Journal of Theoretical and Applied Information Technology
15th September 2022. Vol.100. No 17

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

OPTICAL HEVC CRYPTOSYSTEM USING INPUT AND FRACTIONAL FOURIER PLANES RANDOM ENCODING

MOHAMMED A. ALZAIN

Department of Information Technology, College of Computers and Information Technology,

Taif University, P.O. Box 11099, Taif 21944, Saudi Arabia

E-mail: m.alzain@tu.edu.sa

ABSTRACT

This paper present an efficient optical High efficiency video coding (HEVC) cryptosystem using input and Fractional Fourier (FrFT) planes random encoding. The encryption of the proposed optical HEVC cryptosystem using input and FrFT planes random encoding starts by separating each HECV plainvideo frame into RGB channel components and every one of HEVC RGB channel components is modulated in the input plane with the first random phase mask (RPM1). After that, the FrFT is applied to each one of HEVC RGB channel components. Then, every one of modulated HEVC RGB channel components in the FrFT is modulated again with the other RPM2 and the inverse of FrFT is employed. Finally, the HEVC RGB channel components are merged to get the HECV ciphervideo frame. The decryption of the proposed optical HEVC cryptosystem using input and FrFT planes random encoding starts by separating each HECV ciphervideo frame into RGB channel components and every one of HEVC ciphervideo frame RGB channel components is subjected to FrFT and modulated in the FrFT plane using the conjugate of RPM2. After that, the inverse of FrFT is applied to every one of modulated HEVC ciphervideo frame RGB channel components and modulated in the input plane using the conjugate of RPM1. Finally, the decrypted HEVC ciphervideo frame RGB channel components are combined to get the deciphered HECV frame. The proposed the proposed optical HEVC cryptosystem using input and FrFT planes random encoding is tested with different security metrics like visual inspecting, statistical, cipher quality, differential, and occluding tests. The outcome of tests ensures and confirms the effectiveness of the proposed optical HEVC cryptosystem using input and FrFT planes random encoding.

Keywords: *Optical Encryption, HEVC, Fractional Fourier Transform (FrFT)*

1. INTRODUCTION

Now, multimedia security technology has gained a lot of interest as a research topic because of the spread evolution in applying multimedia over the Internet and communication networks [1-5]. The multimedia streaming market may include hot commercial names like Netflix, Whatsapp, YouTube, Facebook, and Instagram. The multimedia streaming market may be subjected many attacks and so efficient security techniques must be employed to secure this market [6-12].

Multimedia encryption may be divided into scrambling-based encryption systems and substitution-based encryption systems [13-14]. In scrambling-based encryption systems, the main idea is based changing only the location of pixels. However scrambling-based encryption systems offer simplicity, and high speeds, but they suffer from weak security since they depend only on changing the positions of pixels. Examples of scrambling-based encryption systems may include chaos encryption [15-18]. A lot of researchers have introduced chaos encryption as a tool to achieve multimedia security. But, there exist many serious issues related to chaos encryption such as data expansion, performance speed, and weakness against differential attacks.

In substitution-based encryption systems, the main idea is based changing the values of pixels [19-22]. However substitution-based encryption systems offer good security, but they suffer serious issues like speed and their suitability to multimedia contents. Examples of substitution-based encryption systems may include RC5 [23], RC6 [24-25], and AES [26].

Optical encryption presents various benefits compared to common cipher systems. Optical encryption can encrypt with full speed and has no impact on the performance. In addition, it has low

computational costs, can work with different transport protocols and there is no need for any extra hardware [27-33].

In [34], the authors presented an optical image encryption system that encrypts an image into a cipherimage which appears as a white noise on each other. The encryption is performed in the fractional Fourier domain. Their system depends on a quadratic phase system (QPS) which provides the necessary planes for encryption. The encryption key consists of 6 parameters that control the QPS alongside the RPM. The tests have shown that this system is secure than other previous optical encryption systems.

In [35], the authors proposed a mono-spectral integral imaging encryption approach which is based on mono-spectral camera array (MCA). Their system removes color crosstalk between the neighboring spectral channels. Their system reduces the color image encryption to grayscale image encryption and consequently, their system is approximately three times faster than similar color image encryption. They also presented an optimized super-resolution rebuilding system to improve the viewing resolution of the images.

Most of optical encryption systems are symmetric. Symmetric encryption systems have the key distribution problem, which address how to securely transfer the key to the receiver for decryption. This problem does not exist in the asymmetric encryption systems.

In [36], the authors presented a biometric key-based asymmetric optical ciphering system. Their system is constructed using phase-retrieval system and phase-truncated Fourier transformation (PTFT). The encryption keys are the biometric and the PTFT RPM keys. The decryption keys are the binary and the PTFT phase-only mask keys.

In [37], the authors presented proposed a double opto encryption. The encrypted image is acquired by encoding it twice; first at the sender and then at the receiver. Consequently, no key exchange is required between the transmitter and the receiver. They presented two variants of their system; the first one utilizes optical encryption for both encryption operations. The second variant utilizes optical encryption for the first encryption operation and numerical encryption for the second encryption operation. Their tests have shown that the scheme produces high-quality decrypted images.

In [38], the authors presented opto image encryption using the DRPE and the Kronecker product of two random matrices in the Fresnel transform. The proposed system is analyzed and showed a high degree of robustness against various attacks.

In [39], the authors proposed optical encryption system that is capable of encrypting multiple images as once. Their system is based on computer generated hologram (CGH) and angle multiplexing. The images are encrypted in the Fresnel domain by modulating them using two independent phase keys with different diffraction distances, then a compound image is generated by coherent superposition the modulated images with solid angle multiplexed reference beams. Lastly, the Roman coding technique is used to encode the compound image to a CGH. This system has the advantage of using multiple keys in the form of diffraction distance and wavelength. In addition, this system is both time- and space-efficient.

In [40], the authors presented an optical image cipher system using joint transform correlator (JTC) and confused cipher image. Their system has enhanced security compared to traditional JTC cryptosystem since it eliminates the linear characteristics of the JTC-based cryptosystem. Their system is secure against linear attacks based on iterative Fourier Transform (IFT). In addition, their system is simple and cheap to implement.

The primary contributions of the proposed optical HEVC cryptosystem using input and FrFT planes random encoding are:

1- The proposed optical HEVC cryptosystem using input and FrFT planes random encoding has the ability to resist different types of attacks.
2- The proposed optical HEVC cryptosystem using input and FrFT planes random encoding is simple and can maintain low and minimized computational cost.
3- The proposed optical HEVC cryptosystem using input and FrFT planes random encoding has a negligible impact on the HEVC encoding efficiency.
4- The proposed optical HEVC cryptosystem using input and FrFT planes random encoding can be adapted for both low- resolution and high-resolution HEVC bitstreams.

The rest of paper is organized as follows. Section 2 presents the fractional Fourier transform (FrFT). Section 3 introduces the proposed optical HEVC cryptosystem using input and FrFT planes random encoding. Section 4 explores the obtained results and discussions. Section 5 presents the results of occluding with different percentages. Section 6 illustrates a comparative study of the proposed

optical HEVC cryptosystem using input and FrFT planes random encoding and a recent proposed scheme. Finally, Section 7 gives the conclusion of the paper.

2. FRACTIONAL FOURIER TRANSFORM (FRFT)

The FrFT represents a generalized form of conventional FT. The FrFT operates by rotating continuously the signal in time plane coordinates (i, j) to frequency plan coordinates (u, v) with a rotating angle $\alpha = a\pi/2$, $0 \le a \le 1$.

The FrFT of $x(i)$, with a transforming angle α is denoted $X_\alpha(u)$ and can be mathematically expressed as [41-47]:

$$X_\alpha(u) = \int_{-\infty}^{\infty} x(i)\, k_\alpha(i,u)\, dt \tag{1}$$

$$K_\alpha(i,u) = \begin{cases} \sqrt{\frac{1-j\cot\alpha}{2\pi}} \cdot \exp\left(j\frac{i^2+u^2}{2}\cot\alpha - j\frac{iu}{\sin\alpha}\right) & \text{if} \quad \alpha \neq n\pi \\ \delta(u-i) & \text{if} \quad \alpha = n\pi \\ \delta(u+i) & \text{if} \quad \alpha = (2n+1)\pi \end{cases} \tag{2}$$

For a function $f(x)$

$$f_a(u) = F^a[f(x)]$$

$$= C_\alpha \int f(x) \exp\left[i\pi \frac{u^2+x^2}{\tan\alpha} - 2i\pi \frac{ux}{\sin\alpha}\right] dx \tag{3}$$

where

$$\alpha = \frac{a\pi}{2} \tag{4}$$

$$C_\alpha = \frac{\exp\left[-i\left(\frac{\pi.sign(\sin(\alpha))}{4} - \frac{\alpha}{2}\right)\right]}{|\sin\alpha|^{1/2}} \tag{5}$$

where a and α denote the fractional transform order and FrFT operator [41-47].

3. THE PROPOSED OPTICAL HEVC CRYPTOSYSTEM USING INPUT AND FRFT PLANES RANDOM ENCODING

The proposed optical HEVC cryptosystem using input and FrFT planes random encoding has two modules; the encryption module and the decryption module.

The encryption of the proposed optical HEVC cryptosystem using input and FrFT planes random encoding starts by separating each HECV plainvideo frame into RGB channel components and every one of HEVC RGB channel components is modulated in the input plane with the first random phase mask (RPM1). After that, the FrFT is applied to each one of HEVC RGB channel components. Then, every one of modulated HEVC RGB channel components in the FrFT is modulated again with the other RPM2 and the inverse of FrFT is employed. Finally, the HEVC RGB channel components are merged to get the HECV ciphervideo frame. Figure 1 depicts the encryption module of the proposed optical HEVC cryptosystem using input and FrFT planes random encoding.

The encryption module steps of the proposed optical HEVC cryptosystem using input and FrFT planes random encoding are as follows:

1. Separate HEVC plainvideo bitstreams $PVF(x_i, y_j)$ into HEVC plainvideo frames $PVF_1(x_i, y_j)$, $PVF_2(x_i, y_j)$, ……, $PVF_n(x_i, y_j)$.

$$PVF(x_i,y_j) = (PVF_1(x_i,y_j), PVF_2(x_i,y_j), ..., PVF_n(x_i,y_j)) \tag{6}$$

2. Separate each HECV plainvideo frame $PVF_k(x_i, y_j)$ into its red, green and blue components $PVF_{rk}(x_i, y_j)$, $PVF_{gk}(x_i, y_j)$, and $PVF_{bk}(x_i, y_j)$, where $k = 1,2,3,.....n$.

$$PF_k(x_i,y_j) = (PF_{rk}(x_i,y_j), PF_{gk}(x_i,y_j), PF_{bk}(x_i,y_j)) \tag{7}$$

3. Each one of HEVC RGB channel components are modulated using the RPM1.

$$E_1[PVF_k(x_i,y_j)] = \begin{bmatrix} PVF_{rk}(x_i,y_j)\exp(j2\pi\theta_r(x_i,y_j)) \\ PVF_{gk}(x_i,y_j)\exp(j2\pi\theta_g(x_i,y_j)) \\ PVF_{bk}(x_i,y_j)\exp(j2\pi\theta_b(x_i,y_j)) \end{bmatrix} \tag{8}$$

4. The FrFT is applied to each one of HEVC frame RGB components.

$$E_2[PVF_k(x_i,y_j)] = \begin{bmatrix} \text{FrFT}[PVF_{rk}(x_i,y_j)\exp(j2\pi\theta_r(x_i,y_j))] \\ \text{FrFT}[PVF_{gk}(x_i,y_j)\exp(j2\pi\theta_g(x_i,y_j))] \\ \text{FrFT}[PVF_{bk}(x_i,y_j)\exp(j2\pi\theta_b(x_i,y_j))] \end{bmatrix} \tag{9}$$

5. Each one of complex modulated HEVC RGB channel components in the FrFT is again modulated with the RPM2 and the inverse of FrFT is applied.

$$CVF_k(x_i,y_j) = \begin{bmatrix} \text{FrFT}^{-1}[\text{FrFT}[PVF_{rk}(x_i,y_j)\exp(j2\pi\theta_r(x_i,y_j))]\exp(j2\pi\omega_r(u_i,v_j))] \\ \text{FrFT}^{-1}[\text{FrFT}[PVF_{gk}(x_i,y_j)\exp(j2\pi\theta_g(x_i,y_j))]\exp(j2\pi\omega_g(u_i,v_j))] \\ \text{FrFT}^{-1}[\text{FrFT}[PVF_{bk}(x_i,y_j)\exp(j2\pi\theta_b(x_i,y_j))]\exp(j2\pi\omega_b(u_i,v_j))] \end{bmatrix} \tag{10}$$

6. Combine HEVC ciphervideo frames $CVF_k(x_i, y_j)$ to get the HEVC ciphered bitstreams $CVF(x_i, y_j)$.

$$CVF(x_i,y_j) = (CVF_1(x_i,y_j), CVF_2(x_i,y_j), ..., CVF_n(x_i,y_j)) \tag{11}$$

Journal of Theoretical and Applied Information Technology
15th September 2022. Vol.100. No 17

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

The decryption of the proposed optical HEVC cryptosystem using input and FrFT planes random encoding starts by separating each HECV ciphervideo frame into RGB channel components and every one of HEVC ciphervideo frame RGB channel components is subjected to FrFT and modulated in the FrFT plane using the conjugate of RPM2. After that, the inverse of FrFT is applied to every one of modulated HEVC ciphervideo frame RGB channel components and modulated in the input plane using the conjugate of RPM1. Finally, the decrypted HEVC ciphervideo frame RGB channel components are combined to get the deciphered HECV frame. Figure 2 depicts the decryption module of the proposed optical HEVC cryptosystem using input and FrFT planes random encoding.

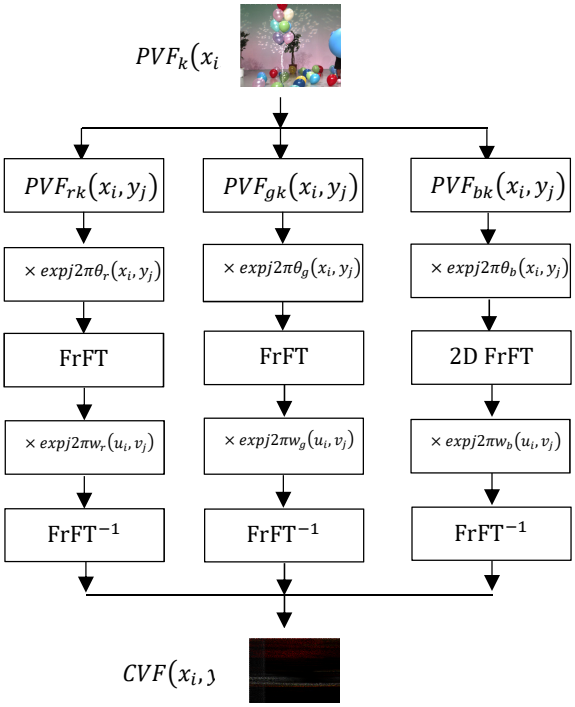


Figure 1: Encryption module of the proposed optical HEVC cryptosystem using input and FrFT planes random encoding

The decryption module steps of the proposed optical HEVC cryptosystem using input and FrFT planes random encoding can be listed as follows:

1. Separate HEVC ciphervideo bitstreams $CVF(x_i,y_j)$ into HEVC ciphervideo frames $CVF_1(x_i,y_j)$, $CVF_2(x_i,y_j)$, ……, $CVF_n(x_i,y_j)$.

$$CVF(x_i,y_j)=(CVF_1(x_i,y_j),CVF_2(x_i,y_j),.....,CVF_n(x_i,y_j)) \quad (12)$$

2. Separate each HECV ciphervideo frame $CVF_k(x_i,y_j)$ into RGB components $CVF_{rk}(x_i,y_j)$, $CVF_{gk}(x_i,y_j)$, and $CVF_{bk}(x_i,y_j)$, where $k=1,2,3,.....n$.

$$CVF_k(x_i,y_j)=(CVF_{rk}(x_i,y_j),CVF_{gk}(x_i,y_j),CVF_{bk}(x_i,y_j)) \quad (13)$$

3. Each one of HEVC ciphervideo frame R, G and B components is subjected to FrFT and modulated in the FrFT plane using the conjugate of RPM2.

$$D_k[CVF_k(x_i,y_j)]=\begin{bmatrix}\text{FrFT}[CVF_{rk}(x_i,y_j)]exp(-j2\pi\omega_r(u_i,v_j))\\ \text{FrFT}[CVF_{gk}(x_i,y_j)]exp-j2\pi\omega_g(u_i,v_j))\\ \text{FrFT}[CVF_{bk}(x_i,y_j)]exp(-j2\pi\omega_b(u_i,v_j))\end{bmatrix} \quad (14)$$

4. The inverse of FrFT is applied to each one of complex modulated HEVC ciphervideo frame red, green and blue components and modulated in the input plane using the conjugate of RPM1.

$$PVF_k(x_i,y_j)=\begin{bmatrix}FrFT^{-1}[\text{FrFT}[CVF_{rk}(x_i,y_j)]exp(-j2\pi\omega_r(u_i,v_j))]\exp(-j2\pi\theta_r(x_i,y_j))\\ FrFT^{-1}[\text{FrFT}[CVF_{gk}(x_i,y_j)]exp(-j2\pi\omega_g(u_i,v_j))]\exp(-j2\pi\theta_g(x_i,y_j))\\ FrFT^{-1}[\text{FrFT}[CVF_{bk}(x_i,y_j)]exp(-j2\pi\omega_b(u_i,v_j))]\exp(-j2\pi\theta_b(x_i,y_j))\end{bmatrix} \quad (15)$$

5. Combine HEVC decrypted ciphervideo frames $PVF_k(x_i,y_j)$ to get the HEVC decrypted bitstreams $PVF(x_i,y_j)$.

$$PVF(x_i,y_j)=(PVF_1(x_i,y_j),PVF_2(x_i,y_j),.....,PVF_n(x_i,y_j)) \quad (16)$$

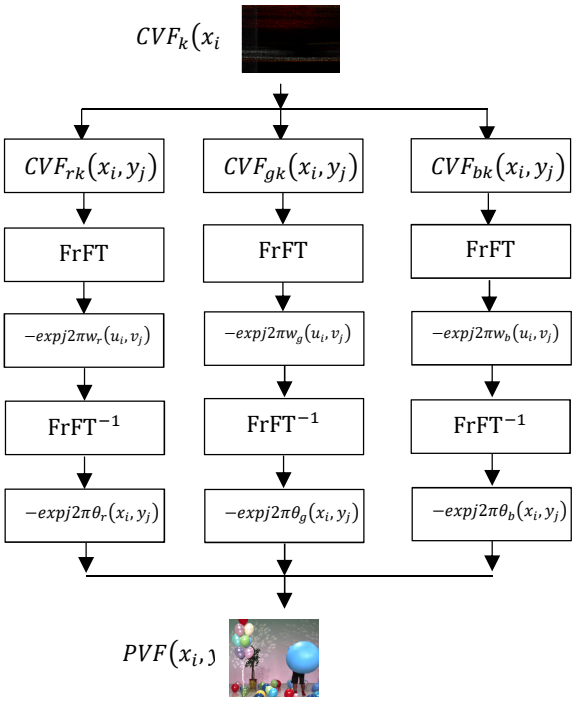


Figure 2: Decryption module of the proposed optical HEVC cryptosystem using input and FrFT planes random encoding

Journal of Theoretical and Applied Information Technology
15th September 2022. Vol.100. No 17

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

4. RESULTS AND DISCUSSIONS

For security testing of the proposed optical HEVC cryptosystem using input and FrFT planes random encoding, four HEVC plainvideos are employed as the source plainvideos which are encrypted using the proposed optical HEVC cryptosystem using input and FrFT planes random encoding. The plainvideos include Vassar, Balloons, Ballet, and Ballaroom videos as depicted Figure 3. For testing the security of the optical HEVC cryptosystem using input and FrFT planes random encoding, a set of tests are employed like visual inspection, entropy, histogram, ciphervideo quality, differential, and noise occluding tests [14-19].

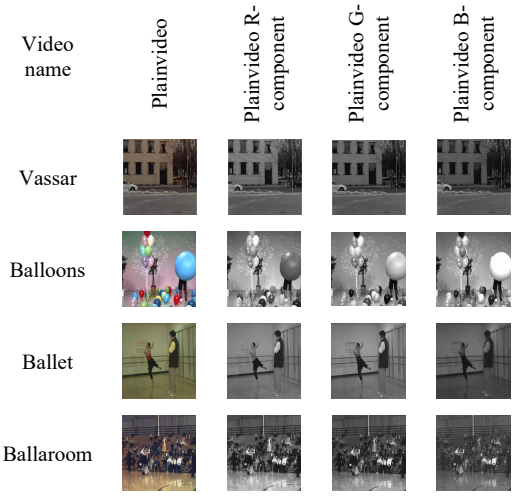


Figure 3: Plainvideo test samples with its RGB channel components

4.1 Visual Inspecting

The visually inspected results for encrypting Vassar, Balloons, Ballet, and Ballaroom plainvideos with their RGB components by the proposed optical HEVC cryptosystem using input and FrFT planes random encoding are illustrated in Figure 4. It is demonstrated that plainvideos RGB channel components are totally hidden. So, the proposed optical HEVC cryptosystem using input and FrFT planes random encoding gained in hiding the specifics of plainvideos.

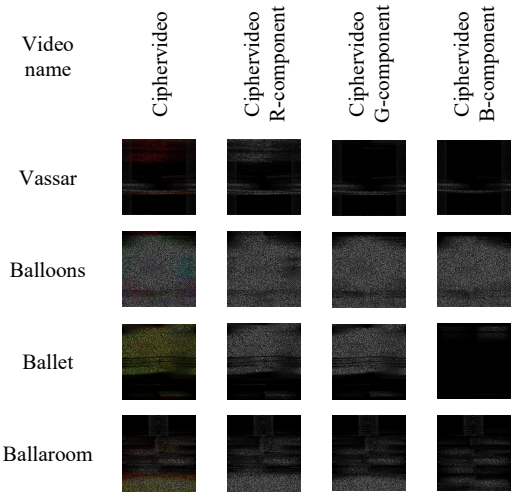
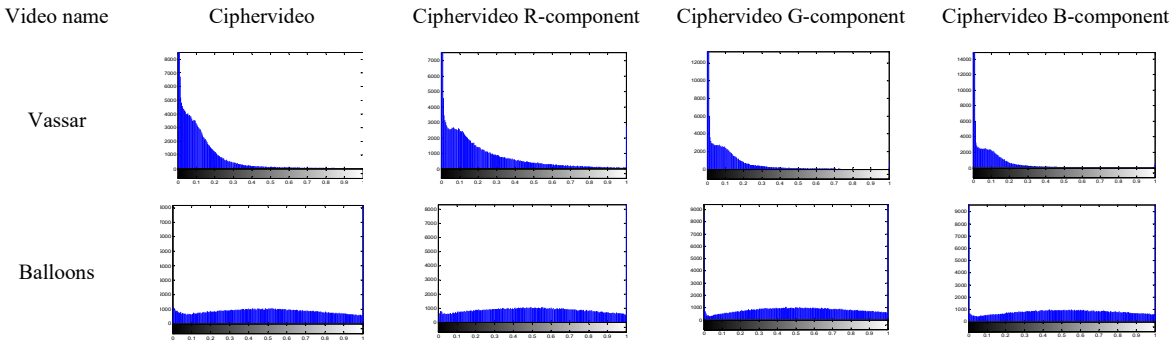


Figure 4: Visual results of ciphervideo RGB channel components of different plainvideo test samples for the proposed optical HEVC cryptosystem using input and FrFT planes random encoding

4.2 Histograms Testing

The histogram of plainvideo frame illustrates the relationship among pixel intensities against the occurrences number of each pixel intensity [48-49]. The histograms of the ciphervideos using the proposed optical HEVC cryptosystem using input and FrFT planes random encoding are shown in Figure 5. It may be confirmed that the ciphervideos statistical distributions are completely different from statistical distributions of their corresponding plainvideos which again confirms the efficiency of the proposed optical HEVC cryptosystem using input and FrFT planes random encoding.



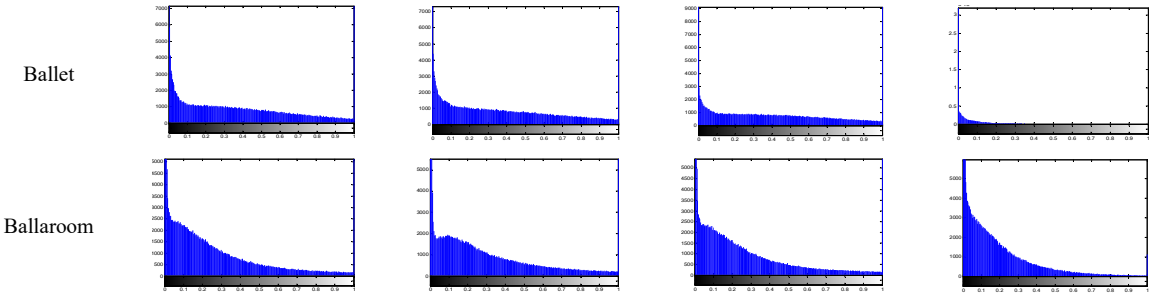


Figure 5: Histogram of ciphervideo RGB channel components of different plainvideo test samples for the proposed optical HEVC cryptosystem using input and FrFT planes random encoding

4.3 Entropy Testing

The entropy may be mathematically formulated as follows [50].

$$IE(x) = \sum_{i=1}^{2^N-1} P(x_i)\log_2 \frac{1}{P(x_i)} \quad (17)$$

where $IE(x)$ and $P(x_i)$ denote the entropy value and the occurrence probability of the symbol x_i.

The entropy results of ciphervideo RGB channel components of different plainvideo test samples for the proposed optical HEVC cryptosystem using input and FrFT planes random encoding is shown in Table 1.

It is obvious that the entropy of ciphervideo RGB channel components of different plainvideo test samples for the proposed optical HEVC cryptosystem using input and FrFT planes random encoding are near to its ideal value of 8.0, which can indicate that the information leakage amount during the ciphering may be neglected. So, the proposed optical HEVC cryptosystem using input and FrFT planes random encoding can be considered immune and resistant to entropy attack.

Table 1: Entropy results of ciphervideo red, green, and blue components of different plainvideo test samples for the proposed optical HEVC cryptosystem using input and FrFT planes random encoding

Video name	Ciphervideo average entropy	Ciphervideo R-component	Ciphervideo G-component	Ciphervideo B-component
Vassar	5.332	5.332	5.332	5.332
Balloons	6.943	6.943	6.943	6.943
Ballet	5.259	5.259	5.259	5.259
Ballaroom	6.903	6.903	6.903	6.903

4.4 Correlation coefficients (CC) Tests

The $\mathrm{CC(P,C)}$ between the plainvideo frame $P(x, y_j)$ and ciphervideo frame $C(x, y_j)$ can be mathematically expressed as [51]:

$$CC(P,C) = \frac{E\{(C-E(C))\cdot(P-E(P))\}}{\sqrt{E\{[C-E(C)]^2\}}\sqrt{E\{[P-E(P)]^2\}}} \quad (18)$$

where $E\{\cdot\}$ is the expectation sign.

The CC results of ciphervideo RGB channel components of different plainvideo test samples for the proposed optical HEVC cryptosystem using input and FrFT planes random encoding is shown in Table 2.

It is obvious that the CC values of ciphervideo RGB channel components of different plainvideo test samples for the proposed optical HEVC cryptosystem using input and FrFT planes random encoding are relatively low, which can indicate that the proposed optical HEVC cryptosystem using input and FrFT planes random encoding can be considered immune and resistant to correlation coefficient attack.

Table 2: Correlation coefficients results of ciphervideo red, green, and blue components of different plainvideo test samples for the proposed optical HEVC cryptosystem using input and FrFT planes random encoding

Video name	Ciphervideo average correlation	Ciphervideo R-component	Ciphervideo G-component	Ciphervideo B-component
Vassar	0.2022	0.2661	0.1665	0.1739
Balloons	0.2251	0.0023	0.1997	0.2394
Ballet	0.2451	0.2668	0.2874	0.1811
Ballaroom	0.4760	0.5602	0.5524	0.3155

4.5 Irregularity tests

The irregular deviation tests the encryption quality with respect to how the deviation due to ciphering is irregular [52].

The irregular deviation DI can be mathematically denoted as follows [52]:

$$\mathrm{D_i} = \frac{\sum_{i=0}^{i=255} \mathrm{HD\ (i)}}{\mathrm{N} * \mathrm{M}} \quad (19)$$

$$HD(i) = |H(i) - HM| \quad (20)$$

where N and M denote the image dimensions. The lower the irregular deviation is, the better the encrypted image quality.

The irregular deviation results of ciphervideo red, green, and blue components of different plainvideo test samples for the proposed optical HEVC cryptosystem using input and FrFT planes random encoding is shown in Table 3.

It is obvious that the irregular deviation of ciphervideo RGB channel components of different plainvideo test samples for the proposed optical HEVC cryptosystem using input and FrFT planes random encoding are low, which can indicate the effectiveness of the proposed optical HEVC cryptosystem using input and FrFT planes random encoding.

Table 3 Irregular deviation results of ciphervideo RGB channel components of different plainvideo test samples for the proposed optical HEVC cryptosystem using input and FrFT planes random encoding

Video name	Ciphervideo average irregularity	Ciphervideo R-component	Ciphervideo G-component	Ciphervideo B-component
Vassar	1.9843	1.9842	1.9843	1.9844
Balloons	1.9769	1.9777	1.9765	1.9765
Ballet	1.9846	1.9812	1.9807	1.9919
Ballaroom	1.9825	1.98148	1.9817	1.9844

5. EFFECT OF OCCLUSION ATTACK

The immunity to occlusion attack is the ability to decipher the ciphervideo correctly while subjected to occlusion during transmission. The resistance to occlusion attack of the proposed system is tested by occluding the ciphervideo with different occlusion percentages prior to decryption. Several measures are used to test the impact of occluding attack like peak signal to noise ratio (PSNR), Structure Similarity Index Method (SSIM) and Features Similarity Index Matrix (FSIM).

The PSNR is calculated as [53-54]:

$$\mathrm{PSNR(O,D)} = 10\ \log_{10}\frac{(255)^2}{\mathrm{MSE(O,D)}} \quad (21)$$

where MSE is defined as [53-54]:

$$\mathrm{MSE(O,D)} = \frac{1}{\mathrm{MN}}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}[\mathrm{O(x,y_j)} - \mathrm{D(x_i,y_j)}]^2 \quad (22)$$

where $O(x_i, y_j)$ and $D(x_i, y_j)$ represent the pixel value at position x_i, y_j.

The SSIM is calculated as follows [55]:

$$\mathrm{SSIM} = \frac{(2m_o m_r + c_1)(2\sigma_{or} + c_2)}{(m_o^2 m_r^2 + c_1)(\sigma_o^2 + \sigma_r^2 + c_2)} \quad (23)$$

The FSIM can be calculated as [56]:

$$FSIM = [S_{pc}]^a . [S_G]^b \quad (24)$$

$$S_{pc} = \frac{2PC_1PC_2 + T_1}{PC_1^2 + PC_2^2 + T_1} \quad (25)$$

$$S_G = \frac{2G_1G_2 + T_2}{G_1^2 + G_2^2 + T_2} \quad (26)$$

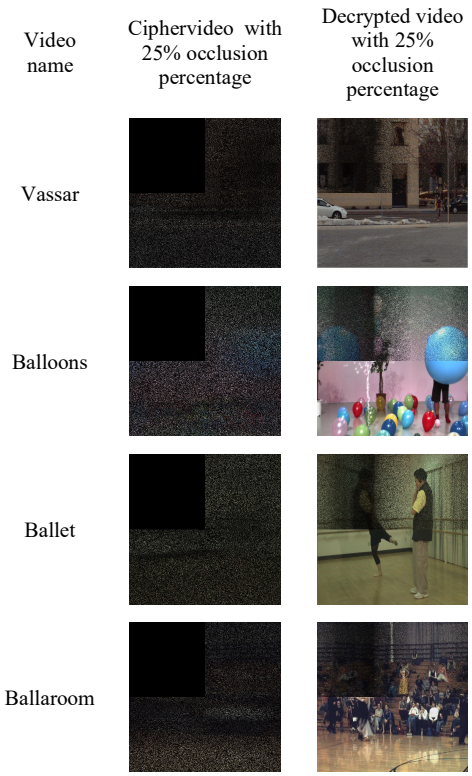
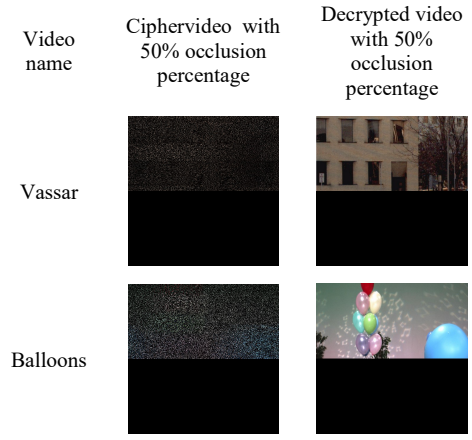


Figure 6: Ciphervideos and decrypted ciphervideos with 25% occlusion percentage of different plainvideo test samples for the proposed optical HEVC cryptosystem using input and FrFT planes random encoding



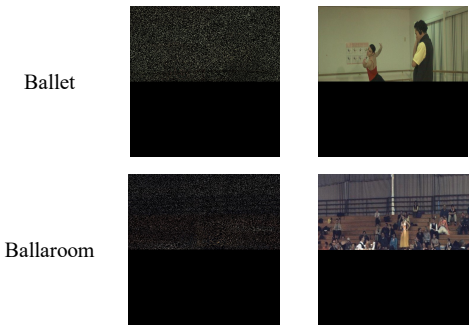


Figure 7: Ciphervideos and decrypted ciphervideos with 50% occlusion percentage of different plainvideo test samples for the proposed optical HEVC cryptosystem using input and FrFT planes random encoding

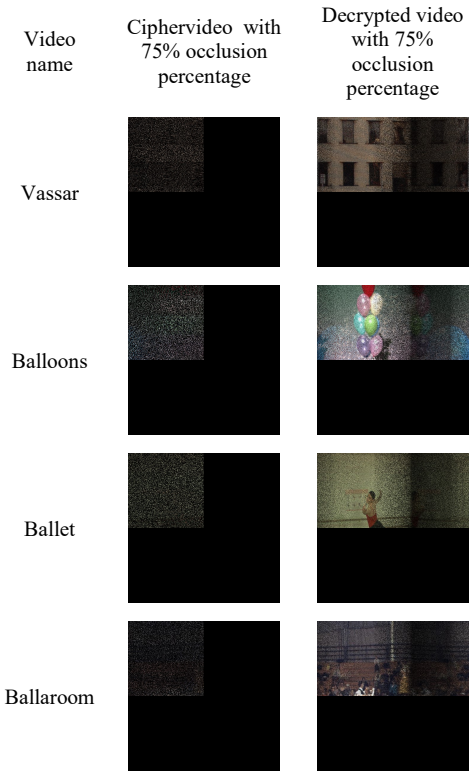


Figure 8: Ciphervideos and decrypted ciphervideos with 75% occlusion percentage of different plainvideo test samples for the proposed optical HEVC cryptosystem using input and FrFT planes random encoding

The visual inspecting results of ciphervideos and decrypted ciphervideos with 25%, %50, and %75 occlusion percentages of different plainvideo test samples for the proposed optical HEVC cryptosystem using input and FrFT planes random encoding are illustrated in Figures 6, 7, and 8. The visual inspecting results confirm the success of the proposed optical HEVC cryptosystem using input and FrFT planes random encoding in decrypting the ciphervideos even with 25%, %50, and %75 occlusion percentages and retrieving most of the plainvideos. But, the probability of retrieving decrypted videos increases with decreased occlusion percentages.

The results of PSNR between the plainvideo and decrypted ciphervideos with 25%, %50, and %75 occlusion percentages for the proposed optical HEVC cryptosystem using input and FrFT planes random encoding are shown in Tables 4, 5, and 6. From the PSNR results, we can make a conclusion that the PSNR increases with decreasing the occlusion percentage.

Table 4: PSNR results of decrypted ciphervideos with 25% occlusion percentage and their corresponding plainvideos for the proposed optical HEVC cryptosystem using input and FrFT planes random encoding

Video name	Ciphervideo average PSNR	Ciphervideo R-component	Ciphervideo G-component	Ciphervideo B-component
Vassar	65.61	64.32	65.56	66.96
Balloons	61.40	61.300	61.34	61.58
Ballet	63.65	62.73	62.77	65.46
Ballaroom	66.90	66.37	67.36	66.98

Table 5: PSNR results of decrypted ciphervideos with 50% occlusion percentage and their corresponding plainvideos for the proposed optical HEVC cryptosystem using input and FrFT planes random encoding

Video name	Ciphervideo average PSNR	Ciphervideo R-component	Ciphervideo G-component	Ciphervideo B-component
Vassar	60.19	59.73	60.26	60.60
Balloons	55.65	55.36	56.18	55.44
Ballet	59.84	58.63	58.76	62.13
Ballaroom	58.21	56.88	58.10	59.65

Table 6: PSNR results of decrypted ciphervideos with 75% occlusion percentage and their corresponding plainvideos for the proposed optical HEVC cryptosystem using input and FrFT planes random encoding

Video name	Ciphervideo average PSNR	Ciphervideo R-component	Ciphervideo G-component	Ciphervideo B-component
Vassar	59.47	58.86	59.54	60.00
Balloons	54.62	54.60	54.99	54.25
Ballet	58.46	57.38	57.41	60.59
Ballaroom	57.60	56.38	57.55	58.88

The results of SSIM of the plainvideo and decrypted ciphervideos with 25%, %50, and %75

occlusion percentages for the proposed optical HEVC cryptosystem using input and FrFT planes random encoding are shown in Tables 7, 8, and 9. From the SSIM, we can make a conclusion that the SSIM increases with decreasing the occlusion percentage.

Table 7: SSIM results of decrypted ciphervideos with 25% occlusion percentage and their corresponding plainvideos for the proposed optical HEVC cryptosystem using input and FrFT planes random encoding

Video name	Ciphervideo average SSIM	Ciphervideo R-component	Ciphervideo G-component	Ciphervideo B-component
Vassar	0.9978	0.9971	0.9978	0.9984
Balloons	0.9945	0.9942	0.9944	0.9949
Ballet	0.9965	0.9958	0.9959	0.9977
Ballaroom	0.9985	0.9983	0.9987	0.9985

Table 8: SSIM results of decrypted ciphervideos with 50% occlusion percentage and their corresponding plainvideos for the proposed optical HEVC cryptosystem using input and FrFT planes random encoding

Video name	Ciphervideo average SSIM	Ciphervideo R-component	Ciphervideo G-component	Ciphervideo B-component
Vassar	0.9913	0.9903	0.9915	0.9921
Balloons	0.9752	0.9734	0.9782	0.9742
Ballet	0.9894	0.9869	0.9873	0.9941
Ballaroom	0.9859	0.9818	0.9861	0.9899

Table 9: SSIM results of decrypted ciphervideos with 75% occlusion percentage and their corresponding plainvideos for the proposed optical HEVC cryptosystem using input and FrFT planes random encoding

Video name	Ciphervideo average SSIM	Ciphervideo R-component	Ciphervideo G-component	Ciphervideo B-component
Vassar	0.9901	0.9887	0.9903	0.9913
Balloons	0.9694	0.9690	0.9722	0.9671
Ballet	0.9865	0.9836	0.9837	0.9921
Ballaroom	0.9843	0.9799	0.9845	0.9883

The results of FSIM of the plainvideo and decrypted ciphervideos with 25%, %50, and %75 occlusion percentages for the proposed optical HEVC cryptosystem using input and FrFT planes random encoding are shown in Tables 10, 11, and 12. From the FSIM, we can make a conclusion that the FSIM increases with decreasing the occlusion percentage.

Table 10: FSIM results of decrypted ciphervideos with 25% occlusion percentage and their corresponding plainvideos for the proposed optical HEVC cryptosystem using input and FrFT planes random encoding

Video name	Ciphervideo average FSIM	Ciphervideo R-component	Ciphervideo G-component	Ciphervideo B-component
Vassar	0.9488	0.9479	0.9481	0.9505
Balloons	0.9599	0.9616	0.9573	0.9607
Ballet	0.9536	0.9519	0.9523	0.9567
Ballaroom	0.9798	0.9819	0.9813	0.9762

Table 11: FSIM results of decrypted ciphervideos with 50% occlusion percentage and their corresponding plainvideos for the proposed optical HEVC cryptosystem using input and FrFT planes random encoding

Video name	Ciphervideo average FSIM	Ciphervideo R-component	Ciphervideo G-component	Ciphervideo B-component
Vassar	0.9523	0.9546	0.9539	0.9486
Balloons	0.9361	0.9378	0.9342	0.9363
Ballet	0.9288	0.9257	0.9261	0.9345
Ballaroom	0.9414	0.9401	0.9413	0.9419

Table 12: FSIM results of decrypted ciphervideos with 75% occlusion percentage and their corresponding plainvideos for the proposed optical HEVC cryptosystem using input and FrFT planes random encoding

Video name	Ciphervideo average FSIM	Ciphervideo R-component	Ciphervideo G-component	Ciphervideo B-component
Vassar	0.9223	0.9247	0.9214	0.9209
Balloons	0.8904	0.8950	0.8897	0.8866
Ballet	0.8857	0.8819	0.8832	0.8919
Ballaroom	0.9169	0.9166	0.9173	0.9168

6. COMPARATIVE ANALYSIS

To prove the efficiency of the proposed optical HEVC cryptosystem using input and FrFT planes random encoding for efficient transmission of HEVC, a comparison is performed on the proposed optical HEVC cryptosystem and a recent proposed scheme [57] in terms of PSNR, SSIM, and FSIM. The comparison is employed using the Balloons video and the results of comparison are listed in Table 13. Form the comparative PSNR, SSIM, and FSIM results in Table 13; it is observed clear that the proposed optical HEVC cryptosystem using input and FrFT planes random encoding outperforms the proposed scheme in [57] in terms of PSNR, SSIM, and FSIM.

Table 13: Comparison between proposed optical HEVC cryptosystem using input and FrFT planes random encoding and a recent state-of-the-art scheme [57]

Measure \ Scheme	Proposed	Ref. [57]
PSNR	61.40	9.8048
SSIM	0.9945	0.0457
FSIM	0.9599	0.5337

7. CONCLUSION

This paper introduced an efficient optical HEVC cryptosystem using input and FrFT planes random encoding. The proposed optical HEVC cryptosystem using input and FrFT planes random encoding has two modules; the encryption module and the decryption module. The proposed optical HEVC cryptosystem using input and FrFT planes random encoding modulates the HEVC plainvideo bitstreams in the input plane using RPM1 and in FrFT using RPM2. A group of security tests like visual inspecting, statistical, cipher quality, differential, and occluding attacks are performed on the proposed optical HEVC cryptosystem using input and FrFT planes random encoding. The results of security tests indicate that the proposed optical HEVC cryptosystem using input and FrFT planes random encoding is resistant and immune against different types of security attacks.

REFERENCES:

[1] Gutub, A., Al-Juaid, N., & Khan, E. (2019). Counting-based secret sharing technique for multimedia applications. Multimedia Tools and Applications, 78(5), 5591-5619.

[2] Botta, M., Cavagnino, D., & Pomponiu, V. (2014). Protecting the content integrity of digital imagery with fidelity preservation: an improved version. ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM), 10(3), 29.

[3] Al-Ghamdi, M., Al-Ghamdi, M., & Gutub, A. (2018). Security enhancement of shares generation process for multimedia counting-based secret-sharing technique. Multimedia Tools and Applications, 1-28.

[4] Dutta, T., & Gupta, H. P. (2017). An efficient framework for compressed domain watermarking in p frames of high-efficiency video coding (HEVC)--encoded video. ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM), 13(1), 1-24.

[5] Xu, D. (2019). Commutative Encryption and data hiding in HEVC Video Compression. IEEE Access, 7, 66028-66041.

[6] Long, M., Peng, F., & Li, H. Y. (2018). Separable reversible data hiding and encryption for HEVC video. Journal of Real-Time Image Processing, 14(1), 171-182.

[7] Yang, J., & Li, S. (2018). An efficient information hiding method based on motion vector space encoding for HEVC. Multimedia Tools and Applications, 77(10), 11979-12001.

[8] Wang, C., Shan, R., & Zhou, X. (2018). Anti-HEVC recompression video watermarking algorithm based on the all phase biorthogonal transform and SVD. IETE Technical Review, 35(sup1), 42-58.

[9] Chang, P. C., Chung, K. L., Chen, J. J., Lin, C. H., & Lin, T. J. (2014). A DCT/DST-based error propagation-free data hiding algorithm for HEVC intra-coded frames. Journal of Visual Communication and Image Representation, 25(2), 239-253.

[10] El-Latif, A. A. A., Abd-El-Atty, B., Hossain, M. S., Rahman, M. A., Alamri, A., & Gupta, B. B. (2018). Efficient quantum information hiding for remote medical image sharing. IEEE Access, 6, 21075-21083.

[11] Guesmi, R., Farah, M. A. B., Kachouri, A., & Samet, M. (2016). Hash key-based image encryption using crossover operator and chaos. Multimedia tools and applications, 75(8), 4753-4769.

[12] Zou, L., Sun, J., Gao, M., Wan, W., & Gupta, B. B. (2019). A novel coverless information hiding method based on the average pixel value of the sub-images. Multimedia Tools and Applications, 78(7), 7965-7980.

[13] Patidar, V., Pareek, N. K., & Sud, K. K. (2009). A new substitution–diffusion-based image cipher using chaotic standard and logistic maps. Communications in Nonlinear Science and Numerical Simulation, 14(7), 3056-3075.

[14] Xu, L., Gou, X., Li, Z., & Li, J. (2017). A novel chaotic image encryption algorithm using block scrambling and dynamic index-based diffusion. Optics and Lasers in Engineering, 91, 41-52.

[15] 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.

[16] Zhu Z, Zhang W, Wong K, Yu H (2011) A chaos-based symmetric image encryption scheme using a bit-level permutation. Information Sciences 181(6):1171-1186

[17] Özkaynak, F., & Özer, A. B. (2016). Cryptanalysis of a new image encryption algorithm based on chaos. Optik-International Journal for Light and Electron Optics, 127(13), 5190-5192.

[18] Gan Z, Chai X, Han D, Chen Y (2019) A chaotic image encryption algorithm based on 3-D bit-plane permutation. Neural Computing and Applications 31(11):7111-7130

[19] Chen, J., Zhu, Z. L., Zhang, L. B., Zhang, Y., & Yang, B. Q. (2018). Exploiting self-adaptive permutation–diffusion and DNA random encoding for secure and efficient image encryption. Signal Processing, 142, 340-353.

[20] Seyedzadeh S, Mirzakuchaki S (2012) A fast color image encryption algorithm based on coupled two-dimensional piecewise chaotic map. Signal processing 92(5):1202-1215

[21] Xu L, Gou X, Li Z, Li J (2017) A novel chaotic image encryption algorithm using block scrambling and dynamic index-based diffusion. Optics and Lasers in Engineering 91:41-52

[22] 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

[23] O. S. Faragallah, A. I. Sallam and H. S. El-Sayed, "Visual protection using RC5 selective encryption in telemedicine," Intelligent Automation & Soft Computing, vol. 31, pp. 1717-190, 2022.

[24] O. S. Faragallah, A. Afifi, W. El-Shafai, H. S. El-sayed, M. A. AlZain, J. F. Al-Amri, and F. E. Abd El-Samie, "Efficiently encrypting color images with few details based on RC6 and different operation modes for cybersecurity applications," IEEE Access, vol. 8, pp. 103200-103218, 2020.

[25] O. S. Faragallah, H. S. El-sayed, A. Afifi, and S. F. El-Zoghdy, "Small details gray scale image encryption using RC6 block cipher," wireless Personal Communications, vol. 118, no. 2, pp. 1559-1589, 2021.

[26] A. Arab, M. J. Rostami and B. Ghavami, "An image encryption method based on chaos system and AES algorithm," The Journal of Supercomputing, vol. 75, pp. 6663–6682, 2019.

[27] Yu C, Li J, Li X, Ren X, Gupta B (2018) Four-image encryption scheme based on quaternion Fresnel transform, chaos and computer generated hologram. Multimedia Tools and Applications 77(4):4585-4608

[28] Liu S, Guo C, Sheridan J (2014) A review of optical image encryption techniques. Optics & Laser Technology 57:327-342

[29] Sudheesh K Rajput, Osamu Matoba, "Optical voice encryption based on digital holography," Opt Lett., vol. 42(22), pp. 4619-4622, 2017, doi: 10.1364/OL.42.004619. 2017.

[30] Chen, J. X., Zhu, Z. L., Fu, C., & Yu, H. (2015). Optical image encryption scheme using 3-D chaotic map based joint image scrambling and random encoding in gyrator domains. Optics Comm., 341, 263-270.

[31] Yu, C., Li, J., Li, X. et al. Four-image encryption scheme based on quaternion Fresnel transform, chaos and computer-generated hologram. Multimed Tools Appl (2018) 77: 4585.

[32] Ahmad M. Elshamy, Fathi E. Abd El-Samie, Osama S. Faragallah, Sayed M. Elshamy, Hala S. El-sayed, S. F. El-Zoghdy, Ahmed N. Z. Rashed, Abd El-Naser A. Mohamed, and Ahmad Q. Alhamad, "Optical Image Cryptosystem Using Double Random Phase Encoding and Arnold's Cat Map," Optical and Quantum Electronics, vol. 48(3):212, pp. 1-18, 2016, Springer.

[33] Osama S. Faragallah, Ashraf Afifi, "Optical color image cryptosystem using chaotic baker mapping based-double random phase encoding," Optical and Quantum Electronics, vol. 49(3):89, pp. 1-28, 2017, Springer.

[34] G. Unnikrishnan, J. Joseph, and K. Singh, "Optical encryption by double-random phase encoding in the fractional Fourier domain," Opt. Lett. 25, 887-889 (2000).

[35] Xiaowei Li, Min Zhao, Yan Xing, Lei Li, Seok-Tae Kim, Xin Zhou, and Qiong-Hua Wang, "Optical encryption via monospectral integral imaging," Opt. Express 25, 31516-31527 (2017).

[36] Gaurav Verma, Meihua Liao, Dajiang Lu, Wenqi He, Xiang Peng, Aloka Sinha, An optical asymmetric encryption scheme with biometric keys, Optics and Lasers in Engineering, Volume 116, 2019, Pages 32-40.

[37] Cheremkhin, Pavel A., Nikolay N. Evtikhiev, Vitaly V. Krasnov, Vladislav G. Rodin, Anna V. Shifrina, and Rostislav S. Starikov. "Asymmetric image optical encryption under spatially incoherent illumination." Laser Physics Letters 17, no. 2 (2020): 025204.

[38] Ravi Kumar, Basanta Bhaduri, Optical image encryption using Kronecker product and hybrid phase masks, Optics & Laser Technology, Volume 95, 2017, Pages 51-55.

[39] Sixing Xi, Nana Yu, Xiaolei Wang, Xueguang Wang, Liying Lang, Huaying Wang, Weiwei Liu, Hongchen Zhai, Optical encryption scheme for multiple-image based on spatially angular multiplexing and computer generated hologram, Optics and Lasers in Engineering, Volume 127, 2020, 105953.

[40] Jianjun Cai, Xueju Shen, Cong Fan, Bing Zhou, Security-enhance optical encryption based on JTC architecture with confused ciphertext, Optik, 2019,163742.

[41] J. Dou, Q. He, Y. Peng, Q. Sun, S. Liu, Z. Liu, "A convolution-based fractional transform," Optical and Quantum Electronics, vol. 48(8), pp. 400-407, 2016.

[42] Heba M. Elhoseny, Osama S. Faragallah, Hossam E.H. Ahmed, Hassan B. Kazemian, Hala S. El-sayed, Fathi E. Abd El-Samie, "The Effect of Fractional Fourier Transform in Encryption

Quality for Digital Images," Optik-International Journal for Light and Electron Optics, vol. 127(1), pp. 315-319, 2016.

[43] Heba M. Elhoseny, Hossam E. H. Ahmed, Alaa M. Abbas, Hassan B. Kazemian, Osama S. Faragallah, Sayed M. El-Rabaie, Fathi E. Abd El-Samie, "Chaotic encryption of images in the fractional Fourier transform domain using different modes of operation," Signal, Image and Video Processing Journal, vol. 9(3), pp. 611-622, 2015.

[44] Kong D, Shen X (2014) Multiple-image encryption based on optical wavelet transform and multichannel fractional Fourier transform. Optics & Laser Technology 57:343-349

[45] Liansheng S, Xiao Z, Chongtian H, Ailing T, Asundi A (2019) Silhouette-free interference-based multiple-image encryption using cascaded fractional Fourier transforms. Optics and Lasers in Engineering 113:29-37

[46] Sui L, Gao B (2013) Single-channel color image encryption based on iterative fractional Fourier transform and chaos. Optics & Laser Technology 48:117-127

[47] Ran Q, Zhao T, Yuan L, Wang J, Xu L (2014) Vector power multiple-parameter fractional Fourier transform of image encryption algorithm. Optics and Lasers in Engineering 62:80-86

[48] Liansheng S, Yin C, Zhanmin W, Ailing T, Asundi A (2018) Single-pixel correlated imaging with high-quality reconstruction using iterative phase retrieval algorithm. Optics and Lasers in Engineering 111:108-113

[49] Chai X, Wu H, Gan Z, Zhang Y, Chen Y, Nixon K (2020) An efficient visually meaningful image compression and encryption scheme based on compressive sensing and dynamic LSB embedding. Optics and Lasers in Engineering 124:105837

[50] H. Chen, C. Tanougast, Z. Liu, W. Blondel, and B. Hao, "Optical hyperspectral image encryption based on improved Chirikov mapping and gyrator transform," Optics and Lasers in Engineering, vol. 107, pp. 62-70, 2018.

[51] Chen J, Zhu Z, Zhang L, Zhang Y, Yang B (2018) Exploiting self-adaptive permutation–diffusion and DNA random encoding for secure and efficient image encryption. Signal Processing 142:340-353

[52] O. S. Faragallah, A. Afifi, W. El-Shafai, H. S. El-sayed, E. A. Naeem, M. A. AlZain, J. F. Al-Amri, B. Soh, and F. E. Abd El-Samie, "Investigation of chaotic image encryption in spatial and FrFT domains for cybersecurity applications," IEEE Access, vol. 8, pp. 42491-42503, 2020.

[53] S. Sun, "A Novel Hyperchaotic Image Encryption Scheme Based on DNA Encoding, Pixel-Level Scrambling and Bit-Level Scrambling," IEEE Photonics Journal, vol. 10, pp. 1-14, 2018.

[54] O. S. Faragallah, A. Afifi, I. F. Elashry, E. A. Naeem H. M. El-Hoseny, H. S. El-sayed, and A. M. Abbas, "Efficient optical double image cryptosystem using chaotic mapping-based Fresnel transform," Optical and Quantum Electronics, vol. 53, pp. 1-26, 2021.

[55] O. S. Faragallah, Hala S. El-sayed, Ashraf Afifi, Walid El-Shafai, "Efficient and secure opto-cryptosystem for color images using 2D logistic-based fractional Fourier transform," Optics and Lasers in Engineering, vol. 137, 106333, Feb. 2021.

[56] O. S. Faragallah, W. El-Shafai, A. I. Sallam, I. Elashry, E. M. EL-Rabaie, A. Afifi, M. A. AlZain, J. F. Al-Amri, F. E. Abd El-Samie, and H. S. El-sayed, "Cybersecurity framework of hybrid watermarking and selective encryption for secure HEVC communication," Journal of Ambient Intelligence and Humanized Computing, vol. 13, pp. 1215-1239, 2022.

[57] O. S. Faragallah, W. El-Shafai, A. Afifi, I. Elashry, M. A. AlZain, J. F. Al-Amri, B. Soh, H. M. El-Hoseny, H. S. El-Sayed, F. E. Abd El-Samie, "Efficient three-dimensional video cybersecurity framework based on double random phase encoding," Intelligent Automation & Soft Computing, vol. 28, no.2, pp. 353–367, 2021.