Optics and Lasers in Engineering 57 (2014) 13–19

Contents lists available at ScienceDirect

Optics and Lasers in Engineering

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

# Color information verification system based on singular value decomposition in gyrator transform domains

Muhammad Rafiq Abuturab

*Department of Physics, Maulana Azad College of Engineering and Technology, Patna 801113, India*

ARTICLE INFO

*Article history:*
Received 28 October 2013
Received in revised form
3 December 2013
Accepted 2 January 2014
Available online 28 January 2014

*Keywords:*
Singular value decomposition
Random phase masks
Gyrator transform domains

ABSTRACT

A new color image security system based on singular value decomposition (SVD) in gyrator transform (GT) domains is proposed. In the encryption process, a color image is decomposed into red, green and blue channels. Each channel is independently modulated by random phase masks and then separately gyrator transformed at different parameters. The three gyrator spectra are joined by multiplication to get one gray ciphertext. The ciphertext is separated into *U*, *S*, and *V* parts by SVD. All the three parts are individually gyrator transformed at different transformation angles. The three encoded information can be assigned to different authorized users for highly secure verification. Only when all the authorized users place the *U*, *S*, and *V* parts in correct multiplication order in the verification system, the correct information can be obtained with all the right keys. In the proposed method, SVD offers one-way asymmetrical decomposition algorithm and it is an optimal matrix decomposition in a least-square sense. The transformation angles of GT provide very sensitive additional keys. The pre-generated keys for red, green and blue channels are served as decryption (private) keys. As all the three encrypted parts are the gray scale ciphertexts with stationary white noise distributions, which have camouflage property to some extent. These advantages enhance the security and robustness. Numerical simulations are presented to support the viability of the proposed verification system.



## 1. Introduction

Optical information processing technology has been extensively used in field of information security system because of their multiple parameters and high-speed parallel processing ability. Optical security techniques mainly consist of encryption, recognition, correlation, identification, verification and watermarking. The pioneering work in field of optical image encryption is double-random phase-encoding (DRPE) technique based on the 4-*f* optical correlator to encrypt a primary image into stationary white noise [1]. Other methods based on multiplexing [2], digital holography [3], fractional Fourier domain [4,5], Fresnel domain [6,7], diffractive imaging [8], and polarized light [9] have been proposed. In all these methods, as monochromatic light is used to illuminate a real color image, color information of a retrieved image is lost. Since the color information of an image plays an important role in optical information processing, color image encryption based on an indexed image and DRPE has been proposed [10]. Subsequently this technique has been further developed to increase the security and robustness [11–20].

To the best of my knowledge, most of the color encryption techniques are considered as symmetric cryptosystems in which encryption key is identical to the decryption key. Recently, phase-truncated Fourier transform based asymmetric cryptosystem has been proposed [21]. In this method, encryption cannot be reversed with the encryption keys (public keys) whereas decryption can only be achieved with the decryption keys (private keys). Although, a specific attack method based on an iterative Fourier transform can be applied to break asymmetric cryptosystem when two random phase masks are used as public keys to encode different plaintexts [22]. The asymmetric cryptosystem can be made secure by keeping the encryption keys as private keys or applying different phase keys for different plaintexts during the encryption to evade the known public key attack as well as the specific attack [23–26]. A new image encryption algorithm based on SVD and Arnold transform is proposed [27]. In this scheme, an original image is first transformed in fractional Fourier domain, and then decomposed into three segments by SVD. All the three parts are Arnold transformed at different number of times to obtain three encrypted images. In the decryption process, all the three encrypted parts are inverse Arnold transformed at corresponding times, multiplied in correct order and inverse fractional Fourier transformed with correct fractional orders to reconstruct correct information.

In this paper, for the first time to my knowledge, a new asymmetric cryptosystem using SVD in GT domain is proposed. In encryption process, an input color image is converted into red,

*E-mail address:* rafiq.abuturab@gmail.com

0143-8166/$ - see front matter © 2014 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.optlaseng.2014.01.006

green and blue channels and then multiplied by corresponding random phase masks. The obtained images are gyrator transformed at different transformation angles. The resulting images are combined by multiplication to obtain a single gray ciphertext and then divided into $U$, $S$, and $V$ parts by SVD. Finally, corresponding parts are separately gyrator transformed at different transformation angles. The three gray ciphertexts can be allocated to different permitted users for highly secure authentication. To retrieve original image, the encoded $U$, $S$, and $V$ parts are inverse gyrator transformed at the same encryption parameters, three recovered parts are correctly set to get a gray image, the gray image is individually multiplied with the decryption keys of red, green, and blue channels and corresponding products are inverse gyrator transformed at correct transformation angles to reconstruct red, green, and blue channels. Numerical simulations demonstrate the feasibility of the proposed security system.

Compared to Ref. [27], the proposed method has three advantages. First, this system consists of three asymmetric decryption (private) keys. Second, it provides very high sensitive parameters as three transformation angles of GT. Third, it offers five sensitive-multiplication orders of $U$, $S$, and $V$ parts of SVD. In addition, the MSE values of all parameters are very high for any one incorrect key.

The motivation of this research is to exploit the features of SVD in the proposed verification system. There are three advantages in SVD-based image encryption system: first, the size of the matrices from SVD transformation is not fixed, it is a one-way non-symmetrical decomposition algorithm and is an optimal matrix decomposition in a least-square sense; second, when a small perturbation is added to an image, its singular values do not change significantly; and third, singular values represent intrinsic algebraic image properties [28].

## 2. Theory

### 2.1. Singular value decomposition

The singular value decomposition (SVD) is a numerical technique used to diagonalize matrices. SVD decomposes an $n\times n$ real matrix $A$ into a product of three matrices as

$$A = USV^T = [u_1, u_2, \ldots, \ldots, u_n] \times \begin{bmatrix} \sigma_1 & 0 & \cdots & 0 \\ 0 & \sigma_2 & \cdots & 0 \\ \vdots & 0 & \ddots & 0 \\ 0 & 0 & \ldots & \sigma_n \end{bmatrix} \times [v_1, v_2, \ldots, \ldots, v_n]^T \quad (1)$$

where $S$ is an $n\times n$ diagonal matrix with non-negative real values called singular values. $U$ is an orthogonal matrix and $V^T$ is the transpose of an orthogonal matrix. The columns of $U$ are eigenvectors of $AA^T$ while the columns of $V$ are eigenvectors of $A^TA$. The eigenvalues of $AA^T$ or $A^TA$ are the squares of the singular values for $A$. When $r=\text{rank}[A]$ then $S=\text{diag}(\sigma_1,\sigma,\ldots,\ldots,\sigma_n)$ satisfies $\sigma_1 \geq \sigma_2 \geq \ldots \geq \sigma_r \geq \sigma_{r+1}=\sigma_{r+2}\ldots,\ldots,=\sigma_n=0$ [29].

From the viewpoint of linear algebra, an image can be viewed as a matrix with nonnegative scalar entries. SVD is used to extract algebraic features from an image. Each singular value specifies the luminous of an image, whereas the corresponding pair of signal vectors specifies the geometry of the image. Let $A$ be a matrix whose elements are pixel values of an image. The image can be expressed as

$$A = \sum_{i=1}^{r} \sigma_i u_i v_i^T \quad (2)$$

where $u_i$ and $v_i$ are the $i$th column vectors of $U$ and $V$, respectively.

### 2.2. Gyrator transform

The gyrator transform (GT) of a two-dimensional complex field function $f_i(x_i,y_i)$ at parameter $\alpha$, is defined as [30]

$$f_0(x_0,y_0) = G^{\alpha}[f_i(x_i,y_i)](x_0,y_0) = \frac{1}{|\sin\alpha|}\int\int_{-\infty}^{+\infty} f_i(x_i,y_i) \times \exp\left(i2\pi\frac{(x_0y_0+x_iy_i)\cos\alpha-(x_iy_0+x_0y_i)}{\sin\alpha}\right)dx_idy_i \quad (3)$$

where $G^{\alpha}[]$ indicates GT operator. $(x_i,y_i)$ and $(x_0,y_0)$ are the input and output coordinates, respectively. The GT for large angles $\alpha$ can be realized by an optimized flexible optical system which consists of identical plano-convex cylindrical lenses. The angle $\alpha$ is changed by proper rotation of cylindrical lenses [31]. $G^{\alpha}$ and $G^{2\pi-\alpha}$ are reciprocal transforms which can be applied in optical image encryption. The calculation of discrete GT can be implemented by Fresnel diffraction integral in free space under paraxial approximation [32]. In this computational method, larger computational load is required. Therefore, in this paper, fast algorithm of discrete GT based on convolution operation is used in order to improve computational speed [33]. Recently, gyrator transformed based cryptosystem have been presented for the security of image information [15–20,25,26,34–38].

## 3. Proposed system

The proposed asymmetric color image security system is based on SVD in GT domains. $f_r(x_i,y_i)$, $f_g(x_i,y_i)$ and $f_b(x_i,y_i)$ are, respectively, red, green and blue components of an RGB image $f(x_i,y_i)$.

The encryption algorithm consists of following steps:

First, $f_r(x_i,y_i)$, $f_g(x_i,y_i)$, and $f_b(x_i,y_i)$ are multiplied by random phase masks $\exp[i\phi_R(x_i,y_i)]$ $\exp[i\phi_G(x_i,y_i)]$, and $\exp[i\phi_B(x_i,y_i)]$, respectively. The corresponding randomized images are independently gyrator transformed at transformation angles $\alpha_R$, $\alpha_G$ and $\alpha_B$.

$$g_R(x,y) = G^{\alpha_R}\{f_R(x_i,y_i)\exp[i\phi_R(x_i,y_i)]\} \quad (4)$$

$$g_G(x,y) = G^{\alpha_G}\{f_G(x_i,y_i)\exp[i\phi_G(x_i,y_i)]\} \quad (5)$$

$$g_B(x,y) = G^{\alpha_B}\{f_B(x_i,y_i)\exp[i\phi_B(x_i,y_i)]\} \quad (6)$$

Second, Eqs. (4)–(6) are multiplied to get first encrypted image as

$$E_g(x,y) = g_R(x,y)g_G(x,y)g_B(x,y) \quad (7)$$

Third, $E(x_i,y_i)$ is divided into $U(x,y)$, $S(x,y)$ and $V(x,y)$ parts by using SVD.

$$[U(x,y),S(x,y),V(x,y)] = svd[E_g(x,y)] \quad (8)$$

where $svd$ represents SVD function.

Finally, they are independently gyrator transformed at transformation angles $\alpha_U$, $\alpha_S$ and $\alpha_V$ to get $E_u(x,y)$, $E_S(x,y)$ and $E_s(x,y)$, respectively.

$$E_U(x_0,y_0) = G^{\alpha_U}[U(x,y)] \quad (9)$$

$$E_S(x_0,y_0) = G^{\alpha_S}[S(x,y)] \quad (10)$$

$$E_V(x_0,y_0) = G^{\alpha_V}[V(x,y)] \quad (11)$$

The decryption algorithm consists of following steps:

First, $E_u(x,y)$, $E_S(x,y)$, and $E_V(x,y)$ are separately gyrator transformed at transformation angles $-\alpha_U$, $-\alpha_S$, and $-\alpha_V$, respectively.

$$D_U(x,y) = G^{-\alpha_U}[E_U(x_0,y_0)] \quad (12)$$

$$D_S(x,y) = G^{-\alpha_S}[E_S(x_0,y_0)] \quad (13)$$