Optics Communications 313 (2014) 15–21

Contents lists available at ScienceDirect

Optics Communications

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

Hierarchical security system using real-valued data and orthogonal code in Fourier domain

Hyun-Jun Kim [a], Dong-Hoan Seo [b,*], Kwang-Il Hwang [c], Tae-Woo Lim [d]

[a] Department of Electrical and Electronics Engineering, Korea Maritime and Ocean University, Busan, Republic of Korea
[b] Division of Electrical and Electronics Engineering, Korea Maritime and Ocean University, Busan, Republic of Korea
[c] Division of Mechanical and Energy Systems Engineering, Korea Maritime and Ocean University, Busan, Republic of Korea
[d] Division of Marine Engineering, Korea Maritime and Ocean University, Busan, Republic of Korea

ARTICLE INFO

Article history:
Received 30 August 2013
Received in revised form
23 September 2013
Accepted 24 September 2013
Available online 7 October 2013

Keywords:
Optical encryption
Hierarchical system
Orthogonal code
Optical interference principle
Fault-tolerance property

ABSTRACT

We propose a novel hierarchical encryption scheme using orthogonal code in Fourier domain and decryption based on interferometer system. The proposed system is composed of hierarchical ciphertexts with positive real values which can be applied for practical transmission such as Internet, and decryption keys with real valued function which has orthogonal characteristic in the decryption system. Since the original information is encrypted on the Fourier plane, the proposed encryption is more tolerant to loss of key information by scratching or cutting than encryption in a spatial domain. The resulting image using Fourier transform and an interferometer system with constant phase retarder is then decrypted by use of a ciphertext with different security level and each of decryption keys made from the multiplication of orthogonal code and random phase code in order to enhance the level of security. We demonstrate the efficiency of the proposed method and the fault-tolerance properties of data loss through several simulations.

1. Introduction

In recent years, various security systems based on optical processing techniques have received a great deal of attention because of their inherent capability of high-speed and parallel data processing. Many of these systems use double random phase encoding (DRPE) [1], the application of XOR operations [2], computer-generated hologram (CGH) [3,4], phase only mask [5–14], etc. [15,16] for encryption plus a conventional 4-*f* correlator, a joint transform correlator (JTC), or an interferometer system for decryption [9–19]. In the process of the development of optical information security, several encryption schemes using additional security parameters have been proposed that use different domains for placing the encryption keys, such as fractional Fourier transform (FRT), Fresnel transform [20–22]. However, although theoretical and experimental results have demonstrated that these methods are suitable for security applications, many of these systems require an accurately fabricated complex key or a phase only mask obtained by an accurately iterative computation for fine control of the multi-valued phase. Generally, because optical devices such as spatial light modulators (SLMs) employ only either amplitude or phase modulation, they are difficult to accurately display a complex-valued function using current SLM technology. Also, phase only encryption is sensitive to loss of encrypted data caused by external scratching or cutting, and moreover the decryption result can be easily distorted by mechanical vibration and fluctuation. In addition, in practical systems including electronic interfaces, for practical transmission of encrypted images via digital communication channels, these images should be intensity maps with non-negative values. Also, to meet the requirements of modern applications with a high encoding level, a hierarchical access system which provides an established level of protection has recently become important in many security areas. One of the major purposes of hierarchical encryption is that the users in different levels can handle information at a variety of sensitivity levels without disclosing information to an unauthorized person, and the higher-level users can access the information for the lower-level ones and not vice versa. Recently, hierarchical security system based on the correct sequential order and the distance parameters were proposed [6,7]. These techniques provide the identities of the persons by the cascaded structure for the phase keys to generate different verification images. Another approach using hash function and a modified phase retrieval algorithm (MPRA) provides relatively higher security strength by using the multiple factors such as password-controlled phase lock, one-way hash function, and phase key [14]. These image encryption schemes are also sufficiently suitable to be explained as a hierarchical security system. On the other hand, because some of them can retrieve a part of the original information if an unauthorized user steals and analyzes the amplitude or random phase key due to the vulnerability of randomness of encryption key,

* Corresponding author. Tel./fax: +82 51 410 4412.
E-mail address: dhseo@kmou.ac.kr (D.-H. Seo).

0030-4018/$ - see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.optcom.2013.09.057

security systems using orthogonal code which is totally uncorrelated depending on the offset between the codes have been proposed [23,24].

In this paper, to implement a hierarchical encryption system that the high-level users can access the information for the low-level ones and not vice versa, and to guarantee the fault-tolerance properties of data loss, we propose a real positive encryption scheme using orthogonal code in Fourier domain and a simple image decryption using Mach–Zehnder interferometer without any spatial filter. For encryption, an i-th zero-padded original image, multiplied with an i-th random phase image, is Fourier transformed and its real-valued data is expanded and then encrypted by using orthogonal code and positive operator. Moreover, due to the fact that images to be used as the ciphertext have real positive values, the proposed system is useful for practical transmission of ciphertext via digital communication channels. A decryption using interferometer without any spatial filter is simply performed by Fourier transform for the multiplication of decryption key and the interfered wave which is generated by interference of the constant phase retarder wave with the wave passing through the ciphertext. We demonstrate that the feasibility and the robustness against noise attacks of our proposed method are verified by numerical simulations.

2. Encryption process using orthogonal coding scheme in Fourier plane

Here we discuss the theoretical background of the proposed system. let $f_{iz}(x,y)$ and $\exp[jn(x,y)]$ denote an i-th zero-padded original image, which is placed only in a quarter of the input plane, because a mirror image is reconstructed owing to the use of real-valued patterns and a random phase image, respectively, where $n(x,y)$ is a white sequence uniformly distributed in $[0,2\pi]$. First, to assume that the input image is uniformly distributed in the Fourier plane, we multiply this i-th original image by the random phase image and then perform the Fourier transform given by

$$F(\zeta,\ \eta) = \mathrm{FT}\{f_{iz}(x,y)\exp[jn(x,y)]\} \tag{1}$$

where FT{■} denotes the Fourier-transform operation and the subscript i indicates the hierarchical number of the original images to be encrypted. Since the i-th original image is zero-padded and Fourier transformed, the original information can be obtained by Fourier-transforming only the real-part of $F(\zeta,\eta)$ called a real-valued data $F_{i\_real}(\zeta,\eta)$ which is not encrypted but shown as a white noise and which is normalized and distributed in $[-1,1]$.

Here, an i-th expanded data $F_{i\_real}(u,v)$ is obtained by expanding each pixel of this i-th real-valued data to each of $A_\zeta \times A_\eta$ blocks with the same pixel value in order to apply orthogonal coding scheme as the following:

$$F_{i_{real}}[A_\zeta(\zeta-1)+\alpha,\ A_\eta(\eta-1)+\beta] = F_{i_{real}}(\zeta,\eta)$$
$$\alpha = 1,\ 2,\ 3,\cdots,\ A_\zeta, \qquad \beta = 1,\ 2,\ 3,\cdots,\ A_\eta \tag{2}$$

where $[A_\zeta(\zeta-1)+\alpha,\ A_\eta(\eta-1)+\beta]$ denotes the expanded coordinates in Fourier domain, A_ζ and A_η represent expansion coefficients, and for simplicity, variable $[A_\zeta(\zeta-1)+\alpha,\ A_\eta(\eta-1)+\beta]$ is changed into variable (u,v). In other words, because one pixel of $F_{i\_real}(\zeta,\eta)$ is expanded to $A_\zeta \times A_\eta$ pixels of $F_{i\_real}(u,v)$, $F_{i\_real}(u,v)$ can be denoted as a summation of the $A_\zeta \times A_\eta$ slice data in which one pixel of each block has the same value with one pixel of $F_{i\_real}(\zeta,\eta)$ and the other pixels of one have a value of 0 by the linearity of Fourier transform. Also, we use Walsh code to apply orthogonal coding scheme in the encryption process. The Walsh code [25] is a representative technique that can be used to generate orthogonal codes and is generated by applying the Hadamard transform which is a square array with two states either $+1$ or -1, whose rows (or columns) are orthogonal to one another and where the length of the matrix ($N=2n$) enables N orthogonal codes to be obtained, as described below.

$$H_{2n} = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \tag{3}$$

$$H_4 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} = \begin{bmatrix} C_1 \\ C_2 \\ C_3 \\ C_4 \end{bmatrix} \tag{4}$$

where n is a natural number and C_i is a row matrix of orthogonal sequence. Here, except for the code of the first row having a value of only 1 because it can be operated as a DC component in output plane, we perform that each C_i is rearranged into ordered block B_i which has a square matrix of $A_\zeta \times A_\eta$, and each blocks has orthogonal characteristics among each of the other blocks given by

$$\frac{1}{A_\zeta \times A_\eta} B_i B_j = \begin{cases} 0, & i \neq j \\ 1, & i = j \end{cases} \tag{5}$$

and then the i-th coding key $W_i\ (u,v)$ is generated by the orthogonal coding scheme that each blocks is rearranged on a coding key having the same size with an i-th expanded data $F_{i\_real}(u,v)$ and each of the coding keys has the orthogonal characteristics each other by positioning the same block into different area among them. Here we can see that the cross-correlation between any two coding keys, $W_i\ (u,v)$ and $W_j\ (u,v)$ has the value of 0. And each of encrypted data $E_i(u,v)$ is then obtained by the direct pixel to pixel mapping which is generated from the multiplication of the three data, i.e., the i-th expanded data, the i-th coding key, and a random phase-encoded data $\exp[j\pi R_2(u,v)]$ which has a value of $+1$ or -1 to enhance the level of security given by

$$E_i(u,v) = F_{i\_real}(u,v) W_i \exp[j\pi R(u,v)] \tag{6}$$

where this encrypted data is real-valued data which is distributed in $[-1,1]$ and a random phase-encoded data is used for protecting that illegal users analyze the encrypted data, which is composed of the expanded blocks made from the orthogonal coding scheme. Also, for practical transmission of encrypted data via digital communication channels, these encrypted data should be intensity maps with non-negative values. Finally, the i-th ciphertext $\tilde{E}_i(u,v)$ which has the range of variation [0,2] by adding positive operator can be expressed as

$$\tilde{E}_i(u,v) = E_i(u,v) + 1 \tag{7}$$

where 1 is positive operator which can be compensated by constant phase retarder plate in the decryption process. To implement a hierarchical encryption system, the decryption keys with different security level are simply generated by the multiplication of the coding keys and the phase-encoded image $\exp[j\pi R(u,v)]$ which are used in the encryption process, respectively, given by

$$K_1(u,v) = \frac{1}{1} W_1 \exp[j\pi R(u,\ v)]$$

$$K_2(u,v) = \frac{1}{2}(W_1 + W_2)\exp[j\pi R(u,\ v)] = \ \vdots$$

$$K_n(u,v) = \frac{1}{n}\left\{ \sum_{k=1}^{n} W_k(u,\ v) \right\} \exp[j\pi R(u,\ v)] \tag{8}$$

where $1/n$ factor plays the role of normalizing the decryption key and each of these decryption keys, K_1, K_2, K_3,…, K_n, is real-valued data which has a value between $[-1,1]$.