# Halftone visual cryptography

**Article** *in* IEEE Transactions on Image Processing · September 2006

DOI: 10.1109/TIP.2006.875249 · Source: PubMed



**3 authors**, including:

Giovanni Di Crescenzo
Applied Communication Sciences
**196** PUBLICATIONS **7,700** CITATIONS

SEE PROFILE

# Halftone Visual Cryptography

Zhi Zhou, *Member, IEEE*, Gonzalo R. Arce, *Fellow, IEEE*, and Giovanni Di Crescenzo

***Abstract*—Visual cryptography encodes a secret binary image (SI) into $n$ shares of random binary patterns. If the shares are xeroxed onto transparencies, the secret image can be visually decoded by superimposing a qualified subset of transparencies, but no secret information can be obtained from the superposition of a forbidden subset. The binary patterns of the $n$ shares, however, have no visual meaning and hinder the objectives of visual cryptography. Extended visual cryptography [1] was proposed recently to construct meaningful binary images as shares using hypergraph colourings, but the visual quality is poor. In this paper, a novel technique named halftone visual cryptography is proposed to achieve visual cryptography via halftoning. Based on the blue-noise dithering principles, the proposed method utilizes the void and cluster algorithm [2] to encode a secret binary image into $n$ halftone shares (images) carrying significant visual information. The simulation shows that the visual quality of the obtained halftone shares are observably better than that attained by any available visual cryptography method known to date.**

***Index Terms*—Blue noise halftoning, digital halftoning, digital watermarking, error diffusion, secret sharing, steganography, visual cryptography.**

## I. Introduction

VISUAL CRYPTOGRAPHY (VC) is a type of secret sharing scheme introduced by Naor *et al.* [3], [4]. In a $t$-out-of-$n$ scheme of VC, a secret binary image (SI) is cryptographically encoded into $n$ shares of random binary patterns. The $n$ shares are xeroxed onto $n$ transparencies, respectively, and distributed amongst $n$ participants, one for each participant. No participant knows the share given to another participant. Any $t$ or more participants can visually reveal the secret image by superimposing any $t$ transparencies together. The secret cannot be decoded by any $t-1$ or fewer participants, even if infinite computational power is available to them.

Being a type of secret sharing scheme, visual cryptography can be used in a number of applications including access control. For instance, a bank vault must be opened every day by three tellers, but for security purposes, it is desirable not to entrust any single individual with the combination. Hence, a vault-access system that requires any two of the three tellers may be desirable. This problem can be solved using a two-out-of-three threshold scheme. Aside from the obvious application to access control, secret sharing schemes are used in a number of other cryptographic protocols and applications such as threshold cryptography, private multiparty computations, electronic cash and digital elections. More specifically, visual threshold schemes have found immediate applications in certain types of cryptographic protocols, including authentication and identification [5], and copyright protection and watermarking [6], [7].

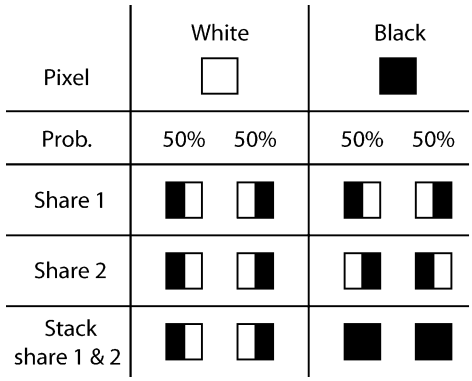



Fig. 1. Construction of a two-out-of-twoVC scheme: a secret pixel can be encoded into two subpixels in each of the two shares.

To illustrate the principles of VC, consider the simplest two-out-of-two visual threshold scheme where each pixel $p$ of the SI is encoded into a pair of subpixels in each of the two shares. If $p$ is white, one of the two columns tabulated under the white pixel in Fig. 1 is selected. If $p$ is black, one of the two columns tabulated under the black pixel is selected. In each case, the selection is performed by randomly flipping a fair coin, such that each column has 50% probability to be chosen. Then, the first two pairs of subpixels in the selected column are assigned to share 1 and share 2, respectively. Since, in each share, $p$ is encoded into a black–white or white–black pair of subpixels with equal probabilities, independent of whether $p$ is black or white, an individual share gives no clue as to the value of $p$. In addition, as each pixel is encrypted independently, no secret information can be gained by looking at groups of pixels in each share. Now consider the superposition of the two shares as shown in the last row of Fig. 1. If a pixel $p$ is white, the superposition of the two shares always outputs one black and one white subpixel, no matter which column of subpixel pairs is chosen during encoding. If $p$ is black, it yields two black subpixels. There is a contrast loss in the reconstruction, however, the decoded pixel is readily visible.

As an example, encoding the secret image shown in Fig. 2(a) leads to the two shares shown in Fig. 2(b) and (c), respectively. Superimposing these two shares leads to the output secret as

Manuscript received November 19, 2003; revised July 25, 2005. This work was prepared through collaborative participation in the Communications and Networks Consortium sponsored by the U.S. Army Research Laboratory under the Collaborative Technology Program, Cooperative Agreement DAAD19-01-2-0011. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Zhigang (Zeke) Fan.

Z. Zhou and G. R. Arce are with the Department of Electrical and Computer Engineering, University of Delaware, Newark, DE 19716 USA (e-mail: zzhou@ece.udel.edu; arce@ece.udel.edu).

G. Di Crescenzo is with the Mathematical Sciences Research Center, Telcordia Technologies, Inc., Morristown, NJ 07960 USA (e-mail:giovanni@research.telcordia.com).

Digital Object Identifier 10.1109/TIP.2006.875249

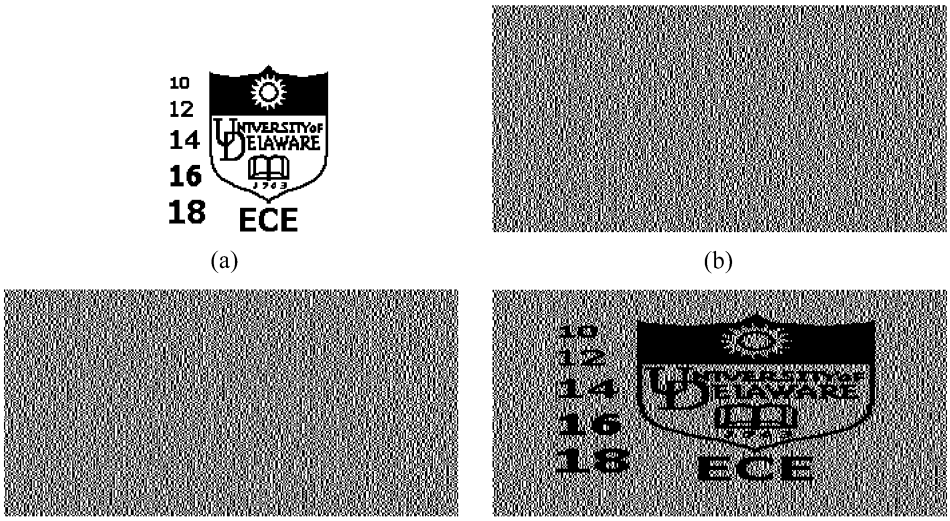



Fig. 2. Two-out-of-two VC scheme: (a) the secret image was encoded into (b), (c) the two shares, and was (d) decoded by superimposing these two shares with 50% loss of contrast. (a) Secret image. (b) Share 1. (c) Share 2. (d) Decoded image.

shown in Fig. 2(d). The decoded image is clearly identified, although some contrast loss is observed. Some binary pixels appear to be "grey" due to the shrinking of the image for layout purpose, which are observed in other binary images in Section III, as well. The width of the decoded image is twice that of the original secret image since each pixel $p$ is expanded to two subpixels in each share as shown in Fig. 1. This effect is referred to as *pixel expansion*.

The two-out-of-two visual threshold scheme demonstrates a special case of $t$-out-of-$n$ schemes [3], [4], [8]–[10]. A more general model for visual sharing schemes based on general access structures has been recently studied in [11], [12], where all qualified and forbidden subsets of the participants are defined. The participants in a qualified subset can recover the secret image while the participants in a forbidden subset cannot. The properties of a $t$-out-of-$n$ scheme including the conditions needed for optimal contrast and the minimum pixel expansion attainable can be found in [8]–[10]. The concepts of VC have been recently extended such that the secret image is allowed to be a grey-level image rather than a binary image [13], [14]. Although the secret image is grey scale, shares are still constructed by random binary patterns. In [15] and [16], the concepts are further generalized where a secret color image is encrypted into shares consisting of randomly distributed color pixels.

As described above, all of these VC methods suffer from a severe limitation, which hinders the objectives of VC. The limitation lies in the fact that all shares are inherently random patterns carrying no visual information, raising the suspicion of data encryption. Very recently, the method referred to as extended VC has been implemented in [1], where hypergraph colourings are used aimed at constructing meaningful binary images as shares. Extended VC, however, provides very low quality visual information in the shares, as illustrated later in this paper. Since hypergraph colourings are constructed by random distributed pixels, the resultant binary shares contain strong white noise consequently leading to inadequate results. The shares also suffer from low contrast between hypergraph black and hypergraph white pixels.

This paper focuses on developing a general halftone visual cryptography framework, where a secret binary image is encrypted into high-quality halftone images, or *halftone shares*. In particular, the proposed method applies the rich theory of blue noise halftoning to the construction mechanism used in conventional VC to generate halftone shares, while the security properties are still maintained. The same contrast is obtained over the whole decoded image. The halftone shares carry significant visual information to the viewers, such as landscapes, buildings, etc. The visual quality obtained by the new method is significantly better than that attained by extended VC or any other available VC method known to date.

This paper is organized as follows. Section II introduces the fundamental principles of visual cryptography, based on which halftone visual threshold methods are proposed to construct the simplest two-out-of-two scheme and, further, a general access structure scheme. Section III shows the simulation results of the proposed method. Finally, conclusions are drawn in Section IV.

## II. Halftone Visual Cryptography

### A. Fundamental Principles of VC

The proposed halftone VC is built upon the model of general access structures developed by G. Ateniese *et al.* [11]. The model describes a set of qualified subsets $\Gamma_{\mathrm{Qual}}$ and a set of forbidden subsets $\Gamma_{\mathrm{Forb}}$ on $n$ participants $\mathcal{P} = \{1, 2, \ldots, n\}$. The participants of any qualified subset can jointly decode the secret image, while those from a forbidden subset cannot. The pair $(\Gamma_{\mathrm{Qual}}, \Gamma_{\mathrm{Forb}})$ is called the access structure of the scheme.

Denote $2^{\mathcal{P}}$ as the set of all subsets of $\mathcal{P}$. We obtain $\Gamma_{\mathrm{Qual}} \subseteq 2^{\mathcal{P}}$, $\Gamma_{\mathrm{Forb}} \subseteq 2^{\mathcal{P}}$, and $\Gamma_{\mathrm{Qual}} \cap \Gamma_{\mathrm{Forb}} = \phi$ since there is no participant subset that can be both qualified and forbidden simultaneously. If the participants in a subset $X \in \Gamma_{\mathrm{Qual}}$ can decode the secret image, usually, the participants in any superset $Y$ of $X$ $(X \subset Y)$ should be able to decode the secret image as well. Thus, $Y \in \Gamma_{\mathrm{Qual}}$. Such $\Gamma_{\mathrm{Qual}}$ is called *monotone increasing*. If the participants in a subset $X \in \Gamma_{\mathrm{Forb}}$ cannot decode the secret image, usually, the participants in any $Y$, a subset of $X$

$(Y \subset X)$, should not be able to decode the secret image either. Thus, $Y \in \Gamma_{\mathrm{Forb}}$. Such $\Gamma_{\mathrm{Forb}}$ is called *monotone decreasing*. If $\Gamma_{\mathrm{Qual}}$ is monotone increasing, $\Gamma_{\mathrm{Forb}}$ is monotone decreasing and $\Gamma_{\mathrm{Qual}} \cup \Gamma_{\mathrm{Forb}} = 2^{\mathcal{P}}$, then the access structure is said to be *strong* [11]. Let $\Gamma_0 = \{X \in \Gamma_{\mathrm{Qual}}: Y \notin \Gamma_{\mathrm{Qual}} \text{ for all } Y \subset X\}$ be the set of all minimal qualified subsets. In a strong access structure, $\Gamma_{\mathrm{Qual}}$ is the *closure* of $\Gamma_0$. Thus, $\Gamma_0$ is termed a *basis*, from which a strong access structure can be derived. Unless otherwise specified, only strong access structures are discussed in this paper, which is the usual setting for the traditional secret sharing. If $\Gamma_{\mathrm{Qual}}$ contains a single-element subset, such a subset can be trivially dealt with by just directly distributing the secret (image) to the only participant. The $n$-participant access structure, thus, can be decomposed into a one-participant access structure and an $(n-1)$-participant access structure. Without loss of generality, we assume that each subset in $\Gamma_{\mathrm{Qual}}$ contains at least two participants. The aforementioned concepts are illustrated in the following Example 2.1.

*Example 2.1:* The strong access structure $(\Gamma_{\mathrm{Qual}}, \Gamma_{\mathrm{Forb}})$ of the two-out-of-three scheme can be written as $\Gamma_{\mathrm{Qual}} = \{\{1,2\}, \{2,3\}, \{1,3\}, \{1,2,3\}\}$, and $\Gamma_{\mathrm{Forb}} = \{\phi, \{1\}, \{2\}, \{3\}\}$. It can be verified that $\Gamma_{\mathrm{Qual}}$ is monotone increasing and $\Gamma_{\mathrm{Forb}}$ is monotone decreasing. Let $X = \{1,2,3\} \in \Gamma_{\mathrm{Qual}}$ and $Y = \{1,2\} \subset X$. Since $Y \in \Gamma_{\mathrm{Qual}}$, it follows that $X$ is not in $\Gamma_0$, that is, $X \notin \Gamma_0$. Now let $X = \{1,2\} \in \Gamma_{\mathrm{Qual}}$. Any $Y \subset X$ satisfies $Y \notin \Gamma_{\mathrm{Qual}}$, so $X \in \Gamma_0$. The same results can be obtained on $\{2,3\}$ and $\{1,3\}$. Such that $\Gamma_0 = \{\{1,2\}, \{2,3\}, \{1,3\}\}$.

In conventional VC, a secret binary pixel $p$ is encoded into $m$ subpixels in each of the $n$ shares, where $m$ is the pixel expansion. These subpixels can be described as a $n \times m$ Boolean matrix $M$, where a value 0 corresponds to a white subpixel and a value 1 corresponds to a black subpixel. The $i$th $(i = 1,2,\ldots,n)$ row of $M$, denoted as $r_i$, contains the subpixels to be assigned to the $i$th share. Let $X = \{i_1, i_2, \ldots, i_s\}$ denote the indices of a subset of shares assigned to $s$ participants. Superimposing the shares in $X$ is equivalent to an OR-logical operation on the corresponding rows $r_{i_k}$ $(k = 1,2,\ldots,s)$ of M, resulting in a row vector $V = \mathrm{OR}(r_{i_1}, r_{i_2}, \ldots, r_{i_s})$. The grey level of the reconstructed pixel $p$, obtained by such superimposing, is proportional to the Hamming weight of $V$, denoted as $w(V)$. In Definition 2.1, the construction conditions of matrix $M$ are given so as to satisfy the requirements of conventional VC.

*Definition 2.1 ([11]):* Let $(\Gamma_{\mathrm{Qual}}, \Gamma_{\mathrm{Forb}})$ be an access structure on a set of $n$ participants. Two collections of $n \times m$ Boolean matrices $C_0$ and $C_1$ constitute a VC scheme if there exist a value $\alpha(m)$ and values $t_X$ for every $X$ in $\Gamma_{\mathrm{Qual}}$ satisfying the following.

1) *Contrast condition:* any (qualified) subset $X = \{i_1, i_2, \ldots, i_u\} \in \Gamma_{\mathrm{Qual}}$ of $u$ participants can recover the secret image by stacking the corresponding transparencies. Formally, we define for a matrix $M \in C_j$ $(j = 0,1)$ the row vectors $V_j(X,M)$ as the OR of the rows $r_{i_1}, r_{i_2}, \ldots, r_{i_u}$ in $M$. It holds that

$$w(V_0(X,M)) \le t_X - \alpha(m) \cdot m, \text{ for all } M \in C_0 \quad (1)$$

and

$$w(V_1(X,M)) \ge t_X, \text{ for all } M \in C_1. \quad (2)$$

2) *Security Condition:* any (forbidden) subset $X = \{i_1, i_2, \ldots, i_v\} \in \Gamma_{\mathrm{Forb}}$ of $v$ participants has no information of the secret image. Formally, the two collections of $v \times m$ matrices $D_j$ $(j = 0,1)$, formed by extracting rows $i_1, i_2, \ldots, i_v$ from each matrix in $C_j$, are indistinguishable.

In the above definition, $t_X$ is the *threshold* to visually interpret the reconstructed pixel as black or white, and $\alpha(m)$ is called the *relative difference* referred to as the contrast of the decoded image. From (1) and (2), it can be obtained that

$$t_X = \min(w(V_1(X,M)))$$

over all matrices $M \in C_1$ and

$$\alpha(m) = \frac{\min(w(V_1(X,M))) - \max(w(V_0(X,M)))}{m}$$

over all $X$ and $M$. Given $C_0$ and $C_1$, the matrix $M$ is randomly selected from $C_0$ if the secret pixel $p$ is white, and from $C_1$ if $p$ is black.

*Definition 2.2 ([11]):* Two matrices $S^0$, $S^1$ are called *basis matrices*, if the two collections $C_0$ and $C_1$ in Definition 2.1 are obtained by permuting the columns of $S^0$, $S^1$ in all possible ways, respectively, and $S^0$, $S^1$ satisfy the following two conditions.

1) *Contrast condition:* if $X = \{i_1, i_2, \ldots, i_u\} \in \Gamma_{\mathrm{Qual}}$, the row vectors $V_0$ and $V_1$, obtained by performing OR operation on rows $i_1, i_2, \ldots, i_u$ of $S^0$ and $S^1$, respectively, satisfy $w(V_0) \le t_X - \alpha(m) \cdot m$ and $w(V_1) \ge t_X$.
2) *Security Condition:* if $X = \{i_1, i_2, \ldots, i_v\} \in \Gamma_{\mathrm{Forb}}$, one of the two $v \times m$ matrices, formed, respectively, by extracting rows $i_1, i_2, \ldots, i_v$ from $S^0$ and $S^1$, equals to a column permutation of the other.

The construction of the basis matrices is a topic of study in conventional VC. Several design procedures, such as the method using cumulative arrays, are readily available [11]. An example of $S^0$, $S^1$, $C_0$, and $C_1$ is given next to illustrate the above-mentioned concepts.

*Example 2.2:* The basis matrices and the collections of the encoding matrices in the conventional two-out-of-two scheme (shown in Fig. 1) can be written as

$$S^0 = \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}, \quad S^1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad (3)$$

$$C_0 = \left\{ \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix} \right\}$$

$$C_1 = \left\{ \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \right\}. \quad (4)$$

In this example, the pixel expansion is $m = 2$. For any matrix $M \in C_0$, the row vector $V_0 = \mathrm{OR}(r_1, r_2)$ satisfies $w(V_0) = 1$. For any $M \in C_1$, the row vector $V_1 = \mathrm{OR}(r_1, r_2)$ satisfies $w(V_1) = 2$. Thus, the two-out-of-two visual threshold scheme can be implemented by using these two collections. The secret image can be visually decoded with the threshold

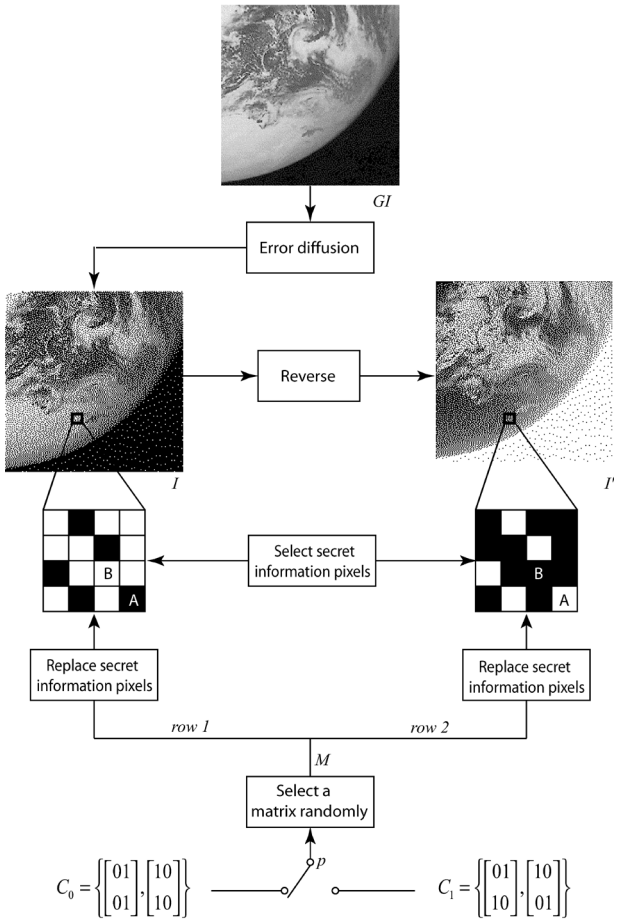



Fig. 3. Construction of a two-out-of-two scheme. Cell size is $Q = 4$.

$t_X = \min(w(V_1)) = 2$, having a relative difference $\alpha(m) = ((\min(w(V_1)) - \max(w(V_0)))/m) = (1/2)$.

Halftone VC is built upon the basis matrices and collections available in conventional VC. In particular, in halftone VC a secret binary pixel $p$ is encoded into an array of $Q_1 \times Q_2$ subpixels, referred to as a *halftone cell*, in each of the $n$ shares. The pixel expansion in halftone VC is thus $Q_1 Q_2$. Generally, a square halftone cell, obtained when $Q_1 = Q_2$, leads to undistorted reconstructed images and is used in our simulations. By using halftone cells with an appropriate size, visually pleasing halftone shares can be obtained, while the contrast and security conditions are still maintained. In Section II-B, the proposed algorithm is introduced by constructing a two-out-of-two scheme. The method is subsequently extended into a general access structure scheme.

### B. Two-out-of-Two Halftone Visual Cryptography Method

To describe the principles of halftone VC, the simplest two-out-of-two halftone visual threshold scheme is shown in Fig. 3. In the proposed method, a halftone image $I$, obtained by applying any halftoning method such as the error diffusion algorithm [17] on a grey level image GI, is assigned to participant 1, and its complementary image $\bar{I}$, obtained by reversing all black/white pixels of $I$ to white/black pixels, is assigned to participant 2. To encode a secret pixel $p$ into a $Q_1 \times Q_2$ halftone cell in each of the two shares, only two pixels, referred to as the

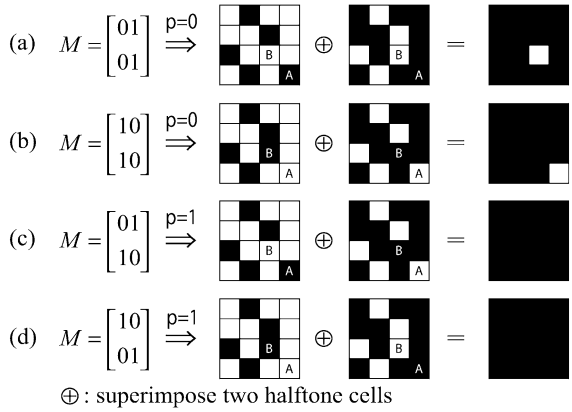



Fig. 4. Replacing the secret information pixels with the corresponding subpixels in a matrix $M$, which is randomly selected as (a), (b) from $C_0$ if $p = 0$, or (c), (d) from $C_1$ if $p = 1$. The secret pixel $p$ can be visually decoded by superimposing the two shares.

*secret information pixels*, in each halftone cell need to be modified. The two secret information pixels should be at the same positions in the two shares, such as pixels $A$ and $B$ in Fig. 3. If $p$ is white, a matrix $M$ is randomly selected from the collection of matrices $C_0$ of conventional VC. If $p$ is black, $M$ is randomly selected from $C_1$. The secret information pixels in the $i$th $(i = 1, 2)$ share are replaced with the two subpixels in the $i$th row of $M$, as shown in Fig. 4. Since $C_0$ and $C_1$ are the collections of conventional VC, these modified pixels carry the encoded secret. The other pixels in the halftone cell which were not modified are referred to as *ordinary pixels*, maintaining halftone information. It can also be found that if $p$ is white, one out of $Q_1 Q_2$ pixels in the reconstructed halftone cell, obtained by superimposing the two encoded halftone cells, is white while all other pixels are black [see Fig. 4(a) and (b)]. If $p$ is black, all pixels in the reconstructed halftone cell are black, as shown in Fig. 4(c) and (d). Thus, the contrast condition is satisfied. The secret pixel $p$ can be visually decoded with contrast $(1/Q_1 Q_2)$.

In the above procedure, the selection of the secret information pixels in a halftone cell is important as it affects the visual quality of the resultant halftone shares. However, as long as their locations are independent of the secret information, it will be proved shortly that such construction satisfies the security condition. The simplest method to select the locations of the secret information pixels is random selection. The corresponding pixel replacements, however, are equivalent to adding white noise, which leads to poor visual quality. To obtain better visual results, the void and cluster algorithm [2] is applied to choose these pixel locations. The void and cluster algorithm, performed on a binary dither pattern of the halftone cell, first applies a low-pass finite-impulse response (FIR) filter to obtain a measure of minority pixel density (m.p.d.) at each minority pixel location. The minority pixel is white/black and the majority pixel is black/white, if the halftone cell contains more black/white pixels. The minority pixel with the highest density, denoted as pixel $A$, is replaced with a majority pixel. The dither pattern is then filtered again by the same low-pass FIR filter to obtain a measure of m.p.d. at each majority pixel location. The majority pixel (different from pixel $A$) with the lowest density, denoted as pixel $B$, is then replaced with a minority pixel. Since the

complementary pair has the same distribution of the minority and majority pixels, the located pixels $A$ and $B$ are at the same positions in the two shares. The void and cluster algorithm, in essence, identifies the minority pixel $A$ with the highest m.p.d. and the majority pixel $B$ with the lowest m.p.d., and switches their locations. This, in effect, spreads the minority pixels as homogeneously as possible leading to an improved blue noise[1] halftone cell in each share.

The locations of the secret information pixels are then chosen as that of the pixels $A$ and $B$. Once the matrix $M$ is randomly selected, the $j$th $(j = 1, 2)$ located secret information pixel in the $i$th $(i = 1, 2)$ share is replaced with the $j$th subpixel in the $i$th row of $M$. The replacement in each share either keeps their original values or switches them with equal probabilities. If the values are kept original, the blue noise halftone cell, generated by the error diffusion algorithm, is used, e.g., the first halftone cell in Fig. 4(a) and (c), and the second halftone cell in Fig. 4(b) and (c). On the other hand, if the values are switched, the new blue noise halftone cell, generated by the void and cluster algorithm, is used, e.g., the first halftone cell in Fig. 4(b) and (d), and the second halftone cell in Fig. 4(a) and (d). Visually pleasing halftone shares are thus obtained.

In the void and cluster algorithm, generally, the filter window covers multiple neighboring halftone cells besides the one currently being processed. If a white secret pixel $p = 0$ was encoded into one of the neighboring halftone cells, there is discrepancy in the distribution of the minority/majority pixels between two shares, such as Fig. 4(a) and (b). If the conventional void and cluster algorithm [2] is performed on each share, it may result in different locations of the secret information pixels in the two shares, which is highly undesirable in the halftone VC scheme. To address this problem, a slightly modified void- and cluster-finding filter, as shown in (5), is used to find the m.p.d.

$$\mathrm{DA}(x,y) = \sum_{p=-W/2}^{W/2} \sum_{q=-W/2}^{W/2} f(p,q) \cdot P(x+p, y+q) \quad (5)$$

where $\mathrm{DA}(x,y)$ is the m.p.d. of the pixel with coordinate $(x,y)$, $f(p,q)$ is the filter, also called weighting function, $W$ is the filter's window width, and $P(x+p, y+q)$ is the pixel value at $(x+p, y+q)$ defined as follows:

$$P(x+p,y+q) = \begin{cases} 0.5, & \text{if } P(x+p,y+q) \text{ is a secret informational pixel} \\ 1, & \text{if } P(x+p,y+q) \text{ is a minority pixel} \\ 0, & \text{if } P(x+p,y+q) \text{ is a majority pixel.} \end{cases} \quad (6)$$

The Gaussian filter is used in [2] as

$$f(p,q) = \exp\left(-\frac{p^2+q^2}{2\sigma^2}\right) \quad (7)$$

[1]Minority pixels distributed homogeneously create a pattern containing no low-frequency spectral components, which is referred to as blue noise halftoning since the spectrum resembles that of blue light. From our understanding of the human visual system, blue noise halftoning creates the visually optimal arrangement of dots [17].

where $\sigma$ is a scalar constant, offering best results at $\sigma = 1.5$ in the void and cluster algorithm based on Ulichney's simulations. Unlike the conventional void- and cluster-finding filter, each secret information pixel in the previously processed neighboring cells always takes the value 0.5 in our method, regardless if it is a minority or majority pixel, as shown in (6). The value 0.5 is the statistical mean of each secret information pixel, because it has equal probability to be a minority or majority pixel. The above modification of the void and cluster algorithm guarantees that the selection of the secret information pixels $A$ and $B$ is independent of the value of any secret information pixel in the previous halftone cells. Thus, no secret can be inferred from the locations of the secret information pixels which can be detected by comparing the original halftone image and the corresponding halftone share. In addition, since the values of secret information pixels come from the basis matrices/collections of conventional VC, no secret can be obtained by looking at the values of secret information pixels of one share either. Thus, the proposed halftone visual threshold scheme is fully secure.

The above proposed construction implements a two-out-of-two halftone VC scheme with a pixel expansion $m^h = Q_1 Q_2$ and relative difference $\alpha^h(Q_1, Q_2) = (1/Q_1 Q_2)$, where the superscript "$h$" indicates that the parameters are for halftone VC. Visually pleasing halftone shares are generated by the blue noise halftoning techniques and the secret image can be reconstructed by superimposing the two shares. The peak signal-to-noise ratio (PSNR) of each halftone share, compared to its original halftone image, can be estimated as

$$\begin{aligned} \mathrm{PSNR} &= 10 \log \frac{255^2}{|0-255|^2 \cdot \frac{2}{Q_1 Q_2} \cdot 50\%} \\ &= 10 \log Q_1 Q_2 \end{aligned} \quad (8)$$

where the item $|0 - 255|$ denotes the value difference of switching a secret information pixel, the item $(2/Q_1 Q_2)$ indicates that two out of $Q_1 Q_2$ pixels are secret information pixels, and the item 50% indicates that each secret information pixel is either unmodified or switched with equal probabilities. Thus, the larger the halftone cell size, the higher the PSNR. Also, better performance of the void and cluster algorithm can be obtained in larger halftone cells, leading to higher visual quality halftone shares. On the contrary, the relative difference $\alpha^h(Q_1, Q_2)$ is proportional to the reciprocal of the cell size. Larger halftone cell sizes lead to lower contrast of the decoded secret image. Therefore, a tradeoff exists between the visual quality of the halftone shares and the contrast of the reconstructed secret image. This will be illustrated shortly. In addition, the share size is usually limited. If the number of subpixels is increased, the size of subpixels becomes smaller, which leads to difficulty of superimposing.

### C. General Halftone Visual Cryptography

In this section, the technique underlying the two-out-of-two halftone visual threshold scheme is extended to a scheme for an arbitrary access structure $(\Gamma_{\mathrm{Qual}}, \Gamma_{\mathrm{Forb}})$, where a secret binary image SI is hidden into $n$ halftone shares. The resulting scheme can be divided into two phases; first, an assignment of complementary pairs of images is done to the participants so

that each qualified subset in $\Gamma_{\mathrm{Qual}}$ contains at least one complementary pair of images; second, in each of the shares, a secret pixel $p$ is encoded into a $Q_1 \times Q_2$ halftone cell, and $m$ ($m < Q_1Q_2$) secret information pixels in each halftone cell are selected and replaced with the corresponding subpixels in the basis matrices/collections of conventional VC, where $m$ and $Q_1Q_2$ are the pixel expansions of conventional VC and halftone VC, respectively.

In the two-out-of-two halftone VC scheme, each participant was assigned a single halftone image. In the method for an arbitrary access structure, we may require more halftone images to be assigned to each participant. A halftone image is generated by the method of blue noise halftoning, or pixel reversal if a complementary pair of halftone images is necessary. Recall that the complementary pair of halftone images used in the two-out-of-two halftone VC scheme guarantees that the superposition of ordinary pixels in two halftone cells are all black. Hence, all secret pixels can be consistently decoded using the same visual threshold. In a similar fashion, the halftone image assignment in the general scheme must satisfy that any qualified subset of participants contains at least one complementary pair of halftone images. Since $\Gamma_{\mathrm{Qual}}$ is a closure of $\Gamma_0$, it is equivalent to require that any subset $X \in \Gamma_0$ contains at least one complementary pair of halftone images. This requirement, however, may not be satisfiable for all access structures unless we distribute more than one image per participant. For instance, in the two-out-of-three halftone VC scheme, $\Gamma_{\mathrm{Qual}}$ is a closure of $\Gamma_0 = \{\{1,2\},\{1,3\},\{2,3\}\}$. If a complementary pair of halftone images is assigned to participants 1 and 2, respectively, a single third halftone image cannot be a reversal of both the first and the second halftone images at the same time. An immediate way to overcome this limitation consists of independently generating two complementary pairs of images $(I_1, \bar{I}_1)$ and $(I_2, \bar{I}_2)$, and distributing $I_1$ to participant 1, $\bar{I}_1, I_2$ to participant 2 and $\bar{I}_1, \bar{I}_2$ to participant 3. Then, the entries of the matrices of a two-out-of-two conventional VC scheme are inserted into the secret information pixels of both $(I_1, \bar{I}_1)$ and $(I_2, \bar{I}_2)$. Simple extensions of this technique to an arbitrary access structure may require distributing several images to participants. For instance, one could assign an independent complementary pair to each subset in $\Gamma_0$, thus giving $|\Gamma_0|$ images to each participant; or to each pair $i, j$ of participants, thus giving $n(n+1)/2$ images to each participant. A more efficient assignment can be the following. Assume, for simplicity, that $n = 2^k$, for some integer $k$, and let $(I_j, \bar{I}_j) = (I_{j,0}, I_{j,1})$, for $j = 1, \ldots, k$, be complementary pairs of images that were generated independently. Then, each participant $u$ is given images $I_{j,u_j}$, for $j = 1, \ldots, k$, where $u_1|\cdots|u_k$ is the binary expansion of $u$. We note that this assignment technique works for any access structure and requires only $k = \log n$ images to be distributed to each participant. Even more efficient schemes for some specific access structures can be constructed using the hypergraph decomposition techniques in [18].

From now on, we assume for simplicity that there are only $n$ images. Two collections of $n \times m$ Boolean matrices $\bar{C}_j$ ($j = 0, 1$) satisfying the contrast and security conditions need to be constructed to implement the general access structure. Furthermore, such collections should satisfy one more condition. Formally, for any matrix $M \in \bar{C}_j$, $M$ can be written as concatenation of $m/2$ submatrices of size $n \times 2$. Therefore, the $m$ secret information pixels can be selected pair by pair using the void and cluster algorithm, and the $k$th ($k = 1, 2, \ldots, m/2$) pair is replaced with the corresponding subpixels in the $k$th submatrix of $M$. The complementary pair of halftone images, which the void and cluster algorithm is performed on, is referred to as the *key complementary pair*. To obtain pleasing visual quality of the key complementary shares, it is required that the corresponding rows in each submatrix of $M$ contain one black and one white subpixels. This additional condition is referred to as *halftone condition*.

Let $S^j$ ($j = 0, 1$) be two $n \times m$ basis matrices of conventional VC. Each $S^j$ is divided into $m/2$ groups of two columns. Denote the divided basis matrices as $\bar{S}^j$, which should satisfy that the rows corresponding to the key complementary shares in each group contain one black and one white subpixels. The two collections of matrices $\bar{C}_j$ ($j = 0, 1$) are constructed by permuting the groups and/or the columns in the same group of the corresponding basis matrices $\bar{S}^j$, such that the contrast and halftone conditions are always satisfied. The permutation of columns in different groups is not allowed; otherwise, the halftone condition may not be satisfied. To verify the security condition, if $X = \{i_1, i_2, \ldots, i_v\} \in \Gamma_{\mathrm{Forb}}$ is a forbidden subset of $v$ participants, the two collections of $v \times m$ matrices $\bar{D}_j$ ($j = 0, 1$), formed by extracting the rows $i_1, i_2, \ldots, i_v$ from each matrix in $\bar{C}_j$, should be indistinguishable. We enumerate all possible ways to divide $S^j$ until the security condition is satisfied.

Once the collections $\bar{C}_j$ ($j = 0, 1$) are obtained, the encoding procedure of a secret pixel $p$ can be summarized as follows.

1) A matrix $M$ is randomly selected from the collection $\bar{C}_0$ if a secret pixel $p$ is white, or from $\bar{C}_1$ if $p$ is black. Let $k$ be the index of the pair of secret information pixels to be located. Set $k = 1$ initially.
2) The void and cluster algorithm is performed on the key complementary pair to locate the $k$th pair of secret information pixels among the ordinary pixels in each halftone cell of the $n$ shares. The two secret information pixels located in the $i$th ($i = 1, 2, \ldots, n$) share are replaced with the subpixels at row $i$, columns $2k - 1$ and $2k$ of $M$, respectively.
3) If $k < (m/2)$, increase $k$ by 1 and go back to the previous step. Otherwise, the encoding procedure is complete.

The second step of the algorithm is executed $m/2$ times, each iteration locating two secret information pixels which were not selected previously. A total of $m$ secret information pixels are found in each halftone cell. Also, each time the second step is executed, the pixel replacement in the key complementary pair results in either keeping the original values or switching the values of the two secret information pixels. In either case, the blue noise properties of halftones are kept, leading to pleasing visual quality. As to the other shares, since the selection of the secret information pixels is independent of their image contexts, the locations of the corresponding secret information pixels in these other shares are randomly distributed. Thus, the corresponding pixel replacements introduce white noise, leading to

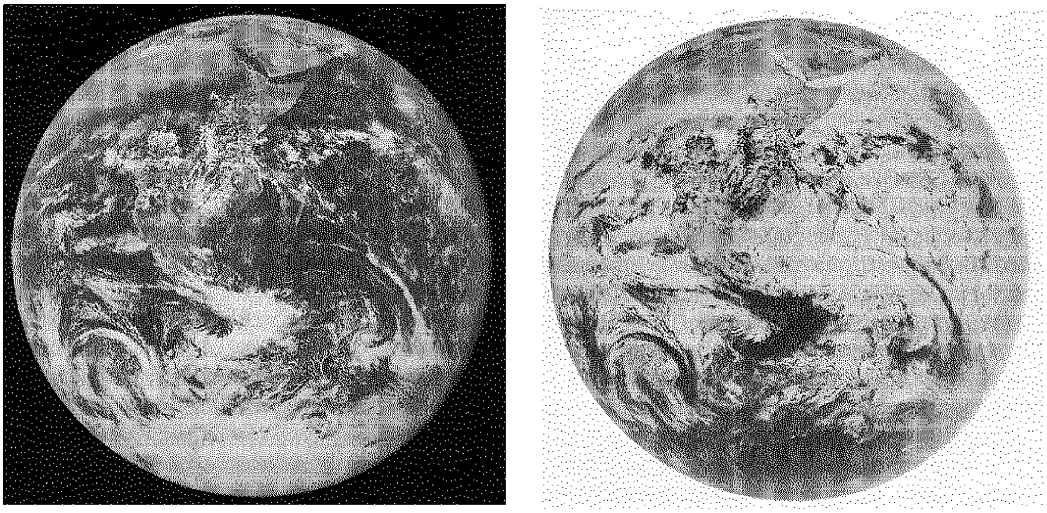


Fig. 5. Original complementary halftone images generated by error diffusion algorithm and pixel reversal, respectively.

poor visual quality of these shares. A global optimization algorithm, where the visual quality of all shares are jointly optimized, will be proposed shortly in Section II-D.

Now consider the superposition of all the shares in a qualified subset $X \in \Gamma_{\text{Qual}}$. The $Q_1Q_2 - m$ ordinary pixels in each reconstructed halftone cell are always black since $X$ contains at least one complementary pair of halftone images. According to the contrast condition in Definition 2.1, if a secret pixel $p$ is white, at most $t_X - \alpha(m)\cdot m$ out of $m$ secret information pixels are black, while all other pixels are white in the corresponding reconstructed halftone cell. Here $t_X$ and $\alpha(m)$ are the threshold and relative difference of conventional VC, respectively. If the reconstructed halftone cell is denoted as $V_0$, then the Hamming weight of $V_0$ satisfies

$$\begin{aligned} w(V_0) &\le Q_1Q_2 - m + t_X - \alpha(m)\cdot m \\ &= (Q_1Q_2 - m + t_X) - \frac{\alpha(m)\cdot m}{Q_1Q_2}\cdot Q_1Q_2. \end{aligned} \tag{9}$$

If a secret pixel $p$ is black, at least $t_X$ out of $m$ secret information pixels are black, while all other pixels are white in the corresponding reconstructed halftone cell. If the reconstructed halftone cell is denoted as $V_1$, then the Hamming weight of $V_1$ satisfies

$$w(V_1) \ge Q_1Q_2 - m + t_X. \tag{10}$$

Thus, the secret image can be visually decoded with the threshold $t_X^h = Q_1Q_2 - m + t_X$, having a relative difference $\alpha^h(Q_1, Q_2) = ((\alpha(m)\cdot m)/(Q_1Q_2))$, where the superscript "$h$" indicates that the parameters are for halftone VC.

Recall that in the modified void and cluster algorithm, the filter is used to locate all pairs of secret information pixels such that their locations are independent of the value of any secret information pixel. Therefore, the secret cannot be inferred from the location of the secret information pixels. Furthermore, the security condition of the collections $\bar{C}_0$ and $\bar{C}_1$ guarantees that no secret can be obtained from the values of the secret information pixels in any forbidden subset $X \in \Gamma_{\text{Forb}}$ either. A fully secure visual threshold scheme is thus obtained.

In the key complementary pair of shares, each pair of secret information pixels is either unmodified or switched with equal probabilities, such that the PSNR of these two shares with respect to their original halftones can be estimated by

$$\begin{aligned} \text{PSNR} &= 10\log\frac{255^2}{|0-255|^2\cdot\frac{m}{Q_1Q_2}\cdot 50\%} \\ &= 10\log\frac{Q_1Q_2}{m}. \end{aligned} \tag{11}$$

The PSNRs of the other shares depend on the distribution of black and white subpixels in the corresponding rows of $\bar{S}^j$, and they are monotone increasing functions of the cell size $Q_1 \times Q_2$ as well. Obviously, the same conclusion as in the two-out-of-two scheme can be obtained that there exists the tradeoff between the visual quality of the halftone shares and the contrast of the reconstructed secret image.

### *D. Global Optimization*

As described in the previous section, since the location of the secret information pixels is determined using the image characteristic of the key complementary pair, the location of the secret information pixels on other shares are, in essence, randomly distributed, leading to poor visual quality. To address this limitation, a global optimization approach across all halftone shares is thus proposed. Based on the void and cluster algorithm, the optimization method jointly rearranges the pixels of the $n$ shares in order to obtain better overall visual quality of the $n$ shares, while the contrast and security conditions are still maintained.

Without loss of generality, assume shares 1 and 2 are the key complementary pair among the $n$ halftone shares. The visual quality optimization method is performed on the 3rd, 4th, ..., $n$th share successively. For an arbitrary halftone cell $E$ in the $k$th ($k = 3, 4, \ldots, n$) share, the optimization algorithm is summarized as follows.

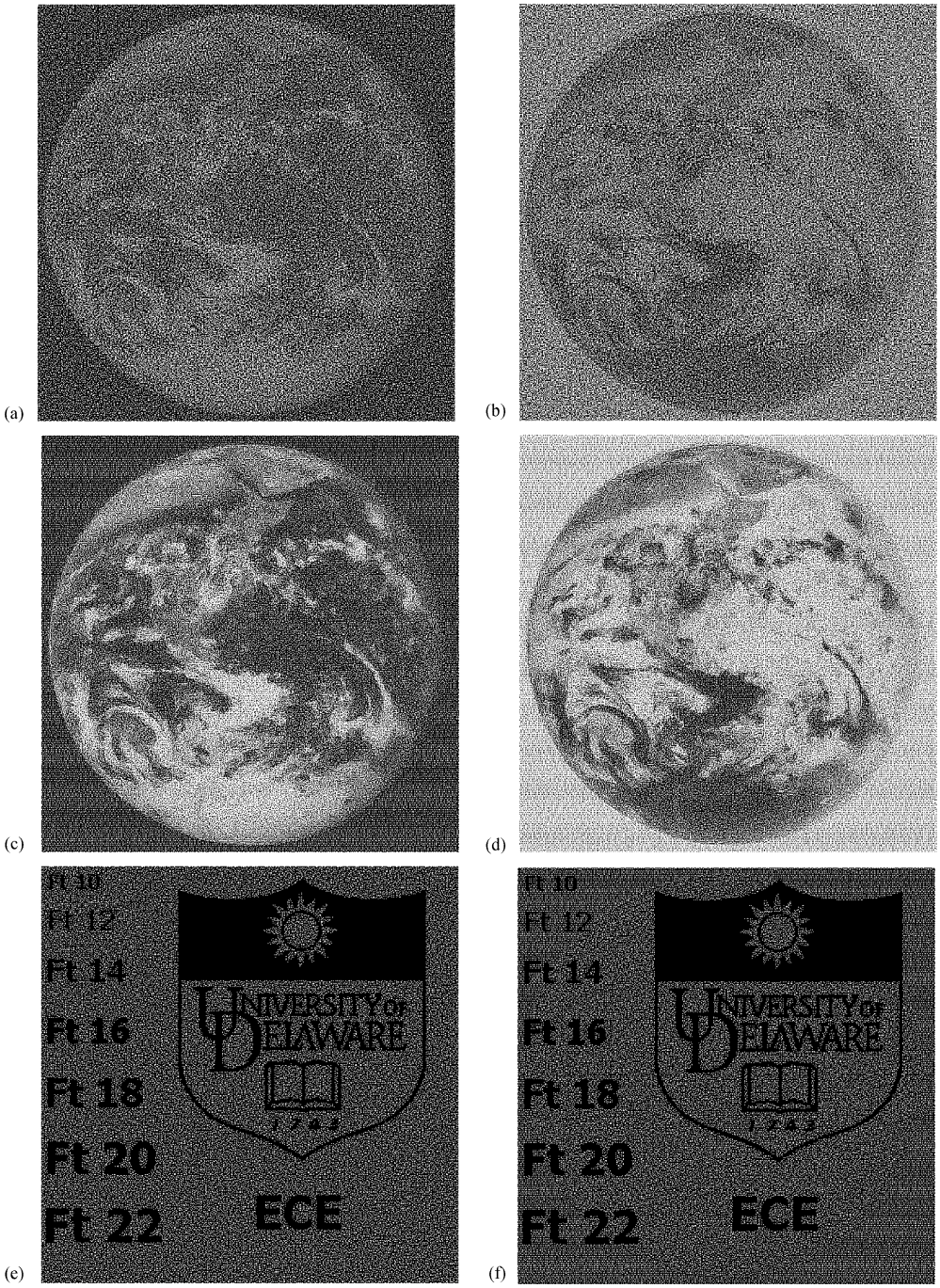



Fig. 6. Comparison between extended VC and halftone VC ($Q_1 = Q_2 = 2$). (a), (b) Two shares of extended VC. (c), (d) Two shares of halftone VC. (e) Decoded image of extended VC. (f) Decoded image of halftone VC.

1) A low-pass FIR filter is applied on the binary dither pattern of the halftone cell $E$ to obtain a measure of m.p.d. at each minority pixel location.
2) Select $r$ minority pixels with the highest densities in the halftone cell $E$. Denote the selected minority pixels as $q_i^k$ $(i = 1, 2, \ldots, r)$.
3) For each selected minority pixel $q_i^k$, select $s$ majority pixels in the halftone cell $E$ based on the void and cluster algorithm. The selection method will be described later. Denote the selected majority pixels as $g_{i,j}^k$ $(j = 1, 2, \ldots, s)$. By doing so, totally $r \times s$ switching candidates $(q_i^k, g_{i,j}^k)$ are formed.
4) For each switching candidate, estimate the global visual deterioration if such switching is performed in all of the $n$ shares.
5) Select the pair associated with the least deterioration from $r \times s$ switching candidates. Perform the switching in all of the $n$ shares.

In step 3), the void and cluster algorithm is applied to obtain $s$ majority pixels $g_{i,j}^k$ $(j = 1, 2, \ldots, s)$ for each selected minority pixel $q_i^k$. More specifically, $q_i^k$ is temporarily set to a majority pixel first. The dither pattern of the halftone cell $E$ is then filtered using the same low-pass FIR filter as in step 1) to obtain a measure of m.p.d. at each majority pixel location. Select $s$ ma-

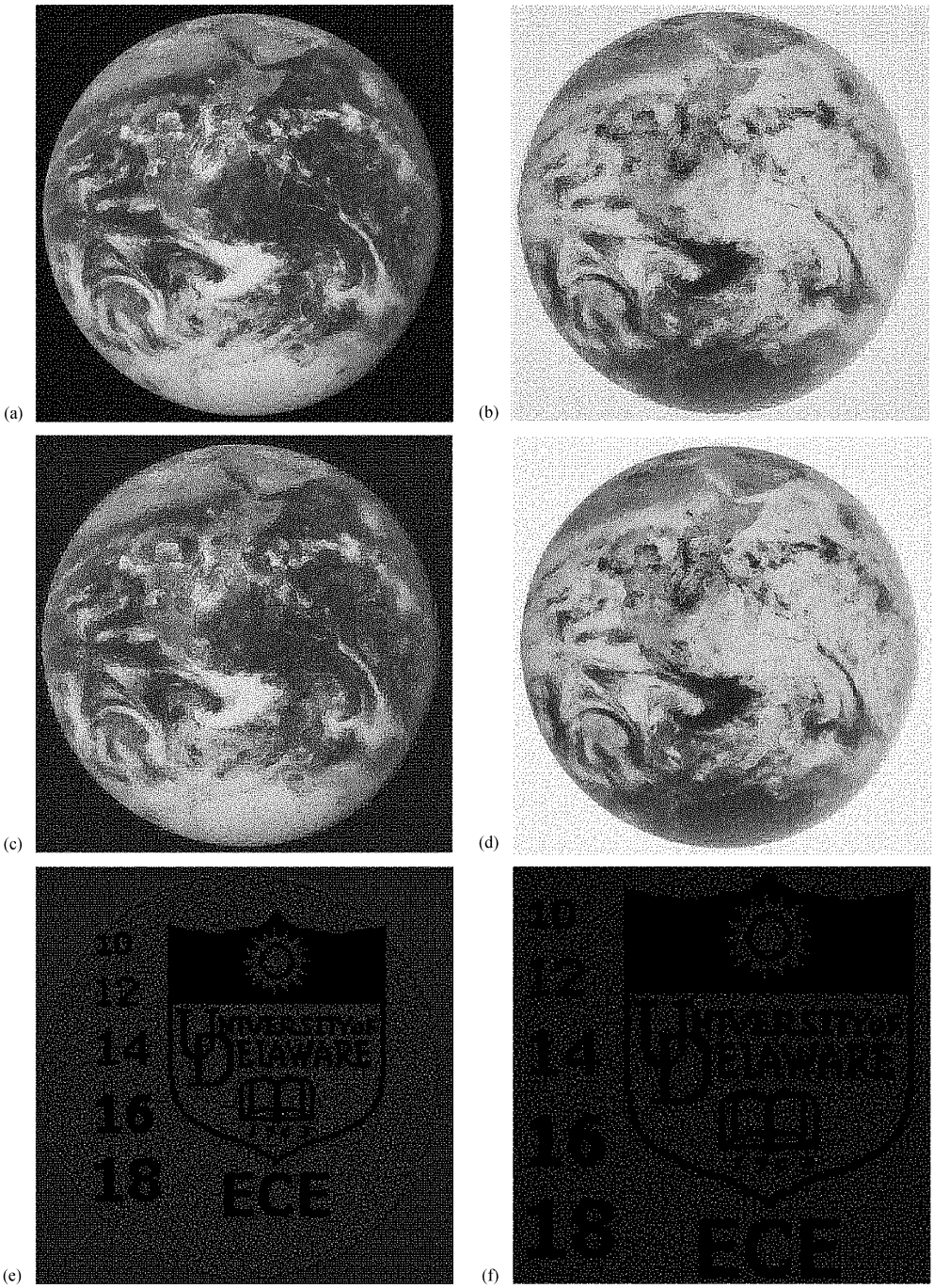



Fig. 7. Tradeoff between the quality of the shares and the contrast of the decoded image in halftone VC. (a), (b) Two shares with $Q_1 = Q_2 = 3$. (c), (d) Two shares with $Q_1 = Q_2 = 4$. (e) Decoded image of (a) and (b). (f) Decoded image of (c) and (d).

jority pixels (different from $q_i^k$) with the lowest densities, and at last set $q_i^k$ back to a minority pixel.

In step 4), for any $i$ and $j$, denote $(q_i^l, g_{i,j}^l)$ $(l = 1, 2, \ldots, k-1, k+1, \ldots, n)$ as the pixels in halftone share $l$, which have the same coordinates as $(q_i^k, g_{i,j}^k)$. When the pixels $(q_i^l, g_{i,j}^l)$ are switched with each other, it may introduce deterioration into share $l$ if $q_i^l$ and $g_{i,j}^l$ are not equal. According to halftoning theory [17], the larger the m.p.d. of the minority pixel, the less the deterioration. On the other hand, the larger the m.p.d. of the majority pixel, the more the deterioration. Let $f(q_i^l)$ and $f(g_{i,j}^l)$ be the m.p.d. of $q_i^l$ and $g_{i,j}^l$, respectively. Based on the above argument, the deterioration $d_{i,j}^l$ caused by switching pixels $q_i^l$ and $g_{i,j}^l$ in the $l$th share can be measured as

$$d_{i,j}^l = \begin{cases} f\left(g_{i,j}^l\right) - f(q_i^l), & \text{if } q_i^l \text{ is a minority pixel and } g_{i,j}^l \text{ is a majority pixel} \\ f(q_i^l) - f(g_{i,j}^l), & \text{if } q_i^l \text{ is a majority pixel and } g_{i,j}^l \text{ is a minority pixel} \\ c, & \text{otherwise} \end{cases} \tag{12}$$

Fig. 8. Halftone VC scheme of $\Gamma_0 = \{\{1,2,3\},\{1,2,4\}\}$ without global optimization $(Q_1 = Q_2 = 4)$. (a)–(d) Four shares. (e) Decoded image by superimposing the shares (a)–(c). (f) Superposition of (a) and (b).

where $c$ is a constant negative value indicating no deterioration is introduced since both $q_i^l$ and $g_{i,j}^l$ are minority pixels or majority pixels. In performing the visual optimization of the halftone cell $E$ in the $k$th share, the deterioration in shares $k+1, k+2, \ldots, n$ can be ignored. Thus, the overall visual deterioration $D_{i,j}^k$ can be estimated as

$$D_{i,j}^k = \sum_{t=1}^{k-1} d_{ij}^t. \tag{13}$$

In step 5), the switching of $q_u^k$ ($q_u^l$, resp.) and $g_{u,v}^k$ ($g_{u,v}^l$, resp.), leading to the least visual deterioration of the previous $k-1$ shares, is selected as

$$(u,v) = \arg\min_{(i,j)} D_{i,j}^k. \tag{14}$$

It is observed that when the optimization method is performed on the $k$th share, the edges in the $k$th halftone image are blurred by such switching. To overcome this problem, the optimization method is only applied on the halftone cells where strong image edges are not present.


Fig. 9. Halftone VC scheme of $\Gamma_0 = \{\{1, 2, 3\}, \{1, 2, 4\}\}$ with global optimization $(Q_1 = Q_2 = 4)$. (a)–(d) Four shares. (e) Decoded image by superimposing the shares (a)–(c). (f) Superposition of (a) and (b).

The first three steps of the above algorithm search $r \times s$ switching candidates. In the last two steps, one and only one pair will be selected from the candidates based on the least global deterioration criterion, and the switching is performed in all of the $n$ shares. The visual quality of the $k$th share is improved, since the minority pixels are more homogeneously spread by such switching. The contrast condition is maintained since the switching is performed in all of the $n$ shares. The security condition is satisfied as well, since the selection of the switching candidates is independent of the secret information. After all the $n$ shares are optimized, with some deterioration in the key complementary pair, the visual quality of the other shares is improved, leading to better overall performance.

## III. Simulation Results

Simulation results for the proposed halftone visual threshold method are illustrated in this section, including the comparison of the proposed method with the method of extended VC. The relationship between the visual quality of the halftone shares and the contrast of the decoded secret image is also revealed. Finally, the results of the global optimization approach are illustrated.

### A. Halftone Visual Cryptography vs. Extended Visual Cryptography

To compare the result of halftone VC with that of extended VC, a $256 \times 256$ secret binary image is cryptographically encoded into two $512 \times 512$ halftone images using the two methods, respectively. The pixel expansion (halftone cell size) and the relative difference of both methods are the same, being $m = 4$ and $\alpha = (1/4)$, respectively. The original halftone images, obtained by the error diffusion algorithm and pixel reversal are shown in Fig. 5. Applying the extended VC method [1] outputs two shares with poor visual quality and low contrast as shown in Fig. 6(a) and (b). The average PSNR of these two shares with respect to their original halftones is 3.46 dB. The halftone VC method results in the two visually pleasing halftone shares shown in Fig. 6(c) and (d). The PSNR of these two halftone shares is 6.02 dB. The new method gains 2.56 dB. Having the same relative difference in both methods indicates that the same contrast of the reconstructed secret images can be obtained by both methods. This is precisely the case, as shown in Fig. 6(e) and (f). The superiority of the proposed method is that halftone shares with much better visual quality can be generated, reducing the suspicion of encrypted secret. Note that the positions of secret information pixels in halftone shares are content-based, selected by the void and cluster algorithm. It causes the appearance of some content information in reconstructed secret images, such as the shape of the earth in Fig. 6(f).

### B. Tradeoff Between the Halftone Shares Quality and the Contrast of the Decoded Secret

As stated in Sections II-B and II-C, the proposed method can generate increasingly better visual quality halftone shares, as larger cell sizes are used. For instance, if a $3 \times 3$ halftone cell size is selected, two halftone shares with $\mathrm{PSNR} = 9.54$ dB are obtained as shown in Fig. 7(a) and (b). If the halftone cell size is increased to $4 \times 4$, better visually pleasing halftone shares are obtained, each with $\mathrm{PSNR} = 12.04$ dB, as shown in Fig. 7(c) and (d). However, larger halftone cell sizes lead to lower contrast of the decoded secret image. It can be identified that the contrast of (f), the output of stacking Fig. 7(c) and (d), is lower than that of Fig. 7(e), the output of stacking Fig. 7(a) and (b). It is observed as well that when the cell size (i.e., pixel expansion) is increased, the capacity, or resolution of the secret image is reduced, as seen in Fig. 7(e) and (f).

### C. Without Global Optimization Versus Global Optimization

The halftone VC scheme of $\Gamma_0 = \{\{1,2,3\},\{1,2,4\}\}$ is implemented in this section. Select the halftone shares $\{1,2\}$ as the key complementary pair, such that every qualified subset contains one complementary pair of halftone images. Using the method described in Section II-C, the basis matrices $\bar{S}^j$ are obtained as

$$\bar{S}^0 = \left[\begin{array}{c|c} \mathbf{01} & \mathbf{01} \\ \mathbf{01} & \mathbf{10} \\ 00 & 11 \\ 00 & 11 \end{array}\right], \quad \bar{S}^1 = \left[\begin{array}{c|c} \mathbf{01} & \mathbf{01} \\ \mathbf{01} & \mathbf{10} \\ 11 & 00 \\ 11 & 00 \end{array}\right] \qquad (15)$$

where the rows in bold correspond to the key complementary pair. Applying the halftone VC based on the basis matrices (15), the obtained four shares are shown in Fig. 8(a)–(d). The secret image can be decoded by superimposing a qualified subset of shares, such as Fig. 8(e) which is the output of stacking shares 1, 2, and 3. Superimposing a forbidden subset of shares gains no secret information, such as the superposition of shares 1 and 2 shown in Fig. 8(f). The visually pleasing results obtained on the key complementary pair, shares 1 and 2, are apparent while the other shares contain white noise characteristics. Performing global optimization leads to the results shown in Fig. 9. The key complementary pair is deteriorated somewhat as shown in Fig. 9(a) and (b), but more significant gains in visual quality are obtained in non-key complementary shares as shown in Fig. 9(c) and (d). Note that the contrast and security conditions are maintained with global optimization as shown in Fig. 9(e) and (f).

## IV. Conclusion

In this paper, a general framework of halftone visual cryptography is proposed. Applying the rich theory of blue noise halftoning into the construction mechanism of conventional VC, the proposed method generates visually pleasing halftone shares carrying significant visual information. The obtained visual quality is better than that attained by any other available VC method known to date. The new method can be broadly used in a number of visual secret sharing applications which require high-quality visual images, such as watermarking, electronic cash, etc.

## References


[1] G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, "Extended capabilities for visual cryptography," *Theoret. Comput. Sci.*, vol. 250, no. 1–2, pp. 134–161, 2001.

[2] R. A. Ulichney, "The void-and-cluster method for dither airay generation," in *Proc. SPIE, Human Vision, Visual Processing, Digital Displays IV*, Sep. 1996, vol. 1913, pp. 332–343.

[3] M. Naor and A. Shamir, "Visual cryptography," *Adv. Cryptol.: EUROCRYPT, Lecture Notes Comput. Sci.*, vol. 950, pp. 1–12, 1995.

[4] ——, "Visual cryptography II: Improving the contrast via the cover base," in *Security in Communication Networks, Lecture Notes in Computer Science*. Amalfi, Italy: , 1996, vol. 1189, pp. 197–202.

[5] M. Naor and B. Pinkas, "Visual authentication and identification," *Crypto, Lecture Notes Comput. Sci.*, vol. 1294, pp. 322–340, 1997.

[6] C. Chang and H. Wu, "A copyright protection scheme of images based on visual cryptography," *Imag. Sci. J.*, vol. 49, no. 3, pp. 141–150, 2001.

[7] C. Wang, S. Tai, and C. Yu, "Repeating image watermarking technique by the visual cryptography," *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.*, vol. E83A, no. 8, pp. 1589–1598, Aug. 2000.

[8] C. Blundo, A. De Santis, and D. R. Stinson, "On the contrast in visual cryptography schemes," *J. Cryptol.: J. Int. Assoc. Cryptol. Res.*, vol. 12, no. 4, pp. 261–289, 1999.

[9] C. Blundo, P. D'Arco, A. De Santis, and D. R. Stinson, "Contrast optimal threshold visual cryptography schemes," *SIAM J. Discrete Math.*, vol. 16, no. 2, pp. 224–261, 2003.

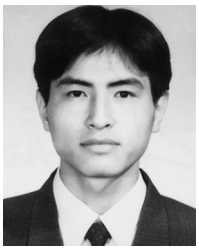
[10] T. Hofmeister, M. Krause, and H. U. Simon, "Contrast-optimal k out of n secret sharing schemes in visual cryptography," *Theoret. Comput. Sci.*, vol. 240, no. 2, pp. 471–485, Jun. 2000.

[11] G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, "Visual cryptography for general access structures," *Inf. Comput.*, vol. 129, no. 2, pp. 86–106, Sep. 1996.

[12] ——, "Constructions and bounds for visual cryptography," in *Proc. 23rd Int. Colloq. Automata, Languages and Programming*, 1996, vol. 1099, pp. 416–428.

[13] C. Blundo, A. De Santis, and M. Naor, "Visual cryptography for grey level images," *Inf. Process. Lett.*, vol. 75, pp. 255–259, 2000.

[14] L. A. MacPherson, "Grey Level Visual Cryptography for General Access Structures," M.S. thesis, Univ. Waterloo, Waterloo, ON, Canada, 2002.
[15] H. Koga and H. Yamamoto, "Proposal of a lattice-based visual secret sharing scheme for color and gray-scale images," *IEICE Trans. Fundam.*, vol. E81-A, no. 6, pp. 1263–1269, Jun. 1998.
[16] T. Ishihara and H. Koga, "New constructions of the lattice-based visual secret sharing scheme using mixture of colors," *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.*, vol. E85A, no. 1, pp. 158–166, Jan. 2002.
[17] D. L. Lau and G. R. Arce, *Modern Digital Halftoning*. New York: Marcel-Dekker, 2000, pp. 52–89.
[18] G. Di Crescenzo and C. Galdi, "Hypergraph decomposition and secret sharing," in *Proc. 14th Int. Symp. Algorithms and Computation, LNCS*, Sep. 1996, vol. 1913, pp. 332–343.



**Zhi Zhou** (M'04) received the B.S. degree in electrical engineering from the University of Science and Technology of China, Hefei, in 1997, the M.S. degree in signal processing from the Chinese Academy of Sciences, Beijing, in 2000, and the Ph.D. degree in electrical engineering from University of Delaware, Newark, in 2004.

He joined the Digital Media Solution Lab, Samsung Information Systems America, Irvine, CA, in 2003, where he is currently a Senior Research Engineer. His research interests include image and video processing, statistical and nonlinear signal processing, and multimedia security. He has eight patent applications currently pending.

**Gonzalo R. Arce** (F'00) received the Ph.D. degree from Purdue University, West Lafayette, IN, in 1982.

Since 1982, he has been with the Faculty of the Department of Electrical and Computer Engineering, University of Delaware, Newark, where he is the Charles Black Evans Distinguished Professor and Department Chairman. His research interests include statistical and nonlinear signal processing, multimedia security, electronic imaging, and signal processing for communications and networks. He is the coauthor of the textbooks *Digital Halftoning* (Marcel-Dekker, 2001), *Nonlinear Signal Processing and Applications* (CRC, 2003), and *Nonlinear Signal Processing: A Statistical Approach* (Wiley, 2004). He is a frequent consultant to industry in the areas of image printing and digital video. He holds ten U.S. patents.

Dr. Arce was the Co-Chair of the 2001 EUSIPCO/IEEE Workshop on Nonlinear Signal and Image Processing (NSIP'01), the 1991 SPIE's Symposium on Nonlinear Electronic Imaging, and the 2002 and 2003 SPIE ITCOM conferences. He has served as Associate Editor for the IEEE TRANSACTIONS ON SIGNAL PROCESSING, as Senior Editor of the *Applied Signal Processing Journal*, as Guest Editor for the IEEE TRANSACTIONS ON IMAGE PROCESSING, and as Guest Editor for *Optics Express*. He received the National Science Foundation Research Initiation Award. He is a Fellow of the IEEE for his contributions on nonlinear signal processing and its applications.

**Giovanni Di Crescenzo** received the Ph.D. degree in computer science and engineering from the University of California, San Diego, and the Ph.D. degree in applied mathematics and computer science from the University of Naples, Naples, Italy.

He is a Senior Research Scientist at Telcordia Technologies, Morristown, NJ. His main research activity has been in various areas of mathematics and theoretical computer science, such as security (intrusion detection and tolerance, password security, security over mobile *ad hoc* networks), cryptography (private-key and public-key encryption, data and entity authentication, secure protocols, financial cryptography), and computational complexity (interactive proofs, program checking, zero-knowledge proofs), and regularly uses tools from number theory, coding theory, combinatorics, and probability. He has had six patent applications awarded or currently pending, and has published more than 60 scientific publications in major refereed conferences and journals in his research areas. He regularly referees papers for the major conferences and journals in his areas of expertise.