http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet

Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 9 (2): 298-304, 2010
ISSN 1812-5638

Shadow Size Reduction and Multiple Image Secret Sharing Based on Discrete Fractional Random Transform

[1,2]Zhenfei Zhao, [3]Hao Luo and [3]Zhe-Ming Lu
[1]Sun Yat-sen University, Guangzhou,
[2]Heilongjiang Institute of Science and Technology, Harbin,
[3]School of Aeronautics and Astronautics, Zhejiang University, Hangzhou, 310027,
People's Republic of China

Abstract: This study proposes an improved image secret sharing scheme based on the discrete fractional random transform. In this (r, n)-threshold prototype, the shadow size is reduced to 1/r of the secret image. In contrast, all shadows are of the same size as that of the secret image in the original scheme. Consequently, much storage space and transmission time is saved. Besides, our scheme can be naturally extended to multi-image secret sharing, i.e., r secret images can be encrypted in n shadows at a time. Meanwhile, the security is perfectly preserved due to the randomness of the discrete fractional random transform. Experimental results demonstrate the effectiveness of our scheme.

Key words: Image secret sharing, shadow size reduction, discrete fractional random transform

INTRODUCTION

Secret sharing plays an important role in image encryption. In the (r, n)-threshold model (Shamir, 1979), the secret image is encrypted and shared in n shadows. If any r or more than r shadows polled, the original secret can be decrypted, while r-1 or fewer shadows cannot recover any meaningful information. Thien and Lin (2002) first apply the Shamir's paradigm for image secret sharing. After that, various image secret sharing schemes are reported in literatures. Most of these schemes made great efforts in two aspects. (1) Reducing the shadow size (Wu *et al*., 2004; Lin and Tsai, 2003; Yang and Chen, 2005, 2006; Wang and Su, 2006). In Shamir's paradigm, each shadow is of the same size as the secret image. Thus a heavy burden is laid on network resources and transmission channels. Reducing the shadow size can alleviate this problem. (2) Encrypting multiple secret images. In recent years, multi-secret sharing is investigated in literatures (Yang *et al*., 2004; Feng *et al*., 2005; Tsai *et al*., 2002; Wu and Chang, 2005). Obviously, hiding multiple secrets instead of one enhances the sharing efficiency.

It is necessary to note that, most of the available image secret sharing schemes such as the above mentioned methods are based on spatial domain pixels operations. Recently, Liu *et al*. (2008) proposed an (r, n)-threshold scheme for image sharing from a new prospect, i.e., based on transform domain coefficients operations. In particular, the discrete fractional random transform (DFRNT) (Liu *et al*., 2005) is employed to achieve this. This scheme is effective and perfectly secure due to the DFRNT exploited. However, in this scheme all of the shadows are of the same size as that of the secret image and thus much storage space is required and more transmission time is spent. Another important property of Liu *et al*. (2008) scheme is that only one secret image can be encrypted at a time. Thus its encryption efficiency is not very high. In fact, a Largrange interpolation-based method for shadow size reduction has been proposed by Thien *et al*. (2002), with each shadow being 1/r size of the secret image. In this study, we improve Liu *et al*. (2008) scheme to achieve this goal. Moreover, our scheme still preserves high security due to the randomness of DFRNT. Our improvement can be naturally extended to multi-image secret sharing.

As both Liu *et al*.'s and our schemes are based on DFRNT, we briefly review the DFRNT (Liu *et al*., 2005) and Liu *et al*.'s image sharing scheme (Liu *et al*., 2005). DFRNT is a generalized transform for one or two-dimensional discrete signal analysis derived from the discrete fractional Fourier transform (DFrFT). Specifically, we focus on the DFRNT usage on two-dimensional data. The DFRNT of a two-dimensional image X can be represented as:

Corresponding Author: Hao Luo, School of Aeronautics and Astronautics, Zhejiang University, Hangzhou, 310027, People's Republic of China

$$Y=R^{\alpha}X(R^{\alpha})^{T} \tag{1}$$

where, R^{α} and α denote the kernel matrix and the fractional order of DFRNT, respectively. The superscript T means matrix transposition. The output matrix Y is composed by the transform coefficients in the DFRNT domain.

To construct a transform matrix R^{α}, a random matrix P must be generated obtain in advance as:

$$P=\frac{(Q+Q^{T})}{2} \tag{2}$$

where, Q is a real nonsingular matrix with elements randomly generated. Suppose $V = (v_1,v_2,\dots v_N)$ denotes the normalized eigenvector matrix of P. That is, the ith column of V, v_q $(1\le q\le N)$ corresponds to the qth eigenvector. Obviously, any two eigenvectors are orthonormal because P is a real symmetric matrix. Then we can obtain R^{α} as:

$$R^{\alpha}=VD^{\alpha}V^{T} \tag{3}$$

where, D^{α} is a diagonal matrix defined as:

$$D^{\alpha} = \mathrm{diag}[1,\exp(-i\frac{2\pi\alpha}{t}),\dots\exp(-i\frac{2(N-1)\pi\alpha}{t})] \tag{4}$$

where, t denotes the periodicity of DFRNT.

Obviously, DFRNT is a random transform due to the randomness of R^{α}. In other words, a different P (i.e., Q) corresponds to a different R^{α} and further different DFRNT. Specifically, when $\alpha = kt/2$ (k is a constant integer), the output of DFRNT is also real for a real signal (Liu *et al*., 2005). For simplicity, we set $t = 1$, $k = 1$ and $\alpha = 0.5$ in our context.

In Liu *et al*. (2008) scheme the original image X is encrypted via DFRNT first and then the DFRNT coefficient matrix Y can be obtained according to Eq. 1. Next, r-1 random nonsingular matrices K_1, K_2, $\dots K_{r-1}$ are generated. Finally, n shadows are produced as:

$$\begin{aligned}
S_1 &= w_{1,1}K_1 + w_{1,2}K_2 + \dots + w_{1,r-1}K_{r-1} + w_{1,r}Y \\
S_2 &= w_{2,1}K_1 + w_{2,2}K_2 + \dots + w_{2,r-1}K_{r-1} + w_{2,r}Y \\
&\dots \\
S_n &= w_{n,1}K_1 + w_{n,2}K_2 + \dots + w_{n,r-1}K_{r-1} + w_{n,r}Y
\end{aligned} \tag{5}$$

where, $w_{i,j}$ $(1\le i\le n,\ 1\le j\le r)$ is the weighting factor chosen in advance. In decryption, assume r shadows are collected, a linear equation set can be constructed with r shadows and the associated weighting factors are known, while K_1, K_2, $\dots$, K_{r-1} and Y are unknown. Thus the task of recovering the DFRNT coefficient matrix Y is reduced to solving this equation set. At last, the inverse DFRNT is performed on Y and thus the secret image X is reconstructed.

PROPOSED SCHEME

Motivation: In Liu *et al*.'s scheme, the random matrices K_1, K_2, $\dots$, K_{r-1} produced in encryption are no longer required during decryption. This is one of the key advantages in their scheme. However, this principle leads to the each shadow S_i $(1\le i\le n)$ is equal sized as the input secret image Y, i.e., X. In addition, only one secret Y is encrypted in Eq. 5. After carefully examined the strategies of Liu *et al*.'s scheme, we find that besides Y, actually the other r-1 coefficients K_1, K_2, $\dots$, K_{r-1} are also decrypted along with the secret image. Motivated by this, we can also exploit K_1, K_2, $\dots$, K_{r-1} to carry some secret image information instead of meaningless random matrices. In this way, Liu *et al*.'s scheme can be improved in two cases. One is the shadow size can be reduced and the other is multiple secret images instead of one can be encrypted every time.

Reducing shadow size: In the shadow size reduction improvement, the input content is a single image. Suppose the input secret image I is a gray-level image with the size of W×H pixels, the encryption and decryption procedures are described below.

Encryption stage: The encryption stage is described as follows:

Step 1: Permute the secret image I into X with a pseudo-random sequence. This operation aims to decorrelate the secret image pixels in spatial domain. Although our method's security is guaranteed by the randomness of DFRNT as explained in the later context, this step is still necessary to scramble the input image so that the finally shadows seem as random noise.

Step 2: Partition the permuted image X into r equal sized segments X_1, X_2, $\dots$, X_r, i.e., 1/r size of X. Suppose each of X_1, X_2, $\dots$, X_r is of the size $W_s\times H_s$ pixels.

Step 3: Generate a random matrix Q according to a secret key k_Q and obtain R_s^{α} as that in Liu *et al*.'s scheme. The difference between Liu *et al*.'s and our scheme lies in our transform matrix is prepared for the segments of input image, not for the input image in Liu *et al*.'s scheme. In particular, firstly generate a random real nonsingular matrix Q of the size $W_s\times H_s$. Secondly, the matrix P is obtained according to Eq. 2. Obviously, P and Q are of the same size. Thirdly, a $W_s\times H_s$ transform matrix R_s^{α} of DFRNT is produced according to Eq. 3 and 4.

Step 4: Perform the DFRNT transform on $X_1, X_2, \ldots, X_r$ respectively according to Eq. 6 and the corresponding $Y_1, Y_2, \ldots, Y_r$ are obtained.

$$Y_j=R_s^{\alpha}X_j(R_s^{\alpha})^T \tag{6}$$

where, $1 \le j \le r$.

Step 5: Generate n shadows $S_1, S_2, \ldots, S_n$ as:

$$\begin{aligned}
S_1 &= w_{1,1}Y_1 + w_{1,2}Y_2 + \ldots + w_{1,r-1}Y_{r-1} + w_{1,r}Y_r \\
S_2 &= w_{2,1}Y_1 + w_{2,2}Y_2 + \ldots + w_{2,r-1}Y_{r-1} + w_{2,r}Y_r \\
&\ldots \\
S_n &= w_{n,1}Y_1 + w_{n,2}Y_2 + \ldots + w_{n,r-1}Y_{r-1} + w_{n,r}Y_r
\end{aligned} \tag{7}$$

where, $w_{i,j}$ ($1 \le i \le n$, $1 \le j \le r$) is the element of a constant weight matrix given in advance. Note this constant weight matrix must not be a singular matrix. In this way, n shadows are produced with each being $W_s \times H_s$ pixels, i.e., 1/r size of the input secret image.

Decryption stage: The decryption stage is described below:

Step 1: Suppose r different shadows $S'_1, S'_2, \ldots, S'_r$ are collected for decryption. Construct a linear equation set as:

$$\begin{aligned}
S'_1 &= w'_{1,1}Y_1 + w'_{1,2}Y_2 + \ldots + w'_{1,r-1}Y_{r-1} + w'_{1,r}Y_r \\
S'_2 &= w'_{2,1}Y_1 + w'_{2,2}Y_2 + \ldots + w'_{2,r-1}Y_{r-1} + w'_{2,r}Y_r \\
&\ldots \\
S'_r &= w'_{r,1}Y_1 + w'_{r,2}Y_2 + \ldots + w'_{r,r-1}Y_{r-1} + w'_{r,r}Y_r
\end{aligned} \tag{8}$$

where, $S'_1, S'_2, \ldots, S'_r$ are r different shadows collected from $S_1, S_2, \ldots, S_n$ and $w'_{i,j}$ are the associated weighting factors retrieved from the weight matrix. Thereby, $Y_1, Y_2, \ldots, Y_r$ can be obtained by solving this linear equation set. If more than r shadows are collected, these coefficient matrices also can be decrypted similarly from any r shadows randomly selected among them.

Step 2: Generate a random matrix Q according to a same key k_Q, further obtain the R_s^{α} as Eq. 3 and 4.

Step 3: Perform the inverse DFRNT transform on $Y_1, Y_2, \ldots, Y_r$ as Eq. 9 and thus the corresponding secret image segments $X_1, X_2, \ldots, X_r$ are recovered.

$$X_j=(R_s^{\alpha})^{-1}Y_j((R_s^{\alpha})^T)^{-1} \tag{9}$$

where, $1 \le j \le r$ and the superscript -1 denotes the inverse matrix.

Step 4: Obtain the permuted secret image X by rearranging $X_1, X_2, \ldots, X_r$.

Step 5: Perform the inverse permutation on X with the same pseudo-random sequence and thus the original secret image I is reconstructed.

Multiple secret images sharing: In the multiple secret images sharing improvement, the input content is composed by a set of equal sized secret images $I_1, I_2, \ldots, I_r$. Each of the secret images can be any type of content. Suppose each of them is a gray-level image with the size of W×H pixels, the encryption and decryption procedures are described below.

Encryption stage: The encryption stage is described as follows:

Step 1: Permute the secret images $I_1, I_2, \ldots, I_r$ into $X_1, X_2, \ldots, X_r$ with a pseudo-random sequence. This operation is for neighboring pixels decorrelation.

Step 2: Generate a random matrix Q according to a secret key k_Q and obtain R_m^{α}. That is, firstly generate a random real nonsingular matrix Q of the size W×H. Secondly, the matrix P is obtained according to Eq. 2. Obviously, P and Q are of the same size. Thirdly, a W×H transform matrix R_m^{α} of DFRNT is produced according to Eq. 3 and 4.

Step 3: Perform the DFRNT transform on $X_1, X_2, \ldots, X_r$ respectively according to Eq. 10 and the corresponding $Y_1, Y_2, \ldots, Y_r$ are obtained.

$$Y_j=R_m^{\alpha}X_j(R_m^{\alpha})^T \tag{10}$$

where, $1 \le j \le r$.

Step 4: Generate n shadows $S_1, S_2, \ldots, S_n$ as Eq. 7. Hence, n shadows are produced with each being W×H pixels.

Decryption stage: The decryption stage is described below:

Step 1: Suppose r different shadows $S'_1, S'_2, \ldots, S'_r$ are collected for decryption. Construct a linear equation set as Eq. 8. $S'_1, S'_2, \ldots, S'_r$ are r different shadows collected from $S_1, S_2, \ldots, S_n$. Thereby, $Y_1, Y_2, \ldots, Y_r$ can be obtained by solving this linear equation set. If more than r shadows are collected, these coefficient matrices also can be decrypted similarly from any r shadows randomly selected among them.

Step 2: Generate a random matrix Q according to a same key k_Q, further obtain the R_m^α as Eq. 3 and 4.

Step 3: Perform the inverse DFRNT transform on $Y_1, Y_2, \ldots, Y_r$ as Eq. 11 and thus the corresponding secret image segments $X_1, X_2, \ldots, X_r$ are recovered:

$$X_j=(R_m^\alpha)^{-1}Y_j((R_m^\alpha)^T)^{-1} \quad (11)$$

where, $1 \le j \le r$ and the superscript -1 denotes the inverse matrix.

Step 4: Perform the inverse permutation on $X_1, X_2, \ldots, X_r$ with the same pseudo-random sequence and thus the original secret image $I_1, I_2, \ldots, I_r$ is reconstructed.

RESULTS

Four 512×512 gray-level images, Lena, Boat, Barbara and F16 as shown in Fig. 1 are selected as test images to evaluate the performance of our scheme. In our experiments, both Q and W are uniformly distributed random nonsingular matrices. First, the shadow size reduction performance of our scheme is validated. The Lena image is chosen as the secret image and shared with a (4, 6)-threshold model (Fig. 2a-m). It is permuted before encryption as shown in Fig. 2b and partitioned into four equal sized segments. Then each segment is encrypted with DFRNT and thus four corresponding encrypted segments are produced, as shown in Fig. 2d-g. Next, these encrypted segments are shared in 6 shadows as shown in Fig. 2h-m.

Fig. 1: 512×512 test secret images, Lena, Boat, Barbara and F16 (from left to right)

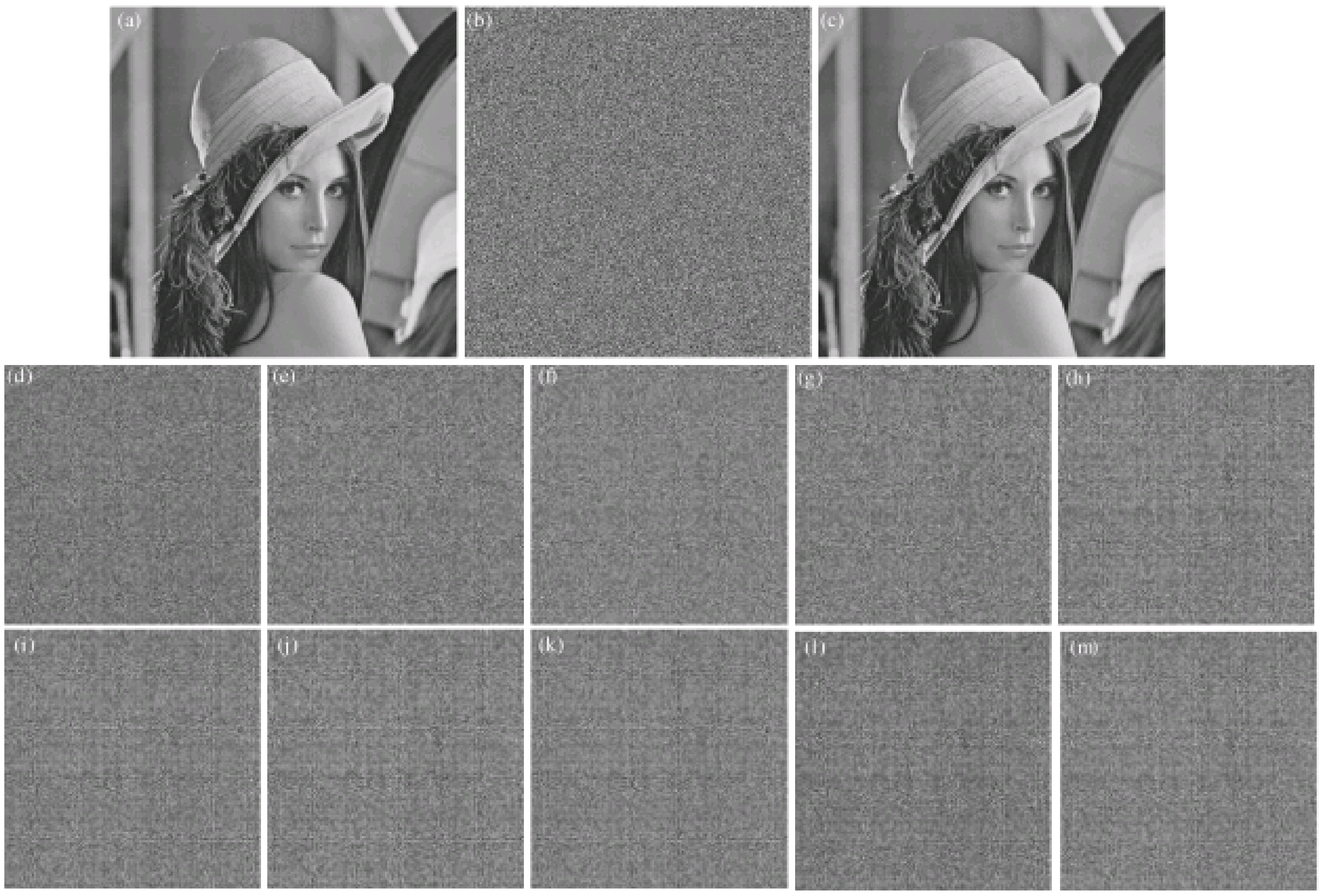

Fig. 2: Sharing Lena image with a (4, 6)-threshold model, (a) the original secret image, (b) the permuted secret image, (c) the reconstructed image, (d-g) the DFRNT coefficients of four segments and (h-m) six shadows S_1-S_6

In decryption, suppose four shadows S_1, S_3, S_4, S_6 shown in Fig. 2h, j, k, m are collected and then four DFRNT coefficient matrices are obtained by solving a simultaneous equation set constructed by these four shadows. Next, the inverse DFRNT transform is performed on these DFRNT coefficients matrices and thereby the corresponding X_1, X_2, X_3 and X_4 are recovered. Then X_1, X_2, X_3 and X_4 are rearranged into the permuted secret image X. At last, X is inversely permuted to the secret Lena image. If the shadows are accurately stored and transmitted, the reconstructed Lena as shown in Fig. 2c is exactly the same as the original one.

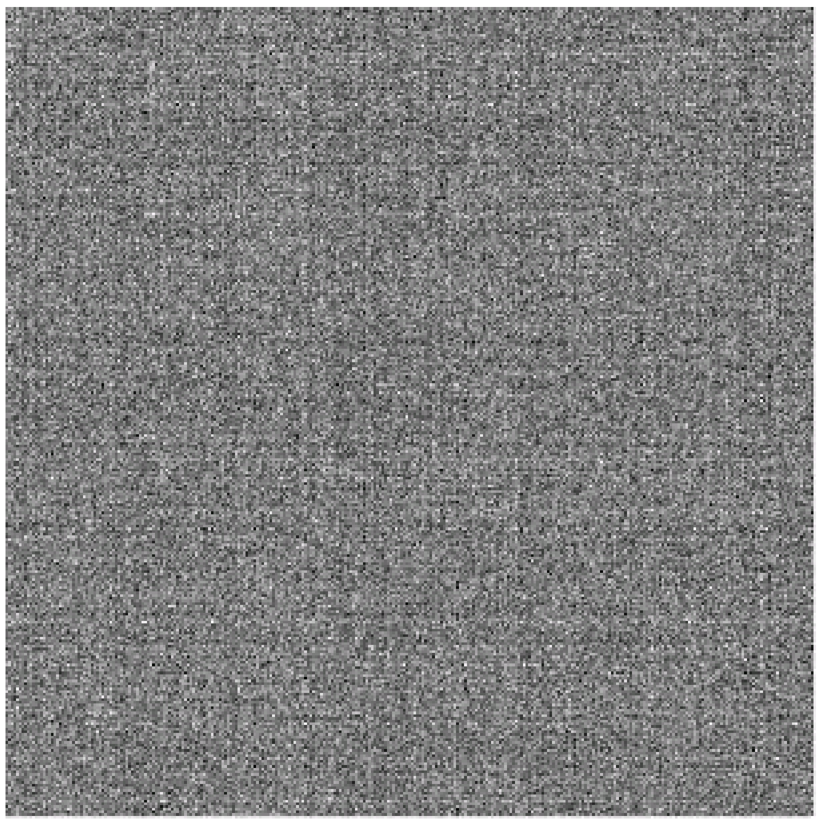

Fig. 3: The reconstructed secret image with a wrong R^α

To test the security of our scheme, we also apply another R_s^α to decrypt the secret Lena. Actually, this R_s^α is different from that used in Fig. 2 because it is generated by another random Q matrix. From the results shown in Fig. 3, there is no meaningful content revealed. This demonstrates that the security of our scheme is still guaranteed due to the DFRNT's sensitivity of R_s^α. In practice, the weight matrix also can be used as an extra key if necessary.

Second, the multi-image secret sharing ability of our scheme is tested. This is also achieved by employing the usage of random matrices produced in encryption. Suppose the Boat, Barbara and F16 images are shared together with a (3, 5)-threshold model. We only need to permute and encrypt them respectively. In this way, three corresponding DFRNT coefficient matrices are produced and further five 512×512 shadows are generated according to Eq. 7. The secret decryption is the inverse process of encryption and each original image is reconstructed individually. The encryption and decryption strategies are shown in Fig. 4 and 5, respectively.

It is necessary to note that, besides gray-level image, our scheme is also suitable for color image secret sharing. Given a color image, we only need to decompose it into red, green and blue channels and encrypt each channel as a gray-level image.

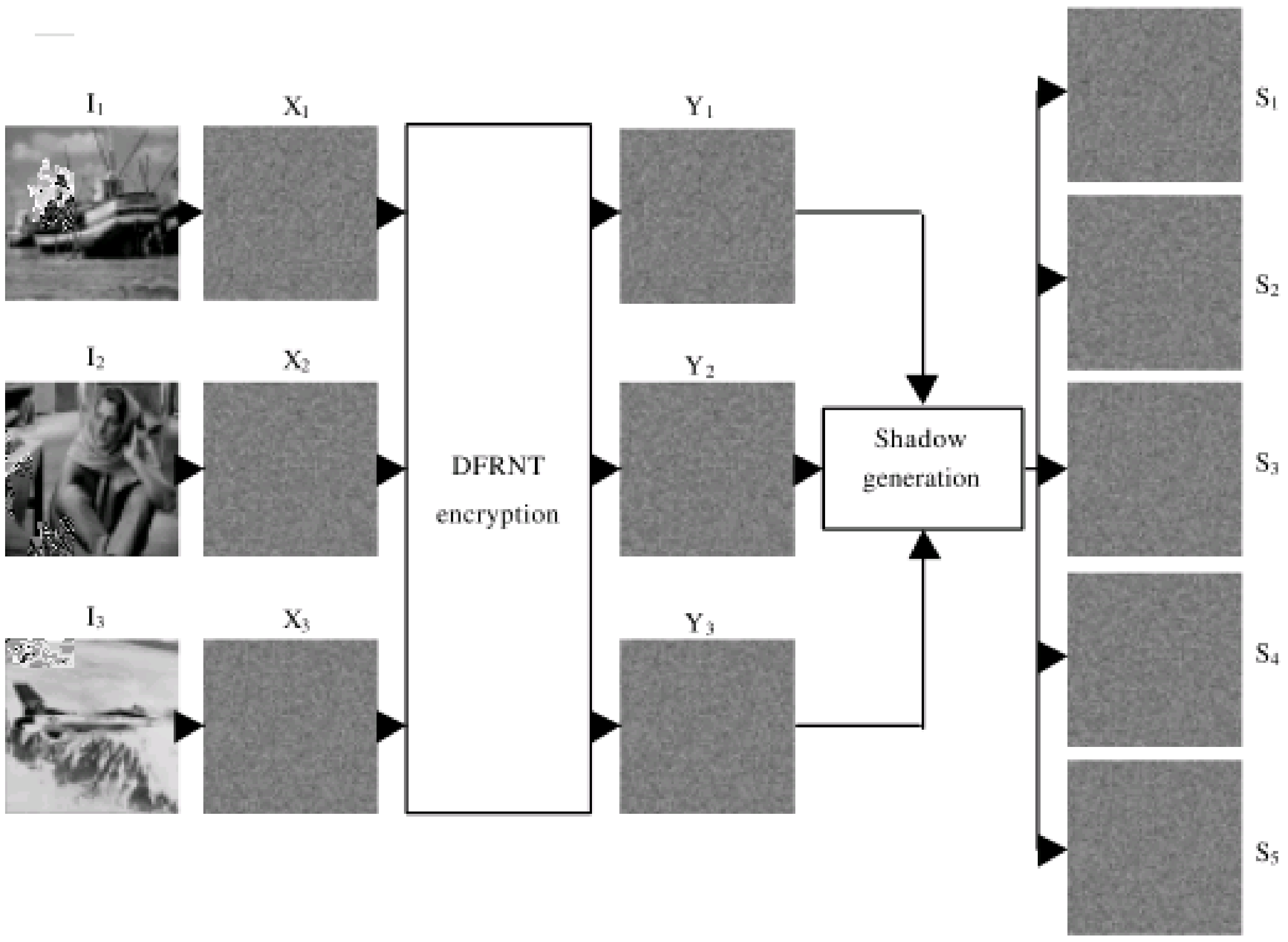

Fig. 4: Encryption strategy of multi-image secret sharing based on DFRNT

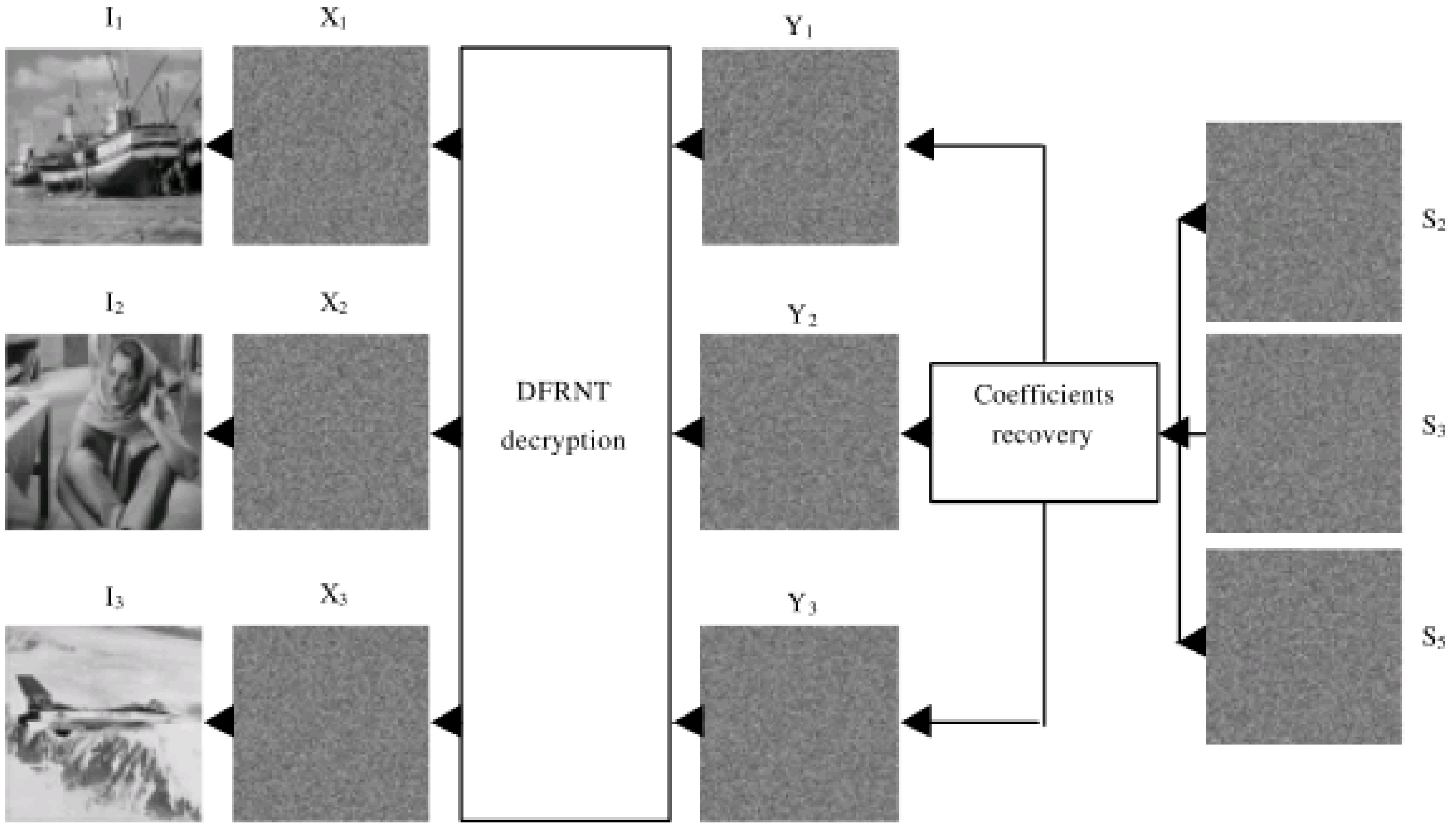

Fig. 5: Decryption strategy of multi-image secret sharing based on DFRNT

DISCUSSION

According to the experimental results, we can find that the difference between our scheme and the existing methods lies in the following two aspects. (1) The security of our scheme is guaranteed by several keys. One is the kernel transform of DFRNT, i.e., the matrix Q. The other is the permutation key used for scrambling the input images. This is different from the available image secret sharing schemes for usually only one key is preserved in decryption. In other words, our scheme can be maintain a higher security when both keys are required in decryption. (2) Our scheme maintains the two-layer abilities. One is for shadow size reduction to 1/r and the other is for multiple image secret sharing. Both of them are easily realized with DFRNT. In contrast, most image secret sharing schemes proposed in literatures are designed for only one purpose. That is, in one case, a single image is shared for small shadows; in the other case, multiple images are input for encryption at the same time. In a word, our scheme is a novel prototype for both application scenarios.

CONCLUSION

An improved (r, n)-threshold image secret sharing scheme based on DFRNT is proposed in this paper. To share one secret image, the size of each shadow is reduced to 1/r size of the original image and thus much storage space and transmission time is saved. In addition, our scheme can be naturally extended to a (r, n)-threshold multi-image secret sharing prototype. It allows parallel secret sharing and reconstruction. That is, r secret images can be shared in n shadows at a time and decrypted simultaneously. Perfect security is preserved in our scheme due to the randomness of DFRNT.

REFERENCES

Feng, J.B., H.C. Wu, C.S. Tsai and Y.P. Chu, 2005. A new multi-secret images sharing scheme using Largranges interpolation. J. Syst. Software, 76: 327-339.

Lin, C.C. and W.H. Tsai, 2003. Secret image sharing with capability of share data reduction. Opt. Eng., 42: 2340-2345.

Liu, Z., H. Zhao and S. Liu, 2005. A discrete fractional random transform. Optics Commun., 255: 357-365.

Liu, Z., S. Liu and M.A. Ahmad, 2008. Image sharing scheme based on discrete fractional random transform. Opt. Int. J. Light Electron. Opt., 10.1016/j.ijleo.2008.07.029

Shamir, A., 1979. How to share a secret. Commun. ACM, 22: 612-613.

Thien, C.C. and J.C. Lin, 2002. Secret image sharing. Comput. Graphics, 26: 765-770.

Tsai, C.S., C.C. Chang and T.S. Chen, 2002. Sharing multiple secrets in digital images. J. Syst. Software, 64: 163-170.

Wang, R.Z. and C.H. Su, 2006. Secret image sharing with smaller shadow images. Pattern Recognition Lett., 27: 551-555.

Wu, Y.S., C.C. Thien and J.C. Lin, 2004. Sharing and hiding secret images with size constraint. Pattern Recognition, 37: 1377-1385.

Wu, H.C. and C.C. Chang, 2005. Sharing visual multi-secrets using circle shares, Comput. Standards Interfaces, 28: 123-135.

Yang, C.C., T.Y. Chang and M.S. Hwang, 2004. A (t, n) multi-secret sharing scheme. Applied Mathematics Comp., 151: 483-490.

Yang, C.N. and T.S. Chen, 2005. Aspect ratio invariant visual secret sharing schemes with minimum pixel expansion. Pattern Recognition Lett., 26: 193-206.

Yang, C.N. and T.S. Chen, 2006. Reduce shadow size in aspect ratio invariant visual secret sharing schemes using a square block-wise operation. Pattern Recognition, 39: 1300-1314.