Journal of Information Hiding and Multimedia Signal Processing ©2014 ISSN 2073-4212
Ubiquitous International Volume **5**, Number **3**, July **2014**

Friendly Medical Image Sharing Scheme

Hao-Kuan Tso

Department of Computer Science and Communication Engineering
Army Academy R.O.C.
No.750, Longdong Rd., Zhongli City, Taoyuan County 320, Taiwan
haokuantso@gmail.com

Tsung-Ming Lo

Department of Computer and Communication Engineering
China University of Technology
No.530, Sec.3, Zhong-Shan Rd., Hukou, Hsinchu, Taiwan
c36ltm@cute.edu.tw

Wei-Kuei Chen

Department of Computer Science and Information Engineering
Chien Hsin University of Science and Technology
Chungli, Taoyuan 320, Taiwan
wkchen@uch.edu.tw

Received September, 2013; revised January, 2014

Abstract. *In recent years, visual sharing technique has drawn much attention for researchers due to the characteristics of security and simpleness. We can utilize visual sharing technique to divide a secret image into meaningless shares and one of them cannot reveal any information about the secret image unless superimposing the shares by the authorized users. However, the meaningless shares are difficult to identify and manage. In the applications of military and medical images, the constructed shares should be meaningful ones that are easier for users to manage and identify them. In the paper, a friendly visual sharing scheme is proposed to protect the security of the medical images. First the random-grid algorithm is utilized to construct two meaningless shares. Then a friendly pattern is superimposed on the shares that can make the users manage and identify them easily. No one can obtain the information about patients' images by observing the appearance of the shares. Therefore, the medical images cannot be abused and patients' privacy can be assured. Experimental results can show the feasibility of the proposed scheme.mance discussion, we can prove that our method does not only to provide the improved embedding capacity but also to maintain good stego image quality.*
Keywords: Visual sharing, medical images, friendly sharing, pixel expansion, random grid.

1. **Introduction.** The development of computer network can make us transmit digital data to far relatives and friends rapidly. Therefore we can save much precious time than traditional deliver modes. Businesses can also save a lot of expenses by selling their products to customers in networks. Furthermore, the establishment of medical information system gives us a lot of convenience. When a patient is transferred to another hospital, the digitized medical information, such as patients diagnosis reports and x-ray images, can be transmitted to another hospital through networks. In this case, patient and hospital both can save lots of expenses in photographing

When everyone is enjoying the convenient life environment, some crackers intend to intrude businesses' and hospitals' computers and steal the important information. How to prevent unauthorized people accessing the sensitive information has become a very important work. Two well-known technologies that are cryptography and data hiding can be utilized to protect the security of the important information. Cryptography technique has been utilized in many applications of daily life, such as smart card, E-commerce and data encryption. By encrypting the secret information into disordering codes, the unauthorized users cannot observe the original secret information unless the key is obtained. Data hiding technique is also extensively discussed in recent years due to the characteristic of imperceptibility. Therefore we can further combine data hiding and cryptography techniques to achieve the goal of protecting information.

Another well-known technique is visual sharing firstly proposed by Naor and Shamir [1] in 1995. Simpleness and security are the main characteristics. We can utilize visual sharing technique to encode a secret image into n meaningless shares and transmit them to n participators. Unauthorized users cannot observe the original information from one of the meaningless shares unless superimposing greater than or equal to m ($m \leq n$) shares. In the applications of medical images, visual sharing can be applied to protect patients' diagnosis reports and images. If one of the shares is disappeared, the original information can still be recovered from other participators.

Fig. 1 shows the example of the (2, 2) visual sharing technique. By utilizing the predesigned codebook (as shown in Table 1), we can encode a secret image (Fig. 1(a)) into two expanded meaningless shares shown as Fig. 1(b)-(c). From one of the shares, we cannot recover any information about the secret image. Furthermore, the secret image can be revealed (Fig. 1(d)) by superimposing two shares.

TABLE 1. The codebook of (2,2) visual sharing

Pixel	Sharing 1	Sharing 2	Stacked results	Pixel	Sharing 1	Sharing 2	Stacked Results
□	▄	▄	■	■	▄	▀	■
	▄	▄	■		▄	▄	■
	▖	▖	▌		▖	▗	■
	▗	▗	▟		▗	▖	■
	▚	▚	▚		▚	▚	■
	▞	▞	▞		▞	▞	■

Lukac and Plataniotis [2] extended the above-mentioned concept and proposed a visual sharing method using bit-level decomposition. In the sharing process, a gray-scale image is first decomposed into bit planes where each plane can be viewed as a binary image. Then each plane is encoded into two images by using the codebook proposed by Naor and Shamir. By stacking the images, two gray-scale shares can be constructed. The recovery process is the reversion of the sharing process. Experimental results show that the original gray-scale image can be recovered without distortion. The two methods mentioned above have the common disadvantages. That is to say, the constructed shares are expanded and

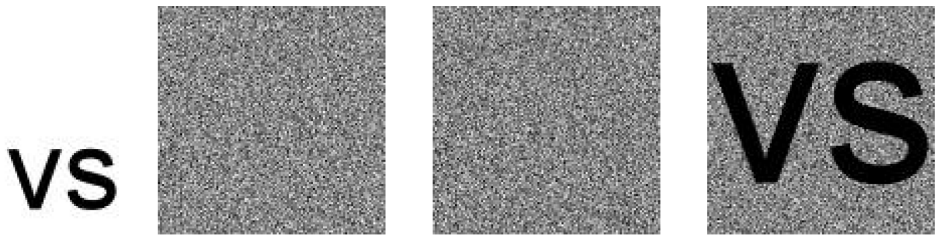


FIGURE 1. The example of the (2, 2) visual sharing technique. (a) the secret image, (b)-(c) the shares, (d) the revealed image.

meaningless ones which are difficult to manage and can occupy lots of storage space for participators.

To improve the problem of pixel expansion, the non-expanded sharing techniques based on random grid [3] have been proposed in recent years [4-9]. The three methods of random grid can be described as follows.

[Method 1]

1. Generate a sharing image $R1$ as a random grid, where $R1$ consists of random value of 0 or 1.
2. For every pixel of the image S:

$for\ i = 1\ to\ m;$
$for\ j = 1\ to\ n;$
$if\ S(i,j) == 0;$
$R2(i,j) = R1(i,j);$
$else$
$R2(i,j) = \overline{R1}(i,j);$
end
end
end

[Method 2]

1. Generate a sharing image $R1$ as a random grid, where $R1$ consists of random value of 0 or 1.
2. For every pixel of the image S:

$for\ i = 1\ to\ m;$
$for\ j = 1\ to\ n;$
$if\ S(i,j) == 0;$
$R2(i,j) = R1(i,j);$
$else$
$R2(i,j) = Random\_pixel(0,1);$
end
end
end

Where Random_pixel(0, 1) indicates the function that consists of random value of 0 or 1.

[Method 3]

1. Generate a sharing image $R1$ as a random grid, where $R1$ consists of random value of 0 or 1.
2. For every pixel of the image S:

$for\ i = 1\ to\ m;$

```
    for j = 1 to n;
        if S(i, j) == 0;
            R2(i, j) = Random_pixel(0, 1);
        else
            R2(i, j) = R1(i, j);
        end
    end
end
```

Shyu [4] utilized the random grid to construct the non-expanded shares in 2007. We take a gray-scale image as an example. First a gray-scale image is transformed into halftone image. Then the halftone image is encoded into two shares by utilizing the algorithm of the random grid. Chen and Tsao [5] also proposed a threshold visual sharing method based on random grid. They utilize the algorithm of the random grid to encode a binary image into n shares. Less than k ($k \leq n$) shares cannot reveal the information of the secret image unless greater than or equal to k shares are superimposed. The common disadvantages of the two methods mentioned above include: (1) The constructed shares are meaningless ones that are difficult to manage them for users. (2) The secret images cannot be completely recovered which can affect the users' judgments, especially in the applications of military and medical images.

As you see, meaningless shares will cause the difficulty in management and identification. To solve the problem, many friendly sharing methods have been proposed in recent years [10-14]. Friendly sharing means that the constructed shares are meaningful images which can be identified quickly and managed conveniently. Fang [11] utilized a cover image to construct the friendly shares. First a secret image is expanded to the same size as the cover image. Then the expanded secret image and the cover image are encoded into n friendly shares by utilizing the pre-designed codebook. Owing to the appearance of friendly shares, participators are more convenient to manage them. Furthermore, the secret image can be completely recovered by superimposing all of the shares. The disadvantage of the method is that the constructed shares have the problem of pixel expansion. Yang et al. [12] proposed a friendly sharing method by using polynomial. They first modify the secret image by calculating the differences between neighbor pixels of current block and embedding the indicators of the prime number to the pixels of previous block. Then the polynomial function is utilized to construct the shares where the constructed shares are the shrunken version of the secret image. However, the quality of the reconstructed image must be improved. Chan et al. [13] proposed a friendly sharing method by utilizing JPEG-LS predictor to improve the disadvantage of Yang et al. method [12]. Chan et al. firstly utilize the JPEG-LS predictor that is the latest standard for lossless and close lossless image compression to predict the differences between neighbor pixels in a block. Then the polynomial function is utilized to construct the shares as Yang et al. method. Although the experimental results show that the quality of the reconstructed image has improved, the original image cannot be completely recovered.

To improve the above-mentioned disadvantages, the paper proposes a friendly visual sharing method to protect the security of the medical image. The rest of the paper is organized as follows. The proposed sharing method is drawn in Section 2. Experimental results are shown in Section 3. Discussions are illustrated in Section 4. Conclusions are given in Section 5.

2. **The proposed method.**

The proposed visual sharing method consists of two stages: sharing and recovery stages. In the sharing stage, the random-grid algorithm is utilized to construct two meaningless shares. Then a friendly pattern is superimposed on the

shares that can make the users manage and identify them easily. In the recovery stage, performing Exclusive-OR operation between the shares, the secret image can be recovered without distortion. The detailed processes are described as follows.

2.1. **Sharing stage.** Input: A medical image MI and meaningful binary pattern P with size of m by n.
Output: Two shares S^1 and S^2 with size of m by n.

Step 1: Utilize a pseudo random number generator to generate a random grid $RG1$ with size of m by n, where the range of the value is $[1, 2^B]$ and B represents bit level.

Step 2: Decompose the medical image MI and random grid $RG1$ into bit planes, where MI and $RG1$ can be represented as follows.

$$MI_{(i,j)} = 2^b \times MI^b_{(i,j)} + 2^{b-1} \times MI^{b-1}_{(i,j)} + ... + 2^2 \times MI^2_{(i,j)} + 2^1 \times MI^1_{(i,j)}, \tag{1}$$

$$RG1_{(i,j)} = 2^b \times RG1^b_{(i,j)} + 2^{b-1} \times RG1^{b-1}_{(i,j)} + ... + 2^2 \times RG1^2_{(i,j)} + 2^1 \times RG1^1_{(i,j)}, \tag{2}$$

Where $b = 1 \dots B$.

Step 3: Sequentially take the results of Step 2 into Eq. (3) to construct B random images.

$$RG2^b_{(i,j)} = \begin{cases} RG1^b_{(i,j)} \ , \ if \quad MI^b_{(i,j)} = 0 \\ \overline{RG1^b_{(i,j)}} \ , \ if \quad MI^b_{(i,j)} = 1, \end{cases} \tag{3}$$

Where $\overline{RG1^b_{(i,j)}}$ represents the complement of $RG1^b_{(i,j)}$.

Step 4: Separatelly superimpose B random images and the meaningful pattern P to construct two friendly shares, described as follows.

$$S^1_{(i,j)} = 2^{b+1} \times P + 2^b \times RG1^b_{(i,j)} + 2^{b-1} \times RG1^{b-1}_{(i,j)} + ... + 2^2 \times RG1^2_{(i,j)} + 2^1 \times RG1^1_{(i,j)}. \tag{4}$$

$$S^2_{(i,j)} = 2^{b+1} \times P + 2^b \times RG2^b_{(i,j)} + 2^{b-1} \times RG2^{b-1}_{(i,j)} + ... + 2^2 \times RG2^2_{(i,j)} + 2^1 \times RG2^1_{(i,j)}. \tag{5}$$

Step 5: Stop.

2.2. **Recovery stage.** Input: Two shares S^1 and S^2 with size of m by n.
Output: The recovered medical image with size of m by n.

Step 1: Decompose the shares S^1 and S^2 into bit planes as Eq. (6) and Eq. (7).

$$S^1_{(i,j)} = 2^{b+1} \times P + 2^b \times RG1^b_{(i,j)} + 2^{b-1} \times RG1^{b-1}_{(i,j)} + ... + 2^2 \times RG1^2_{(i,j)} + 2^1 \times RG1^1_{(i,j)}. \tag{6}$$

$$S^2_{(i,j)} = 2^{b+1} \times P + 2^b \times RG2^b_{(i,j)} + 2^{b-1} \times RG2^{b-1}_{(i,j)} + ... + 2^2 \times RG2^2_{(i,j)} + 2^1 \times RG2^1_{(i,j)}. \tag{7}$$

Step 2: Extract $RG1$ and $RG2$ from the results of Step 1 as Eq. (8) and Eq. (9).

$$RG1_{(i,j)} = 2^b \times RG1^b_{(i,j)} + 2^{b-1} \times RG1^{b-1}_{(i,j)} + ... + 2^2 \times RG1^2_{(i,j)} + 2^1 \times RG1^1_{(i,j)}, \tag{8}$$

$$RG2_{(i,j)} = 2^b \times RG2^b_{(i,j)} + 2^{b-1} \times RG2^{b-1}_{(i,j)} + ... + 2^2 \times RG2^2_{(i,j)} + 2^1 \times RG2^1_{(i,j)}. \tag{9}$$

Step 3: Perform Exclusive-OR operations between bit planes of $RG1^b$ and $RG2^b$ as Eq.(10).

$$MI'_{(i,j)}{}^{b} = RG1^{b} \oplus RG2^{b}_{(i,j)}. \tag{10}$$

Step 4: Sequentially superimpose bit planes of Step 3 to recover the medical image as Eq. (1).

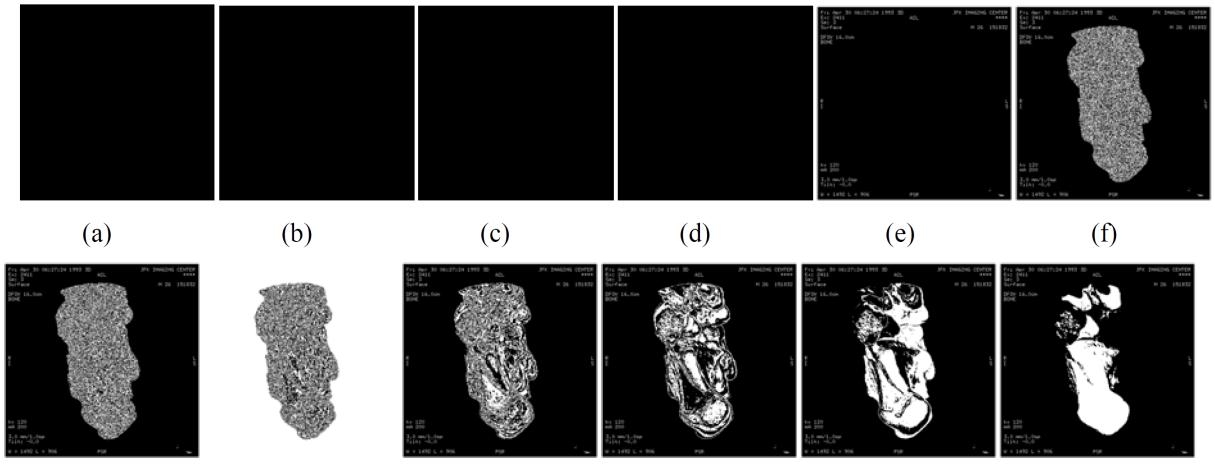
Step 5: Stop.

3. **The experimental results.** The experiments will show the feasibility of the proposed method. In the first experiment, the 12-bit medical image "Ankle" with size of 512 by 512 is utilized to be the test image shown as Fig. 2(a). The meaningful pattern is utilized to be the friendly share shown as Fig. 2(b). First we utilize a pseudo random number generator to generate the random grid RG1 with size of 512 by 512 shown as Fig. 2(c). Then the medical image and random grid RG1 are sequentially decomposed into bit planes as shown in Fig. 3 and Fig. 4.

(a) (b) (c)

FIGURE 2. The experimental images. (a) the test image, (b) the meaningful pattern, (c) random grid $RG1$.

By performing the algorithm of the random grid as Eq. (3), we can obtain 12 random images with size of 512 by 512 that are similar to Fig. 4. The above 12 random images can be constructed into random grid $RG2$ with size of 512 by 512 as shown in Fig 5(a). To easily manage the shares, the meaningful pattern (Fig. 2(b)) is superimposed on random grid $RG1$ to construct the friendly share S^1 with size of 512 by 512 shown as Fig.



(a) (b) (c) (d) (e) (f)

(g) (h) (i) (j) (k) (l)

FIGURE 3. The bit planes of the medical image. (a)-(l) bit plane 1 to 12.

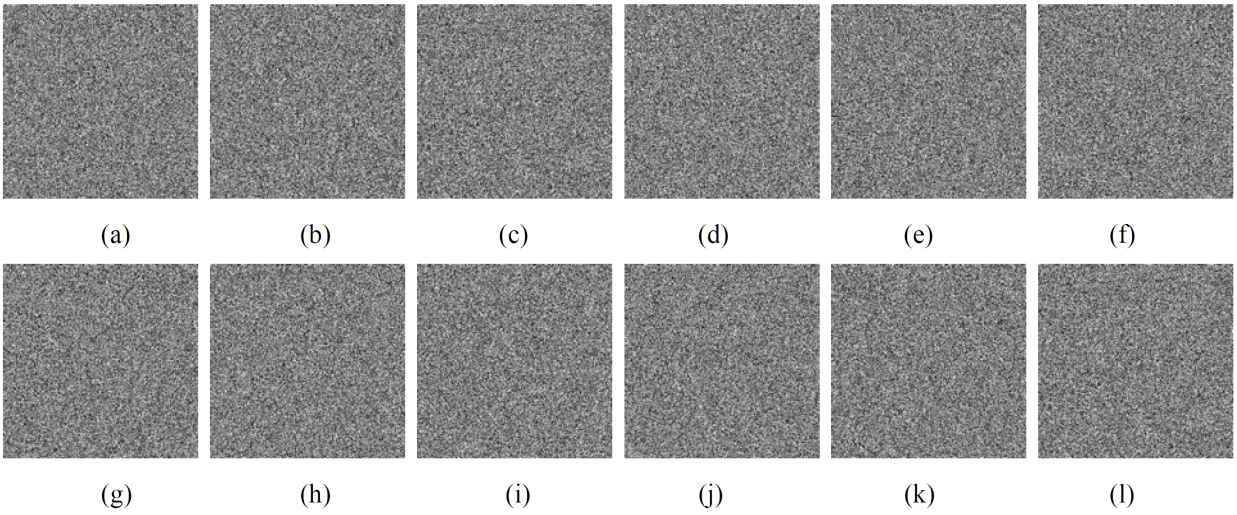


FIGURE 4. The bit planes of the random grid $RG1$. (a)-(l) bit plane 1 to 12.

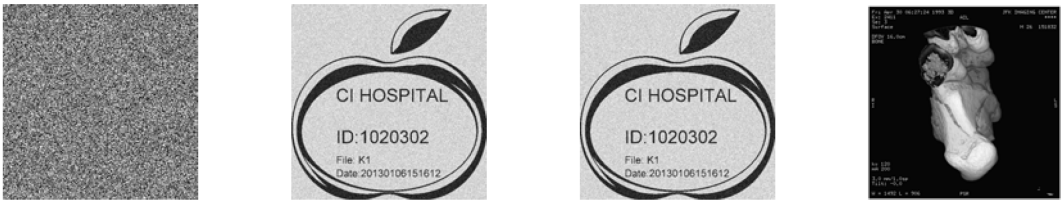


FIGURE 5. The experimental results. (a) the random grid $RG2$, (b) and (c) the shares S^1 and S^2,(d) the recovered medical image.

5(b). Furthermore, the meaningful pattern is also superimposed on random grid $RG2$ to construct another friendly share S^2 with size of 512 by 512 shown as Fig. 5(c).

As you see, the friendly shares are easier to manage for doctors and hospitals. Furthermore, one of shares cannot reveal the original information about the medical image. Therefore, the security of the medical image will be greatly increased. To recover the medical image, we first decompose the shares S^1 and S^2 and obtain the random grids $RG1$ and $RG2$. Then by performing Exclusive-OR operations between bit planes of the random grids $RG1$ and $RG2$, bit planes of the medical image will be recovered. Finally, the original medical image can be completely recovered (shown as Fig. 5 (d)) by sequentially superimposing the above-mentioned bit planes. The evaluation method of the recovered image is mean square error (MSE) that can be represented as Eq. (11).

$$MSE = \frac{1}{MN} \sum_{i=1}^{m} \sum_{j=1}^{n} [MI(i,j) - MI'(i,j)]^2. \tag{11}$$

Where MI and MI' represent the original and retrieved images respectively. After taking the original and retrieved images into Eq. (11), the obtained MSE is 0 that represents the retrieved image is lossless.

In the following experiment, The 12-bit medical image "Brain" with size of 512 by 512 is utilized to be the test image and another meaningful pattern is utilized to be the friendly

share shown as Fig. 6(a) and Fig. 6(b). Fig. 6(c) shows the random grid $RG1$ with size of 512 by 512 generated by utilizing the pseudo random number generator. First we decompose random grid $RG1$ and the medical image "Brain" into bit planes. Fig. 7(a)-(l) show the 12 bit planes of the medical image. Then the algorithm of the random grid is utilized to construct the random grid $RG2$ with size of 512 by 512 as shown in Fig. 8(a). Finally the meaningful pattern is superimposed on random grids $RG1$ and $RG2$ to construct the friendly shares S^1 and S^2 with size of 512 by 512 shown as Fig. 8(b) and Fig. 8(c)

FIGURE 6. The experimental images. (a) the test image, (b) the meaningful pattern, (c) random grid $RG1$.

To recover the medical image, the recovery process is similar to the first experiment. Fig 8 (d) shows the recovered medical image. The obtained MSE is 0 that represents the retrieved image is lossless. As you see, the two experimental results show that the friendly shares have no the disadvantage of pixel expansion and the recovered medical images cannot cause the fault judgment of the doctors. Furthermore, the experimental results also show that the proposed method can effectively protect patients' privacy and prevent the abuse of the medical images.

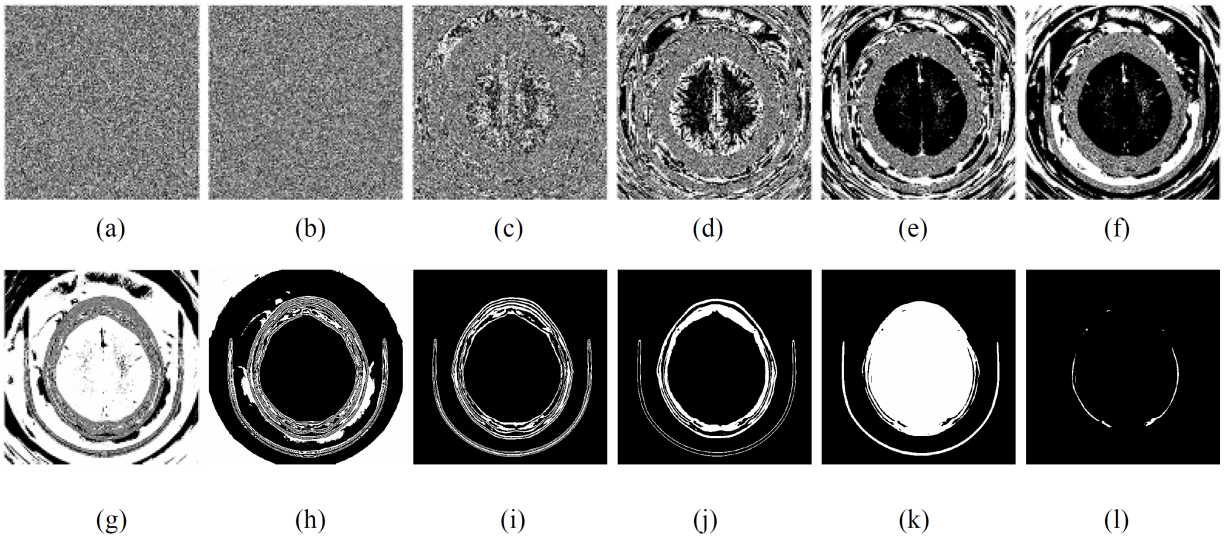
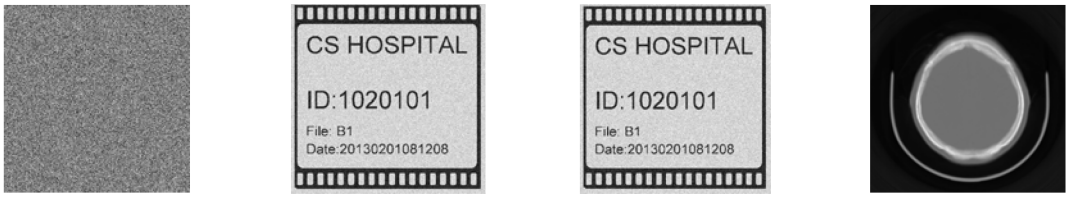


FIGURE 7. The bit planes of the medical image. (a)-(l) bit plane 1 to 12.

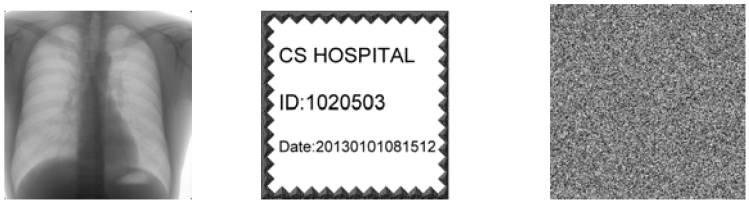
In the third experiment, The 10-bit medical image "Chest" with size of 440 by 440 is utilized to be the test image and another meaningful pattern is utilized to be the friendly share shown as Fig. 9(a) and Fig. 9(b). Fig. 9(c) shows the random grid RG1 with size of 440 by 440 generated by utilizing the pseudo random number generator. Fig. 10(a)-(j)



(a) (b) (c) (d)

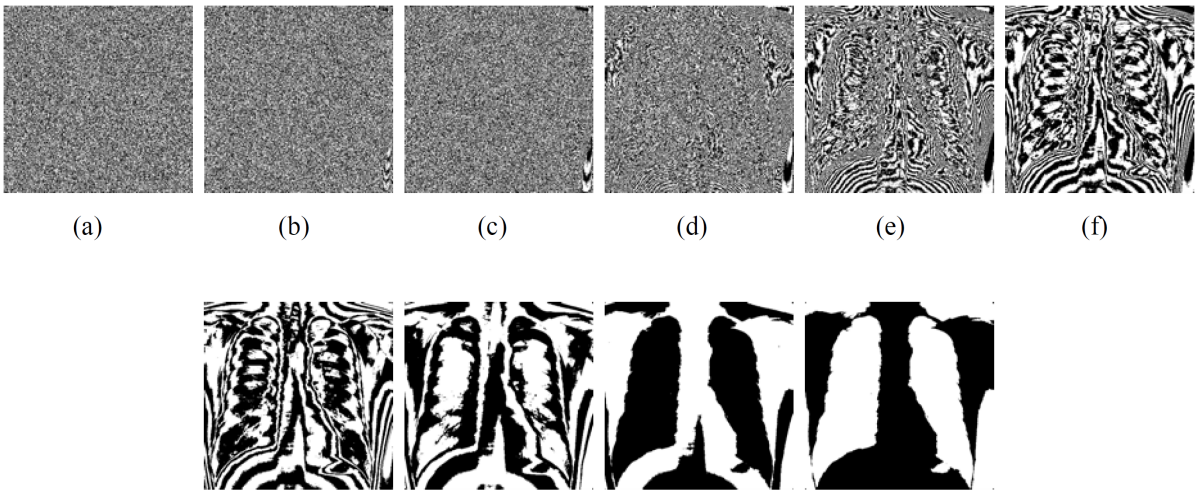
FIGURE 8. The experimental results. (a) the random grid $RG2$, (b) and (c) the shares S^1 and S^2, (d) the recovered medical image.

show the 10 bit planes of the medical image. Fig. 11(a)-(c) shows the random grids RG2 and two friendly shares with size of 440 by 440 respectively. The retrieved medical image is shown in Fig. 11(d). The obtained MSE is 0 that represents the retrieved image is lossless.



(a) (b) (c)

FIGURE 9. The experimental images. (a) the test image, (b) the meaningful pattern, (c) random grid $RG1$.



(a) (b) (c) (d) (e) (f)

(g) (h) (i) (j)

FIGURE 10. The bit planes of the medical image. (a)-(j) bit plane 1 to 10.

If authenticators wrongly put two same shares together, that is only using the share S^1 or S^2, the recovered results can be the black images as shown in Figs. 12(a) and 12(b). Furthermore, if authenticators superimpose two incorrect shares, for example, Figs 5(b) and 8(c) or Figs 5(c) and 8(b), the recovered images can be the noise images that cannot be recognized as shown in Figs. 12(c) and 12(d).

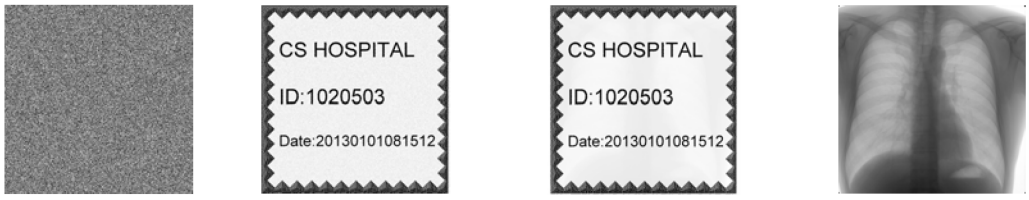


FIGURE 11. The experimental results. (a) the random grid $RG2$, (b) and (c) the shares S^1 and S^2, (d) the recovered medical image.

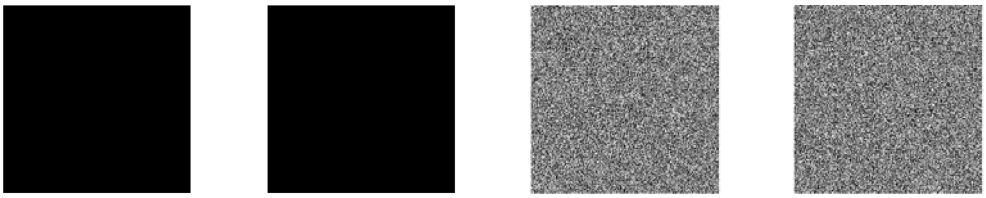


FIGURE 12. The experimental results. (a) the recovered results of S^1 and S^1, (b) the recovered results of S^2 and S^2, (c) the recovered results of Figs 5(b) and 8(c), (d) the recovered results of Figs 5(c) and 8(b).

4. **Discussions.** In the paper, a friendly sharing method is proposed to protect the security of medical images. The advantages of the proposed method can be summarized as follows.
(1) Non-expanded shares. Traditional visual cryptography based on codebook has the disadvantage of pixel expansion. The proposed method based on random grid removes the above-mentioned problem, which can save lots of storage space(2) Friendly shares. Many published methods encode the secret images into meaningless shares. As you can see, the meaningless shares are difficult to manage and identify. The proposed friendly sharing method can construct the secret images into meaningful shares that are easier for users to manage and identify them(3) Computation cost. Several published methods based on polynomial [12-14] must take much computation time to construct the shares. The proposed schemes only decompose the medical image and random grid into bit planes (similarly to the Lukac-Plataniotis method [2]) and perform Exclusive-OR operations in the sharing and recovery stages. For example, in the first and second experiments, the size of 12-bit images is 512 by 512. By using the computer with Intel Pentium Dual CPU T3200 2GHZ and memory 2GB to implement the method, the execution time is 0.181 second from constructing random grids to performing Exclusive-OR operations. The constructed shares are about 426KB. In the third experiment, the size of 10-bit image is 440 by 440. The execution time is 0.152 second. The constructed shares are about 266KB. Therefore, the scheme is still feasible when the size of images is increasing(4) Lossless recovery. In the applications of military and medical images, the lossy images can cause the fault judgement for users. The proposed method ustilizes Exclusive-OR operations to achieve the lossless recovery.

As you can see, the proposed method improves the disadvantages of pixel expansion, meaningless sharing and lossy recovery. The comparison results between some published methods and the proposed method are shown as Table 2.

TABLE 2. The comparison between the published and the proposed methods.

Methods	Kernel	Non-expanded pixel	Friendly shares	Lossless recovery
Shyu [4]	Random grid	Yes	No	No
Chen and Tsao [5]	Random grid	Yes	No	No
Chen and Tsao [6]	Random grid	Yes	No	No
Chen and Tsao [7]	Random grid	Yes	No	No
Fang [8]	Random grid	No	No	No
Wang et al [9]	Random grid	Yes	No	No
Fang [11]	Codebook	No	Yes	Yes
Yang et al [12]	polynomial	Yes	Yes	No
Chan et al [13]	polynomial	Yes	Yes	No
The proposed method	Random grid	Yes	Yes	Yes

5. **Conclusions.** Visual sharing method has been extensively discussed in recent years due to the characteristics of security and simpleness. In the paper, a friendly visual sharing method based on random grid is proposed to protect the security of the medical images. Friendly sharing can help users manage the shares easily. That is to say, users can easily identify the shares and correctly recover the original images. The original images can be completely recovered without distortion that is helpful to doctors' judgment. Furthermore, the experimental results show that no one can obtain the original information by observing the appearance of the shares. Therefore, the security of the medical images can be greatly increased. Compared with other published methods, the superiority of the proposed method can be revealed. In the future, the threshold sharing method and progressive recovery will be the main research directions.

Acknowledgment. The authors would like to thank the anonymous referees and the editor for their valuable opinions. This research was partially supported by National Science Council of the Republic of China under grants NSC 101-2221-E-539-005-.

REFERENCES

[1] M. Naor, and A. Shamir, Visual cryptography, *Proc. of Advances in Cryptology-EUROCRYPT'94, Workshop on the Theory and Application of Cryptographic Techniques*, LNCS 950, Springer, pp. 1-12, 1995.

[2] R. Lukac, and K. N. Plataniotis, Bit-level based secret sharing for image encryption, *Journal of Pattern Recognition*, Vol. 38, no. 5, pp. 767-772, 2005.

[3] O. Kafri, and E. Keren, Encryption of pictures and shapes by random grids, *Optics Letters*, vol. 12, no. 6, pp. 377-379, 1987.

[4] S. J. Shyu, Image encryption by random grids, *Pattern Recognition*, vol. 40, no. 3, pp. 1014-1031, 2007.

[5] T. H. Chen, and K. H. Tsao, Threshold visual secret sharing by random grids, *Journal of System and Software*, vol. 84, no. 7, pp. 1197-2008, 2011.

[6] T. H. Chen, and K. H. Tsao, Visual secret sharing by random grids revisited, *Pattern Recognition*, vol. 42, no. 9, pp. 2203-2217, 2009.

[7] H. K. Tso, and D. C. Lou, Sharing secret image based on random grids, *Proc. of The 2nd International Workshop on Multimedia, Information Privacy and Intelligent Computing Systems, Workshop on Computer Science and Its Applications*, pp. 399-403, 2009.

[8] W. P. Fang, Non-expansion visual secret sharing in reversible style, *International Journal of Computer Science and Network Security*, vol. 9, no. 2, pp. 204-208, 2009.

[9] Z. H. Wang, M. S. Pizzolatti, and C. C. Chang, Reversible visual secret sharing based on random-grids for two-image encryption, *International Journal of Innovative Computing, Information and Control*, vol. 9, no. 4, pp. 1691-1701, 2013.

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

[11] W. P. Fang, Friendly progressive visual secret sharing, *Pattern Recognition*, vol. 41, no. 4, pp. 1410-1414, 2008.

[12] C. N. Yang, K. H. Yu, and R. Lukac, User-friendly image sharing using polynomials with different primes, *International Journal of Imaging Systems and Technology*, vol. 17, no. 1, pp. 40V47, 2007.

[13] C. S. Chan, C. C. Chang, and P. V. Hung, A user-friendly image sharing scheme using JPEG-LS median edge predictor, *Journal of Information Hiding and Multimedia Signal Process*, vol. 3, no. 4, pp. 340-351, 2012.

[14] P. VO. Hung, A user-friendly image sharing scheme using JPEG-LS prediction and LSB matching function, *International Journal of Modern Engineering Research*, vol. 3, no. 1, pp. 139-148, 2013.