Image Double Encryption Based on Parametric Discrete Cosine Transform

Han Cao, Yicong Zhou*, C. L. Philip Chen
Department of Computer and Information Science, University of Macau
Macau 999078, China
* yicongzhou@umac.mo

***Abstract*—This paper introduces a new image encryption algorithm based on the parametric discrete cosine transform (PDCT). It combines the PDCT with the phase encoding technique to form a double-level encryption and provides high security protection to images with a low computation cost. Simulations and analysis are provided to show the excellent encryption performance of the proposed algorithm in protecting different types of images.**

***Index Terms*—Parametric discrete cosine transform, image encryption, phase encoding, double encryption**

I. Introduction

With rapid development of networks and communications, more and more private and sensitive images spread on the Internet. Security of these images attract more concerns of people and researchers. Image encryption is a tool of protecting images by transforming them into noise-like formats. The fundamental challenges in image encryption are often derived from three factors [1]: 1) image files are of large volumes; 2) image pixels generally have strong correlations; 3) image encryption is required for real-time processing. Therefore, traditional encryption methods i.e. the public-key encryption method, advanced encryption standard (AES) and international data encryption algorithm (IDEA), are not suitable for image encryption due to the high computational complexity [1, 2].

To encrypt images efficiently with an acceptable level of security, many image encryption techniques have been proposed [3–7]. Encryption algorithms have been developed based on the discrete cosine transform (DCT) due to the wide use of DCT. They first transfer images into the frequency domain using the DCT, and encrypt images by utilizing different technologies to change the DCT coefficient matrices [3, 5], quantization tables [7] and Huffman tables [8]. The encryption performance and security of the DCT based algorithms are dependent only on these used technologies.

Several image encryption methods are based on parametric discrete transforms such as the fractional Fourier transform [9], parametric cosine transform [4] and randomized orthogonal transform [6]. They encrypt images by controlling the parameters of these discrete transforms.

All these methods can protect images with a high level of security. Security keys are extremely important for authorized users because the original images can be completely recovered only when the correct security keys are being utilized. Otherwise, the incorrectly decrypted images are generally noise-like and unrecognizable.

However, this phenomenon provides a new direction for image encryption, namely, using one set of security keys to encrypt the original image and a different set of security keys for the decryption process to generate the final encrypted image. Theoretically, this encryption scheme has a large key space but requires double processes (encryption and decryption) to encrypt images. Correspondingly, it may require a high computation cost.

Using this new concept while avoiding this side effect, this paper proposes a new image encryption algorithm using the parametric DCT (PDCT) and phase encoding technique. The proposed algorithm first encrypts the original images by transforming them into the frequency domain using the PDCT with one set of parameters, applies phase encoding and scrambling to encrypt the PDCT coefficients, and utilizes the inverse PDCT (IPDCT) with a different set of parameters to transfer the images back into the spatial domain, obtaining the final encrypted images. The proposed algorithm uses these double-level encryption processes to protect images with a high level of security while maintaining the computation cost similar to existing frequency-domain-based encryption methods. Experimental results and analysis will be given.

The rest of this paper is organized as follows. Section II reviews the PDCT. In Section III, the proposed algorithm is presented in detail. Section IV shows the simulation results on different types of images. In Section V, the security analysis is demonstrated. Section VI concludes this paper.

II. Parametric Discrete Cosine Transformation

The parametric discrete cosine transformation (PDCT) is a generalization of the traditional DCT, in which a different set of parameters results in a different type of DCT. The expression of PDCT is described as [4]

$$Y_k = \sum_{n=0}^{N-1} \mu_{n,k} y_n \cos\left(\frac{\pi}{M} a_0 (n + a_1)(k + a_2)\right) \qquad (1)$$

where n, k are integers, $0 \leq n, k \leq (N-1)$ and $\{M, a_0, a_1, a_2, \mu_{n,k}\}$ are parameters. By applying this transformation to an input sequence $(y_0, y_1, y_2, \ldots, y_{N-1})$, its frequency coefficients $(Y_0, Y_1, Y_2, \ldots, Y_{N-1})$ will be obtained. Using different combinations of parameters, Equation (1) can generate a set of different DCTs. Especially, by selecting certain values of $\{M, a_0, a_1, a_2, \mu_{n,k}\}$, 8 traditional DCTs (i.e. DCT-I, DCT-II, ..., DCT-VIII) can be generated from the PDCT.

978-1-4799-2827-9/13/$31.00 ©2013 IEEE

By extending the PDCT concept into the two dimension (2D) version, the 2D PDCT is defined here,

$$Y_{k_1,k_2} = \sum_{n_1=0}^{N_1-1}\sum_{n_2=0}^{N_1-1} \mu_{n_1,k_1}\mu_{n_2,k_2}y_{n_1,n_2} \cos\left(\frac{\pi}{M_1}a_{10}(n_1+a_{11})(k_1+a_{12})\right) \cos\left(\frac{\pi}{M_2}a_{20}(n_2+a_{21})(k_2+a_{22})\right) \quad (2)$$

where $\{M_1, a_{10}, a_{11}, a_{12}, \mu_{n_1,k_1}, M_2, a_{20}, a_{21}, a_{22}, \mu_{n_2,k_2}\}$ are parameters of the 2D PDCT. With 10 parameters, the 2D PDCT becomes a powerful tool for the 2D data (i.e. image) processing.

III. Image Double Encryption Algorithm

Here, we propose a new concept of image encryption. It encrypts an original image using one set of security keys and then follows a decryption process with a different set of security keys to obtain the encrypted image. This concept, however, may have a high computation cost because it needs two processes to generate the encrypted images. Using this concept while minimizing the computation cost, this section introduces a new PDCT based image double encryption algorithm, called the PDCT-IDEA.

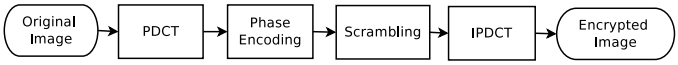


Fig. 1. Block diagram of the proposed algorithm.

The proposed PDCT-IDEA is shown in Fig. 1. The original image is transformed into the frequency domain by the PDCT with parameters: $\{M_1, a_{10}, a_{11}, a_{12}, \mu_{n_1,k_1}, M_2, a_{20}, a_{21}, a_{22}, \mu_{n_2,k_2}\}$. The algorithm changes values of the PDCT coefficients using a phase encoding process, changes their locations using a scrambling process, and then uses an IPDCT with parameters $\{M_1^{'}, a_{10}^{'}, a_{11}^{'}, a_{12}^{'}, \mu_{n_1,k_1}^{'}, M_2^{'}, a_{20}^{'}, a_{21}^{'}, a_{22}^{'}, \mu_{n_2,k_2}^{'}\}$ to transfer them back into the spatial domain, obtaining the encrypted image.

When the PDCT and IPDCT use different sets of parameters, based on the new concept, they are considered as the image encryption and decryption processes, respectively. The proposed PDCT-IDEA provides a double-level encryption to images. The first-level encryption is performed by the PDCT and IPDCT while the second-level encryption consists of the phase encoding and scrambling processes.

Notice that, when the PDCT and IPDCT use the same set of parameters, they have functions similar to the traditional DCT and IDCT. Due to the fact that the DCT and IDCT are mandatory processes for the DCT-based image processing, the PDCT and IPDCT perform image encryption without additional computation costs.

With specific parameter settings, the PDCT and IPDCT can revert back to the DCT and IDCT. Thus, the proposed PDCT-IDEA becomes a DCT-based encryption method. It contains only the phase encoding and scrambling processes which act as the substitution and permutation roles, respectively. The phase encoding processing is defined by,

$$d(u,v) = g(u,v)\ cos\left(2\pi\ p(u,v)\right) \quad (3)$$

where $g(u,v)$ is the PDCT coefficient matrix of the original image with size of $W \times L$; $d(u,v)$ is the resulting coefficient matrix; $p(u,v)$ is a random matrix with the data range of $[0,1]$ and the same size of $g(u,v)$. Note that $p(u,v)$ is considered as a random phase to $g(u,v)$.

$p(u,v)$ is generated from the logistic map which can be expressed here,

$$x_{n+1} = rx_n(1-x_n) \quad (4)$$

where x_0 and r ($r \in [3.57, 4]$) are the initial value and parameter, respectively.

To compute $p(u,v)$, we first use $\{x_{01}, r_1\}$ to generate a 1D sequence S_1 with length of WL, and covert it into $p(u,v)$ using Equation (5),

$$p(u,v) = 2^{32}S_1((u-1)L+v) - \lfloor 2^{32}S_1((u-1)L+v)\rfloor \quad (5)$$

where $\lfloor\cdot\rfloor$ is a floor operator which maps the input value into its largest previous integer.

After phase encoding, scrambling is designed to change the coefficient locations within the matrix $d(u,v)$ and break the coefficient correlations. In this paper, scrambling is implemented using the logistic map with the initial parameter settings $\{x_{02}, r_2\}$. The scrambled coefficient matrix $h(u,v)$ is obtained according to the following Algorithm 1,

Algorithm 1 The Scrambling Algorithm

Input: The coefficient matrix $d(u,v)$ with size of WL and parameters $\{x_{02}, r_2\}$
1: Generate S_2 using Equation (4) with parameters $\{x_{02}, r_2\}$
2: Obtain Q from S_2: $Q(i) \leftarrow round((2^{32}S_2(i) - \lfloor 2^{32}S_2(i)\rfloor)WL)$
3: Convert $d(u,v)$ to a 1D matrix D: $D((u-1)L+v) \leftarrow d(u,v)$
4: **for** $i = 1$ to WL **do**
5: Swapping the values of $D(i)$ and $D(Q(i))$
6: **end for**
7: Convert D to a 2D matrix $h(u,v)$ with size of WL: $h(u,v) \leftarrow D((u-1)L+v)$
Output: The scrambled coefficient matrix $h(u,v)$

For image decryption, when the authorized users utilize the correct security keys and follow the inverse steps of the PDCT-IDEA in Fig. 1, the original image can be completely reconstructed.

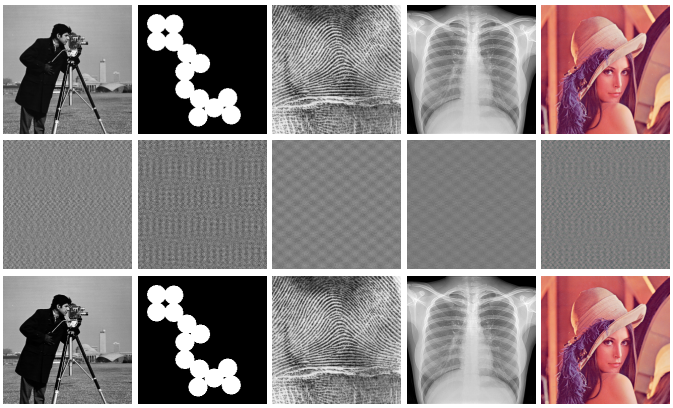
The security keys of the PDCT-IDEA consist of four portions: (1) the PDCT parameters $\{M_1, a_{10}, a_{11}, a_{12}, \mu_{n_1,k_1}, M_2, a_{20}, a_{21}, a_{22}, \mu_{n_2,k_2}\}$; (2) parameters for phase coding $\{x_{01}, r_1\ \}$; (3) parameters for the scrambling process $\{x_{02}, r_2\}$; and (4) the IPDCT parameters $\{M_1^{'}, a_{10}^{'}, a_{11}^{'}, a_{12}^{'}, \mu_{n_1,k_1}^{'}, M_2^{'}, a_{20}^{'}, a_{21}^{'}, a_{22}^{'}, \mu_{n_2,k_2}^{'}\}$. Thus, there are 24 parameters in total. Each parameter has a large number of possible choices. The PDCT-IDEA can withstand the brute-force attack.

In summary, the proposed PDCT-IDEA is based on a new concept of image encryption, and protects different types of images using a double-level encryption. It has a similar computation cost to most existing frequency-domain-based encryption algorithms. The original images is protected with a high level of security.

IV. Simulation Results

This section provides several simulation results using the PDCT-IDEA to encrypt different types of images such as grayscale, binary, medical, biometric and color images. For

simplicity, in the rest of this paper, we follow the same parameter settings unless specified. The PDCT and IPDCT use a set of predefined keys $\{M_1 = W, a_{10} = 1, a_{11} = 0, a_{12} = 0.5, \mu_{n_1,k_1} = \begin{cases} \sqrt{2/W} & (n \neq 0) \\ \sqrt{1/W} & (n = 0) \end{cases}, M_2 = L, a_{20} = 1, a_{21} = 0, a_{22} = 0.5, \mu_{n_2,k_2} = \begin{cases} \sqrt{2/L} & (n \neq 0) \\ \sqrt{1/L} & (n = 0) \end{cases}\}$ and $\{M_1 = W, a_{10} = 1, a_{11} = 0.5, a_{12} = 0.5, \mu_{n_1,k_1} = \sqrt{2/W}, M_2 = L, a_{20} = 1, a_{21} = 0.5, a_{22} = 0.5, \mu_{n_2,k_2} = \sqrt{2/L}\}$. We set parameters of the logistic map $\{x_{01} = 0.25, r_1 = 3.9\}$ to generate random phase matrix for phasing encoding, and $\{x_{02} = 0.27, r_2 = 3.8\}$ for the scrambling process.



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

Fig. 2. The PDCT-IDEA encryption results of different types of images. The top, middle and bottom rows show the original, encrypted and reconstructed images; (a) grayscale image; (b) binary image; (c) biometric image; (d) medical image; (e) color image.

Fig. 2 shows the experimental results on the grayscale, binary, biometric, medical and color images. It is clear to see that all encrypted images are texture-like and unrecognizable (see images in the middle row), and that the original images are completely recovered (i.e. images in the bottom row) when the correct security keys are being utilized.

V. Security Analysis

In this section, the security analysis will be performed, including key space, key sensitivity, differential and correlation analysis.

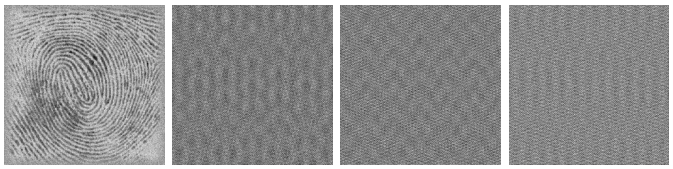
A. Security Key Space

As mentioned in Section III, the security keys of the PDCT-IDEA contain 24 parameters which are rational numbers. $\{x_{01}, r_1\}$ and $\{x_{02}, r_2\}$ are parameters of the logistic map. The data ranges of x_{01}, x_{02} and r_1, r_2 are $(0, 1)$ and $[3.57, 4]$, respectively. Each of them has a large number of possible choices. For 20 parameters in the PDCT and IPDCT, although there are limited number of the qualified combinations of the PDCT parameters to ensure that the PDCT is invertible, total possible choices of these 20 parameters are still sufficiently large. For example, suppose there are only 10 possible choices for each parameter, the PDCT-IDEA's key space is 10^{24}. Thus, the PDCT-IDEA has an extremely large key space and is able to withstand the brute-force attack.

B. Key Sensitivity Analysis

For an excellent encryption algorithm, the encryption and decryption procedures should be highly sensitive to the security key changes. Here, we perform the key sensitivity tests in both the encryption and decryption procedures.

1) Key Sensitivity in Image Encryption: $x_{01}$is one of two keys in the phase encoding stage. We choose it for the key sensitivity test in the image encryption procedure. The results are shown in Fig. 3. First, the original image in Fig. 3(a) is encrypted using two groups of security keys. The only difference between two key groups is that x_{01} is 0.3 in one group but 0.4 in the other group. The corresponding encrypted images are shown in Figs. 3(b) and (c). Their pixel-to-pixel difference is shown in Fig. 3(d).

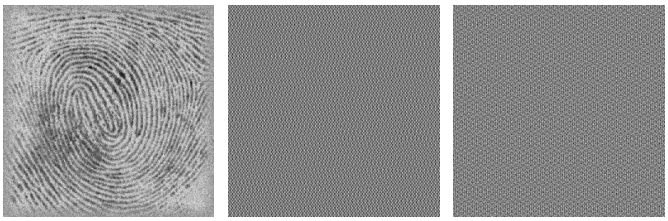


(a) (b) (c) (d)

Fig. 3. Key sensitivity test for image encryption with a small change applied to x_{01}; (a) original image; (b) encrypted image, $x_{01} = 0.3$; (c) encrypted image, $x_{01} = 0.4$; (d) the difference between (b) and (c).

As can be seen, the encrypted results of the PDCT-IDEA are totally different (see Fig. 3(d)) when x_{01} has a small change. This demonstrates that a small change in the security keys will lead to completely different encrypted images.

2) Key Sensitivity in Image Decryption: In this test, x_{02}, r_2 in scrambling stage are chosen. First, $\{x_{02} = 0.5, r_2 = 3.9\}$ are used to encrypt a fingerprint image in the encryption procedure. Then, we use {0.5, 3.9}, {0.5, 3.8} and {0.4, 3.9} as different settings of $\{x_{02}, r_2\}$ for image decryption. The decrypted images are shown in Fig. 4. As shown in Fig. 4(a), the original image can be completely reconstructed only when the correct security keys are being utilized. Otherwise, even a slight change in the security keys will result in different, texture-like and unrecognized decrypted images such as Figs. 4(b) and (c).



(a) (b) (c)

Fig. 4. Key sensitivity test for image decryption; Images are decrypted with (a) the correct keys: $x_{02} = 0.5, r_2 = 3.9$; (b) a small change in r_2: $r_2 = 3.8$; (c) a small change in x_{02}: $x_{02} = 0.4$, respectively.

Based on the key sensitivity tests in both the encryption and decryption procedures, the PDCT-IDEA has high sensitivity to the security key changes.

C. Correlation Coefficients Analysis

In this analysis, we use the medical image in Fig. 2(d) as an example to show the image correlation changes before and after applying the PDCT-IDEA. In the horizontal, vertical and diagonal directions, 5000 pairs of adjacent pixels are chosen randomly both in the original image (the image in the first

row of Fig. 2(d)) and its encrypted image (the image in the second row of Fig. 2(d)). The correlation diagrams in each direction are shown in Fig. 5. As can be seen, pixels in the original image have high correlations in each direction because the values of adjacent pixels are equal or much close. However adjacent pixel values in the encrypted image in all directions distribute dramatically in a large dynamic range.

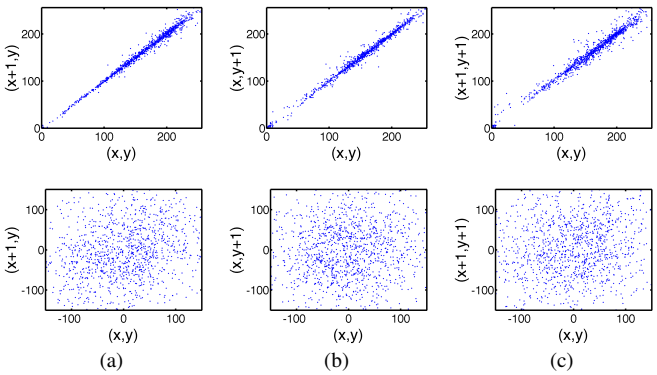


Fig. 5. Adjacent pixel correlations within the image before and after applying the PDCT-IDEA. The top and bottom rows plot correction diagrams of the original and encrypted images in the (a) horizontal (b) vertical and (c) diagonal directions, respectively.

D. Differential Analysis

To demonstrate the PDCT-IDEA's performance in against of the differential attack, we show the experimental results of the sensitivity test on changes in the original image.

In this experiment, changing one pixel in the original image at the location (200, 200) to 0, we obtain two images (Figs. 6(a) and (b)). They are then encrypted by the PDCT-IDEA with the same set of security keys. The encryption results are shown in Figs. 6(d) and (e). Their pixel-to-pixel difference is shown in Fig. 6(f). It is clear to see that one pixel change in the original image leads to completely different encrypted images. This demonstrates that the PDCT-IDEA is extremely sensitive to the change of the original image and can resist the differential attack.

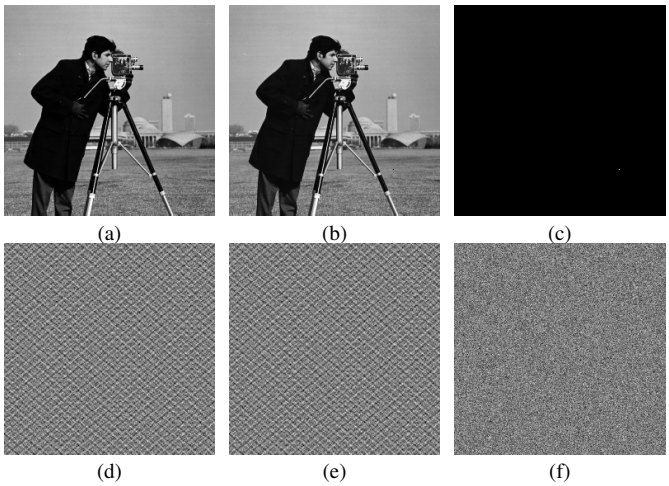


Fig. 6. Differential Analysis; (a) The original image; (b) The image generated from (a) after one pixel change in the original image at location (200, 200); (c) Difference between (a) and (b); (d) Encrypted image of (a); (e) Encrypted image of (b); (f) Difference between (d) and (e).

VI. Conclusion

In this paper, the PDCT based double encryption algorithm has been proposed for protecting different types of images. In the proposed algorithm, the PDCT and IPDCT are combined with the phase encoding technique to form a double encryption algorithm. The PDCT and IPDCT for image encryption here follow the new concept of using the encryption and decryption processes to encrypt the images while avoiding the high computation cost. The phase encoding and scrambling are applied to enhance the encryption effect of the PDCT and IPDCT. Simulation and analysis results have shown that the PDCT-IDEA is able to protect different types of images with a high level of security.

Acknowledgment

This work was supported in part by the Macau Science and Technology Development Fund under grant 017/2012/A1 and by the Research Committee at University of Macau under grants MYRG113(Y1-L3)-FST12-ZYC and MRG001/ZYC/2013/FST

References

[1] S. Liu, J. Sun, and Z. Xu, "An improved image encryption algorithm based on chaotic system," *Journal of Computers*, vol. 4, no. 11, pp. 1091–1100, Nov. 2009.

[2] M. Yang, "Data-image-video-encryption," *IEEE Potentials*, pp. 28–34, 2004.

[3] Z. Liu, L. Xu, T. Liu, H. Chen, P. Li, L. Chuang, L. Shutian, C. Lin, and S. Liu, "Color image encryption by using arnold transform and color-blend operation in discrete cosine transform domains," *Optics Communications*, vol. 284, no. 1, pp. 123–128, Jan. 2011.

[4] Y. Zhou, K. Panetta, and S. Agaian, "Image encryption using discrete parametric cosine transform," in *2009 Conference Record of the Forty-Third Asilomar Conference on Image Processing*, 2009, pp. 395–399.

[5] E. Wharton, K. Panetta, and S. Agaian, "Simultaneous encryption / compression of images using alpha rooting," in *Data Compression Conference*, 2008.

[6] Y. Wu, "Randomization of discrete orthogonal transforms and encryption," in *Hadamard Transforms*, 2012, ch. 14, pp. 617–627.

[7] S. Sudharsanan, "Shared key encryption of JPEG color images," *IEEE Transactions on Consumer Electronics*, vol. 51, no. 4, pp. 1204–1211, 2005.

[8] J. Zhou, Z. Liang, Y. Chen, and O. C. Au, "Security analysis of multimedia encryption schemes based on multiple huffman table," *IEEE Signal Processing Letters*, vol. 14, no. 3, pp. 201–204, 2007.

[9] Z. Liu, J. Dai, X. Sun, and S. Liu, "Triple image encryption scheme in fractional Fourier transform domains," *Optics Communications*, vol. 282, no. 4, pp. 518–522, Feb. 2009.