

Opto-Video Encryption Based on Logistic Adjusted Sine map in FrFT

Osama S. Faragallah^{1,*}, Ashraf Afifi¹, Ibrahim F. Elashry², Ensherah A. Naeem³,
Heba M. El-Hoseny⁴, Ahmed I. Sallam⁵ and Hala S. El-sayed⁶

¹Department of Information Technology, College of Computers and Information Technology, Taif University,
P.O. Box 11099, Taif 21944, Saudi Arabia

²Department of Electrical Engineering, Kafrelsheikh University, Kafrelsheikh 61519, Egypt

³Electrical Department, Faculty of Industrial Education, Suez University, Suez 43527, Egypt

⁴Department of Electronics and Electrical Communication Engineering, Al-Obour High Institute for Engineering
and Technology 3036, Egypt

⁵Department of Computer Science and Engineering, Faculty of Electronic Engineering, Menoufia University,
Menouf 32952, Egypt

⁶Department of Electrical Engineering, Faculty of Engineering, Menoufia University, Shebin El-Kom 32511, Egypt

*Corresponding Author: Osama S. Faragallah. Email: o.salah@tu.edu.sa

Received: 27 April 2021; Accepted: 23 June 2021

Abstract: In the last few years, videos became the most common form of information transmitted over the internet, and a lot of the traffic is confidential and must be protected and delivered safely to its intended users. This introduces the challenges of presenting encryption systems that can encode videos securely and efficiently at the same time. This paper presents an efficient opto-video encryption system using Logistic Adjusted Sine map (LASM) in the Fractional Fourier Transform (FrFT). In the presented opto-video LASM-based FrFT scheme, the encoded video is split into distinct frames and transformed into optical signals utilizing an optical supply. Each of the developed optical video frames is ciphered by utilizing the LASM in optical FrFT system using two-phase modulation forms on the video frame, the first in the time-domain and the second in the FrFT domain. In the end, the ciphervideo frame is spotted utilizing a CCD digital camera and transformed into a digital structure that can be managed using a computer. We test the proposed opto-video LASM-based FrFT scheme using various security tools. The outcomes demonstrate that the presented scheme can effectively encrypt and decrypt video signals. In addition, it encrypts videos with a high level of encryption quality without sacrificing its resistance to noise immunity. Finally, the test outcomes demonstrate that the presented scheme is immune to known attacks.

Keywords: Optical encryption; FrFT; logistic-adjusted sine map



This work is licensed under a Creative Commons Attribution 4.0 International License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

1 Introduction

Since the presentation of video cameras in the mid of 19th century, watching movies and videos have become a norm in our daily lives. For instance, we watch movies and films for entertainment and educational purposes. Videos have also been utilized for many other applications, including but not limited to video chatting and conferencing to communicate with people, advertising products and services and playing video games. Videos are considered nowadays the most common form of information transmitted over the internet. Online video traffic had increased from 67% of all internet traffic in 2014 to 80% of all internet traffic in 2019. This increase is due to advancements in internet speeds. A lot of video traffic is confidential and must be kept only for the intended users [1,2]. For instance, video chatting and conferencing can be hacked to obtain secret information. In addition, paid Video on Demand (VoD) services must be kept only for the rightful subscribers. Copyrighted films and videos must be kept safe from tampering or stealing. That is why in many applications encrypting videos while being transmitted over the internet is a must.

Since videos are large, traditional encryption systems are not practically used to encrypt videos. Therefore, we must consider the trade-off between performance and security. To address this issue, many works in encrypting videos had been introduced in the literature. Xu et al. [3] presented an efficient video encryption system. Their system is based on generating a keystream to encrypt videos selectively. This keystream is created using a chaotic pseudo-random number generator (RNG). The experimental outcomes demonstrate that their system is efficient, and it can withstand cryptanalysis attacks.

Fahmeeda et al. [4] presented a computational and time-efficient video encryption system suitable for real-time video applications such as VOD and pay-per-view without affecting security. Their system does not require any special hardware requirements, and the encryption/decryption keys are small and manageable. In their system, the video frames in the videos are twisted by an angle and encrypted using keys created by Faro in an out perfect scrambling algorithm.

Altaf et al. [5] presented a selective video encryption system that considers increasing security with minimal computational resources. Their system also preserves the video compression and fulfillment to the video format. First, their system compresses the video data in a way the statistical and structural properties are maintained. Then, chaotic maps alter the substitution boxes in the advanced encryption standard (AES) [6]. Then the video is encrypted utilizing the altered AES and H.264/AVC [7]. The test results show that their system has reasonably distorted the encrypted video without negatively affecting the video format and compression. Valli et al. [8] proposed two video encryption systems based on chaotic maps. The first is based on a high 12D chaotic map, and the second one is founded on the Ikeda delay differential equation (DDE). To encrypt the videos, the proposed system uses the chaotic maps to scramble the first frame, then the scrambled first frame is then XORed with the second frame, and the result is scrambled using the chaotic map and so on. This technique in encryption is called cipher block chaining (CBC). Their systems are secure against cryptanalysis attacks, but this comes with the cost of not supporting parallel processing. Salamudeen et al. [9] presented a video encryption system that uses spin and element anti-diagonal matrices to encrypt videos. The spin matrix is used to divide the video frame into blocks of pixels, and then the element anti-diagonal matrix is used to encrypt/decrypt these blocks. Their system is computationally efficient and fast, which makes it suitable for online video streaming. In addition, the proposed system effectively degrades the quality of the encrypted video, and it does not rely on the video format. Their system can withstand cryptanalysis attacks. In [10], Xu presented a hybrid encryption/steganographic system used to secure high efficiency video coding (HEVC). Their system is commutative, i.e., the embedded data has no negative effect on decrypting

an encrypted video, and the inserted data can be properly recovered from the ciphered video. The HEVC parameters of motion vector difference (MVD) sign, the intra-prediction mode (IPM) and the quantized transform coefficient (QTC) signs are encoded. This results in a huge degradation in the video quality. The proposed system embeds the data in the QTC, which minimizes the effect of the embedded data on the video. The proposed system allows extracting the embedded data from both the encrypted and decrypted versions of the video. Nalawade et al. [11] introduced a video encryption scheme that is built on the RSA algorithm, named after its inventors Rivest, Lihua et al. [12] and Pseudo Noise (PN). This system is suitable for videos that require a high-security level regardless of the encryption/decryption speeds. Their system is designed to encrypt Audio Video Interleaved (AVI) [13] video format, but it can be easily modified to encrypt Moving Picture Experts Group (MPEG) [14] video format. The frames and the audio of the foundation video file are encrypted twice using the RSA algorithm followed by PN to increase the security level. Khyioon et al. [15] introduced a video encryption method built on the NTRU [16] encryption (an open-source cryptosystem based on the lattice) and chaotic maps. Their system works with various video formats, including AVI, Windows Media Video (WMV), MOV, which is a format for QuickTime and MP4. Their system encrypts videos using the NTRU encryption while decrypts videos using chaotic maps. This allows a high level of security while maintaining a high decryption speed. They implemented their system using visual basic.

Long et al. [17] proposed a hybrid steganographic/encryption system that works for the HEVC video format. The signs of residual coefficients and the amplitudes of motion vector differences are encrypted using RC4 [18] using an encryption key. At the same time, data can be embedded in nonzero AC residual coefficients using a hiding key, which is independent of the encryption key. Their system is separable, i.e., a receiver can decrypt the video with an acceptable quality if he possesses the decryption key but cannot get the hidden data without the hiding key. On the other hand, the receiver can get the inserted data using the hiding key but cannot decrypt the video without the decryption key. Thus, he must have both keys to decrypt the video and extract the inserted data.

The remainder of the paper is sectioned as follows. Section 2 explores the fundamental transform frameworks, including the Logistic-adjusted-Sine map (LASM) and the Fractional Fourier Transform (FrFT). Section 3 presents the opto-video LASM-based FrFT scheme. Section 4 represents the simulation outcomes of the proposed opto-video LASM-based FrFT scheme. Finally, section 5 represents the conclusions of the paper.

2 Fundamental Transform Frameworks

This part presents the two essential components utilized to construct the proposed video encryption system; the Logistic-adjusted-Sine map and the Fractional Fourier Transform (FrFT).

2.1 Logistic Adjusted Sine Map (LASM)

The LASM represents a 2D chaotic mapping that can mix the pixels in a video frame. Its mathematical form is as follows [19,20]:

$$\begin{cases} x_{i+1} = \sin(\pi \mu (y_i + 3) x_i (1 - x_i)) \\ y_{i+1} = \sin(\pi \mu (x_{i+1} + 3) y_i (1 - y_i)) \end{cases} \quad (1)$$

where $\mu \in [0,1]$. The LASM is a mixture of Sine and Logistic maps. Firstly, the logistic equation $x_i(1 - x_i)$ is modulated by μ after adding it to the Sine map. Next, the phase matrix is expanded to 2D. With the LASM, the two inputs are controlled, and the resulted (x_{i+1}, y_{i+1}) are distributed to the 2D phase matrix. It is much more complicated than the Sine and Logistic maps and the outcomes are more complicated than predicted [19,20].

2.2 The Fractional Fourier Transform (FrFT)

The FrFT represents a linear alteration thought as a generality of the classical Fourier Transform (FT). Hence, the FrFT is named rotational FT. The FrFT kernel is expressed as follows [21–23]:

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

The FrFT works by revolving the entered signal in the continuous time-frequency plane anticlockwise from (t, w) coordinates to (u, v) coordinates via an angle $\alpha = a\pi/2, 0 \leq a \leq 1$. The FrFT of a signal $x(t)$ is expressed as follows:

$$X_\alpha(u) = \int_{-\infty}^{\infty} x(t) k_\alpha(t, u) dt \quad (3)$$

where u is some hybrid time-frequency variable. For a generalized function $f(x)$,

$$f_a(u) = F^a[f(x)] = C_\alpha \int f(x) \exp\left[i\pi \frac{u^2 + x^2}{\tan\alpha} - 2i\pi \frac{ux}{\sin\alpha}\right] dx \quad (4)$$

where a is the FrFT transform fractional order and α is the operator of FrFT [21–23].

3 The Proposed Encryption Mechanism

In the proposed opto-video LASM-based FrFT scheme, the plainvideo frames are split into distinct frames and then transformed to optical signals utilizing an optical source. Each of the developed optical video frames is ciphered by utilizing the LASM in optical FrFT system using two-phase modulation forms; the first in the time-domain and the second in the FrFT domain. Lastly, the video frame is collected and transferred into a digital structure that can be managed via a computer. Therefore, the encryption steps for the presented opto-video LASM-based FrFT scheme can be reviewed as follows:

- a) Read the plainvideo bit-streams.
- b) Divide the incoming condensed plainvideo bit-streams into separated plainvideo frames.
- c) For each plainvideo frame, apply the LASM and the optical FrFT, apply LASM and the inverse of optical FrFT to get the ciphervideo frame.
- d) Collect all ciphervideo frames to create the ciphervideo bit-streams.
- e) Send the ciphervideo bit-streams via a communication network to the receiver.

In the decryption mechanism of the proposed opto-video LASM-based FrFT scheme, each ciphervideo frame is subjected to the optical FrFT and the inverse of LASM, and then apply the inverse of optical FrFT and again the inverse of LASM to get the plainvideo frame. Finally, the decrypted video frames are accumulated to acquire the plainvideo bit-streams. Therefore, the receiver begins collecting the ciphervideo bit-streams. Thus, the steps of the decoding process for the proposed opto-video LASM-based FrFT scheme can be reviewed as follows:

- a) Receive the ciphervideo bit-streams.
- b) Divide the incoming ciphervideo bit-streams into separated ciphervideo frames.
- c) For each ciphervideo frame, apply the optical FrFT and the inverse of LASM, apply the inverse of optical FrFT and again the inverse of LASM to get the plainvideo frame.
- d) Collect all plainvideo frames to produce the recovered plainvideo bit-streams.

4 Experimental Results

We test the proposed opto-video LASM-based FrFT scheme using four samples of different video frames presented in Fig. 1.



Figure 1: Different samples of original video frames

We first visually inspect the encoded and decoded video frames of the proposed opto-video LASM-based FrFT scheme. Then, we test the quality of the encoded video frames utilizing the entropy [24], the correlation coefficient [25], the histogram deviation (D_I) [26], the irregular deviation (D_H) [27], the number of pixel change rate (NPCR) and the unified average change intensity (UACI) [28]. We also compare histograms [29] of the source, the encrypted, and the decrypted video frames. Next, we test the noise resistance of the presented opto-video LASM-based FrFT scheme using the peak signal to noise ratio (PSNR), the Structural Similarity Index (SSIM) and the Feature Similarity Index (FSIM) [30]. Finally, we test the immunity of the presented opto-video LASM-based FrFT scheme against some recognized attacks such as occlusion and edge detection.

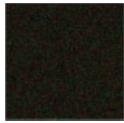
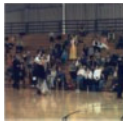

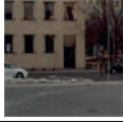

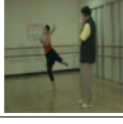


4.1 Visual Inspection

We visually inspect the encrypted and decrypted video frames quality. The visual results are depicted in Tab. 1. From these figures, we can see that the proposed opto-video LASM-based FrFT scheme can conceal the details of the video frames and successfully retrieve back the original frames without any noticeable quality distortion.

4.2 Encryption Quality

We first explain the measurements used to investigate the encryption quality of the presented opto-video LASM-based FrFT scheme, and then we show and discuss the results.

Table 1: Encryption and decrypted video frames using the proposed opto-video LASM-based FrFT scheme

Video Frames	Encrypted video frames	Decrypted video frames
Ballaroom 200		
Vasar 150		
Ballet 20		
Balloons 150		

4.2.1 The Entropy

Information entropy is used to measure how much information is in a video frame [24]. It is built on the chances of the existence of every pixel's value in the video frame. The more the entropy is, the more the chances of every pixel's value in the video frame are close to each other. Consequently, the more improved is the characteristic of the encoded video frames [24]. The information entropy can be expressed as:

$$IE(x) = \sum_{i=1}^{2^N-1} P(x_i) \log_2 \frac{1}{P(x_i)} \quad (5)$$

where $IE(x)$ is the entropy in bits and $P(x_i)$ is the chance of the existence of the pixel x_i .

4.2.2 Correlation Coefficient

An accepted video encryption system must hide any statistical similarity among the video frame and its encoded form. This is essential to avoid any leak of the video frame data. The correlation coefficient is a measurement of the statistical hardness of encryption systems. A recognized characteristic of video frames is that the neighboring pixels are vastly correlated. An accepted video encryption system should conceal this correlation. The correlation coefficient $CC(P, C)$ among the video frame $P(x_i, y_j)$ and the encrypted video frame $C(x_i, y_j)$ is expressed as [25]:

$$CC(P, C) = \frac{E \{ (C - E(C)) \cdot (P - E(P)) \}}{\sqrt{E \{ [C - E(C)]^2 \}} \sqrt{E \{ [P - E(P)]^2 \}}}, \quad (6)$$

where $E \{ \cdot \}$ is the expectation symbol. Small CC values imply better encryption system.

4.2.3 The Histogram Deviation (D_H)

The histogram deviation D_H measures the deviation characteristics of the video encryption system either by evaluating the variation among the original and encoded video frames [26] or by calculating the variance among the spaces under the histogram plots using the equation:

$$D_H = \frac{\left(\sum_{i=0}^{255} d(i) \right)}{W \times H}, \quad (7)$$

where $d(i)$ is the absolute change between the amplitudes at pixel level i of the acquired histograms of the plain and encoded video frames. The size of the plain and encoded video frames is denoted as $W \times H$. High D_H values imply more enhanced characteristics of the encoded video frame [26].

4.2.4 The Irregular Deviation (D_I)

The video encryption quality can be calculated by finding the D_I value from encrypting the video frame [27]. The D_I can be calculated as:

$$D_I = \frac{\left| \sum_{i=0}^{255} h_d(i) \right|}{W \times H} \quad (8)$$

$$h_d(i) = |h(i) - M| \quad (9)$$

where $h(i)$ is the video frame histogram at level i , and M is the mean histogram distribution value for an ideal encrypted video frame. The less the value of DI is, the more improved the encoded video frames [27].

4.2.5 NPCR and UACI

A vital characteristic of a video encryption system is the diffusion characteristic [28]. A minimal alteration in the video frame before encryption leads to a whole transformation in the encrypted video frame. This is essential for video encryption systems to endure cryptanalysis attacks. Two tools are utilized to measure the diffusion characteristic; the NPCR and the UACI [26]. The NPCR determines the number of altered pixels between the two video frames. Suppose that $C^1(x_i, y_j)$, and $C^2(x_i, y_j)$ are two encrypted video frames such that these two video frames are changed in only one pixel. The NPCR can be expressed as [28]:

$$\text{NPCR}(C^1, C^2) = \frac{\sum_{i,j} D(x_i, y_j)}{N} \times 100\%, \quad (10)$$

where N is the pixels number in the video frame and $D(x_i, y_j)$ can be expressed as:

$$D(C^1, C^2) = \begin{cases} 0, & C^1(x_i, y_j) = C^2(x_i, y_j) \\ 1, & C^1(x_i, y_j) \neq C^2(x_i, y_j) \end{cases} \quad (11)$$

The UACI calculates the average intensity change between $C^1(x_i, y_j)$ and $C^2(x_i, y_j)$.

It can be expressed as [28]:

$$\text{UACI}(C^1, C^2) = \frac{1}{N} \left[\sum_{i,j} \frac{|C^1(x_i, y_j) - C^2(x_i, y_j)|}{255} \right] \times 100\%, \quad (12)$$

High NPCR and UACI values imply more enhanced encoded video frames quality. The outcomes of the entropy, the correlation coefficients, the histogram deviation (DH), the irregular deviation (DI), NPCR and UACI of the proposed opto-video LASM-based FrFT scheme are listed in [Tab. 2](#).

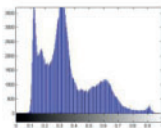
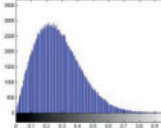
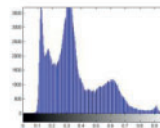
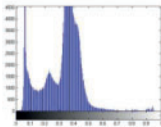
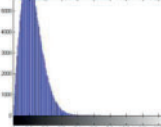
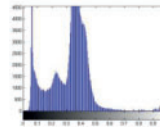
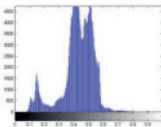
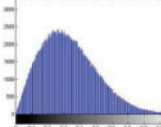
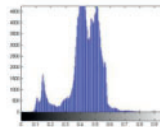
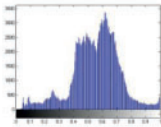
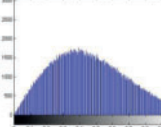
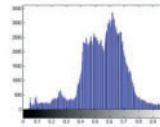
Table 2: The quality matrices results of the proposed opto-video LASM-based FrFT scheme

Video frames	Entropy	Corr.	DH	DI	NCPR	UACI
Ballaroom 200	7.2044	0.0087	0.5907	1.9844	100	0
Vasar 150	6.2507	-0.0062	1.2210	1.9844	100	0
Ballet 20	6.8923	-0.0095	1.2601	1.9843	100	0
Balloons 150	7.5719	-0.0101	0.6367	1.9791	100	0

4.2.6 The Histogram Analysis

The histogram of a video frame is a plot that demonstrates the relationship among the pixel values and their occurrences in the video frame [29]. The more constant the plot is, the more enhanced is the encrypted video frames quality. Furthermore, the plainvideo and ciphervideo frames histogram must be dissimilar to ensure no statistical information leak about these frames. In addition, the histograms of the decrypted and the original frames must be identical for perfect decryption. The histograms of the plainvideo, ciphervideo, and decoded frames are shown in [Tab. 3](#).

Table 3: Histogram outcomes of the plainvideo, ciphervideo, and decoded frames using the proposed opto-video LASM-based FrFT scheme

Video frames	Source frames Histogram	Encrypted frames Histogram	Histogram of the decrypted frames
Ballaroom 200			
Vasar 150			
Ballet 20			
Balloons 150			

4.3 Noise Immunity

The noise immunity for the proposed opto-video LASM-based FrFT scheme is defined as the capability of the encryption system to successfully decrypt the video frame when it is vulnerable to noise throughout the communication. The noise immunity of the proposed opto-video LASM-based FrFT scheme is verified using the Additive White Gaussian Noise (AWGN) and salt and pepper noise of multiple intensities. After that, we compare the decrypted ciphervideo frame quality. The assessment of the noise immunity is done using visual inspection, the PSNR, the SSIM and the FSIM [30].

The PSNR is the fraction between the maximum pixel value (255 in the case of gray scale frames or $2^{24} - 1$ in RGB frames) to the mean square error (MSE).

The PSNR can be expressed as [30]:

$$\text{PSNR}(O, D) = 10 \log_{10} \frac{(255)^2}{\text{MSE}(O, D)} \quad (13)$$

where MSE is calculated as [30]:

$$\text{MSE}(O, D) = \frac{1}{MN} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} [O(x_i, y_j) - D(x_i, y_j)]^2 \quad (14)$$

where $O(x_i, y_j)$ and $D(x_i, y_j)$ denote the pixel values at places x_i, y_j in plainvideo and the deciphered ciphervideo frames, correspondingly [30].

The SSIM measures the decrypted video frame quality compared with the original video frame for the structure information, the luminance masking and the contrast masking [30]. The SSIM ranges between 1 and -1 where 1 shows that both video frames are matching. It is expressed as follows [30]:

$$\text{SSIM} = \frac{(2m_o m_r + c_1)(2\sigma_{or} + c_2)}{(m_o^2 m_r^2 + c_1)(\sigma_o^2 + \sigma_r^2 + c_2)} \quad (15)$$

where m , m^2 and σ represent the video frame mean, variance, and standard deviation. The o , r are the plain and decoded video frames. σ_{or} denotes the covariance of both video frames. c_1, c_2 are constants [30].

The Feature Similarity Index Method (FSIM) measures the features resemblance of two video frames using two factors; the Phase Congruency (PC) and Gradient Magnitude (GM) [26]. The PC detects the video frame structures in the frequency domain while the GM gets the video frame gradient [30].

Assume two video frames; O for the plainvideo and R for the decrypted ciphervideo frame. The congruency of the decrypted and the original video frames are PC_1 and PC_2 . We also obtain the magnitude gradients G_1 and G_2 from the decrypted and original video frames correspondingly. The FSIM can be evaluated as follows [30]:

$$S_{pc} = \frac{2PC_1 PC_2 + T_1}{PC_1^2 + PC_2^2 + T_1} \quad (16)$$

Next, we find the resemblance between both video frames based on G_1 and G_2 as follows:

$$S_G = \frac{2G_1 G_2 + T_2}{G_1^2 + G_2^2 + T_2} \quad (17)$$

where T_1, T_2 are positive constants.

FSIM of the two video frames can be formulated using S_{pc} and S_G as follows [30]:

$$\text{FSIM} = [S_{pc}]^a \cdot [S_G]^b \quad (18)$$

where a and b are the factors of comparative standing between the PC and the MG [30]. The decrypted video frames are shown in Tab. 4. The results of PSNR, SSIM and FSIM among the plainvideo and decrypted ciphervideo frames with AWGN and salt and pepper noises are depicted in Tabs. 5–7.

Table 4: The decrypted video frames utilizing the presented opto-video LASM-based FrFT scheme in the presence of AWGN and Salt & Peppers noises

Video frames	Encrypted video frames with adjusting sine logistic optical fraction							
	AWGN				Salt & peppers			
	0.05	0.15	0.25	0.35	0.05	0.15	0.25	0.35
Ballaroom 200								
Vasar 150								
Ballet 20								
Balloons 150								

Table 5: PSNR for the decrypted video frames utilizing the presented opto-video LASM-based FrFT scheme in the presence of AWGN and Salt & Peppers noises

Video frames	PSNR							
	AWGN				Salt & peppers			
	0.05	0.15	0.25	0.35	0.05	0.15	0.25	0.35
Ballaroom 200	19.0976	14.9629	11.5360	9.0210	18.1444	13.4208	11.2152	9.7121
Vasar 150	19.1220	14.9090	11.4259	8.8141	18.1802	13.3935	11.1501	9.7038
Ballet 20	19.0444	14.8876	11.4144	8.8535	18.6219	13.8189	11.0104	10.1868
Balloons 150	19.2768	15.2770	12.0191	9.7841	18.3899	13.6270	11.4071	9.9535

Table 6: SSIM for the decrypted video frames utilizing the presented opto-video LASM-based FrFT scheme in the presence of AWGN and Salt & Peppers noises

Video frames	Structural Similarity index (SSIM)							
	AWGN				Salt & peppers			
	0.05	0.15	0.25	0.35	0.05	0.15	0.25	0.35
Ballaroom 200	0.6441	0.6003	0.5485	0.4975	0.5818	0.3409	0.2369	0.1732
Vasar 150	0.5436	0.4887	0.4377	0.3945	0.4924	0.2606	0.1713	0.1233
Ballet 20	0.4581	0.4327	0.4039	0.3852	0.4197	0.2106	0.1404	0.1016
Balloons 150	0.5487	0.5354	0.5187	0.5099	0.4969	0.2831	0.1997	0.1507

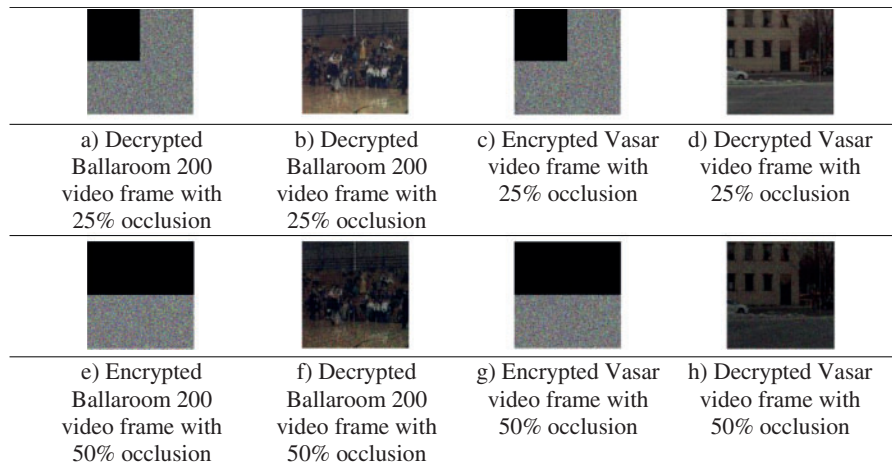
Table 7: FSIM for the decrypted video frames utilizing the presented opto-video LASM-based FrFT scheme in the presence of AWGN and Salt & Peppers noises

Video frames	Feature Similarity index (FSIM)							
	AWGN				Salt& peppers			
	0.05	0.15	0.25	0.35	0.05	0.15	0.25	0.35
Ballaroom 200	0.8712	0.8682	0.8561	0.8401	0.8563	0.7242	0.6509	0.6018
Vasar 150	0.8149	0.8060	0.8020	0.8001	0.8030	0.6279	0.5433	0.4921
Ballet 20	0.7368	0.7338	0.7351	0.7400	0.7270	0.5322	0.4507	0.4024
Balloons 150	0.8275	0.8184	0.7931	0.7592	0.8121	0.6504	0.5703	0.5169

4.4 Immunity Against Occlusion Attacks

The occlusion attack is an attack that crops the encrypted video frames, and the proposed opto-video LASM-based FrFT scheme can withstand this attack if most of the features can be recovered in the decryption. We test the proposed opto-video LASM-based FrFT scheme by attacking the encrypted video frames with 25% and 50% occlusions and testing the similarity between the original and decrypted video frames. The occlusion attack results for Ballaroom 200 and Vasar video frames illustrated in Tab. 8 prove the immunity of the presented opto-video LASM-based FrFT scheme against the occlusion attack.

Table 8: Immunity of the presented opto-video LASM-based FrFT scheme to occlusion attack for the encrypted 3VD Ballaroom 200 and Vasar with 25%, and 50% occlusions



5 Conclusions

This paper presents an efficient and secure opto-video LASM-based FrFT scheme based on LASM and FrFT. In the proposed opto-video LASM-based FrFT scheme, the encoded video frames are split into distinct frames and then transformed from electrical signals to optical signals utilizing an optical supply. Each of the optical video frames is encrypted by utilizing the LASM in the optical

FrFT system using two-phase modulation forms; the first in the time-domain and the second in the FrFT domain. In the end, the video frame is captured with a CCD digital camera and transformed into a digital format which can be handled with the computer. We tested the quality of the proposed opto-video LASM-based FrFT scheme using the visual inspection, the entropy, the correlation coefficient, the DH, the DI, the histogram analysis, the NPCR and the UACI. The results showed that the presented opto-video LASM-based FrFT scheme effectively encrypts and decrypts video signals without forfeiting its resistance to noise immunity. In addition, the presented opto-video LASM-based FrFT system was tested for its immunity vs. recognized attacks such as the occlusion attack and the edge detection, and the results showed that its immunity against these types of attacks. To conclude, the proposed opto-video LASM-based FrFT scheme can be used to secure videos transmitted over the internet without sacrificing its efficiency.

Acknowledgement: The authors would like to thank the Deanship of Scientific Research, Taif University Researchers Supporting Project Number (TURSP-2020/08), Taif University, Taif, Saudi Arabia for supporting this research work.

Funding Statement: This study was funded by the Deanship of Scientific Research, Taif University Researchers Supporting Project Number (TURSP-2020/08), Taif University, Taif, Saudi Arabia.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

- [1] H. Kwon, H. Yoon and K. Park, "Multi-targeted backdoor: Identifying backdoor attack for multiple deep neural networks," *IEICE Transactions on Information and Systems*, vol. 103, no. 4, pp. 883–887, 2020.
- [2] H. Kwon, Y. Kim, H. Yoon and D. Choi, "Random untargeted adversarial example on deep neural network," *Symmetry*, vol. 10, no. 12, pp. 738, 2018.
- [3] H. Xu, X. Tong and X. Meng, "An efficient chaos pseudo-random number generator applied to video encryption," *Optik*, vol. 127, no. 20, pp. 9305–9319, 2016.
- [4] S. S. Fahmeeda and D. C. Shubhangi, "Video encryption algorithm and key management using perfect shuffle," *International Journal of Engineering Research and Applications*, vol. 7, no. 2, pp. 1–5, 2017.
- [5] M. Altaf, A. Ahmad, F. A. Khan, Z. Uddin and X. Yang, "Computationally efficient selective video encryption with chaos-based block cipher," *Multimedia Tools and Applications*, vol. 77, no. 21, pp. 27981–27995, 2018.
- [6] Ç. Unal, S. Kacar, Z. Ahmet and I. Pehlivan, "A novel hybrid encryption algorithm based on chaos and S-AES algorithm," *Nonlinear Dynamics*, vol. 92, no. 4, pp. 1745–1759, 2018.
- [7] H. Yuan, C. Guo, J. Liu, X. Wang and S. Kwong, "Motion-homogeneous-based fast transcoding method from H.264/AVC to HEVC," *IEEE Transactions on Multimedia*, vol. 19, no. 7, pp. 1416–1430, 2017.
- [8] D. Valli and K. Ganesan, "Chaos based video encryption using maps and Ikeda time delay system," *The European Physical Journal Plus*, vol. 132, no. 12, pp. 542, 2017.
- [9] A. Salamudeen, M. M. Iddrisu and M. I. Daabo, "Perceptual video encryption via unit anti-diagonal matrix," *Applied Mathematics and Information Sciences*, vol. 12, no. 5, pp. 923–929, 2018.
- [10] D. Xu, "Commutative encryption and data hiding in HEVC video compression," *IEEE Access*, vol. 7, pp. 66028–66041, 2019.
- [11] C. V. Nalawade, S. N. Sayyad and P. S. Sutar, "Dual-layer video encryption and decryption using RSA algorithm," *International Journal of Innovative Research in Computer and Communication Engineering*, vol. 116, no. 1, pp. 33–40, 2017.

- [12] G. Lihua, Q. Kaide, D. Chengzhi and Z. Nanrun, "An optical 3DV frame compression and encryption scheme based on compressive sensing and RSA algorithm," *Optics and Lasers in Engineering*, vol. 121, pp. 169–180, 2019.
- [13] Y. Yang, Z. Xu, L. Liu and G. Sun, "A security carving approach for AVI video based on frame size and index," *Multimedia Tools and Applications*, vol. 76, no. 3, pp. 3293–3312, 2017.
- [14] N. Barman and M. G. Martini, "H.264/MPEG-AVC, H.265/MPEG-HEVC and VP9 codec comparison for live gaming video streaming," in *IEEE Ninth Int. Conf. on Quality of Multimedia Experience (QoMEX)*, Erfurt, Germany, pp. 1–6, 2017.
- [15] Z. Khyioon, A. R. T. Shawe, S. A. Hussein, F. N. Abbas and A. K. Ridha, "Encryption video using NTRU and chaotic algorithms," *Journal of Southwest Jiaotong University*, vol. 54, no. 6, pp. 1–7, 2019.
- [16] A. Martin, S. Bai and L. Ducas, "A subfield lattice attack on overstretched NTRU assumptions," *Annual International Cryptology Conference*, vol. 9814, pp. 153–178, 2016.
- [17] M. Long, F. Peng and H. Li, "Separable reversible data hiding and encryption for HEVC video," *Journal of Real-Time Image Processing*, vol. 14, no. 1, pp. 171–182, 2018.
- [18] M. H. Abood, "An efficient 3DV frame cryptography using hash-LSB steganography with RC4 and pixel shuffling encryption algorithms," in *Annual Conf. on New Trends in Information & Communications Technology Applications (NTICT)*, Baghdad, Iraq, pp. 86–90, 2017.
- [19] O. S. Faragallah and H. S. El-Sayed, "Secure opto-audio cryptosystem using XORing mask and hartley transform," *IEEE Access*, vol. 9, pp. 25437–25449, 2021.
- [20] Z. Hua and Y. Zhou, "Image encryption using 2D logistic-adjusted-Sine map," *Information Sciences*, vol. 339, no. 8, pp. 237–253, 2016.
- [21] O. S. Faragallah, A. Afifi, W. El-Shafai, H. S. El-sayed, E. A. Naeem *et al.*, "Investigation of chaotic image encryption in spatial and FrFT domains for cybersecurity applications," *IEEE Access*, vol. 8, pp. 42491–42503, 2020.
- [22] O. S. Faragallah, H. S. El-sayed, A. Afifi and W. El-Shafai, "Efficient and secure opto-cryptosystem for color images using 2D logistic-based fractional Fourier transform," *Optics and Lasers in Engineering*, vol. 137, no. 6, pp. 106333, 2021.
- [23] O. S. Faragallah, M. A. AlZain, H. S. El-sayed, J. F. Al-Amri, W. El-Shafai *et al.*, "Secure color image cryptosystem based on chaotic logistic in the FrFT domain," *Multimedia Tools and Applications*, vol. 79, no. 3, pp. 2495–2519, 2020.
- [24] O. S. Faragallah, A. I. Sallam and H. S. El-Sayed, "Utilization of HEVC ChaCha20-based selective encryption for secure telehealth video conferencing," *Computers, Materials & Continua*, vol. 7, pp. 831–845, 2021.
- [25] 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. 177–190, 2021.
- [26] A. Sallam, E. EL-Rabaie and O. S. Faragallah, "CABAC-based selective encryption for HEVC using RC6 in different operation modes," *Journal of Multimedia Tools and Applications*, vol. 77, no. 21, pp. 28395–28416, 2018.
- [27] 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.
- [28] A. Sallam, E. EL-Rabaie and O. S. Faragallah, "HEVC selective encryption using RC6 block cipher technique," *IEEE Transactions on Multimedia*, vol. 20, no. 7, pp. 1636–1644, 2018.
- [29] O. S. Faragallah, A. Afifi, W. El-Shafai, H. S. El-sayed, M. A. AlZain *et al.*, "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.
- [30] O. S. Faragallah, A. Afifi, I. F. Elashry, E. A. Naeem, H. M. El-Hoseny *et al.*, "Efficient optical double image cryptosystem using chaotic mapping-based Fresnel transform," *Optical and Quantum Electronics*, vol. 53, no. 305, pp. 1–26, 2021.