EFFICIENT DISCRETE FRACTIONAL HIRSCHMAN OPTIMAL TRANSFORM AND ITS APPLICATION

Wen-Liang Hsue[1]*, Soo-Chang Pei*[2]*, and Jian-Jiun Ding*[2]

[1]Department of Electrical Engineering, Chung Yuan Christian University, Taiwan

[2]Department of Electrical Engineering, National Taiwan University, Taipei, Taiwan

Email addresses: wlhsue@cycu.edu.tw, pei@cc.ee.ntu.edu.tw, djj@cc.ee.ntu.edu.tw

Outline

I. Introduction

II. The Hirschman Optimal Transform (HOT)

III. Properties of the HOT

IV. Proposed Efficient Discrete Fractional HOT Transform

V. Application and Experiment Results

VI. Conclusions

VII. References

I. Introduction (1/3)

- Discrete fractional Fourier transform (DFRFT):
  - Discrete version of continuous FRT
  - Generalization of DFT with one fractional parameter
- Many existing discrete fractional signal transforms:
  - Multiple-parameter DFRFT, Random DFRFT
  - Fractional DCT
  - Fractional DST
  - etc
- All existing 1-D N-point discrete fractional transforms require $O(N^2)$ computation complexity.

I. Introduction (2/3)

- We will propose a new discrete fractional signal transform with $O(N^{1.5})$ computations.
- The new transform is a fractional version of Hirschman optimal transform (HOT).
- HOT transform:
  - a DFT-based transform [12]-[13]
  - was used to reduce computations for convolution [14]

I. Introduction (3/3)

- Fractional HOT transform will be extended to have linear $O(N)$ computation complexity.
- We apply the new efficient transform to encrypt digital images.

II. The Hirschman Optimal Transform (HOT) (1/5)

- HOT transform (by DeBrunner *et al.* in 2000):
  - A DFT-based signal transform
  - More efficient than the DFT
- *Defintion* (Kronecker product): Let **A** and **B** be $M\times N$ and $R\times S$.

$$\mathbf{A}\otimes\mathbf{B}=\begin{bmatrix} a_{11}\cdot\mathbf{B} & a_{12}\cdot\mathbf{B} & \cdots & a_{1N}\cdot\mathbf{B} \\ a_{21}\cdot\mathbf{B} & a_{22}\cdot\mathbf{B} & \cdots & a_{2N}\cdot\mathbf{B} \\ \vdots & \vdots & \ddots & \vdots \\ a_{M1}\cdot\mathbf{B} & a_{M2}\cdot\mathbf{B} & \cdots & a_{MN}\cdot\mathbf{B} \end{bmatrix}_{(M\cdot R)\times(N\cdot S)}$$

- A property: $(\mathbf{A}\otimes\mathbf{B})(\mathbf{C}\otimes\mathbf{D})=(\mathbf{AC})\otimes(\mathbf{BD})$

II. The Hirschman Optimal Transform (HOT) (2/5)

- The $K \times K$ DFT matrix is

$$[\mathbf{F}]_{m,n} = \frac{1}{\sqrt{K}} e^{-j\frac{2\pi}{K}mn}, \quad 0 \le m, n \le K-1$$

- *Defintion:* $K^2 \times K^2$ discrete HOT transform matrix is

$$\mathbf{H}_{K^2} = \mathbf{F}_K \otimes \mathbf{I}_K$$

where $\mathbf{F}_K$: $K \times K$ DFT matrix

$\mathbf{I}_K$: $K \times K$ identity matrix

II. The Hirschman Optimal Transform (HOT) (3/5)

- A 9-point HOT example:

$$\begin{bmatrix} H(0) \\ H(1) \\ H(2) \\ H(3) \\ H(4) \\ H(5) \\ H(6) \\ H(7) \\ H(8) \end{bmatrix} = \frac{1}{\sqrt{3}} \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & e^{-j\frac{2\pi}{3}} & 0 & 0 & e^{-j\frac{4\pi}{3}} & 0 & 0 \\ 0 & 1 & 0 & 0 & e^{-j\frac{2\pi}{3}} & 0 & 0 & e^{-j\frac{4\pi}{3}} & 0 \\ 0 & 0 & 1 & 0 & 0 & e^{-j\frac{2\pi}{3}} & 0 & 0 & e^{-j\frac{4\pi}{3}} \\ 1 & 0 & 0 & e^{-j\frac{4\pi}{3}} & 0 & 0 & e^{-j\frac{8\pi}{3}} & 0 & 0 \\ 0 & 1 & 0 & 0 & e^{-j\frac{4\pi}{3}} & 0 & 0 & e^{-j\frac{8\pi}{3}} & 0 \\ 0 & 0 & 1 & 0 & 0 & e^{-j\frac{4\pi}{3}} & 0 & 0 & e^{-j\frac{8\pi}{3}} \end{bmatrix} \begin{bmatrix} x(0) \\ x(1) \\ x(2) \\ x(3) \\ x(4) \\ x(5) \\ x(6) \\ x(7) \\ x(8) \end{bmatrix}$$

- It is interesting that (shown next page)

  9-point HOT transform ≡ 3 separate 3-point DFTs

II. The Hirschman Optimal Transform (HOT) (4/5)

$$\begin{bmatrix} H(0) \\ H(3) \\ H(6) \end{bmatrix} = \frac{1}{\sqrt{3}} \begin{bmatrix} 1 & 1 & 1 \\ 1 & e^{-j\frac{2\pi}{3}} & e^{-j\frac{4\pi}{3}} \\ 1 & e^{-j\frac{4\pi}{3}} & e^{-j\frac{8\pi}{3}} \end{bmatrix} \begin{bmatrix} x(0) \\ x(3) \\ x(6) \end{bmatrix}$$

$$\begin{bmatrix} H(1) \\ H(4) \\ H(7) \end{bmatrix} = \frac{1}{\sqrt{3}} \begin{bmatrix} 1 & 1 & 1 \\ 1 & e^{-j\frac{2\pi}{3}} & e^{-j\frac{4\pi}{3}} \\ 1 & e^{-j\frac{4\pi}{3}} & e^{-j\frac{8\pi}{3}} \end{bmatrix} \begin{bmatrix} x(1) \\ x(4) \\ x(7) \end{bmatrix}$$

$$\begin{bmatrix} H(2) \\ H(5) \\ H(8) \end{bmatrix} = \frac{1}{\sqrt{3}} \begin{bmatrix} 1 & 1 & 1 \\ 1 & e^{-j\frac{2\pi}{3}} & e^{-j\frac{4\pi}{3}} \\ 1 & e^{-j\frac{4\pi}{3}} & e^{-j\frac{8\pi}{3}} \end{bmatrix} \begin{bmatrix} x(2) \\ x(5) \\ x(8) \end{bmatrix}$$

II. The Hirschman Optimal Transform (HOT) (5/5)

- In general,

  K^2-point HOT ≡ K separate K-point DFT

- If $N=K^2$, the computation complexity of N-point HOT is $O(K\cdot(K\log K))=O(N\log K)$.
- HOT is more efficient in computation than DFT.

III. Properties of the HOT (1/2)

- Basic properties:
  - Unitary: $\mathbf{H}^*\mathbf{H}=\mathbf{H}\mathbf{H}^*=\mathbf{I}$, where * denotes conjugate transpose
  - Symmetric: $\mathbf{H}^T=\mathbf{H}$
  - Periodic: $\mathbf{H}_{K^2}^4 = \mathbf{I}_{K^2}$
- (Eigendecomposition of **H**): Let **h** be an eigenvector of $\mathbf{F}_K$ corresponding to eigenvalue λ, and $\{\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_K\}$ be any orthonormal basis of the $K\times 1$ vector space. Then $\mathbf{h}\otimes\mathbf{e}_1$, $\mathbf{h}\otimes\mathbf{e}_2$, …, $\mathbf{h}\otimes\mathbf{e}_K$ are all eigenvectors of $\mathbf{H}_{K^2}$ corresponding to the same eigenvalue λ.

III. Properties of the HOT (2/2)

- Eigenvalues of $\mathbf{H}_{K^2}$:
  - Has only four distinct eigenvalues {1, -*j*, -1, *j*}
  - If $\{m_1, m_{-j}, m_{-1}, m_{+j}\}$ are eigenvalue multiplicities of $\mathbf{F}_K$,
    $\Rightarrow \{K \cdot m_1, K \cdot m_{-j}, K \cdot m_{-1}, K \cdot m_{+j}\}$ are the eigenvalue multiplicities of $\mathbf{H}_{K^2}$

- Commuting matrices:

  If $\mathbf{S}_K$ is any commuting matrix of $\mathbf{F}_K$, i.e.,
  $\mathbf{S}_K \cdot \mathbf{F}_K = \mathbf{F}_K \cdot \mathbf{S}_K$,
  $\Rightarrow \quad (\mathbf{S}_K \otimes \mathbf{I}_K)$ is a commuting matrix of $\mathbf{H}_{K^2}$

IV. Proposed Efficient Discrete Fractional HOT Transform (1/4)

- *Definition:* $K^2 \times K^2$ discrete fractional HOT (DFRHOT) with fractional parameter a:

$$\mathbf{H}_{K^2}^{a} = \mathbf{F}_{K}^{a} \otimes \mathbf{I}_{K}^{a}$$

where $\mathbf{F}_{K}^{a}$ is the ath-order fractional DFT:

$$\mathbf{F}_{K}^{a} = \sum_{i=0}^{K-1} \lambda_i^a \mathbf{h}_i \mathbf{h}_i^T$$

- If we choose $\mathbf{I}_{K}^{a} \equiv \mathbf{I}_{K}$, we have simplified DFRHOT as:

$$\mathbf{H}_{K^2}^{a} = \mathbf{F}_{K}^{a} \otimes \mathbf{I}_{K} \qquad (1)$$

which is used hereafter.

IV. Proposed Efficient Discrete Fractional HOT Transform (2/4)

- From (1), K^2-point DFRHOT can be computed by ***K* separate *K*-point fractional DFT**.
- If $N=K^2$, computation complexity of N-point DFRHOT is $O(K\cdot(K^2))= O(N^{1.5})$.
- Efficient N-point DFRHOT requires only $1/\sqrt{N}$ computations of existing discrete fractional transforms.

IV. Proposed Efficient Discrete Fractional HOT Transform (3/4)

- Proposed DFRHOT has many good properties:
  - Boundary property: $\mathbf{H}_{K^2}^{0} = \mathbf{I}_{K^2}$
  - Order additivity:
$$\mathbf{H}_{K^2}^{a} \cdot \mathbf{H}_{K^2}^{b} = (\mathbf{F}_{K}^{a} \otimes \mathbf{I}_{K}) \cdot (\mathbf{F}_{K}^{b} \otimes \mathbf{I}_{K})$$
$$= (\mathbf{F}_{K}^{a} \cdot \mathbf{F}_{K}^{b}) \otimes (\mathbf{I}_{K} \cdot \mathbf{I}_{K})$$
$$= \mathbf{F}_{K}^{a+b} \otimes \mathbf{I}_{K} = \mathbf{H}_{K^2}^{a+b}$$
  - Inverse transform: $(\mathbf{H}_{K^2}^{a})^{-1} = \mathbf{H}_{K^2}^{-a}$
  - Reduction to the ordinary HOT when a=1:
$$\mathbf{H}_{K^2}^{a} = \mathbf{H}_{K^2}^{1} = \mathbf{F}_{K}^{1} \otimes \mathbf{I}_{K} = \mathbf{H}_{K^2}$$
  - Unitarity: If * denotes the conjugate transpose,
$$(\mathbf{H}_{K^2}^{a})^{*} \cdot (\mathbf{H}_{K^2}^{a}) = (\mathbf{H}_{K^2}^{a}) \cdot (\mathbf{H}_{K^2}^{a})^{*} = \mathbf{I}_{K^2}$$

IV. Proposed Efficient Discrete Fractional HOT Transform (4/4)

- Extended DFRHOT (EDFRHOT): If *L* is a fixed integer independent of *N*, then EDFRHOT can be defined as:

$$\mathbf{H}_N^a = \mathbf{F}_L^a \otimes \mathbf{I}_{(N/L)}$$

- *N*-point EDFRHOT can be computed by:

  N/L separate *L*-point fractional DFT.

- EDFRHOT has linear computation complexity: $O((N/L)\cdot(L^2))=O(N\cdot L)$

V. Application and Experiment Results (1/3)

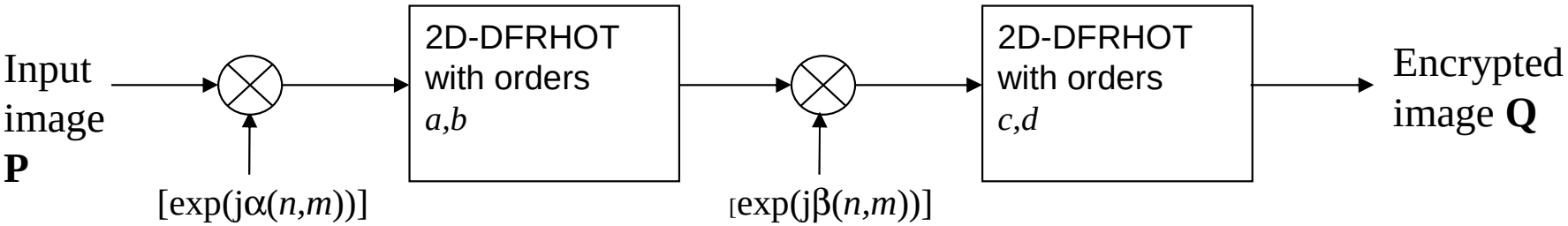

Fig. 1. Encryption process of the double random phase encoding in the DFRHOT domain.

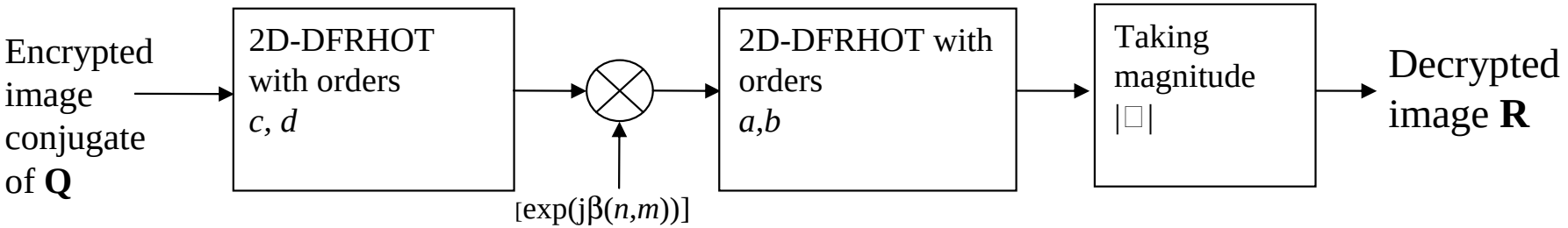

Fig. 2. Decryption process of the double random phase encoding in the DFRHOT domain.

V. Application and Experiment Results (2/3)

- 2-D DFRHOT can be applied for image encryption.
- All of the fractional parameters *a*, *b*, *c*, *d*, and random phases in Fig. 1 can be used as the encryption keys.
- 2-D DFRHOT of an *N*×*M* input image **P**

$$\mathbf{P}_{(a,b)} = \mathbf{H}_N^a \cdot \mathbf{P} \cdot \mathbf{H}_M^b$$

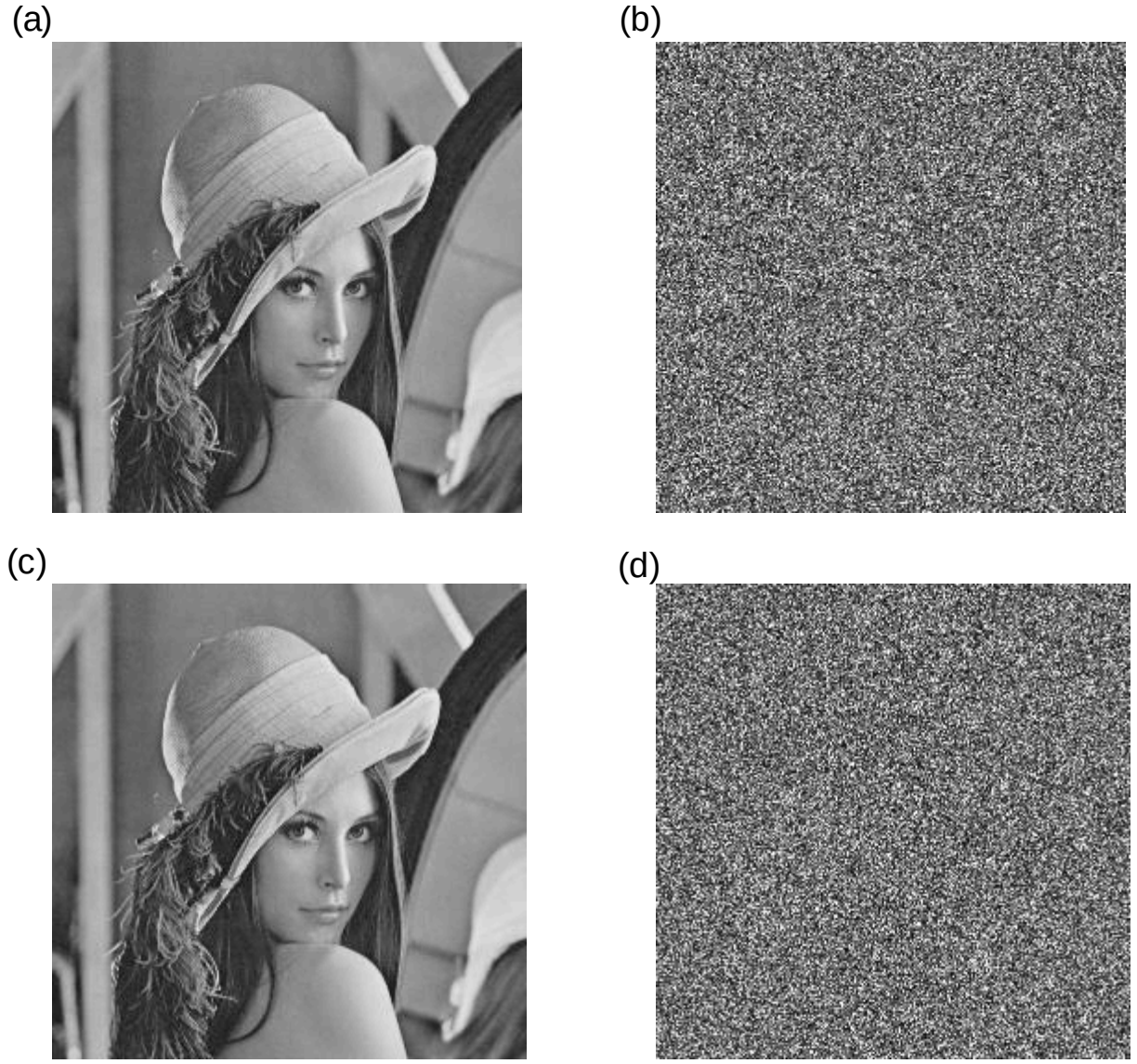

Fig. 3. Double random phase encoding in the DFRHOT domain. (a) Original image. (b) Encrypted image. (c) Decrypted image with correct fractional parameters for decryption. (d) Decrypted image with incorrect fractional parameters for decryption.

VI. Conclusions (1/1)

- We define a new DFRHOT as Kronecker product of fractional DFT and identity matrix.
- Proposed DFRHOT is significantly more efficient than all existing discrete fractional transforms.
- DFRHOT reduces computation complexity of fractional transforms from $O(N^2)$ to $O(N^{1.5})$ or even to $O(N^1)$.
- DFRHOT has all good properties that a fractional transform should possess.
- We also apply DFRHOT to encrypt digital images.

VII. **REFERENCES (1/2)**

[1] H. M. Ozaktas, Z. Zalevsky, and M. A. Kutay, *The Fractional Fourier Transform with Applications in Optics and Signal Processing*. New York, John Wiley & Sons, 2000.

[2] L. B. Almeida, “The fractional Fourier transform and time-frequency representations,” *IEEE Trans. Signal Processing*, vol. 42, pp. 3084-3091, Nov. 1994.

[3] V. Namias, “The fractional order Fourier transform and its application to quantum mechanics,” *J. Inst. Math. Appl.*, vol. 25, pp. 241-265, 1980.

[4] G. Unnikrishnan and K. Singh, “Double random fractional Fourier-domain encoding for optical security,” *Opt. Eng.,* vol. 39, pp. 2853-2859, 2000.

[5] S. C. Pei and M. H. Yeh, “Improved discrete fractional Fourier transform,” *Opt. Lett.*, vol. 22, pp. 1047-1049, 1997.

[6] C. Candan, M. A. Kutay, and H. M. Ozaktas, “The discrete fractional Fourier transform,” *IEEE Trans. Signal Processing*, vol. 48, pp. 1329-1337, May 2000.

[7] S. C. Pei and W. L. Hsue, “The multiple-parameter discrete fractional Fourier transform,” *IEEE Signal Processing Letters*, vol. 13, no. 6, pp. 329-332, June 2006.

[8] G. Cariolaro, T. Erseghe, and P. Kraniauskas, “The fractional discrete cosine transform,” *IEEE Trans. Signal Processing*, vol. 50, no. 4, pp. 902-911, Apr. 2002.

[9] S. C. Pei and M. H. Yeh, “The discrete fractional cosine and sine transforms,” *IEEE Trans. Signal Processing*, vol. 49, no. 6, pp. 1198-1207, Jun. 2001.

VII. REFERENCES (2/2)

[10] C. C. Tseng, “Eigenvalues and eigenvectors of generalized DFT, generalized DHT, DCT-IV and DST-IV matrices,” *IEEE Trans. Signal Processing*, vol. 50, no. 4, pp. 866-877, Apr. 2002.

[11] H. M. Ozaktas, O. Arikan, M. A. Kutay, and G. Bozdagi, “Digital computation of the fractional Fourier transform,” *IEEE Trans. Signal Processing*, vol. 44, no. 9, pp. 2141-2150, Sep. 1996.

[12] V. DeBrunner, M. Ozaydin, T. Przebinda, and J. Havlicek, “The optimal solutions to the continuous- and discrete-time versions of the Hirschman uncertainty principle,” in *Proc. ICASSP’00,* Istanbul, Turkey, June 5-9, 2000.

[13] T. Przebinda, V. DeBrunner, and M. Ozaydin, “The optimal transform for the discrete Hirschman uncertainty principle,” *IEEE Trans. Information Theory*, vol. 47, no. 5, pp. 2086-2090, July 2001.

[14] V. DeBrunner and E. Matusiak, “An algorithm to reduce the complexity required to convolve finite length sequences using the Hirschman optimal transform (HOT),” in *Proc. ICASSP’03,* vol. II, pp. 577-580, 2003.

[15] W.-H. Steeb, *Problems and Solutions in Introductory and Advanced Matrix Calculus*. London, World Scientific, 2006.

[16] P. Refregier and B. Javidi, “Optical image encryption based on input plane and Fourier plane random encoding,” *Opt. Lett.*, vol. 20, pp. 767-769, 1995.