Optik 126 (2015) 2663–2670

Contents lists available at ScienceDirect

Optik

journal homepage: www.elsevier.de/ijleo

Securely compressive sensing using double random phase encoding

Hong Liu [a,b], Di Xiao [a,*], Yanbing Liu [b], Yushu Zhang [c]

[a] Key Laboratory of Dependable Service Computing in Cyber Physical Society (Chongqing University) of Ministry of Education, College of Computer Science, Chongqing University, Chongqing 400044, China
[b] College of Software Engineering, Chongqing University of Posts and Telecommunications, Chongqing 400065, China
[c] School of Electronics and Information Engineering, Southwest University, Chongqing 400715, China

ARTICLE INFO

Article history:
Received 11 May 2014
Accepted 26 June 2015

Keywords:
Securely compressive sensing
Fractional Fourier transform
Random phase encoding

ABSTRACT

Recently, the weakness of existing compressive sensing process from the perspective of the chosen-plaintext attack has been discovered. To enhance the security and performance of compressive sensing process, double random phase encoding (DRPE) based block compressive sensing has been designed, which is a chaos-based random phase encoding in fractional Fourier domain for each image block. Moreover, this article presents a combined compressive sensing and optical image encryption method. The experimental results demonstrate that the proposed encryption method not only achieves high security level but also has comparable performance with existing encryption methods.

1. Introduction

Recently, some researchers proposed a kind of compression-combined encryption method based on Compressive Sensing (CS) [1,2]. It combines sampling and compression together through a random measurement process. The compression-combined encryption methods based on CS were proposed in [3–8]. Rachlin and Baron [3] demonstrate that, although the CS-based encryption scheme cannot achieve perfect security, it is still meaningful owing to the high computational complexity of cracking. Orsdemir et al. [4] proposed the notion of robust encryption, meaning that the cipher image is tolerant of some level of noise contamination. The security is analyzed in terms of brute force and structured attacks. They claim that the computational complexity of these two attacks renders them infeasible in practice. Considering the unavoidable problem of packet loss during wireless transmission, Liu et al. [5] and Gao et al. [6] quantify the anti-packet loss ability of CS-based encryption paradigm. Lu et al. [7] proposed an image information encryption method based on CS and double random-phase encoding. This encryption scheme has the following features: low data volume for encryption and high security of information.

Although these methods [3–8] have been proven to provide satisfactory results, there are still some issues to be addressed: The existing compressive sensing process directly uses Gaussian matrix as the measurement matrix to do linear dimension reduction projection, which does not provide high security level and fails to resist the chosen-plaintext attack. Meanwhile, it is not optimal to directly use Gaussian matrix as the measurement matrix in real time applications, such as limited-resource sensors and video surverllance.

In this paper, for security enhancement, we design DRPE-based block compressive sensing process, which is a chaos-based random phase encoding in fractional Fourier domain for each image block. Not only block compressive sensing but also fractional Fourier transform and non-linear chaotic scrambling are adopted to resist against the chosen-plaintext attack. Moreover, we propose a combined compressive sensing and optical image encryption method, which uses structurally random matrices [9] and supports block-based compressive sensing operations.

The rest of this paper is organized in the following sequence. In Section 2, the proposed image encryption method is addressed. Some numerical simulations are given in Section 3 to demonstrate the security and performance. Concluding remarks are summarized in the final section.

2. Proposed scheme

2.1. Encryption process

The flow chart of proposed image encryption method using DRPE-based block compressive sensing is shown in Fig. 1. The image is firstly divided into blocks, then each block is transformed by discrete cosine transform and the coefficients are scrambled by chaotic scrambling technology. In order to enhance the security and performance of the compressive sensing process, we design the DRPE-based block compressive sensing process [9,10], which is

* Corresponding author. Tel.: +86 23 8633 3521; fax: +86 23 6510 4570.
E-mail address: xiaodi_cqu@hotmail.com (D. Xiao).

http://dx.doi.org/10.1016/j.ijleo.2015.06.079
0030-4026/

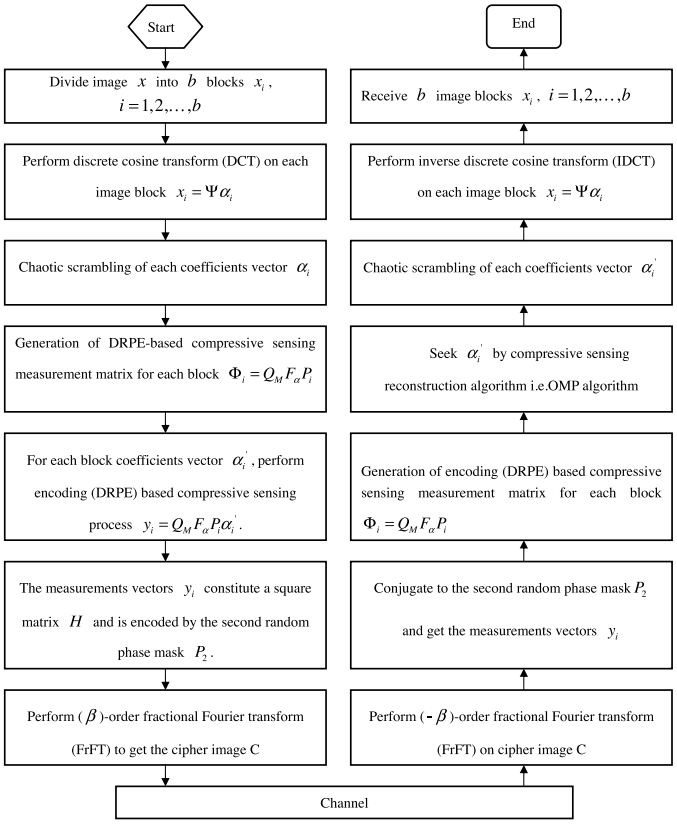

Fig. 1. Image encryption using DRPE-based block compressive sensing.

a chaos-based random phase encoding in fractional Fourier domain for each image block, denoted by

$$\Phi_i = Q_M F_r P_i \tag{1}$$

where $P_i \in R^{N\times N}$ is a random phase mask matrix, which is to scramble the signal's sample location. $F_r \in R^{N\times N}$ is fractional Fourier transform, which is to spread the information of the signal's samples over all measurements. $Q_M \in R^{M\times N}$ is a subsampling matrix, which selects a random subset of rows of $F_r P_i$. In matrix representation, Q_M is a random subset of M rows of the identity matrix of size $N\times N$. At last, the second random phase encoding is used to complete the encryption. The detail encryption steps are as follows:

(1) The original image is divided into b blocks. We assume the size of each block is $\sqrt{N}\times\sqrt{N}$ and vectorize them into one-dimensional vectors in raster order. The ith block's pixel vector is denoted by x_i, $i=1, 2, \ldots, b$.
(2) Perform discrete cosine transform (DCT) on each image block x_i to get the coefficients vector $\alpha_i=\Psi x_i$, $i=1, 2, \ldots, b$.
(3) Scramble each coefficients vector α_i with the chaotic scrambling technology in the following and we get permuted coefficients vector α_i'.
  (a) The key K_1 is used as the initial value χ of Tent map [11] to generate chaotic sequence $S_1=\{0<s_i<1|i=1, 2, \ldots, b\}$. The size of the sequence S_1 is b, which is the number of image blocks. The tent map is defined as

$$G(\chi)=\begin{cases}\dfrac{\chi}{p}, & 0\le\chi\le p\\ \dfrac{\chi-p}{1-p}, & p\le\chi\le 1\end{cases} \tag{2}$$

  (b) Then each sequence element s_i is used as the initial value x_k of logistic map [11] to generate chaotic sequence $R=\{r_i(m)|m=1, 2, \ldots, N\times 1\}$ for block-based chaotic scrambling. The logistic map is defined as

$$x_{k+1}=\mu x_k(1-x_k) \tag{3}$$

  (c) Sort the sequence R in ascending order or descending order, and then obtain new sequence $R'=\{r_i[w(m)]|m=1, 2, \ldots, N\times 1\}$. The value and the number of the elements do not change but the positions of the elements are varied. The m-th element in R' corresponds to the $w(m)$-th element in R. Consequently, w represents address code.
  (d) Use address code w to reorder the coefficients vector α_i, and then obtain the scrambled coefficients vector $\alpha_i'=\{\alpha'(m)\}$, $m=1, 2, \ldots, N\times 1\}$, where $\alpha_i'(m)=\alpha_i[w(m)]$.
(4) Generate DRPE-based compressive sensing measurement matrix $\Phi_i=Q_M F_\alpha P_i$ for each image block. The detailed substeps are as follows:
  (a) The key K_2 is used as the initial value of Tent map to generate chaotic sequence $S_2=\{0<s_i<1|i=1, 2, \ldots, b\}$. The size of the sequence S_2 is b, which is the number of image blocks.
  (b) Then each sequence element s_i is used as the initial value of Tent map to generate chaotic sequence $L_i=\{0<l_i<1|i=1, 2, \ldots, N\times N\}$. The random matrix C_i of size $N\times N$ is created column by column using the chaotic sequence L_i. With the help of random matrix C_i, we get random phase mask $P_i=e^{i\pi C_i}$.
  (c) At last, with the matrices F_α and Q_M, the compressive sensing measurement matrix $\Phi_i=Q_M F_\alpha P_i$ for each block is obtained.
(5) Perform DRPE-based compressive sensing process for each block with the designed compressive sensing measurement matrix $\Phi_i=Q_M F_\alpha P_i$ and get the measurements vector $y_i=Q_M F_\alpha P_i \alpha_i'$. The detailed substeps are as follows:
  (a) Each scrambled coefficients vector α_i' with the length of $N\times 1$ (from previous step (3)) is randomized and encoded by the random phase mask matrix P_i of size $N\times N$ (from previous step (4)), denoted by $\bar{P}_i=P_i\alpha_i'$, $i=1, 2, \ldots, b$.
  (b) The key K_3 is used as the fractional order of fractional Fourier transform, then perform (α)-order fractional Fourier transform (FrFT) on $\bar{P}_i$, denoted by $\hat{I}_i=F_\alpha[\bar{P}_i]$.
  (c) Randomly select M rows of $\hat{I}_i$ to get subsampling measurement. This step corresponds to multiplying the $N\times N$ matrix $\hat{I}_i$ with the $M\times N$ matrix Q_M, denoted by $y_i=Q_M\hat{I}_i$. Then we get the compressed measurements vector y_i with size $M\times 1$.
(6) These measurements vectors y_i, $i=1, 2, \ldots, b$, constitute a matrix H with size $\sqrt{Mb}\times\sqrt{Mb}$.
(7) The measurements vector matrix H is randomized and encoded by the second random phase mask matrix P_2 with size $\sqrt{Mb}\times\sqrt{Mb}$, denoted by $\tilde{I}=P_2H$. The detailed substeps are as follows:
  (a) The key K_4 is used as the initial value of Tent map to generate chaotic sequence $g=\{0<g_i<1|i=1, 2, \ldots, \sqrt{Mb}\times\sqrt{Mb}\}$. The size of the sequence g is $\sqrt{Mb}\times\sqrt{Mb}$, which is the size of compressed image. The random matrix C_2 of size $\sqrt{Mb}\times\sqrt{Mb}$ is created column by column using the chaotic sequence g. With the help of random matrix C_2, we get second random phase mask $P_2=e^{i\pi C_2}$.
  (b) The measurements vector matrix H (from previous step (6)) is randomized and encoded by the second random phase mask matrix P_2, denoted by $\tilde{I}=P_2H$.
(8) The key K_5 is used as the fractional order of fractional Fourier transform, then perform (β)-order fractional Fourier transform (FrFT) on $\tilde{I}$ to get the final cipher image, denoted by $C=F_\beta[\tilde{I}]$.

2.2. Decryption process

The decryption process is mainly based on block-based compressive sensing reconstruction and fractional Fourier transform. The complete reconstruction process is shown in Fig. 1. With the