stacked image is larger, and the shape is distorted. If we want to avoid distortion, we can encode each pixel into a block of $2 \times 2$ sub-pixels on each share. However, the pixel expansion becomes larger; that is, four sub-pixels. We can glance at Figure 3, which is a recovered image with a pixel expansion $m = 4$. On the contrary, the size of the stacked image (See Figure 1(c)) generated by the proposed MPEM is the same as that of the secret image, and naturally, the shape is not changed. Moreover, the recovered logo is as visually perceivable as that of Naor and Shamir’s method. It should be noted that the spirit of visual cryptographic method is that the stacked image is decoded by human eyes; hence, the secret should be visually perceivable. Therefore, the proposed MPEM attain the requirement just like the traditional method does.

2.2 Contrast and Security
Let $\Gamma = (P, F, Q)$ be an access structure on a set of $n$ participants. A VSS scheme for $(P, F, Q)$ with relative difference $\alpha(r)$ and set of thresholds $\{(X, t_X)\} \in Q$ is realized using the two $n \times r$ basis matrices $M_0$ and $M_1$ if the following two conditions hold (Ateniese et al, 1996b).

1. If $X = \{i_1, i_2, \ldots, i_p\} \in Q$, then the $r$-vector $V$ formed by “OR”-ing rows $i_1$, $i_2$, ..., $i_p$ of $M_0$ satisfies $H(V) \leq t_X - \alpha(r) \cdot r$; whereas, for $M_1$ it results that $H(V) \geq t_X$.
2. If $X = \{i_1, i_2, \ldots, i_p\} \in F$, then the two $p \times m$ matrices obtained by restricting $M_0$ and $M_1$ to rows $i_1, i_2, \ldots, i_p$ are equal up to column permutation.

In the conditions above, $H(V)$ denotes the Hamming weight of the $r$-vector $V$, i.e. the number of bit ‘1’ in $V$, and $t_X$ denotes a threshold and $1 \leq t_X \leq r$. The first condition is referred to as contrast; that is, the number of black pixels within the $r$-vector $V$ corresponding to white pixels of the secret image has to be smaller than $t_X - \alpha(r) \cdot r$, while that of black pixels within the $r$-vector $V$ corresponding to black pixels of the secret image has to be larger than $t_X$. Therefore, the blackness of $r$-vector $V$ corresponding to white pixels will obviously differ from that corresponding to black pixels. The second condition is referred to as security; that is, the original secret is totally invisible if analyzed by any other method from the stacked image of the forbidden set.

Every encryption sequence of the secret image is encoded either by $M_0$ or $M_1$, depending on its type. Since both $M_0$ and $M_1$ have to satisfy the security condition, the security of the proposed MPEM is based on the security of visual cryptography. In accordance with the contrast condition of the basis matrices, the $r$-vector corresponding to the black encryption sequence contains more black pixels than that corresponding to the white encryption sequence on the stacked image, which produces the contrast as Equation 1. That means that the black area looks blacker than the white area. Hence the proposed MPEM can hold the contrast condition of visual cryptography.

3. THE VISUAL CRYPTOGRAPHIC METHOD FOR GREY-LEVEL IMAGES WITH $m=1$
As we mentioned earlier, most studies about visual cryptographic methods need to expand pixels, especially those methods for grey-level and chromatic images (Blundo et al., 2000; Hou, 2003; Rijmen and Preneel, 1996; Verheul and van Tilborg, 1997; Yang and Laih, 2000). This research usually tries to design respective basis matrices for different colours on a secret continuous-tone image (Blundo et al., 2000; Verheul and van Tilborg, 1997; Yang and Laih, 2000). In this paper, we introduce a technique, called halftoning, which can transform a continuous-tone image into a bi-
level image (Mese and Vaidyanathan, 2002). By employing halftoning, we can apply the proposed MPEM to grey-level and chromatic images easily. In this section, we will describe halftoning briefly and demonstrate how we incorporate halftoning in MPEM to encode a grey-level secret image.

3.1 Halftoning

The main idea of halftoning is to utilize the density of printed dots to simulate the grey scale of pixels. Human eyes can integrate the fine detail in an image viewed from a distance and record only the overall intensity. The denser the dots are, the darker the image is; on the contrary, the sparser the dots are, the lighter the image is. Therefore, we can use two colours – black and white – to simulate a continuous tone so that a continuous-tone image can be transformed into a bi-level image. For example, a grey-level image (Figure 2(a)) is transformed into a bi-level image (Figure 2(b)) with black and white dot only by halftoning. Although, in fact, Figure 2(b) is a black-and-white image, we can still perceive the change of the grey level as if it is a grey-level image.

Most visual cryptographic methods are for black-and-white images, so if we utilize halftoning to transform a grey-level image into a bi-level image, those visual cryptographic methods can be applied to halftone images directly. For example, we can use the (2, 2)-threshold VSS scheme proposed by Naor and Shamir (1995) to encrypt Figure 2(b). The result is shown in Figure 3, which illustrates the suitability and feasibility of using halftoning to construct a visual cryptographic scheme for grey-level images. In this paper, we will not discuss halftoning in detail. The emphasis will be put on that the bi-level feature of the grey-level and chromatic images can extend the application of the black-and-white visual cryptographic method.

3.2 The Proposed Scheme for Grey-level Images and Experimental Results

Let $M_0$ and $M_1$ denote the two $n \times r$ basis matrices corresponding to a white and a black pixel, respectively. For applying the two basis matrices to grey-level images directly, we incorporate the halftoning into the encryption procedure. The whole encryption procedure of the proposed scheme for chromatic images is as follows.

1. Transform the secret grey-level image $SI$ into a halftone image $SI'$.
2. Encode $SI'$ by MPEM.
We take Figure 2(b) as the secret grey-level image and implement a (2, 3)-threshold visual secret sharing scheme by MPEM. The access structure can be represented as \( \Gamma = (P = \{1, 2, 3\}, F = \{\{1\}, \{2\}, \{3\}\}, Q = \{\{1, 2\}, \{2, 3\}, \{1, 3\}, \{1, 2, 3\}\}) \). The white and black basis matrices are as follows:

\[
M_0 = \begin{bmatrix}
0 & 0 & 1 \\
0 & 0 & 1 \\
0 & 0 & 1 
\end{bmatrix}, \quad M_1 = \begin{bmatrix}
0 & 0 & 1 \\
0 & 1 & 0 \\
1 & 0 & 0 
\end{bmatrix}
\]  

Hence this scheme will generate three shares, and stacking at least two shares can recover the secret as shown in Figure 4(a) to Figure 4(d).

Traditionally, researchers tend to utilize the technique of pixel expansion to handle continuous-tone images, such as grey-level images (Blundo et al., 2000; Hou, 2003; Rijmen and Preneel, 1996; Verheul and van Tilborg, 1997; Yang and Laih, 2000). With the help of halftoning, we can easily extend the MPEM to encode continuous-tone images without pixel expansion. However, Ito et al. (1999) only proposed a black-and-white visual cryptographic method and did not mention how to apply their method to encode grey-level images. Moreover, instead of encoding one pixel each time like Ito et al.’s method, we simultaneously handle \( r \) successive white (resp. black) pixels each time. Hence we can avoid severe variation of grey levels in a small area and make sure of a better visual effect of the stacked images. We compare the proposed MPEM with Ito et al.’s method for the same secret image. The experimental results of Ito et al.’s method are shown in Figure 4(e) to Figure 4(h). Obviously, the visual effect of Ito et al.’s results is messier than MPEM’s. The variations of grey levels for black and white encryption sequences are examined in Section 5.

Figure 3: The stacked image (1024 \( \times \) 1024 pixels, 300 dpi)
Figure 4: The (2, 3)-threshold VSS scheme for grey-level images by MPEM and Ito et al’s method (512 × 512 pixels, 300 dpi)
Observing the basis matrices (i.e. Equation 3), we can see that the 3-vector of any two rows of \( M_0 \) (resp. \( M_1 \)) has one (resp. two) black so that the probability that a white (resp. black) pixel on the halftone image becomes black on the stacked image is 1/3 (resp. 2/3). In addition, the 3-vector of three rows of \( M_0 \) (resp. \( M_1 \)) has one (resp. three) black so that the probability that a white (resp. black) pixel on the halftone image becomes black on the stacked image is 1/3 (resp. 3/3). Therefore, the contrasts of \((S1+S2)\), \((S2+S3)\), and \((S1+S3)\) are 1/3, and the contrast of \((S1+S2+S3)\) is 2/3.

4. THE VISUAL CRYPTOGRAPHIC METHOD FOR CHROMATIC IMAGES WITH \( m=1 \)

4.1 Basis Theorem of Colour

A colour model is a generally accepted way to specify colours (Mese and Vaidyanathan, 2002). It can be represented as a three-dimensional space, where each colour is represented by a single point. There are many kinds of the colour model, and RGB and CMY are two common models.

In terms of the RGB colour model, each colour is mixed with red, green, and blue, which are the three primary colours of light. This model is commonly used for on-screen display. Mixtures of pure red, pure green and pure blue light produce white light; therefore, the three colours are also called additive primaries, and the RGB model is also called the additive model. In the terms of CMY colour model, each colour is mixed with cyan, magenta, and yellow, which are the three primary colours of pigments. This model is commonly used for colour printing. Mixtures of pure cyan, magenta, and yellow pigments produce black. The wavelength of light determines the colour of light. The colour of an object depends on the reflection of light that strikes it. Some or all of the light may be absorbed depending on the pigmentation of the object. What we see as colour, are the wavelengths of light that are not absorbed. Different wavelength of light is absorbed by different colour of pigments. The more colours of pigments are mixed, the more wavelengths of light are absorbed. The mixtures of pure cyan, pure magenta and pure yellow absorb all wavelengths of light and hence produce black. Therefore these three colours are called subtractive primaries, and the CMY model is also called the subtractive model. Since the shares of colour visual cryptography are printed on transparencies and stacking the shares produces colour mixing as colour printing, we adopt the CMY colour model to decompose a secret chromatic image into three monochromatic images in tones of cyan, magenta, and yellow. The monochromatic intensity of each image ranges from 0–255, so each image can be treated as a grey-level image and hence can be transformed to a bi-level image by means of halftoning. Afterward we can use the proposed MPEM to produce the shares of the secret chromatic image.

4.2 The Proposed Scheme for Chromatic Images and Experimental Results

Let \( M_0 \) and \( M_1 \) denote the two \( n \times r \) basis matrices corresponding to a white and a black pixel, respectively. We decompose the secret chromatic image into three monochromatic images in tones of cyan, magenta, and yellow, respectively. Then each monochromatic image is transformed to a halftone image, where each pixel has only two possible values: blank or not blank, and hence can be handled by the proposed MPEM. For presentation clarity, we call these two possible values as white and black, respectively. The whole encryption procedure of the proposed scheme for chromatic images is as follows:

1. Decompose the secret chromatic image \( SI \) into three monochromatic images, \( C, M, Y \).
2. Transform the three monochromatic images \( C, M, Y \) into three halftone images \( C', M', Y' \).
3. Encode \( C', M', Y' \) by MPEM, respectively.
4. The $i$-th shares of the halftone images $C', M', Y'$ are combined to form the $i$-th share of the secret chromatic image $SI$.

We implement the (2, 3)-threshold VSS scheme to illustrate the above algorithm with Figure 5. Equation 3 is the two basis matrices, and Figure 5(a) is the secret chromatic image. The secret image is decomposed into three monochromatic images in continuous-tone, which are then transformed into three bi-level images, $C'$, $M'$, $Y'$, by means of halftoning, respectively. We utilize MPEM to generate respective shares of $C'$, $M'$, and $Y'$: $(C_1, C_2, C_3)$, $(M_1, M_2, M_3)$, and $(Y_1, Y_2, Y_3)$. $C_1$, $M_1$, and $Y_1$ are merged into the first share of the secret chromatic image (Figure 5(b)); $C_2$, $M_2$, and $Y_2$ are merged into the second share of the secret chromatic image (Figure 5(c)); $C_3$, $M_3$, and $Y_3$ are

![Figure 5: The (2, 3)-threshold VSS scheme for the chromatic image by MPEM (512 × 512 pixels, 300 dpi)](image-url)
merged into the third share of the secret chromatic image (Figure 5(d)). The colour of each pixel on the share is mixed with the colours of the corresponding pixels on $C_i, M_i,$ and $Y_i$, where $i=1, 2, 3$. The stacked images are shown in Figure 5(e) to Figure 5(h).

On the basis of the security of basis matrices, each share of the halftone images generated by MPEM has no clue to the shared halftone image. Therefore the merged shares, $S_i$, cannot perceive any information about the secret image naturally. On the basis of the contrast of basis matrices, the stacked images corresponding to the qualified set (Figure 5(e) to Figure 5(h)) can make a difference between colours, whereas the stacked image corresponding to the forbidden set (Figure 5(b) to Figure 5(d)) can’t reveal any information about the secret image. From the experimental result, we can see that the stacked image corresponding to the qualified set cannot only recover the secret image but also has good visual effect.

5. DISCUSSIONS AND CONCLUSIONS

We have demonstrated that the proposed MPEM is more suitable for continuous-tone images than Ito et al’s method in Section 3. Since Ito et al (1999) encrypt one pixel each time, they cannot make sure that each $r$ pixels corresponding to a white (resp. black) encryption sequence on the stacked images has the same number of black pixels. Therefore, in a small area, they may not attain the ratio of $p_0$ and $p_1$ as defined in Equation 1 and cause a sharp variation of the grey level so that the stacked images look chaotic. In our method, we take a white (resp. black) encryption sequence of the secret image as a unit of encryption at a time. For each set of $r$ pixels on the share corresponding to a white (resp. black) encryption sequence, the number of black pixels within it is fixed; in other words, the grey level of each encryption sequence is the same; thus the standard deviation is 0, and the grey level will not vary sharply in a large extent of a white (resp. black) area. That is the reason that MPEM can make sure of a better visual effect and is more suitable for grey-level and chromatic images than Ito et al’s method is.

We take Figure 4 to explain the variation of the grey level of the black or white encryption sequences on the stacked images and use the average and standard deviation to represent the variation. The average and standard deviation of the grey level of the black or white encryption sequences are defined as Equation 4 and Equation 5.

\[
\mu_b = \frac{\sum_{i=1}^{n_b} B_i}{n_b}, \quad \sigma_b = \sqrt{\frac{\sum_{i=1}^{n_b} (B_i - \mu_b)^2}{n_b}}
\]

\[
\mu_w = \frac{\sum_{i=1}^{n_w} B_i}{n_w}, \quad \sigma_w = \sqrt{\frac{\sum_{i=1}^{n_w} (B_i - \mu_w)^2}{n_w}}
\]

In the above equations, $\mu_b$ (resp. $\mu_w$) and $\sigma_b$ (resp. $\sigma_w$) are the average and standard deviation of the grey level of black (resp. white) encryption sequences on the stacked image, and $n_b$ (resp. $n_w$) is the number of black (resp. white) encryption sequences on the stacked image. $B_i$ is the number of black pixels within the $i$-th encryption sequence on the stacked image and can be seen as the grey level of a encryption sequence. The statistic results are shown in Table 1. Observing the results of
A Visual Cryptographic Technique for Chromatic Images Using Multi-pixel Encoding Method

<table>
<thead>
<tr>
<th></th>
<th>MPEM</th>
<th>Ito et al’s method</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Black encryption sequence</td>
<td>White encryption sequence</td>
</tr>
<tr>
<td></td>
<td>( \mu_b )</td>
<td>( \sigma_b )</td>
</tr>
<tr>
<td>S1 + S2</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>S2 + S3</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>S1 + S3</td>
<td>2</td>
<td>0</td>
</tr>
</tbody>
</table>

Table 1: The variation of the grey level for each white (black) encryption sequence on stacked images of Figure 4

<table>
<thead>
<tr>
<th></th>
<th>Black Encryption Sequence</th>
<th>White Encryption Sequence</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>( \mu_b )</td>
<td>( \sigma_b )</td>
</tr>
<tr>
<td>S1 + S2</td>
<td>C</td>
<td>1.9986</td>
</tr>
<tr>
<td></td>
<td>M</td>
<td>1.9964</td>
</tr>
<tr>
<td></td>
<td>Y</td>
<td>1.9973</td>
</tr>
<tr>
<td>S2 + S3</td>
<td>C</td>
<td>2.0010</td>
</tr>
<tr>
<td></td>
<td>M</td>
<td>2.0038</td>
</tr>
<tr>
<td></td>
<td>Y</td>
<td>1.9983</td>
</tr>
<tr>
<td>S1 + S3</td>
<td>C</td>
<td>2.0004</td>
</tr>
<tr>
<td></td>
<td>M</td>
<td>1.9997</td>
</tr>
<tr>
<td></td>
<td>Y</td>
<td>2.0043</td>
</tr>
<tr>
<td></td>
<td>C</td>
<td>3.0000</td>
</tr>
<tr>
<td>S1 + S2 + S3</td>
<td>M</td>
<td>3.0000</td>
</tr>
<tr>
<td></td>
<td>Y</td>
<td>3.0000</td>
</tr>
</tbody>
</table>

Table 2: Analysis of the variation of the grey level of Ito et al’s method for each white (black) encryption sequence

MPEM in Table 1, we can see that the averages of both encryption sequences are always 2 and 1, respectively, and the standard deviations of both encryption sequences are always 0, so in Figure 4 (a) to Figure 4(d), the grey level varies moderately. That is why MPEM can attain good visual quality of the stacked images.

On the contrary, as regards Ito et al’s method, although the averages for (S1+S2) (Figure 4(e)), (S2+S3) (Figure 4(f)), and (S1+S3) (Figure 4(g)) are near the theoretical value, the standard deviations are higher than 0.8, which means that the grey level varies severely on the stacked images. For the stacked image (S1+S2+S3) (Figure 4(h)), the grey level of black encryption sequences does not vary because there is at least one ‘1’ in every column of the black basis matrix, so the black pixels of the secret image can be recovered totally on the stacked image (S1 + S2 + S3). However, the standard deviation of white encryption sequences is still very high. That is why the stacked images of Ito et al’s method (Figure 4(e) to Figure 4(h)) look more chaotic compared to MPEM’s stacked images (Figure 4(a) to Figure 4(d)). Since each row of the white basis matrix is the same, the averages and standard deviations of the white encryption sequence of Ito et al’s method are the same for all stacked images (See Table 1).

The situation is the same when Ito et al’s method is applied to the chromatic image (i.e. Figure 5(a)). According to the basic theorem of colour, we can decompose a stacked image into three mono-
chromatic images in tones of cyan (C), magenta (M), and yellow (Y), respectively. The grey level of the black and white encryption sequences on them still varies severely (See Table 2). Therefore, it is possible the colour of each pixel on the chromatic stacked image may not be well mixed.

Visual cryptography is very suitable for decryption without computers, but most studies utilize the technique of pixel expansion, which leads to distortion of shares, difficulty in taking along, and waste of space. In this paper, we employ halftoning and colour decomposition so that a black-and-white visual cryptographic method can be easily extended to grey-level and chromatic images. However, the existing method is not necessarily suitable for such an extension. In this paper, we propose a new method, called MPEM, to improve the drawback of Ito et al.’s method. We utilize two $n \times r$ basis matrices to simultaneously encrypt $r$ white (resp. black) pixel for each time. The experimental results show that MPEM can have a better visual effect on stacked images. Besides, the MPEM can not only attain the security and contrast proved by the basis matrix, but also achieve the goal of image size invariant.

6. ACKNOWLEDGEMENTS
This work was supported in part by a grant from the National Science Council of the Republic of China under the project NSC90-2213-E-008-047.

REFERENCES


A Visual Cryptographic Technique for Chromatic Images Using Multi-pixel Encoding Method


**BIOGRAPHICAL NOTES**

Young-Chang Hou received the BSc degree in Atmospheric Physics from the National Central University, Taiwan, R.O.C. in 1972, the MSc degree in Computer Applications from the Asian Institute of Technology, Bangkok, Thailand, in 1983 and PhD degree in Computer Science and Information Engineering from the National Chiao-Tung University, Taiwan, R.O.C. in 1990. From 1976 to 1987, he was a senior engineer of Air Navigation and Weather Services, Civil Aeronautical Administration, R.O.C. where his work focused on the automation of weather services. From 1987 to 2004, he joined the faculty at the National Central University. Currently, he is a professor in the Department of Information Management, TamKang University. His research interests include digital watermarking and information hiding, fuzzy logic, genetic algorithm, and cryptography.

Shu-Fen Tu received the BAc degree in Management Information System from the National ChengChi University, Taiwan, R.O.C. in 1996 and the MAc degree in Information Management from the National ChiNan University, Taiwan, R.O.C. in 1998, and a PhD in Information Management from the National Central University, Taiwan, R.O.C. in 2005. From 1998 to 1999, she was a software engineer at The Syscom Group Co., Taiwan, R.O.C. Currently, she is an assistant professor in the Department of Information Management, Chao Yang University of Technology. Her research interests include digital watermarking and copyright protection, secret sharing and visual cryptography.