9.6

Visual Cryptography: The Combinatorial and Halftoning Frameworks

Gonzalo R. Arce
University of Delaware

Giovanni Di Crescenzo
Telcordia Technologies

Zhi Zhou
Samsung Information Systems America

1 Introduction

Visual cryptography (VC), introduced in [15], is a recently emerging research area in cryptography, where *images* are used as an encoding of possibly secret information and *human vision* is used to perform decoding operations previously done by cryptographic algorithms run by computer. In its main paradigm, a VC scheme would require a secret binary image to be cryptographically encoded into n shares of random binary patterns. The n shares are then copied onto n transparencies respectively and distributed among n participants, one for each participant. No participant knows the share given to another participant. Any majority number of participants can visually reveal the secret image by superimposing their transparencies together. On the other hand, any minority number of participants cannot recover the secret image or even obtain any information about the secret image. Here, the security of the scheme is unconditional, not depending on any hardness of any computational problem. In other words, no information at all about the secret can be computed by any minority number of participants, even if infinite computational power is available to them.

1.1 Visual Cryptography: The Combinatorial Framework

The main instantiation of VC realizes a cryptographic protocol, called *secret sharing* (SS). In a conventional SS scheme, a secret is shared among n participants in such a way that subsets of qualified participants can pull their shares and recover the secret but subsets of forbidden participants can obtain no information about it. Here, both the sharing phase and the reconstruction phase involve algorithms that are run by computers (specifically, a dealer runs a distribution algorithm and a set of qualified parties can run a reconstruction algorithm). The surprising novelties of a visual SS scheme are in representing data as images and in an elementary realization of the reconstruction phase, consisting of just viewing the image obtained after stacking transparencies. Visual SS schemes inherits all applications of conventional SS schemes; most notably, access control. As an example, consider a bank vault that must be opened every day by five tellers, but for security purpose it is desirable not to entrust any two individuals with the combination. Hence, a vault-access system that requires any three of the five tellers

may be desirable. This problem can be solved using a 3-out-of-5 threshold scheme. In addition to access control, visual SS schemes can be applied to a number of other cryptographic protocols and applications using conventional SS, such as threshold signatures, private multiparty function evaluation, electronic cash and digital elections.

Another, quite intriguing, instantiation of VC schemes realizes visual SS with innocent-looking images as shares. This version of visual SS has applications to a multiparty variant of *steganography*. In a conventional steganography scheme, a user A sends an innocent-looking image to another user B, in such a way that B can recover some hidden image, but no observer of the communication between A and B even suspects that the communication contains some hidden image. In a multiparty variant of conventional steganography schemes, a user A sends innocent-looking images to users, $B_1, \ldots, B_n$, in such a way that qualified subsets of the recipients can recover some hidden image, but no observer of the communication between A and any of $B_1, \ldots, B_n$, even suspects the existence of hidden images. Interestingly, a version of visual SS with innocent-looking images as shares can implement this steganography variant. In practice, however, both regular visual SS and visual SS with innocent-looking images work by expanding a single pixel of an image into multiple pixels, with consequences on image quality. It is indeed of great interest to design schemes achieving high image quality.

Although the literature has paid a significant amount of attention to visual SS, some different paradigms of VC have also been studied, giving rise to visual versions of other types of cryptographic protocols, such as authentication and identification [14], and copyright protection and watermarking [8, 18]. Constructions for the latter protocols are still strongly influenced by constructions for visual SS schemes.

1.2 Visual Cryptography: The Halftoning Framework

These VC constructions are exclusively based on combinatorial techniques. In the halftoning framework for VC, a secret binary image is encrypted into high-quality halftone images, or *halftone shares*. In particular, this method applies the rich theory of blue noise halftoning to the construction mechanism used in conventional visual SS schemes to generate halftone shares, while the security properties are still maintained. The decoded secret image has uniform contrast. 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 any other available visual SS method known to date. As a result, adversaries, inspecting a halftone share, are less likely to suspect that cryptographic information is hidden. A higher security level is thus achieved.

1.3 This Chapter

The goal of this chapter is to review both the combinatorial and the halftoning frameworks for VC, paying especially attention on the latter. We start by reviewing basic notions, definitions, and combinatorial constructions of VC, focusing mostly on visual SS schemes. In particular, we present combinatorial constructions for both conventional visual SS schemes, where the shares distributed to participants are random-looking sequences of pixels and visual SS schemes with innocent-looking images as shares. We then describe in detail the halftoning framework for VC. In particular, we present one halftone visual SS scheme for the 2-out-of-2 structure and one for any arbitrary access structure. Simulation studies are presented and comparisons are drawn with the combinatorial methods for VC with innocent-loking shares.

Section 2 presents the definitions and constructions of conventional visual SS. In Section 3 we consider visual SS with innocent-looking images, by focusing on halftone visual SS methods, and showing constructions and simulation studies. Finally, additional work is cited and conclusions are drawn in Section 4.

2 Visual Secret Sharing

We review the notion of visual secret sharing, by describing the basic ideas and formal definitions for this notion in Section 2.1 and by presenting some constructions from the literature in Section 2.2.

2.1 Notion and Formal Definitions

To illustrate the principles of visual SS, consider the example of a 2-out-of-2 visual threshold scheme where each pixel p of the secret image 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 a 50% probability of being 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 information about to the value of p. In addition as each pixel is encoded 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 are chosen during encoding. If p is black, it yields two black subpixels. There is a contrast

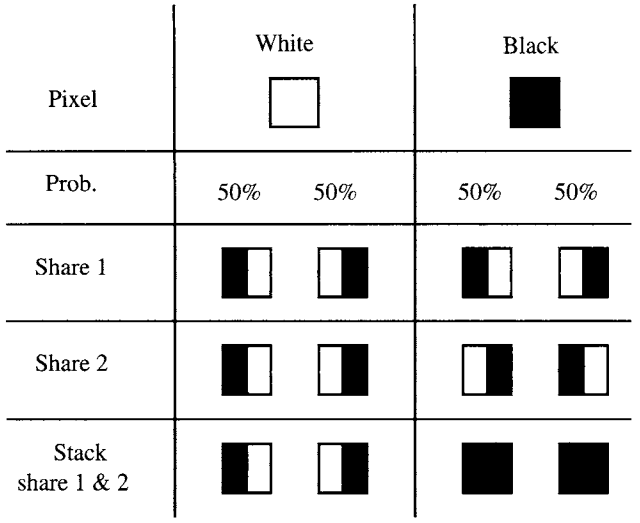


FIGURE 1 Construction of 2-out-of-2 visual SS scheme: A secret pixel can be encoded into two subpixels in each of the two shares.

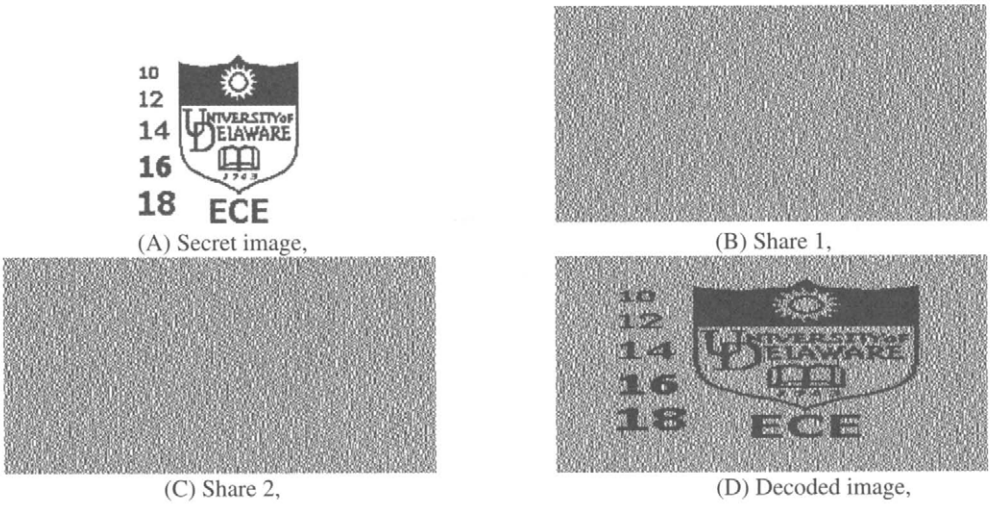
loss in the reconstruction, however, the decoded pixel is readily visible.

For instance, encoding the secret image shown in Fig. 2A leads to the two shares shown in Figs. 2B and 2C. Superimposing these two shares leads to the output secret as shown in Fig. 2D. The decoded image is clearly identified, although some contrast loss is observed. 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 scheme described demonstrates a special case of a visual threshold scheme for a specific access structure (that is, 2-out-of-2). Similar to the area of secret sharing, more general structures have been studied in the visual cryptography literature, such as t-out-of-n threshold structures (see, [6, 7, 10, 15, 16]) and arbitrary monotone access structures (see, [2, 3]), where all qualified and forbidden subsets of the participants are defined. We now proceed with a more formal treatment, by presenting a formal definition of visual secret sharing schemes and recalling constructions of such schemes from the literature.

2.1.1 Formal Modeling

Let $\mathcal{P} = \{1, 2, \ldots, n\}$ be a set of n participants, and let $2^{\mathcal{P}}$ be the set of all subsets of $\mathcal{P}$. Also, we let $\Gamma_{Qual} \subseteq 2^{\mathcal{P}}$ be a set of *qualified subsets* and $\Gamma_{Forb} \subseteq 2^{\mathcal{P}}$ and a set of *forbidden subsets* Γ_{Forb}; the pair $(\Gamma_{Qual}, \Gamma_{Forb})$ is called the *access structure* of the scheme. Thus, the access structure specifies which participants (those in Γ_{Qual}) can jointly decode the secret image, and which participants (those in Γ_{Forb}) can obtain no information at all about it. If the participants in a subset $X \in \Gamma_{Qual}$ 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, $Y \in \Gamma_{Qual}$. Such Γ_{Qual} is called *monotonically increasing*. If the participants in a subset $X \in \Gamma_{Forb}$ 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, $Y \in \Gamma_{Forb}$. Such Γ_{Forb} is called *monotonically decreasing*. If Γ_{Qual} is monotonically increasing, Γ_{Forb} is monotonically decreasing and $\Gamma_{Qual} \cup \Gamma_{Forb} = 2^{\mathcal{P}}$, then the access structure is said to be *strong*. Let $\Gamma_0 = \{X \in \Gamma_{Qual} : Y \notin \Gamma_{Qual} \text{ for all } Y \subset X\}$ be the set of all minimal qualified subsets. In a strong access structure, Γ_{Qual} is the *closure* of Γ_0. Thus, Γ_0 is termed a *basis*, from which strong access structure can be derived. Unless otherwise specified, only strong access structures are discussed in this chapter, which is the usual setting for traditional secret sharing. The aforementioned concepts are illustrated in the following Example 2.1.



(A) Secret image, (B) Share 1,

(C) Share 2, (D) Decoded image,

FIGURE 2 A 2-out-of-2 visual SS scheme: the secret image (A) was encoded into the two shares (B) and (C), and was decoded (D) by superimposing these two shares with 50% loss of contrast.

Example 2.1 *The strong access structure* $(\Gamma_{Qual}, \Gamma_{Forb})$ *of the 2-out-of-3 scheme can be written as* $\Gamma_{Qual} = \{\{1,2\}, 2,3\}, \{1,3\}, \{1,2,3\}\}$ *and* $\Gamma_{Forb} = \{\{1\},\{2\},\{3\}\}$. *It can be verified that* Γ_{Qual} *is monotonically increasing and* Γ_{Forb} *is monotonically decreasing. Let* $X = \{1,2,3\} \in \Gamma_{Qual}$ *and* $Y = \{1,2\} \subset X$. *Since* $Y \in \Gamma_{Qual}$, X *does not satisfy the definition of* Γ_0, *that is,* $X \notin \Gamma_0$. *Now let* $X = \{1,2\} \in \Gamma_{Qual}$. *Any* $Y \subset X$ *satisfies* $Y \notin \Gamma_{Qual}$, *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 visual SS, 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, called *encoding matrix*, where a matrix entry 0 corresponds to a white subpixel and a matrix entry 1 corresponds to a black subpixel. The ith $(2i = 1,2,\ldots,n)$ row of M, denoted as r_i, contains the sub-pixels to be assigned to the ith share. Let $X = \{i_1, i_2, \ldots, i_s\}$ denote the indexes of a subset of shares assigned to s participants. Superimposing the shares in X is equivalent to OR-logical operation on the corresponding rows r_{i_k} $(k = 1,2,\ldots,s)$ of M, resulting in a row vector $V = OR(r_{i_1}, r_{i_2}, \ldots, r_{i_s})$. The binary level of the reconstructed pixel p, obtained by such superimposition, 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 visual SS.

Definition 2.1 *Let* $(\Gamma_{Qual}, \Gamma_{Forb})$ *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 visual SS scheme if there exists a value* $\alpha(m)$ *and a set* $\{X, t_X\}_{X \in \Gamma_{Qual}}$ *satisfying:*

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

$$w(V_0) \leq t_X - \alpha(m) \cdot m, \tag{1}$$

and

$$w(V_1) \geq t_X. \tag{2}$$

The value $t_X = \min(w(V_1))$ *is the* threshold *to visually interpret the reconstructed pixel as black or white, and* $\alpha(m) = \frac{\min(w(V_1)) - \max(w(V_0))}{m}$ *is called the* relative *difference referred to as the contrast of the decoded image.*

2. Security condition: *Any (forbidden) subset* $X = \{i_1, i_2, \ldots, i_v\} \in \Gamma_{Forb}$ *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.*

Given C_0 and C_1, the encoding matrix M is randomly selected from C_0 if the secret pixel p is white, and from C_1 if p is black.

2.2 Some Constructions

We now review some of the most important results on the design of visual secret sharing schemes: the notion of basis matrices, and constructions of visual SS schemes for two types of threshold access structures and for any arbitrary access structure.

2.2.1 Basis Matrices

Most constructions for visual SS schemes are based on so-called basis matrices. These are two matrices S^0, S^1 satisfying some simplified contrast and security properties. It turns out that the collections of matrices C_0 and C_1 of a visual SS scheme can be defined as the collections of all matrices obtained by all possible permutations of columns in S^0 and S^1, respectively. We now present a formal definition of basis matrices.

Definition 2.2 *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* $X = \{i_1, i_2, \ldots, i_u\} \in \Gamma_{Qual}$, *the row vectors* V_0 *and* V_1, *obtained by performing OR operation on rows* $i_1, i_2, , i_u$ *of* S^0 *and* S^1 *respectively, satisfy* $w(V_0) \leq t_X - \alpha(m) \cdot m$ *and* $w(V_1) \geq t_X$.
2. Security condition: *if* $X = \{i_1, i_2, \ldots, i_v\} \in \Gamma_{Forb}$, *one of the two* $v \times m$ *matrices, formed respectively by exacting rows* $i_1, i_2, \ldots, i_v$ *from* S^0 *and* S^1, *equals to a column permutation of the other.*

An example of S^0, S^1, C_0, and C_1 is given next to illustrate these concepts.

Example 2.2 *The basis matrices and the collections of the encoding matrices in the conventional 2-out-of-2 scheme (shown in Fig.* 1*) can be written as*

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

$$C_0 = \left\{ \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix} \right\}, \; C_1 = \left\{ \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \right\}. \tag{4}$$

In this example, the pixel expansion is $m = 2$. *For any encoding matrix* $M \in C_0$, *the row vector* $V_0 = OR(r_1, r_2)$ *satisfies* $w(V_0) = 1$. *For any* $M \in C_1$, *the row vector* $V_1 = OR(r_1, r_2)$ *satisfies* $w(V_1) = 2$. *Thus, the 2-out-of-2 visual threshold scheme can be implemented by using these two collections. The secret image can be visually decoded with the threshold* $t_X = \min\ (w(V_1)) = 2$, *having a relative difference* $\alpha(m) = [\min(w(V_1)) - \max(w(V_0))]/(m) = \frac{1}{2}$.

2.2.2 Visual Secret Sharing for Threshold Access Structures

We now recall the construction in [15] of basis matrices $\hat{S}^0$ and $\hat{S}^1$ for a t-out-of-t visual SS scheme. Let $E = \{e_1, e_2, \ldots, e_t\}$ be a set of t elements. Let $\pi_1, \pi_2, \ldots, \pi_{2^{t-1}}$ be a list of all the subsets of E having even cardinality. Let $\sigma_1, \sigma_2, \ldots, \sigma_{2^{t-1}}$ be a list of all the subsets of E having odd cardinality. For $1 \le i \le t$ and $1 \le j \le 2^{t-1}$, let $\hat{S}^0[i,j]=1$ if and only if $e_i \in \pi_j$ and $\hat{S}^1[i,j] = 1$ if and only if $e_i \in \sigma_j$. As an example, when $t=3$, the basis matrices $\hat{S}^0$ and $\hat{S}^1$ are found as

$$\hat{S}^0 = \begin{bmatrix} 0110 \\ 0101 \\ 0011 \end{bmatrix}, \quad \hat{S}^1 = \begin{bmatrix} 1001 \\ 0101 \\ 0011 \end{bmatrix}. \tag{5}$$

To see that this scheme satisfies the contrast condition, we note that one column of matrix $\hat{S}^0$, the one associated with the empty subset, contains all zeros. On the other hand, no such column exist in $\hat{S}^1$. This implies that the OR of any t rows in any permutation of $\hat{S}^0$ results in a string with $2^{t-1} - 1$ ones, while the OR of any t rows in any permutation of $\hat{S}^1$ results in a string with 2^{t-1} ones.

To see that this scheme satisfies the security condition, we note that any $t-1$ rows of $\hat{S}^0$ or $\hat{S}^1$ have a similar structure: If we consider the rows as subsets of a ground set of size 2^{t-1}, every intersection of $t-1$ rows or their complement has size equal to two. Therefore, a random permutation of columns of the basis matrices gives equally distributed matrices.

2.2.3 Visual Secret Sharing for Arbitrary Monotone Structures

We now recall a construction in [3], based on cumulative arrays, of basis matrices $\hat{S}^0$ and $\hat{S}^1$ for a visual SS scheme for an arbitrary access structure. Specifically, let $(\Gamma_{Qual}, \Gamma_{Forb})$ be a strong access structure on the set $\mathcal{P} = \{1, 2, \ldots, n\}$ of participants. Let $Z_M = \{X \in \Gamma_{Forb} : X \cup \{i\} \in \Gamma_{Qual}$ for all $i \in \mathcal{P} \backslash X\}$ be the collection of the maximal forbidden sets. Assume $t = |Z_M|$ and $Z_M = \{X_1, X_2, \ldots, X_t\}$.

Example 2.3 *Let $(\Gamma_{Qual}, \Gamma_{Forb})$ be a strong access structure on the set of participants $\mathcal{P} = \{1,2,3,4\}$, where Γ_{Qual} is the closure of $\Gamma_0 = \{\{1,2,3\}, \{1,2,4\}\}$, namely, $\Gamma_{Qual} = \{\{1,2,3\}, \{1,2,4\}, \{1,2,3,4\}\}$, and $\Gamma_{Forb} = \{\{1\}, \{2\}, \{3\}, \{4\}, \{1,2\}, \{1,3\}, \{1,4\}, \{2,3\}, \{2,4\}, \{3,4\}, \{1,3,4\}, \{2,3,4\}\}$. It holds that*

$$Z_M = \{\{1,3,4\}, \{2,3,4\}, \{1,2\}\}, \tag{6}$$

where $X_1 = \{1,3,4\}$, $X_2 = \{2,3,4\}$, $X_3 = \{1,2\}$ and $t=3$.

A *cumulative array* for Γ_{Qual}, denoted as CA, is an $n \times t$ boolean matrix, which is obtained from the maximal forbidden sets Z_M. For any $1 \le i \le n$ and $1 \le j \le t$, let $CA[i,j] = 1$ iff $i \notin X_j$. In Example 2.3, it holds that $i = 1 \notin X_2$, such that $CA[1,2] = 1$, as shown in Eq. (7) derived from Eq. (6).

$$CA = \begin{bmatrix} 010 \\ 100 \\ 001 \\ 001 \end{bmatrix}. \tag{7}$$

Let $\hat{S}^0$ and $\hat{S}^1$ be the basis matrices for a t-out-of-t visual SS scheme, as from the construction in [15], also recalled above. The basis matrices S^0 and S^1 of the access structure $(\Gamma_{Qual}, \Gamma_{Forb})$ can be constructed based on $\hat{S}^0$ and $\hat{S}^1$. For any fixed i, let $j_{i,1}, j_{i,2}, \ldots, j_{i,g_i}$ be the integers j such that $CA[i,j] = 1$. The ith row of S^0 (S^1, resp.) is obtained by performing *OR* on the rows $j_{i,1}, j_{i,2}, \ldots, j_{i,g_i}$ of $\hat{S}^0$ ($\hat{S}^1$, resp.). In Example 2.3, since $CA[1,2] = 1$ on the first row of CA in Eq. (7), the first row of S^0 (S^1, resp.) comes from the second row of $\hat{S}^0$ ($\hat{S}^1$, resp.) in Eq. (5), namely, it is $[0,1,0,1]$. By using this method, the basis matrices S^0 and S^1 are obtained as

$$S^0 = \begin{bmatrix} 0101 \\ 0110 \\ 0010 \\ 0011 \end{bmatrix}, \quad S^1 = \begin{bmatrix} 0101 \\ 0110 \\ 1100 \\ 1100 \end{bmatrix}. \tag{8}$$

3 Visual Steganography

All the visual SS methods presented in Section 2 suffer from a severe limitation, which hinders some major applications of visual cryptography. The limitation lies in the fact that all shares are inherently random patterns carrying no visual information, raising the suspicion of data encryption. In this section we present techniques that construct meaningful binary images as shares of a visual SS scheme. We classify these techniques into two types: combinatorial techniques (described in Section 3.1) and halftoning techniques (described in Section 3.2), both types using constructions for visual SS as those described in Section 2 as an atomic tool. We focus most of our attention on the latter type as they seem to achieve the best quality of shares and secret images among currently known techniques.

3.1 Combinatorial Techniques

The possibility of designing visual SS methods with innocent-looking shares was already advocated in [15], where a 2-out-of-2 scheme was proposed. Later, a method referred to as "extended visual cryptography" has been presented in [4]. In this method, which we now informally describe, hypergraph colorings are used to construct meaningful binary images as shares of a visual SS scheme for any arbitrary access structure.

A *hypergraph* is a set of subsets of a given set and can be formally defined as a pair of the form $H = (X, F)$, where $F \subseteq 2^X$, elements of X are called *vertices* and elements of F are called *hyperedges*. A *k-coloring* of a hypergraph $H = (X, F)$ is a function $\phi : X \to \{1, \ldots, k\}$ such that $|\phi(x) : x \in F| \geq 2$ for all $S \in F$ such that $|S| \geq 2$. Note that in a k-coloring every hyperedge with at least two vertices has at least two vertices with different colors. Now, let $(\Gamma_{Qual}, \Gamma_{Forb})$ be a strong access structure on the set $\mathcal{P} = \{1, 2, \ldots, n\}$ of participants, and let Γ_0 be the set of all minimal qualified subsets of $\mathcal{P}$; that is, $\Gamma_0 = \{A \in \Gamma_{Qual} : A' \notin \Gamma_{Qual}$, for each $A' \subseteq A$, $A' \neq A\}$. The construction in [4] uses the basis matrices S^0, S^1 of a conventional visual SS for $(\Gamma_{Qual}, \Gamma_{Forb})$ and a k-coloring ϕ of hypergraph $(\mathcal{P}, \Gamma_0)$, as follows.

Fix a given pixel of the secret image. Let c_i be the color of the associated pixel in the i-th share image, for $i = 1, \ldots, n$. Then, an $n \times k$ matrix $D = D(c_1, \ldots, c_n)$ is constructed as follows: for $i = 1, \ldots, n$, if color c_i is desired to be black, then all entries of the i-th row of D are set equal to 1; otherwise, entry $(i, \phi(i))$ is set equal to 0 and all others are set equal to 1. Finally, given desired pixels $c_1, \ldots, c_n$ (each for one of the n shares), the two desired collections of matrices are obtained as the set of all permutations matrices $\hat{S}^b = (S^b|D)$, for $b = 0, 1$.

Despite its elegance, the technique of "extended visual cryptography" provides very low quality visual information in the shares, as illustrated later in this chapter. Due to the random nature of hypergraph colorings, 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.

3.2 Halftoning Techniques

We now describe a general halftone visual cryptography framework, where a secret binary image is hidden into high-quality halftone images, or *halftone shares*. In particular, this method applies the rich theory of blue noise halftoning to the construction mechanism used in conventional visual SS to generate halftone shares, thus resulting in high visual quality of the shares. Furthermore, the security properties of the conventional visual SS are still maintained. The decoded secret image has uniform contrast, and the halftone shares carry significant visual information to the viewers, such as landscapes, buildings, and so forth. We note that the visual quality obtained by this method is significantly better than that attained by any other available visual SS method known to date. As a result, adversaries, inspecting a halftone share, are less likely to suspect that cryptographic information is hidden and a higher security level is thus achieved.

Halftone visual SS is built on the basis matrices and collections available in conventional visual SS. In particular, in halftone visual SS a secret binary pixel p is encoded into an array of $Q \times Q$ subpixels, referred to as a *halftone cell*, in each of the shares. The pixel expansion in halftone visual SS is thus Q^2. By choosing appropriate size of halftone cells, visually pleasing halftone shares can be obtained, while the contrast and security conditions are still maintained. In Section 3.2.1, the halftone visual SS technique is introduced by constructing a 2-out-of-2 scheme. This technique is subsequently extended in Section 3.2.2. to a scheme for an arbitrary access structure.

3.2.1 Halftone Visual Secret Sharing: 2-out-of-2 Structures

To describe the principles of halftone visual SS, the simplest 2-out-of-2 halftone visual threshold scheme is shown in Fig. 3. In this method, a halftone image I, obtained by applying any halftoning method such as the error diffusion algorithm [13] on a gray-level image GI, is assigned to participant 1, and its complementary image 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 $Q \times Q$ halftone cell in each of the two shares, only two pixels, referred to as the *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 visual SS. If p is black, M is randomly selected from C_1. The secret information pixels in the ith ($i = 1, 2$) share are replaced with the two subpixels in the ith row of M, as shown in Fig. 4. Since C_0 and C_1 are the collections of conventional visual SS, these modified pixels carry the encoded secret. The other pixels in the halftone cell that 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^2 pixels in the reconstructed halftone cell, obtained by superimposing the two encoded halftone cells, is white while all other pixels are black (Figs. 4A and 4B). If p is black, all pixels in the reconstructed halftone cell are black, as shown in Figs. 4C and 4D. Thus, the contrast condition is satisfied. The secret pixel p can be visually decoded with contrast $1/Q^2$.

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 can be proved 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 [17] 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

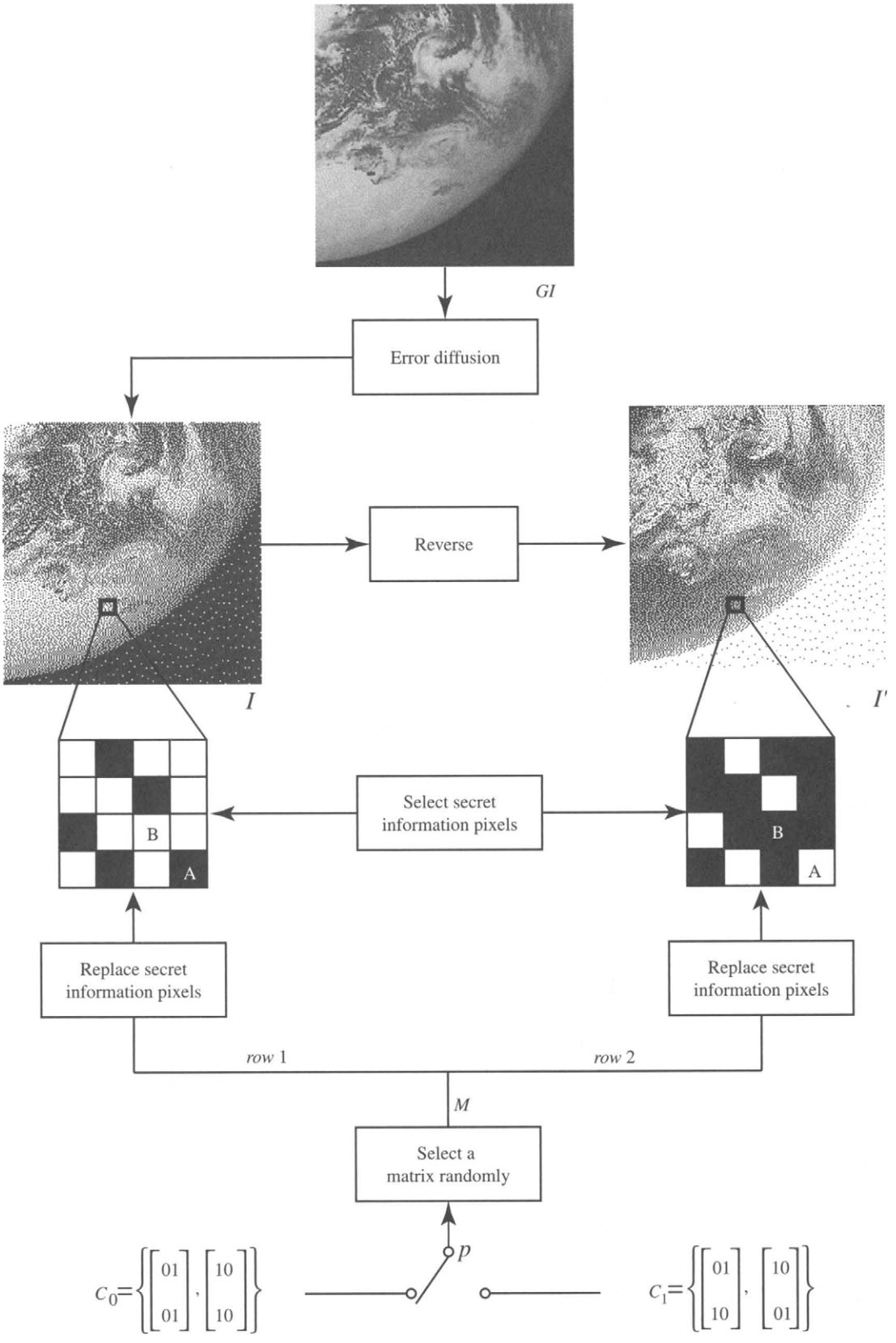


FIGURE 3 Construction of 2-out-of-2 scheme. Cell size is $Q = 4$.

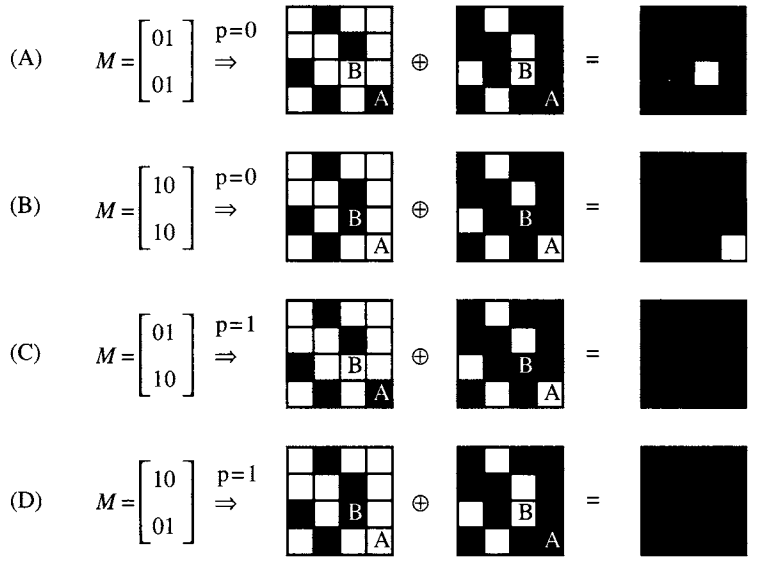


FIGURE 4 Replacing the secret information pixels with the corresponding subpixels in an encoding matrix M, which is randomly selected as (A),(B) from C_0 if $p=0$, or (C), (D) from C_1 if $p=1$. The secret pixel p can be visually decoded by imposing the two shares.

density (m.p.d.) at each minority pixel location. 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 those of the pixels A and B. Once the encoding matrix M is randomly selected, the jth $(j=1,2)$ located secret information pixel in the ith $(i=1,2)$ share is replaced with the jth subpixel in the ith 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 Figs. 4A and 4C, and the second halftone cell in Figs. 4B and 4C). 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 Figs. 4B and 4D, and the second halftone cell in Figs. 4A and 4D. 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 Figs. 4A and 4B. If the conventional void and cluster algorithm [17] 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 visual SS scheme. To address this problem, a slightly modified void- and cluster-finding filter, as shown in Eq. (9), is used to find the m.p.d.

$$DA(x,y)=\sum_{p=W/2}^{W/2}\sum_{q=W/2}^{W/2} f(p,q)\cdot P(x+p,y+q), \tag{9}$$

where $DA(x,y)$ 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,

$$P(x+p,y+q)=\begin{cases}0.5 & \text{secret information pixel}\\ 1 & \text{minority pixel}\\ 0 & \text{majority pixel.}\end{cases} \tag{10}$$

[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 [13].

The Gaussian filter is used in [17] as

$$f(p,q) = exp(-\frac{p^2+q^2}{2\sigma^2}), \tag{11}$$

where σ is a scalar constant, offering best results at $\sigma = 1.5$ in the void and cluster algorithm. 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 of whether it is a minority or majority pixel, as shown in Eq. (10). 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. In addition, since the values of secret information pixels come from the basis matrices/collections of conventional visual SS, no secret can be obtained by looking at the values of secret information pixels of one share either. Thus, the halftone visual threshold scheme is fully secure.

The above construction method implements a 2-out-of-2 halftone visual SS scheme with a pixel expansion $m^h = Q^2$ and relative difference $\alpha^h(Q) = 1/Q^2$, where the superscript "h" indicates that the parameters are for halftone visual SS. Visually pleasing halftone shares are generated by the blue noise halftoning techniques and the secret image can be reconstructed by superimposing the two shares. Since the two secret information pixels in each halftone cell are either unmodified or switched with equal probabilities, the peak signal-to-noise ratio (PSNR) of each halftone share, compared with its original halftone image, can be calculated as

$$\begin{aligned} \text{PSNR} &= 10\log\frac{255^2}{255^2 \cdot \frac{2}{Q^2} \cdot \frac{1}{2}} \\ &= 10\log Q^2. \end{aligned} \tag{12}$$

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 $\alpha^h(Q)$ 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.

3.2.2 Halftone Visual Secret Sharing: Arbitrary Structures

In this section, the technique underlying the 2-out-of-2 halftone visual threshold scheme is extended to a scheme for an arbitrary access structure $(\Gamma_{Qual}, \Gamma_{Forb})$, where a secret binary image SI is hidden into 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 Γ_{Qual} contains at least one complementary pair of images; second, in each of the shares, a secret pixel p is encoded into a $Q \times Q$ halftone cell, and m ($m < Q^2$) secret information pixels in each halftone cell are selected and replaced with the corresponding subpixels in the basis matrices/collections of conventional visual SS, where m and Q^2 are the pixel expansions of conventional visual SS and halftone visual SS, respectively.

Assignment of Complementary Pairs of Images. In the 2-out-of-2 halftone visual threshold method 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 2-out-of-2 halftone visual SS 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 Γ_{Qual} is a closure of Γ_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 2-out-of-3 halftone visual SS scheme, Γ_{Qual} is a closure of $\Gamma_0 = \{\{1,2\}, \{1,3\}, \{2,3\}\}$. If a complementary pair of halftone images are 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 matrices of a 2-out-of-2 conventional visual SS scheme are then inserted in 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 Γ_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 [9].

Halftone Cells Generation. Define the $(I_{j,0}, I_{j,1})$—*restriction* of Γ_0 as the subset of Γ_0 containing all subsets of participants that contain at least one participant that was given $I_{j,0}$ and at least one participant that was given $I_{j,1}$. We now elaborate on the halftone cell generation phase, where, for $j = 1, \ldots, k$, matrices of a conventional visual SS scheme for the $(I_{j,0}, I_{j,1})$—restriction of Γ_0 are properly inserted into images $I_{j,0}$ and $I_{j,1}$ and then properly distributed to all participants. Specifically, fix $j \in \{1, \ldots, k\}$ and recall that in each of the shares $I_{j,0}, I_{j,1}$ distributed to the participants, a secret pixel p is encoded into a $Q \times Q$ halftone cell; moreover, m ($m < Q^2$) secret information pixels in each halftone cell are selected and replaced with the corresponding subpixels in a randomly chosen matrix of a conventional visual SS for the $(I_{j,0}, I_{j,1})$—restriction of Γ_0, where m and Q^2 are the pixel expansions of the conventional visual SS used and of the halftone visual SS, respectively. Note that half of the participants have received image $I_{j,0}$ and half have received $I_{j,1}$, and, although multiple complementary pairs may exist in these n halftone images, the selection of the secret information pixels is still performed on one pair, referred to as the *key complementary pair*. To obtain the m secret information pixels in a halftone cell, the void and cluster algorithm described in Section 2.2 is applied to the halftone cell $m/2$ times, each time locating a pair of minority and majority pixels which were not selected previously. Let S^j ($j = 0, 1$) be two $n \times m$ basis matrices of conventional visual SS. Each S^j is divided into $m/2$ groups of two columns, such that each pair of secret information pixels in the n shares will be replaced with a group of subpixels. Denote the divided basis matrices as $\overline{S}^j$. As long as the row corresponding to the key complementary share in each group contains one black and one white pixels, pleasing visual quality of the key complementary share can be obtained. This property is referred to as *dividing condition* 1.

The two collections of matrices $\overline{C}_j$ ($j = 0, 1$) are constructed by permuting the groups and/or the columns in the same group of the corresponding basis matrices $\overline{S}^j$. The permutation of columns in different groups is not allowed. Thus, each encoding matrix in $\overline{C}_j$ satisfies the dividing condition 1. Such collections $\overline{C}_j$ should satisfy the security condition as well. Namely, if $X = \{i_1, i_2, \ldots, i_v\} \in \Gamma_{Forb}$ is a forbidden subset of v participants, the two collections of $v \times m$ matrices $\overline{D}_j$ ($j = 0, 1$), formed by extracting the rows $i_1, i_2, \ldots, i_v$ from each matrix in $\overline{C}_j$, are indistinguishable. This property is referred to as *dividing condition* 2. The desired basis matrices $\overline{S}^j$, subjected to the dividing conditions 1 and 2, can be obtained by enumerating all possible ways of dividing S^j. Examples of $\overline{S}^j$ and $\overline{C}_j$ are given next to illustrate the aforementioned concepts.

Example 3.1 *Let $(\Gamma_{Qual}, \Gamma_{Forb})$ be a strong access structure of the participants $P = \{1, 2, 3, 4\}$, where Γ_{Qual} is the closure of $\Gamma_0 = \{\{1, 2, 3\}, \{1, 2, 4\}\}$, namely, $\Gamma_{Qual} = \{\{1, 2, 3\}, \{1, 2, 4\}, \{1, 2, 3, 4\}\}$. Let the halftone shares $\{1, 2\}$ be the key complementary pair, and let every qualified subset contain one complementary pair of halftone images. The conventional basis matrices S^j ($j = 0, 1$) are constructed as shown in Eq. (8). The basis matrices $\overline{S}^j$ satisfying the two dividing conditions are found as*

$$\overline{S}^0 = \left[\begin{array}{cc|cc} \boldsymbol{01} & \boldsymbol{01} \\ \boldsymbol{01} & \boldsymbol{10} \\ 00 & 11 \\ 00 & 11 \end{array}\right], \quad \overline{S}^1 = \left[\begin{array}{cc|cc} \boldsymbol{01} & \boldsymbol{01} \\ \boldsymbol{01} & \boldsymbol{10} \\ 11 & 00 \\ 11 & 00 \end{array}\right], \tag{13}$$

where the rows in bold correspond to the key complementary pair. The corresponding collections $\overline{C}_j$ are obtained by permuting the groups and/or the columns in the same group of the corresponding basis matrices $\overline{S}^j$, shown below

$$\overline{C}_0 = \left\{ \left[\begin{array}{cc|cc} \boldsymbol{01} & \boldsymbol{01} \\ \boldsymbol{01} & \boldsymbol{10} \\ 00 & 11 \\ 00 & 11 \end{array}\right], \left[\begin{array}{cc|cc} \boldsymbol{10} & \boldsymbol{01} \\ \boldsymbol{10} & \boldsymbol{10} \\ 00 & 11 \\ 00 & 11 \end{array}\right], \left[\begin{array}{cc|cc} \boldsymbol{01} & \boldsymbol{01} \\ \boldsymbol{10} & \boldsymbol{01} \\ 11 & 00 \\ 11 & 00 \end{array}\right], \cdots \right\},$$

$$\overline{C}_1 = \left\{ \left[\begin{array}{cc|cc} \boldsymbol{01} & \boldsymbol{01} \\ \boldsymbol{01} & \boldsymbol{10} \\ 11 & 00 \\ 11 & 00 \end{array}\right], \left[\begin{array}{cc|cc} \boldsymbol{10} & \boldsymbol{01} \\ \boldsymbol{10} & \boldsymbol{10} \\ 11 & 00 \\ 11 & 00 \end{array}\right], \left[\begin{array}{cc|cc} \boldsymbol{01} & \boldsymbol{01} \\ \boldsymbol{10} & \boldsymbol{01} \\ 00 & 11 \\ 00 & 11 \end{array}\right], \cdots \right\}.$$

Let $X = \{1, 3\} \in \Gamma_{Forb}$ be a forbidden participant subset. The corresponding collections $\overline{D}_j$, formed by extracting the first and third rows from each matrix in $\overline{C}_j$, are shown below

$$\overline{D}_0 = \left\{ \left[\begin{array}{cc|cc} \boldsymbol{01} & \boldsymbol{01} \\ 00 & 11 \end{array}\right], \left[\begin{array}{cc|cc} \boldsymbol{10} & \boldsymbol{01} \\ 00 & 11 \end{array}\right], \left[\begin{array}{cc|cc} \boldsymbol{01} & \boldsymbol{01} \\ 11 & 00 \end{array}\right], \cdots \right\},$$

$$\overline{D}_1 = \left\{ \left[\begin{array}{cc|cc} \boldsymbol{01} & \boldsymbol{01} \\ 11 & 00 \end{array}\right], \left[\begin{array}{cc|cc} \boldsymbol{10} & \boldsymbol{01} \\ 11 & 00 \end{array}\right], \left[\begin{array}{cc|cc} \boldsymbol{01} & \boldsymbol{01} \\ 00 & 11 \end{array}\right], \cdots \right\}.$$

For any matrix in $\overline{D}_0$, an identical matrix can be found in $\overline{D}_1$. Hence, these two collections $\overline{D}_j$ are indistinguishable.

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

1. An encoding matrix M is randomly selected from the collection $\overline{C}_0$ if a secret pixel p is white, or from $\overline{C}_1$ 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 kth 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 ith ($i = 1, 2, \ldots, n$) share are replaced with the ith row of subpixels in the kth group in M.
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, locating two secret information pixels, which were not selected previously, in each iteration. 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 are 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 poor visual quality of these shares. A global optimization algorithm, where the visual quality of all shares are jointly optimized, will be introduced shortly.

Now consider the superposition of all the shares in a qualified subset $X \in \Gamma_{Qual}$. The $Q^2 - m$ 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 visual SS, respectively. If the reconstructed halftone cell is denoted as V_0, then the Hamming weight of V_0 satisfies

$$w(V_0) \le Q^2 - m + t_X - \alpha(m) \cdot m$$

$$= (Q^2 - m + t_X) - \frac{\alpha(m) \cdot m}{Q^2} \cdot Q^2. \tag{14}$$

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

$$w(V_1) \ge Q^2 - m + t_X. \tag{15}$$

Thus, the secret image can be visually decoded with the threshold $t_X^h = Q^2 - m + t_X$, having a relative difference $\alpha^h(Q) = \frac{\alpha(m) \cdot m}{Q^2}$, where the superscript "h" indicates that the parameters are for halftone visual SS.

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 $\overline{C}_0$ and $\overline{C}_1$ guarantees that no secret can be obtained from the values of the secret information pixels in any forbidden subset $X \in \Gamma_{Forb}$ either. A fully secure visual threshold scheme is thus obtained.

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

$$\text{PSNR} = 10 \log \frac{255^2}{255^2 \cdot \frac{m}{Q^2} \cdot \frac{1}{2}}$$

$$= 10 \log \frac{2Q^2}{m}. \tag{16}$$

The PSNRs of the other shares depend on the distribution of black and white subpixels in the corresponding rows of $\overline{S}^j$, but they are monotonically increasing functions of the cell size Q^2 as well. Thus, the larger the halftone cell size, the higher the PSNR. Note also that as the cell size is made larger, the void and cluster algorithm performs better, leading to higher visual quality in the halftone shares. On the contrary, the relative difference $\alpha^h(Q)$ is proportional to the reciprocal of the cell size. Thus, larger halftone cell sizes lead to lower contrast in the decoded image. Therefore, a tradeoff exists between the visual quality of the halftone shares and the contrast of the reconstructed secret image in a general access structure scheme.

Global Optimization. As described above, since the location of the secret information pixels is determined using the image characteristic of the key complementary pair, the locations 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 performed. 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. Please refer to [1] for the details of this method.

3.3 Simulation Results

Simulation results for the halftone visual threshold method are illustrated in this section, including the comparison of the halftone visual SS scheme with the method of extended visual SS [4]. 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.

3.3.1 Halftone Visual Secret Sharing vs. Combinatorial Visual Secret Sharing

To compare the result of halftone visual SS with that of extended visual SS, a 256×256 secret binary image is cryptographically encoded into two 512×512 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 $\alpha = \frac{1}{4}$, respectively. The original halftone images, obtained by the error diffusion algorithm and pixel reversal are shown in Fig. 5. Applying the extended visual SS method, [4] outputs two shares with poor visual quality and low contrast as shown in Figs. 6A and 6B. The average PSNR of these two shares with respect to their original halftones is 3.46 dB. The halftone visual SS method results in the two visually pleasing halftone shares shown in Figs. 6C and 6D. 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 Figs. 6E and 6F. The superiority of the halftone visual SS method is that halftone shares with much better visual quality can be generated, reducing the suspicion of encrypted secret.

3.3.2 Shares Quality and Secret Contrast

As stated in Sections 3.2 and 3.3, the halftone visual SS method can generate increasingly better visual quality halftone shares, as larger cell sizes are used. For instance, if a 3×3 halftone cell size is selected, two halftone shares with PSNR = 9.54 dB are obtained as shown in Figs. 7A and 7B. If the halftone cell size is increased to 4×4, better visually pleasing halftone shares are obtained, each with PSNR = 12.04 dB, as shown in Figs. 7C and 7D. However, larger halftone cell sizes lead to lower contrast of the decoded secret image. It can be identified that the contrast of Fig. 7F, the output of stacking Figs. 7C and 7D, is lower than that of Fig. 7E, the output of stacking Figs. 7A and 7B. 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 Figs. 7E and 7F.

Without Global Optimization vs. Global Optimization. The halftone visual SS scheme of $\Gamma_0 = \{\{1,2,3\}, \{1,2,4\}\}$ discussed in Example 3.1 is implemented in this section. The obtained four shares are shown in Figs. 8A, 8B, 8C, and 8D. The secret image can be decoded by superimposing a qualified subset of shares, such as Fig. 8E, 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

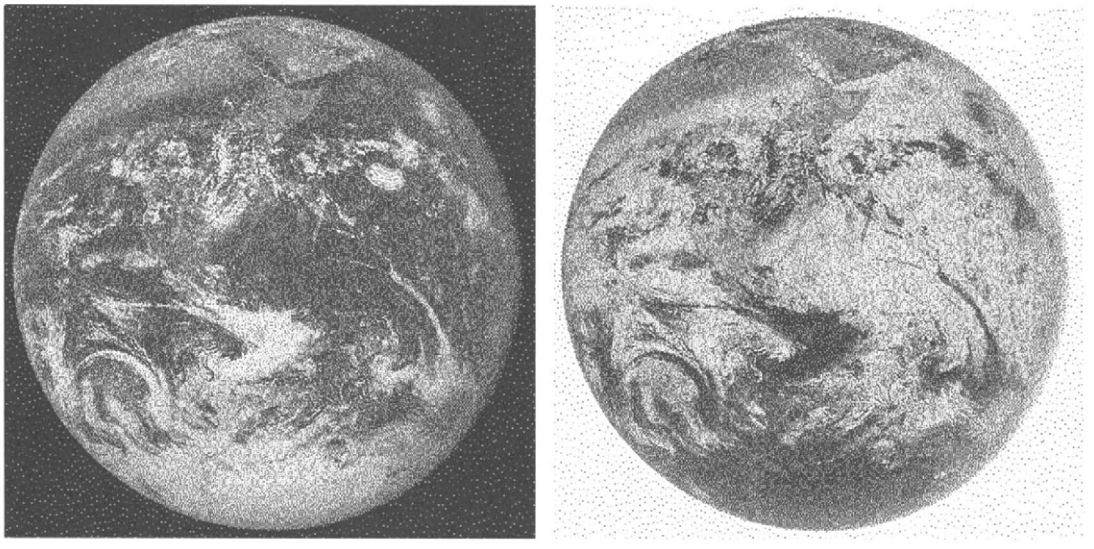


FIGURE 5 Original complementary halftone images generated by error diffusion algorithm and pixel reversal, respectively.

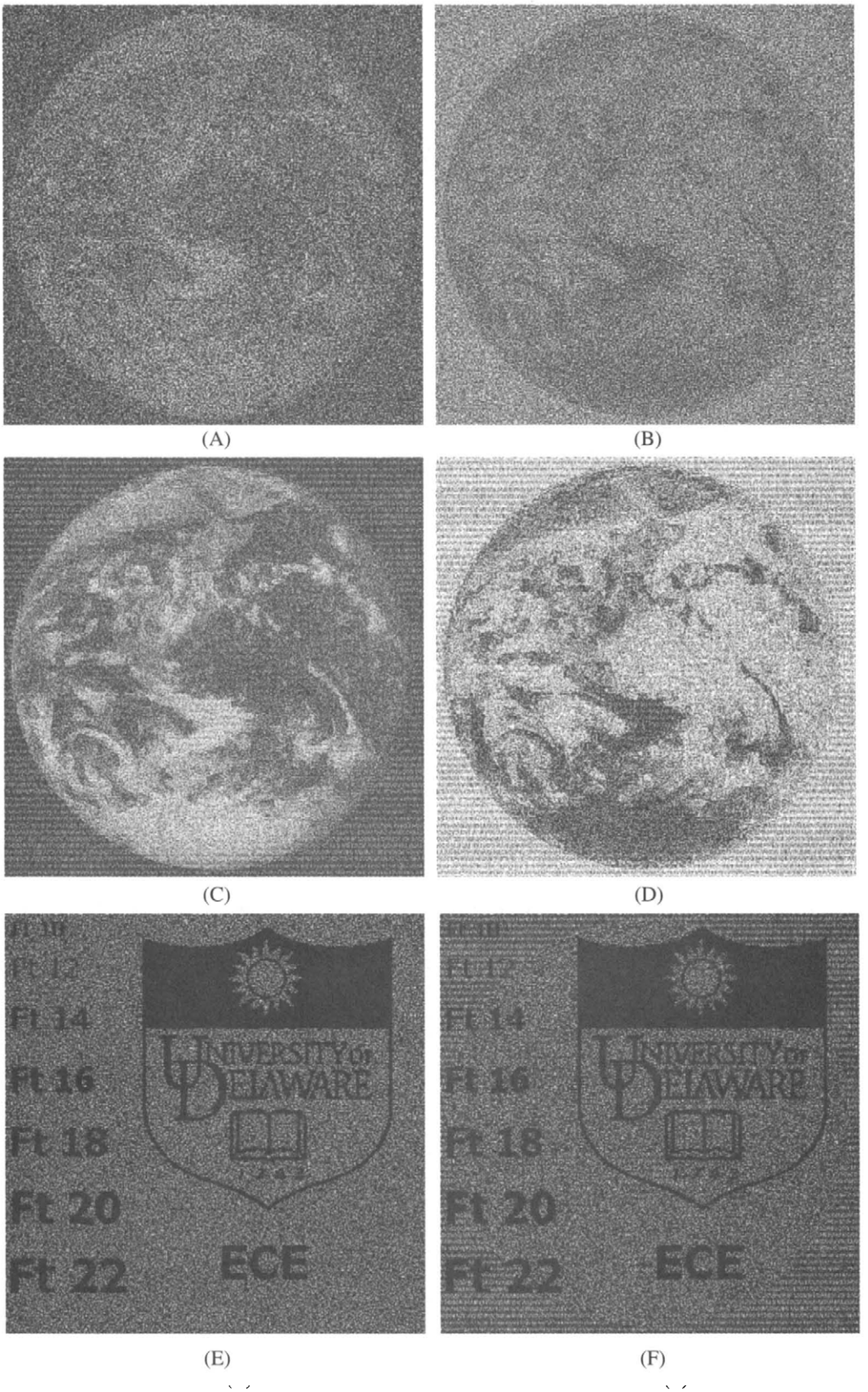


FIGURE 6 Comparison between extended visual secret sharing (SS) and halftone visual SS ($Q=2$): (A, B) the two shares of extended visual SS; (C, D) the two shares of halftone visual SS; (E) decoded image of extended visual SS; (F) decoded image of halftone visual SS.

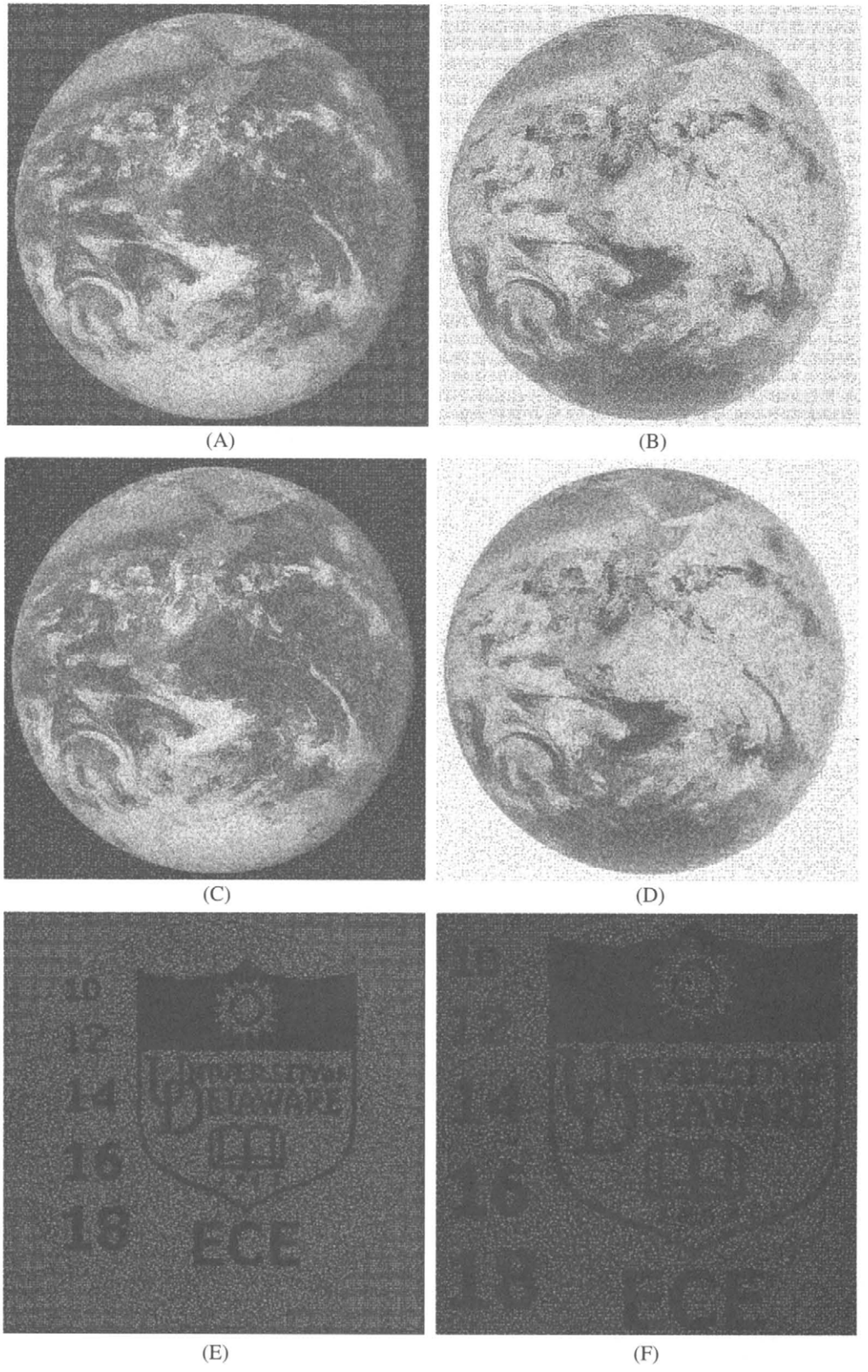


FIGURE 7 Tradeoff between the quality of the shares and the contrast of the decoded image in halftone visual secret sharing (SS): (A, B) the two shares with $Q=3$; (C, D) the two shares with $Q=4$, (E) decoded image with $Q=3$; (F) decoded image with $Q=4$.

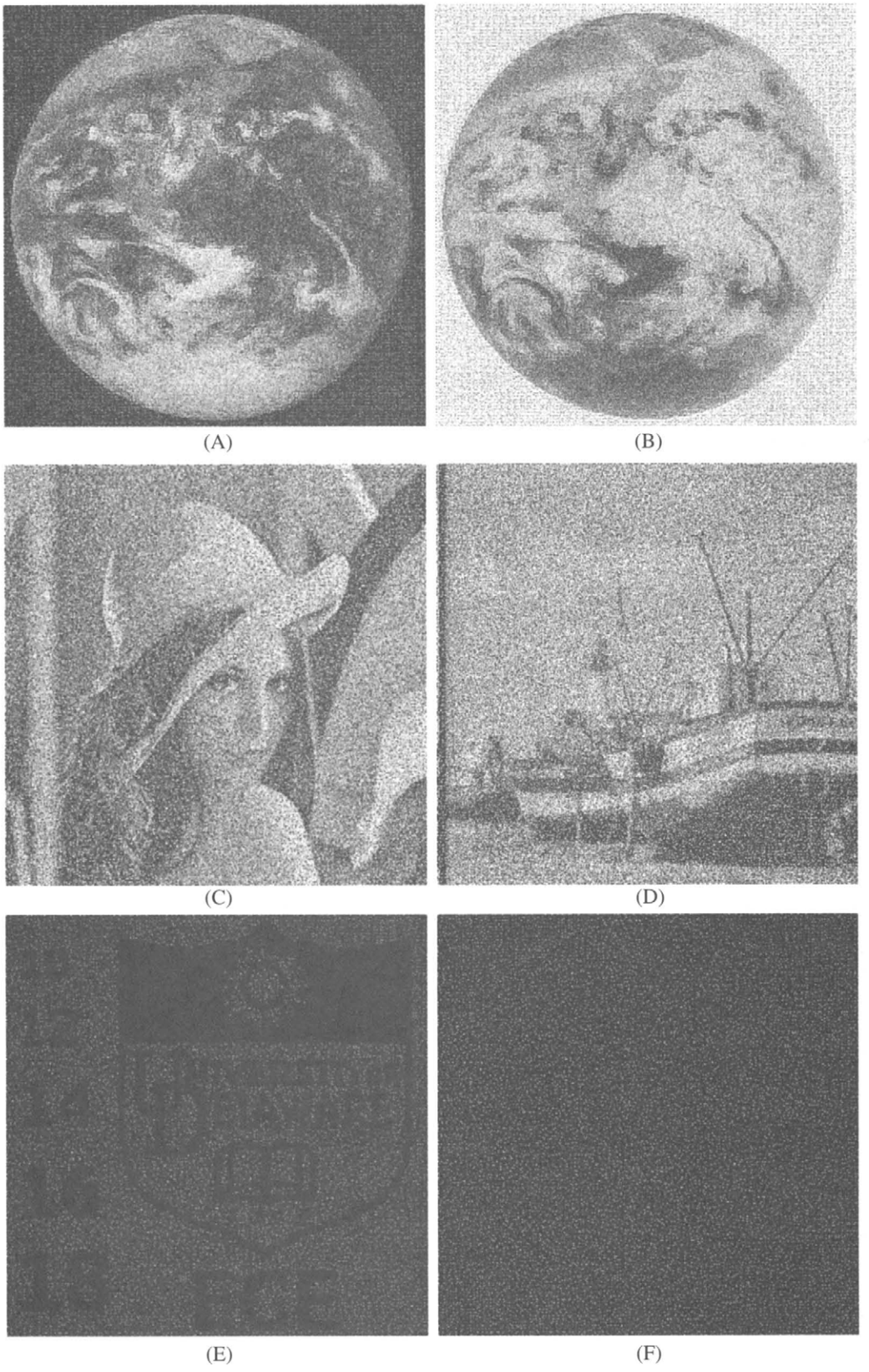


FIGURE 8 Halftone visual secret sharing (SS) scheme of $\Gamma_0 = \{\{1, 2, 3\}, \{1, 2, 4\}\}$ without global optimization ($Q = 4$): (A–D) the four shares; (E) decoded image by superimposing the shares (A–C); (F) superposition of (A) and (B).

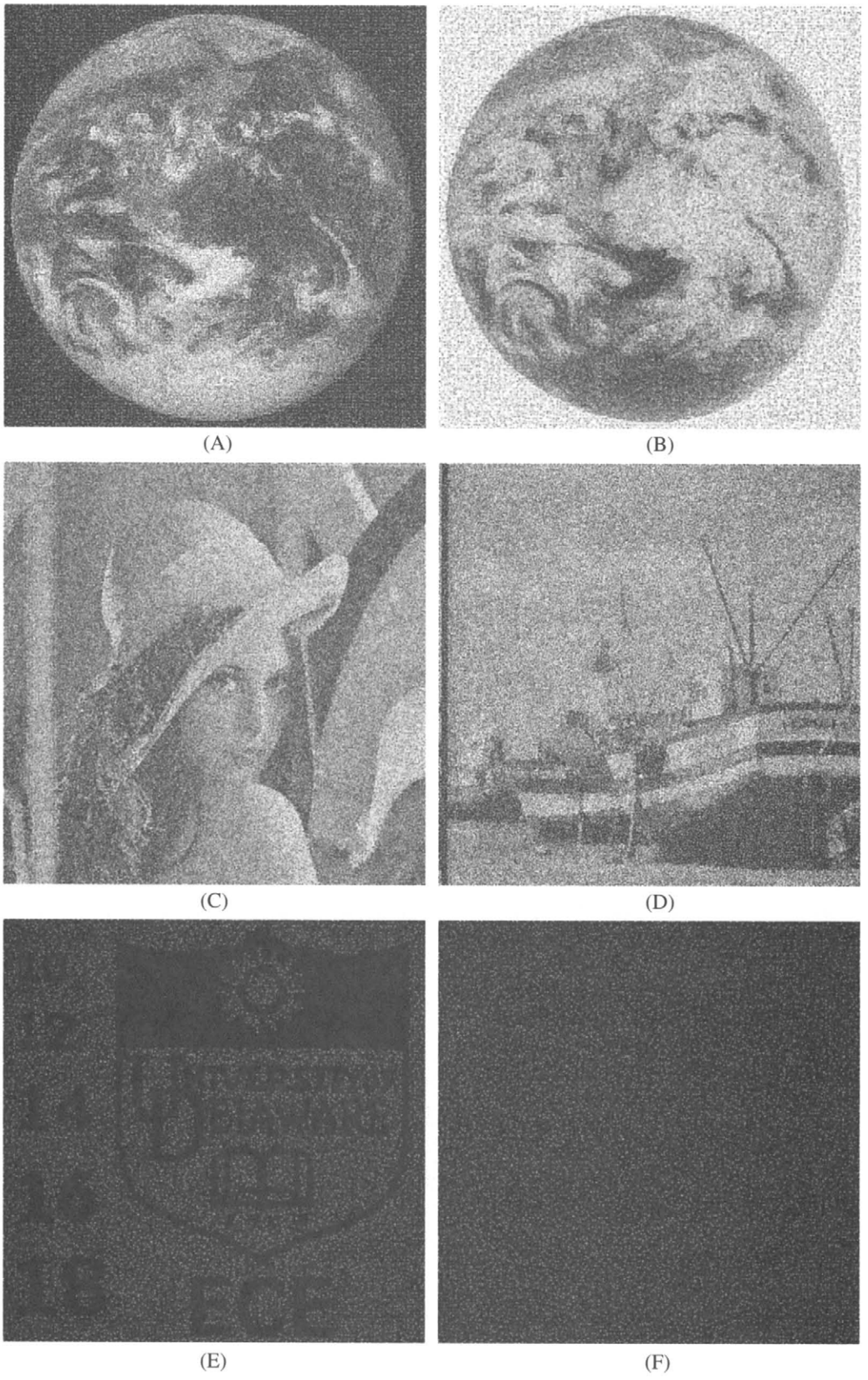


FIGURE 9 Halftone visual secret sharing (SS) scheme of $\Gamma_0 = \{\{1, 2, 3\}, \{1, 2, 4\}\}$ with global optimization ($Q = 4$): (A–D) the four shares; (E) decoded image by superimposing the shares (A–C); (F) superposition of (A) and (B).

shown in Fig. 8F. 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 Figs. 9A and 9B, but more significant gains in visual quality are obtained in nonkey complementary shares as shown in Figs. 9C and 9D. Note that the contrast and security conditions are maintained with global optimization as shown in Figs. 9E and 9F.

4 Other Work and Conclusions

Further studies on properties of visual SS schemes, including conditions needed for optimal contrast and minimum pixel expansion attainable can be found, for instance, in [6–10]. The concepts of visual cryptography have been recently extended such that the secret image is allowed to be a gray-level image rather than a binary image (see, e.g., [5]). Although the secret image is gray scale, shares are still constructed by random binary patterns. In other papers, including, for instance, [11, 12], these concepts are further generalized where a secret color image is encrypted into shares consisting of randomly distributed color pixels.

In this chapter we have reviewed the area of visual cryptography, by recalling combinatorial constructions in the literature and by describing a general framework of halftone visual cryptography. Applying the rich theory of blue noise halftoning into the construction mechanism of conventional visual cryptography, the halftone visual scheme generates visually pleasing halftone shares carrying significant visual information. The obtained visual quality is better than that attained by any other available visual cryptography method known to date. The new method can be broadly used in a number of visual secret sharing applications that require high visual quality images, such as watermarking, electronic cash, and so forth. Also, a higher security level is achieved since adversaries are less likely to suspect that these halftone shares contain cryptographic information.

References

[1] G. R. Arce, Z. Zhou, and G. Di Crescenzo, "Visual cryptography via halftoning," in *Proceedings of SPIE,* 5293, (2004).

[2] G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, "Visual cryptography for general access structures," *Information and Computation,* 129, 86–106 (1996).

[3] G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, "Constructions and bounds for visual cryptography," in *Proc. of 23rd Int. Colloquium on Automata, Languages and Programming,* 1099, Springer-Verlag, Berlin, 416–428 (1996).

[4] G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, "Extended capabilities for visual cryptography," *Theoret. Comput. Science,* 250, 134–161, (2001).

[5] C. Blundo, A. De Santis, and M. Naor, "Visual cryptography for grey level images," *Information Processing Letters,* 75, 255–259 (2000).

[6] C. Blundo, A. De Santis, and D. R. Stinson, "On the contrast in visual cryptography schemes," *J. Cryptol.* 12, 261–289 (1999).

[7] C. Blundo, P. D'Arco, A. De Santis, and D. R. Stinson, "Contrast optimal threshold visual cryptography schemes," *Siam J. Discrete Math.* 16, 224–261 (2003).

[8] C. Chang and H. Wu, "A copyright protection scheme of images based on visual cryptography," *Imaging Science J.* 49, 141–150 (2001).

[9] G. Di Crescenzo and C. Galdi, "Hypergraph decomposition and secret sharing," *Proc. of 14th International Symposium on Algorithms and Computation,* LNCS vol. 2906, 645–654 (2003).

[10] T. Hofmeister, M. Krause, and H. U. Simon, "Contrast-optimal k out of n secret sharing schemes in visual cryptography," *Theoret. Comput. Science,* 240, 471–485 (2000).

[11] T. Ishihara and H. Koga, "New constructions of the lattice-based visual secret sharing scheme using mixture of colors," *IEICE Trans. Fund. Electron. Commun. Comput. Sciences,* E85A, 158–166 (2002).

[12] H. Koga and H. Yamamoto, "Proposal of a lattice-based visual secret sharing scheme for color and gray-scale images," *IEICE Trans. Fund.* E81-A, 1263–1269 (1998).

[13] D. L. Lau and G. R. Arce, Modern Digital Halftoning (Marcel Dekker, New York, 2000).

[14] M. Naor and B. Pinkas, "Visual authentication and dentification," *Proc. Crypto 97* LNCS vol. 1294, 322-336 (1997).

[15] M. Naor and A. Shamir, "Visual cryptography," *Proc. Eurocrypt 94* LNCS vol. 950, 1–12 (1995).

[16] M. Naor and A. Shamir, "Visual cryptography II: Improving the contrast via the cover base," *Proc. 1996 Security Protocols Workshop* LNCS vol. 1189, 197–202 (1996).

[17] R. A. Ulichney, "The void-and-cluter method for dither array generation," in *Proc. SPIE, Hum. Vis. Visual Process. Dig. Displays IV,* 1913, 332–343 (1996).

[18] C. Wang, S. Tai, and C. Yu, "Repeating image watermarking technique by the visual cryptography," *IEICE Trans. Fund. Electron. Commun. Comput. Sciences,* E83A, 1589–1598 (2000).