

HALFTONE VISUAL CRYPTOGRAPHY VIA DIRECT BINARY SEARCH

Zhongmin Wang[†], Gonzalo R. Arce[†] and Giovanni Di Crescenzo[‡]

[†]Department of Electrical and Computer Engineering
University of Delaware, Newark, DE, USA, 19716

[‡]Telcordia Technologies, Piscataway, NJ, 08854, USA

email: zhongmin@udel.edu, arce@ece.udel.edu, giovanni@research.telcordia.com

ABSTRACT

This paper considers the problem of encoding a secret binary image SI into n shares of meaningful halftone images within the scheme of visual cryptography (VC). Secret pixels encoded into shares introduce noise to the halftone images. We extend our previous work on halftone visual cryptography [1] and propose a new method that can encode the secret pixels into the shares via the direct binary search (DBS) halftoning method. The perceptual errors between the halftone shares and the continuous-tone images are minimized with respect to a human visual system (HVS) model [2]. The secret image can be clearly decoded without showing any interference with the share images. The security of our method is guaranteed by the properties of VC. Simulation results show that our proposed method can improve significantly the halftone image quality for the encoded shares compared with previous algorithms.

1. INTRODUCTION

Visual cryptography (VC) is a type of cryptographic scheme [3]. To illustrate the principles of visual cryptography, con-















Pixel		
Prob	50% 50%	50% 50%
Share 1	 	 
Share 2	 	 
Stack 1 & 2	 	 

Figure 1: Construction of 2-out-of-2 scheme.

sider a simple 2-out-of-2 visual cryptography scheme shown in Fig. 2. Figure 2(a) shows the secret binary image SI to be encoded. Each pixel p of SI is split into two sub-pixels in each of the two shares. If p is white (black), one of the first (last) two columns tabulated under the white (black) pixel in Fig. 1 is selected with 50 percent probability. Then, the first two sub-pixels in that column are assigned to share 1 and the following two sub-pixels to share 2. In each share, p is encoded into two sub-pixels of black-white or white-black with equal probabilities, independent of whether p is black or white. Thus an individual share gives provably no clue as whether p is black or white [4].

Now consider the superposition of the two shares as shown in the last row of Fig. 1. If the pixel p was black, the superposition of the two shares outputs two black sub-pixels

corresponding to a grey level 1. If p is white, it results in one white and one black sub-pixels, corresponding to a grey level $1/2$. Compared with the secret image, there is a contrast loss in the reconstructed image.

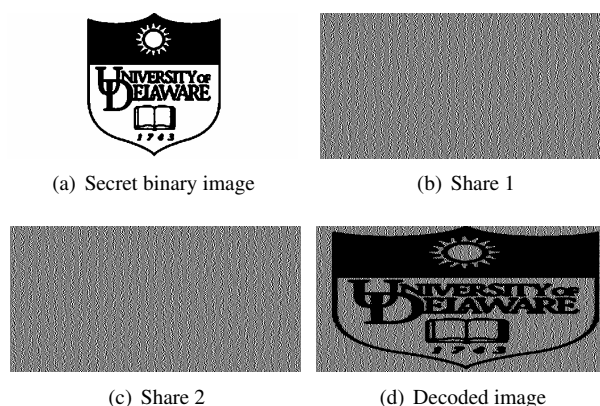


Figure 2: Example of 2-out-of-2 scheme.

Based on the process described above, we can construct two shares for SI , as shown in Fig. 2(b) and Fig. 2(c). Superimposing the two shares leads to the output secret image shown in Fig. 2(d). The decoded image is clearly identified, although some contrast loss occurs. The width of the decoded image is twice that of the original secret image since each pixel is expanded to two sub-pixels in each share as shown in Fig. 1.

The visual cryptography scheme introduced in [3] has been extended to general access structures in [5] where an access structure is a specification of all qualified and forbidden subsets of shares. The general techniques to construct visual cryptography schemes for any access structures have also been proposed in [5]. To alleviate the problem of contrast loss in the reconstructed secret images, an optimal contrast k out of n scheme has been proposed in [6]. However, the above method generates shares that have random structure which may lead to suspicion of secret information encryption.

An extended visual cryptography scheme (Extended VC) has been proposed in [7] where hypergraph colorings are used to produce shares that are meaningful binary images. A trade-off between the contrast of the reconstructed image and the contrast of the image of each share is discussed. Extended VC provides very low quality visual information in the shares and the shares also suffer from low contrast between hypergraph black and white pixels. Extended VC has been extended for natural images in [8]; In such method, the

security property is not guaranteed. The trade-off between the image quality and security has to be evaluated by observing the actual results.

Based on the principle of blue-noise dithering, halftone visual cryptography has been proposed in [1, 4] to produce meaningful halftone images for the shares in the VC scheme. Halftone visual cryptography utilizes the void and cluster algorithm [9] which is implicitly based on a low-pass HVS model to encode a secret binary image into n halftone shares carrying significant visual information. The same contrast can be obtained over the whole decoded image. Meanwhile, the security properties of the visual cryptography are still preserved.

Given that the direct binary search method can achieve significantly better output halftone image quality than error diffusion or screening, we exploit a model-based approach which is based on the direct binary search method in this paper. Our objective is to simultaneously produce high quality halftone images for the shares and encode the secret image into the shares. This is achieved by minimizing the perceived errors between the halftone shares and the continuous-tone images with respect to some specific HVS model. Simulations show that our proposed method can produce much better halftone images for the shares that show natural images compared with those produced by halftone visual cryptography. The secret image can be clearly decoded without showing any interference with the share images.

The remaining part of this paper is organized as follows: In Sec. 2, we give a brief introduction of visual cryptography and halftone visual cryptography. Section 3 is devoted to presenting our proposed method for encoding secret images via DBS. To show the effectiveness of our proposed method, simulation results are presented in Sec. 4. Finally, conclusions and future research directions are presented in Sec. 5.

2. PRINCIPLES OF VISUAL CRYPTOGRAPHY AND HALFTONE VISUAL CRYPTOGRAPHY

2.1 Visual Cryptography

Let $\mathcal{P} = \{1, \dots, n\}$ be a set of elements called participants, a visual cryptography scheme for a set \mathcal{P} of n participants is a method to encode a secret image SI into n shadow images called shares, where each participant in \mathcal{P} receives one share. Let $2^{\mathcal{P}}$ denote the set of all subsets of \mathcal{P} and let $\Gamma_{Qual} \subseteq 2^{\mathcal{P}}$ and $\Gamma_{Forb} \subseteq 2^{\mathcal{P}}$, where $\Gamma_{Qual} \cap \Gamma_{Forb} = \emptyset$. We refer to members of Γ_{Qual} as qualified sets and call members of Γ_{Forb} forbidden sets. The pair $(\Gamma_{Qual}, \Gamma_{Forb})$ is called the access structure of the scheme [5].

Any qualified set of participants $X \in \Gamma_{Qual}$ can visually decode the secret image, but forbidden set of participants $Y \in \Gamma_{Forb}$ has no information of SI [5, 7]. A visual recovery for a set $X \in \Gamma_{Qual}$ consists of xeroxing the shares given to the participants in X onto transparencies and then staking them together. The participants in X are able to observe the secret image without performing any cryptographic computation. VC is characterized by two parameters: the pixels expansion, which is the number of sub-pixels on shares that each pixels on the secret image is encoded into, and the contrast, which is the measurement of the difference of a black pixel and a white pixel in the reconstructed image [6].

For each secret binary pixel p that is encoded into m sub-pixels in each of the n shares, these sub-pixels can be described as $n \times m$ Boolean matrix M , where a value 0 cor-

responds to a white sub-pixel and a value 1 corresponds to a black sub-pixel. The i th row of M , r_i , contains the sub-pixels to be assigned to the i th share. The gray level of the reconstructed pixel p , obtained by superimposing the transparencies in a participant subset $X = \{i_1, i_2, \dots, i_s\}$, is proportional to the Hamming weight $w(V)$ of the vector $V = OR(r_{i_1}, r_{i_2}, \dots, r_{i_s})$, where $r_{i_1}, r_{i_2}, \dots, r_{i_s}$ are the corresponding rows in the matrix M [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 VC scheme if there exist a value $\alpha(m)$ and values t_X for every $X \in \Gamma_{Qual}$ satisfying [7]:

1. Contrast condition: any (qualified) subset $X = \{i_1, i_2, \dots, i_u\} \in \Gamma_{Qual}$ of u participants can recover the secret image by stacking the corresponding transparencies. Formally, for a matrix $M \in C_j$, ($j = 0, 1$) the row vectors $V_j(X, M) = OR(r_{i_1}, r_{i_2}, \dots, r_{i_u})$. It holds that: $w(V_0(X, M)) \leq t_X - \alpha(m) \cdot m$ for all $M \in C_0$ and $w(V_1(X, M)) \geq t_X$ for all $M \in C_1$. $\alpha(m)$ is called the relative difference referred to as the contrast of the decoded image and t_X is the threshold to visually interpret the reconstructed pixel as black or white.
2. Security Condition: Any (forbidden) subset $X = \{i_1, i_2, \dots, i_v\} \in \Gamma_{Forb}$ has no information of the secret image. Formally, the two collections D_j ; ($j = 0, 1$), obtained by extracting rows i_1, i_2, \dots, i_v from each matrix in C_j , are indistinguishable.

If the given secret pixel p is black (white), M is randomly selected from C_0 (C_1). The collections can be obtained by permuting the columns of the corresponding basis matrix S_0 or S_1 in all possible ways [7]. For an example of how to construct S_0, S_1, C_0 and C_1 in a 2-out-of-2 scheme, refer to [1].

2.2 Halftone Visual Cryptography

Halftone VC was introduced in [1, 4] and is built upon the basis matrices and collections available in conventional VC. A secret binary pixel p in halftone VC is encoded into an array of $Q_1 \times Q_2$ sub-pixels, referred to as a halftone cell, in each of the n shares. The pixel expansion in halftone VC is thus $Q_1 \times Q_2$. If $Q_1 = Q_2$, an undistorted reconstructed image can be obtained. The secret pixel p in the reconstructed image can be visually decoded with contrast $\frac{1}{Q_1 Q_2}$ [1].

In a 2-out-of-2 halftone visual threshold scheme, a halftone image I , obtained by any halftoning method on a grey level image GI , is assigned to participant 1. 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 2 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. If p is white, a matrix M is randomly selected from the collection of matrices C_0 . If p is black, M is randomly selected from the collection of matrices C_1 . The secret information pixels in the i th ($i = 1, 2$) share are replaced with the two sub-pixels in the i th row of M . These modified pixels carry the secret information of the encoded image. The other pixels in the halftone cells that are not modified are called ordinary pixels [1].

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 the positions of the secret information pixels are independent of the secret information, the arrangement of the modified pixels satisfies the security requirements. To obtain better visual results, the void and cluster algorithm [9] which spreads the minority pixels as homogeneously as possible was used to achieve improved halftone image quality in each share. The void and cluster algorithm uses a Gaussian filter to determine the locations of voids and clusters in the halftone images, which actually employs a low-pass filter as a HVS model implicitly. One disadvantage of using the void and cluster algorithm to choose the secret information pixels is that the selection of the position of the secret information pixel depends on the white/black pixel distribution of the original halftone image. The reconstructed image may reveal trace of the original halftone image shares.

3. DIRECT BINARY SEARCH FOR VISUAL CRYPTOGRAPHY

3.1 Basic principles

Unlike the two-step procedure (namely, blue noise halftoning and pixel replacing used in [1, 4]) for halftone visual cryptography, we encode the secret image (pixel replacing) in the process of image halftoning. In halftone VC, the original image for each share is divided into cells of size $Q_1 \times Q_2$. The positions and values of the secret information pixels in each cell should satisfy the contrast and security conditions. The secret information pixels are distributed as homogeneously as possible in our method. For a given secret binary image, we can randomly select a matrix M for each halftone cell from C_0 or C_1 depending on the value of the secret pixel p for that halftone cell. The secret information pixels of the corresponding halftone cell in the i th share are replaced with the i th row of M . Thus the locations and the values of the secret information pixels in each halftone cell for each share can be determined before any halftoning process.

Since DBS generally produces much better halftone image quality than screening or error diffusion, we choose DBS for the subsequent halftoning process. Our objective is to minimize the perceived errors between the continuous-tone images and the halftone shares which encode the secret information with respect to some specific HVS model. Because of the existence of the predetermined secret information pixels, the operations in DBS are constrained, as will be explained below.

3.2 DBS with secret pixel encoding

Direct binary search (DBS) uses a HVS model to minimize the perceived error between the continuous-tone image and the output halftone image by searching for the best possible configuration of the binary values in the halftone image iteratively [10]. The HVS model is a linear shift-invariant low-pass filter based on the contrast sensitivity function (CSF) of the human visual system and is denoted as $H(u, v)$ (u, v in *cycle/degree*) in the frequency domain. The point spread function $\tilde{h}(\tilde{x}, \tilde{y})$ (\tilde{x}, \tilde{y} in *degree*) of the HVS is obtained by taking the inverse Fourier transform of $H(u, v)$.

To convert the angular units to the units on the printed page, we can use the approximation:

$$\tan^{-1}(x/D) \approx x/D, \text{ for } x > 0, D > 0 \text{ and } x \ll D, \quad (1)$$

where D is the distance from the eye to the image. Assuming a printer with resolution R (in *dpi*) and the image is viewed at a distance D (in *inch*), the discrete filter characterizing the HVS model in the spatial domain is given by [2]:

$$h(m, n) = \frac{180^2}{\pi^2 D^2} \tilde{h}\left(\frac{180m}{\pi R D}, \frac{180n}{\pi R D}\right). \quad (2)$$

The error between the continuous-tone image $f(m, n)$ and the halftone image $g(m, n)$ is given by:

$$e(m, n) = g(m, n) - f(m, n). \quad (3)$$

The perceptually filtered error is:

$$\tilde{e}(m, n) = e(m, n) \otimes h(m, n), \quad (4)$$

where \otimes indicates convolution. The error metric ε is defined as:

$$\varepsilon = \sum_{m, n} |\tilde{e}(m, n)|^2. \quad (5)$$

An alpha stable human visual system model is used in our simulation for the DBS algorithm. Alpha stable models use less parameters than Gaussian mixture model to characterize the tails and bandwidth of the HVS model [2]. The stable distributions are decided by four parameters: an index of stability $\alpha \in (0, 2]$, a dispersion parameter $\gamma > 0$, a skewness parameter $\delta \in [-1, 1]$, and a location parameter $\beta \in R$. With $\alpha = 1$, $\beta = 0$ and $\gamma = 1$, we can obtain the CSF for the HVS model as (Cauchy filter):

$$H(\rho) = \frac{\gamma}{2\pi} \cdot \frac{1}{(\gamma^2 + \rho^2)^{\frac{3}{2}}} \quad (6)$$

where ρ is the radial frequency (in *cycle/degree*). The parameters of the model are tuned so that a homogeneous, blue noise halftone pattern is created [2].

In DBS [2], an initial halftone image $g_0(m, n)$ in which the positions and values of the secret information pixels are preserved is provided for a continuous-tone image $f(m, n)$. Then the algorithm evaluates the difference between $f(m, n)$ and $g_0(m, n)$ to produce the error image $e(m, n)$ and filters $e(m, n)$ through the HVS model. The error metric ε is evaluated for the first time. Then the algorithm starts to evaluate changes in the initial halftone image $g_0(m, n)$ that could lead to a decrease in error ε . The main operations are toggle (change the status of the current pixel) and swap (swap the values of the current pixel and one of its 8 nearest neighboring pixels that has a different value).

In our proposed method, the positions and values of the secret information pixels for each halftone cell are determined before the DBS begins. So, they should not be changed during the iterative search. If the current pixel processed is a secret information pixel, toggle is forbidden. If the current pixel or one of its 8 nearest neighboring pixel is a secret information pixel, the swap between these two pixels is also forbidden. The operation (toggle or swap) that results in the greatest decrease in the error ε is then accepted.

When all the pixels in the image have been visited, the first iteration is over. The process is iteratively repeated over the newly obtained halftone image until the error ε has converged to a local minimum. In this way, we can produce a halftone share that has minimal difference with respect to the

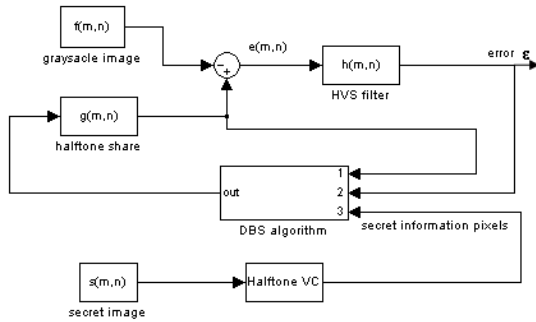


Figure 3: Block diagram for Halftone VC via DBS.

original continuous-tone image in the sense of HVS and also contains the secret image information. The whole process is also illustrated in fig.3. All the shares except the complementary share are produced via DBS. The complementary image which is a structured image but not a natural image is obtained by reversing all pixels of its complementary pair except the secret information pixels which are determined by the matrix M . DBS on the natural image pair introduces noise on the complementary share, but not on any other halftone shares.

Much like the method in [1, 4], our proposed method for visual cryptography can be easily extended to general access structure $(\Gamma_{Qual}, \Gamma_{Forb})$ when the essential share number satisfies $k \geq 3$. For a given secret image, we assign m secret information pixels for each halftone cell based on the basis matrix S^j . When all the secret information pixels are decided in each share, we use DBS to produce a halftone image for each share. Except the complementary share, all the shares can be produced independently via DBS. To maintain the contrast condition for the decoded image, we need to satisfy the condition that each qualified participant subset must contain at least one complementary pair of halftone images.

4. SIMULATION RESULTS

In this section, we show simulation results for the qualified set $\Gamma_{Qual} = \{\{1, 2, 3\}, \{1, 2, 4\}\}$. The halftone shares 1, 2 are selected as the key complementary pair, such that every qualified subset contains one complementary pair of halftone images. The basis matrix \bar{S}^j are obtained as:

$$\bar{S}^0 = \begin{bmatrix} 01 & 01 \\ 01 & 10 \\ 00 & 11 \\ 00 & 11 \end{bmatrix}, \bar{S}^1 = \begin{bmatrix} 01 & 01 \\ 01 & 10 \\ 11 & 00 \\ 11 & 00 \end{bmatrix} \quad (7)$$

where the first two rows correspond to the key complementary pair. The collections C_j ($j = 1, 2$) are constructed by permuting the groups and/or the columns in the same group of the corresponding basis matrices S^j . A 128×128 secret binary image 2(a) is encoded into four 512×512 halftone images. The pixel expansion $m = 4$ and the halftone cell size is $Q_1 = Q_2 = 4$.

The original grayscale image for the complementary pair is shown in Fig. 4(a). The obtained encoded four shares via DBS are shown in Fig. 4(b) to Fig. 4(e). Figure 4(b) and Fig. 4(c) are complementary pairs. Figure 4(b), 4(d) and 4(e) are obtained from grayscale images via DBS directly. Figure 4(f) shows the decoded secret image by stacking all 4

shares together. The secret image is clearly revealed and the relative contrast on the resultant image is $1/16$. No information can be obtained by stacking share 1 and 2, as shown in Fig. 4(g).

To compare our method with previously proposed methods, we show share 1 when halftone VC [1, 4] is used in Fig. 4(h) and share 1 when Extended VC [7] is used. The image quality deterioration on Extended VC is obvious. To compare our results with halftone VC, we use peak signal to noise ratio (PSNR) as the performance metric. Compared with the original grayscale image, Fig. 4(b) has PSNR of $7.78dB$ and Fig. 4(h) produced by halftone VC has PSNR of $6.54dB$.

5. CONCLUSION

In this paper, we have shown how halftone visual cryptography can be improved to achieve better halftone images by simultaneously encoding the secret image and producing the halftone shares via DBS. Simulation results show the effectiveness of our proposed method. Future research will concentrate on the application of our method on the color image encryption to produce high quality halftone image shares.

REFERENCES

- [1] Z. Zhou, G. R. Arce, and G. Di Crescenzo, "Halftone Visual Cryptography," *IEEE Trans on Image Processing*, to appear in 2006.
- [2] A. J. Gonzalez, G. R. Arce, J. Bacca Rodriguez, and D. L. Lau, "Human visual alpha-stable models for digital halftoning," in *18th Annual Symposium on Electronic Imaging Science and Technology: Human Vision and Electronic Imaging XI*, San Jose, CA, Jan 2006.
- [3] M. Naor and A. Shamir, "Visual Cryptography," in *Proceedings of Eurocrypt 1994, lecture notes in Computer Science*, 1994, vol. 950, pp. 1–12.
- [4] Z. Zhou, G. R. Arce, and G. Di Crescenzo, "Halftone Visual Cryptography," in *Proc. of IEEE International Conference on Image Processing*, Barcelona, Spain, Sept 2003, vol. 1, pp. 521–524.
- [5] G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, "Visual Cryptography for General Access Structures," *Electronic Colloquium on Computational Complexity (ECCC)*, vol. 3, no. 20, 1996.
- [6] 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.
- [7] G. Ateniese, C. Blundo, A. D. Santis, and D. R. Stinson, "Extended Capabilities for Visual Cryptography," *Theoretical Computer Science*, vol. 250, pp. 143–161, 2001.
- [8] M. Nakajima and Y. Yamaguchi, "Extended Visual Cryptography for Natural Images," *Journal of WSCG*, vol. 10, no. 2, 2002.
- [9] R. A. Ulichney, "The Void-and-cluster Method for Dither Array Generation," in *Proc. of SPIE, Human Vision, Visual Processing, Digital Displays*, 1996, vol. 1913.
- [10] S. H. Kim and J. P. Allebach, "Impact of HVS models on model-based halftoning," *IEEE Transactions on Image Processing*, vol. 11, pp. 258–269, Mar 2002.

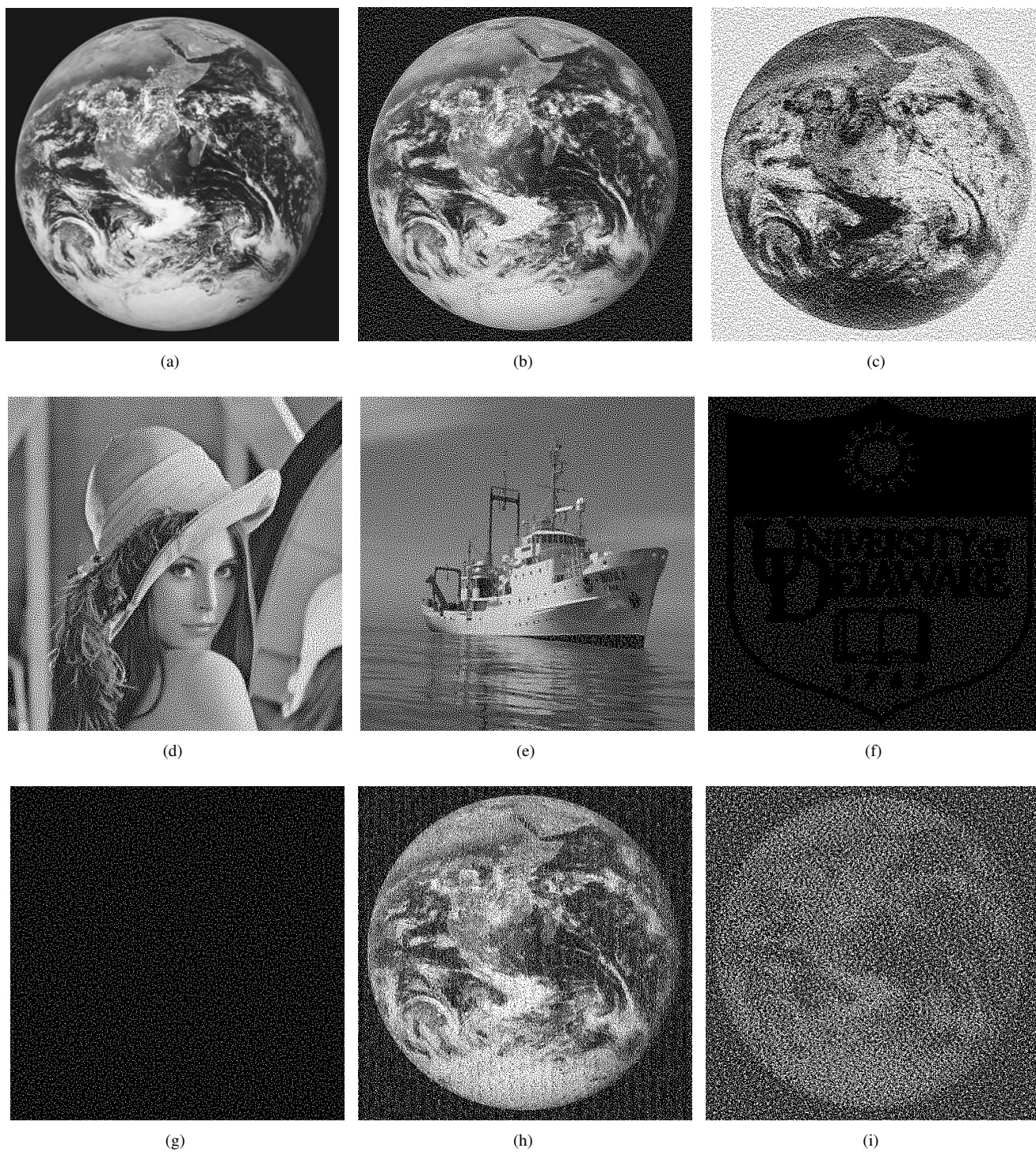


Figure 4: Simulation result for $\Gamma_{Qual} = \{\{1,2,3\}, \{1,2,4\}\}$. 4(a) original grayscale image; (4(b),4(c)) share 1 and share 2 (complementary pair); (4(d), 4(e)) share3 and share 4; 4(f) result of stacking (4(b)-4(e)); 4(g) result of stacking (4(b), 4(c)); 4(h) share 1 by halftone VC [4]; 4(i) share 1 by extended VC [7].