Joint Screening Halftoning and Visual Cryptography for Image Protection*

Chao-Yung Hsu[1,2], Chun-Shien Lu[2,**], and Soo-Chang Pei[1]

[1]Graduate Institute of Communication Eng., National Taiwan University, Taipei, Taiwan, ROC
[2]Institute of Information Science, Academia Sinica, Taipei, Taiwan, ROC
lcs@iis.sinica.edu.tw

Abstract. Since digital right management of digital media data has received considerable attention recently, protection of halftone image documents becomes another important topic. Image-based visual cryptography is found to provide an alternative for applications of copyright protection by overlapping more than one secret embedded image to show the hidden information. In this paper, we propose a novel screening halftoning-based visual cryptography method for halftone image protection. Compared with the existing methods, the major contributions of our method contain (i) improved quality of the halftone images and extracted secrets; (ii) unlimited database size of protected halftone images; (iii) more than two halftone images can be overlapped to show the hidden secret; (iv) only one conjugate screen pair in our method is able to achieve the maximum clarity of extracted secrets in random screening. Experimental results and comparisons with a state of the art method demonstrate the effectiveness of our method.

1 Introduction

With the advent of media data digitization and popularization of bi-level devices such as printers, scanners, and fax machines in our daily lives, digital halftoning has been an indispensable technology. Halftoning [8,9,12] refers to the physical process of converting a continuous tone image to a special image format, halftone image, which is composed of white and black dots, as shown in Fig. 1. We can find that the halftone image approximately keeps the visual characteristic of the continuous tone image.

Since digital right management (DRM) of digital media data has received considerable attention recently, protection of halftone image documents becomes another important topic. Two popular embedding-based copyright protection schemes for halftoning images are invisible watermarking and watermarking-based visual cryptography. Invisible watermarking refers to the insertion of invisible watermarks into the multimedia data for copyright protection [2]. The

* This research was supported by the National Science Council NDAP-R & DTD-Digital Archives System Related Technology Research & Development Project: NSC 95-2422-H-001-008 and 94-2422-H-003-007.

** Contact author.

Y.Q. Shi and B. Jeon (Eds.): IWDW 2006, LNCS 4283, pp. 212–225, 2006.

characteristic of this method is that the copyright of *halftone* images can be verified by the watermark, which is extracted from a *scanned* suspect image. Unfortunately, the geometric distortions, which are induced during the scanning process, have not been efficiently dealt with the currently known halftone image watermarking approaches [4,5]. On the other hand, halftone images can be more efficiently protected by exploiting the unique characteristic of visual cryptography by way of double-side printing, for example. In view of this, this paper will focus on digital halftone image protection by means of watermarking-based visual cryptography.

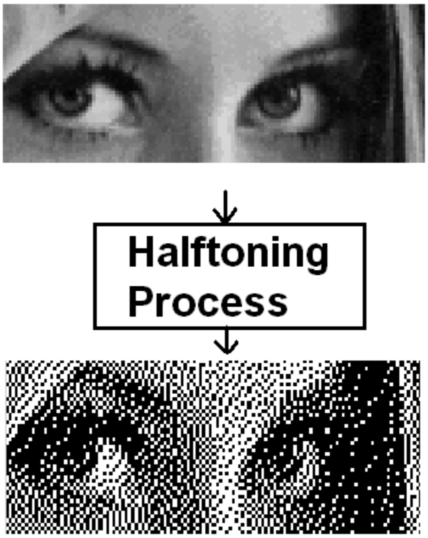


Fig. 1. Digital halftoning process

Visual cryptography [10] is a technique of hiding information into cover data and extracting the hidden information by overlapping more than one stego data. This technique provides an alternative to protect copyrights of halftone images without incurring the process of print-and-scan and avoiding the induced distortions. In the literature, few methods were proposed to combine halftoning and visual cryptography for the purpose of image protection. Fu and Au [3] proposed a method, called DHSED, to hide binary patterns into two images, which are generated by different error diffusion techniques. Specifically, one is generated by regular error diffusion and the other is generated by stochastic error diffusion. If these two images are overlapped, then the hidden visual pattern appears. In [6], they further proposed to use self-conjugate error diffusion for data hiding so that better image quality and more visible visual patterns can be satisfied.

However, the aforementioned methods still cannot be used for copyright protection because each image is required to be processed twice in different ways. It is foreseeable that the size of the image database is doubled accordingly.

In order to keep the size of an image database unchanged, Pei and Guo [11] proposed a noise-balanced error diffusion technique such that the two to be overlapped halftone images can be generated from different gray-tone images and the extracted information still exhibits acceptable visual quality. The weakness is that each stego image must be restricted to be superimposed with a key image so as to successfully reveal the hidden information. This restriction will pose the problems of insecurity and inflexibility.

In order that the hidden information can be extracted by overlapping *any* two images, Knox [7] proposed a novel halftone image watermarking scheme based on stochastic screen patterns. In this method, a stochastic screen block is first selected and one or more than one stochastic screen blocks that are related to the first one are derived. Then, the first halftone image is generated from the screen image that is yielded from the first screen block and the second halftone image is generated from the screen image that is formed by randomly combining the other screen blocks with the watermark signal. In this study, the watermark signal is composed of two components: the dark component and the bright component, as shown in Fig.2. However, our studies find that Knox's method still exhibits two major disadvantages: worse halftoning quality and limited database size of protected images.

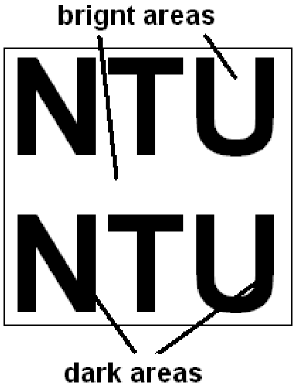


Fig. 2. A watermark signal is composed of the bright and dark components

In this work, we investigate a joint screening halftoning and visual cryptography scheme for image copyright protection. The major differences distinguishing the state of the art technology presented by Knox [7] from ours include: (1) halftone images with better quality can be obtained by two conjugate basic screens; (2) the size of a halftone image database is not limited.

2 Background

Both the technologies of screening halftoning and visual cryptography are briefly described to complete this paper.

2.1 Screening Halftoning

In screening halftoning, a so-called threshold matrix or screen block, as shown in Fig. 3, is needed to perform continue tone-to-halftone transformation. In fact, the output pixel block is independently determined by comparing the corresponding input pixel block with a screen block. Let T be a two-dimensional screen block and let I be an input image. In the implementation, both the elements of T and I are normalized to fall within the interval $[0 \quad 1]$ during the halftoning process. Specifically, the screening halftoning process is performed as follows to obtain the halftone image H, whose pixel value is defined as

$$H(x,y) = \begin{cases} 1, & \text{if } I(x,y) \geq T(x,y); \\ 0, & \text{otherwise.} \end{cases} \tag{1}$$

In Eq. (1), $H(x,y) = 0/1$ denotes that the halftone pixel is black/white.

6	11	7	10
15	1	16	4
8	9	5	12
13	3	14	2

Fig. 3. An example of a 4 × 4 screen block

2.2 Visual Cryptography

The basic concept of visual cryptography [10] states that a secret message is divided into s partitions, $Share_1$, $Share_2$, $\cdots$, and $Share_s$, which are viewed as

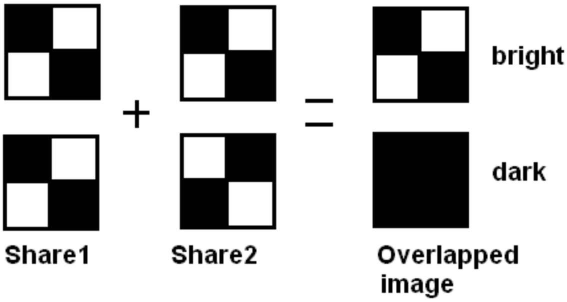


Fig. 4. An example of 2×2 image visual cryptography. In the overlapped image, bright area is labeled with level 0.5 while dark area is labeled with level 0.

random noise images. When any k ($k \leq s$) partitions are overlapped together, the secret will appear on the overlapped image. Here, a secret contains two levels of illumination (see Fig. 2): bright areas are labeled with level 0.5 and level 0 is used to represent dark areas. Fig. 4 illustrates two simple examples of secret sharing from two shares of size 2×2. The first example indicates that if two shares are the same, then bright illumination will be shown, while the second one shows that if two shares are different, then dark illumination will be shown. A practical example of visual cryptography is shown in Fig. 5.

3 Our Method

In [7], Knox proposed to generate halftone images by means of combining one or more stochastic (random) screens. However, we find that combination of random screens results in poor quality of halftone images because random screening cannot disperse block and white dots uniformly, as shown in Fig. 6. We can observe that the halftone image generated by random screening is worse than classic screening in visual quality. On the other hand, if the size of an image database is large, then more random screens are required in order to make sure that any two images are generated from different screen combinations. As a result, how to generate sufficient number of screens is problematic for a large image database in [7].

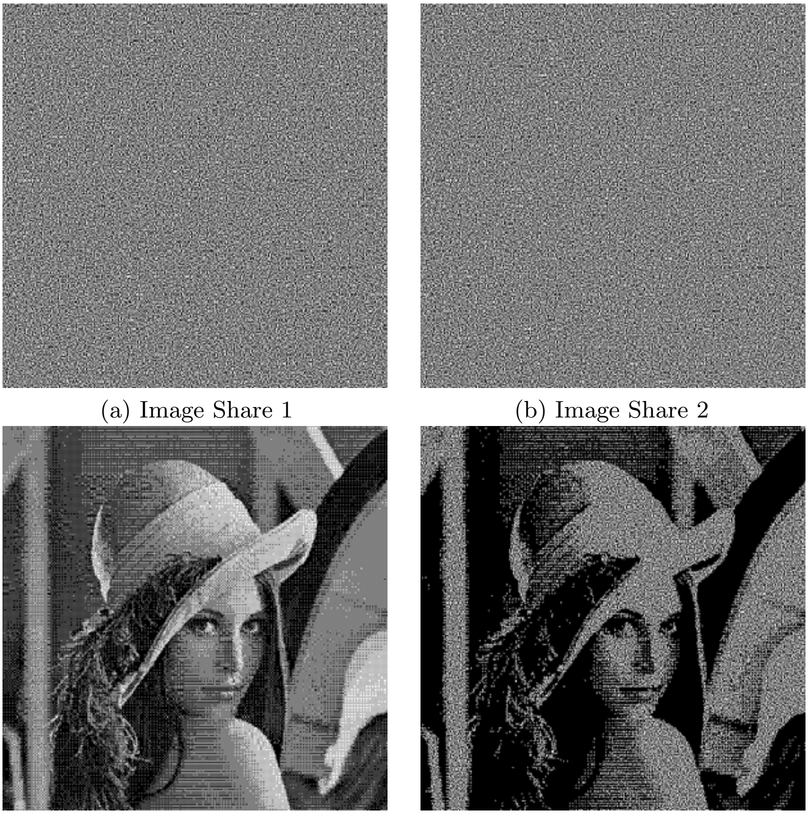
In order to deal with these problems, we propose a new method, which relies only on a pair of conjugate screens. Our scheme is composed of three parts: generation of basic screen blocks, generation of screen block group, and generation of screen images. We further employ "average dark degree" to analyze the quality of the extracted secrets.

The block diagram of our method is shown in Fig. 7 for clarification.

3.1 Basic Screen Pair Generation

To generate a pair of basic screens, we select arbitrarily from a pool of screen blocks the first screen block of size $m \times m$, denoted as S_1. Usually, the initial screen is designed with a property that larger threshold values intersect with smaller ones for consideration of good halftone image quality. This interleaving structure is helpful to generate uniformly distributed white and black pixels in a halftone image such that various gray levels can be represented to show good quality of resultant halftone images.

Fig. 3 shows an example of a selected screen block of size 4×4. We can derive the second screen S_2, which is conjugate to S_1, by arbitrarily exchanging the positions of the first $\frac{m \times m}{2}$ larger threshold values (e.g., indicated with 9,10,...,16) with the remaining ones (e.g., indicated with 1,2,...,8). This pair of screen blocks is crisscross in that the process of generating conjugate screen blocks does not incur noises that are sensitive to human eyes. An example of a screen block conjugate to Fig. 3 is shown in Fig. 8. In addition, we can generate more screen blocks by randomly combining the conjugate pair of screen blocks, as discussed in next section.



(a) Image Share 1

(b) Image Share 2

(c) Secret image S

(d) Result obtained by overlapping (a) and (b)

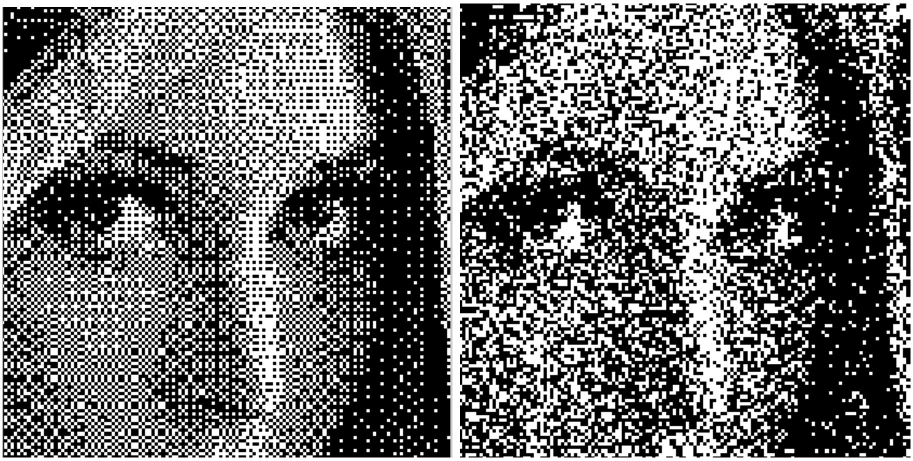
Fig. 5. An illustration of image visual cryptography

3.2 Group of Screen Blocks

If a new pair of screen blocks are generated from a pair of basic conjugate screen blocks (e.g., Fig. 3 and Fig. 8), they will possess conjugate halftone structure, too. By exploiting this property, we can randomly combine two basic screen blocks to generate extended screen blocks of size $2m \times 2m$, as shown in Fig. 9. The extended screens will be used to screen a cover image to finish secret embedding. In fact, the group of eight extended screen blocks shown in Fig. 9 will be used to generate screen images. In the group, each extended screen block (e.g., (a)) has a corresponding conjugate partner ((b)) and six half-conjugate partners ((c)∼(h)). Of course, the size of the extended screen group should be properly determined.

3.3 Secret-Dependent Screen Image Generation

Given a group of extended screen blocks and a secret message (or watermark signal) that is to be embedded into a cover image, a secret-dependent screen



(a) Result of classical screening (b) Result of stochastic screening

Fig. 6. Visual quality comparison between classical and stochastic screening results

image having the size the same with the cover halftone image will be generated. This procedure contains three steps. First, the embedded signal is divided into several message blocks, each of which has the same size with the extended screens. Second, a screen block is randomly selected and is fixedly used for message blocks belonging to bright component, as shown in Fig. 2. Third, if the message block belongs to dark areas, then an extended screen is randomly selected from the screen group. After performing the above procedure, the selected extended screens constitute a secret-dependent screen image, which can be used to generate stego halftone images via, for example, Eq. (1) for visual cryptography.

3.4 Quality Metric of an Extracted Secret

When any two halftone images (shares) are overlapped, it is important to measure whether the extracted hidden message is visually acceptable. As shown in Fig. 2, we are interested in the average dark degree of the extracted messages.

Let I_d and I_b, respectively, denote the average illumination in the dark and bright areas of an overlapped image. Let B_d denote the average dark degree of an extracted secret in an overlapped image. B_d is defined as the number of black pixels over the number of total pixels in the dark area of an overlapped image. Let B_1 and B_2, which are independent uniform random variables within the interval $[0, 1]$, denote the average dark degree in the dark area of the first and second share images, respectively. We will now analyze and compare the achievable average dark degree between random screening [7] and our screening halftoning-based method.

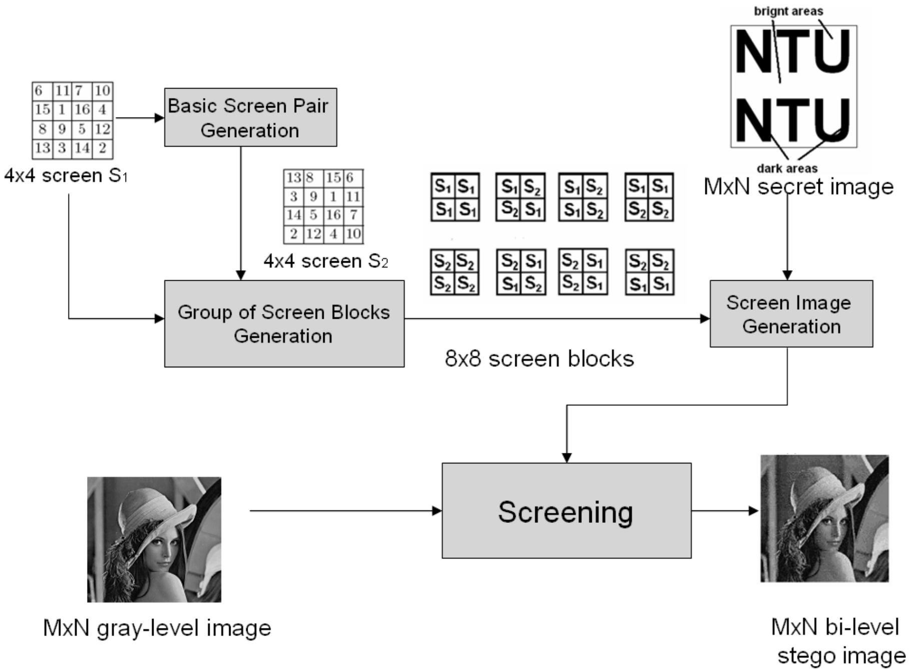


Fig. 7. Block diagram of our method

13	8	15	6
3	9	1	11
14	5	16	7
2	12	4	10

Fig. 8. Screen block conjugate to the one in Fig. 3

In the random screening process, by considering n random screens the average dark degree can be derived as:

$$B_d = \frac{n-1}{n}(1-(1-B_1)\cdot(1-B_2)) + \frac{1}{n}\max(B_1, B_2). \qquad (2)$$

In Eq. (2), $(1-(1-B_1)\cdot(1-B_2))$ denotes the average dark degree when B_1 and B_2 are, respectively, generated from different screens. According to random screening, this probability is $\frac{n-1}{n}$. In addition, $max(B_1, B_2)$ represents the maximum average dark degree when B_1 and B_2 are both generated from the same screen. The probability for this situation in random screening is $\frac{1}{n}$. When n approaches infinity, the maximum B_d can be derived as:

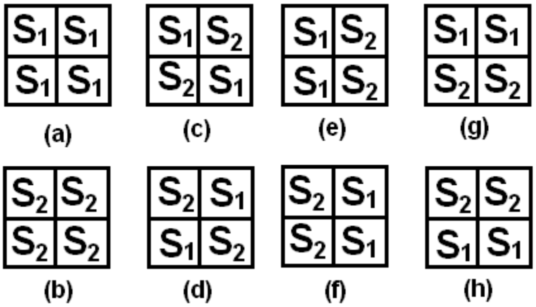


Fig. 9. A group of eight extended screens. In this group, each extended screen block has a corresponding conjugate partner ((b)) and six half-conjugate partners ((c) (h)).

$$B_d = \lim_{n\to\infty} \frac{n-1}{n}(1-(1-B_1)\cdot(1-B_2)) + \frac{1}{n}\max(B_1, B_2) = 1-(1-B_1)\cdot(1-B_2). \tag{3}$$

Moreover, the mean value of the maximum dark degree, $E(B_d)$, in random screening can be derived as:

$$\begin{aligned} E(B_d) &= E(1-(1-B_1)\cdot(1-B_2)) \\ &= \int_{b_1}\int_{b_2}(1-(1-b_1)(1-b_2))f(b_1,b_2)db_2db_1 \\ &= 1-\int_{b_1}\int_{b_2} db_2db_1 = 0.75, \end{aligned} \tag{4}$$

where $f(b_1, b_2)$ denotes the joint probability density function of B_1 and B_2, which is equal to 1 because B_1 and B_2 are independent uniform random varibles. Thus, we know that the upper bound of $E(B_d)$ in random screening is 0.75.

In our screening halftoning-based method, since each extended screen block in a group of eight extended screen blocks (Fig. 9) has one corresponding conjugate partner and six half-conjugate partners, the average dark degree of an extracted secret in an overlapped image is calculated as:

$$\begin{aligned} B_d = &\frac{1}{8}min\left(B_1+B_2,1\right) \\ &+\frac{6}{8}\left(\frac{1}{2}min\left(B_1+B_2,1\right)+\frac{1}{2}max\left(B_1,B_2\right)\right) \\ &+\frac{1}{8}max\left(B_1,B_2\right) \\ = &\frac{1}{2}min\left(B_1+B_2,1\right)+\frac{1}{2}max\left(B_1,B_2\right), \end{aligned} \tag{5}$$

where $min\left(B_1+B_2,1\right)$ is the minimum average dark degree when B_1 and B_2 are generated from a conjugate screen pair (which occurs with probability $\frac{1}{8}$),

$\frac{1}{2}min\,(B_1+B_2,1)+\frac{1}{2}max\,(B_1,B_2)$ represents the average dark degree when B_1 and B_2 are generated from a half-conjugate screen pair (which occurs with probability $\frac{6}{8}$), and $max\,(B_1,B_2)$ is the maximum average dark degree when B_1 and B_2 are generated from the same screen (which occurs with probability $\frac{1}{8}$). The mean of average dark degree achieved by means of our method can be derived as:

$$\begin{aligned}E(B_d) &= E(\frac{1}{2}\min(B_1+B_2,1)+\frac{1}{2}(B_1,B_2))\\ &= \frac{1}{2}(\int_0^1\int_0^{1-b_1}(b_1+b_2)db_2db_1+\frac{1}{2}+\int_0^1\int_0^{b_1}b_1db_2db_1+\int_0^1\int_0^{b_2}b_2db_1db_2)\\ &= 0.75. \end{aligned} \tag{6}$$

In this paper, we only use two basic screen blocks ($n=2$ in our method) to generate a group of extended screen blocks to satisfy visually acceptable halftone images. As a result, we know that the mean value of B_d in our method achieves the upper bound (corresponding to $n\rightarrow\infty$) in random screening.

Since the quality of stego halftone image obtained using our method is better than that obtained using random screening, we will show later in the experimental results that our extracted secrets on the overlapped image is more clear than Knox's.

4 Experimental Results

In this section, we will demonstrate the performance of the proposed joint screening halftoning and visual cryptography scheme for image copyright protection. Our experiment was conducted using ten common 10 images of size 512 × 512, as shown in Fig. 10. The embedded secret (Fig. 2) is an image with size the same as the cover image. In order for performance evaluation, the average dark degree, denoted as B_d, in the dark area of an overlapping image is employed. In addition, the halftone PSNR (HTPSNR) between the cover (I) and stego (I^e) halftone images defined as

$$HTPSNR(I,I^e)=PSNR(HVS(I),HVS(I^e)), \tag{7}$$

is used for objective quality evaluation, where $HVS()$ denotes a contrast sensitivity function of the human visual system [1].

Since we have investigated to find only Knox's method [7] among the existing approaches can achieve the fact that the hidden information can be extracted by overlapping *any* two images. As a result, Knox's method is regarded as state of the art technology in this respect and is selected for the purpose of performance comparison.

Experimental results regarding halftone PSNR and average dark degree are summarized in Table 1. The results obtained from stochastic screening [7] with 2, 8, and 64 stochastic screens, respectively, were also used for comparisons.

(I1) (I2) (I3) (I4) (I5)

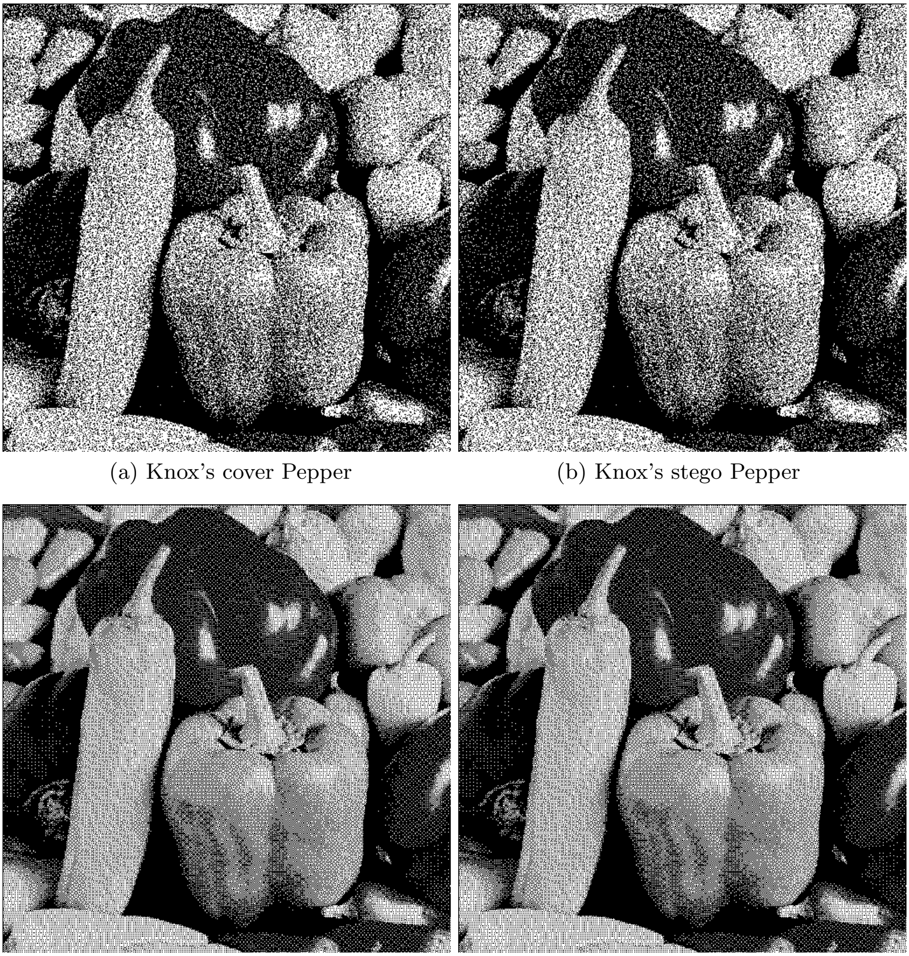
(I6) (I7) (I8) (I9) (I10)

Fig. 10. Cover images

Table 1. Comparison of halftone PSNR (HTPSNR) and average dark degree between Knox's method [7] and our method

	Proposed Method		Stochastic Screen n=2		Stochastic Screen n=8		Stochastic Screen n=64	
	HTPSNR	B_d	HTPSNR	B_d	HTPSNR	B_d	HTPSNR	B_d
I1	29.91	0.85	26.78	0.82	24.48	0.85	24.27	0.86
I2	29.77	0.77	24.95	0.71	22.38	0.76	22.02	0.77
I3	29.15	0.81	25.46	0.77	23.39	0.82	23.03	0.83
I4	28.21	0.76	23.81	0.71	22.51	0.76	22.50	0.77
I5	29.01	0.76	24.96	0.71	23.05	0.76	22.96	0.77
I6	30.01	0.80	24.75	0.76	23.41	0.80	23.37	0.81
I7	29.27	0.68	23.56	0.65	23.12	0.69	23.29	0.70
I8	30.10	0.67	25.95	0.63	24.07	0.67	24.01	0.68
I9	29.63	0.78	25.30	0.74	23.84	0.78	23.41	0.79
I10	28.85	0.80	25.35	0.76	23.03	0.80	22.68	0.81

According to Table. 1, it is observed that our method achieves higher quality of stego halftone images under the constraint that the average dark degrees of extracted messages between Knox's method and ours are approximately the same. An illustration of quality comparison between the cover and stego halftone images, respectively, obtained using Knox's method and our method is shown in Fig. 11 for visual inspection. We can observe that both Knox's cover and stego images appear to be rather noisy, while the visual quality of our cover and stego images looks naturally and smoothly In addition, no perceptual differences can be perceived by comparing the cover and stego halftone images.



(a) Knox's cover Pepper

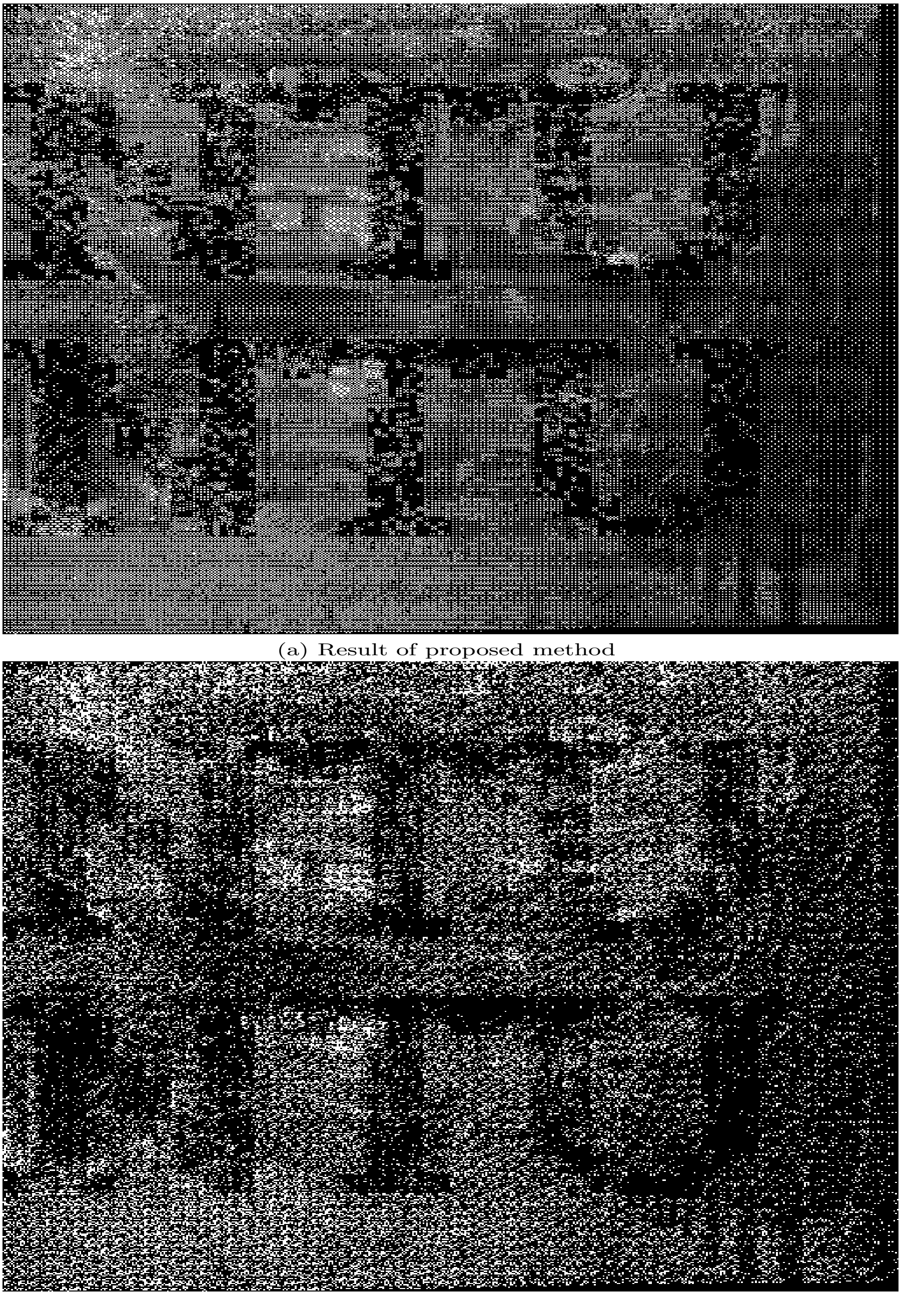
(b) Knox's stego Pepper

(c) Our cover Pepper

(d) Our stego Pepper

Fig. 11. Perceptual quality comparison between the cover and stego images obtained using Knox's method [7] and our method

In Fig. 12, we further show the extracted secret message by overlapping more than two embedded images for visual inspection subjectively. It can be observed that although both the dark degree obtained by our method and Knox's method is almost the same, our extracted secret image appears to be more clearer because knox's overlapped halftone image is rather noisy. In addition, if only two ($n = 2$) screens is used in Knox's method, then their extracted secrets become visually unclear.



(a) Result of proposed method

(b) Result of stochastic screening

Fig. 12. Comparison of secret extraction between our screening halftoning-based method and Knox's method [7]

5 Conclusion

In this paper, we study screening halftoning-based visual cryptography for image copyright protection. Our contributions contain (i) better quality of halftone images and the revealed secrets; (ii) unlimited size of image database; (iii) more than two halftone images can be overlapped to show the hidden secret; (iv) only one conjugate screen pair in our method is able to achieve the upper bound of average dark degree in random screening. The currently known methods have not achieved the above characteristics, simultaneously.

Future work will extend the current work for secret communication by studying the tradeoff between the resolution and quality of the embedded secrets.

References

1. P. J. Barten, "Physical model for the contrast sensitivity of the human eye," *in Proc. IS&T/SPIE Int. Symp. on Electronic Imaging Science and Technology*, Vol. 1666, San Jose, CA, Feb. 9-14, pp. 57-74, 1992.
2. I. J. Cox, M.L. Miller, and J.A. Bloom, Digital Watermarking, Morgan Kaufmann, 2002.
3. M. S. Fu and O. C. Au, "Hiding data in halftone image using modified data hiding error diffusion," *Proc. SPIE Conf. Visual Communication and Image Processing*, Vol. 4067, pp. 1671-1680, 2000.
4. M. S. Fu, and O.C. Au, "Data hiding in halftone images by stochastic error diffusion," *Proc. ICASSP* , Vol. 3, pp. 1965-1968, 2001.
5. M. S. Fu, and O.C. Au, "Data hiding watermarking for halftone images," *IEEE Trans. on Image Processing*, Vol. 11, pp. 477-484, 2002.
6. M.S. Fu, O.C. Au, "A novel self-conjugate halftone image watermarking technique," *Proc. of IEEE Int. Symposium on Circuits and Systems*, Vol. 3, pp. 790-793, 2003.
7. K. T. Knox, "Digital watermarking using stochastic screen patterns," U.S. Patent 5 734 752, September 1996.
8. D. E. Knuth, Digital halftones by dot diffusion, *ACM Trans. On Graphics*, Vol. 6, No. 4, pp. 245-273, 1987.
9. D. L. Lau, and G. R. Arce, Modern digital halftoning, Marcel Dekker, 2001.
10. M. Noar and A. Shamir, "Visual Cryptography," *Advances in Cryptography Eurocrypt'94*, Lecture Notes in Computer Science, Springer-Verlag, Vol. 950, pp. 1-12, 1995.
11. S. C. Pei, and J. M. Guo, "Hybrid pixel-based data hiding and block-based watermarking for error-diffused halftone images," *IEEE Trans. on Circuits and Systems for Video Technology*, Vol. 13, pp. 867-884, 2003.
12. P. W. Wong, and N. D. Memon, "Image processing for halftones," *IEEE Signal Processing Magazine*, Vol. 20, pp. 59-70, 2003.