Optics Communications 338 (2015) 164–167

Contents lists available at ScienceDirect

Optics Communications

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

Correlated-imaging-based chosen plaintext attack on general cryptosystems composed of linear canonical transforms and phase encodings

Jingjing Wu [a], Wei Liu [a], Zhengjun Liu [b], Shutian Liu [a,*]

[a] Department of Automation Measurement and Control, Harbin Institute of Technology, Harbin 150001, PR China
[b] Department of Physics, Harbin Institute of Technology, Harbin 150001, PR China

ARTICLE INFO

Article history:
Received 9 September 2014
Received in revised form
24 November 2014
Accepted 25 November 2014
Available online 29 October 2014

Keywords:
Attack
Cryptosystem
Correlated imaging

ABSTRACT

We introduce a chosen-plaintext attack scheme on general optical cryptosystems that use linear canonical transform and phase encoding based on correlated imaging. The plaintexts are chosen as Gaussian random real number matrixes, and the corresponding ciphertexts are regarded as prior knowledge of the proposed attack method. To establish the reconstruct of the secret plaintext, correlated imaging is employed using the known resources. Differing from the reported attack methods, there is no need to decipher the distribution of the decryption key. The original secret image can be directly recovered by the attack in the absence of decryption key. In addition, the improved cryptosystems combined with pixel scrambling operations are also vulnerable to the proposed attack method. Necessary mathematical derivations and numerical simulations are carried out to demonstrate the validity of the proposed attack scheme.

1. Introduction

Over the past two decades, optical image encryption has attracted much attention since Refrégiér and Javidi pioneered the double random phase encoding (DRPE) technique in 1995 [1]. Various security-enhanced methods have been proposed [2–6], and the extended DRPEs in Fractional Fourier domain and Fresnel domain are the most widely used. Notice that Fourier transform, Fresnel transform and fractional Fourier transform are all special cases of linear canonical transform (LCT) [7,8], the concept of LCT-based random phase encoding (LCT-RPE) is used to describe the DRPEs based on them. Cryptanalysis on these exploited LCT-RPE systems has been performed and reported, and it has been well known that known-plaintext attack (KPA) [9,10], chosen-plaintext attack (CPA) [11–13] and chosen-ciphertext attack (CCA) [14] pose the greatest security threat. To our knowledge, most of the above reported attack schemes are motivating to reproduce the keys of the optical security systems, and each of them can only deal with one specific security system. In fact, it must be noted that the ultimate aim of cryptanalysis is to retrieve the original plaintext, and key-cracking is just an indirect way which can be quite different for each cryptosystem. Especially, the existing attacks are invalid if each encryption uses different keys [12]. Consequently, it can be interesting to raise the issue of exploring a method that can directly decipher the secret plaintext regardless of the key distributions and encryption principles.

In this work, we propose and demonstrate a method of CPA on the LCT-RPE systems using correlated imaging technique [15–18], which can directly retrieve the secret plaintext without deciphering and knowing the keys. Furthermore, this method is also effective to cryptosystems which are composed of any number of LCT-RPE systems and pixel scrambling operations in random order.

2. The principle of correlated imaging

The setup illustrated in Fig. 1 shows the principle of pseudothermal correlated imaging [16,17]. The speckle field is generated by illuminating a rotating diffuser with a parallel laser beam, and then it is split by a beam splitter into the signal beam and the reference beam. The signal beam passing through the object o is converged by a convex lens L, and the converging spot intensity distribution detected by a 'bucket' detector BD (a single-pixel sensor without spatial resolution) is written as

$$B_i = \int r_i(x, y) o(x, y)\, dx\, dy, \tag{1}$$

of which $r_i(x, y)$ denotes the incident intensity illuminated on the object and $o(x, y)$ is the transmission function of the object. The intensity distribution of the reference beam is directly detected by a CCD camera simultaneously and it is equal to $r_i(x, y)$. By rotating

* Corresponding author. Tel.: +86 451 86418042; fax: +86 451 86414335.
E-mail address: stliu@hit.edu.cn (S. Liu).

http://dx.doi.org/10.1016/j.optcom.2014.10.050
0030-4018/

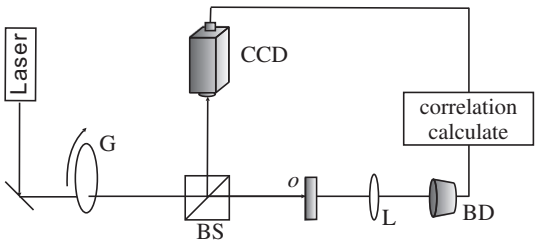

Fig. 1. Optical setup for pseudothermal correlated imaging. G is a controlled rotating ground glass, BS is beam splitter, o is the object, L is a convex lens, BD is a 'bucket' detector.

the diffuser N times, one can detect N pairs of detected intensity which are represented as B_i and $r_i(x, y)$ $(i=1, 2,\ldots,N)$. The final imaging result $o'(x, y)$ is obtained by calculating the normalized second-order correlation of the recorded results, which can be given as [19]

$$o'(x, y) = \frac{\langle r_i(x, y)B_i\rangle}{\langle r(x, y)\rangle\langle B\rangle}, \tag{2}$$

where $\langle r(x, y)\rangle$ and $\langle B\rangle$ indicate the statistical average value which are given by

$$\langle r(x, y)\rangle = \frac{1}{N}\sum_{i=1}^{N} r_i(x, y), \quad \langle B\rangle = \frac{1}{N}\sum_{i=1}^{N} B_i. \tag{3}$$

Based on the introduced imaging technology, we are going to present a CPA scheme to decipher the LCT-RPE systems. In our scheme, N Gaussian random real number matrixes $r_i(x, y)$ $(i = 1, 2, \ldots, N)$ are chosen as the plaintexts, and its corresponding encryption result can be represented as

$$b_i(\xi, \eta) = E\{r_i(x, y)\}, \tag{4}$$

of which the operator 'E{}' indicates the encryption process. The sketch of encryption system is shown in Fig. 2(a). $r_i(x, y)$ and $b_i(\xi, \eta)$ $(i = 1, 2, \ldots, N)$ can be known to the attacker while considering CPA scheme. Now, attacker is assumed to have eavesdropped a ciphertext $a(\xi, \eta)$ indicated by

$$a(\xi, \eta) = E\{o(x, y)\}. \tag{5}$$

To recover the original secret image $o(x, y)$, we use the technique of correlated imaging. Suppose there is a virtual test path setup of correlated imaging plotted in Fig. 2(b). We treat the chosen-plaintexts $r_i(x, y)$ as the speckle fields which illuminates on the object and treat $o(x, y)$ as the transmission function of the object. As $r_i(x, y)$ is already known, according to theory of correlated imaging (see Eq. (2)), the object distribution $o(x, y)$ can only be retrieved by knowing the value of B_i. To calculate the value of B_i, the relationship between $a(\xi, \eta)b_i(\xi, \eta)$ and $r_i(x, y)o(x, y)$ is figured out firstly.

Suppose two optical fields $f(X)$ and $g(X)$ (use 1-D representation here for simplify)are treated as inputs of a linear canonical

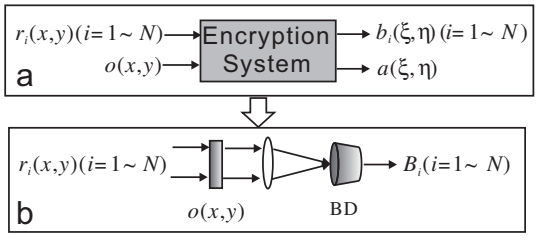

Fig. 2. (a) Sketch of encryption system. (b) Signal path of virtual correlated imaging process.

transform (represented as 'LCT{}'), then the outputs are

$$f_1(X_1) = \mathrm{LCT}\{f(X)\}, \quad g_1(X_1) = \mathrm{LCT}\{g(X)\}. \tag{6}$$

According to the Parseval's theorem of LCT, we have [7]

$$\int f_1(X_1)g_1^*(X_1)\,dX_1 = \int f(X)g^*(X)\,dX, \tag{7}$$

where $*$ denotes the phase conjugation operation. Similarly, if $f(X)$ and $g(X)$ are inputs of random phase encode process (represented as 'RPE{}') as

$$f_2(X_2) = \mathrm{RPE}\{f(X)\}, \quad g_2(X_2) = \mathrm{RPE}\{g(X)\}, \tag{8}$$

suppose the random phase used is $R(X)$, we can obtain a result as

$$\begin{aligned}&\int f_2(X_2)g_2^*(X_2)\,dX_2\\ &= \int f(X)R(X)g^*(X)R^*(X)\,dX\\ &= \int f(X)g^*(X)\,dX.\end{aligned} \tag{9}$$

For a LCT-RPE system (represented as 'E{}') combined with a number of LCTs and RPEs, let $f(X)$ and $g(X)$ are inputs of it, then we have

$$f_c(X_c) = E\{f(X)\}, \quad g_c(X_c) = E\{g(X)\}. \tag{10}$$

By combining Eqs. (6)–(10), it will be straightforward to deduce that

$$\int f_c(X_c)g_c^*(X_c)\,dX_c = \int f(X)g^*(X)\,dX. \tag{11}$$

Therefore, for Eq. (4) and (5), we can draw a conclusion

$$\int a(\xi, \eta)b_i^*(\xi, \eta)\,d\xi\,d\eta = \int o(x, y)r_i(x, y)\,dx\,dy, \tag{12}$$

where $r_i(x, y)$ is equal to $r_i^*(x, y)$ because $r_i(x, y)$ are real number matrixes. From the above equations, we can obtain B_i as

$$B_i = \int a(\xi, \eta)b_i^*(\xi, \eta)\,d\xi\,d\eta. \tag{13}$$

Hence one can obtain the imaging result $o'(x, y)$ by bringing B_i and $r_i(x, y)$ $(i = 1, 2, \ldots, N)$ into Eq. (2). Also one can use compressive correlated imaging proposed in Ref. [20] to get imaging result. Compressive correlated imaging can decrease the needed number of chosen plaintext and increase the quality of attack result. We use compressive correlated imaging in our scheme to evaluate the final imaging result $o'(x, y)$ via a convex optimization. The convex optimization demands that the L_1-norm of a sparse transform of image $o'(x, y)$, $\|\Psi\{o'(x, y)\}\|_{L1}$, minimized, under the constraint of

$$\int r_i(x, y)o'(x, y)\,dx\,dy = B_i, \quad \forall_{i=1\ldots N}, \tag{14}$$

where Ψ is the sparse transform (e.g., the discrete cosine transform, DCT) and $o'(x, y)$ is the reconstructed image. An orthogonal matching pursuit (OMP) algorithm is used as the reconstruction algorithm to solve this optimization problem. The basic idea of this algorithm is to pick columns in a greedy iteration method. At each iteration, we find the column of measurement matrix (which consists of r and the sparse matrix Ψ) that is most strongly correlated with the remaining part (which is the difference between measurement data and approximation data). Then we subtract off its contribution to the measurement data (which is B in this paper) and iterate on the residual. After a number of iterations (which is equal to the sparsity level of the ideal signal after sparse transform normally), then stop and output the approximation signal. The detail process can be found in Ref. [21].