Optik 125 (2014) 5414–5417

Contents lists available at ScienceDirect

Optik

journal homepage: www.elsevier.de/ijleo

Implementing compressive fractional Fourier transformation with iterative kernel steering regression in double random phase encoding

Nitin Rawat[a], Rajesh Kumar[b], Byung-Geun Lee[a,*]

[a] School of Mechatronics, Gwangju Institute of Science & Technology, Gwangju, South Korea
[b] Jaypee University of Information Technology, Waknaghat, Solan, HP 173234, India

ARTICLE INFO

Article history:
Received 4 October 2013
Accepted 27 May 2014

Keywords:
Compressive sensing
Fractional Fourier transform
DRPE
Kernel steering regression
TwIST

ABSTRACT

This paper proposes a novel approach in double random phase encryption based on compressive fractional Fourier transform along with the kernel steering regression. The method increases the complexity of the image by using fractional Fourier transform and taking fewer measurements from the image data. Numerical results are given to analyze the validity of this technique. Considering natural images to be sparse in some domain, we apply a compressive sensing (CS) approach by using a TwIST algorithm. The encryption process has kernel steering regression algorithm for denoising and compressive sensing technique for image compression along with the fractional Fourier transform that makes the image in more complex form.

1. Introduction

Considering the threat of accessing and tempering data by an unauthorized person, a secure transmission of multimedia information like image data using the cryptography technique has received attention in recent years. The encryption methods enable security of data by converting the image into its complex form. Unlike the text message, image encryption by traditional encryption algorithm such as RSA and DES are not suitable as large image data takes a lot of time to encrypt [1]. Besides the electronic encryption [2], an optical encryption method is a more secure method as it involves sophisticated optical techniques [3]. It enhances the security of the data by scrambling the content which can be unlocked only by the right decrypted key. Moreover, encryption possesses a greater degree of freedom due to features such as phase, amplitude, wavelength, polarization, and the time it takes for the information to encrypt. Among the optical encryption methods such as digital holography [3], multiplexing [4], Fresnel domain [5], polarized light [6] and interferometry [7], the double random phase encryption (DRPE) has widely accepted due to simple implementation, robustness and easy application on different image formats viz. black and white, gray level or colored images [8]. The DREP involves a random phase mask in the input plane which whitens the input image and a second random phase mask at the Fourier plane which whitens the Fourier spectrum. The random phase mask placed in the Fourier plane serves as the only key in DREP scheme. Since we always look for ways to enhance the security of the data, the fractional Fourier transformation (FRFT) involves an extra parameter of the transform order from 0 to 1 [9,10]. Therefore, the transform order enlarges the key space resulting in a higher security of data as compared to the Fourier transformation (FT) [1].

Besides security, the database and communication problems are also critical due to large data size and complexity. It has become important to reduce the size of the data while preserving the complexity. Recently, the compressive sensing (CS) technique has gained a wide acceptance [11]. It states that most natural images are sparse in some domain. In the conventional way, where we try to sample as much data as possible, CS provides a platform to reconstruct the data from a fewer measurements, i.e. if an image is sparse in some domain, then a perfect recovery can be reconstructed from its few measurements.

In this letter, we propose a DRPE encryption method incorporating the FRFT and CS approaches along with the kernel steering regression algorithm. Here, we use a noisy image and apply kernel regression for denoising. Further, FRFT enhances the degree of freedom to decrypt an image under experiment, and CS reduces the bandwidth of the data transmission.

2. CS approach

According to CS, small collections of non-adaptive linear measurements of a compressible signal or image have enough

* Corresponding author. Tel.: +82 62 715 3231.
E-mail address: bglee@gist.ac.kr (B.-G. Lee).

http://dx.doi.org/10.1016/j.ijleo.2014.06.022
0030-4026/

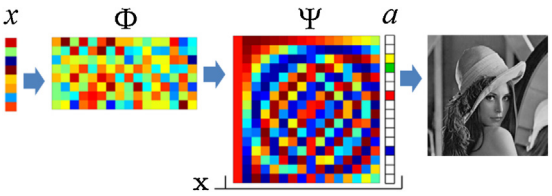

Fig. 1. Schematic of CS approach.

measurements to reconstruct it perfectly [12,13]. Almost all natural images have concise representations in some basis. The CS theory can be summarized in the following ways:

$$y = \Phi f = \Phi\Psi x \tag{1}$$

where Φ represents the $M \times N$ measurement matrix, and y as a $M \times 1$ vector, while f is $N \times 1$. The x is an image and Ψ is the image representation in some basis. The K-sparse image implies that it has at most K non-zero elements and the rest are zeros. Here, K is assumed to be much less than N. CS relies on signal sparsity and the incoherence between the sensing matrix and the sparsifying operator defined to be mutually coherence and can be expressed as:

$$\mu(\Phi, \Psi) = \sqrt{n} \cdot \max_{1 \le k,j \le n} |\langle \varphi_k, \psi_j \rangle| \tag{2}$$

where φ_k, ψ_j denotes the column vector of Φ and Ψ respectively and n is the length of the column vector. If Φ and Ψ are highly correlated, the coherence is large, else it is small. It follows $\mu(\Phi, \Psi) \in [1, \sqrt{n}]$.

The CS approach is shown in Fig. 1 where the image is sparse in some domain and from fewer measurement; a signal can be easily extracted. Usually, natural images are sparse in some sparsifying operator Ψ (i.e. wavelet or DCT). We can choose a Gaussian random sensing basis as it is well known CS operator, which means that it fits to signals sparsity in any domain having a mutual coherence $\mu \approx \sqrt{2\log N}$ regardless of Ψ. If both Ψ and Φ of them are uncorrelated, then x can be well recovered from $n = O(d \log N)$ measurements if it satisfies the *Restricted Isometry Property* (RIP) [13]. Once the above conditions satisfy CS theory, we can recover the signal by using l_1-norm minimization; the proposed reconstruction is given by $f^* = \Psi x^*$, where x^* is the solution to the convex optimization program ($||x||_{l_1} := \sum_i |x_i|$). Here, we have chosen the two-step iterative shrinkage threshold (TwIST) algorithm [14]. The TwIST algorithm is composed of a least square minimization term.

3. DRPE using FRFT

The security of transmitted data depends on the complexity of the random phase function and the key. The extraction procedures using the FRFT techniques [9,15,16] are complex compared to the conventional Fourier transform (FT) since FRFT provides extra degree of freedom. The FRFT is a generalization of the FT [15]. In case of FRFT, the parameters, such as Fractional orders and the scaling factors along with the x and y-axis [16] make it complex to decode as they serve as additional keys for image decryption. Furthermore, the FRFT mixes the signal by rotating it through any arbitrary angle in frequency-space domain. Here $(\alpha, \beta) = p\pi/2$ are the angles at which FRFT can be calculated.

In this method, the image is multiplied by independent random phase functions and is transformed through the FRFT order. In a two-dimensional case, the notation for FRFT is further discussed. The ath order FRFT f^α of a function $f(x,y)$ is expressed as:

$$f^\alpha = \int\int_{-\infty}^{+\infty} K^\alpha(x, y; x', y') f(x, y) dx dy \tag{3}$$

The f^α is the transform kernel given by

$$K^\alpha(x, y; x', y') = A_\varphi \exp[i\pi(x^2 + y^2 + x'^2 + y'^2)\cot\varphi_\alpha - 2(xx' + yy')\cot\varphi_\alpha] \tag{4}$$

where $A_\varphi = \exp[-i\pi\,\mathrm{sgn}(\sin\varphi)/4 + i\varphi/2]$, $\varphi = \alpha\pi/2$ is the transform angle and $0 < |\alpha| < 2$ is the range.

Fig. 2 shows a conventional double random phase encoding process. Let's say an image, $I(x, y)$ is shuffled by two different random phase functions, $\exp[i\phi_{1\,\mathrm{and}\,2}(x, y)]$. An FRFT is performed through an order of (α, β) where the range of the order is considered between $(-2$ to $2)$. Hence the final encrypted image $E(x, y)$ can be obtained by the FRFT order expressed as

$$E(x, y) = F_\alpha\{F_\beta\{[I(x, y)\exp[i\phi_1(x, y)]\exp[i\phi_2(x, y)]\}\} \tag{5}$$

where $F_{\alpha,\beta}$ represents the order of FRFT. Similarly the decryption procedure is defined as

$$D(x, y) = F_\beta^{-1}\{\{F_\alpha^{-1}[E(x, y)\exp[i\phi_2(x, y)^*]\}\exp[i\phi_1(x, y)]^*\} \tag{6}$$

where $F_{\alpha,\beta}^{-1}$ represents the inverse fractional Fourier transform through the order of (α, β). The image $I(x, y)$ is multiplied by the random phase $\phi_1(x, y)$. An FRFT of αth order is taken and multiplied by random phase $\phi_2(x', y')$. Another bth order of FRFT gives the encrypted image in the fractional domain. It is evident that random

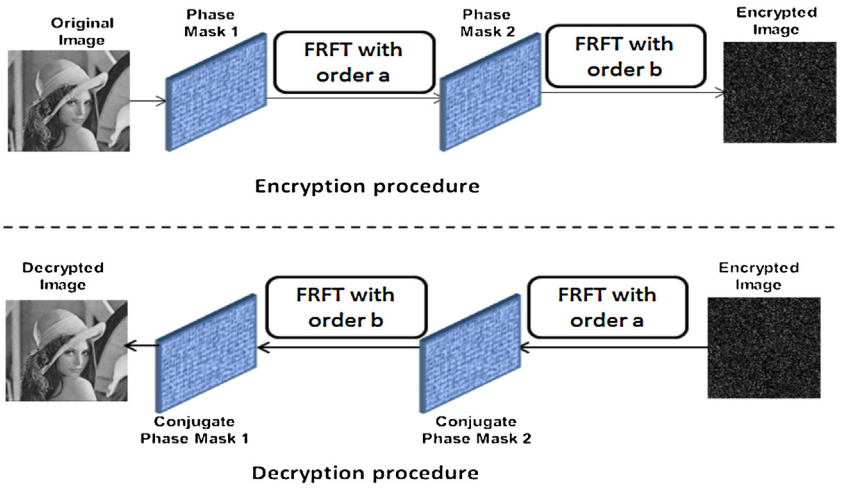

Fig. 2. Conventional double random phase encoding process.