The rest of this chapter consists of the introduction and explanation of a newly defined image encryption algorithm known as the tensor transform-based method of image encryption that is based on the tensor transformation from Refs. 46 and 47. The tensor image encryption scheme uses a symmetric key (thus, the key should be kept secret) and is able to perform grayscale image encryption and decryption using MATLAB® on images of size 1024 × 1024 in 1.3 s or less (one way, thus a total of 2.3 s or less) with correlation values as low as 10^{-5}. Note that the speed of encryption and decryption could be magnitudes smaller if implemented in a lower-level language such as C+. The tensor image encryption scheme (tensor transform-based method of image encryption) can also be used to encrypt RGB color images by encrypting each color channel separately, then recombining the channels to produce the encrypted color image.

7.4 Image, Tensor Representation, and Fourier Transform

In this section, we describe the concept of the splitting of the 2D discrete Fourier transform (2D DFT) by the 1D transforms of the signals that uniquely represent the image. Such a representation is called the vector or tensor representation and was developed by Grigoryan[48–55] and later described in detail by Grigoryan and Agaian in Refs. 46 and 56–62. Such representation can also be used for Hadamard, Hartley, cosine, and other unitary transformations.[46,54,59,63,64]

In many recent publications, these concepts with various applications in digital image processing were published under various names, as mentioned in Refs. 65–67. Such names include the discrete Radon transform, fast multidimensional Radon transform, the finite Radon transform, a new discrete transform based on the exact discrete Radon (or Mojette) transform, the discrete periodic Radon transform, the orthogonal discrete periodic Radon transform, and the generalized finite Radon transform.

In tensor representation, the 2D grayscale image is presented as a set of 1D signals, and the 2D DFT of the image is calculated or defined by the 1D DFTs of these signals. The mathematical structure of the 2D DFT is thus revealed by a 1D signal, which we call the splitting signal of the image, or simply the image signal. These splitting signals allow effective calculation of the 2D DFT of the image as well as for processing the image through the splitting signals. Such examples include image enhancement and image restoration.[68–77] The modification of the tensor representation, which removes the redundancy of the tensor representation of the image when its size is, for instance, a power of 2 or a prime odd number, is called the paired representation and can effectively be used in image filtration, enhancement, and compression.[47,78–85]

For simplicity of calculation, we consider that the discrete image $f_{n,m}$ is of the size $N \times N$ and is on the Cartesian lattice $X = X_{N,\ N} = \{(n, m);\ n, m = 0{:}\ (N-1)\}$. The general case of $N \times M$ images when $N \neq M$ is similarly considered.[46,47,79,80] The tensor representation of the image of size $N \times N$ is defined as a set of splitting signals of length N each. In other words, this is a unique transformation of the image into a set of 1D signals:

$$\chi = \chi_{N,N} : \{f_{n,m}\} \rightarrow \{f_{T_{p,s}} = \{f_{p,s,t};\ t = 0 : (N-1)\}\}_{(p,s)\in J}.$$

This transformation is called the tensor transformation and was derived from the properties of the 2D DFT of the image:

$$F_{p,s} = \sum_{n=0}^{N-1}\sum_{m=0}^{N-1} f_{n,m} W^{np+ms}, \qquad p,s = 0 : (N-1),$$

where the kernel of the transform is $W = W_N = \exp(-2\pi i/N)$, and $i^2 = -1$. The components of the splitting signals are calculated as the sums of the discrete image along the parallel lines passing through the notes of the lattice:

$$f_{p,s,t} = \sum_{(n,m)\in X} \{f_{n,m};\ np + ms = t\text{mod}N\}, \qquad t = 0 : (N-1).$$

The tensor representation is a 2D frequency $(p,\ s)$ and 1D time t representation of the image. For each $(p,\ s)$ from the subset J, the corresponding splitting signal is $f_{T_{p,\ s}} = \{f_{p,s,t};\ t = 0 : (N-1)\}$. In the notation of this splitting signal $f_{T_{p,s}}$, we use the cyclic group

$$T_{p,s} = \{(kp\text{mod}N, ks\text{mod}N); k = 0,1,2,\ldots,(N-1)\}$$

because the 2D DFT of the image at frequency points of this group is the DFT of the spitting signal:

$$F_{kp\text{mod}N,ks\text{mod}N} = F_k = \sum_{t=0}^{N-1} f_{p,s,t} W^{kt}, \qquad k = 0 : (N-1).$$

As an example, Fig. 7.12(a) shows the maximum of stacked images of green by fluorescence *in situ* hybridization (FISH) for detection of gene copy numbers in cancer and other diseases[86–88] of size 512×512, while Fig. 7.12(b) shows the splitting signal of length 512, which is generated by the frequency point $(p,\ s) = (3,1)$. The 1D DFT of the splitting-signal in absolute scale is shown in Fig. 7.12(c), and the 2D DFT of the image and

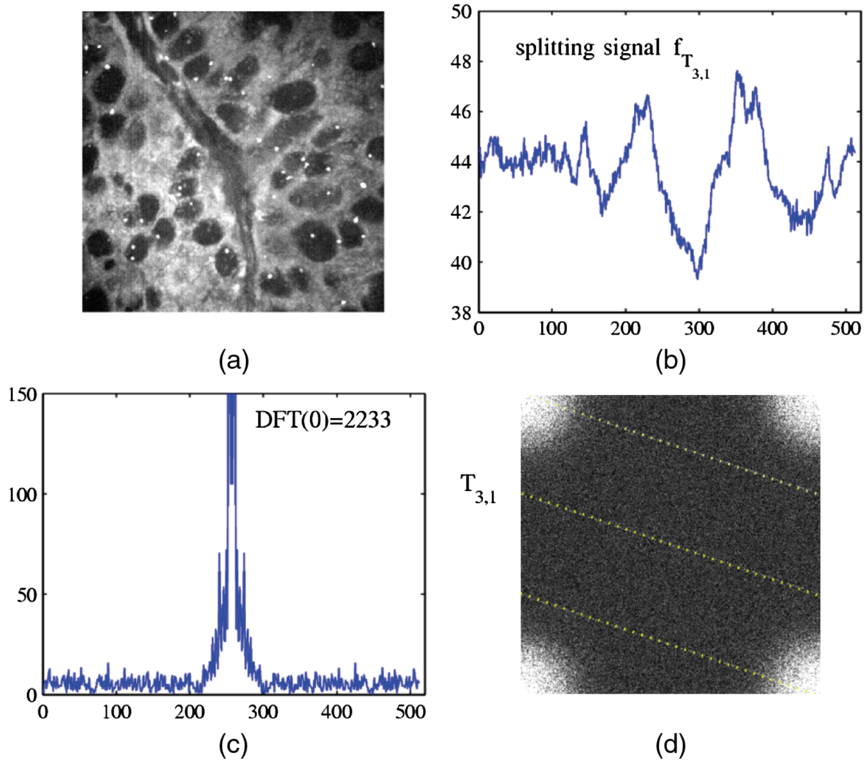

Figure 7.12 (a) 512 × 512 original image, (b) the splitting signal $f_{T_{3,1}}$, (c) the magnitude 1D DFT of this splitting signal, which is cyclically shifted to the middle, and (d) the arrangement of values of the 1D DFT in the 2D DFT of the image at frequency points of the set $T_{3,1}$.

the location of all frequency points of the cyclic group $T_{3,1}$ are shown in Fig. 7.12(d).

Given a triplet (p, s, t), where $(p, s) \in X$ and $t \in \{0,1,2,\ldots N-1\}$, we define the following set of points (n, m) of the lattice $V_{p,s,t} = \{(n,m); n,m = 0 : (N-1), \overline{np + ms} = t\}$, where $l = l$ mod N, and consider its characteristic function:

$$\chi_{p,s,t}(n,m) = \begin{cases} 1, & \text{if } (n,m) \epsilon V_{p,s,t} \\ 0, & \text{otherwise.} \end{cases} \tag{7.5}$$

The set $V_{p,s,t}$ (if it is not empty) is the set of points (n, m) along a maximum of $p + s$ parallel straight lines at the angle of $\varphi = \text{arctg}(s/p)$ to the horizontal axis. In the square domain $[0, N] \times [0, N]$, the equations for the set $\mathcal{L}_{p,s,t}$ of parallel lines are $xp + ys = t + kN$, where $k = 0 : (p + s - 1)$. It is interesting to note that the direction of parallel lines of $\mathcal{L}_{p,s,t}$ is perpendicular to the direction of frequency points of the group $T_{p,s}$.

Example 3: Tensor transform of an (8 × 8) image

In the lattice $X_{8,8}$ in the spatial domain (or the image plane), we consider the generator $(p, s) = (2,1)$ and two sets of three parallel lines $\mathcal{L}_1 = \mathcal{L}_{2,1,1}$ and $\mathcal{L}_2 = \mathcal{L}_{2,1,2}$ each. For the family $\mathcal{L}_1$, these parallel lines are

$$y_1 : 2x + y = 1, \qquad y_9 : 2x + y = 9, \qquad y_{17} : 2x + y = 17.$$

One point (0,1) of the set $V_{2,1,1}$ lies on the first line of $\mathcal{L}_1$, four points (1,7), (2,5), (3,3), (4,1) lie on the second line, and three points (5,7), (6,5), (7,3) lie on the third line. Therefore, the first component of the splitting signal $f_{T_{2,1}}$ is calculated as

$$f_{2,1,1} = (f_{0,1}) + (f_{1,7} + f_{2,5} + f_{3,3} + f_{4,1}) + (f_{5,7} + f_{6,5} + f_{7,3}).$$

The parallel lines of the family $\mathcal{L}_2$ are defined by

$$y_2 : 2x + y = 2, \qquad y_{10} : 2x + y = 10, \qquad y_{18} : 2x + y = 18.$$

Therefore, the second component $f_{2,1,2}$ of the splitting signal is calculated as

$$f_{2,1,2} = (f_{0,2} + f_{1,0}) + (f_{2,6} + f_{3,4} + f_{4,2} + f_{5,0}) + (f_{6,6} + f_{7,4}).$$

The disposition of the points lying on the parallel lines of these sets is given in Fig. 7.13. The location of the frequency points of the group $T_{2,1}$ is also shown. Two parallel lines pass through these frequency points, which are defined in the frequency plane (ω_1,ω_2) as l_1: $2\omega_2 - \omega_1 = 0$ and l_2: $2\omega_2 - \omega_1 = 8$. The parallel lines l_1 and l_2 are perpendicular to the parallel lines of both sets $\mathcal{L}_1$ and $\mathcal{L}_2$.

Due to Eq. (7.4), the following two statements are valid:

1. The image $f_{n,m}$ can be presented as a set of splitting signals $f^{(k)} = f_{T_k}$, $k = 1 : l$, of length N each,

$$\{f_{n,m};(n,m) \in X_{n,m}\} \quad \{f^{(1)},f^{(2)},f^{(3)},\ldots,f^{(l)}\}.$$

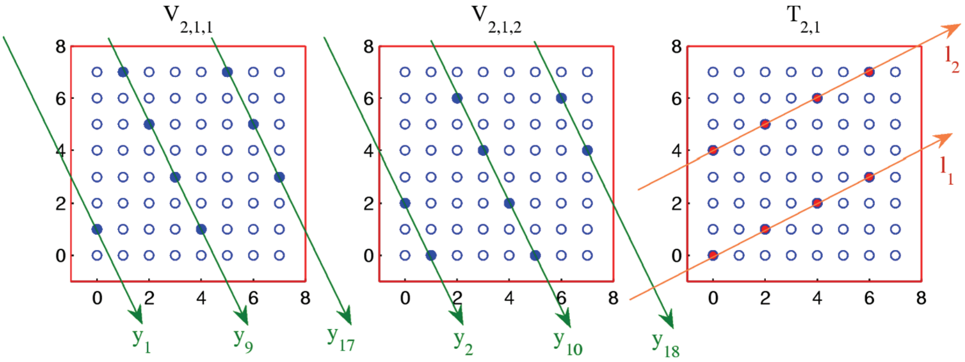

Figure 7.13 The locations of points of sets $V_{2,1,1}$ and $V_{2,1,2}$ and frequency points of the group $T_{2,1}$.

2. The 2D DFT of the image $F_{N,\ N}[f]$ can be split by 1D transforms $F_N[f^{(k)}]$ of the splitting signals:

$$F_{N,N}[f] = \{F_N[f^{(1)}],F_N[f^{(2)}],F_N[f^{(3)}],\ldots,F_N[f^{(l)}]\}.$$

The number l of the splitting signals in such a representation (tensor representation) is considered to be minimal. This number depends on N and can be determined by the set of generators $J = J_{N,N}$ for the splitting signals. This set is defined as a set for which the totality of cyclic groups $\{T_{p,s};\ (p,\ s) \in J_{N,N}\}$ is an irreducible covering of the discrete lattice of frequency points $X_{N,N} = \{(p,\ s)\,;p,\ s = 0:(N-1)\}$. Given N, one can construct different sets $J_{N,N}$; however, their cardinalities are equal. For cases when $N = 4$,5,7, and 8, we obtain $l = 6$,6,8, and 12, respectively. The following sets of generators can be considered:

$$J_{4,4} = \{(1,0),(1,1),(1,2),(1,3),(0,1),(2,1)\},$$
$$J_{4,4} = \{(0,2),(1,1),(2,1),(3,1),(1,0),(1,2)\},$$
$$J_{5,5} = \{(1,0),(1,1),(1,2),(1,3),(1,4),(0,1)\},$$
$$J_{5,5} = \{(0,1),(1,1),(2,1),(3,1),(4,1),(1,0)\},$$
$$J_{7,7} = \{(1,0),(1,1),(1,2),(1,3),(1,4),(1,5),(1,6),(0,1)\},$$
$$J_{7,7} = \{(0,1),(1,1),(2,1),(3,1),(4,1),(5,1),(6,1),(1,0)\},$$
$$J_{8,8} = \{(1,0),(1,1),(1,2),(1,3),(1,4),(1,5),(1,6),(0,1),(2,1),(4,1),(6,1)\},$$
$$J_{8,8} = \{(0,1),(1,1),(2,1),(3,1),(4,1),(5,1),(6,1),(1,0),(1,2),(1,4),(1,6)\}.$$

Example 4: Tensor transform of a (4 × 4) image

Consider that $N = 4$ and the following discrete image or (4 × 4) matrix:

$$[f_{n,m}] = \begin{bmatrix} \underline{10} & 20 & 30 & 40 \\ 120 & 130 & 140 & 50 \\ 110 & 160 & 150 & 60 \\ 100 & 90 & 80 & 70 \end{bmatrix}.$$

The 2D DFT of this image is the following (4 × 4) complex matrix:

$$[F_{p,s}] = \begin{bmatrix} \underline{1360} & -60-180i & 120 & -60+180 \\ -380-100i & -40+160i & -60-60i & 80-80i \\ -200 & -60+20i & -80 & -60-20i \\ -380+100i & 80+80i & -60+60i & -40-160i \end{bmatrix}. \tag{7.6}$$

We start with the generator $(p,\ s) = (0,1)$. It is not difficult to see that the corresponding splitting signal $f_{T_{0,1}} = \{f_{0,1,t};\ t = 0:3\}$ is $\{100,440,480,340\}$. The four-point DFT of this signal equals

$$F_4[f_{T_{0,1}}] = \{1360, -380-100i, -200, -380+100i\}.$$