Color Image Encryption Using Angular Graph Fourier Transform

Liuqing Yang, Beijing Forestry University, Engineering Research Center for Forestry-Oriented Intelligent Information Processing of National Forestry and Grassland Administration, China
Wei Meng, Beijing Forestry University, Engineering Research Center for Forestry-oriented Intelligent Information Processing of National Forestry and Grassland Administration, China
Xudong Zhao, Beijing Institute of Technology, China

https://orcid.org/0000-0002-6942-136X

ABSTRACT

In this paper, an angular graph Fourier transform (AGFT) is introduced to encrypt color images with their intrinsic structures. The graph Fourier transform (GFT) is extended to the AGFT and proven to have the desired properties of angular transform and graph transform. In the proposed encryption method, color images are encoded by DNA sequences and confused under the control of chaotic key streams firstly. Secondly, sparse decomposition based on the random walk is applied to scramble pixels spatially, and a series of sub-images are obtained. This step increases encryption efficiency. Finally, the intrinsic sub-image structure is reflected by graphs, and the signals on different subgraphs are transformed into different AGFT domains with particular angular parameters, which makes the proposed method relevant to the original image structure and enhances security. The experimental results demonstrate that the proposed algorithm can resist various potential attacks and achieve better performance than the state-of-the-art algorithms.

KEYWORDS

Angular Transform, Chaotic Sequence, DNA Coding, Graph Fourier Transform, Graph Signal Processing, Image Encryption, Random Walk, Sparse Decomposition

1. INTRODUCTION

With the development of the Internet, smartphones and cellular networks, the transmitting of secure information has been becoming vital. Since images carry sensitive information and transmit in public environments universally, data protection such as image encryption represents a significant portion of the research undertaken nowadays (Artiles et al., 2019; Chen et al., 2018; Ding et al., 2018; Chen et al., 2018). Optical systems with transforms are of growing interest for image encryption because of their distinct advantages of processing two-dimensional data in parallel and at high speed (Javidi et al., 1995; Chen et al., 2006; Huang et al., 2016). Among them, double random phase encryption (DRPE) proposed by Refregier and Javidi is the most widely used encryption scheme (Liu et al., 2001). This method uses two random phase masks to encrypt the original image, one in the input plane and the other in the Fourier plane. Afterwards, to increase the security of the classical DRPE, some transforms have been used to instead of the Fourier transform such as the fractional Fourier transform (Unnikrishnan et al., 2000; Annaby et al., 2016).
These improved algorithms have shown their advantages in image security. However, because they are independent of plaintext, the encryption techniques based on transforms have been proven to be vulnerable to chosen-ciphertext, known-plaintext, chosen-plaintext attacks (Wu et al., 2015; Rajput et al., 2013; Peng et al., 2006; Carnicer et al., 2005). Although several enhancement strategies have been proposed to avoid this vulnerability (Alfalou et al., 2013; Kumar et al., 2009; Dong et al., 2008), the security of transforms themselves have been threatened by a ciphertext-only attack with the phase retrieval algorithm (Liao et al., 2017; Guo et al., 2016). Relating the transform with plaintext and its relevant information is efficient to enhance security under cryptographic attacks.

As an efficient model, the graph Fourier transform (GFT) (Sandryhaila et al., 2013; Shuman et al., 2013) enables us to analyze the structural data sets described by graphs. Recently, the graph spectral interpretation of traditional 2D images has been researched and demonstrated advancement in some digital image processing areas, such as image compression (Shen et al., 2010), restoration (Liu et al., 2015) and filtering (Chen et al., 2015). Since the underlying graphs reveal signal structures and the signal samples at vertexes are analyzed for their correlation and similarity, the graph transforms are naturally related with plaintexts and can enhance the security under plaintext attack and ciphertext attack. So far, there are only a few methods using graph signal processing methods for gray-level image encryption (Fracastoro et al., 2017; Sharm et al., 2018; Gondim et al., 2019), and color image encryption is even not researched. When the GFT is used for encryption, the problem appears that the parameters are fixed for the whole image, which can not provide large parameter space. Meanwhile, the energy of encrypted images is still assembled in particular intervals, which makes the transformed signal non-uniform and vulnerable for different attacks.

In this paper, an angular graph Fourier transform (AGFT) is introduced to encrypt color images with their intrinsic structures. To enlarge parameter space, the GFT is extended to the AGFT which has the desired multiple-parameter property of angular transform and the structural-related property of graph transform. Then, an image encryption method based on the AGFT is proposed to encrypt images with their intrinsic structures for better security. In the proposed encryption method, color images are encoded by DNA sequences, and the DNA encoded diffused image is confused under the control of the spatiotemporal chaotic key streams firstly. Then, a color image is decomposed into several sparse sub-images. Since these sub-images comprise random walk paths reflecting pixels correlation of image, this step improves the randomness of spatial distribution. Afterwards, the Laplacian matrix is used to indicate the underlying graph structure, which makes the encryption process not only related to the transform operator but also related to the intrinsic image structure. Thus, the security of the proposed algorithm under plaintext attacks is enhanced. Then, the signals are transformed into the AGFT domains with different angular parameters, which determine the energy distribution of the original signal on eigenvectors and control the uniformity of signal energy distribution. Finally, the experimental results demonstrate that the proposed algorithm significantly enhances data security and achieves better performance than state-of-art algorithms.

The outline of this paper is as follows. Related works are first discussed in Section II. Preliminary work is firstly discussed in Section III. Then the angular graph Fourier transform and its properties are presented in Section IV. The image encryption algorithm based on the AGFT is discussed in Section V. Finally, experimental results and conclusions are presented in Section VI and Section VII, respectively.

2. RELATED WORKS

To achieve security in data transfer, new encryption techniques have been developed recently including cryptosystems based on chaos (Chai et al., 2017; Li et al., 2017; Belazi et al., 2016), DNA computing (Zhen et al., 2016; Kumar et al., 2016), fractional transforms (Unnikrishnan et al., 2000; Annaby et al., 2016). Among those methods, spatial encryption methods based on the chaos system have attracted extensive concerns for the close connection between chaos and encryption. However, discrete chaotic
systems will become periodic eventually and can cause a harmful effect in higher dimensional chaotic systems (Wheeler et al., 1989; Corless et al., 1991). To overcome the short period issue existing in discrete chaotic system, spatiotemporal chaotic system with longer period such as Logistic-Sine system (LSS) in the coupled map lattice (CML) (Wang et al., 2015), Mixed Linear Nonlinear Coupled Map Lattices (MLNCML) system (Tao et al., 2007). But the image encryption system only using a chaotic system has less security, and other new mechanisms are needed for enhancing the security. DNA technology has been infiltrated into a chaotic cryptosystem to double assurance the security of image cryptosystem due to extraordinary information density. A new encryption system based on the multiple improved chaotic systems for color image performs well (Wu et al., 2015). Kong presented a new technique based on a chaotic system, cellular automation, and DNA (Zhen et al., 2016). In (Hu et al., 2017), the DNA deletion and DNA insertion pseudo-operations are used to confuse the DNA encoded diffused image under the control of the key streams. But the common DNA operations can only diffuse the DNA-encoded image (Huang et al., 2014). Further, the DNA methods have low sensitivity to plain text.

To overcome the periodic problem and enhance security, fractional transform-based methods are proposed. Transform domain encryption methods themselves (for example, the fractional Fourier transform (Annaby et al., 2016), the fractional Hartley transform (Singh et al., 2017; Liu et al., 2010; Kang et al., 2017) and the discrete fractional angular transform (DFAT) (Liu et al., 2008), etc.) cannot directly achieve the effect of image encryption. To achieve this purpose, it is often necessary to combine some other pixel scrambling method. Liu (Liu et al., 2005) defines a stochastic discrete fractional transformation. The eigenvalues are similar to the fractional Fourier transform while the eigenvectors are taken from the eigenvectors of a symmetric random matrix. In (Liu et al., 2008), a discrete fractional angular transform (DFAT) with two parameters angle and factional order, which determine the eigenvalues and eigenvalues, respectively, has been proposed for fast image encryption. Then a double image encryption algorithm is designed based on Arnold transform and DFAT, where the parameters of transforms serve as the additional keys for enhancing the security (Liu et al., 2012). These angular transforms have larger key spaces and a higher level of security. However, the transforms still have the problem calculating the transformation kernel function repeatedly for the order change and lead to low security under plaintext attacks. To enhance the security under plaintext attack and ciphertext attack, a graph wavelet transform-based steganography using graph signal processing (GSP) is presented, which results in better visual quality image and extracts secret image (Sharm et al., 2018). So far, there are only a few methods using graph signal processing methods for gray-level image encryption (Gondim et al., 2019), and color image encryption is even not researched. But the GFT methods used for encryption cannot provide large parameter space and vulnerable for different attacks.

Combing the advantages of DNA coding, angular transform and graph transform and compare the proposed AGFT with other competitive encryption approaches, the main contributions are summarized as follows.

1. The GFT is extended to the AGFT which has the desired multiple-parameter property of angular transform and the structural-related property of graph transform. The AGFT can provide detailed information on signals for potential analysis. Considering both the pixels intensity and the intrinsic structure, the AGFT can enhance security under cryptographic attacks.
2. An image encryption method based on the AGFT and DNA coding is proposed to encrypt images with their intrinsic structures, which enhances data security and achieves better performance than the state-of-art algorithms.
3. PRELIMINARIES

An undirected, connected, weighted graph is defined as $G = \{V, E, W\}$, where $V$ is a finite set of vertices with $|V| = N$, $E$ is a set of edges, and $W$ is a weighted adjacency matrix (Chung, 1996). A signal $f : V \rightarrow \mathbb{R}$ defined on the vertices of the graph is represented as a vector $f \in \mathbb{R}^N$, where the $n$th component of the vector $f$ represents the signal value at the $n$th vertex in $V$. The non-normalized graph Laplacian is defined as $L := D - W$, where $D$ is the diagonal degree matrix with $d$ being the diagonal elements of $D$, $d_n = \sum_{m=0}^{N} W_{mn}$ is the degree of vertex $n$. As the graph Laplacian $L$ is a real symmetric matrix, it has a complete set of orthonormal eigenvectors, which are denoted by $\{v_i\}_{i=0,1,...,N-1}$. Then the associated real, nonnegative Laplacian eigenvalues are ordered as $0 = \lambda_0 < \lambda_1 \leq \lambda_2 \leq \ldots \leq \lambda_{N-1} = \lambda_{\text{max}}$.

The eigenvectors of the Laplacian matrix are then used to define the GFT. Formally, for any signal $f \in \mathbb{R}^N$ residing on the vertices of $G$, its GFT is defined in (Sandryhaila et al., 2013) as

$$\hat{f}(l) = \langle v_l, f \rangle = \sum_{n=0}^{N} v_l^*(n)f(n), l = 0,1,...,N-1. \quad (1)$$

The inverse GFT follows as

$$f(n) = \sum_{l=0}^{N-1} \hat{f}(l)v_l(n), n = 1,2,...,N. \quad (2)$$

4. THE PROPOSED ANGULAR GRAPH FOURIER TRANSFORM

The proposed AGFT has the desired multiple-parameter property of angular transform (Liu et al., 2008; Liu et al., 2012) and the structural-related property of graph transform (GFT) (Sandryhaila et al., 2013; Shuman et al., 2013). Furthermore, the proposed AGFT also possesses other excellent properties.

4.1. Definition

Given the eigenvalues $\lambda_k$ and the eigenvectors $v(k)$ of $L$ corresponding to the GFT, any other bases of the corresponding eigenspace can be defined by rotating the vectors $V_N$ as $V_N^\theta = R^\theta N V_N$, where the angle $\theta$ is the main variable in $V_N^\theta$ (Fracastoro et al., 2017). The eigenvectors $V_N^\theta$ of the AGFT are determined by the angular variables $\theta$ and the eigenvectors. Similar to the GFT in Equation1, the AGFT of graph signal $f$ can be expressed as $\hat{f} = (V_N^\theta)^{-1}f$.

To introduce the eigenvectors $V_N^\theta$ of the new transform AGFT, the rotation matrix $R(\theta)$ (Liu et al., 2008) is researched first. If $R$ is an orthogonal matrix, the matrix

$$R_{2N} = \frac{1}{\sqrt{2}} \begin{bmatrix} R_N & R_N^* \\ -R_N^* & R_N \end{bmatrix} \quad (3)$$
and

\[
R_{2N+1} = \frac{1}{\sqrt{2}} \begin{bmatrix}
R_N & R_N & \frac{R_0}{\sqrt{2}}
R_0 & R_0 & \frac{R_0}{\sqrt{2}}
-R_N & R_N & \frac{R_0}{\sqrt{2}}
\end{bmatrix}
\]  

(4)

are both orthogonal matrices. The matrix \( R_N \) is defined by upside down the matrix \( R_N \), \( R_0 \) is a \( 1 \times N \) zero vector. Then the matrix \( R_N \) and \( R_{2N} \) (or \( R_{2N+1} \)) can define the eigenvector matrix. For all \( 2 \times 2 \) matrix, the matrix

\[
R_2^\theta = \begin{bmatrix}
\cos \theta & \sin \theta \\
-\sin \theta & \cos \theta
\end{bmatrix}
\]  

(5)

is an orthogonal matrix. \( R_2^\theta \) can also be considered as a coordinate rotation matrix. Similarly, the matrix \( R_3^\theta \) is a kind of special orthogonal matrix

\[
R_3^\theta = \begin{bmatrix}
\cos \theta & \sin \theta & 0 \\
0 & 0 & 1 \\
-\sin \theta & \cos \theta & 0
\end{bmatrix}
\]  

(6)

The construction methods of \( R_{2N}^\theta \) and \( R_{2N+1}^\theta \) are similar with \( R_2^\theta \) and \( R_3^\theta \) respectively. Through Equation 3-Equation 6, the orthogonal angle matrix of any other dimensions can be computed iteratively. Therefore, arbitrary \( R_N^\theta (N > 3) \) can be computed by a similar process. A new AGFT operator is obtained by rotating the corresponding eigenvectors of the eigenvector matrix of the graph Laplacian

\[
V_N^\theta = R_N^\theta V_N.
\]  

(7)

Take \( V_2^\theta \) and \( V_3^\theta \) as examples

\[
\begin{bmatrix} v_1^\theta \\ v_2^\theta \end{bmatrix} = \begin{bmatrix}
\cos \theta & \sin \theta \\
-\sin \theta & \cos \theta
\end{bmatrix} \begin{bmatrix} v_1 \\ v_2 \end{bmatrix}
\]  

(8)

\[
\begin{bmatrix} v_1^\theta \\ v_2^\theta \\ v_3^\theta \end{bmatrix} = \begin{bmatrix}
\cos \theta & \sin \theta & 0 \\
0 & 0 & 1 \\
-\sin \theta & \cos \theta & 0
\end{bmatrix} \begin{bmatrix} v_1 \\ v_2 \\ v_3 \end{bmatrix}
\]  

(9)
where \( \theta \) is an angle between \([0, 2\pi]\). For the eigenvalues \( \{\lambda_l\}_{l=0,1,\ldots,N-1} \) of the Laplacian matrix, the eigenvectors are rotated corresponding to them. A new eigenvector matrix \( V_N^\theta \in \mathbb{R}^{N \times N} \) can be obtained by replacing the vector \( v_N \) with a rotated vector \( v_N^\theta \), where eigenvectors are represented as \( \{v_l\}_{l=0,1,\ldots,N-1} \), the vector \( \theta \in \mathbb{R}^N \) contains all the angles used. Particularly, the GFT matrix is \( (V_N^\theta)^{-1} = (V_N^0)^{-1} \in \mathbb{R}^{N \times N} \). The rotation matrix \( R_N^\theta \in \mathbb{R}^{N \times N} \) is defined by Equation 3-Equation 6. When a signal on the graph \( x \in \mathbb{R}^N \) is given, its AGFT \( x^\theta \in \mathbb{R}^N \) can be defined as

\[
\hat{x}^\theta = \langle v_l^\theta, x \rangle = \sum_{n=0}^{N-1} [v_l^\theta(n)]^* x(n), \quad l = 0, 1, \ldots, N - 1. \tag{10}
\]

Equation 10 can be seen as the expansion of signal \( x \) in terms of the eigenfunction of the rotated Laplacian operator.

The inverse of the AGFT can be defined as

\[
x(n) = \sum_{l=0}^{N-1} \hat{x}^\theta(l)v_l^\theta(n), \quad n = 1, 2, \ldots, N, \tag{11}
\]

where \( x(n) \) means the synthesis of all the spectral components.

### 4.2. Properties

In this section, some properties of the proposed AGFT are presented as follows.

**Invertibility:** From Equation 10 and Equation 11, the AGFT is proved to be an invertible operator.

\[
(V_N^\theta)^T (V_N^\theta) = (R_N^\theta V)^T (R_N^\theta V)
= V^T (R_N^\theta)^T R_N^\theta V
= V^T V = I, \tag{12}
\]

where \( T \) denotes the transpose operation.

2. **Linearity:** The AGFT satisfies the superposition principle and is a linear transform.

\[
F_N^\theta \{af(x) + bf(y)\} = (V_N^\theta)^{-1} \{af(x) + bf(y)\}
= a(V_N^0)^{-1} f(x) + b(V_N^\theta)^{-1} f(y)
= aF_N^0 f(x) + bF_N^\theta f(y). \tag{13}
\]

3. **Periodicity:** For the eigenvectors are periodic functions of \( \theta \), the AGFT satisfies multiplicity

\[
F_N^\theta = F_N^{\theta + 2\pi}. \tag{14}
\]
4. Parseval: From the geometric point of view, the AGFT represents rotation on the spectral plane. The rotation keeps the total energy of signals in the eigen-space

\[ \sum_{n=1}^{N} |\hat{x}_n|^2 = \sum_{n=1}^{N} |\hat{x}_n^\theta|^2. \]  

(15)

Besides, the proposed AGFT has the desired multiple-parameter property of angular transform and the structural property of the graph transform. It is completed by the eigendecomposition of the Laplacian matrix and rotation of eigenvectors of the GFT. The first step uses the underlying graph structure information of the original data. The information includes the weights matrix and coordinates, whose random parameters can be used as the private keys in image encryption. The relevance of AGFT with the data structure is guaranteed by the random weights matrices \( W \). The rotation of eigenvectors of the GFT, as Equation 7 shown, has introduced angular parameter \( \theta \) which can be used as the private keys in image encryption. These random parameters can extend the key space of encryption.

5. IMAGE ENCRYPTION ALGORITHM BASED ON THE AGFT

In this section, an image encryption method is proposed based on the proposed AGFT, which encrypts images using both pixel intensity and underlying graph structure. As shown in Figure 1, an overview of the proposed AGFT encryption system is provided firstly.

5.1. DNA Encoding

In the proposed image encryption method, the key streams are firstly generated by the Mixed Linear Nonlinear Coupled Map Lattices (MLNCML) system (Tao et al., 2007). Although numerical
realizations of any chaos would be periodic, the period of the MLMCML is sufficiently long to ensure security. The MLMCML is defined as follows

\[
x_{n+1}(i) = (1-\varepsilon)f[x_n(i)] + \ldots + (1-\eta)\{f[x_n(i+1)] + f[x_n(i-1)]\} + \ldots + \eta \frac{\varepsilon}{2}\{f[x_n(j)] + f[x_n(k)]\},
\]

where \(i, j, k\) are the lattices \((1 \leq i, j, k \leq L)\), \(\varepsilon\) and \(\eta\) are the coupling parameters \((0 \leq \varepsilon \leq 1, 0 \leq \eta \leq 1)\) and \(n\) is the index \((n = 1, 2, 3, \ldots)\). The one-dimensional logistic map \(f(x)\) is

\[
f(x) = ux(1-x),
\]

where \(u(3.6 \leq u \leq 4)\) is the bifurcation parameter. The relation of \(i, j, k\) is defined by the Arnold cat map

\[
\begin{bmatrix} j \\ k \end{bmatrix} = A \begin{bmatrix} i \\ j \end{bmatrix} \mod L = \begin{bmatrix} 1 & p \\ q & pq + 1 \end{bmatrix} \begin{bmatrix} i \\ j \end{bmatrix} \mod L.
\]

The MLNCML system uses the spatial nonlinear coupling that can generate better pseudo-random sequences than that use adjacent coupling to scramble pixels spatially. The key streams are generated using specific \(p, q, \eta, \varepsilon, u\).

Then the DNA encoding system is used to encode the original image, where the DNA deletion and DNA insertion pseudo-operations are used to confuse the DNA encoded diffused image under the control of the key streams as previous work (Hu et al., 2017). The encrypted image is obtained after decoding the confused DNA image. The original image is encrypted successfully by the diffusion and confusion operations. During the confusion stage, DNA deletion and insertion operations are performed on the DNA-encoded chaotically scrambled image (Figure 2).

5.2. Image Sparse Decomposition Based on Random Walk

Then the key streams with piecewise values generated are used to decompose a digital image into several sparse sub-images. Further, the subgraphs are obtained based on the probability transfer matrix as shown in Figure 3.

In the sparse decomposition step, an image can be modelled as a graph whose vertices are pixels. The pixels are divided into sparse subgraphs according to the arrangement of chaotic sequences. The decomposition system is as follows,

\[
\text{input}(i) = f(x, y, z)
\]

\[
\text{control}(i) = g(\text{input}(i), \text{freq}(t))
\]

\[
\text{output}(i) = h(\text{control}(i), \text{freq}(t)),
\]

where \(z\) is the intensity value at the location \((x, y)\) and \(f, g, h\) are functions. In the proposed method, a pixel needs to restrict to exactly one sparse image. Every pixel location is tested with the control functions until the pixel is allowed into a sparse image. The MLNCML function is used as a
control function. Then for the output function, the function divides the range of the MLNCML function $I = (0,1)$ into some equal-length sub-intervals. Each interval has a sparse image associated with it. The output of the MLNCML function is tested against the upper and lower bounds of these sub-intervals. A pixel will then belong to a sparse image corresponding to an interval if the value output by the MLNCML function falls between that interval. Once the sparse sub-images are gained, pixels of subgraphs can be connected to generate a random walk path and generate a $K$-connectivity graph.

In this step, the original image is decomposed into sparse subgraphs. This step not only reduces the amount of data in a single calculation but also scrambles the pixel coordinates. While reducing the computational complexity and amount, the security of the image is enhanced spatially.
5.3. Encryption By The AGFT

In the former steps, DNA coding and sparse decomposition scramble the coordinates of pixels to realize spatial encryption. Then the AGFT is used to make the encryption process related to the transform operator and the intrinsic image structure. Given a $\sqrt{N} \times \sqrt{N}$ pixel block, each pixel in the block is treated as a vertex in a graph $G$ and connect it to its four immediate neighbors, resulting in a 4-connectivity graph. Given the graph, the adjacency matrix $W$ can be defined, where $W_{i,j} = W_{j,i} = 1$ if pixel positions $i$ and $j$ are connected, and 0 otherwise. The degree matrix $D$ can then be computed. Then, using matrices $W$ and $D$, the graph Laplacian matrix is computed as $L = D - W$. Finally, pixels are stacked in the $\sqrt{N} \times \sqrt{N}$ patch into a length-$N$ vector $x$ and compute the AGFT.

In the proposed method, the $N$ point sparse subgraphs with pseudo-random coordinates are obtained in the former step. The Laplacian matrix of the subgraph is $L_m$, where $m = 1, \cdots, M$ is the number of subgraphs. The pixels in the sparse subgraphs are indicated by $x_m$. For $L_m$ is a symmetric matrix, it can be decomposed into a set of complete orthogonal bases with real eigenvalues

$$L_m v_{m,l} = \lambda_{m,l} v_{m,l},$$

where $l = 0, 1, \cdots, N-1$. The matrix $V_{MN}$ comprises eigenvectors $\{v_{m,l}\}_{l=0,1,\cdots,N-1}$. According to Equation7, the rotated eigenvectors of subgraphs are

$$V_{MN}^\theta = R_N^\theta V_{MN},$$

where $R_N^\theta$ is the rotation matrix, the column vectors of $V_{MN}^\theta$ are depicted as $\{v_{m,l}^\theta\}_{l=0,1,\cdots,N-1}$ respectively and then used to compute the AGFT of signals according to Equation 10. As Figure 1 shows, the encrypted signals are depicted as

$$X_m = [V_{m,N}^\theta]^{-1} x_m.$$

Here the AGFT with different angles $\theta$ is used for subgraphs, which means the corresponding parts of the original image are transformed into particular AGFT domains. For the structural property of the AGFT, this step also makes each part of the image have a specific geometric structure and avoids high local correlation, which improves the security of the system.

As the invertibility showed in Equation 11, the decryption process is the inverse process of encryption

$$x_m = V_{m,N}^\theta X_m.$$
6. EXPERIMENTAL RESULTS

In this section, experiments are given to prove the validity of the encryption method. In all of the following experiments, \(256 \times 256 \times 3\) color images are used as original images, such as Figure 4 (a). Figure 4 (b) is the encrypted image, and Figure 4 (c) is the decrypted image obtained when the keys are all correct. From Figure 4 (b), the encrypted image presents as a stable white noise and no information can be obtained on the original image by eyes. Then the performance of the proposed algorithm is compared with that of other state-of-art algorithms. A good encryption system should resist all known attacks, such as plaintext attack, chosen ciphertext attack, statistical attack and all kinds of violent attacks. The security analysis is carried out, including exhaustive analysis, statistical analysis, security analysis, computation analysis.

6.1. Exhaustive Analysis

6.1.1. Key Space

The key space of encryption algorithms should be large enough to make the brute force attacks infeasible. Besides the random numbers \(x_0\) associated with a plain image, the secret keys of the cryptosystem include \(p, q, \eta, \varepsilon, u\) of the MLNCML system. All these keys have a precision of \(10^{-15}\) (The numerical simulations are implemented by double-precision floating-point arithmetic), and the entire key space size is more than \(10^{75}\). Table 1 provides a comparison of the key space between the proposed algorithm and other encryption methods. Attackers can not decrypt image correctly by large scale exhaustive searches. Thus the proposed encryption algorithm has a good ability to resist brute-force attacks.

6.1.2. Key Sensitivity

For the key sensitivity analysis, it is supposed that 0.0001 is changed in the studied key and other keys keep unchanged. The change of the parameter \(\eta, \varepsilon\) will cause the change of pixel extraction and

| Algorithm     | AGFT | Liu et al., 2008 | Yu et al., 2017 | Fracastoro et al., 2017 | Gondim et al., 2019 | Hu et al., 2017 |
|---------------|------|-----------------|----------------|------------------------|-------------------|----------------|
| Key space     | \(10^{75}\) | \(10^{14}\) | \(133 \times 10^{14}\) | \(2^{120}\) | \(2^{256}\) | \(2^{149}\) |
lead to different chaotic sequences. The bifurcation parameter $u$ plays the same role. The simulation and analysis show that the algorithm is sensitive to the keys, and small changes of keys will lead to a significant change of encrypted images. For the quantitative analysis of each key, mutual information is used to evaluate the key sensitivity of two encrypted images $X_1$ and $X_2$, which are generated from the same original image with different keys. A lower value of the mutual information between $X_1$ and $X_2$ means higher key sensitivity. At the other extreme, if $X_1$ and $X_2$ are the same, then all the information of $X_1$ is shared with $X_2$, so the key sensitivity does not exist. The mutual information is

$$I(X_1, X_2) = H(X_1) - H(X_1 | X_2).$$

(24)

In the simulation experiments, the sensitivity of the keys is compared. Equation 24 is used to calculate the sensitivity of each key. As shown in Table 2, the information shared between $X_1$ and $X_2$ is close to zero. The highest and least sensitivities of parameters in a single algorithm are very close, so the attackers cannot distinguish which is the varied parameter in secret keys.

| Table 2. Mutual information comparison |
|--------------------------------------|
| | Lake | Pepper | House | Baboon | Airplane |
|---|---|---|---|---|---|
| $\eta$ | 0.5680 | 0.5709 | 0.5694 | 0.5677 | 0.5704 |
| $\varepsilon$ | 0.5706 | 0.5701 | 0.5676 | 0.5688 | 0.5687 |
| $u$ | 0.5715 | 0.5688 | 0.5709 | 0.5684 | 0.5689 |
| $p$ | 0.5672 | 0.5684 | 0.5660 | 0.5716 | 0.5749 |
| $q$ | 0.5725 | 0.5667 | 0.5696 | 0.5705 | 0.5669 |

6.1.3. Key Limitation
As a symmetric encryption method, a single key is used in the proposed AGFT, the strength of encryption relies on the size of the key and used and image transmitted. The algorithm using a long key is harder to be cracked than the algorithms using a small key. In the case of encryption with data transmission, there is a significant change in the performance of different symmetric key schemes, since most of the resources are consumed for data transmission rather than computation. Image encryption with key(s) provides strong security for the use of keys in encryption, but key generation and distribution by MLNCML system is the most tedious task. Both the Keys and Keyless Approaches are useful in encryption of image application and have benefits and liabilities.

6.2. Statistical Analysis
6.2.1. Histogram Analysis
The histogram of the image shows the distribution of pixel values. The attackers may discover the pixels’ statistical nature of the original image from the encrypted image by the histogram diagramming the number of pixels for each grey-level. Thus ideal encrypted image should have a different histogram with the original image. Figure 5 shows the color images and their histograms. The images are encrypted with different keys. An image histogram is a total distribution in a digital image by plotting
the number of pixels for each tonal value. An image encryption algorithm is considered “ideal” if the encrypted image has uniformly distributed histogram. From Figure 5 and Figure 6, we can see the histograms of proposed AGFT distribute like stable Gaussian distribution instead of uniform distribution, which helps to resist statistical attack and the effects of noise. While histograms of other competitive methods still have a unique distribution for each image, the histograms of the encrypted images using proposed AGFT differ from the original ones, and all distribute like stable Gaussian distribution. Thus the proposed encryption system does not provide any clue to use any statistical attack.

6.2.2. Correlation Analysis

Adjacent image pixels are highly correlated in horizontal, vertical or diagonal directions. The correlation between adjacent pixels needs to be significantly reduced for encrypted images. To test the pixel correlation of the original and encrypted images, 1000 pairs of adjacent pixels is firstly selected from the images. Then, the correlation coefficients of the adjacent pixels in the vertical, horizontal and diagonal direction are calculated as

\[ r_{xy} = \frac{\text{cov}(x, y)}{\sqrt{D(x)}\sqrt{D(y)}}, \]  

(25)
where the expectation is $E(x) = \frac{1}{S} \sum_{i=1}^{S} x_i$, the variance is $D(x) = \frac{1}{S} \sum_{i=1}^{S} (x_i - E(x))^2$, $\text{cov}(x, y) = \frac{1}{S} \sum_{i=1}^{S} (x_i - E(x))(y_i - E(y))$. $x$ and $y$ denote two adjacent pixels and $S$ is the total number of pixel pairs $(x, y)$. Then the correlation coefficients of original and encrypted images are listed in Table 3. The average is computed as follows

$$\text{average} = \frac{|a| + |b| + |c|}{3},$$

(26)

where $a, b, c$ are the three coefficients of the same image for three different directions.

Table 4 compares the average decorrelation ability of the proposed AGFT method with other algorithms. The average performance is computed after testing the color images used in this section.
Compared with existed methods, pixels in the encrypted images using the proposed AGFT show an obvious lower correlation. The reason is the underlying graph structures of original images are encrypted and the correlation of two adjacent pixels is reduced. Thus the proposed method is robust against the statistical analysis attacks.

6.2.3. Information Entropy

The information entropy $H$ is an important index for measuring the uncertainty and the distribution of the values in the image

$$H(s) = \sum_{i=0}^{2^{N} - 1} P(s_i) \log_2 \frac{1}{P(s_i)},$$  \hspace{1cm} (27)

where $P(s_i)$ represents the probability of symbol $s_i$ presence. The more uniform the distribution of information entropy is, the closer it is to its ideal value. For the pure random information source $s$ with $2^N$ states, the information entropy is $H(s) = N\log_2 s$. The information entropy of the encrypted image is given in Table 5. The entropy of encrypted image obtained by this method is closer to 8, which shows the robustness of this method to entropy attack.

### Table 3. The decorrelation ability of AGFT

| Original Image | lake  | pepper | house | baboon | airplane |
|----------------|-------|--------|-------|--------|----------|
| Horizontal     | 0.9546| 0.9690 | 0.9349| 0.9260 | 0.9282   |
| Vertical       | 0.9575| 0.9655 | 0.9644| 0.9466 | 0.9395   |
| Diagonal       | 0.9274| 0.9360 | 0.9121| 0.9059 | 0.8789   |
| Average        | 0.9465| 0.9568 | 0.9371| 0.9261 | 0.9155   |
| Encrypted Image| lake  | pepper | house | baboon | airplane |
| Horizontal     | 0.0095| 0.0002 | 0.0053| 0.0099 | -0.0026  |
| Vertical       | 0.0142| 0.0039 | -0.0030| 0.0005 | -0.0020  |
| Diagonal       | 0.0089| 0.0048 | 0.0043| 0.0129 | -0.0140  |
| Average        | 0.0109| 0.0030 | 0.0022| 0.0078 | -0.0062  |

### Table 4. Comparison of the decorrelation ability

| Image        | Algorithm       | Direction | Horizontal | Vertical | Diagonal | Average |
|--------------|-----------------|-----------|------------|----------|----------|---------|
| Original     | Proposed AGFT   |           | 0.9474     | 0.9541   | 0.9132   | 0.9383  |
| Encrypted    | Liu et al., 2008|           | 0.0050     | -0.0003  | 0.0017   | -0.0021 |
|              | Yu et al., 2017 |           | 0.3354     | 0.6153   | 0.1447   | 0.3652  |
|              | Fracastoro et al., 2017 |  | -0.0534   | 0.3122   | -0.0029  | 0.0853  |
|              | Gondim et al., 2019 |           | -0.2926 | -0.0449  | -0.1447  | -0.1607 |
|              | Hu et al., 2017 |           | -0.1372   | 0.0699   | -0.0665  | -0.0446 |
|              |                 |           | -0.0077   | 0.0002   | -0.0055  | 0.0043  |
6.3. Security Analysis

6.3.1. Differential Attack

In general, the attackers can make a slight change to the original image (for example, only one-pixel change), and then observe the changes in the encrypted image. In this way, an attacker may find the relationship between two encrypted images and the original image. NPCR (number of pixels change rate) and UACI (unified average changing intensity) is used to test the performance under differential attacks.

\[
D(i, j) = \begin{cases} 
1, & x_1(i, j) \neq x_2(i, j) \\
0, & \text{otherwise}
\end{cases}
\]

\[
NPCR = \frac{\sum_{i,j} D(i, j)}{M \times N} \times 100\%,
\]

where \(M\) and \(N\) are the rows and columns of image pixels, \(x_1(i, j)\) and \(x_2(i, j)\) are the encrypted pixels of the original and changed image. The expected NPCR and UACI are calculated as

\[
NPCR_{\text{expected}} = \left(1 - 1/L\right) \times 100\%,
\]

\[
UACI_{\text{expected}} = \frac{1}{L^2} \left(\sum_{l=1}^{L-1} L(L+1)/(L-1)\right) \times 100\%,
\]

where \(L\) is the grey level of one channel. The expected NPCR and UACI for an 8-bit image \((L = 256)\) are 99.6094\% and 33.4635\%, respectively. One pixel randomly fetched from the original image is altered to measure the plain-image sensitivity. Two encrypted images are produced by encrypting the original, and the changed images using the proposed image cryptosystem and five plaintext images are used for tests. The NPCR and UACI performance of the proposed algorithm are shown in Table 6 and Table 8, where the average performance of algorithms under differential attacks is compared. From Table 7 and Table 9, the proposed AGFT performs better than other methods. The reason is that other algorithms consider transform operators with no relationship with the

---

Table 5. Information entropies analysis of five different color images

| Algorithm          | lake    | pepper  | house   | baboon  | airplane |
|--------------------|---------|---------|---------|---------|----------|
| Original Image     | 7.7395  | 7.7037  | 7.0687  | 7.6787  | 6.6788   |
| Proposed Algorithm | 7.9991  | 7.9990  | 7.9991  | 7.9991  | 7.9990   |
| Liu et al., 2008   | 5.3667  | 5.4475  | 5.1990  | 5.2530  | 5.1479   |
| Yu et al., 2017    | 4.4304  | 4.4453  | 4.3833  | 4.4336  | 4.4253   |
| Fracastoro et al., 2017 | 3.8956  | 3.9103  | 4.2914  | 3.8129  | 4.3681   |
| Gondim et al., 2019 | 7.7394  | 7.1941  | 7.6787  | 7.1372  | 7.9204   |
| Hu et al., 2017    | 7.9961  | 7.9965  | 7.9961  | 7.9968  | 7.9964   |
plaintexts. The proposed AGFT method takes the intrinsic image structure into consideration, and the transform operator is related with plaintexts, so the change of the pixel value of any location point will affect the change of the ciphertext of almost all points. The NPCR and UACI are close to the expected values, so the proposed method can resist the differential attack.

Table 6. NPCR analysis of AGFT

| Encrypted Image | lake | pepper | house | baboon | airplane |
|-----------------|------|--------|-------|--------|----------|
| Red             | 0.9961 | 0.9960 | 0.9964 | 0.9963 | 0.9957   |
| Green           | 0.9956 | 0.9961 | 0.9960 | 0.9962 | 0.9964   |
| Blue            | 0.9963 | 0.9962 | 0.9960 | 0.9960 | 0.9960   |
| Average         | 0.9960 | 0.9961 | 0.9961 | 0.9961 | 0.9960   |

Table 7. Comparison of the NPCR

| Algorithm | Proposed | Liu et al., 2008 | Yu et al., 2017 | Fracastoro et al., 2017 | Gondim et al., 2019 | Hu et al., 2017 |
|-----------|----------|------------------|----------------|-------------------------|---------------------|---------------|
| Red       | 0.9961   | 0.0428           | 0.5952         | 0.0029                  | 0.9956              | 0.9958        |
| Green     | 0.9962   | 0.03              | 0.5897         | 0                       | 0.9962              | 0.9964        |
| Blue      | 0.9961   | 0.403             | 0.6329         | 0.0016                  | 0.9965              | 0.9959        |
| Average   | 0.9961   | 0.0377            | 0.6059         | 0.0015                  | 0.9961              | 0.9962        |

Table 8. UACI analysis of AGFT

| Encrypted Image | lake | pepper | house | baboon | airplane |
|-----------------|------|--------|-------|--------|----------|
| Red             | 0.3325 | 0.3338 | 0.3363 | 0.3341 | 0.3339   |
| Green           | 0.3345 | 0.3338 | 0.3356 | 0.3372 | 0.3354   |
| Blue            | 0.3333 | 0.3348 | 0.3347 | 0.3345 | 0.3342   |
| Average         | 0.3334 | 0.3341 | 0.3355 | 0.3353 | 0.3345   |

Table 9. Comparison of the UACI

| Algorithm | Proposed | Liu et al., 2008 | Yu et al., 2017 | Fracastoro et al., 2017 | Gondim et al., 2019 | Hu et al., 2017 |
|-----------|----------|------------------|----------------|-------------------------|---------------------|---------------|
| Red       | 0.3347   | 0.0002           | 0.0719         | 0.0011                  | 0.3328              | 0.3332        |
| Green     | 0.3355   | 0.0001           | 0.0719         | 0                       | 0.3339              | 0.3336        |
| Blue      | 0.3348   | 0.0002           | 0.0894         | 0.0004                  | 0.3367              | 0.3334        |
| Average   | 0.335    | 0.0001           | 0.0777         | 0.0005                  | 0.3345              | 0.3334        |
6.3.2. Chosen-Plaintext Attack

When an encryption algorithm is analyzed under cryptanalysis attacks, it is assumed that a cipher decipher can accurately know the design and operation of the encryption system. That means the cipher decipher knows any information other than the keys. The security of the encryption system does not depend on the encryption algorithm itself but depends on the keys. Commonly used cryptanalysis techniques include ciphertext-only attack, known-plaintext attack, chosen-plaintext attack, and chosen-ciphertext attack. The proposed encryption algorithm can resist the chosen-plaintext attack because the encryption keys are one-time pads so that the keys are different even encrypting the same image. Another reason is the use of cryptographic feedback in the step of the AGFT. In the encryption algorithm, the ciphertext and keys are mixed, and attackers cannot solve the keystream or the equivalent keys. Also, the initial value of the MLNCML system is related to the unique attributes of the plaintext image, such as the mean value of pixels and the image entropy. From Equation 22, the encrypted image is decided by both the original image and the intrinsic structure. Even if an attacker deciphers the key streams by selecting a special plaintext image, he cannot decipher the corresponding underlying structure of the image, and the target ciphertext is secure.

6.3.3. Occlusion Attack

When encrypted images are transmitted in an unsafe communication channel, some information may be lost. To verify the tolerance for occlusion attack, the decryption effect of encrypted images blocked 6.25%, 12.5%, 25% and 50% pixels are tested, respectively. As Figure 7 shown, even with a 50% loss of dense map data, the decryption image is still visible. The results show that the proposed algorithm is tolerant of the loss of encrypted data because the energy of each pixel of the original image is extended to the whole space of the encrypted image. When a part of the encrypted data is lost, the remaining data still carry the information of all the pixels. However, losing data from the encrypted image will cause a decline in the peak signal-to-noise ratio (PSNR) and normalization coefficient of the decrypted image. The post-processing methods such as image denoising and image enhancement can improve the quality of the decrypted images (Table 10).
6.3.4. Noise Attack

When an encrypted image is transmitted in a low SNR channel, it will be contaminated by noise such as additive Gaussian white noise. To test the tolerance for noise, Gaussian white noises with different degrees are added to the encrypted image. It is assumed that the effect of noise on the density map satisfies the following model

\[
E' = E(1 + \sigma G),
\]

(31)

where \(E\) and \(E'\) are encrypted image and encrypted image with noise respectively, the parameter \(\sigma\) is the weight of noise intensity, \(G\) is the Gaussian white noise with zero mean. Figure 8 shows that the decrypted images are still discernible when the secret map is transmitted in a noisy channel. Therefore, the proposed method has a certain ability to resist noise. As shown in Table 11, the peak signal-to-noise ratio (PSNR) and normalization coefficient of the decrypted image are reduced by a noisy channel.

6.3.5. Histogram Equalization Attack

Histogram equalization is used to strengthen image contrast by adjusting intensities. Figure 9 displays the encrypted image after histogram equalization and the corresponding decrypted image. The PSNR is 17.2840 and normalization coefficient is 0.9696. It could be found out that the proposed cryptosystem could withstand against the histogram equalization attack.

---

Table 10. AGFT performance under occlusion attack

| Data Occlusion | 6.25% | 12.5% | 25% | 50% |
|----------------|-------|-------|-----|-----|
| PSNR           | 16.0159 | 12.6487 | 11.8365 | 11.1462 |
| Normalization Coefficient | 0.9590 | 0.9145 | 0.8920 | 0.8727 |

Figure 8. Decryption results of AGFT under noise attack. \(\sigma\) of the first column equals to 0.1. The other three are 0.3, 0.5 and 0.7, respectively.

Table 11. AGFT performance under noise attack

| Noise Intensity | 0.1  | 0.3  | 0.5  | 0.7  |
|----------------|------|------|------|------|
| PSNR           | 12.3822 | 10.6466 | 9.9073 | 9.4884 |
| Normalization Coefficient | 0.9086 | 0.8650 | 0.8402 | 0.8240 |
6.4. Extended Algorithm for 3D Shape

Signal processing on geometric data is an active field of research recently for the rapidly developing graph signal processing (GSP). For the proposed method is based on the graph Fourier transform, we can generalize the proposed AGFT to non-Euclidean domains by considering the respective Laplacian of these domains (Thanou et al., 2016). A 3D shape is modelled as a connected smooth compact two-dimensional manifold embedded into $\mathbb{R}^3$.

The proposed algorithm can be extended for a 3D shape encryption. The difference between the extended algorithm and image algorithm is the geometric structure of signals. The merits of an image algorithm still keep in the extended algorithm. Furthermore, the computational complexity of the extended algorithm does not increase proportionally with dimensions. Therefore, the proposed algorithm is also efficient in 3D shape encryption. From the example shown in Figure 10, the proposed AGFT can encrypt the original 3D shape with the specific color distribution. The color distribution of the encrypted 3D shape is uniform without original information.
6.5. Computational and Complexity Analysis

The running speed influenced by the computational complexity is also a significant aspect on a great image encryption system. To evaluate the running speed, the encryption time of the algorithm is tested. All tests are implemented in MATLAB 2016a and the Windows 7 professional version of the operating system. The computer is of an Intel Core i7-6700@3.40GHz processor, 16GB RAM and 750GB hard disk. Three images containing 256 gray levels are listed in Table 12, each image is encrypted ten times and the average execution times are listed for comparison. When analyzing the execution time, it can be found that the time-consuming part of the calculation is eigendecomposition operation of the Laplacian matrix. As shown in Table 12, the average eigendecomposition time of larger size images is longer than multiple sub-images. Thus, the algorithm can be sped up by sparse decomposition of images. From Table 12, the running time of most competitive methods increases proportionally with the pixel number, which is because the structure of the image is fixed to quadruple. Further, the computational complexity of the extended algorithm increases with numbers of points instead of the size of the 3D cube because the 3D shape is represented by a graph. As Table 12 shows, the running speed of the proposed cryptosystem is not fast comparing with other related work but acceptable, which will be further considered and improved in our further work using fast graph transform algorithm.

7. Conclusion

In this paper, an image encryption method based on the angular graph Fourier transform (AGFT) is proposed to encrypt images with structural information for better performance. First, the graph Fourier transform (GFT) is introduced, and the AGFT is presented with its properties. Then, the image encryption method based on the AGFT and DNA coding is proposed. The experimental results demonstrate that the proposed algorithm significantly enhances data security and achieves better performance than other state-of-art algorithms. Compared with other competitive methods, the major advantage of the proposed method is that it combines structural information from graph transform and random parameter generated by angular transform in a joint transform operator. The proposed method considers image structure to extend the key space and improve the security of the encryption system. However, the proposed method still has some common limitations of encryption methods using a symmetric key. For example, lots of resources are consumed for data transmission rather than computation. Furthermore, extending the proposed AGFT for high-dimensional data also requires more research. Last, lowering the computational burden of the proposed AGFT can further promote its practical application in target information security, medical information security in telemedicine etc.
REFERENCES

Alfalou, A., Brosseau, C., Abdallah, N., & Jridi, M. (2013). Assessing the performance of a method of simultaneous compression and encryption of multiple images and its resistance against various attacks. Academic Press.

Annaby, M. H., Rushdi, M. A., & Nehary, E. (2016). Image encryption via discrete fractional Fourier-type transforms generated by random matrices. Academic Press.

Artiles, J. A., Chaves, D. P., & Pimentel, C. (2019). Image encryption using block cipher and chaotic sequences. Academic Press.

Belazi, A., El-Latif, A. A. A., Diaconu, A. V., Rouma, R., & Belghith, S. (2017). Chaos-based partial image encryption scheme based on linear fractional and lifting wavelet transforms. Optics and Lasers in Engineering, 88, 37–50. doi:10.1016/j.optlaseng.2016.07.010

Carnicer, A., Montes-Usategui, M., Arcos, S., & Juvels, I. (2005). Vulnerability to chosen-cyphertext attacks of optical encryption schemes based on double random phase keys. Academic Press.

Chai, X., Chen, Y., & Broyde, L. (2017). A novel chaos-based image encryption algorithm using DNA sequence operations. Optics and Lasers in Engineering, 88, 197–213. doi:10.1016/j.optlaseng.2016.08.009

Chen, K., Xu, D. (2018). An efficient reversible data hiding scheme for encrypted images. Academic Press.

Chen, L., & Zhao, D. (2006). Optical color image encryption by wavelength multiplexing and lensless Fresnel transform holograms. Academic Press.

Chen, S., Sandryhaila, A., Moura, J. M., & Kovacevic, J. (2014). Signal denoising on graphs via graph filtering. Paper presented at the 2014 IEEE Global Conference on Signal and Information Processing (GlobalSIP). doi:10.1109/GlobalSIP.2014.7032244

Cheng, X., Cai, L., Wang, Y., Meng, X., Zhang, H., Xu, X., & Dong, G. (2008). Security enhancement of double-random phase encryption by amplitude modulation. Academic Press.

Chung, F. R., & Graham, F. C. (1997). Spectral graph theory. American Mathematical Soc.

Corless, R. M., Essex, C., & Nerenberg, M. A. H. (1991). Numerical methods can suppress chaos. Physics Letters. [Part A], 157(1), 27–36. doi:10.1016/0375-9601(91)90404-V

Ding, W., Liu, K., Yan, X., & Liu, L. (2018). Polynomial-based secret image sharing scheme with fully lossless recovery. Academic Press.

Fracastoro, G., & Magli, E. (2017). Steerable discrete Fourier transform. Academic Press.

Gondim, M. A., de Oliveira Neto, J. R., & Lima, J. (2019). Steerable Fourier number transform with application to image encryption. Academic Press.

Guo, C., Muniraj, I., & Sheridan, J. (2016). Phase-retrieval-based attacks on linear-canonical-transform-based DRPE systems. Academic Press.

Hu, T., Liu, Y., Gong, L.-H., Guo, S.-F., & Yuan, H.-M. (2017). Chaotic image cryptosystem using DNA deletion and DNA insertion. Academic Press.

Huang, H., & Yang, S. (2016). Colour image encryption based on logistic mapping and double random-phase encoding. Academic Press.

Huang, X., & Ye, G. (2014). An image encryption algorithm based on hyper-chaos and DNA sequence. Multimedia Tools and Applications, 72(1), 57–70. doi:10.1007/s11042-012-1331-6

Kang, X., Han, Z., Yu, A., & Duan, P. (2017). Double random scrambling encoding in the RPMPFrHT domain. Paper presented at the 2017 IEEE International Conference on Image Processing (ICIP). doi:10.1109/ICIP.2017.8297106

Kumar, P., Kumar, A., Joseph, J., & Singh, K. (2009). Impulse attack free double-random-phase encryption scheme with randomized lens-phase functions. Academic Press.
Kumar, M., Iqbal, A., & Kumar, P. (2016). A new RGB image encryption algorithm based on DNA encoding and elliptic curve Diffie–Hellman cryptography. *Signal Processing, 125*, 187–202. doi:10.1016/j.sigpro.2016.01.017

Li, Y., Wang, C., & Chen, H. (2017). A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation. *Optics and Lasers in Engineering, 90*, 238–246. doi:10.1016/j.optlaseng.2016.10.020

Liao, M., He, W., Lu, D., & Peng, X. (2017). Ciphertext-only attack on optical cryptosystem with spatially incoherent illumination: from the view of imaging through scattering medium. Academic Press.

Liu, S., Mi, Q., & Zhu, B. (2001). *Optical image encryption with multistage and multichannel fractional Fourier-domain filtering*. Academic Press.

Liu, X., Cheung, G., & Wu, X. (2015). Joint denoising and contrast enhancement of images using graph Laplacian operator. Paper presented at the 2015 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). doi:10.1109/ICASSP.2015.7178376

Liu, Z., Ahmad, M. A., & Liu, S. (2008). *A discrete fractional angular transform*. Academic Press.

Liu, Z., Dai, J., Sun, X., & Liu, S. (2010). Color image encryption by using the rotation of color vector in Hartley transform domains. Academic Press.

Liu, Z., Gong, M., Dou, Y., Liu, F., Lin, S., & Ahmad, M. A. (2012). *Double image encryption by using Arnold transform and discrete fractional angular transform*. Academic Press.

Liu, Z., Zhao, H., & Liu, S. (2005). A discrete fractional random transform. *Optics Communications, 255*(4-6), 357–365. doi:10.1016/j.optcom.2005.06.031

Peng, X., Zhang, P., Wei, H., & Yu, B. (2006). Known-plaintext attack on optical encryption based on double random phase keys. Academic Press.

Rajput, S. K., & Nishchal, N. K. (2013). Known-plaintext attack-based optical cryptosystem using phase-truncated Fresnel transform. Academic Press.

Refregier, P., & Javidi, B. (1995). Optical image encryption based on input plane and Fourier plane random encoding. Academic Press.

Sandryhaila, A., & Moura, J. M. (2013). *Discrete signal processing on graphs: Graph Fourier transform*. Paper presented at the 2013 IEEE International Conference on Acoustics, Speech and Signal Processing. doi:10.1109/ICASSP.2013.6638850

Shao, Z., Liu, X., Yao, Q., Na, Q., Shang, Y., & Zhang, J. (2019). Multiple-image encryption based on chaotic phase mask and equal modulus decomposition in quaternion gyrator domain. Academic Press.

Sharma, V. K., Srivastava, D. K., & Mathur, P. (2018). Efficient image steganography using graph signal processing. Academic Press.

Shen, G., Kim, W.-S., Narang, S. K., Ortega, A., Lee, J., & Wey, H. (2010). Edge-adaptive transforms for efficient depth map coding. Paper presented at the 28th Picture Coding Symposium. doi:10.1109/PCS.2010.5702565

Shuman, D. I., Narang, S. K., Frossard, P., Ortega, A., & Vandergheynst, P. (2013). *The emerging field of signal processing on graphs: Extending high-dimensional data analysis to networks and other irregular domains*. Academic Press.

Singh, P., Yadav, A., & Singh, K. (2017). Phase image encryption in the fractional Hartley domain using Arnold transform and singular value decomposition. Academic Press.

Thanou, D., Chou, P. A., & Frossard, P. (2016). *Graph-based compression of dynamic 3D point cloud sequences*. Academic Press.

Unnikrishnan, G., Joseph, J., & Singh, K. (2000). Optical encryption by double-random phase encoding in the fractional Fourier domain. Academic Press.

Wang, X. Y., Zhang, Y. Q., & Bao, X. M. (2015). A novel chaotic image encryption scheme using DNA sequence operations. *Optics and Lasers in Engineering, 73*, 53–61. doi:10.1016/j.optlaseng.2015.03.022
Wheeler, D. D. (1989). Problems with chaotic cryptosystems. *Cryptologia, 13*(3), 243–250. doi:10.1080/0161-118991863934

Wu, J., Liu, W., Liu, Z., & Liu, S. (2015). Correlated-imaging-based chosen plaintext attack on general cryptosystems composed of linear canonical transforms and phase encodings. Academic Press.

Wu, X., Kan, H., & Kurths, J. (2015). A new color image encryption scheme based on DNA sequences and multiple improved 1D chaotic maps. *Applied Soft Computing, 37*, 24–39. doi:10.1016/j.asoc.2015.08.008

Xiang, T., Wong, K.-w., & Liao, X. (2007). *Selective image encryption using a spatiotemporal chaotic system*. Academic Press.

Yu, J., Li, Y., Xie, X., Zhou, N., & Zhou, Z. (2017). *Image encryption algorithm by using the logistic map and discrete fractional angular transform*. Academic Press.

Zhen, P., Zhao, G., Min, L., & Jin, X. (2016). Chaos-based image encryption scheme combining DNA coding and entropy. *Multimedia Tools and Applications, 75*(11), 6303–6319. doi:10.1007/s11042-015-2573-x

---

Liuqing Yang received her BS degree in School of Information Science and Technology from Beijing Forestry University, Beijing, China, in 2017. She is currently pursuing her MS degree with Software Engineering in Beijing Forestry University, Beijing, China. Her research interests include graph theory and digital image processing.

Wei Meng, Associate Professor, School of Information Science and Technology, Beijing Forestry University, member of CCF, received her Ph.D. in Harbin Institute of Technology in 2005. Her research fields are machine learning, Internet of Things technology and information fusion technology.

Xudong Zhao received the B.S. degree in Science and Technology of Electronic Information department from Beijing Institute of Technology, Beijing, China, in 2016. He is currently pursuing her Ph.D. degree with Information and Communication Engineering in Beijing Institute of Technology (BIT), Beijing, China. His research interests include fractional Fourier transform, graph theory and remote sensing image process.