Image Encryption Using Discrete Parametric Cosine Transform

Yicong Zhou, *Member, IEEE*, Karen Panetta, *Fellow, IEEE*, and Sos Agaian, *Senior Member, IEEE*

***Abstract*—This paper introduces a new effective image encryption algorithm using the Discrete Parametric Cosine Transform (DPCT). The new algorithm transforms images into the frequency domain using the DPCT with a set of parameters, and then converts images back into the spatial domain using the inverse DPCT with a different set of parameters to obtain the encrypted images. Its security keys are the combination of the parameters of the DPCT and inverse DPCT. The simulation results show that the algorithm can fully or partially encrypt different types of digital images with efficiency while preserving the quality of the images. The algorithm can be used to protect different types of multimedia data. It can be also used for simultaneous data encryption and compression by embedding it in a data compression process such as JPEG.**

***Index Terms*—Image Encryption, Discrete Parametric Cosine Transform**

I. Introduction

NETWORKS and communication technologies provide a large number of opportunities for people all over the world to transmit, share and download images and videos. These images and videos may contain vast quantities of private information. Visual surveillance systems and networks make remote video monitoring available for homeland security purposes in many important areas such as airports, commercial centers, banks, and also military strategic positions. These applications can generate large amounts of video and image content and need to be transmitted and stored securely. Security of multimedia data is also very important in many other areas such as covert communications and medical imaging applications. Image encryption is a ubiquitous and effective method to protect multimedia data by transforming it into an unrecognizable format such that the protected objects are difficult to decode by an unauthorized user.

Several encryption methods have been developed to encrypt images and videos in recent years. The encryption schemes based on the principles of cryptography are designed to ensure the confidentiality of multimedia data [1-3]. Such solutions may not be suitable for real-time secure applications since their encryption processes require vast resources including computing complexity, time and power.

The Discrete Cosine Transform (DCT) possesses a good energy compaction property and is widely used in image coding and compression, feature extraction, filtering, and image encryption. The DCT based encryption schemes have been developed to protect multimedia data in the frequency domain by encrypting the DCT coefficients/blocks [1, 2], the quantization table [3, 4], or Huffman table [5, 6]. These encryption schemes have a significantly lower computational cost, meeting the critical requirements of the encryption speed for multimedia contents in real-time applications such as mobile computing and server-end computing [7]. Since the DCT based encryption methods are usually combined with the data compression process, they may not be suitable for applications requiring high quality data.

Several algorithms for multimedia encryption have been developed by using different parametric discrete transforms. Examples include the discrete fractional Fourier Transform [8-10] and fractional wavelet transform [11, 12]. These algorithms encrypt multimedia by modifying the transform parameters such that the multimedia data will be changed during their encryption process.

In this paper, we apply a Discrete Parametric Cosine Transform (DPCT) for image encryption. This encryption process is independent of any data compression process. The new encryption algorithm is straightforward and effective. The principles behind the presented solution may be applied to a variety of systems including image, audio, and video systems.

The rest of this paper is organized as follows. Section II will present the definition of the DPCT and its properties. Section III will introduce the new DPCT-based image encryption algorithm. Experimental results will be shown in section IV. Security analysis for the presented algorithm will be discussed in section V and Section VI will discuss the conclusion.

II. Discrete Parametric Cosine Transform

In this section, we review the Discrete Parametric Cosine Transform (DPCT) and its properties. Then, we extend this concept and introduce the 2D Discrete Parametric Cosine

Yicong Zhou and Karen Panetta are with Department of Electrical and Computer Engineering, Tufts University, Medford, MA 02155 USA (YZ phone:1-617-627-5183; fax:1-617-627-3220; e-mail: yzhou0a@ece.tufts.edu; KP e-mail: karen@ece.tufts.edu).

Sos Agaian is with Department of Electrical and Computer Engineering, University of Texas at San Antonio, San Antonio, TX 78249, USA (e-mail: Sos.Agaian@utsa.edu).

Transform (2D DPCT).

A. DPCT

Let the sequence $(x_0, x_1, ..., x_{N-1})$ be mapped to $(X_0, X_1, ..., x_{N-1})$ by the following transformation [13].

$$X_k = \sum_{n=0}^{N-1} \mu_{n,k} x_n \cos\left[\frac{\pi}{M}\alpha_0\left(n+\alpha_1\right)\left(k+\alpha_2\right)\right] \quad (1)$$

where $0 \le n,k \le N-1$ and coefficients $(N, M, \alpha_0, \alpha_1, \alpha_2, \mu_{n,k})$ are parameters. This transformation is called the Discrete Parametric Cosine Transform (DPCT).

Based on the definition in equation (1), the DPCT changes with the different combinations of the parameters $(N, M, \alpha_0, \alpha_1, \alpha_2, \mu_{n,k})$. For example,

1) If $M = N, \alpha_0 = 1, \alpha_1 = \alpha_2 = 0, \mu_{n,k} = \mu_n \mu_k$ and $\mu_p = \begin{cases} 1/\sqrt{2} & p = 0 \\ 1 & 0 < p \le N-1 \end{cases}$, then DPCT becomes the DCT-I,

$$X_k = \sqrt{\frac{2}{N}} \sum_{n=1}^{N-1} \mu_n \mu_k x_n \cos\left[\frac{\pi k}{N}\left(n+\frac{1}{2}\right)\right] \quad (2)$$

2) If $M = N, \alpha_0 = 1, \alpha_1 = \frac{1}{2}, \alpha_2 = 0$ and $\mu_{n,k} = \begin{cases} 1/\sqrt{N} & k = 0 \\ \sqrt{2/N} & 0 < k \le N-1 \end{cases}$, the DPCT is the DCT-II, i.e.

$$X_k = \mu_{n,k} \sum_{n=1}^{N-1} x_n \cos\left[\frac{\pi k}{N}\left(n+\frac{1}{2}\right)\right] \quad (3)$$

3) If $M = N, \alpha_0 = 1, \alpha_1 = 0, \alpha_2 = \frac{1}{2}$ and $\mu_{n,k} = \sqrt{2/N}$, the DPCT is the DCT-III, namely,

$$X_k = \sqrt{\frac{2}{N}} \sum_{n=0}^{N-1} x_n \cos\left[\frac{\pi n}{N}\left(k+\frac{1}{2}\right)\right] \quad (4)$$

4) If $M = N, \alpha_0 = 1, \alpha_1 = \frac{1}{2}, \alpha_2 = \frac{1}{2}$ and $\mu_{n,k} = 2/\sqrt{N}$, the DPCT changes to the DCT-IV, i.e.

$$X_k = \sqrt{\frac{2}{N}} \sum_{n=1}^{N-1} x_n \cos\left[\frac{\pi}{N}\left(n+\frac{1}{2}\right)\left(k+\frac{1}{2}\right)\right] \quad (5)$$

B. 2D DPCT

Based on the 2D DCT, The DPCT can be extended to the 2D DPCT which is defined by,

$$X_{k_1,k_2} = \sum_{n_1=0}^{N_1-1} \sum_{n_2=0}^{N_2-1} \mu_{n_1,k_1} \mu_{n_2,k_2} x_{n_1,n_2} \cos\left[\frac{\pi}{M_1}\alpha_{10}\left(n_1+\alpha_{11}\right)\left(k_1+\alpha_{12}\right)\right] \times \cos\left[\frac{\pi}{M_2}\alpha_{20}\left(n_2+\alpha_{21}\right)\left(k_2+\alpha_{22}\right)\right] \quad (6)$$

From the definition in equation (6), there are 12 parameters in the 2D DPCT, i.e. $P = (N_1, M_1, \mu_{n_1,k_1}, \alpha_{10}, \alpha_{11}, \alpha_{12}, N_2, M_2, \mu_{n_2,k_2}, \alpha_{20}, \alpha_{21}, \alpha_{22})$. The 2D DPCT will be different when these parameters change. For example, the 2D DCT is a special case of the 2D DPCT. If $M_1 = N_1 = M_2 = N_2 = N, \alpha_{10} = \alpha_{20} = 1$, and $\alpha_{11} = \alpha_{21} = \frac{1}{2}, \alpha_{12} = \alpha_{22} = 0$, $\mu_{n_1,k_1} = \mu_{k_1}, \mu_{n_2,k_2} = \mu_{k_2}$, the 2D DPCT becomes the 2D DCT,

$$X_{k_1,k_2} = \sum_{n_1=0}^{N-1} \sum_{n_2=0}^{N-1} \mu_{k_1} \mu_{k_2} x_{n_1,n_2} \cos\left[\frac{\pi k_1}{N}\left(n_1+\frac{1}{2}\right)\right] \cos\left[\frac{\pi k_2}{N}\left(n_2+\frac{1}{2}\right)\right] \quad (7)$$

where

$$\mu_k = \begin{cases} 1/\sqrt{N} & k = 0 \\ \sqrt{2/N} & 0 < k \le N-1 \end{cases}$$

The 2D DPCT is a complex cosine transform that requires 12 parameters and is challenging to design in real world applications. However, these parameters make the 2D DPCT more powerful and provide robust characteristics. The 2D DPCT also offers the users design flexibility in achieving design requirements of real world applications.

Similar to the inverse 2D DCT, the inverse 2D DPCT can be given by,

$$x_{n_1,n_2} = \sum_{k_1=0}^{N_1-1} \sum_{k_2=0}^{N_2-1} \mu_{n_1,k_1} \mu_{n_2,k_2} X_{k_1,k_2} \cos\left[\frac{\pi}{M_1}\alpha_{10}\left(n_1+\alpha_{11}\right)\left(k_1+\alpha_{12}\right)\right] \times \cos\left[\frac{\pi}{M_2}\alpha_{20}\left(n_2+\alpha_{21}\right)\left(k_2+\alpha_{22}\right)\right] \quad (8)$$

III. New Image Encryption Algorithm

In this section, we introduce a new image encryption algorithm using the new 2D DPCT.

The new algorithm transforms the original images into the frequency domain using the new 2D DPCT with $P = (N_1, M_1, \mu_{n_1,k_1}, \alpha_{10}, \alpha_{11}, \alpha_{12}, N_2, M_2, \mu_{n_2,k_2}, \alpha_{20}, \alpha_{21}, \alpha_{22})$. It then uses an inverse 2D DPCT with different parameters $P' = (N_1', M_1', \mu_{n_1,k_1}', \alpha_{10}', \alpha_{11}', \alpha_{12}', N_2', M_2', \mu_{n_2,k_2}', \alpha_{20}', \alpha_{21}', \alpha_{22}')$ to convert the images back into the spatial domain to obtain the encrypted images. The encryption algorithm is shown in Fig.1.

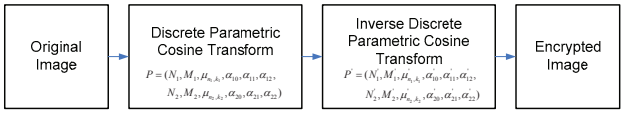

Fig. 1. Block diagram of the image encryption algorithm

The presented new encryption algorithm is a simple and straightforward process. Its inverse process for recovering the original images is the image decryption algorithm depicted in Fig.2. The algorithm converts the encrypted image into the frequency domain using the 2D DPCT with parameters $P' = (N_1', M_1', \mu_{n_1,k_1}', \alpha_{10}', \alpha_{11}', \alpha_{12}', N_2', M_2', \mu_{n_2,k_2}', \alpha_{20}', \alpha_{21}', \alpha_{22}')$. The original image is reconstructed by using the 2D inverse DPCT with $P = (N_1, M_1, \mu_{n_1,k_1}, \alpha_{10}, \alpha_{11}, \alpha_{12}, N_2, M_2, \mu_{n_2,k_2}, \alpha_{20}, \alpha_{21}, \alpha_{22})$ to transfer the image back into the spatial domain.

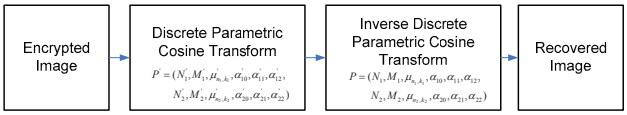

Fig. 2. Block diagram of the image decryption algorithm

The presented algorithm can also be used to encrypt other

types of images such as 2D and 3D medical images and color images. Color images or 3D medical images usually contain several 2D components. For example, color images have three color planes and 3D medical images consist of a number of slice images. Thus, the presented algorithm can encrypt all their 2D components individually and then combine the encrypted results to obtain the encrypted 3D medical images or encrypted color images.

IV. Experimental Results

This section provides several encryption results of grayscale, medical and color images in order to show the performance of the presented algorithm for image encryption. In all examples in this section, the 2D DPCT and inverse 2D DPCT are specified as different types of the traditional 2D DCT as described in the subsection A in Section II. This takes advantage of the fact that these types of DCTs have inverse transforms that are easy to generate and implement.

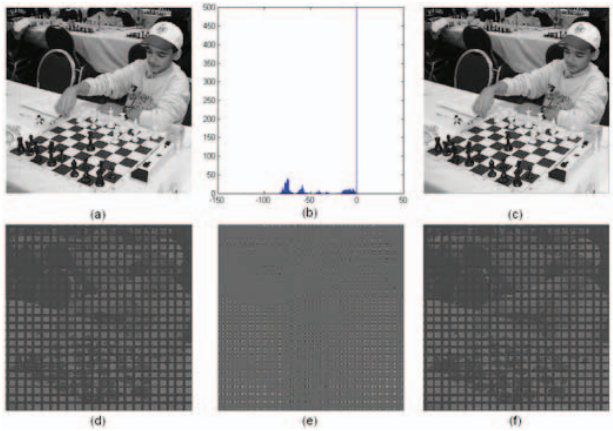

Fig.3. Grayscale image Encryption using the same type of DPCT transforms with different window sizes. (a) Original image; (b) Histogram of the difference between the reconstructed and original images; (c) Reconstructed image; (d) the DPCT result of the original image; (e) Encrypted image; (f) The reconstructed DPCT result.

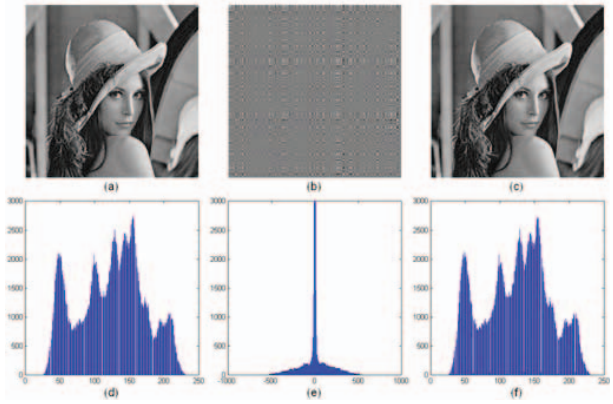

Fig.4. Grayscale image Encryption using the different types of DPCT transforms with different window sizes. (a) Original image; (b) Encrypted image; (c) Reconstructed image; (d) Histogram of the original image; (e) Histogram of the encrypted image; (f) Histogram of the reconstructed image.

An example of the grayscale image encryption is shown in Fig. 3. The original image is converted into the frequency domain by specifying the 2D DPCT as the 2D DCT-II with a window size of 3×3. The DCT result of the original image is shown in Fig. 3(d). The encrypted image (Fig.3(e)) is obtained by transforming the DCT result in Fig. 3(d) back into the spatial domain using the inverse 2D DCT-II with a window size of 7×7. It is completely indiscernible from the original image.

To reconstruct the original image, the encrypted image is applied the 2D DCT-II with a window size of 7×7. The result is shown in Fig. 3(f). The reconstructed image (Fig. 3(c)) is obtained by using an inverse 2D DCT-II with a window size of 3×3. It is visually the same as the original image in Fig. 3(a). However, the reconstructed image is slightly different compared to the original image based on the difference histogram (Fig. 3(b)) between the reconstructed image and the original image. This is because the 2D DCT-II converts image data into the floating format while the original images are integer, for example, the pixel values of a grayscale image are integer gray levels from 0 to 255.

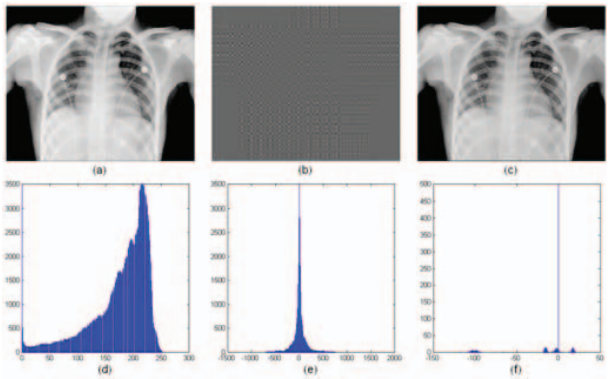

Fig.5. Medical image Encryption using the same type of DPCT transforms with different window sizes. (a) Original image; (b) Encrypted image; (c) Reconstructed image; (d) Histogram of the original image; (e) Histogram of the encrypted image; (f) Histogram of the difference between the reconstructed and original images.

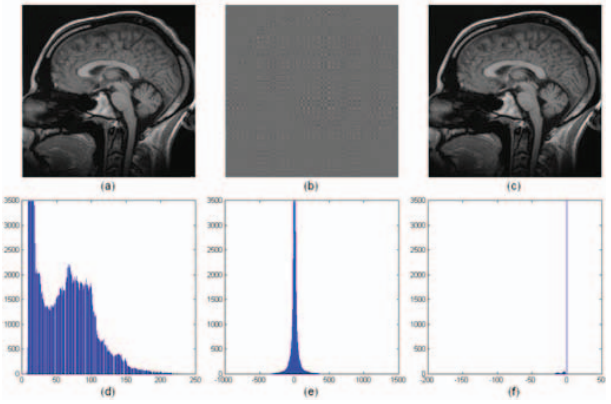

Fig.6. Medical image Encryption using different types of DPCT transforms with different window sizes. (a) Original image; (b) Encrypted image; (c) Reconstructed image; (d) Histogram of the original image; (e) Histogram of the encrypted image; (f) Histogram of the difference between the reconstructed and original images.

Fig. 4 shows another example of grayscale image encryption using different types of DPCTs and window sizes. The original image in Fig. 4(a) is encrypted by a 2D DCT-III with a window size of 3×3 and an inverse 2D DCT-IV with a window size of 5×5. The reconstructed image and its histogram look identical to those of the original image.

Fig. 5 gives an example of medical image encryption. In this case, the encryption process uses the same type of the DPCT but different window size. 2D DCT-II with a window size of 3×3 and inverse 2D DCT-II with a window size of 10×10 are chosen in this example.

Fig. 6 provides another example of the medical image encrypted by different types of the DPCT and different window sizes. The encryption process uses the 2D DCT-II with a window size of 7×7 and the inverse 2D DCT-IV with a window size of 5×5.

All these examples of 2D image encryption show that the encrypted images result in totally different images from the original images and that the original images are fully encrypted.

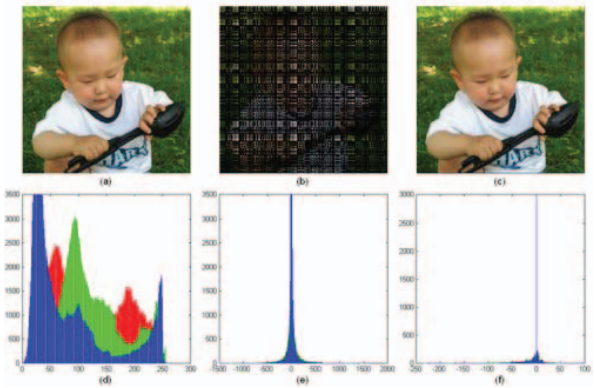

Fig.7. Color image Encryption using the same parameters for each color planes. (a) Original image; (b) Encrypted image; (c) Reconstructed image; (d) Histogram of the original image; (e) Histogram of the encrypted image; (f) Histogram of the difference between the reconstructed and original images.

Fig. 7 provides an example of color image encryption. All its 2D components are encrypted by using the same parameters. The encryption process uses the 2D DCT-II with a window size of 4×4 and then the inverse 2D DCT-II with a window size of 11×11. The original image is partially encrypted. The reconstructed color image is slightly different with the original one. This can be verified by the difference histogram in Fig. 7(f).

V. Security Analysis

This section discusses the security issues of the presented algorithm such as the security key space and attacks.

A. Security Key Space

The security keys of the presented algorithm consist of the parameters $P=(N_1, M_1, \mu_{n_1,k_1}, \alpha_{10}, \alpha_{11}, \alpha_{12}, N_2, M_2, \mu_{n_2,k_2}, \alpha_{20}, \alpha_{21}, \alpha_{22})$ for 2D DPCT and $P'=(N_1', M_1', \mu_{n_1,k_1}', \alpha_{10}', \alpha_{11}', \alpha_{12}', N_2', M_2', \mu_{n_2,k_2}', \alpha_{20}', \alpha_{21}', \alpha_{22}')$ for inverse 2D DPCT in encryption process. Therefore, there are 24 security keys for the presented algorithm. Theoretically, each parameter has unlimited possible values. However, each 2D DPCT should have an inverse matrix to reconstruct the original images in the decryption process. This means that the 2D DPCT has to be an invertible/nonsingular square matrix, namely, $N_1=M_1=N_2=M_2$ and $N_1'=M_1'=N_2'=M_2'$. After applying these conditions, 16 security keys still remain. These security keys are extremely important for the presented algorithm. The results in Fig. 8 show that the original image can be reconstructed only if the correct security keys are being utilized.

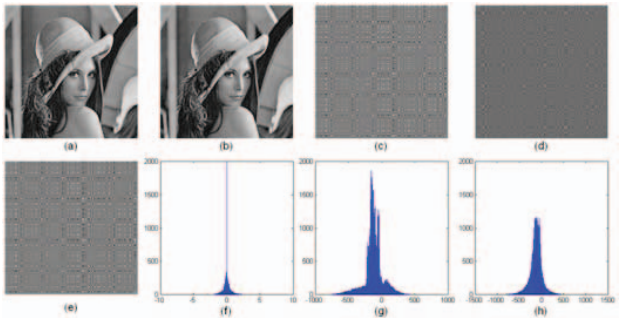

Fig.8. Image reconstruction using different security keys. (a) Original image; (b) Reconstructed image, 2D DCT-II with 5×5 and inverse 2D DCT-II with 8×8; (c) Reconstructed image, 2D DCT-II with 8×8 and inverse 2D DCT-II with 8×8; (d) Reconstructed image, 2D DCT-III with 8×8 and inverse 2D DCT-III with 5×5; (e) Encrypted image, 2D DCT-II with 8×8 and inverse 2D DCT-II with 5×5; (f) Histogram of the difference between (a) and (b); (g) Histogram of the difference between (a) and (c); (h) Histogram of the difference between (a) and (d).

There are a very large number of possible choices for each parameter. Thus, the security key space of the presented algorithm is quite large. The algorithm can withstand the brute force attack in which an attacker tries to guess the security keys of the algorithm by exclusively searching its key space.

B. Plaintext Attacks

In the cryptography, the plaintext is the original information to be encrypted. The ciphertext is the encrypted plaintext by an encryption algorithm. The chosen-plaintext attack is an attack model in which the attacker can choose a number of plaintexts and then determine their corresponding ciphertexts. In this attack, the attacker can choose any useful information as the plaintext in order to deduce the security keys of encryption algorithms, or reconstruct the original plaintexts from the unknown ciphertexts [14]. Thus, it is an advanced attack model. In general, an algorithm can withstand other plaintext attacks if it can overcome the chosen-plaintext attack.

The presented algorithm changes the image data during the entire encryption process by applying the 2D DPCT and the inverse 2D DPCT to the images. All histograms of the encrypted images in the Section IV show that the pixel values of the encrypted image are completely different from the original images. Thus, the data of the encrypted images are not useful for the plaintext attacks. This ensures that the

presented algorithm can withstand the plaintext attacks.

VI. Conclusion

We have introduced a new effective algorithm for image encryption. The new algorithm is based on the discrete parametric cosine transform. The encryption process is a straightforward data transformation from the spatial domain to the frequency domain and then back into the spatial domain. The process is controlled by different parameters of the DPCT. The idea behind the algorithm is to encrypt an image by changing the image data using the DPCT with different parameters.

Experimental results have demonstrated that the presented algorithm can fully or partially protect the 2D and 3D images. The original images can be reconstructed with well-pleasing quality despite the existence of very small errors between the reconstructed images and the original images due to floating operations that occur during the data transformation by the 2D DPCT and the inverse 2D DPCT.

There are more than 16 security keys in the presented algorithm. All of them have a large number of possible values. This makes it difficult for unauthorized users to decode the images. The presented algorithm can withstand the brute force attack and plaintext attacks. The original images can be protected with a high level of security and reconstructed only when the correct security keys have been applied.

The new algorithm can be combined with an image compression process like JPEG, such that the images can be simultaneously encrypted and compressed. This makes the algorithm suitable for real-time applications.

References

[1] **T. Li, et al., "A new scrambling method based on semi-frequency domain and chaotic system," in *Neural Networks and Brain, 2005. ICNN&B '05. International Conference on*, 2005, pp. 607-610.**

[2] **S. Lian, J. Sun, and Z. Wang, "A novel image encryption scheme based-on JPEG encoding," in *Information Visualisation, 2004. IV 2004. Proceedings. Eighth International Conference on*, 2004, pp. 217-220.**

[3] **T.-S. Chen, C.-C. Chang, and M.-S. Hwang, "A virtual image cryptosystem based upon vector quantization," *Image Processing, IEEE Transactions on,* vol. 7, pp. 1485-1488, 1998.**

[4] **S. Sudharsanan, "Shared key encryption of JPEG color images," *Consumer Electronics, IEEE Transactions on,* vol. 51, pp. 1204-1211, 2005.**

[5] **J. M. Rodrigues, W. Puech, and A. G. Bors, "Selective Encryption of Human Skin in JPEG Images," in *Image Processing, 2006 IEEE International Conference on*, 2006, pp. 1981-1984.**

[6] **J. Zhou, et al., "Security Analysis of Multimedia Encryption Schemes Based on Multiple Huffman Table," *Signal Processing Letters, IEEE,* vol. 14, pp. 201-204, 2007.**

[7] **C.-P. Wu and C. C. J. Kuo, "Design of integrated multimedia compression and encryption systems," *Multimedia, IEEE Transactions on,* vol. 7, pp. 828-839, 2005.**

[8] **S.-C. Pei and W.-L. Hsue, "The multiple-parameter discrete fractional Fourier transform," *Signal Processing Letters, IEEE,* vol. 13, pp. 329-332, 2006.**

[9] **W. Jin and C. Yan, "Optical image encryption based on multichannel fractional Fourier transform and double random phase encoding technique," *Optik - International Journal for Light and Electron Optics,* vol. 118, pp. 38-41, 2007.**

[10] **Z. Liu and S. Liu, "Double image encryption based on iterative fractional Fourier transform," *Optics Communications,* vol. 275, pp. 324-329, 2007.**

[11] **L. Chen and D. Zhao, "Optical image encryption based on fractional wavelet transform," *Optics Communications,* vol. 254, pp. 361-367, 2005.**

[12] **Y.-H. Seo, H.-J. Choi, and D.-W. Kim, "Digital hologram encryption using discrete wavelet packet transform," *Optics Communications,* vol. 282, pp. 367-377, 2009.**

[13] **K. O. Egiazarian, S. S. Agaian, and J. T. Astola, "Parametric family of discrete trigonometric transforms," in *Image and Video Processing IV*, San Jose, CA, USA, 1996, pp. 42-53.**

[14] **A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone *Handbook of Applied Cryptography*. New York: CRC Press, Inc., 1997.**