Hybrid Color and Grayscale Images Encryption Scheme Based on Quaternion Hartley Transform and Logistic Map in Gyrator Domain

Jianzhong Li*  
Department of Mathematics and Statistics, Hanshan Normal University, Chaozhou, Guangdong 521041, China  

(Received November 19, 2015 : revised January 6, 2016 : accepted January 6, 2016)

A hybrid color and grayscale images encryption scheme based on the quaternion Hartley transform (QHT), the two-dimensional (2D) logistic map, the double random phase encoding (DRPE) in gyrator transform (GT) domain and the three-step phase-shifting interferometry (PSI) is presented. First, we propose a new color image processing tool termed as the quaternion Hartley transform, and we develop an efficient method to calculate the QHT of a quaternion matrix. In the presented encryption scheme, the original color and grayscale images are represented by quaternion algebra and processed holistically in a vector manner using QHT. To enhance the security level, a 2D logistic map-based scrambling technique is designed to permute the complex amplitude, which is formed by the components of the QHT-transformed original images. Subsequently, the scrambled data is encoded by the GT-based DRPE system. For the convenience of storage and transmission, the resulting encrypted signal is recorded as the real-valued interferograms using three-step PSI. The parameters of the scrambling method, the GT orders and the two random phase masks form the keys for decryption of the secret images. Simulation results demonstrate that the proposed scheme has high security level and certain robustness against data loss, noise disturbance and some attacks such as chosen plaintext attack.

Keywords : Quaternion Hartley transform, Two-dimensional logistic map, Gyrator transform, Image encryption  
OCIS codes : (060.4785) Optical security and encryption; (070.2590) ABCD transforms; (100.2000) Digital image processing

I. INTRODUCTION

Optical technology for security applications has received increasing interest in the last few decades [1-3]. In particular, the double random phase encoding (DRPE) [1] technique, in which the image is encoded to be a white noise pattern with two statistically independent random phase masks (RPM), has attracted much attention. The DRPE encryption technique is constructed by using two RPMs as keys: one is located at the input domain and the other is at the Fourier domain. To enlarge the key space, it has been further extended from the Fourier transform domain to the Fresnel transform domain [4, 5], the fractional Fourier transform domain [6], the Gyrator transform (GT) domain [7] and the Hartley transform (HT) domain [8], etc. In these encryption systems, the parameters (e.g. the propagation distance, the fractional order, etc) are introduced and served as extra keys. Since the HT is mathematically equivalent to the Fourier transform but is purely real, it has a computational advantage over the aforementioned transforms for not having to manage the real and imaginary parts [9]. Though most of the DRPE-based encryption techniques are quite robust and secure, the recovered image loses its color information, which is useful in image processing and practical applications, and in decryption since the original image is illuminated with monochromatic light [10].

Using the DRPE technique, Zhang and Karim reported a single-channel encryption algorithm for color image in the Fourier domain [11]. Chen et al. suggested a method using coherent diffractive imaging for optical color-image encryption and synthesis in the Fresnel domain [3]. Joshi et al. [12] have proposed an approach for the encryption of color images via using a fractional Fourier transform. By use of the Arnold transform and an interference method,
a color image encryption technique is proposed in [13]. A method for securing color image based on the Arnold transform and the gyrator transform is reported in [10]. Based on polarization encoding, Nishchal et al. proposed two asymmetric color image cryptosystem techniques [14-15]. Li and Zhao [16] designed a color image encryption method based on the fractional HT. However, the aforementioned encryption methods for color image ignore the potential interactions between different color channels [17, 18]. In these methods, a color image is separated into the three color channels, and encryption is carried out in each channel independently. Recently, quaternion theory [20] has been used in DRPE-based encryption. Based on the discrete quaternion Fourier transform (DQFT) and DRPE, a color image encryption method is reported [17]. With an iterative phase retrieval algorithm, an algorithm to encrypt double color images in quaternion gyrator domain is described [18]. Using quaternion representation, the color image is processed holistically as a vector field rather than as separated color components in both of the two methods. However, the method in [17] is vulnerable to some attacks (such as chosen-plaintext attack, etc) caused by the linearity of the cryptosystem, while the algorithm in [18] has high computational cost due to the phase retrieval iteration process.

In this paper, based on the quaternion Hartley transform (QHT), logistic-based scrambling technique, GT-based DRPE and three-step phase-shifting interferometry (PSI), a novel hybrid color and grayscale image encryption method is presented. In the proposed approach, the QHT is defined and its calculation for a quaternion matrix is developed first. Then a color image and a grayscale image are processed holistically in a vector manner using QHT. To resist an attack such as chosen plaintext attack, the components of the QHT-transformed images are permuted by use of the designed scrambling algorithm based on logistic maps. Since the flexible configuration of the GT based system, which means fixed distances between the generalized lenses and the manipulation of the transformation angle using lens rotation, makes the setup useful for image encryption [19], the GT-based DRPE technique is used to encrypt the images after QHT and permutation. The resulting encrypted signal from the cryptosystem is recorded as interferograms by the interferometer. Numerical simulations have been made for demonstrating the feasibility and performance of this encryption.

II. RELATED BACKGROUND

In this section, we come back to some related theories before extending the traditional HT to the quaternion domain, showing how to calculate the QHT of a quaternion matrix and developing the logistic maps-based scrambling technique, etc.

2.1. Quaternion Number

Quaternions can be viewed as generalizations of complex numbers. A quaternion number can be represented as follows [18]:

\[ q = a + bi + cj + dk, \]

where \( a, b, c, \) and \( d \) are real numbers, and \( i, j, \) and \( k \) are three imaginary units obeying the following rules

\[ i^2 = j^2 = k^2 = ijk = -1, \quad ij = -ji = k, \quad jk = -kj = i, \quad ki = -ik = j. \]

The conjugate and modulus of a quaternion are respectively defined by

\[ q^* = a - bi - cj - dk, \quad |q| = \sqrt{a^2 + b^2 + c^2 + d^2}. \]

When \( a = 0, \) \( q \) is a pure quaternion.

2.2. Hartley Transform

In mathematics, the HT, which transforms real-valued functions to real-valued functions, is an integral transform closely related to the Fourier transform. HT has two main properties: one is that it is a real transform; the other is that it and its inverse transform are identical [21]. Therefore it can have computational advantages over the Fourier transform [21]. The HT [8] of a real function \( f(x, y) \) is defined as

\[ H(u, v) = HT[f(x, y)] = \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} f(x, y) \cos[2\pi(ux + vy)] dx dy, \]

and the inverse Hartley transform (IHT) is defined as

\[ f(x, y) = IHT[H(u, v)] = \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} H(u, v) \cos[2\pi(ux + vy)] du dv, \]

where \( \cos = \cos + \sin, \) \( HT[\cdot] \) and \( IHT[\cdot] \) denote the Hartley and inverse Hartley operators.

2.3. Double Random Phase Encoding in the Gyrator Domain

In mathematics, the GT with respect to parameter \( \alpha \), called as a fractional order [7], of a two-dimensional function \( f(x, y) \) can be expressed as [7, 9]

\[ G_\alpha(p, s) = GT^\alpha[f(x, y)] = \int \int f(x_0, y_0) \exp\left\{ j2\pi \frac{(x_0y_0 + px)\cos \alpha - x_0s - y_0p}{\sin \alpha}\right\} dx_0dy_0, \]

(6)
where the \( G_\alpha(p,s) \) and \( f(x_0,y_0) \) are the output and input of the transform, respectively. \( G^\alpha[t] \) represents gyrator operator. The inverse \( G \) (\( \text{IGT} \)) corresponds to the \( G \) with respect to \( -\alpha \) and is given by

\[
f(x_0, y_0) = \text{IGT}[G_\alpha(p, s)] = G^{-\alpha}[G^\alpha[f(x_0, y_0)]],
\]

where \( \text{IGT}[] \) denotes the inverse gyrator operator. The \( G \) can be achieved either by using an optical system \([9]\) or by using a fast algorithm \([22]\).

In Fig. 1, the optical setup of DRPE in the gyrator domain is shown. Three planes are defined as the input plane, the transform plane, and the output plane. The corresponding coordinates of the three planes are \((x_0,y_0), (p,s)\) and \((x_1,y_1)\), respectively. The two random phase masks \( \text{RPM}_1 \) and \( \text{RPM}_2 \) are represented by \( \exp[j2\pi\phi(x_0,y_0)] \) and \( \exp[j2\pi\phi(p,s)] \), where \( \phi(x_0,y_0) \) and \( \phi(p,s) \) are two random functions distributed uniformly in the interval \([0,1]\). Using a system which is composed of three generalized lenses \( L_1, L_2 \) and \( L_1 \) with fixed equal distances between them, the \( G \) can be implemented optically. \( G \) at order \( \alpha \) is reached by rotation of these lenses \([9]\). In Fig. 1, the dashed block \( \text{GT}_1 \) which contains lenses \( L_1, L_2 \) and \( L_1 \) indicates the first optical \( G \) with respect to \( \alpha_1 \), and the other \( \text{GT}_2 \) containing lenses \( L'_1, L'_2 \) and \( L'_1 \) indicates the second optical \( G \) with respect to \( \alpha_2 \). When the security system is illuminated perpendicularly by a plane wave, the encrypted data \( g(x_1,y_1) \) is obtained at the output plane \([9]\):

\[
g(x_1,y_1) = \text{GT}^{\alpha_2}[\text{GT}^{\alpha_1}[f(x_0,y_0)\exp[j2\pi\phi(x_0,y_0)]]\exp[j2\pi\phi(p,s)]]\).
\]

By applying \( \text{IGT} \) to the encrypted data with the conjugates of \( \text{RPM}_1 \) and \( \text{RPM}_2 \), the decrypted image can be obtained as follows \([9]\):

\[
f'(x_0,y_0) = \text{GT}^{-\alpha_2}[\text{GT}^{-\alpha_1}[g(x_1,y_1)\exp[-j2\pi\phi(p,s)]]\exp[-j2\pi\phi(x_0,y_0)]]
\]

### 2.4. Phase-shifting Interferometry

Since digital holography \([2]\) provides a convenient form of recording the complex encrypted images after passing through the DRPE systems, phase-shifting interferometry is employed to record the complex resulting encrypted signal in the proposed scheme. A variety of PSI techniques have been developed, including three-step, four-step, etc \([23]\).

Let \( A(x,y)\exp[j\psi(x,y)] \) and \( A_\delta \exp[j\delta_\delta] \) be the complex amplitude distributions of the object wave in the recording plane and the reference wave in that plane at the \( k \)-th exposure, respectively. Here, \( \delta_\delta \) is a constant, \( \delta_\delta \) is the phase shift of the reference wave between two adjacent steps and \( k=1,2,\ldots,N \). The \( k \)-th interference pattern \( I_k(x,y) \) can be represented as \([24]\):

\[
I_k(x,y) = A^*(x,y) + A(x,y)\cos[\psi(x,y) - \delta_\delta] + A_\delta^2.
\]

For a known set \{\( \delta_\delta \)\} \((k=1,2,\ldots,N)\), a digital hologram \( U(x,y) \) can be derived as a function \( \{I_3\} \) \([24]\). In the three-frame case, \( N \) is 3. When \( \delta_\delta = 0, \delta_\delta = \pi/2 \) and \( \delta_\delta = \pi \), a digital hologram \( U(x,y) \) from the three interferograms \( I_1, I_2 \) and \( I_3 \) can be expressed as \([24, 25]\)

\[
U(x,y) = ([I_1 - I_3] + j(2I_2 - I_1 - I_3))/(4A).
\]

### 2.5. Logistic Map

Chaos theory is an evolutionary theory, which describes that the nonlinear dynamical systems change from ordered state to disordered state \([26]\). The dynamical systems are established based on various chaos functions such as logistic maps, which are extremely sensitive to the initial conditions. These functions generate iterative values which are completely random in nature. In this paper, the two-dimensional (2D) logistic map is used to make the change of sequence of image pixels. It is defined as \([26]\)

\[
\begin{align*}
X(n+1) &= \varepsilon A X(n)[1 - X(n)] + \rho Y(n) \\
Y(n+1) &= \varepsilon A Y(n)[1 - Y(n)] + \rho X(n)
\end{align*}
\]

The dynamic behavior of 2D logistic is controlled by the parameters \( \varepsilon, \lambda_1, \lambda_2 \) and \( \rho \) shown in Eq. (12). When \( \varepsilon = 4, \rho = 0.1, 0.65 \leq \lambda_1 \leq 0.9 \) and \( 0.65 \leq \lambda_2 < 0.9 \), the dynamical system is in a chaotic state and slight variations of the initial value will yield a drastically different result which is a non-periodic and non-converging sequence over time \([26]\).

## III. Quaternion Hartley Transform

### 3.1. Definition

Due to the non-commutative multiplication property of quaternions, there are different types of QHT that can be defined. In this work, the left-side QHT (QHT\(^L\)) and the right-side QHT (QHT\(^R\)) are defined:
Hybrid Color and Grayscale Images Encryption Scheme Based on Quaternion Hartley … - Jianzhong Li 45

- Left-side QHT:

$$QH_L(u,v) = QHT^L[f_q(x,y)]$$
$$= \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} \mu_q(x,y) \cos[2\pi(ux+vy)]dxdy,$$  \hspace{1cm} (13)

- Right-side QHT:

$$QH_R(u,v) = QHT^R[f_q(x,y)]$$
$$= \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} f_q(x,y) \cos[2\pi(ux+vy)]dxdy,$$  \hspace{1cm} (14)

where \(f_q(x,y)\) is a two-dimensional quaternion function and \(\mu\) is a pure unit quaternion which meets the constraint that \(\mu^2 = -1\). \(QHT^L()\) and \(QHT^R()\) are the left-side QHT and right-side QHT operations, respectively.

Corresponding to QHT, two forms of the inverse QHT (IQHT) are defined as follows

- Left-side IQHT (IQHT^L):

$$f_q(x,y) = IQHT^L[QH_L(u,v)]$$
$$= -\int_{-\infty}^{\infty} \int_{-\infty}^{\infty} \mu QH_L(u,v) \cos[2\pi(ux+vy)]dxdy,$$  \hspace{1cm} (15)

- Right-side IQHT (IQHT^R):

$$f_q(x,y) = IQHT^R[QH_R(u,v)]$$
$$= -\int_{-\infty}^{\infty} \int_{-\infty}^{\infty} QH_R(u,v) \cos[2\pi(ux+vy)]dxdy,$$  \hspace{1cm} (16)

Here, \(IQHT^L()\) and \(IQHT^R()\) are the inverse left-side QHT and right-side QHT operations, respectively. QHT and IQHT are transformation pairs of each other. They ensure that a quaternion function \(f_q(x,y)\) which is transformed into the QHT domain can be reconstructed completely by the inverse process without losing any information.

### 3.2. QHT Calculation

In this sub-section, the method which makes full use of the existing HT algorithm to calculate the QHT of a quaternion matrix is presented. Since the left-side QHT is used in this work, only the calculation method for it is described. By using the HT algorithm, the QHT can be implemented efficiently.

Since \(f_q(x,y)\) is a quaternion function, it can be represented as

$$f_q(x,y) = f_0(x,y) + if_1(x,y) + jf_2(x,y) + kf_3(x,y),$$  \hspace{1cm} (17)

where \(f_0(x,y), f_1(x,y), f_2(x,y)\) and \(f_3(x,y)\) are real value functions.

For left-side QHT, substituting (17) into (13), we have

$$QH_L(u,v) = \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} [f_0(x,y) + if_1(x,y) + jf_2(x,y) + kf_3(x,y)]$$
$$\times \cos[2\pi(ux+vy)]dxdy.$$  \hspace{1cm} (18)

Considering the general unit pure quaternion \(\mu = \xi i + \eta j + \zeta k\ (\xi, \eta \text{ and } \gamma \text{ are real numbers}),\) substituting \(\mu\) into (18) and using the properties of the quaternion shown in Eq. (2), we have

$$QH_L(u,v) = A_0(u,v) + iA_1(u,v) + jA_2(u,v) + kA_3(u,v),$$  \hspace{1cm} (19)

where

$$A_0(u,v) = -\xi HT[f_q(x,y)] - \eta HT[f_q(x,y)] - \gamma HT[f_q(x,y)],$$
$$A_1(u,v) = \xi HT[f_q(x,y)] + \eta HT[f_q(x,y)] - \gamma HT[f_q(x,y)],$$
$$A_2(u,v) = \eta HT[f_q(x,y)] + \gamma HT[f_q(x,y)] - \xi HT[f_q(x,y)],$$
$$A_3(u,v) = \gamma HT[f_q(x,y)] + \xi HT[f_q(x,y)] - \eta HT[f_q(x,y)].$$  \hspace{1cm} (20)

Similarly, applying left-side IQHT to Eq. (19), the reconstructed \(f_q(x,y)\) can be obtained.

$$f_q(x,y) = IQHT^L[QH_L(u,v)]$$
$$= IQHT^L[A_0(u,v) + iA_1(u,v) + jA_2(u,v) + kA_3(u,v)]$$
$$= f_0(x,y) + if_1(x,y) + jf_2(x,y) + kf_3(x,y),$$  \hspace{1cm} (21)

where

$$f_0(x,y) = \xi HT[A_0(u,v)] + \eta HT[A_1(u,v)] + \gamma HT[A_2(u,v)] + \delta HT[A_3(u,v)],$$
$$f_1(x,y) = \gamma HT[A_0(u,v)] - \xi HT[A_1(u,v)] - \eta HT[A_2(u,v)],$$
$$f_2(x,y) = \eta HT[A_0(u,v)] - \gamma HT[A_1(u,v)] - \delta HT[A_2(u,v)],$$
$$f_3(x,y) = \delta HT[A_0(u,v)] - \eta HT[A_1(u,v)] - \gamma HT[A_2(u,v)].$$  \hspace{1cm} (22)

It can be observed from formulas (18)–(22), the left-side QHT and IQHT of a quaternion matrix can be calculated effectively by using the traditional HT and IHT algorithms. Notice that the right-side QHT can be processed in a similar way.
IV. THE 2D LOGISTIC MAP-BASED IMAGE SCRAMBLING METHOD

By using a scrambling technique, He et al. claimed that an optical security system can resist some potential attacks such as chosen plaintext attack [27]. Since the dynamic response of the chaotic system is highly sensitive to the initial values and parameters of chaotic variables, and the chaotic trajectory is unpredictable, a 2D logistic map-based image scrambling technique is proposed to permute the position of image pixels.

Let \( I(m,n) \) be the to-be-permuted image. The scrambling method is described as follows:

1) Calculate the height \( M \) and the width \( N \) of \( I(m,n) \).
2) Initialize \( X(1) \) and \( Y(1) \) randomly and choose an arbitrary natural number \( t \) first, then iteratively generate the chaotic sequences \( X(i) \) and \( Y(i) \) whose lengths both are \( MN+t \) by using Eq. (12). Here, \( i=1, 2, \ldots, MN+t \).
3) Generate two integers \( s_1 \) and \( s_2 \) which are between 1 and \( t \) randomly first. In other words, \( 1 \leq s_1 \leq t \) and \( 1 \leq s_2 \leq t \). Then truncate \( NM \) elements of \( X(i) \) from the \( s_1 \)th element to obtain a chaotic sequence \( L_1=\{X(i), i=s_1, s_1+1, \ldots, s_1+MN-1\} \). Similarly, another chaotic sequence \( L_2=\{Y(i), i=s_2, s_2+1, \ldots, s_2+MN-1\} \) can be obtained by truncating from \( Y(i) \).
4) Compute the chaotic sequences \( L_1 \) and \( L_2 \) using the following equation:
\[
L_1 = 10^dL_1 - \text{round}(10^dL_1), \quad L_2 = 10^dL_2 - \text{round}(10^dL_2),
\]
where \( \text{round}(Z) \) is the operation that rounds the elements of \( Z \) to the nearest integers, and \( d \) is an integer. After calculation, the irregularity and distribution uniformity of the sequences \( L_1 \) and \( L_2 \) can be enhanced, and all the elements of \( L_1 \) and \( L_2 \) are larger than -0.5 and less than 0.5 [28]. That is \(-0.5 < L_1 < 0.5 \) and \(-0.5 < L_2 < 0.5 \).
5) Sort the sequences \( L_1 \) and \( L_2 \) in a certain (ascending or descending) order to obtain two new sequence \( L' \) and \( L'' \) and their corresponding permutation indices \( I'X1 \) and \( I'Y2 \). In \( I'X1 \) and \( I'Y2 \), there are \( MN \) elements respectively. The relations between \( L_1 \) and \( L' \), and between \( L_2 \) and \( L'' \) are \( L' = L_1(I'X_1) \) and \( L'' = L_2(I'Y_2) \), respectively. For example, the \( m^{th} \) element in \( L' \) corresponds to the \( iX1(m) \)th element in \( L_1 \).
6) Map \( I(m,n) \) into a one-dimensional (1D) array \( I' \) using the zigzag algorithm [29]. So the length of \( I' \) is \( MN \).
7) Use the permutation indices \( I'X1 \) and \( I'Y2 \) to permute \( I' \) and the scrambled vector \( I'' \) can be obtained as follows:
\[
I'' = I'(I'X1), \quad I'' = I''(I'Y2).
\]
8) Finally, the scrambled image \( I' \) can be achieved by applying inverse zigzag scan [29] process to \( I'' \).

The inverse image scrambling process is similar to the image scrambling process. In decryption (inverse scrambling process), obtain the permutation indices \( I'X1 \) and \( I'Y2 \) as described in steps (1)-(5) with the same parameters first. Then map the scrambled image \( SI' \) into a 1D vector \( SI'' \) using the zigzag algorithm. Subsequently, permute \( SI'' \) back to their original position using the following equations:
\[
SI''(I'Y2) = SI', \quad SI''(I'X1) = SI''.
\]

Finally, the decrypted image \( DI \) can be retrieved by applying the inverse zigzag algorithm to \( SI'' \). Since the proposed logistic-based scrambling method is highly sensitive to the parameters, including the initial values \( X(1) \) and \( Y(1) \), \( \lambda_1 \), \( \lambda_2 \), \( \alpha_1 \), and \( \alpha_2 \), it offers a huge level of security.

V. THE PROPOSED HYBRID COLOR AND GRAYSCALE IMAGE ENCRYPTION AND DECRYPTION

Let \( f_{RGB}(x,y) \) be a color image with size \( M \times N \) in the RGB color space. In principle, each image pixel of \( f_{RGB}(x,y) \) can be treated as a pure quaternion number with real part equal to zero [17]:
\[
f_q(x, y) = f_{R}(x, y)i + f_{G}(x, y)j + f_{B}(x, y)k,
\]
where \( f_{R}(x, y) \), \( f_{G}(x, y) \), and \( f_{B}(x, y) \) are the red, green, and blue channels of \( f_{RGB}(x,y) \), respectively. By using this representation, each color triple can be treated as a whole unit and be applied in encryption and watermarking [17, 18, 30]. Hence, a color image which is represented by a pure quaternion can be processed holistically in a vector manner using QHT. Furthermore, it should be noticed that a quaternion contains four parts, which results that more than a simple color image can be processed in encryption. For example, the real part of the quaternion matrix can be used to represent a grayscale image while the three imaginary parts represent a color image.

Therefore, based on the QHT, the scrambling method and the GT-based DRPE, a hybrid color and grayscale images encryption scheme is proposed. In the proposed method, the three-step PSI is used to record the encrypted data. The optoelectronic setup of the proposed encryption process is shown in Fig. 2. Supposing \( f_{c}(x,y) \) denotes a grayscale image with size \( M \times N \), the proposed method is described as follows:

1) Normalize \( f_{RGB}(x,y) \) and \( f_{c}(x,y) \) first. To treat the color image and grayscale image in a holistic manner, \( f_{RGB}(x,y) \) and \( f_{c}(x,y) \) are represented by quaternion:

...
Hybrid Color and Grayscale Images Encryption Scheme Based on Quaternion Hartley

2) Apply QHTL to \( q(x,y) \): 
\[
HF(u,v) = QHTL[f_q(x,y)] = A_0(u,v) + iA_1(u,v) + jA_2(u,v) + kA_3(u,v).
\]
Here, \( QHTL \) is the left-side QHT operation. \( A_0, A_1, A_2 \) and \( A_3 \) can be computed by using Eq. (20).

3) With \( A_0, A_1, A_2 \) and \( A_3 \), form a new matrix using the following formula.
\[
AI = \begin{bmatrix} A_0 & A_1 \\ A_2 & A_3 \end{bmatrix}
\]  
(27)
Since the length and width of \( f_{RGB}(x,y) \) and \( f_g(x,y) \) are both \( M\times N \), the size of \( A \) is \( 2M\times 2N \).

4) Permute \( AI \) to obtain \( AIS \) by the proposed chaos-based scrambling method mentioned in Section 4 with the parameters \( \lambda(1), \lambda(1), \lambda(2), s_1 \) and \( s_2 \). That is \( AIS = \text{scramble}(AI, X(1), Y(1), \lambda(1), \lambda(2), s_1, s_2) \). Here scramble() is the scrambling operation.

5) Let \( EA = AIS_1 + jAIS_2 \), where \( AIS_1 = AIS[1:M, 1:2N] \) is the first half part of matrix \( AIS \) and \( AIS_2 = AIS[M+1:2M, 1:2N] \) is the second half part of \( AIS \), respectively. \( EA \) can be regarded as the complex amplitude that will be encrypted by the DRPE technique in the gyrator domain. The size of \( EA \) is \( M\times 2N \).

6) The complex amplitude \( EA \) is multiplied by \( RPM_1 \), mathematically represented by function \( U(x_0,y_0) = EA(x_0,y_0) \exp[j2\pi\phi(x_0,y_0)] \).

7) As shown in Fig. 2, import \( U(x_0,y_0) \) into the first spatial light modulator (SLM) SLM1 which is located in the input plane under the control of the computer, and then optically transformed by first GT at order \( \alpha_1 \). The resulting complex distribution \( U(p,s) \) can be represented by
\[
U_1(p,s) = GT^{\alpha_1}[U(x,y)] = GT^{\alpha_1}[EA(x_0,y_0) \exp[j2\pi\phi(x_0,y_0)]].
\]  
(28)

8) Subsequently, the complex function \( U_1(p,s) \) is multiplied by \( RPM_2 \) displayed on the SLM2 which is located in GT plane, and then optically transformed by second GT at order \( \alpha_2 \). So the object wave becomes
\[
U_2(x_1,y_1) = GT^{\alpha_2}[U_1(p,s) \exp[j2\pi\phi(p,s)]] = A_1(x_1,y_1) \exp[j\psi(x_1,y_1)],
\]  
(29)
where \( A_1(x_1,y_1) \) and \( \psi(x_1,y_1) \) are the amplitude and the phase of \( U(x_1,y_1) \), respectively.

9) For convenience of storage and transmission, the object wave and reference wave overlap to produce real-valued interferograms. As shown in Fig. 2, the resulting encrypted data is recorded as three interference patterns \( I_1, I_2 \) and \( I_3 \) in three-step PSI case mentioned in Sub-section 2.4.

In the encryption process mentioned above, the steps (1)–(6) will be performed digitally. In Fig. 2, \( M1, M2 \) are mirrors, and \( BS1 \) and \( BS2 \) are beam splitters. \( GT1 \) and \( GT2 \) are corresponding to the gyrator transform systems \( GT1 \) and \( GT2 \) shown in Fig. 1, respectively. As shown in Fig. 2, the complex function \( U(x_0,y_0) \) obtained in step (6) and the \( RPM_2 \) are entered into the SLM1 and SLM2 respectively under the control of computer in order to be transformed, respectively. The phase shift \( \delta_k (k=1, 2, 3) \) is introduced by a mirror attached with a Piezoelectric Transducer (PZT) controlled by a computer at the \( k \) exposure [31]. Finally, the resulting encrypted signal is captured and recorded as three interference patterns by a charge coupled device (CCD) which is placed at the output plane of the encryption system. The flowchart of the encryption process is shown in Fig. 3.

The parameters of the proposed encryption method, including \( \lambda(1), \lambda(1), \lambda(2), s_1, s_2 \), \( RPM_1 \), \( RPM_2 \) and the orders of GT \( \alpha_1 \) and \( \alpha_2 \), form a very large key space enhancing the security level of the encryption system. Only when all the right keys are simultaneously used for decryption can the
encrypted data be reconstructed correctly.

The decryption process, which is similar to the encryption process, but in the reversed order is depicted as follows:

1) Using the three interferograms \( I_1, I_2 \) and \( I_3 \), an encrypted digital hologram \( UE(x_1,y_1) \) can be achieved using Eq. (11).
2) Apply a GT to \( UE(x_1,y_1) \) with order \( -\alpha_2 \) and then multiply the obtained complex distribution by the conjugate of the \( RPMI \).
3) Make another GT with order \( -\alpha_1 \) and then multiply the achieved complex distribution by the conjugate of the \( RPMI \). The resulting distribution function is as follows

\[
EA'(x_0,y_0) = GT^{-\alpha_1}[GT^{-\alpha_2}[UE(x_1,y_1)]]
\]

\[
\exp[-j2\varphi(p,s)]\exp[-j2\varphi(x_0,y_0)]
\]

where \( EA(x_0,y_0) \) and \( EA(x_0,y_0) \) are the real part and imaginary part of \( EA(x_0,y_0) \), respectively.
4) With \( EA_1 \) and \( EA_2 \) form a new matrix using the following formula.

\[
AIS' = \frac{EA_1}{EA_2}
\]

5) With the parameters \( \lambda_1, \lambda_2, s_1 \) and \( s_2 \), \( AIS' \) is permuted by the proposed inverse scrambling process mentioned in Section 4 to obtain \( AI' \).
6) First, let \( A''=AI'[1:1,M,1:N] \), \( A''=AI'[1:1,M,N+1:1:N] \), \( A'\prime=AI'[M+1:1,M,1:N] \) and \( A'\prime=AI'[M+1:1,M,N+1:1:N] \). Then let \( HF'(u,v)=A''(u,v)+jA'(u,v) \) and \( HF'(u,v)=A'(u,v) \).
7) Apply IQHT to \( HF'(u,v) \) to achieve \( f_3(x,y) \).

\[
f_3(x,y) = IQHT^{-1}[HF'(u,v)]
\]

\[
= f_3'(x,y) + if_3'(x,y) + if_3'(x,y) + kf_3'(x,y)
\]

8) With the normalized \( f_3''(x,y) \) and \( f_3''(x,y) \) the decrypted color image \( f_3''(x,y) \) and the normalized \( f_3''(x,y) \) is the decrypted grayscale image.

Figure 4 depicts the decryption process. In Fig. 4, \( \text{conj}(RPM2) \) and \( \text{conj}(RPM1) \) are the conjugate of \( RPM2 \) and the conjugate of \( RPM1 \), respectively.

VI. NUMERICAL SIMULATION RESULTS

To verify the feasibility of the proposed encryption technique, numerical simulations are performed on the color image “Peppers” and the grayscale image “Lena”, which sizes are both 512×512, shown in Fig. 5(a) and Fig. 4(b). We carried out tests on a notebook computer with Intel(R) Core(TM) i7-4700HQ CPU @ 2.40GHz and 8G DDR3L and with the MATLAB R2013a. In the experiments, the system parameters are \( \mu=(i+j+k)/15 \), \( \alpha_1=0.92, \alpha_2=0.75, \varphi=4, \rho=0.1 \), \( \lambda(1)=0.24, \lambda(1)=0.67, r=50000, \lambda_1=0.716, \lambda_2=0.881, s_1=12345, s_2=36578 \) and \( d=4 \). To evaluate the performance of image reconstruction quantitatively, the normalized mean square error (NMSE) [18] was used to calculate the similarity between the decrypted image and the original image, which is expressed as

\[
\text{NMSE} = \frac{\sum_{x=1}^{M} \sum_{y=1}^{N} f_3(x,y) - f_3(x,y)}{\sum_{x=1}^{M} \sum_{y=1}^{N} f_3(x,y)} (33)
\]

where, \( f_3(x,y) \) and \( f_3(x,y) \) are the normalized original and decrypted images respectively, and \( M \times N \) is the size of the images.

6.1. Performance of the Encryption System

Using the proposed encryption scheme, the “Peppers” and “Lena” are encrypted and three encrypted interferograms are obtained, which are shown in Figs. 5(e)~5(e). Figs. 5(f)~5(g) display the retrieved color and grayscale images with the correct keys respectively, which are perfect, without any noise or distortion. As shown in Table 1, the NMSE between Figs. 5(a) and Fig. 5(f) and that between Fig. 5(b) and Fig. 5(g) are 1.7017×10^-30 and 1.173×10^-30, respectively.

Now we investigate the sensitivity of retrieved image to small change of the parameters of 2D logistic map-based scrambling technique on the decrypted results. Figure 6 showed the derivation of NMSE versus the parameters \( \lambda(1), \lambda(1), \lambda_1, \lambda_2, s_1 \) and \( s_2 \), respectively. Figs. 7(a)~7(l) show the decrypted color and grayscale images with wrong keys \( \lambda(1)=0.24+1.0 \times 10^{-15}, \lambda(1)=0.67+1.0 \times 10^{-15}, \lambda_1=0.716+1.0 \times 10^{-16}, \lambda_2=0.881-1.0 \times 10^{-16}, s_1=12344 \) and \( s_2=36578 \), respectively.
TABLE 1. Comparison between the NSMEs of the decrypted “Peppers” and “Lena” by use of correct and incorrect keys

| Cases                                      | NSME for Peppers | NSME for Lena |
|--------------------------------------------|------------------|---------------|
| With all correct keys                      | 1.7017×10⁻30     | 1.173×10⁻30   |
| \(X(1) = 0.24 + 1.0 \times 10^{-15}\) with other correct keys | 0.5191           | 0.4662        |
| \(Y(1) = 0.67 - 1.0 \times 10^{-15}\) with other correct keys | 0.5875           | 0.4148        |
| \(\lambda_1 = 0.716 + 1.0 \times 10^{-16}\) with other correct keys | 0.6044           | 0.429         |
| \(\lambda_2 = 0.881 - 1.0 \times 10^{-16}\) with other correct keys | 0.5342           | 0.4982        |
| \(s_1 = 12344\) with other correct keys   | 0.6237           | 0.4327        |
| \(s_2 = 36579\) with other correct keys   | 0.5672           | 0.4787        |
| Lack of RPM1 with other correct keys       | 0.467            | 0.4662        |
| RPM1 shifted by one pixel with other correct keys | 0.5875           | 0.4148        |
| Lack of RPM2 with other correct keys       | 0.6044           | 0.429         |
| RPM2 shifted by one pixel with other correct keys | 0.5342           | 0.4982        |
| \(\alpha_1 = 0.92 + 0.004\) with other correct keys | 0.6             | 0.5831        |
| \(\alpha_2 = 0.75 - 0.004\) with other correct keys | 0.6305           | 0.6169        |

The corresponding NMSEs are listed in the upper part of Table 1. Please note that in the above experiments, the other keys remain correct while a key is changed in decryption. As illustrated in Figs. 6(a)–6(d) and Figs. 7(a)–7(h), we cannot obtain any information from the decryption images visually when the absolute values of deviations of \(X(1)\) and \(Y(1)\) are up to \(10^{-15}\) and those of \(\lambda_1\) and \(\lambda_2\) are up to \(10^{-16}\). In addition, we know from Figs. 6(e)–6(f) and Figs. 7(i)–7(l) that if the parameters \(s_1\) and \(s_2\) are less 1 or more 1 than the correct value, the decrypted images cannot afford any

valid information. From the NMSE values shown in Table 1, it can also be concluded that the decrypted images cannot be recognized even if the keys of the scrambling system are changed slightly. So, the parameters \(X(1), Y(1), \lambda_1, \lambda_2, s_1\) and \(s_2\) are highly sensitive to the proposed method.

In the experiments, one of the two \(RPMs\) was removed or just one of them was shifted transversely by one pixel. The NMSE values of the decrypted images are listed in the middle part of Table 1. Figs. 8(a)–8(b) display the decrypted color and grayscale images, which are totally unrecognizable, with other correct keys but without \(RPM1\). The recovered color and grayscale images, which were obtained from \(RPM1\) shifted transversely by one pixel, are shown in Figs. 8(c)–8(d). These two images cannot be recognized too. The lack of the \(RPM2\) or small changes to \(RPM2\) in the decryption step also leads to similar results which are exhibited in Figs. 8(e)–8(h). Experimental results convincingly demonstrate that both \(RPMs\) are necessary in decryption and that the illegal users cannot access the security system without the \(RPMs\).

To examine the sensitivity of small change of the orders of the GT, the decryption processes are performed by fixing one order and varying the other. The relationship curves between the NMSE and the deviation of the GT order are shown in Fig. 9, in which the deviation ranges from -0.1 to 0.1 and the step is 0.001. As can be seen from Fig. 9, the NMSE value approximates to zero when \(\alpha_1\) or \(\alpha_2\) is correct while the value sharply increases when \(\alpha_1\) or \(\alpha_2\) slightly departs from the correct value, which indicates that any tiny fluctuation will result in false decryption. The NMSE values shown in the lower part of Table 1 also indicate that if the orders of inverse GT are changed by 0.004 from their correct values, the decrypted images are noise-like images as displayed in Fig. 10 and cannot be recognized.

Next we estimate the key space of the proposed encryption
scheme. According to the description of the proposed method, we know that the key space of the cryptosystem consists of the RPMs, the orders of GT and the parameters of 2D logistic map. In addition, the chaotic permutation module is independent from the GT-based DRPE system. In the logistic-based permutation process, the key spaces of the parameters $X(1), Y(1), \lambda_1$, and $\lambda_2$ should be analyzed, which are denoted by $Z_1, Z_2, Z_3, Z_4, Z_5$ and $Z_6$, respectively. In the GT-based DRPE system, the key spaces of $RPM_1$, $RPM_2$ and the orders $\alpha_1$ and $\alpha_2$, should be analyzed, which are denoted by $Z_7, Z_8, Z_9$ and $Z_{10}$ respectively. From Figs. 6(a)–6(d) and Figs. 7(a)–7(h), the parameters $X(1), Y(1), \lambda_1$ and $\lambda_2$ maintain 15, 15, 16 and 16 digits after decimal point respectively, so $Z_1 \times Z_2 \times Z_3 \times Z_4 = 10^{62}$. Since $1 \leq s_1 \leq t$ and $1 \leq s_2 \leq t$, $Z_5 \times Z_6 = t^2$. Therefore, $Z_5 \times Z_6 \times Z_7 \times Z_8 \times Z_9 = t^7 \times 10^{62}$. In our experiments, $Z_5 \times Z_6 \times Z_7 \times Z_8 \times Z_9 = 2.5 \times 10^{71}$ since $t = 50000$. Suppose that 256 levels are chosen for a pixel in initial random functions $\phi(x_0, y_0)$ and $\phi(p, s)$ of $RPM_1$ and $RPM_2$, the two RPMs with size of $M \times 2N$ need to be decoded with $2 \times 256^{M \times 2N}$ attempts. In this case, $M \times N = 512$, so $Z_7 \times Z_8 = 2 \times 256^{12} \times 10^{64}$. Considering the sensitivity to one GT order of encryption system is 0.004, the fractional orders $\alpha_1$ and

![FIG. 6. The NMSEs of the proposed method: (a), (b) the NMSEs for deviation of $X(1)$ and $Y(1)$; (c), (d) the NMSEs for deviation of $\lambda_1$ and $\lambda_2$; (e), (f) the NMSEs for deviation of $s_1$ and $s_2$.](image-url)
Hybrid Color and Grayscale Images Encryption Scheme Based on Quaternion Hartley

Jianzhong Li

FIG. 7. The decrypted color “Peppers” and grayscale “Lena” with: (a), (b) incorrect $\lambda_1=0.24+1.0 \times 10^{-15}$; (c), (d) incorrect $\lambda_1=0.716+1.0 \times 10^{-16}$; (e), (f) incorrect $\lambda_2=0.881-1.0 \times 10^{-16}$; (g), (h) incorrect $s_1=12344$; (k), (l) incorrect $s_2=36579$.

FIG. 8. The decrypted color “Peppers” and grayscale “Lena” with: (a), (b) lack of RPM1; (c), (d) RPM1 is shifted transversely by one pixel; (e), (f) lack of RPM2; (g), (h) RPM2 is shifted transversely by one pixel.

$\alpha_2$ can be varied with steps of 0.001 in fractional orders range [0, 1] [7], which results in $Z_9 \times Z_{10} = (1/0.001)^2 = 10^6$. Therefore, the entire key space of the cryptosystem is $Z_1 \times Z_2 \times Z_3 \times Z_4 \times Z_5 \times Z_6 \times Z_7 \times Z_8 \times Z_{10} = 5 \times 256 \times (10^{17} \times 10^{18}) \approx 256^{312 \times 1024} \times 2^{258}$. As stated in [32], to acquire a high level of security, the size of key space should at least be larger than $2^{100}$. It is apparent that the key space of the proposed encryption system is far larger than $2^{100}$ and enormous enough to resist brute force attack.

6.2. Robustness of the Method Against Attacks

Information loss or noise contamination may occur during data transmission. Now, the robustness of this scheme against occlusion attack which is regarded as data loss is tested. Figure 11(a) shows one of the interferograms occluded by 50%. The recovered images obtained with all correct keys are illustrated in Figs. 11(b)~11(c). It’s well known that Gaussian noise [33] and salt & pepper noise [33] are frequently appearing noises during the information transmission. The robustness test is further verified against noise attacks on the encrypted results. Figure 12(a) is one of the interferograms distorted by Gaussian noise with mean value 0 and standard deviation 20. The corresponding retrieved images are displayed in Figs. 12(b)~12(c). Fig. 12(d) exhibits one of the interferograms damaged by salt & pepper noise with density 0.02 added. Figs. 12(e)~12(f) depicts the corresponding retrieved images. Although all the results shown in Figs. 11(b)~11(c), Figs. 12(b)~12(c) and Figs. 12(e)~12(f) are interfered with seriously by noise and the corresponding NMSEs are big,
has acquired the GT orders resist other attacks if it can resist chosen plaintext attack.

Zhang and Xiao stated that the security system should be distinguished from the DRPE system in such attacks [27]. In addition, the chosen plaintext attack can prevent the attacker from accessing the ciphertext obtained by use of the DRPE system but does not know the parameters of the proposed method can be produced by utilizing the two random phase masks of the proposed method. Using two fake color and gray images as the plaintexts, the two random phase masks are generated by choosing Figs. 13(a)-13(b) as the fake plaintext images and then employed to decrypt the ciphertext of “Peppers” and “Lena”. As shown in Figs. 13(c)-13(d), the retrieved images cannot reveal any information visually. Therefore, the robustness against chosen-ciphertext attack is greatly enhanced because of the suggested logistic-based scrambling technique, which strengthens the nonlinearity in QHT domain. According to [32], the proposed encryption approach can also resist the other attacks mentioned above.

### 6.3. Complexity Analysis

In the numerical simulation, the encrypted results were obtained by computer. So the computational complexity of the proposed encryption technique is calculated. The calculation depends on three main factors. First, to deal with a color image and a grayscale image holistically in a vector manner, the QHT is computed one time. According to the developed calculation method in sub-section 3.2, the QHT can be implemented via calculating HT four times. For an image with size $M \times N$, the cost to compute the HT is $O(MN \log_2 MN)$ [35]. Hence, the complexity of QHT calculation is $O(4MN \log_2 MN)$. Second, to scramble a matrix using the proposed chaos-based technique, the 2D logistic map operation, the round operation, the quicksort operation [36], the zigzag scan operation, the inverse zigzag scan operation and the sequence permutation operation are performed one time, two times, two times, one time, and one time, respectively. As shown in the steps (3) and (4) of the proposed encryption method, the size of the to-be-scrambled matrix $AI$ is $2M \times 2N$ though the sizes of the color image and grayscale image are both $M \times N$. Therefore, the computational cost of the scrambling procedure is $O(2(4MN + t) + 2(4MN + t) + 2(4MN + t) \log_2(4MN + t) + (4MN + t) + (4MN + t) + (4MN + t))$. Here, $t$ is the natural number shown in step (2) of the proposed scrambling method. Since $4MN + t \approx 4MN$ and $\log_2(4MN + t) \approx 2 + \log_2 MN$ as $MN$ tends to infinity, the complexity of the scrambling procedure is $O(8MN \log_2 MN + 4MN)$. The last factor is the complexity of the virtual optical encryption process. In the proposed encryption method, an encrypted interferogram can be obtained after the complex amplitude being modulated two times by use of random phase masks $RPM_1$ and $RPM_2$. The secret images among the noise fluctuation can still be distinguished.

Four attacks, including cipher only attack, known plaintext attack, chosen plaintext attack and chosen ciphertext attack [32], are often used to attack the DRPE-based optical security system to recover the ciphered images. Among these attacks, the chosen-plaintext attack is the most powerful attack [32]. He et al. claimed that permutation techniques can prevent the attacker from accessing the ciphertext obtained from the DRPE system in such attacks [27]. In addition, Zhang and Xiao stated that the security system should resist other attacks if it can resist chosen plaintext attack [32]. For the proposed method, we assume that the attacker has acquired the GT orders $\alpha_1$ and $\alpha_2$ of the GT-based DRPE system but does not know the parameters of the logistic-based scrambling algorithm. Using two fake color and gray images as the plaintexts, the two random phase masks of the proposed method can be produced by utilizing the chosen plaintext attack described in [34]. By use of these achieved keys, the attacker can crack the original ciphertext. Two keys $RPM_{1}'$ and $RPM_{2}'$ are generated by performing one time, two times, two times, one time, and one time, respectively. As shown in the steps (3) and (4) of the proposed encryption method, the size of the to-be-scrambled matrix $AI$ is $2M \times 2N$ though the sizes of the color image and grayscale image are both $M \times N$. Therefore, the computational cost of the scrambling procedure is $O(2(4MN + t) + 2(4MN + t) + 2(4MN + t) \log_2(4MN + t) + (4MN + t) + (4MN + t) + (4MN + t))$. Here, $t$ is the natural number shown in step (2) of the proposed scrambling method. Since $4MN + t \approx 4MN$ and $\log_2(4MN + t) \approx 2 + \log_2 MN$ as $MN$ tends to infinity, the complexity of the scrambling procedure is $O(8MN \log_2 MN + 4MN)$. The last factor is the complexity of the virtual optical encryption process. In the proposed encryption method, an encrypted interferogram can be obtained after the complex amplitude being modulated two times by use of random phase masks $RPM_1$ and $RPM_2$. The secret images among the noise fluctuation can still be distinguished.
transformed two times by use of GT and interfered one time by use of the reference wave. For a matrix with size \( M \times N \), the complexities of GT operation, modulation operation and interference operation are \( O(2MN \log_2 MN) \) [22], \( O(MN) \) [37] and \( O(4MN) \) [37], respectively. Because the size of complex amplitude is \( M \times 2N \), the computational cost of the above process is \( O(3(8MN \log_2 (2MN + 4MN + 8MN)) = O(24MN \log_2 MN + 60MN) \). Thus, the total computational complexity of the proposed encryption scheme is \( O(36MN \log_2 MN + 104MN) \). Since \( O(MN \log_2 MN) > O(MN) \), compared with the quaternion gyrator transform-based image encryption method whose computational complexity is \( O(4000MN \log_2 MN) \) [18], the proposed scheme is more efficient. In the experiments, the execution time for the encrypted results is 6.7728 seconds.

VII. CONCLUSION

In the paper, a novel definition of quaternion Hartley transform and its implementation are presented first. Then a new method for hybrid color and grayscale images encryption is proposed, in which the QHT combined with the developed chaos-based pixel scrambling technique, the GT-based DRPE and the three-step PSI is used to encrypt the color and grayscale images. By use of QHT, a color image and a grayscale image are processed holistically in a vector manner without separating the color image into three channels and manipulating the grayscale image independently, so that the complexity of the security system can be reduced effectively without any reduction of its security. The components of the QHT-transformed original images are combined as the complex amplitude which will be strengthened the nonlinearity by the designed chaos-based scrambling technique and encrypted by the GT-based DRPE technique. In addition, the encrypted interferograms which are recorded by three-step PSI are real-valued, so they are convenient for storage and transmission. One needs to specify all the right keys to recover the original images correctly. Simulation results demonstrate that the proposed scheme has a quite sensitivity to the decryption keys, an enormous key space to resist brute force attack and a good robustness against Gaussian noise, salt & pepper noise and some attacks such as chosen plaintext attack.

ACKNOWLEDGMENT

This work is partly supported by the Natural Science Foundation of Guangdong Province (No. 2014A030310038), the Educational Commission of Guangdong Province (No. 2013KJCX0127), the 2015 Educational Commission of Guangdong Province, the 2015 quality project of Educational Commission of Guangdong Province, the Science and Technology Planning Project of Chaozhou (No. 2013G01) and the Research Fund of Hanshan Normal University (No. LT201201).

REFERENCES

1. P. Refregier and B. Javidi, “Optical image encryption based on input plane and Fourier plane random encoding,” Opt. Lett. 20, 767-769 (1995).
2. E. Tajahuerce, O. Matoba, S. C. Verrall, and B. Javidi, “Optoelectronic information encryption with phase-shifting interferometry,” Appl. Opt. 39, 2313-2320 (2000).
3. I. H. Lee and M. J. Cho, “Double random phase encryption using orthogonal encoding for multiple-image transmission,” J. Opt. Soc. Korea 18, 201-206 (2014).
4. J. C. Zheng and X. Q. Li, “Image authentication using only partial phase information from a double-random-phase-encrypted image in the Fresnel domain,” J. Opt. Soc. Korea 19, 241-247 (2015).
5. S. Yuan, Y. H. Xin, M. T. Liu, S. X. Yao, and X. J. Sun, “An improved method to enhance the security of double random-phase encoding in the Fresnel domain,” Optics & Laser Technology 44, 51-56 (2012).
6. N. K. Nischal, J. Joseph, and K. Singh, “Securing information using fractional Fourier transform in digital holography,” Opt. Commun. 235, 253-259 (2004).
7. Q. Wang, Q. Guo, and L. Lei, “Double image encryption based on phase-amplitude mixed encoding and multistage phase encoding in gyration transform domains,” Optics & Laser Technology 48, 267-279 (2013).
8. I. Muniraj, C. L. Guo, B. G. Lee, and J. T. Sheridan, “Interferometry based multispectral photolimited 2D and 3D integral image encryption employing the Hartley transform,” Opt. Express 23, 15907-15920 (2015).
9. N. Sundararajan, “2-D Hartley transforms,” Geophysics 60, 262-267 (1995).
10. M. R. Abuturab, “Securing color information using Arnold transform in gyrator transform domain,” Optics and Lasers in Engineering 50, 772-779 (2012).
11. S. Q. Zhang and M. A. Karim, “Color image encryption using double random phase encoding,” Microwave Opt. Technol. Lett. 21, 318-323 (1999).
12. M. Joshi, C. Shakher, and K. Singh, “Color image encryption and decryption for twin images in fractional Fourier domain,” Opt. Commun. 281, 5713-5720 (2008).
13. W. Chen, C. Quan, and C. Tay, “Optical color image encryption based on Arnold transform and interference method,” Opt. Commun. 282, 3680-3685 (2009).
14. S. K. Rajput and N. K. Nishchal, “Asymmetric color cryptosystem using polarization selective diffractive optical element and structured phase mask,” Appl. Opt. 51, 5377-5386 (2012).
15. I. Mehra and N. K. Nishchal, “Image fusion using wavelet transform and its application to asymmetric cryptosystem and hiding,” Opt. Express 22, 5474-5482 (2014).
16. X. X. Li and D. M. Zhao, “Optical color image encryption with redefined fractional Hartley transform,” Optik 121, 673-677 (2010).
17. X. L. Wang, H. C. Zhai, Z. L. Li, and Q. Ge, “Double
random-phase encryption based on discrete quaternion Fourier-transforms,” Optik 122, 1856-1859 (2011).
18. Z. H. Shao, H. Z. Shu, J. S. Wu, Z. F. Dong, G. Coatrieux, and J. L. Coatrieux, “Double color image encryption using iterative phase retrieval algorithm in quaternion gyrator domain,” Opt. Express 22, 4932-4943 (2014).
19. M. R. Abuturab, “Generalized Arnold map-based optical multiple color-image encoding in gyrator transform domain,” Opt. Commun. 343, 157-171 (2015).
20. W. R. Hamilton, Elements of Quaternions (Cambridge University Press, Cambridge, UK, 2009), Chapter 2.
21. N. Gupta and D. K. Saxena, “Implementation and contrasting comparision of transform techniques of OFDM,” International Journal of Computer Applications 72, 47-51 (2013).
22. Z. J. Liu, D. Z. Chen, J. P. Ma, S. Y. Wei, Y. L. Zhang, J. M. Dai, and S. T. Liu, “Fast algorithm of discrete gyrator transform based on convolution operation,” Optik 122, 864-867 (2011).
23. S. Zhang, D. V. D. Weide, and J. Oliver, “Superfast phase-shifting method for 3-D shape measurement,” Opt. Express 18, 9684-9689 (2010).
24. L. Z. Cai, Q. Liu, and X. L. Yang, “Phase-shift extraction and wave-front reconstruction in phase-shifting interferometry with arbitrary phase steps,” Opt. Lett. 28, 1808-1810 (2003).
25. L. Z. Cai, M. Z. He, Q. Liu, and X. L. Yang, “Digital image encryption and watermarking by phase-shifting interferometry,” Appl. Opt. 43, 3078-3084 (2004).
26. D. M. Chen, Y. M. Liu, X. D. Chen, Y. P. Chang, and J. Wang, “A novel chaotic map and DES based file encryption algorithm,” International Journal of Advancements in Computing Technology 3, 198-205 (2011).
27. M. Z. He, Q. F. Tan, L. C. Cao, Q. S. He, and G. F. Jin, “Security enhanced optical encryption system by random phase key and permutation key,” Opt. Express 17, 22462-22473 (2009).
28. Y. Wang, D. L. Zheng, and L. Ju, “Digital image encryption algorithm based on three-dimension Lorenz chaos,” Journal of University of Science and Technology Beijing 26, 678-682 (2004). (in Chinese)
29. M. Smila and S. Sankar, “Novel algorithms for finding an optimal scanning path for JPEG image compression,” IJETCSE 8, 230-236 (2014).
30. T. K. Tsui, X. P. Zhang, and D. Androutsos, “Color image watermarking using multidimensional Fourier transforms,” IEEE Trans. Inform. Forensics Secur. 3, 16-28 (2008).
31. X. G. Wang and D. M. Zhao, “Image encryption based on anamorphic fractional Fourier transform and three-step phase-shifting interferometry,” Opt. Commun. 268, 240-244 (2006).
32. Y. Zhang and D. Xiao, “Double optical image encryption using discrete Chirikov standard map and chaos-based fractional random transform,” Opt. Lasers Eng. 51, 472-480 (2013).
33. R. C. Gonzalez and R. E. Woods, Digital Image Processing, 3rd ed. (Prentice Hall, New Jersey, USA, 2007), Chapter 5.
34. X. Peng, H. Z. Wei, and P. Zhang, “Chosen-plaintext attack on lensless double-random phase encoding in the Fresnel domain,” Opt. Lett. 31, 3261-3263 (2006).
35. P. Rajavel, “Directional Hartley transform and content based image retrieval,” Signal Processing 90, 1267-1278 (2010).
36. C. B. Li, Data Structure (Tsinghua University Press, Beijing, PRC, 2013), Chapter 9. (in Chinese)
37. X. Su, “Virtual optical encryption system based on coupling sawtooth spatiotemporal chaos,” Master Thesis, Nanjing University of Posts and Telecommunications (2014). (in Chinese)