Optics and Laser Technology 109 (2019) 456–464

Contents lists available at ScienceDirect

Optics and Laser Technology

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

Full length article

Hybrid attack free optical cryptosystem based on two random masks and lower upper decomposition with partial pivoting

Y. Xiong, C. Quan*

Department of Mechanical Engineering, National University of Singapore, 9 Engineering Drive 1, Singapore 117576, Singapore

HIGHLIGHTS

- Validated LUDP with partial pivoting to decompose binary image with singular intensity matrix.
- Proposed nonlinear optical cryptosystem using LUDP and two random phase masks.
- Verified algorithm to noise, occlusion, known-plaintext, amplitude-phase retrieval attacks.

ARTICLE INFO

Keywords:
Optical image encryption
Asymmetric cryptosystem
Lower upper decomposition with partial pivoting (LUDP)

ABSTRACT

We propose a novel asymmetric optical image encryption scheme using two random phase masks (RPMs) and lower upper decomposition with partial pivoting (LUDP), in which the encryption process is different from the decryption process and encryption keys are also different from decryption keys. In the proposed algorithm, LUDP is a matrix decomposition operation, which is used to replace the phase-truncated (PT) operation in the encryption path of conventional optical image encryption schemes based on phase-truncated Fourier transform (PTFT). In the proposed decryption process, the original image is completely retrieved by an optical architecture based on the modified 4*f* system with two private keys generated in the encryption process. Compared to conventional PTFT-based cryptosystems which are vulnerable to special attacks based on the amplitude-phase retrieval technique, our proposed algorithm is immune to the iterative attack and has a higher security level. Numerical simulations are presented to demonstrate the feasibility and robustness of the proposed encryption scheme.

1. Introduction

Due to its multiple-dimensional operation and high-speed parallel processing abilities, Optical technique used in information security systems plays an increasingly important role and has drawn much more attention. Since Refregier and Javidi [1] proposed a pioneering scheme named double random phase encoding (DRPE), various schemes using DRPE technique [2–8] have been widely employed in information security systems. Subsequently, formal optical cryptoanalysis has also been carried out to evaluate the security level of optical cryptosystems. It has been found that DRPE-based cryptosystems are vulnerable to various attacks due to their inherent linearity [9–12]. To address the issue, various nonlinear optical schemes based on phase retrieval algorithm [13–17] have been proposed. However, time-consuming iterative processes are involved into these algorithms, making the encryption and decryption processes more complex and difficult to achieved optically. Some other techniques, such as compressive sensing [18–20], interference [21], nonuniform beam [22,23], spherical wave illumination [24], three-dimensional space [25,26], are also employed to build secure image encryption schemes.

Besides the aforementioned methods, an asymmetric cryptosystem based on PTFT proposed by Qin and Peng [27] is one of the most attracting scheme to remove the inherent linearity of DRPE. In a PTFT-based cryptosystem, PT and phase-reserved (PR) operations are used to remove the linearity to ensure the security of the cryptosystem. In addition, decryption keys are generated in the encryption process and each plaintext corresponds to unique decryption keys. Hence, the decryption keys cannot be reused, which guarantees a high-level security. Moreover, two RPMs used as encryption keys are public keys, which can be used to encode different plaintexts. Since then, several optical image encryption techniques based on PTFT have been further developed [28–30]. However, in a PTFT-based cryptosystem, decryption keys are required to be transmitted to the authorized users in every communication, which causes the problem of key distribution.

* Corresponding author.
E-mail address: mpeqcg@nus.edu.sg (C. Quan).

https://doi.org/10.1016/j.optlastec.2018.08.033
Received 22 May 2018; Received in revised form 20 July 2018; Accepted 14 August 2018
0030-3992/ © 2018 Elsevier Ltd. All rights reserved.

Additionally, a PTFT-based cryptosystem has been found vulnerable to various specific attacks based on amplitude-phase retrieval technique [31–34]. Subsequently, some cryptosystems combining PTFT and other techniques have been proposed to resist the existing attacks. The motivation is to increase the number of private keys. For example, a position parameter set is used as an additional private key in the cryptosystem using PTFT and joint transform correlator (JTC) [35]. However, our recent work found that the position parameter set has low key sensitivity and contributes less to security strength [36]. Since the encryption keys RPMs are used as public keys, it provides enough constraints to crack the optical PTFT-based cryptosystem. Hence, some schemes to redesign the public and private key structures have been proposed. Wang and Zhao [37] proposed a cryptosystem using two PTFTs and a random amplitude mask (RAM), in which the plaintext is encrypted by the second PTFT using two encryption keys generated in the process that the RAM is encrypted by the first PTFT. Sui et al [38] proposed a cryptosystem using PTFT and interference, in which two RPMs are used as inputs of interference technique to generate two encryption keys in PTFT. Compared with the classical PTFT scheme, the security level of these cryptosystems has been further improved. However, it has been found these cryptosystems still can be cracked by our proposed attack [39,40].

He et al. [41] have made a comment on the concept of the optical asymmetric cryptosystem in [42]. They claimed that considering the PTFT-based cryptosystem and its derivates as asymmetric cryptosystems is inappropriate and the public and private keys should be independent of the plaintext in a true asymmetric cryptosystem. But in the reply to this comment [43], Liu et al. argued that novel schemes, algorithms according to the special features of the optical systems should be investigated and it is not necessary for optical cryptosystem to follow exactly terminology, structures, and algorithms of general cryptography. In this paper, we proposed a novel cryptosystem based on PTFT scheme in [27] using LUDP. In our proposed algorithm, LUDP is used to replace the PT operation in a PTFT-based scheme. The proposed scheme has some advantages. Firstly, two RPMs used as public keys can be used to encode different plaintexts. Secondly, the proposed encryption process can be easily achieved digitally while the decryption process can be easily implemented optically based on modified 4*f* system. No iterative process is involved in the encryption and decryption process. Thirdly, our proposed algorithm is immune to hybrid attacks, such as noise attack, occlusion attack, known-plaintext attack and special attack based on amplitude-phase retrieval technique.

2. Theoretical analyses

2.1. Principle of LUDP

LUDP [44] is an operation to decompose a square matrix (dimension $N \times N$) into a permuted lower triangular matrix, an upper triangular matrix and a permutation matrix, which can be expressed as

$$P \times A = L \times U \tag{1}$$

where L represents a lower triangular matrix having unit elements on the diagonal and the multipliers below the diagonal, U represents an upper triangular matrix having some coefficients on the diagonal and the multipliers above the diagonal, and P represents a permutation matrix of zeros and ones that in per-multiplying A performs the necessary row exchange. A is a matrix to be decomposed which have the following structure,

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \vdots & \vdots & \vdots & \\ a_{p1} & a_{p2} & \dots & a_{pn} \\ \vdots & \vdots & \vdots & \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix}$$

If the first pivot a_{11} is zero, the *1st* row is permuted with p^{th} row such that $a_{p1} \neq 0$. If there is no row exchange in the matrix A, the permutation matrix P is an identity matrix. From the generation process of the permutation matrix P, it can be seen that the matrix P is a non-singular matrix and the corresponding inverse matrix exists. In addition, the products of LUDP have asymmetric forms and this property can be utilized to image encryption.

An image can be regarded as a matrix with nonnegative scalar entries from the viewpoint of the linear algebra. LUDP is used to extract algebraic features from an image. Hence, an image I can be expressed as:

$$I = P^{-1} \times L \times U \tag{2}$$

where I represents an image to be decomposed, P^{-1} represents an inverse matrix of a permutation matrix.

Compared to the conventional lower upper decomposition without pivoting (LUD), LUDP has two major advantages [44]. Firstly, LUD cannot work on a matrix in which a diagonal coefficient that is equal to 0, which may fail to decompose intensity matrices of binary images. In the LUDP, row interchange is used to rearrange the equations during the reduction to upper triangular form to avoid a zero pivot. Hence, LUDP can be used to decompose a singular matrix. Secondly, partial pivoting can reduce rounding error and improve calculation accuracy. At each stage of Gaussian elimination in LUDP, the pivotal equation is chosen to maximize the absolute value of the pivot. Thus, multipliers in the sequent subtraction process are reduced so that they are all at most one in magnitude. Any rounding errors preset are less likely to be magnified as they permeate the rest of the calculation.

A simulation is carried out to perform LUD and LUDP on the binary image "QR" and the results are shown in Fig. 1. The original image "QR" to be decomposed is shown in Fig. 1(a). The products of LUDP (l_1, u_1 and p_1) are respectively shown in Fig. 1(b)–(d) while the products of LUD (l_2 and p_2) are respectively shown in Fig. 1(e) and (f). The values of pixels on the 1st column and the diagonal in the intensity matrix l_2 are 1 while the pixel values of other columns cannot obtain. The values of pixels on the 1st and 2nd rows in the intensity matrix p_2 are 1 and 0, respectively while the values of pixels on other rows cannot obtain. From Fig. 1(e) and (f), it can be seen that the products of LUD have incorrect structures, which means that LUP fails to decompose the target image. Taking products of LUDP into Eq. (2), the retrieved image I_1 is shown in Fig. 1(g). The retrieved image I_2 using products of LUD is shown in Fig. 1(h) in which all pixel values in the intensity matrix cannot obtain. From the simulation results shown in Fig. 1, it can be seen that LUDP can be used to decompose the binary image which has a singular intensity matrix. Consequently, LUDP can be used in the image encryption system.

2.2. Principle of proposed cryptosystem

The schematic diagram of the proposed cryptosystem is shown in Fig. 2. $R_1(x, y)$ and $R_2(u, v)$ are two random phase masks distributed uniformly in the interval $[0, 2\pi]$. (x, y) and (u, v) are indices of an image in the input and Fourier plane, respectively. The intensity distribution of the plaintext $f(x, y)$is imported to the cryptosystem and the digital image encryption is carried out as follows:

1. A Fourier transform is performed on $f(x, y)R_1(x, y)$and the Fourier spectrum is then divided by LUDP, the intermediate matrix $g(u, v)$ and a private key*Key*1 are given by

$$\begin{aligned} [L_1, U_1, P_1] &= LUDP\{FT[f(x, y)R_1(x, y)]\}, \\ g(u, v) &= P_1^{-1}(u, v), \\ Key1 &= L_1 \times U_1. \end{aligned} \tag{3}$$

where $LUDP\{\cdot\}$ denotes a lower upper decomposition with partial pivoting, $PT\{\cdot\}$ denotes a Fourier transform and $\{\cdot\}^{-1}$ is an operation to obtain the inverse matrix, symbol '×' denotes the matrix multiplication,

Download English Version:

https://daneshyari.com/en/article/11003658

Download Persian Version:

https://daneshyari.com/article/11003658

Daneshyari.com