Optics Communications 359 (2016) 290–296

Contents lists available at ScienceDirect

Optics Communications

journal homepage: www.elsevier.com/locate/optcom

Interference-based image encryption with silhouette removal by aid of compressive sensing

Qiong Gong, Zhipeng Wang, Xiaodong Lv, Yi Qin*

College of Physics and Electronic Engineering, Nanyang Normal University, Nanyang 473061, China

ARTICLE INFO

Article history:
Received 3 July 2015
Received in revised form
24 September 2015
Accepted 26 September 2015

Keywords:
Optical encryption
Compressive sensing
Silhouette problem

ABSTRACT

Compressive sensing (CS) offers the opportunity to reconstruct a signal from its sparse representation, either in the space domain or the transform domain. Exploiting this character, we propose a simple interference-based image encryption method. For encryption, a synthetic image, which contains sparse samples of the original image and the designated values, is analytically separated into two phase only masks (POMs). Consequently, only fragmentary data of the primary image can be directly collected in the traditional decryption scheme. However, the subsequent CS reconstruction will retrieve a high quality image from the fragmentary information. The proposed method has effectively suppressed the silhouette problem. Moreover, it has also some distinct advantages over the previous approaches.

1. Introduction

Information processing based on optical methods has been widely investigated over the past several years, especially in the area of information securities [1–9]. The representative work was devoted by Refregier and Javidi, who invented the double random phase encoding (DRPE) technique in 1995 [10]. Matoba and Javidi extend the DRPE to 3-dimension by employing the positions of the two random phase masks as new keys [11]. Thereafter, more and more derivatives of the DRPE have been further developed [12–15]. However, all of the above mentioned methods are based on the random phase encoding at the input and/or transform planes, and the ciphertexts of them are complex values. In order to record phase information, the holography technology is always necessary. What is more, the decryption is difficult to be performed optically, since the current spatial light modulators (SLMs) are unable to display complex values.

In order to deal with this issue, people commence encrypting the target image into phase only masks (POMs) [16–21]. These methods not only overcome the problem suffered by DRPE, but also possess an additional layer of security, as the POMs are very hard to be duplicated. It should be pointed out that the very simple interference-based encryption (IBE) system first proposed by Zhang caused wide public concern, since the two pure phase masks which contain the image information can be obtained analytically [21]. Nevertheless, there is a security leak in the cryptosystem, as either of the two pure phase masks can reconstruct a silhouette of the original image. Although various approaches are provided to cope with this problem, the removal of it often comes at the cost of increased time of computation and a greater number of POMs. For instance, Zhang et al. presented a method for secrecy enhancement based on exchanging the same parts of two masks [22]. Wang and Zhao proposed to further divide the two analytically-obtained POMs into three POMs [23].

In this article, we proposed a very simple method to solve the silhouette problem by taking advantage of compressive sensing (CS), which has immediate applications in reduction of acquisition time for measurements [24–30]. In particular, CS offers the opportunity to reconstruct a signal from its sparse representation, either in the space domain or the transform domain. Exploiting this character, we construct a synthetic image that contains only partial information of the original image. The SI, instead of the primary image, is sent to the IBE scheme and then separated into two POMs. Numerical results show that the silhouette problem has been eliminated. In addition, the proposed method is also demonstrated to have some obvious merits over the previous IBE schemes.

2. Theoretical analysis

2.1. Compressive sensing

CS is a recently developed technique that enables the reconstruction of a signal sampled in violation of the traditional

* Corresponding author.
E-mail address: 641858757@qq.com (Y. Qin).

http://dx.doi.org/10.1016/j.optcom.2015.09.091
0030-4018/

Nyquist criterion. In other words, it aims to reconstruct signals and images from significantly fewer measurements that were traditionally thought necessary. CS theory relies mainly on two guiding principles, sparsity and incoherence [24]. The sparsity is that any natural signal can be compressed in certain basis and thus the compressed small numbers of measurements reserve adequate information of the primary image to ensure perfect recovery of it. Suppose f with size of $N \times 1$ be the input signal, the sparsity means that f can be represented sparsely in certain basis Ψ, which can be mathematically expressed as

$$f = \Psi\alpha \tag{1}$$

where Ψ is the sparsifying transform (e.g., wavelet), α is an S-sparse (S«N) signal. The signal $\alpha$is S-sparse if S of its N components are nonzero and (N–S) are zero. The acquisition model of CS can be expressed as follows:

$$z = \Phi f = \Phi\Psi\alpha \tag{2}$$

where z represents the measurements and Φ is an $M \times N$ ($M < N$) measurement matrix. The measurement process is not adaptive, meaning that Φ is fixed and does not depend on the signal f. The incoherence principle means that the measurement matrix Φ should be incoherent with Ψ [26]. The coherence between them can be defined as

$$\mu(\Phi, \Psi) = \sqrt{N} \cdot \max_{1 \le p,q \le N} \left|\langle \varphi_p, \psi_q \rangle\right| \tag{3}$$

where φ_p is a row vector of Φ and ψ_q is a column vector of Ψ. Φ and Ψ are considered to be highly uncorrelated if $1/\sqrt{N} \le \mu(\Phi, \Psi) \le 1$.

When both sparsity and incoherence are fulfilled, a perfect recovery of the primary signal is possible from small number of measurements, which are obtained in the space domain or the transform domain. Usually, CS is performed by solving a ℓ1-norm minimization problem stated in general as [30]

$$\min_{\alpha} \|\alpha\|_1 \cdot \text{such that} \cdot z = \Phi\Psi\alpha \tag{4}$$

It is worth noting that, for a general image, its gradient is always sparse. In other words, a natural image is sparse in the gradient domain. Thus, another extensively used minimization problem is performed by minimizing the total variation, which can be interpreted as the ℓ1-norm of the gradient [30]. If we also denote the image (2-D signal) as f, the convex optimization in this case can be given by

$$\min_{f} \text{TV}(f) \text{ such that } z = \Phi f \text{ with}$$

$$\text{TV}(f) = \sqrt{\left(f_{i+1,j} - f_{i,j}\right)^2 + \left(f_{i,j+1} - f_{i,j}\right)^2} \tag{5}$$

2.2. The IBE method and the silhouette problem

In this section, the IBE method will be briefly summarized [21] and the silhouette problem will be reviewed. The optical structure for illustrating the IBE system is shown in Fig. 1, where P_1 and P_2 are two phase masks, and the distances between them and output plane are both equal to l. While P_1 and P_2 are illuminated by a plane wave, the diffractive fields of them will undergo interference at the output plane and the primary image (i. e. the plain text) is generated. Quite evidently, the two phase masks are treated as ciphertexts. The encryption task is to encrypt the primary image into the two POMs.

In order to achieve this goal, the normalized primary image $f(x_o, y_o)$ is first multiplied by a random phase mask to construct a complex value image as [21]

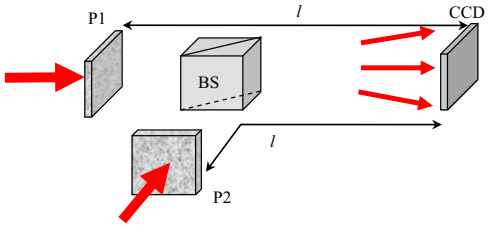

Fig. 1. Schematic of the decryption setup of the IBE method. P: extracted phase-only masks; BS: beam splitter; and CCD: Charge Coupled Device.

$$f'(x_o, y_o) = \sqrt{f(x_o, y_o)} \exp\left[j2\pi R(x_o, y_o)\right] \tag{6}$$

where $R(x_o, y_o)$ is a map randomly distributed in the range of [0, 1]. This complex field is expected to be interference of two plane waves emitting from P1 and P2, and then we have [21]

$$f'(x_o, y_o) = \left[\exp\left[jP_1(x_i, y_i)\right] + \exp\left[jP_2(x_i, y_i)\right]\right] * h(x_i, y_i, l) \tag{7}$$

where

$$h(x_i, y_i, l) = \frac{\exp(j2\pi l/\lambda)}{j\lambda l} \exp\left[j\pi\left(x_i^2 + y_i^2\right)/\lambda l\right] \tag{8}$$

represents the point pulse function of the Fresnel transform, * denotes the convolution operation. Because of the nature of the POMs, we have [21]

$$\left[\exp(jP_1)\right]\left[\exp(jP_1)\right]^* = \left[\exp(jP_2)\right]\left[\exp(jP_2)\right]^* = 1 \tag{9}$$

where the superscript * stands for the complex conjugate. Let us define $D = F^{-1}\{F[g(x, y)]/F[h(x_i, y_i, l)]\}$, where $F[]$ and $F^{-1}[]$ denote the operations of Fourier transform and inverse Fourier transform, respectively. Then the phase distributions of the two masks are calculated as [21].

$$P_1 = \arg(D) - \arccos[\text{abs}(D)/2] \tag{10}$$

$$P_2 = \arg\left[D - \exp(iP_1)\right] \tag{11}$$

where abs[ ] and arg[ ] denote the modulus and phase of a function, respectively. For brevity, we mathematically denote the whole encryption process as

$$P_1 = \Gamma\left[f(x_o, y_o), \lambda; l\right] \tag{12}$$

$$P_2 = \Omega\left[f(x_o, y_o), \lambda; l\right] \tag{13}$$

Compared with many other methods, a distinct merit of IBE is that the decrypted result is exactly the intensity of the complex filed pattern and thus can be directly registered by a CCD camera. Another merit of IBE is that the phase masks for hiding the original image are analytically obtained, as a result of which the time-consuming iterative algorithms employed by other approaches can be avoided. Nevertheless, this encryption scheme has an inherent silhouette problem [22,23]. The silhouette problem was regarded as a vital security leak of the IBE scheme, as an intruder could acquire considerable information of the primary image if he/she masters any one of the two POMs and the parameters of the decryption architecture. To illustrate this problem, we choose an image Peppers (Fig. 2(a)) with the size of 256×256 pixels as the target image, P1 and P2 are obtained by use of Eqs. (6)-(11). A silhouette of the original image can be observed when only one of the two masks is used in the decryption setup shown in Fig. 1, which is displayed in Fig. 2(b) and (c). If we take correlation coefficient (CC) as a criterion to evaluate the quality of the recovered image [14], the CCs for Fig. 2(b) and (c) are 0.6808 and