Journal of Information Hiding and Multimedia Signal Processing ©2013 ISSN 2073-4212
Ubiquitous International Volume **4**, Number **2**, April **2013**

A New Assessment Measure of Shadow Image Quality Based on Error Diffusion Techniques

Xuehu Yan[1], Shen Wang[1], LiLi[1,2], Ahmed A. Abd El-Latif[1,3], Zhiqiang Wei[1,2] and Xiamu Niu[1,2]

School of Computer Science and Technology[1]
Harbin Institute of Technology
92 West Dazhi Street , Nan Gang District, Harbin, 150001, China
xuehu.yan@ict.hit.edu.cn; shen.wang@hit.edu.cn; ahmed rahiem@yahoo.com; and xiamu.niu@ict.hit.edu.cn

Shenzhen Graduate School[2]
Harbin Institute of Technology Shenzhen Graduate School, Shenzhen, 518055, China
li.li@ict.hit.edu.cn; zhiqiang.wei@ict.hit.edu.cn; and xiamu.niu@ict.hit.edu.cn

Mathematics Department, Faculty of Science[3]
Menoufia University
Shebin El-Koom 32511, Egypt
ahmed rahiem@yahoo.com

Received November, 2012; revised January, 2013

Abstract. *A formal approach to study quality of shadow images in secret image sharing schemes based on error diffusion techniques is introduced. A novel secret sharing quality measure for assessment of shadow image quality, namely average flipping rate (AFR), that formulates and judges the visual quality of shadow images is proposed. This quality measure gives an indication about the quality of shadow images, that could be computed before sharing, with less complex computation overhead than the modified peak signal-tonoise ratio (MPSNR). Numerical analysis shows that the proposed quantitative technique has lower computation overhead and keeps in step with those taken by MPSNR. The new quality measure for assessment of shadow image quality will be useful for the development of secret image sharing techniques.*
Keywords: Secret image sharing, Error diffusion, Visual quality, MPSNR, AFR

1. **Introduction.** Secret image sharing techniques are efficient in protecting secret images. Naor and Shamir in 1995 [1] first propose the original threshold-based visual cryptography scheme(VCS) in which a binary secret image is shared by generating corresponding n noise-like shadow images, and any k or more noise-like shadow images are superposed to obtain the secret image based on human visual system (HVS) and probability. The main properties of the VC method are simple recovery and alternative order of the shadow images. However it also suffers from noisy shadow images, lossy recovery and pixel expansion [2, 3]. Afterwards, more research has been done extensively to overcome the disadvantages. The scheme in [4] is meaningful, but still is lossless recovery and has pixel expansion. Yang [5] proposes a probability-based visual sharing scheme which is lossless and has no pixel expansion but not meaningful. Some other researchers [6, 7, 8, 9] utilize halftone technology to get visual and meaningful shadow images which have a higher quality by employing error diffusion techniques [10]. However, these schemes suffer from pixel expansion. Wang et al. [11] proposes a secret sharing scheme based on Boolean operations that is lossless recovery but has pixel expansion. A (k, n) threshold scheme

proposed by Wu et al. [3] via combining Arnold Permutation, error diffusion and Boolean operations with almost all the properties but only $k = n$ not $k < n$. Other researches [12, 13, 14, 15] realize the secret image sharing based on Shamir's polynomial, but they suffer from complex recovery and known order of the shadow images. In the recently work [16], a visual sharing scheme is proposed combining Arnold permutation, error diffusion and maximum likelihood estimation (MLE). It has good properties for sharing the secrets and satisfies all of the properties described above, that is (k, n) threshold sharing, simple recovery computation (needs only addition and comparison), alternative order of shadow images in recovery, meaningful shadow images, lossless recovery of binary secret image and avoiding the pixel expansion.

Roughly speaking, the quality of shadow images for secret sharing schemes can be evaluated by two quality metrics: peak signal-to-noise-ratio ($PSNR$) or $MPSNR$ [3]. $PSNR$ is used to measure the quality of the grayscale shadow image after embedding secret image, while $MPSNR$ is used to evaluate the quality of halftone image based on low pass filter and $PSNR$. It is noted, however, that $PSNR$ doesn't perfectly correlate to perceived visual quality [17]. Furthermore, $MPSNR$ has major issue for judging the quality of shadow images that is computed after secret sharing and the computation is complex.

Motivated by the simplicity and flexibility for measuring the quality of shadow images, which have the coordinate weight or power, for secret sharing schemes based on error diffusion techniques, this paper proposes a novel quality measure for assessment of shadow image quality, namely average flipping rate (AFR), that formulates and judges the visual quality. This quality measure gives an indication about the quality of shadow images with less complex computation overhead than $MPSNR$.

The rest of this paper is organized as follows. In Section 2, we give an overview about the secret image sharing scheme based on error diffusion techniques and a brief review for the visual quality metrics. The proposed quality measure is introduced in Section 3. In Section 4, the experimental analysis and test results are presented to demonstrate the effectiveness of the proposed measure. Finally, Section 5 concludes this paper.

2. **Related works.**

In this Section, an overview about the secret image sharing scheme based on error diffusion techniques and a brief review for the visual quality metrics are given.

2.1. **An overview of secret image sharing based on error diffusion techniques.**

In this section, we review the very recently secret sharing scheme based on error diffusion techniques [16], that we utilize it in testing and analyzing quality measure to judge the visual quality. The scheme in [16] is selected here due to the fact that it achieves almost all the properties of secret sharing, that is (k, n) threshold sharing, simple recovery computation (needs only addition and comparison), alternative order of shadow images in recovery, meaningful shadow images, lossless recovery of binary secret image, and no pixel expansion.

2.1.1. *Secret image sharing threshold scheme based on error diffusion techniques.* Let I be the normalized $M \times N$ image. $\mathrm{I}(i, j)$, $1 \le i \le M$, $1 \le j \le N$ denotes the current pixel of original gray secret image. The binary image after Floyd-Steinberg dithering (FSD) [18] for I is denoted as S^0 with pixel value $S^0(i, j)$. And S^0 is the secret image. $\mathrm{Q}(i, j)$ is its threshold value, H is the error diffusion matrix, $E(i, j)$ is the computation error. The encrypted or permuted version of S^0 is denoted as S^1. The $n(n \ge 3, n \in Z^+)$ grayscale cover images are normalized to obtain C_i, $1 \le i \le n, i \in Z^+$. The dithered version of C_i is denoted as C_i^0. The shadow binary image is represented as C_i^1. Assume t_k is the

least equal bits number in the same location for $k(k \in Z^+, 3 \leq k \leq n)$. shadow images decoded correctly in recovering phase, t_n is for n shadow images in generation phase.

1. Shadow images generation phase
   The shadow images generation is illustrated in Figure 1, and it mainly contains the following five procedures.

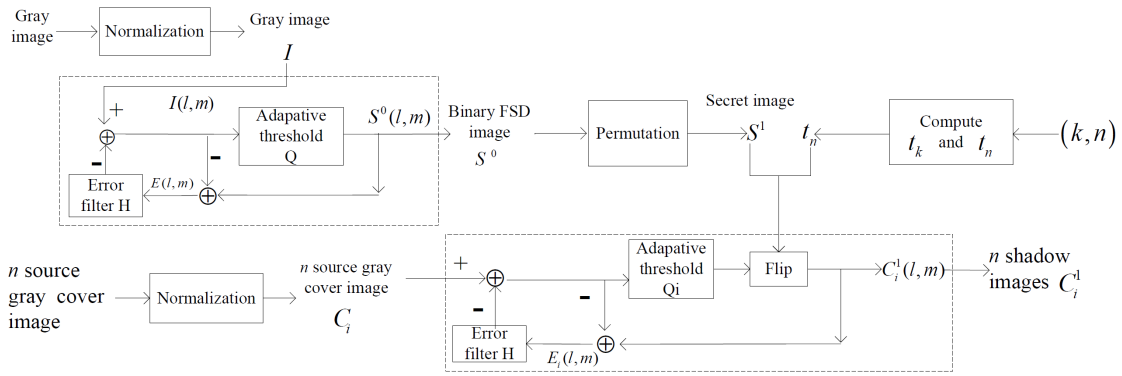

FIGURE 1. Shadow images generation

(1) Normalization
Normalization is to transform the pixel value from integer interval [0, 255] to real interval [0, 1]. Normalize the secret grayscale image and the n grayscale cover images respectively to obtain I and C_i, $1 \leq i \leq n, i \in Z^+$.

(2) Dithering
In the dithering process, the adaptive global threshold by method [19] and the error diffusion [18] matrix H as shown in Eq.(1) are choosed. Use FSD on I to obtain binary image S^0 which is treated as the secret image to share.

$$H = \begin{pmatrix} 0 & (i,j) & \frac{7}{16} \\ \frac{3}{16} & \frac{5}{16} & \frac{1}{16} \end{pmatrix} \tag{1}$$

(3) Permutation
Permute S^0 to obtain S^1. In this method, we use Arnold permutation with $T = 99$ iterations as shown in Eq.(2). (i', j') is the position after permutation corresponding to the original position (i, j). The permutation can also be implemented by other methods, such as chaotic standard map, Baker map encryption [20].

$$\begin{bmatrix} i' \\ j' \end{bmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}^T \begin{bmatrix} i \\ j \end{bmatrix} (\mathrm{mod} M) \tag{2}$$

(4) Compute t_k and t_n
According to the MLE theory, compute t_k and t_n as in Eq. (4) and Eq. (6) in point 3 of the section. MLE is the method that implements the parameter estimation from the maximal posterior probability.

(5) Generating shadow image
The shadow images are generated as follows. For each pixel $C_i(l, m)$ and $S^1(l, m)$, $1 \leq l \leq M, 1 \leq m \leq N$, repeat from step 1 to step 4.
Step 1: Dither C_i by FSD, compute its dithered version $C'_i(l, m)$ and its error $E_i(l, m), 1 \leq i \leq n$.

Step 2: Compute $\{i|C'_i(l,m) = S^1(l,m)\}$. If $|\{i|C'_i(l,m) = S^1(l,m)\}| \geq t_n$, go to Step 4; else go to Step 3.
Step 3: For $\{C'_j(l,m)|C'_j(l,m) \neq S^1(l,m), 1 \leq j \leq n\}$, flip $C'_i(l,m)$ (that is $0 \to 1$ or $1 \to 0$) whose $|E_j(l,m)|$ are the minimal $t_n - |\{i|C'_i(l,m) = S^1(l,m)\}|$ ones. Recompute $E_j(l,m)$ for the flipped shadow images.
Step 4: Perform error diffusion, then go to Step 1 for next pixel.

2. Secret image recovering phase
Any k of the n shadow images C'_j, $1 \leq i \leq k$ are used to recover the original secret image S^0. The following is the revealing procedures as shown in Figure 2.

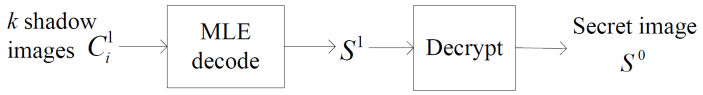

FIGURE 2. Secret image recovery

3. Relation among the (k,n) threshold parameters
First, it should satisfy Eq.(3) to perform MLE, and k shadow images can be decoded correctly based on Eq.(4). In the extreme case, the number of lost shadow images, $n-k$, is the lost number for correct decoding as in Eq.(5). Based on Eqs.(3- 5), we obtain Eq.(6).

$$k \in 2Z^+ + 1, n \in Z^+, k \leq n \tag{3}$$

$$t_k = \left[\frac{k}{2}\right] \tag{4}$$

$$n - k = t_n - t_k \tag{5}$$

$$t_n = \left[n - \frac{k}{2}\right], t_n, n \in Z^+, k \in 2Z^+ + 1, k \leq n \tag{6}$$

2.2. **An overview of the visual quality metrics.** This section gives an overview of the quality metrics that commonly used to date. These include $PSNR$ and $MPSNR$.

2.2.1. *PSNR.* $PSNR$, Eq.(7), is used to measure the quality of the grayscale shadow image after embedding the secret image where MSE, Eq.(8), is used to measure the mean square error between the cover image and shadow image.

$$PSNR = 10\log_{10}(\frac{255^2}{MSE})dB \tag{7}$$

$$MSE = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} [I'(i,j) - I(i,j)]^2 \tag{8}$$

2.2.2. *MPSNR.* $MPSNR$ [3, 17] is a quality metric that models HVS. It is usually used to evaluate the quality of halftone image and computed by low pass filter and $PSNR$.

Computation flowchart of $MPSNR$ is shown in Figure 3. The halftone image $G'(i,j)$ is first inversely halftoned by simple low pass filter to form $G''(i,j)$. Then using Eq.(7) to compute the $PSNR$ of $G''(i,j)$ and $G(i,j)$, and the $MPSNR$ of $G(i,j)$ and $G'(i,j)$ are obtained. In this paper, a 5×5 Gaussian low-pass filter with unit variance is used. The 5×5 Gaussian low-pass filter is shown in Figure 4.

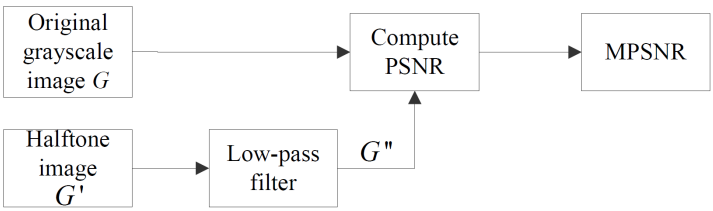

FIGURE 3. Computation flowchart of $MPSNR$

$$\frac{1}{273}\begin{bmatrix} 1 & 4 & 7 & 4 & 1 \\ 4 & 16 & 26 & 16 & 4 \\ 7 & 26 & 41 & 26 & 7 \\ 4 & 16 & 26 & 16 & 4 \\ 1 & 4 & 7 & 4 & 1 \end{bmatrix}$$

FIGURE 4. 5×5 Gaussian low-pass filter

In addition, both $PSNR$ and $MPSNR$ could be commonly used to measure the quality of shadow images. However, $PSNR$ is more suitable for grayscale shadow image, while $MPSNR$ is more suitable for halftone image and to model HVS. Since the proposed quality measure is aimed to measure shadow image which is halftone image based on error diffusion technique, hence the proposed quality measure is compared with $MPSNR$ chiefly.

3. **The proposed quality measure (AFR).** In this section, the proposed quality measure, namely AFR, is defined as that average flipping rate (bits) per shadow image in sharing one secret bit. AFR has lower computation overhead and the same changing trend as $MPSNR$ that is usually used to evaluate the quality of the shadow images based on error diffusion techniques. Further, AFR could be computed before sharing which could be used to guide the parameters selection before the secret sharing phase.

In a (k,n) secret sharing scheme based on error diffusion techniques. m denotes the pixel expansion. Let t be the sharing secret bits per sharing time and s be the flipping bits for n shadow images per sharing time, which can be calculated as follows:

$$s = f(n,k,m,t) \tag{9}$$

where f depends on the secret sharing method based on error diffusion techniques. AFR is defined as:

$$AFR = \frac{s}{nt} = \frac{f(n,k,m,t)}{nt} \tag{10}$$

From Eq.(10), we can find $AFR \in (0, 1)$, and smaller AFR will indicates better visual quality of shadow images. From the experimental results using standard test images as the source gray cover images, the approximately experiential relations between AFR values and the average shadow images quality are shown in Table 1.

TABLE 1. Relations between AFR and shadow image quality

AFR Values	$\frac{1}{3} \leq AFR$	$\frac{1}{4} \leq AFR < \frac{1}{3}$	$\frac{1}{6} \leq AFR < \frac{1}{4}$	$AFR < \frac{1}{6}$
Shadow image quality	Worse, not recognized	Poor, sometimes recognized	Not bad, recognized	Good, easily recognized

4. **Experimental results and numerical investigation.** In this section, the recently proposed secret image sharing scheme based on error diffusion techniques [16] introduced in section 2 is selected to do the experiments to show the effectiveness of the quality measure for assessment of shadow image quality. Here $t = 1, m = 1$, and f depends on the key idea of MLE in [16]. From Eq.(5), we obtain Eq.(11) by dividing the left and right equations by n. Assuming the n shadow images are independent with each other. Then the n bits in the same position with one secret bit of each shadow image are nearly random. That is, the number of 0's and 1's bits are both $\frac{n}{2}$, then the flipping number in the n bits is $s = f(n, k, m, t) = t_n - \frac{n}{2}$, thus we use Eq.(10) to obtain Eq.(12). When $k = n$, the limitation of AFR is shown in Eq.(13).

$$1 - \frac{t_n}{n} < \frac{k}{2n} \Rightarrow 1 - \frac{k}{2n} < \frac{t_n}{n} \tag{11}$$

$$AFR = \frac{t_n - \frac{n}{2}}{n} = \frac{t_n}{n} - \frac{1}{2} > 1 - \frac{k}{2n} - \frac{1}{2} = \frac{1}{2} - \frac{k}{2n} \tag{12}$$

$$AFR \to 0^+ \tag{13}$$

Based on Eqs.(3-6) and Eqs.(11-13), the AFR and $MPSNR$ change values as k, n changes are shown in Table 2.

TABLE 2. AFR and $MPSNR$ changing values as k, n changes

Parameter	t_k	t_n	AFR	$MPSNR$	PSNR
$k \uparrow$	$\uparrow$	$\downarrow$	$\downarrow$	$\uparrow$	$\uparrow$
$n \uparrow$	$=$	$\uparrow$	$\uparrow$	$\downarrow$	$\downarrow$

When $n = 20, k = 3, 5, \cdots, n$. AFR values as k changes are illustrated in Figure 5. When $k = 3, n = k, 4, \cdots, 20$. AFR values as n changes are illustrated in Figure 6. As can be seen from Figure 5 and Figure 6, when n does not change, AFR decreases linearly and is less than 0.5 as k increases. And when k does not change, AFR increases curvedly and is more close to but less than 0.5 as n increases.

Standard cover images with size 256×256 are used to do the experiments. When $n = 20, k = 3, 5, \cdots, n$. $MPSNR$ for the shadow image 1 and the average $MPSNR$ for the 6 FSD images and Floyd-Steinberg dither based sharing ($FSDS$) images as k changes are illustrated in Figure 7. As can be seen from Figure 7, when n does not

change, $MPSNR$ of $FSDS$ images increase as k increases more close to and not larger than FSD images.

When $k = 3, n = k, 4, \cdots, 20$. $MPSNR$ for the shadow image 1 and the average $MPSNR$ for the 6 FSD images and $FSDS$ images as n changes are illustrated in Figure 8.From Figure 8, we can see that when k doesn't change, $MPSNR$ of $FSDS$ images decrease as n increases more different from and not larger than FSD images.

Based on the above observations, in the case n is invariable, as k increases, $MPSNR$ will increase which approach but are not larger than the $MPSNR$ for FSD images and AFR will decrease. In the case k is invariable, as n increases, $MPSNR$ will decrease which is more different from but not larger than the $MPSNR$ for FSD and AFR will increase. The above experimental results show that AFR will denote the $MPSNR$ for the shadow images. From Eq.(12), by the change of k and n, AFR will be calculated easily.

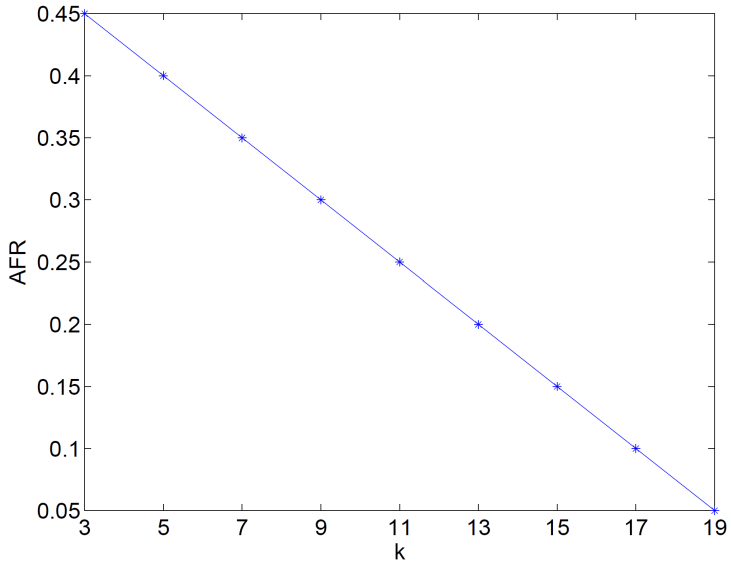

FIGURE 5. AFR values as k changes under $n = 20$

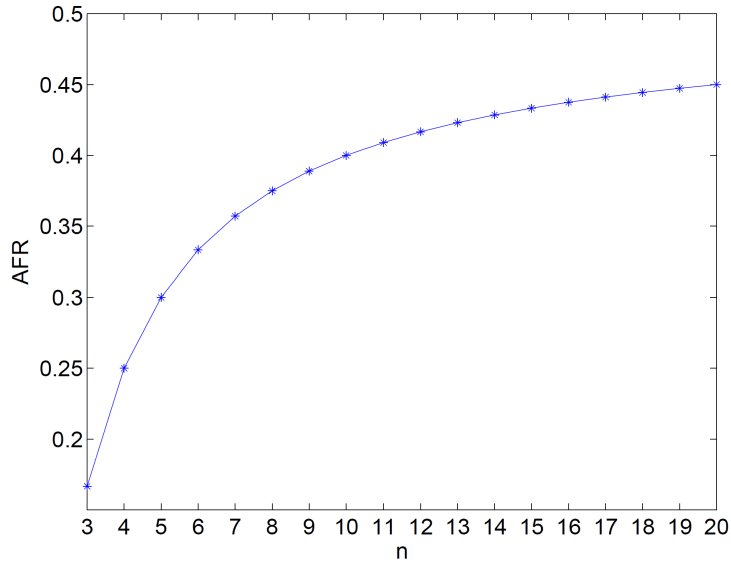

FIGURE 6. AFR values as n changes under $k = 3$

Summarizing, AFR demonstrates an approximate linear relationship with $MPSNR$. Moreover, it has lower complex computation overhead than $MPSNR$ and could be calculated before sharing, which makes it a better candidate to measure the quality of shadow images based on error diffusion techniques.

5. **Conclusions.** This paper introduces a new quality measure for assessment of shadow image quality based on error diffusion techniques. AFR demonstrates an approximate linear relationship with a lower complex computation overhead than MPSNR, and could be evaluated before sharing. Moreover, it can be used as a measure of quality of reconstruction of lossy compression codecs. We hope the new quality measure for assessment of shadow image quality will be useful for the development of secret image sharing techniques.

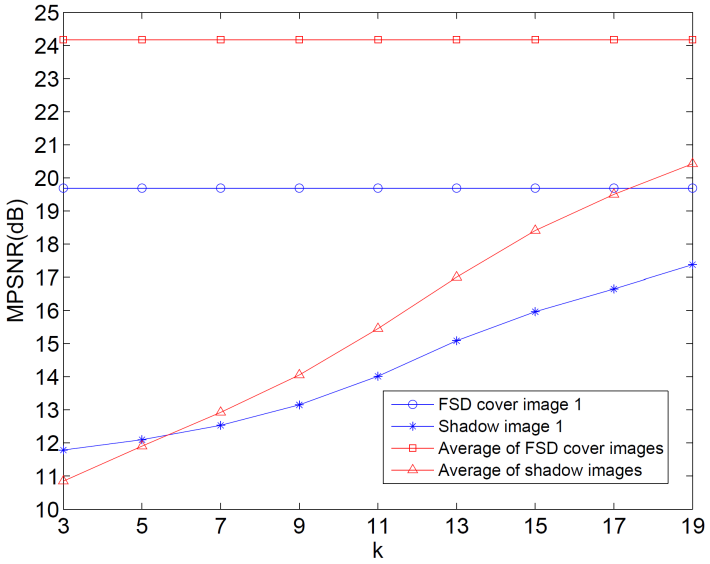

FIGURE 7. $MPSNR$ values as k changes under $n = 20$

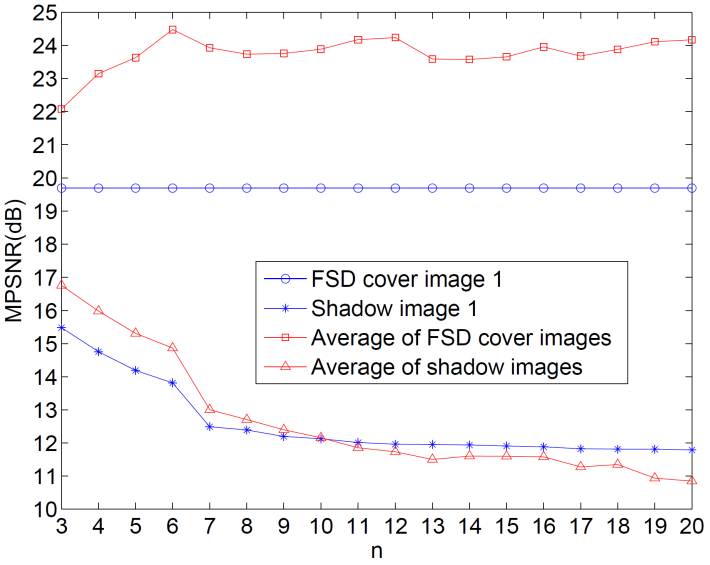

FIGURE 8. $MPSNR$ values as n changes under $k = 3$

6. **Acknowledgement.** This work is supported by the National Natural Science Foundation of China (Grant Number: 60832010, 61100187) and the Fundamental Research Funds for the Central Universities (Grant Number: HIT. NSRIF. 2010046, HIT. NSRIF. 2013061). The authors also gratefully acknowledge the helpful comments and suggestions of the reviewers, which have improved the presentation.

REFERENCES

[1] M. Naor, and A. Shamir, Visual cryptography, *Proc. of Workshop on the Theory and Application of Cryptographic Techniques Perugia*, pp. 1-12, 1994.

[2] J. Weir, and W. Q. Yan, A comprehensive study of visual cryptography, *Published in Transactions on data hiding and multimedia security V*, pp. 70-105, Springer, Berlin-Heidelberg, Germany, 2010.

[3] X. T. Wu, and W. Sun, Image sharing scheme based on error diffusion, *Journal of Computer Applications*, vol. 31, no. 1, pp. 74-81, 2011.

[4] G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, Extended capabilities for visual cryptography, *Journal of Theoretical Computer Science*, vol. 250, no. 1-2, pp. 143-161, 2001.

[5] C. N. Yang, New visual secret sharing schemes using probabilistic method, *Journal of Pattern Recognition Letters*, vol. 25, no. 4, pp. 481-494, 2004.

[6] Z. Zhou, G. R. Arce, and G. D. Crescenzo, Halftone visual cryptography, *IEEE Trans. Image Processing*, vol. 15, no. 8, pp. 2441-2453, 2006.

[7] E. Myodo, S. Sakszawa, and Y. Takishima, Visual cryptography based on void and cluster halftoning technique, *Proc. of IEEE International Conference on Image Processing*, pp. 97-100, 2006.

[8] E. Myodo, K. Takagi, S. Miyaji, and Y. Takishima, Halftone visual cryptography embedding a natural grayscale image based on error diffusion technique, *Proc. of IEEE International Conference on Multimedia and Expo*, pp. 2114-2117, 2007.

[9] Z. Wang, G. R. Arce, and G. D. Crescenzo, Halftone visual cryptography via error diffusion, *IEEE Trans. Information Forensics and Security*, vol. 4, no. 3, pp. 383-396, 2009.

[10] D. L. Lau, and G. Arce, *Modern Digital Halftoning*, Marcel Dekker, New York, USA, 2001.

[11] D. Wang, L. Zhang, N. Ma, and X. Li, Two secret sharing schemes based on Boolean operations, *Journal of Pattern Recognition*, vol. 40, no. 10, pp. 2776-2785, 2007.

[12] J. B. Feng, H. C. Wu, C. S. Tsai, and Y. P. Chu, A new multi-secret images sharing scheme using Lagrange's interpolation, *Journal of Systems and Software*, vol. 76, no. 3, pp. 327-339, 2005.

[13] C. C. Thien, and J. C. Lin, Secret image sharing, *Journal of Computers & Graphics*, vol. 26, no. 5, pp. 765-770, 2002.

[14] C. C. Thien, An image-sharing method with user-friendly shadow images, *IEEE Trans. Circuits and Systems for Video Technology*, vol. 13, no. 12, pp. 1161-1169, 2003.

[15] R. Zhao, J. J. Zhao, F. Dai, and F. Q. Zhao, A new image secret sharing scheme to identify cheaters, *Journal of Computer Standards & Interfaces*, vol. 31, no. 1, pp. 252-257, 2009.

[16] L. Li, X. Yan, N. Wang, A. A. Abd El-Latif, and X. Niu, Meaningful image sharing threshold scheme based on error diffusion, *International Journal of Digital Content Technology and its Applications*, vol. 6, no. 13, pp. 175-284, 2012.

[17] S. K. Yip, O. C. Au, C. W. Ho, and H. M. Wong, PI-preserve data hiding for halftone image, *Proc. of International Symposium on Intelligent Signal Processing and Communication Systems*, pp. 125-128, 2005.

[18] R. W. Floyd, and L. Steinberg, An adaptive algorithm for spatial gray scale, *Proc. of Society for Information Display*, pp. 36, 1975.

[19] N. Otsu, A tlreshold selection method from gray-level histograms, *IEEE Trans. Systems, Man and Cybernetics*, vol. 9, no. 1, pp. 62-66, 1979.

[20] L. Li, A. A. Abd El-Latif, Z. Shi, and X. Niu, A new loss-tolerant image encryption scheme based on secret sharing and two chaotic systems, *Research Journal of Applied Sciences, Engineering and Technology*, vol. 4, no. 8, pp. 877-883, 2012.