# Progressive Color Visual Cryptography

(Final version of the manuscript ID: JEI03158)

Duo Jin, Wei-Qi Yan, Mohan S. Kankanhalli
School of Computing, National University of Singapore
Singapore 117543

This paper was submitted to SPIE Journal of Electronic Imaging (JEI/SPIE) on Nov.15, 2003, revised on Oct.26, 2004, accepted on Jan.4, 2004. Corresponding author : Wei-Qi Yan (e-mail: yanwq@comp.nus.edu.sg).

**Abstract**

Visual cryptography is a powerful technique which combines the notions of perfect ciphers and secret sharing in cryptography with that of raster graphics. A binary image can be divided into shares which can be stacked together to approximately recover the original image. Unfortunately, it has not been used much primarily because the decryption process entails a severe degradation in image quality in terms of loss of resolution and contrast. Its usage is also hampered by the lack of proper techniques for handling grayscale and color images. In this paper, we have developed a novel technique which enables visual cryptography of color as well as grayscale images. With the use of halftoning and a novel microblock encoding scheme, the technique has a unique flexibility which allows a single encryption of a color image but allows three types of decryptions on the same ciphertext. The three different types of decryptions allow for the recovery of the image of varying qualities. The physical transparency stacking type of decryption allows for the recovery of the traditional visual cryptography quality image. An enhanced stacking technique allows for the decryption into a halftone quality image. And finally, a computation based decryption scheme makes the perfect recovery of the original image possible. Based on this basic scheme, we have then established a progressive mechanism to share color images at multiple resolutions. We extract shares from each resolution layer to construct a hierarchical structure; the images of different resolutions can then be restored by stacking the different shared images together. Thus, our technique allows for flexible decryption. We have implemented our technique and present results.

**Index Terms**

Color halftoning, image sharing, multiple resolutions, progressive, secret sharing, visual cryptography

## I. Introduction

### *A. Background on Visual Cryptography*

Visual cryptography was originally proposed for the problem of secret sharing. Secret sharing is one of the early problems to be considered in cryptography. In a ($k$, $n$)-threshold problem, a secret is divided into $n$ pieces. With any $k$ of the $n$ pieces, the secret can be perfectly reconstructed, while even complete knowledge of $k-1$ pieces reveals absolutely no information about the secret. Visual cryptography illustrated a new paradigm to solve the ($k$,$n$) problem. It was originally proposed by Naor and Shamir [1]. The original scheme generates $n$ images (known as *shares*) based on the secret message (the original image) which can be printed on $n$ transparencies. The original message can then be recovered if any $k$ or more than $k$ of the transparencies are stacked together, but no information about the original

image can be gained if fewer than threshold number of $k$ transparencies are stacked. Visual cryptography is a unique technique in the sense that the encrypted messages can be decrypted directly by the human visual system. Therefore, a system employing visual cryptography can be used by anyone without any knowledge of cryptography. Another interesting thing about visual cryptography is that it is a perfectly secure cipher. There is a simple analogy of the one time-pad cipher to visual cryptography.

Besides introducing the new paradigm, Naor and Shamir also provided their constructions of visual cryptographic solutions for the general $k$ out of $n$ secret sharing problem. One can assume that every secret message can be represented as an image, and furthermore that the image is just a collection of black and white pixels i.e. it is assumed to be a binary image. Each original pixel appears in $n$ modified versions (called shares) of the image, one for each transparency. Each share consists of $m$ black and white sub-pixels. Each share of sub-pixels is printed on the transparency in close proximity (to best aid the human perception, they are typically arranged together to form a square with $m$ selected as a square number). The resulting structure can be described by a Boolean matrix $M = (m_{ij})_{n\times m}$ where $m_{ij} = 1$ if and only if the $j$-th sub-pixel of the $i$-th share (transparency) is black. Usually, we will use $R_0$ to refer to the constructed $M$ when the pixel in the original image is white, and similarly $R_1$ when the pixel in the original image is black. The important parameters of the scheme are:

- $m$, the number of pixels in a share. This parameter represents the loss in resolution from the original image to the recovered one.
- $\alpha$, the relative difference in the weight between the combined shares that come from a white pixel and a black pixel in the original image. This parameter represents the loss in contrast.
- $\gamma$, the size of the collection of $C_0$ and $C_1$. $C_0$ refers to the sub-pixel patterns in the shares for a white pixel and black refers to the sub-pixel patterns in the shares for the 1 pixel.

The constructions can be clearly illustrated by a 2 out of 2 visual cryptographic scheme[1]. Define the following collections of $2 \times 2$ matrices:

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

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

The six patterns of shares created based on the above matrices are shown in figure 1. Note that *one* pixel of the original image now corresponds to *four* pixels in each share. A visual cryptography scheme

[1]In some papers, it is often referred to (2,2)-VCS in short. In this paper, we also adopt the same notation.

can then be constructed by picking shares in the following manner:

- if the pixel of the original binary image is white, randomly pick the same pattern 0 of $four$ pixels for both shares. It is important to pick the patterns randomly in order to make the pattern random.
- if the pixel of the original image is black, pick a complementary pair of patterns, i.e., the patterns from the same column in figure 1.

It can be easily verified that the resultant scheme has the parameters $[m = 4, \alpha = \frac{1}{2}, \gamma = 6]$: any two shares of $C_0$ cover *two* out $four$ of the pixels, while any pair of shares from $C_1$ covers all the $four$ pixels[2]. An example of the above scheme is shown in figure 2. The first image is the original image, the next two are the shares and the last image is the recovered original image obtained by performing the equivalent of physically stacking two image shares on top of each other (assuming that they are printed on transparencies). It should be noted that the last three images in figure 2 are four times as large as the first one but we have scaled them to the same size as the original image.

### *B. Our Contribution*

The state of the art in visual cryptography leads to the degradation in the quality of the decoded images, which makes it unsuitable for digital media (image, video) sharing and protection. This is quite obvious in figure 2 where the white background of the original image becomes gray in the decrypted image. In this paper, we propose a series of visual cryptographic schemes that not only can support grayscale and color images, but also allow high quality images including that of perfect (original) quality to be reconstructed.

The nagging presence of the loss of contrast makes traditional visual cryptography scheme practical only when a quality is not an issue which is quite rare. We have therefore focussed our attention on specifically overcoming this problem by primarily devoting our efforts towards improving the quality of the reconstructed images. We first extend the basic scheme from [1] to allow visual cryptography to be directly applied on grayscale and color images. Image halftoning is employed in order to transform the original image from the grayscale/color space into the monochrome space which has proved to be quite effective. To further improve the quality, artifacts introduced in the process of halftoning have been reduced by inverse halftoning.

It is a well known fact that the digital halftoning is always a lossy process [2], which means that whenever a halftoning is used for the transformation, it is impossible to fully reconstruct the original

[2]There are other constructions that can result in a contrast of $\frac{1}{4}$.

secret image. A new encoding scheme has therefore been developed which allows for perfectly lossless transformation between monochrome, grayscale and color spaces. This new encoding scheme can be seamlessly incorporated into the proposed scheme for visual cryptography and it allows the original secret image to be perfectly restored. Moreover, with the aid of an auxiliary mapping table, encoding and decoding become extremely simple and fast.

This puts visual cryptography on an equal footing with the traditional (non-visual) cryptographic schemes while retaining all the advantages of visual cryptography. We believe this advancement in visual cryptography can be useful in secret sharing of images, in transmission of secret images over multiple untrustworthy channels, in e-commerce of digital media and in digital rights management of digital media.

Another advantage is that this scheme allows for a *single encryption, multiple decryptions* paradigm. In our schemes, secret images are encrypted/shared once, and later, based on the shares, they can be decrypted/reconstructed in a plurality of ways. This idea brings tremendous flexibility. Images of different qualities can be extracted, depending on the need of quality as well as the computational resources available. For instance, images with loss of contrast are reconstructed by merely stacking the shares; a simple yet effective bit-wise operation can be applied to restore the halftone image; or images of perfect quality can restored with the aid of the auxiliary look-up table.

We have extended visual cryptography to allow for multiple resolutions in terms of image quality. Different versions of the original image of different qualities can be reconstructed by selectively merging the shares. Not only this, we have developed a spatial multiresolution scheme in which images of increasing spatial resolutions can be obtained as more and more shares are used.

Progressive multiple resolution visual cryptography has the potential application in image distribution. This scheme can be used for secret image delivery and transfer. We can provide multiple level service for secret image transmission in which the secret can be revealed at different levels.

The whole paper is organized as follows: the related work will be introduced in section II; our approach will be described in section III; our experimental results are demonstrated in section IV; the summary of this paper and conclusions are presented in section V.

## II. Related Work

There has been a steadily growing interest in visual cryptography. Despite its appearance of being a simple technique, visual cryptography is a secure and effective cryptographic scheme. Since the origin of this new paradigm, various extensions to the basic scheme have been developed to improve the contrast and the areas of application have also been greatly expanded.

In [1], the construction of ($n$,$n$)-VCS was extended for ($k$,$n$)-VCS. In 1996, the same authors introduced the idea of cover based semi-group to further improve the contrast [3]. Ateniese et al. [4] provided the first construction of (2, $n$)-VCS having the best possible contrast for any $n \leq 2$. Blundo et al. [5] provided a contrast optimal (3,$n$)-VCS and gave a proof on the upper bound on the contrast of any (3,$n$)-VCS. [1] first considered the problem of concealing the existence of the secret image. [6] provided a general solution for that problem.

The random nature of secret shares makes shares unsuitable for transmission over an open channel. [6] used a modified scheme to embed some meaningful images into the shares. [7] used different moire patterns to visualize the secret instead of different gray levels.

As far as extending to color images goes, [8] provided a primitive scheme for images of 24 colors. Hou [9] then proposed a novel approach to share color images based on halftoning. Other interesting topics include visual authentication [10] and watermarking based on visual cryptography [11]. Recently, there has been an attempt to build a physical visual cryptographic system based on optical interferometry [12]. However, all of these earlier works result in a decrypted image of reduced quality.

## III. Our Approach

Our work can be divided into the following: we first extend traditional visual cryptography to support grayscale and color images; secondly we have developed a new encoding scheme to transform an image from grayscale/color space into monochrome space, which allows perfect restoration of the original image and finally we develop the multi-resolution scheme which can decrypt images of varying quality or of varying spatial resolutions.

### *A. Halftone-Based Grayscale and Color Visual Cryptography*

Digital halftoning has been extensively used in printing applications where it has been proved to be very effective. For visual cryptography, the use of digital halftoning is for the purpose of converting the grayscale image into a monochrome image. Once we have a binary image, then the original visual cryptography technique can be applied. However, the concomitant loss in quality is unavoidable in this case.

For color images, there are two alternatives for applying digital halftoning. One is to split the color image into channels of cyan, magenta and yellow. Then each channel is treated as a grayscale image to which halftoning and visual cryptography are applied independently. After the monochrome shares are generated for each channel, channels are combined separately to create the color shares. This is the

approach presented in [9]. The alternative approach would be to directly apply color halftoning, then perform the separation into color channels followed by the application of visual cryptography to each channel independently. Actually, these two approaches lead to the same results finally.

There are many mature halftoning techniques available for selection. We have experimented with the dispersed-dot dithering, clustered-dot dithering and error diffusion techniques. For the second approach, generalized error diffusion described in [13] was used. In practice, we have found that error diffusion usually produces superior quality results compared to the results produced using dithering arrays. Though both of the alternatives have an acceptable performance.

Our halftoning based visual cryptographic scheme can be summarized as follows:

- *Encryption:* This stage is for the creation of shares. This can be further divided into the following steps:
  1) Color halftoning: Standard algorithms such as the ones described in [2], [13] and [14] can be used for this step. One could do the color channel splitting first and then do the grayscale halftoning for each channel:

$$I \xrightarrow{split\ \ CMY} [I^C, I^M, I^Y] \xrightarrow{halftoning} [I^C_{hft}, I^M_{hft}, I^Y_{hft}]$$

  Or one could do color halftoning first followed by the splitting:

$$I \xrightarrow{color\ \ halftoning} I_{hft} \xrightarrow{split\ \ CMY} [I^C_{hft}, I^M_{hft}, I^Y_{hft}]$$

  2) Creation of shares: The technique presented in Section I-A can be used for this step. Considering the case of (2,2)-VCS, the steps are:

$$I^C_{hft} \xrightarrow{(2,2)-VCS} [S^C_0, S^C_1]$$
$$I^M_{hft} \xrightarrow{(2,2)-VCS} [S^M_0, S^M_1]$$
$$I^Y_{hft} \xrightarrow{(2,2)-VCS} [S^Y_0, S^Y_1]$$

- *Decryption:* This stage is for the reconstruction of the original secret image. This can be further divided into the following steps:
  1) Stacking of shares: the following stacking (OR) operation needs to be performed:

$$[S^C_0, S^C_1] \xrightarrow{stacking} I^{mg}_C$$
$$[S^M_0, S^M_1] \xrightarrow{stacking} I^{mg}_M$$
$$[S^Y_0, S^Y_1] \xrightarrow{stacking} I^{mg}_Y$$

2) Subsampling for reconstruction: These operations need to be performed where every block of *four* pixels is sub-sampled into *one* pixel of the final image. This step is optional and should be used only with the XOR recovery described in Section III-B.1 to achieve better quality.

$$[I_C^{mg}, I_M^{mg}, I_Y^{mg}] \xrightarrow{combine\,CMY} I^{mg}$$

Then, for every $2 \times 2$ block $B(i, j)$ of $I$, where

$$B(i,j) = \begin{bmatrix} I^{mg}(2i,2j) & I^{mg}(2i,2j+1) \\ I^{mg}(2i+1,2j) & I^{mg}(2i+1,2j+1) \end{bmatrix}$$

do

$$I^{subsampled}(i,j) = I^{mg}(2i,2j)$$

It is clear that our technique, though independently developed, is quite similar in spirit to the one described in [9]. So both share the same drawback that digital halftoning always leads to permanent loss of information which means that the original image can never be perfectly restored. Inverse halftoning is a possible solution that can attempt to recover the image. Various techniques have been developed such as the ones described in [15], [16] and [17]. The best of these results can obtain a restoration quality of 30 dB measured in PSNR, which is quite good. But this is not sufficient for applications which require that the original image be faithfully recovered. In fact, in all other cryptographic techniques, it is taken for granted that the decryption of a ciphertext perfectly recovers the plaintext. But visual cryptography has been a glaring exception so far.

### *B. Visual Cryptography with Perfect Restoration*

As we have seen earlier, the application of digital halftoning techniques results in some downgrading of the original image quality due to its inherently lossy nature and it is not possible to recover the original image from its halftone version. In this section, we introduce a new encoding method which allows us to transform grayscale and color images into monochrome ones without loss of any information. Furthermore, we seamlessly incorporate this new encoding scheme into our visual cryptography technique so that it can allow *perfect recovery* of the secret grayscale or color image. In short, we will refer to this proposed scheme as PVCS (Perfect Visual Cryptographic Scheme).

The novelty of our approach is that it not only allows the secret image to be just seen but allows the secret image to be reconstructed with perfect quality. The advantage of our approach is that it still retains

the crucial advantages of traditional visual cryptography like simplicity, visual decoding and perfect security. The extra feature is that depending on whether additional computing resources are provided, images of different quality can be decoded from the same set of shares. If only the stacking operation is allowed (i.e. no computations), then our scheme recovers the original visual cryptographic quality. If the XOR operation is provided (instead of the OR operation of stacking), then we can fully restore the original quality image.

*1) Using XOR to Fully Restore Monochrome Secret Images:* We first make the crucial observation that with just one additional computational operation, even traditional visual cryptography can allow full recovery of the secret binary image. Normally, when we superimpose the two shares printed on transparencies, this stacking operation is computationally modeled as the binary OR operation which causes the contrast level to be lowered. By simply substituting this OR operation with the XOR operation, the original binary image can be recovered without any loss in contrast. Table I highlights this operation and it is obvious that the binary image shares combine to recover the original. Furthermore the image can be down-sampled by extracting just one pixel from every $2 \times 2$ block. Thus, the produced image could have a more visually pleasant appearance with less storage space requirement. However, the XOR operation needs computation - the physical stacking process can only simulate the OR operation. Figure 3 recovers the same secret image as in figure 2 using the XOR operation and thus it is clearly evident that the contrast of the original image is restored.

*2) Encoding of Grayscale/Color to Monochrome:* We now present our novel encoding scheme which can allow for the lossless transformation from a grayscale or color image into a monochrome image. We will explain the concepts using the grayscale image example since a color image can be construed to be a set of three grayscale images corresponding to the three color channels. The core idea is to expand each 8-bit grayscale pixel (which can be represented as $b_7$,$b_6$,$b_5$,$b_4$,$b_3$,$b_2$,$b_1$,$b_0$, $b_i$=0 or 1, $i = 0, 1, \cdots, 7$) into a 9-bit microblock of $3 \times 3$ monochrome sub-pixels as shown in figure 4. Each $b_i$ represents the bit value of the grayscale pixel. Eight of the nine sub-pixels can record all the information of the original grayscale value and the center sub-pixel is not used. Like in traditional visual cryptography, we will use the Hamming weights (number of 1 sub-pixels in the microblock) of the microblock to simulate the grayscale levels.

The simplest way of simulating this is to use the 8-bit binary representation of a grayscale value and map each bit to a unique position in the microblock. However, the Hamming weight of the microblock does not correctly reflect its corresponding grayscale value. For example, the grayscale values of 1 and 128 have exactly the same Hamming weights (equal to 1) in their corresponding microblocks but there

is a tremendous difference between their gray values. Ideally, we would like to make a half white and a half black microblock to represent the grayscale value of 128. The simple mapping of the binary string of bits into microblock positions does not allow for this.

We now present our new encoding scheme which can precisely allow us to do this. The key idea is to utilize an auxiliary look-up table. Let $v = (b_7 b_6 b_5 b_4 b_3 b_2 b_1 b_0)_2$ represent the grayscale value of a pixel and let $V = \{v\}$ be the set of all the grayscale values $v$ in their binary representation. Clearly $v \in \{0, 1, \cdots, 255\}$. We need to compute a look-up table such that each grayscale value $g$ is mapped to a unique value $v \in V$ and the gray value can be closely approximated by the Hamming weight of $v$ denoted by $H(v)$. To build such a table, we need to define the partial order $\partial$ on $V$:

$\forall i, j \in V, i \neq j, \partial\{i\} < \partial\{j\}$ iff:

- $H(i) < H(j)$; or
- $H(i) = H(j)$ && $i < j$

Based on $\partial$, the elements of $v \in V$ can be sorted and then mapped bijectively to $[0, 255]$. Table II provides the complete mapping based on this partial ordering. In this table, $g_{orig}$ is the original grayscale value while $g_{new}$ is the new mapped value. Note that $g_{new}$ is sorted on $\partial$ in the table.

If we use table II for encoding the gray-levels into microblocks, the converted monochrome image can simulate 9 grayscale levels (since the microblock is of size $3 \times 3$). However, one can see that the simulated grayscale levels are not uniformly distributed over the entire interval. Figure 5(a) compares the distribution of resulting grayscale levels (curve 2) with the typical 8 levels resulting from the standard uniform quantization (curve 1). As seen in figure 5(b), the nonuniformity makes the luminance of the images contract in the middle range and it can lead to further degradation of image sharpness. It should be noted that more gray-levels can be simulated using a larger microblock structure. For example, a $4 \times 4$ microblock structure can be used to simulate 16 gray-levels. However, the larger the microblock structure, the larger will be the image blow-up.

For a grayscale image, we first need to transform it to the monochrome space using the microblock encoding scheme. This results in an enlarged binary image. Then the visual cryptography shares can be created using the scheme described in reference [1].

For a color image, one can apply this microblock based transformation for each of the individual color channels (CMY) separately and then use the same scheme on the three produced monochrome images. For decryption, one can use the normal stacking operation for the merging of the shares. If one uses the XOR operation instead of the stacking operation, then the perfect reconstruction of the image is possible

albeit with the need for extra computation.

As one can see, the use of a $3 \times 3$ microblock is a slightly wasteful solution since only eight out of the total nine bits are used (the center bit is unused). In fact, an optimal microblock of size $4 \times 2$ could have been similarly constructed except for a slight problem. When shares are created using such a $4 \times 2$ microblock scheme, a $1 \times 2$ block of sub-pixels (instead of $2 \times 2$) should be used in order to compensate for the distortion in the aspect ratio. However, in the next subsection, we will describe how this extra bit can be gainfully utilized.

*3) Extraction of Multiple Images from the Shares:* We will now describe the unique *single encryption, multiple decryptions* feature of our scheme. Consider a (2,2)-VCS in which for a secret image, the two shares, expanded by a factor of $6 \times 6$, are created (since as described in section I-A, each original pixel is replaced by a $2 \times 2$ share encoded by a $3 \times 3$ microblock). When we stack the two shares, the resultant decrypted image is also expanded by a factor of $6 \times 6$ having 9 gray-levels. However, if the XOR operation is used instead of the OR operation, the contrast is restored to the original value since perfect recovery is then possible.

As we have seen earlier, the use of a $3 \times 3$ microblock is sub-optimal. It appears that one bit is wasted. However, we propose to make a novel use of this additional unused bit. The basic idea is to make use of this extra bit to store an additional image. We know that digital halftoning techniques usually do not change the size of the output image, i.e., for each grayscale pixel of the image, only one bit is required to store the monochrome value. Therefore, we can store the halftone version of the original image using this free one bit. Thus the center sub-pixel of the microblock is used to create the shares of the halftone version of the original grayscale image. This is also applicable for color images as each channel is dealt with individually. We can make use of high quality halftoning techniques such as those based on error diffusion which can provide visually pleasing monochrome images.

With this enhanced $3 \times 3$ microblock encoding scheme, we have tremendous flexibility in terms of decryption. We can employ three types of decryptions and all of these extraction methods are simple and fast. For the lowest quality decryption, the bitwise OR operation can be used to simulate the actual stacking process of transparencies (or actual transparencies could be printed out and physically stacked). If a better quality decryption, a subsampling procedure that selectively extracts the center sub-pixel from every $3 \times 3$ microblock can be used along with the XOR operation to decrypt the halftone quality image. If the highest quality decryption is required, the XOR operation along with the microblock encoding table can be employed to extract the original image. The auxiliary encoding look-up table is public and therefore it is not necessary to store it with every share created.

The advantage of the proposed scheme is that it allows visual cryptography to be applied directly on grayscale/color images. The scheme is very flexible in the sense that just a single run of our common encryption method is required while multiple images of different qualities (up to the perfect original quality) can be extracted. The details of the encrypted image are preserved with very little overhead (each original 8-bit pixel is replaced by a 9-bit microblock). Interestingly, in cryptographic terms, the given plaintext (original image) is encrypted into one ciphertext (the shares) but several plaintexts (different quality images) can be extracted using different decryption algorithms.

### *C. Multiresolution Visual Cryptography*

In traditional $(k,n)$ visual cryptography, we only construct an image of single resolution if the threshold $k$ number of shares are available. If more than the threshold number shares are available, it does not add any new information. We will now develop a progressive visual cryptography scheme in which we not only build the reconstructed image by stacking the threshold number of shares together, but also utilize the other shares to enhance the resolution of the final image as shown in figure 6. In the left figure, no image can be reconstructed for less than the threshold number ($k$) of shares. However, having $k$ or more than $k$ (till $n$) number of shares does not help. The right figure illustrates the increasing resolution with more number of shares (greater than the threshold $k$).

*1) Sharing Common Shares across Multiple Secret Images:* Normally shares are created in a random manner in order to obtain the maximum security. In this subsection, we propose a new visual cryptography scheme which allows a single share to be shared across multiple secret images while still retaining the security level. We call this approach common share visual cryptography (or CSVCS in short). This scheme could be extremely useful when a set of images needs to be shared.

The derivation of CSVCS is illustrated with the (2,2) case. Recall that in (2,2)-VCS, each pixel of the secret image is expanded into 4 sub-pixels in each share and this procedure is defined by the following collections of $2\times 2$ matrices: $C_0$ and $C_1$. Any single share in either $C_0$ or $C_1$ is a random choice of 2 white sub-pixels and 2 black sub-pixels. In a (2,2)-CSVCS, a pre-determined common share $S_c$ is given together with the secret image $I$, where $S_c$ is an arbitrary random share created by the traditional (2,2)-VCS. Or it could be created using a secret user key along with a random number generator. Note that $S_c$ is double the size of $I$ in both directions and each of the block of 4 sub-pixels contains 2 black and 2 white sub-pixels. Without loss of generality, let $S_0 = S_c$, then $S_1$ is generated in the following manner:

- if the pixel color in $I$ is white, then $S_1 = S_0$;
- else $S_1[i] = 1 - S_0[i]$ for $i = 0,1,2,3$, where $S_j[i]$ denotes the $i$-th sub-pixel of $S_j$ $(j = 0,1)$.

*2) Multiresolution Visual Cryptography Scheme:* In this section, we describe a new visual cryptography scheme which generates a special set of shares which can allow multiple images of varying resolutions to be reconstructed from it.

Our multiple resolution visual cryptography scheme (MRVCS in short) is based on the simple (2,2)-VCS or any of its extensions including CSVCS or PVCS. In this new scheme, $n$ shares are first created, of which one of the shares is picked in advance to be the common share to be used across the multiple resolutions. Any of the remaining $n-1$ shares together with the common share can be merged to reconstruct the secret image at a certain resolution. Therefore, we call it (2, $n$)-MRVCS. A (2,$n$)-MRVCS is defined as follows:

Let $I$ denote the secret image. A (2,$n$)-MRVCS generates shares $S_0$, $S_1$,$\cdots$,$S_{n-2}$ and the common share $S_c$. The following conditions must be satisfied: for any $k$, $I^k$ is obtained by merging $S_k$ and $S_c$ where $I^k$ is the same image as $I$ but of a different resolution (quality). More precisely, in terms of resolution, $Resolution(I^0) \leq Resolution(I^1) \leq, \cdots, \leq Resolution(I^{n-2}) \leq Resolution(I)$, we use down-sampling by a factor 2 to obtain the different resolution images.

$$Resolution(I^{k-1}) = \frac{Resolution(I^k)}{2}, k = n-2, n-3, \cdots, 1$$

A (2, $n$)-MRVCS can now be easily built on top of the (2,2)-CSVCS scheme. It can be summarized as:

1) Input $[I^0, I^1, \cdots, I^{n-2}]$
2) Apply (2,2)-VCS:

$$I^0 \xrightarrow{(2,2)-VCS} [S_0^0, S_1^0]$$

$$S_0 = S_1^0$$

$$S_c = S_0^0$$

3) for $k = 1$ to $n-2$; do

$$I^k \xrightarrow{(2,2)-CSVCS} [S_c, S_1^k]$$

$$S_k = S_1^k$$

4) Output $[S_0, S_1, \cdots, S_{(n-2)}, S_c]$

Thus, by using $S_c$ with each of the other shares, we can reconstruct images of varying qualities.

*D. Progressive Multiresolution Visual Cryptography*

We now describe how MRVCS can be further extended into a progressive multiresolution visual cryptography scheme (PMRVCS). In PMRVCS, the shares are ordered and merged in such a way that as more shares are used, the bigger is the spatial resolution of the reconstructed image. A (*n*,*n*)-PMRVCS is defined as follows: Let $I$ be the original image, $S_0$, $S_1$, $\cdots$, $S_{n-1}$ are the shares created. For $k = 1, 2, \cdots, n-1$, image $I^k$ can be reconstructed by merging $S_0$ up to $S_k$.

The creation of PMRVCS is derived from the idea of recursive hiding [18]. To best incorporate this idea, images of multiple resolutions are constructed in such a way that the sizes are decreased by a minimum factor of 4 each time a new resolution is created.

The whole creation procedure can be captured in these steps:

1) Input $[I^1, I^2, \cdots, I^{n-1}]$
2) Use (2,2)-VCS:

$$I^1 \xrightarrow{(2,2)-VCS} [S_0^1, S_1^1]$$

$$S_0 = S_0^1$$

$$S_1 = S_1^1$$

3) for $k = 2$ to $n-1$; do

$$Comb^k = \begin{bmatrix} S_0^{k-1} & S_1^{k-1} \\ S_0^{k-1} & S_1^{k-1} \end{bmatrix}$$

$$I^k \xrightarrow[S_c = Comb^k]{(2,2)-CSVCS} [Comb^k, S_1^k]$$

$$S_k = S_1^k; S_0^k = Comb^k$$

4) Output $[S_0, S_1, \cdots, S_{n-1}]$

The reconstruction is straightforward. When reconstructing the image $I^k$, all shares from $S_0$, $S_1$ up to $S_{k-1}$ are combined into $Comb^k$, which later is merged with $S_k$ to get back $I^k$. Thus, this scheme can flexibly encrypt multiple spatial resolutions of the same original image into the ciphertext. And it allows for selective decryption of the original image at any spatial resolution level starting from the smallest image to the biggest one. While we have illustrated PMRVCS for spatial resolutions, it can similarly be applied for reconstructing different quality images of the same size.

## IV. Experimental Results

In this section, we would like to describe the experimental results and its evaluation. Please note that for all the resultant images shown in this paper, they have been scaled down to the same size so as to fit the page requirements. As a result, there could be a loss in quality. Please refer to our web page for the actual result images at their original quality and spatial resolution: *http://www.comp.nus.edu.sg/~mohan/pvc.html*. Figure 7 is the sample output after applying visual cryptography to a grayscale image. Figure 7(a) is the original image, figure 7(b) is the image after halftoning, figure 7(c) & 7(d) are the shares generated by our visual cryptography scheme and figure 7(e) is the reconstructed image using the OR operation. Figure 7(f) shows the reconstruction using the XOR operation which reveals that the halftone image can be completely recovered.

Figure 8 is the sample output when color visual cryptography is applied. Figure 8(a) is the original image, figure 8(b) is the corresponding halftone image, figure 8(c) & 8(d) are the generated shares. Figure 8(e) & 8(f) are the reconstructed images using the OR (stacking) and XOR operations respectively.

Figure 9 demonstrates the extraction of multiple images from the single creation of shares as well as perfect restoration. Figure 9(a) is the original color image, figure 9(b) is the transformed image using our proposed encoding scheme. Figure 9(c) & 9(d) are the two shares created. Figure 9(e) is the reconstructed image using OR and figure 9(f) is the reconstructed image using XOR. Figure 9(g) is the extracted halftone image and figure 9(h) is the perfectly restored image.

Figure 10 demonstrates the multiresolution visual cryptography scheme (MRVCS). Figure 10(a) is the original image, figure 10(b) is the common share and Figure 10(c)-10(e) are the other shares. Figure 10(f)-10(h) are the three reconstructed images by XORing every share with the common share. Figure 10(i)-10(k) are the extracted halftone images at the three resolutions. Figure 10(l)-10(n) are the perfectly recovered images at the three resolutions.

Figure 11 demonstrates the progressive multiresolution visual cryptography scheme (PMRVCS). Figure 11(a) is the original image, Figure 10(b)-10(e) are the shares. Figure 11(f)-11(h) are the three reconstructed images by using the first 2, 3 and 4 shares. Figure 11(i)-11(k) are the halftone images extracted from the images of figure 11(f)-11(h) correspondingly. Figure 11(l)-11(n) are the perfectly restored images from those of Figure 11(f)-11(h).

In summary, our experimental results reveal that:

- Our novel visual cryptography scheme provides a complete solution for all types of images - binary, grayscale, halftone and color.

- Our new encoding scheme is simple and fast. It allows multiple images to be extracted from the same set of shares, with a very small overhead factor of $\frac{1}{8}$.
- Our novel encoding scheme allows for seamless handling of multiple resolutions of images in a progressive manner for all types of images.
- The quality problem of visual cryptography has been solved with the establishment of the feasibility of perfect restoration of the original image.
- Yet it still preserves the crucial advantages of visual cryptography which are simplicity and perfect security.

## V. Conclusion

In this paper, we have extended traditional visual cryptography by employing new schemes which overcome its limitations. We first propose a technique for grayscale and color visual cryptography. Our insight is that the OR operation in the traditional visual cryptography can be replaced by the XOR operation in order to allow for lossless decryption. We then develop a new encoding scheme based on a $3 \times 3$ microblock and its corresponding look-up table to encrypt and losslessly restore a color image. Our scheme is tremendously flexible in the sense that the encryption can be decrypted in three ways to obtain decrypted images of three different qualities (binary, halftone and original). We then build on several schemes to provide for progressive multiresolution visual cryptography. These schemes allow for flexible encryption of images which can enable decryption of scalable qualities and spatial resolutions.

Visual Cryptography allows easy decoding of the secret image by a simple stacking of the printed share transparencies. However, there are some practical issues that need careful consideration. First, the transparencies should be precisely aligned in order to obtain a clear reconstruction. Secondly, there is usually some unavoidable noise introduced during the printing process. Thirdly, the stacking method can only simulate the *OR* operation which always leads to a loss in contrast.

Proper alignment is absolutely essential when superimposing the shares. In real experiments, we have found that obtaining perfect alignment is always troublesome. As visual cryptographic schemes operate at the pixel levels, each pixel on one share must be matched correctly with the corresponding pixel on the other share. Superimposing the shares with even a slight shift in alignment results in a drastic degradation in the quality of the reconstructed image. In the worst case, even a single pixel shift can render the secret image totally invisible. This alignment problem can be resolved if the boundary of each share is clearly marked which can act as guides for the alignment.

For future work, we aim to work on developing robust techniques for print and scan applications

of visual cryptography. We are also considering some practical applications of visual cryptography for watermarking and digital rights management. We believe that the techniques developed in this paper will serve as a basis for all these future investigations.

## ACKNOWLEDGEMENT

Wei-Qi Yan's work is supported by a fellowship from Singapore Millennium Foundation (SMF). We deeply appreciate the constructive suggestions of the anonymous reviewers.

## REFERENCES

[1] M. Naor and A. Shamir, "Visual cryptography," in *Advances in Cryptology -EUROCRYPT'94*, A. D. Santis., Ed., vol. 950. Springer-Verlag, 1995, pp. 1–12.

[2] H. R. Kang, *Digital Color Halftoning*, ser. SPIE/IEE Series on Imaging Science and Engineering, E. R. Dougherty, Ed. Bellingham, Washington USA and New York: Copublished by SPIE Optical Engineering Press and IEEE Press, 1999.

[3] M. Naor and A. Shamir, "Visual cryptography 2: Improving the contrast via the cover base," 1996, a preliminary version appears in "Security Protocols", M. Lomas ed. Vol. 1189 of Lecture Notes in Compute Science, Springer-Verlag, Berlin, pp.197-202, 1997.

[4] A. D. S. G. Ateniese, C. Blundo and D. R. Stinson, "Constructions and bounds for visual cryptography," in *23rd International Colloquium on Automata, Languages and Programming*, ser. Lecture Notes in Computer Science, F. M. auf der Heide and B. Monien, Eds., vol. 1099. Berlin: Springer-Verlag, 1996, pp. 416–428.

[5] C. Blundo, P. D'Arco, A. D. Snatis, and D. R. Stinson, "Contrast optimal threshold visual cryptography schemes," *SIAM Journal on Discrete Mathematics, available at: http://citeseer.nj.nec.com/blundo98contrast.html*, vol. 16, no. 2, pp. 224–261, April 1998.

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

[7] Y. Desmedt and T. V. Le, "Moire cryptography," in *the 7th ACM Conference on Computer and Communications Security '00*, Athens, Greece, 2000.

[8] V. Rijmen and B. Preneel, "Efficient color visual encryption for shared colors of benetton," 1996, EUCRYPTO'96 Rump Session. Availabe at http://www.iacr/org/conferences/ec96/rump/preneel.ps.

[9] Y. C. Hou, C. Y. Chang, and S. F. Tu, "Visual cryptography for color images based on halftone technology," in *International Conference on Information Systems, Analysis and Synthesis. World Multiconference on Systemics, Cybernetics and Informatics. Image, Acoustic, Speech And Signal Processing: Part II*, 2001.

[10] M. Naor and B. Pinkas, "Visual authentication and identification," *Lecture Notes in Computer Science*, vol. 1294, pp. 322–336, 1997. [Online]. Available: citeseer.nj.nec.com/67294.html

[11] Q. B. Sun, P. R. Feng, and R. Deng, in *International Conference on Information Technology: Coding and Computing (ITCC '01), available at: http://dlib.computer.org/conferen/itcc/1062/pdf/10620065.pdf*, Las Vegas, April 2001.

[12] S.-S. Lee, J.-C. Na, S.-W. Sohn, C. Park, D.-H. Seo, and S.-J. Kim, "Visual cryptography based on an interferometric encryption technique," *ETRI Journal*, vol. 24, pp. 373–380, 2002, available at http://etrij.etri.re.kr/etrij/pdfdata/24-05-05.pdf.

[13] D. L. Lau and G. R. Arce, *Modern Digital Halftoning*, ser. Signal Processing and Communications Series. New York: Marcel Dekker, Inc, 2001.

[14] R. Ulichney, *Digital Halftoning*. Cambridge, Mass: The MIT Press, 1987.

[15] P. C. Chang, C. S. Yu, and T. H. Lee, "Hybrid LMS-MMSE inverse halftoning technique," *IEEE Transactions on Image Processing*, vol. 10, no. 1, pp. 95–103, January 2001.

[16] M. Mee and P. P. Vaidyanathan, "Look up table (LUT) inverse halftoning," *IEEE Transactions on Image Processing*, vol. 10, no. 10, pp. 1566–1578, 2001. [Online]. Available: citeseer.nj.nec.com/535989.html

[17] G. B. Unal and A. E. Cetin, "Restoration of error-diffused images using projection onto convex sets," *IEEE Transactions on Image Processing*, vol. 10, no. 12, pp. 1836–1841, December 2001. [Online]. Available: citeseer.nj.nec.com/526555.html

[18] M. Gnanaguruparan and S. Kak, "Recursive hiding of secrets in visual cryptography," *Cryptologia*, vol. 26, pp. 68–76, 2002.

**Duo Jin** received his bachelor degree and master degree of computer science from School of Computing, National University of Singapore in 2002 and 2003 respectively. His research interest is information retrieval on encrypted domain.

**Wei-Qi Yan** received his Ph.D. degree from Chinese Academy of Sciences in 2001. He is a research fellow with School of Computing, National University of Singapore. His research interests are media security and multimedia artifacts removal.

**Mohan S. Kankanhalli** is a faculty member in School of Computing, National University of Singapore. Dr. Kankanhalli received his master and Ph.D. degree in computer and systems engineering from the Rensselaer polytechnic Institute, New York USA. His research interests are multimedia systems and information security.

TABLE I

A COMPARISON BETWEEN XOR AND OR

| **Secret Image** | **Shares** | **OR** | **XOR** |
|---|---|---|---|
| 0 | $\begin{bmatrix}1 & 0\\1 & 0\end{bmatrix}, \begin{bmatrix}1 & 0\\1 & 0\end{bmatrix}$ | $\begin{bmatrix}1 & 0\\1 & 0\end{bmatrix}$ | $\begin{bmatrix}0 & 0\\0 & 0\end{bmatrix}$ |
| 1 | $\begin{bmatrix}1 & 0\\1 & 0\end{bmatrix}, \begin{bmatrix}0 & 1\\0 & 1\end{bmatrix}$ | $\begin{bmatrix}1 & 1\\1 & 1\end{bmatrix}$ | $\begin{bmatrix}1 & 1\\1 & 1\end{bmatrix}$ |

TABLE II

THE MICROBLOCK ENCODING LOOK-UP TABLE

| $g_{orig}$ | $g_{new}$ | $g_{orig}$ | $g_{new}$ | $g_{orig}$ | $g_{new}$ | $g_{orig}$ | $g_{new}$ | $g_{orig}$ | $g_{new}$ |
|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 1 | 2 | 2 | 3 | 4 | 4 | 8 |
| 5 | 16 | 6 | 32 | 7 | 64 | 8 | 128 | 9 | 3 |
| 10 | 5 | 11 | 6 | 12 | 9 | 13 | 10 | 14 | 12 |
| 15 | 17 | 16 | 18 | 17 | 20 | 18 | 24 | 19 | 33 |
| 20 | 34 | 21 | 36 | 22 | 40 | 23 | 48 | 24 | 65 |
| 25 | 66 | 26 | 68 | 27 | 72 | 28 | 80 | 29 | 96 |
| 30 | 129 | 31 | 130 | 32 | 132 | 33 | 136 | 34 | 144 |
| 35 | 160 | 36 | 192 | 37 | 7 | 38 | 11 | 39 | 13 |
| 40 | 14 | 41 | 19 | 42 | 21 | 43 | 22 | 44 | 25 |
| 45 | 26 | 46 | 28 | 47 | 35 | 48 | 37 | 49 | 38 |
| 50 | 41 | 51 | 42 | 52 | 44 | 53 | 49 | 54 | 50 |
| 55 | 52 | 56 | 56 | 57 | 67 | 58 | 69 | 59 | 70 |
| 60 | 73 | 61 | 74 | 62 | 76 | 63 | 81 | 64 | 82 |
| 65 | 84 | 66 | 88 | 67 | 97 | 68 | 98 | 69 | 100 |
| 70 | 104 | 71 | 112 | 72 | 131 | 73 | 133 | 74 | 134 |
| 75 | 137 | 76 | 138 | 77 | 140 | 78 | 145 | 79 | 146 |
| 80 | 148 | 81 | 152 | 82 | 161 | 83 | 162 | 84 | 164 |
| 85 | 168 | 86 | 176 | 87 | 193 | 88 | 194 | 89 | 196 |
| 90 | 200 | 91 | 208 | 92 | 224 | 93 | 15 | 94 | 23 |
| 95 | 27 | 96 | 29 | 97 | 30 | 98 | 39 | 99 | 43 |
| 100 | 45 | 101 | 46 | 102 | 51 | 103 | 53 | 104 | 54 |
| 105 | 57 | 106 | 58 | 107 | 60 | 108 | 71 | 109 | 75 |
| 110 | 77 | 111 | 78 | 112 | 83 | 113 | 85 | 114 | 86 |
| 115 | 89 | 116 | 90 | 117 | 92 | 118 | 99 | 119 | 101 |
| 120 | 102 | 121 | 105 | 122 | 106 | 123 | 108 | 124 | 113 |
| 125 | 114 | 126 | 116 | 127 | 120 | 128 | 135 | 129 | 139 |
| 130 | 141 | 131 | 142 | 132 | 147 | 133 | 149 | 134 | 150 |
| 135 | 153 | 136 | 154 | 137 | 156 | 138 | 163 | 139 | 165 |
| 140 | 166 | 141 | 169 | 142 | 170 | 143 | 172 | 144 | 177 |
| 145 | 178 | 146 | 180 | 147 | 184 | 148 | 195 | 149 | 197 |
| 150 | 198 | 151 | 201 | 152 | 202 | 153 | 204 | 154 | 209 |
| 155 | 210 | 156 | 212 | 157 | 216 | 158 | 225 | 159 | 226 |
| 160 | 228 | 161 | 232 | 162 | 240 | 163 | 31 | 164 | 47 |
| 165 | 55 | 166 | 59 | 167 | 61 | 168 | 62 | 169 | 79 |
| 170 | 87 | 171 | 91 | 172 | 93 | 173 | 94 | 174 | 103 |
| 175 | 107 | 176 | 109 | 177 | 110 | 178 | 115 | 179 | 117 |
| 180 | 118 | 181 | 121 | 182 | 122 | 183 | 124 | 184 | 143 |
| 185 | 151 | 186 | 155 | 187 | 157 | 188 | 158 | 189 | 167 |
| 190 | 171 | 191 | 173 | 192 | 174 | 193 | 179 | 194 | 181 |
| 195 | 182 | 196 | 185 | 197 | 186 | 198 | 188 | 199 | 199 |
| 200 | 203 | 201 | 205 | 202 | 206 | 203 | 211 | 204 | 213 |
| 205 | 214 | 206 | 217 | 207 | 218 | 208 | 220 | 209 | 227 |
| 210 | 229 | 211 | 230 | 212 | 233 | 213 | 234 | 214 | 236 |
| 215 | 241 | 216 | 242 | 217 | 244 | 218 | 248 | 219 | 63 |
| 220 | 95 | 221 | 111 | 222 | 119 | 223 | 123 | 224 | 125 |
| 225 | 126 | 226 | 159 | 227 | 175 | 228 | 183 | 229 | 187 |
| 230 | 189 | 231 | 190 | 232 | 207 | 233 | 215 | 234 | 219 |
| 235 | 221 | 236 | 222 | 237 | 231 | 238 | 235 | 239 | 237 |
| 240 | 238 | 241 | 243 | 242 | 245 | 243 | 246 | 244 | 249 |
| 245 | 250 | 246 | 252 | 247 | 127 | 248 | 191 | 249 | 223 |
| 250 | 239 | 251 | 247 | 252 | 251 | 253 | 253 | 254 | 254 |
| 255 | 255 | | | | | | | | |

Figure list:



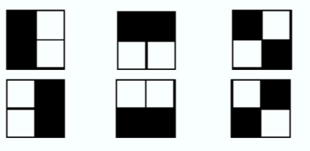
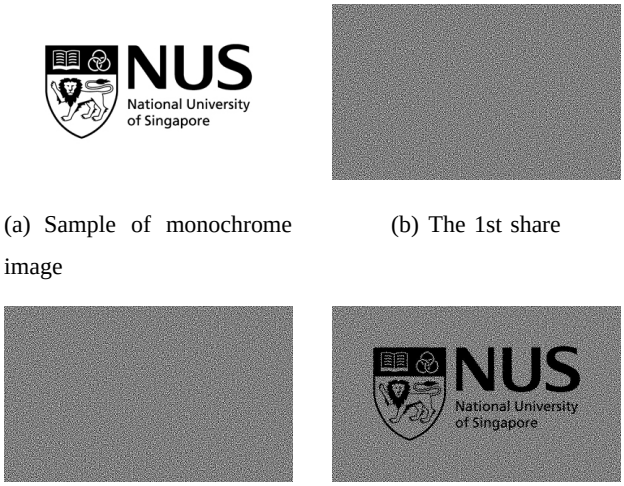


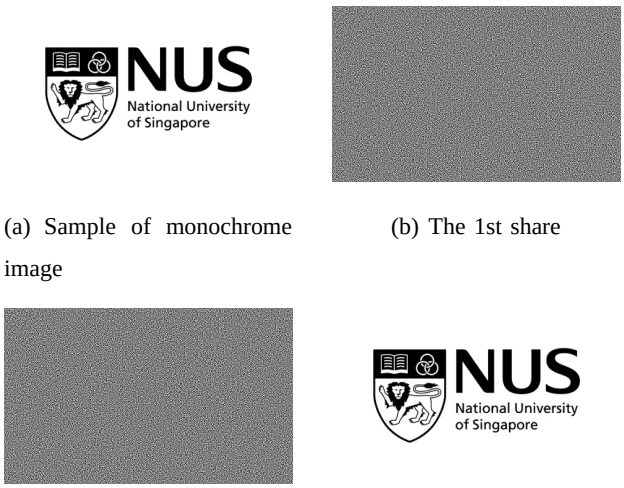
Fig. 1. The six patterns of 4-pixel shares: vertical, horizontal and diagonal.



(a) Sample of monochrome image (b) The 1st share

(c) The 2nd share (d) Stacked image

Fig. 2. Example of (2,2)-VCS for monochrome images.



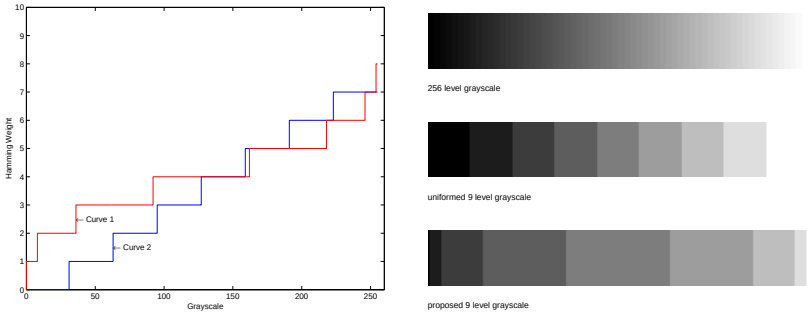
(a) Sample of monochrome image (b) The 1st share

(c) The 2nd share (d) Stacked image with XOR

Fig. 3. Example of (2,2)-VCS for monochrome images with XOR

$$\begin{bmatrix} b_4 & b_0 & b_6 \\ b_2 & 0 & b_3 \\ b_7 & b_1 & b_5 \end{bmatrix}$$

Fig. 4. Positioning of the eight bits inside a microblock.




(a) Grayscale levels distribution curve (b) Grayscale tones

Fig. 5. Grayscale levels distribution using proposed encoding scheme.

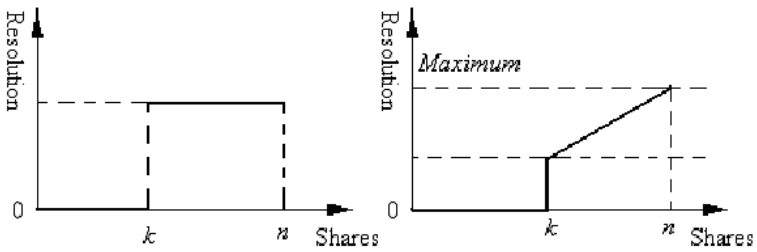
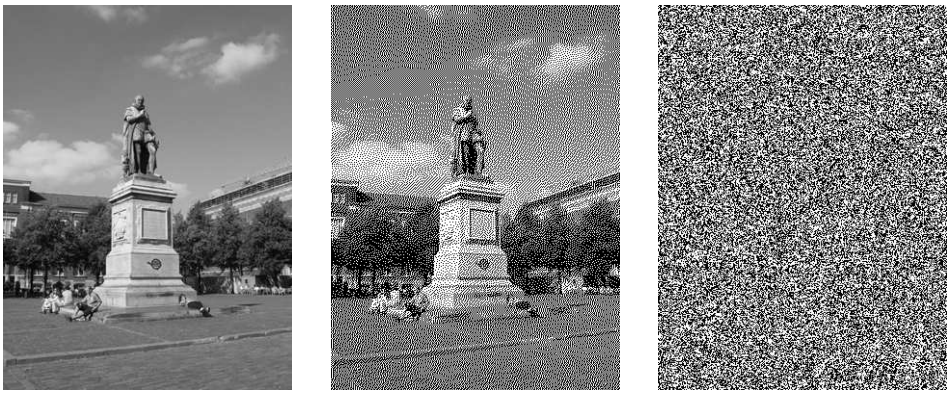
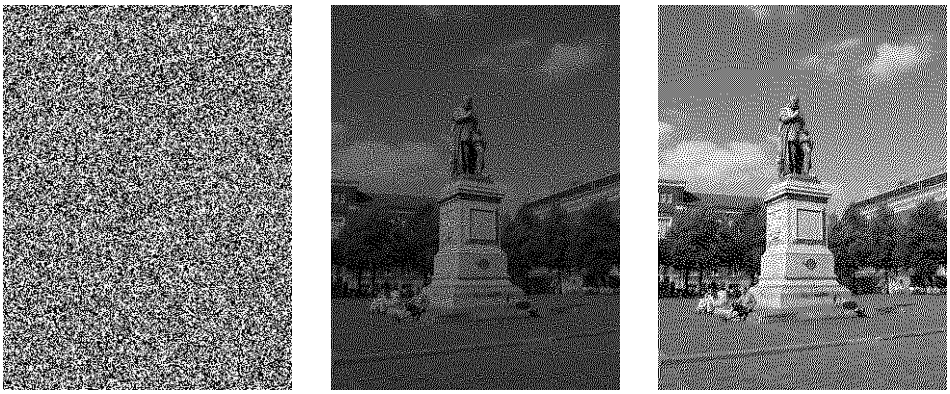



Fig. 6. The difference between traditional visual cryptography and progressive multiresolution visual cryptography.



(a) Original grayscale image (b) Halftone image (c) The 1st share $S_0$



(d) The 2nd share $S_1$ (e) Stacked image using $OR(S_0, S_1)$ (f) Stacked image using $XOR(S_0, S_1)$

Fig. 7. (2,2)-VCS for a grayscale image.

(a) Original color image

(b) Halftone image

(c) The 1st share $S_0$

(d) The 2nd share $S_1$

(e) Stacked image using $OR(S_0, S_1)$

(f) Stacked image using $XOR(S_0, S_1)$

Fig. 8. (2,2)-VCS for a color image.

(a) Original color image

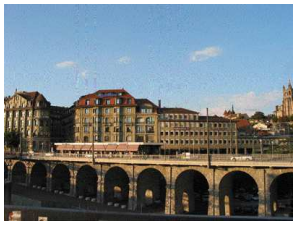
(b) Transformed image by combining three monochrome channels of CMY

(c) The 1st share $S_0$

(d) The 2nd share $S_1$

(e) Stacked image using $OR(S_0, S_1)$

(f) Stacked image using $XOR(S_0, S_1)$



(g) Extracted halftoned image

(h) Extracted color image using perfect restoration

Fig. 9. Perfect restoration and multiple image extraction.

(a) Original color image

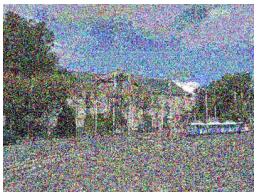
(b) The common share $S_c$

(c) The 1st share $S_0$

(d) The 2nd share $S_1$

(e) The 3rd share $S_2$

(f) Reconstructed image by $XOR(S_0, S_c)$



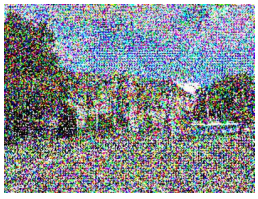
(g) Reconstructed image by $XOR(S_1, S_c)$

(h) Reconstructed image by $XOR(S_2, S_c)$

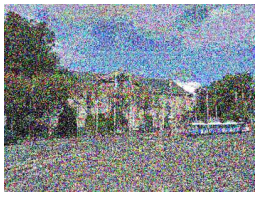
(i) Extracted halftone image from $XOR(S_0, S_c)$

(j) Extracted halftone image from $XOR(S_1, S_c)$

(k) Extracted halftone image from $XOR(S_2, S_c)$



(l) Perfectly restored image from $XOR(S_0, S_c)$

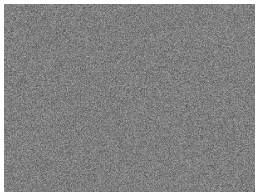


(m) Perfectly restored image from $XOR(S_1, S_c)$

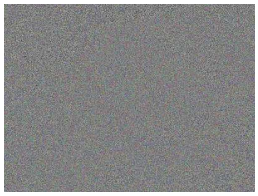
(n) Perfectly restored image from $XOR(S_2, S_c)$

Fig. 10. Multiresolution visual cryptography (MRVCS).

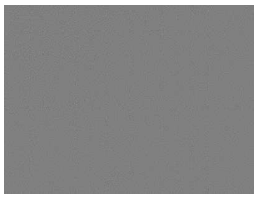
(a) Original color image



(b) The 1st share $S_0$

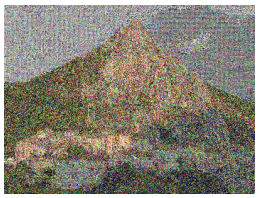


(c) The 2nd share $S_1$

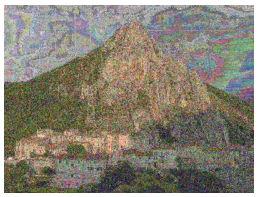


(d) The 3rd share $S_2$

(e) The 4th share $S_3$



(f) Reconstructed image from $(S_0, S_1)$



(g) Reconstructed image from $(S_0, S_1, S_2)$

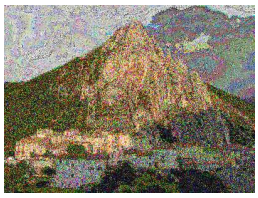
(h) Reconstructed image from $(S_0, S_1, S_2, S_3)$

(i) Extracted halftone image from $(S_0, S_1)$

(j) Extracted halftone image from $(S_0, S_1, S_2)$

(k) Extracted halftoned image from $(S_0, S_1, S_2, S_3)$

(l) Perfectly restored image from $(S_0, S_1)$



(m) Perfectly restored image from $(S_0, S_1, S_2)$

(n) Perfectly restored image from $(S_0, S_1, S_2, S_3)$

Fig. 11. Progressive multiresolution visual cryptography (PMRVCS).