IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received January 26, 2021, accepted February 18, 2021, date of publication February 26, 2021, date of current version March 5, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3062403

Optical Bit-Plane-Based 3D-JST Cryptography Algorithm With Cascaded 2D-FrFT Encryption for Efficient and Secure HEVC Communication

WALID EL-SHAFAI[1,2], IMAN M. ALMOMANI[1,3], (Senior Member, IEEE), AND AALA ALKHAYER[1]

[1]Security Engineering Lab, Computer Science Department, Prince Sultan University, Riyadh 11586, Saudi Arabia
[2]Department of Electronics and Electrical Communications Engineering, Faculty of Electronic Engineering, Menoufia University, Menouf 32952, Egypt
[3]Computer Science Department, King Abdullah II School for Information Technology, The University of Jordan, Amman 11942, Jordan

Corresponding author: Walid El-Shafai (eng.waled.elshafai@gmail.com)

ABSTRACT The rapid growth of multimedia communication systems has expanded the High-Efficiency Video Coding (HEVC) security applications precipitously. Therefore, there is an urgent, elevated need to protect and secure the HEVC content during streaming and communication over insecure channels to ensure the privacy of HEVC data against intruders and attackers. This paper introduces an optical HEVC cipher algorithm based on bit-plane 3D-JST (Three-Dimensional Jigsaw Transform) and multistage 2D-FrFT (Two-Dimensional Fractional Fourier Transform) encryption. The main advantage of employing 3D-JST is its unitary transform that has an inverse transform used to reorganize the HEVC frame-blocks in an indiscriminately way. The proposed algorithm embraces the cascaded 2D-FrFT encryption in the optical domain using a single arbitrary phase code; to be executed all optically with a lone lens. The suggested algorithm utilizes the two 2D-FrFT stages with distinct kernels in mutually dimensions separated by employing the arbitrary phase code. A foregoing bit-plane permutation stage is conducted on the input HEVC frames before the 3D-JST and 2D-FrFT processes to accomplish a high robustness and security level. To validate the efficacy of the proposed cryptography algorithm for secure HEVC streaming, a comprehensive evaluation framework has been introduced and followed to (a) test HEVC streams against different statistical cryptographic metrics, (b) compare the proposed algorithm with recent related works whether optical-based or digital-based algorithms and (c) study the impact of different security attacks on its performance. The evaluation results show a secure and efficient proposed cryptography algorithm that outperforms the conventional and related cryptography algorithms in terms of all examined evaluation metrics.

INDEX TERMS Optical encryption, HEVC communication, 3D-JST, 2D-FrFT, cryptography, multimedia applications, video coding, security, efficiency, diffusion, attack, histogram.

I. INTRODUCTION

Multimedia processing systems have immense processing costs and computation to stream or store enormous amounts of multimedia content [1]–[4]. It is generally endorsed in the research society of multimedia streaming services and applications that the accumulated multimedia content must be pre-processed to acquire the valuable and useful information prior to multimedia transmission over wireless communication networks [5]–[9]. Consequently, there is a compulsory demand for a cost-effective compression procedure for multimedia content before their transmission over resource-restricted communication networks. The video codec of the HEVC standard is the extremely contemporary standard in the multimedia research community [10], [11]. It is employed for encoding high-resolution streams. Hence, it can provide adequate features tailored to numerous applications and services of multimedia streaming.

Nowadays, there is a massive progress in Internet technologies and multimedia streaming applications. Consequently, the confidentiality and protection of the multimedia content are of supreme notoriety with the expansion in velocity, veracity, and volume of the advanced applications of multimedia streaming services. The ciphering procedure typically

The associate editor coordinating the review of this manuscript and approving it for publication was Mohamad Afendee Mohamed.

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 License.
For more information, see https://creativecommons.org/licenses/by-nc-nd/4.0/

plays a crucial and vital role in safeguarding multimedia content [12]–[15]. In the ciphering procedure, the multimedia content is encrypted to be transformed from a comprehensible structure to an incomprehensible one [16]. Thus, after the cryptography procedure, the content of multimedia information becomes meaningless for opponents and invaders, and subsequently, it is preserved and secured [17], [18]. Several ciphering procedures have been introduced in earlier years, but most of these procedures have various constraints. Some procedures are exceedingly robust; however, they have excessive computational processing. Other procedures are unsophisticated and energy cost-effective, but they do not provide satisfactory privacy performance [10], [11], [19]–[22].

The content of HEVC frames has a great correlation between adjoining pixels within the same video frame and among different video frames [19], [21]–[24]. Consequently, most previously suggested and conventional cipher algorithms cannot accomplish multimedia encryption with high secrecy and efficiency. Several kinds of multimedia cryptography algorithms have been introduced and examined [20], [25]–[33]. These cryptography algorithms are mainly classified into two main groups based on the operations utilized to model the ciphering and deciphering processes. These groups are permutation-based and substitution-based.

The ciphering process of video frames applies the two main operations through pixels' values transformation and/or pixels' positions permutation [25], [26]. In the position permutation technique, the pixels of the video frame are displaced without changing their values. While in the values transformation technique, the pixels' values are changed without changing their positions. At this substitution stage, usually reversible operations, such as XOR, are used. The XOR-based encryption process is employed to change the pixel values for enhancing the cryptography performance of the introduced video security technique through XOR-ing the frame pixels with the key's bits [27], [28].

In terms of efficiency and security in the state-of-the-art cryptography algorithms, the limitations in the context of video streaming have motivated this research to introduce a more enhanced algorithm. This algorithm provides a cost-effective implementation of 3D-JST with optical cascaded 2D-FrFT encryption for efficient and secure HEVC communication for multimedia security applications. The HEVC frames are firstly broken up into different bit-planes. Then, the HEVC frames are transformed with a random shifting process using 3D-JST. Each bit-plane of the input HEVC frame undergoes a 3D-JST. After that, the transformed and jigsawed bit-planes are merged and subsequently ciphered utilizing arbitrary phase code and two-cascaded stages of 2D-FrFT encryption. The suggested optical HEVC cryptography algorithm ensures robust HEVC data security. Simultaneously, the random phase codes, the 2D-FrFT parameters, and the 3D-JST are joined together to generate the ciphering keys for secure HEVC content.

The main strengths and advantages of this research are summarized as follows.

1) Conducting a deep comparative analysis among related works attempted to secure video frames including the proposed work.
2) Proposal of optical-based cryptography algorithm for secure and efficient HEVC streaming over insecure channels. The optical-based encryption algorithms have great advantages compared to digital-based encryption algorithms in terms of computational processing, parallelism, and security.
3) Employment of both permutation and diffusion in the proposed cryptography algorithm. This introduces great robustness performance against the intruders.
4) Investigation of extensive security analyses for efficient assessment of the proposed cryptography algorithm with the utilization of more than different fifteen evaluation metrics.
5) Low computational processing time of the proposed optical cryptography algorithm that encourages its utilization for real-time video streaming applications.
6) Achievement of superior security performance for the proposed algorithm compared to the preceding algorithms in terms of almost all evaluation security metrics defined through a comprehensive evaluation framework.

The rest of the paper is organized as follows. Section II describes the preliminary work by discussing the basics of 3D-JST and 2D-FrFT algorithms. Section III provides a comparative analysis among the literature studies on securing the video media. Section IV introduces a detailed explanation of the proposed optical cryptography algorithm for secure HEVC communication. Section V presents a comprehensive evaluation framework to assess the performance of the proposed algorithm. The experiments' results and analysis are provided in section VI. Section VII concludes the paper and recommends future research guidelines.

II. PRELIMINARY WORK

The proposed optical-based cryptography algorithm is built based on 3D-JST and 2D-FrFT. Therefore, in this section, the main basics of the 3D-JST and 2D-FrFT algorithms are presented.

A. THREE-DIMENSIONAL JIGSAW TRANSFORM (3D-JST)

The Jigsaw transform [34] is a non-linear transposition function that alternates the adjacent blocks of an image [35]. One of the Jigsaw transform features is the unitary conservation of the energy during the transformation process. Furthermore, the Jigsaw transform has an inverse function. Figure 1.a illustrates an example of a 2D Jigsaw transform in which the entries were randomly re-positioned in a single plane. However, in Figure 1.b, the re-positioning of the 3D Jigsaw transformation occurs between the bit-planes of an image.

B. TWO-DIMENSIONAL FRACTIONAL FOURIER TRANSFORM (2D-FrFT)

The 2D-FrFT algorithm [36] is considered a simplification of the conventional Fourier Transform (FT) algorithm and is

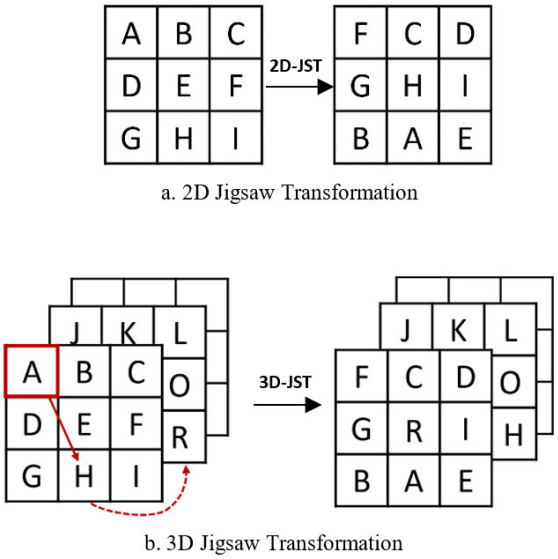


FIGURE 1. An illustrative example of 2D and 3D Jigsaw Transformation.

defined as a linear transformation that turns the input signal by any rotation angle into a diverse transform space domain. Thus, 2D-FrFT has further various parameters like the scaling factors and fractional order along the m and n axes contrasted to the traditional FT algorithm, which can be employed as extra secret keys for effective HEVC ciphering. Therefore, the 2D-FrFT is employed in the proposed HEVC cryptography algorithm as it is mostly and recently utilized in the optics field, and primarily optical statistical and signal processing applications [34], [36], [37]. The arbitrary phase secret key situated at the Fourier plane behaves as the secret key in the ciphering process. The additional amount of freedom presented by the 2D-FrFT is exploited as a new secret key of ciphering. For the aforementioned advantages, the 2D-FrFT is utilized by our proposed cryptography algorithm.

The proposed optical HEVC cryptography algorithm in this paper utilizes an optical ciphering process characterized in two 2D-FrFT stages of encryption with distinguishable secret kernels in mutual dimensions. These cascaded stages of the 2D-FrFT encryption are separated with a random phase code; where the 2D-FrFT transforms with n-stages can offer n-dimensional additional secret keys revealed by means of the fractional orders. So, in the case of one stage of the 2D-FrFT that is owning two distinct fractional orders alongside the m-axis and n-axis, correspondingly, then there are $2n$-dimensional additional secret keys. The employed 2D-FrFT encryption algorithm can be characterized statistically as follows [36].

$$F^{\alpha_1\alpha_2}[O(m,n)](x,y) = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} S_{\alpha_1\alpha_2}(m,n;x,y)O(m,n)dm\,dn \quad (1)$$

with the secret kernel

$$S_{\alpha_1\alpha_1}(m,n;x,y) = S_{\alpha_1}(m,x)S_{\alpha_2}(n,y)$$

where

$$S_{\alpha_1}(m,x) = \begin{cases} B_{\theta_1}\exp\left[i\pi\,(A)\right], & \text{if } \alpha_1 \neq n\pi \\ \delta(m-x), & \text{if } \alpha_1 = 2\,n\pi \\ \delta(m+x), & \text{if } \alpha_1 = (2\,n+1)\pi \end{cases}$$

$$A = m^2\cot\theta_1 - 2\,mx\,\mathrm{cosec}\,\theta_1 + x^2\cot\theta_1$$

and

$$B_{\theta_1} = \frac{\exp\left\{-i\left[\pi\,\mathrm{sgn}\,(\theta_1)/4 - \theta_1/2\right]\right\}}{[|\sin(\theta_1)|]^{1/2}}$$

where the delta function is denoted by $\delta(.), \theta_1 = \alpha_1(\pi/2)$ is the angle related to the FrFT algorithm along the m-axis. The secret kernel along the n-axis $S_{\alpha_2}(n,y)$ can be attained comparably by purely exchanging n for m and y for x, correspondingly. Additional definitions, equations, details, and discussions about the 2D-FrFT are introduced in [34], [36], [37].

III. RELATED STUDIES

This section presents related studies and discusses their main advantages and disadvantages compared to the proposed optical HEVC cryptography algorithm.

In video streaming applications, the video packets transmitted across the network will be stacked and forwarded via several nodes to reach their final destination [38]. There is a need to maintain confidentiality over that communication channels considering the optimized speed and reduced latency required by real-time video transmitting applications. To enforce confidential video streaming in communication, several systems have been proposed. Table 1 summarizes some of the proposed encryption systems in the related work.

Additionally, a core factor in the encryption process is the chosen cryptosystem. Several proposed encryption schemes utilize AES ciphers [39], [40]. However, the computational overhead of AES makes it insufficient for some real-time applications. One of the most recent used video codec streaming standards is High-Efficiency Video Coding (HEVC) due to its significant efficiency in terms of computational processing and compression. A proposed cryptosystem of HEVC was developed by [11] aims to secure the compressed data streams by utilizing three different algorithms, including Arnold chaotic map, DNA (Deoxyribonucleic Acid) sequences, and Mandelbrot sets. To improve security and privacy performance, the cryptosystem's suggested ciphering is applied on three channels (Y, U, and V) of the video streaming by using the Arnold chaotic map. Additionally, to generate confusion features on the three channels, a shift process of the Mandelbrot sets is presented. The simulation results show that the proposed scheme provides a robust and secure method to transform various multimedia resources. Another HEVC steganography based on QFFT scheme has been proposed in [10]. The suggested scheme hides audio messages within the HEVC cover frames. The audio message is initially compressed to utilize the cover capacity, resulting in reducing the size of the secret message. Subsequently, the compressed data

TABLE 1. Comparison among the recent related video encryption algorithms and the proposed algorithm.

Related work	The aim	Video standard	Video elements under study	Approach	Utilized evaluation metrics	Attack
[10]	Hide a secret audio message by encrypting the audio inside a compressed HEVC cover frame	HEVC	Entire frame	Full encryption	PSNR=34.93dB, SSIM=0.95	Steganalysis multimedia attacks
[11]	Secure the compressed data stream of HEVC by implementing a hybrid scheme of three different algorithms	HEVC	Entire frame	Full encryption (hybrid DNA, Mandelbrot sets, and Arnold map)	PSNR=9.38dB, SSIM=0.032	Known/chosen-plaintext attack, channel noise attack, occlusion attack
[19]	Propose a CABAC-based encryption system which implements transparent encryption to reduce the delay and increase the distortion rate	H.265/HEVC	CABAC parameters	Selective encryption	PSNR=19.47dB, SSIM=0.432	Guessing attack
[21]	Maintain the HEVC bit rate by proposing a commutative data hiding and encryption scheme	HEVC	Sign bits of QTC and MVD, magnitude of MVD	Selective encryption and data embedding	PSNR=10.87dB, SSIM=0.32	Replacement attack
[22]	Propose a lightweight encryption system which utilizes the Exclusive OR mechanism	H.265/HEVC	CABAC elements	Selective encryption	PSNR=12.31dB, SSIM=0.203	-
[25]	Achieve ROI encryption by implementing three encryption techniques that adjust the binary symbol	HEVC	Suffixes, transform signals, significant values	Selective encryption	PSNR=10.84dB, SSIM=0.321	-
[26]	Propose an encryption system which takes in consideration energy consumption for IoMT applications	HEVC	IPM, transform coefficients, motion codewords	Selective encryption	PSNR=11.42dB, SSIM=0.237	Interpolation attack
[27]	Deploy tiles to encrypt only the ROI where the secret key is exclusively required for the decryption of ROI	HEVC	MVs, TCs, MV signs, TC signs	Selective encryption	PSNR=11.31dB, SSIM=0.241	-
[28]	Develop a lightweight encryption system by employing extended scrambling with XOR on the syntax sensitive elements	H.264	Video syntax elements	Selective encryption	PSNR=11.64dB, SSIM=0.183	Key guessing, inference attacks, known-plaintext, perceptual attacks
[29]	Utilize the intra prediction mode (IPM) to implement a tunable system to increase the edge lose and visual distortion	H.265/HEVC	(CABAC) syntax elements, edge information	Selective encryption	PSNR=10.68dB, SSIM=0.218	-
[30]	Develop an algorithm to selectively encrypt the CABAC binstrings	HEVC	CABAC binstrings	Selective encryption	PSNR=12.31dB, SSIM=0.203	Plaintext attack, brute-force attack
[31]	Implement a Selective Encryption (SE) by applying a chaos-based ciphering process	HEVC	MV, MVD, TC, TC signs, IPM	Selective encryption based on chaos ciphering	PSNR=11.2dB, SSIM=0.22	Plain-text attack, entropy attack
[32]	Design a nonlinear key stream generation as nonlinear component of cross-coupling chaotic system	SHVC	Slice data payload, NALU frame header	Full encryption	PSNR=11.82dB, SSIM=0.153	Anti-chosen-plaintext attack
[33]	Distort the frame outline sketch by applying selective encryption	HEVC	DCT, IPM	Selective encryption based on scrambling strategies of the macroblocks	SSIM=0.31	MBS sketch attacks
[20]	Secure the battery-based video devices by applying selective encryption	H.264	Significant video metadata	Selective encryption	Perceptual security and battery power consumption	Hijacking and eavesdropping
Proposed work	**Propose an optical HEVC cryptography algorithm**	**HEVC**	**Entire frame**	**Full encryption based on the 3D-JST and multistage (2D-FrFT) encryption**	**PSNR=9.66dB, SSIM=0.043, and more evaluation metrics**	**Noise attack, cropping attack, differential attack, edge attack, and entropy attack**

is encrypted by implementing random projection encryption. The results illustrated that transmitting the cover frame via the proposed approach does not have a clear variation.

Besides the aforementioned applications on securing the HEVC streaming in which the ciphering is applied to the whole video, the encryption process can be implemented to encrypt only the sensitive parts of a video streaming. This selective encryption approach of the syntax elements reduces the time overhead required for the encryption and provides a compression efficiency. The authors of [31] developed a selective encryption solution based on the chaos generator. Several sensitive parameters of the HEVC standard have been chosen to perform the proposed solution, including transform coefficient (TC), motion vector (MV), and intra prediction mode (IPM). However, applying selective encryption on the HEVC videos required preventing the encryption propagation out of the region of interest, consequently resulting in some overhead. Another selective encryption system was proposed by [33]. The suggested scheme applied two different methods to deform the frame's outline by changing the inter and intra frame positions between the macroblocks. Furthermore, the Discrete Cosine Transform (DCT) and the IPM coefficients were decrypted to improve the proposed system's visual security. Even though the results demonstrated an enhanced visual security scrambling, but the file size was affected. Another selective encryption based-approach was proposed by [26]. The suggested system was designed for the Internet of Multimedia Things (IoMT) video streaming. Consequently, it took into consideration the energy consumption for IoMT applications. Initially, the system encrypted the structural, texture, and motion information. However, in case of low energy, only selected syntax elements are encrypted, resulting in reducing the encryption overhead.

Kyungmin *et al.* [20] also proposed a selective encryption scheme which considered the limitations of the present computational devices and communication distances. The suggested framework transferred important video data via a secure sockets layer (SSL), whereas the rest of the video data is transferred via TCP. The important video data was determined by identifying data awareness between the network abstraction layer (NAL) header and the MPEG-2 TS header. Subsequently, the power of the computing resources and the communication distance were considered to decide on the amount of data to be encrypted. In [24], the authors proposed a scalable extension of the HEVC standard for real-time streaming. To reduce the complexity overheads and the delay, the encryption process was implemented to only the sensitive parameters of SHVC for real-time streaming level. Three selective encryption systems of SHVC were defined and compared; the lowest layer, the highest layer, and all SHVC layers. The results revealed that to enforce a high level of security, the encryption must be performed on the lowest layer or all layers. A further proposed system by [27] deployed a distinct concept of HEVC, the tiles, to encrypt only the region of interest (ROI). Consequently, the secret key was exclusively required for the decryption of ROI. The validation results showed that the proposed scheme provided a high level of security of the ROI in real-time applications. Tew *et al.* [25] also suggested a scheme that encrypted the ROI by implementing three encryption techniques that adjust the binary symbol in the chosen coding tree unit. The encryption process was achieved with the minimum parsing overhead by applying the three proposed techniques.

In [28], the authors developed a lightweight encryption system by applying extended permutation with exclusive OR on the syntax elements. The final phase of the encoding generated selected syntax elements. The selective encryption is built based on a diagnostic tool that calculates the success percent of the encryption process by measuring the encoding process's complexity related to the level of encryption. The proposed system was tested against several attacks such as key guessing, inference attacks, known-plaintext, and perceptual attacks. The exclusive OR mechanism was also utilized by Kousar *et al.* [22] in which a lightweight encryption system was proposed to implement transparent encryption.

Several authors have utilized the context-based adaptive binary arithmetic coding (CABAC) in their encryption systems [19], [29], [30]. The authors of [29] have utilized the coefficient and the intra prediction mode (IPM) to implement a tunable system to increase edge loss and visual distortion. Initially, the AES-CTR (Counter-mode encryption) is used to generate a random sequence number. Following that, the CABAC syntax elements were encrypted by the sequence number. To increase the protection level, the coefficients of the edge information was scrambled by calculating the transform units (TUs) of each frame. Another CABAC-based encryption system was proposed by [19]. The suggested scheme implemented transparent encryption on scalable video streaming to reduce the delay and increase the distortion rate. Furthermore, it reduced the computational overhead by utilizing the reduced encryption of B-frames. The examination results of real-time video streaming showed a significant reduction in the delay.

Alongside to implementing the selective approach, recently, several researchers have deployed chaotic system cryptography into the encryption systems [21], [32]. The nonlinear chaotic cryptography follows a deterministic approach aiming to reduce the computational complexity and increase sensitivity. The authors of [21] proposed an enhanced scheme for data hiding and commutative encryption of the HEVC data. To implement the commutative approach, a modified quantized transform coefficient (QTC) element of the HEVC standard has been utilized for data hiding. However, the encryption was realized by using the magnitude of motion vector difference (MVD) and the sign bits of QTC and MVD. The suggested scheme enabled the data to be extracted despite the video being in the encryption or decryption status. Another system that is implemented based on the chaotic system was proposed by [32]. The authors designed a keystream generation method as a nonlinear component of the cross-coupling chaotic system, which prevented the chosen-plaintext attack by relating that component to the

plaintext. Consequently, losing any part of the ciphertext won't affect the decryption of the succeeding units resulting in solving the robustness issue of the video streaming based on the chaotic cipher.

Due to the limitations and restrictions of the existing video cryptography algorithms, this research introduces a cost-effective implementation of 3D-JST with optical cascaded 2D-FrFT encryption for efficient and secure HEVC communication for multimedia security applications. The proposed algorithm aims to overcome the shortcomings of the current cryptography algorithms by encrypting the whole video while preserving a high-security level with minimum cost. In this research, achieving security was measured using several cryptographic metrics. In contrast, the cost was measured through the computational processing time, which is one of the main requirements of efficient live video streaming.

Furthermore, the suggested algorithm's performance is compared against the most related preceding algorithms as shown in Table 1. This table highlights the performance analysis in terms of average PSNR (Peak Signal-to-Noise Ratio) and SSIM (structural similarity) values that were addressed by the related algorithms to appraise video streaming security and efficiency. This comparative study substantiates that the proposed cryptography algorithm affords satisfactory lower average PSNRs and SSIMs for the ciphered HEVC frames. As a result, this proposed optical cryptography algorithm is suitable for HEVC ciphering applications.

IV. PROPOSED OPTICAL HEVC CRYPTOGRAPHY ALGORITHM

This section illustrates the proposed optical-based cryptography algorithm for HEVC communication. The HEVC frames are firstly broken up into different bit-planes. Then, the HEVC frames are transformed with a random shifting process using 3D-JST. Each bit-plane of the input HEVC frame undergoes a 3D-JST. After that, the transformed and jigsawed bit-planes are combined and subsequently ciphered utilizing random phase code and two-cascaded stages of 2D-FrFT encryption. The suggested optical HEVC cryptography algorithm ensures robust HEVC data security, while the random phase codes, the 2D-FrFT parameters, and the 3D-JST are joined together to generate the ciphering keys for secure HEVC content. The structure diagram of the ciphering and deciphering stages of the suggested optical cryptography algorithm is introduced in Fig. 2.

The exhaustive steps of the ciphering procedure shown in Fig. 2 (left) are as follows:

1. The input HEVC frame symbolized as $O(m, n)$ is partitioned into P bit-planes.

$$O(m,n) = \left[O_1(m,n), \ldots\ldots, O_p(m,n)\right] \tag{2}$$

2. Each divided bit-plane $O_i(m, n)$ is transformed with the 3D-JST $J\,[O_i(m, n)]$.

$$J[O(m,n)] = \left[J\,[O_1(m,n)], \ldots\ldots, J\left[O_p(m,n)\right]\right] \tag{3}$$

3. The acquired and transformed 3D-JST bit-planes are composed to form one transformed HEVC frame $T(m, n)$.

$$T(m,n) = J[O(m,n)] \tag{4}$$

4. The obtained transformed HEVC frame is additionally ciphered with the first 2D-FrFT stage with an order of (α_1, α_2) to get the primary encrypted HEVC frame $E_1(m, n)$.

$$E_1(m,n) = 2DFrFT_{(\alpha_1,\alpha_2)}[T(m,n)] \tag{5}$$

5. The first 2D-FrFT stage output is multiplied with a phase arbitrary code $R(m, n)$ encompassing the phase function $\exp[i\psi(m, n)]$ to get the further encrypted HEVC frame $E_2(m, n)$.

$$E_2(m,n) = E_1(m,n) \times \exp[i\psi(m,n)] \tag{6}$$

where $\psi(m, n)$ is an arbitrary function equivalently spread over $[0, 2\pi]$.

6. Employ the second 2D-FrFT stage with an order of $(-\beta_1, -\beta_2)$ to acquire the final ciphered HEVC frame $E(m, n)$.

$$E(m,n) = 2\,\mathrm{DFr}\,FT_{(\beta_1,\beta_2)}\,[E_2(m,n)] \tag{7}$$

The exhaustive steps of the decryption process shown in Fig. 2 (right) are as follows:

1. Employ the first stage of the inverse 2D-FrFT with an order of $(-\beta_1, -\beta_2)$ to the received encrypted frame $E(m, n)$ to get the primary decrypted HEVC frame $Z_1(m, n)$.

$$Z_1(m,n) = 2DFrFT^{-1}_{(-\beta_1,-\beta_2)}[E(m,n)] \tag{8}$$

2. Multiply the resulted HEVC frame from step (1) to a conjugated arbitrary phase code $R^*(m, n)$ encompassing the function $\exp[i\psi(m, n)]^*$ to get the further decrypted HEVC frame $Z_2(m, n)$.

$$Z_2(m,n) = Z_1(m,n) \times \exp[i\psi(m,n)]^* \tag{9}$$

3. Employ the second stage of 2D-FrFT with an order of $(-\alpha_1, -\alpha_2)$ to get the decrypted HEVC frame $Z(m, n)$.

$$Z(m,n) = 2DFrFT^{-1}_{(-\alpha_1-\alpha_2)}\,[Z_2(m,n)] \tag{10}$$

4. Divide the resulted HEVC frame $Z(m, n)$ from step (3) into P bit-planes.

$$Z(m,n) = \left[Z_1(m,n), \ldots\ldots, Z_p(m,n)\right] \tag{11}$$

5. Each divided bit-plane $Z_i(m, n)$ is transformed with the inverse 3D-JST $J^{-1}[Z(m, n)]$.

$$J^{-1}[Z(m,n)] = \left[J^{-1}\,[Z_1(m,n)], \ldots\ldots, J^{-1}\left[Z_p(m,n)\right]\right] \tag{12}$$

6. The acquired 3D-JST transformed bit-planes are composed to get the final deciphered HEVC frame $D(m, n)$.

$$D(m,n) = J^{-1}[Z(m,n)] \tag{13}$$

Consequently, the suggested optical HEVC cryptography algorithm combines two stages: encryption and decryption

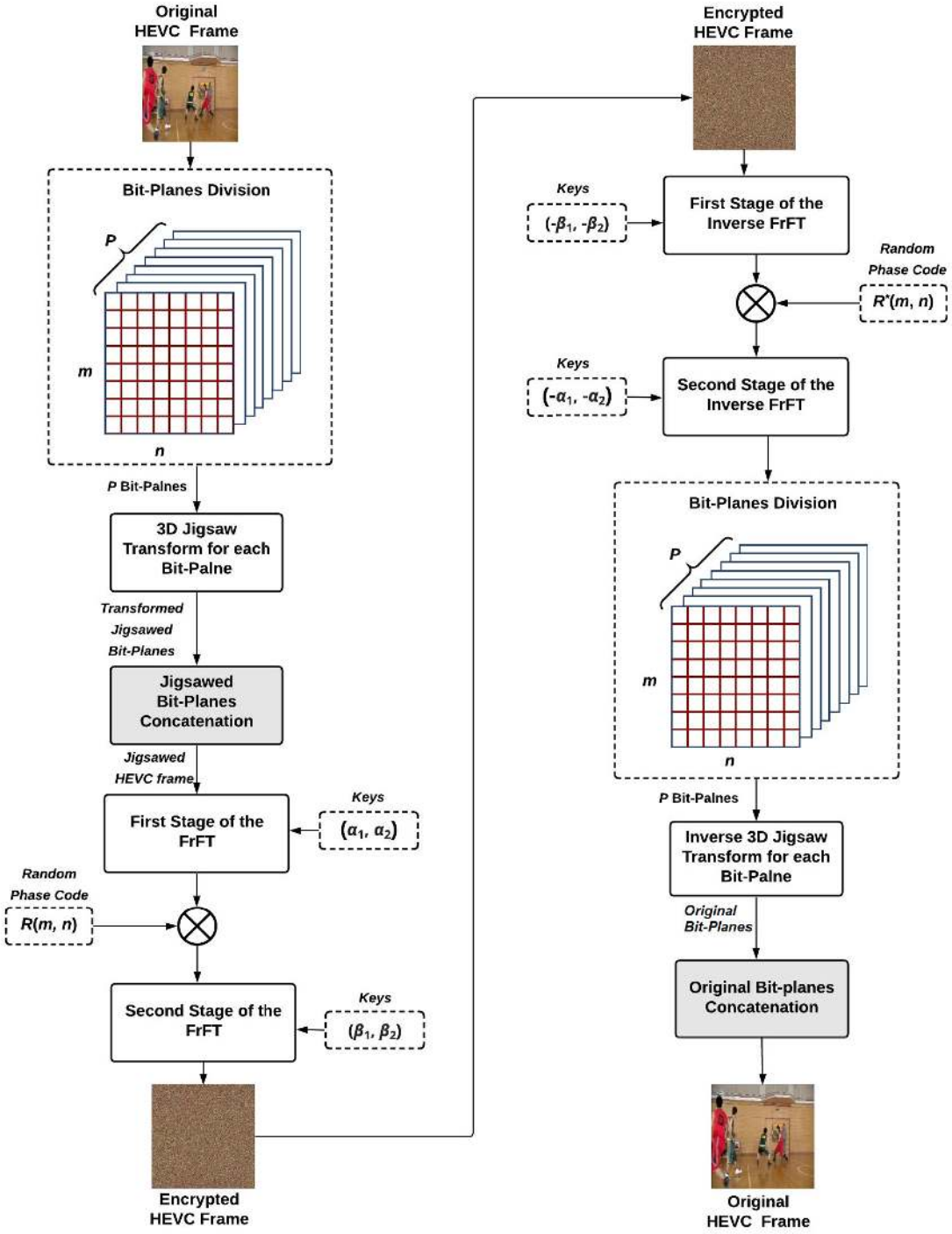


FIGURE 2. The encryption and decryption stages of the proposed HEVC cryptography algorithm.

with two stages of the 2D-FrFT protection scheme. The HEVC frame with a size $M \times M$ is primarily partitioned into different P bit-planes, where we selected $P = 8$ planes in the proposed algorithm. Then, these bit-planes are transformed with the 3D-JST algorithm. The 3D-JST is a unitary transform that has an inverse transform, and thus its energy is well-preserved through the transformation process. Thus, it is used to reorganize the HEVC frame-blocks in an indiscriminately way. Every bit-plane is additionally partitioned into N blocks with a size $m \times n$, where the positions of the whole blocks in each one of the bit-planes are arbitrarily altered to other positions

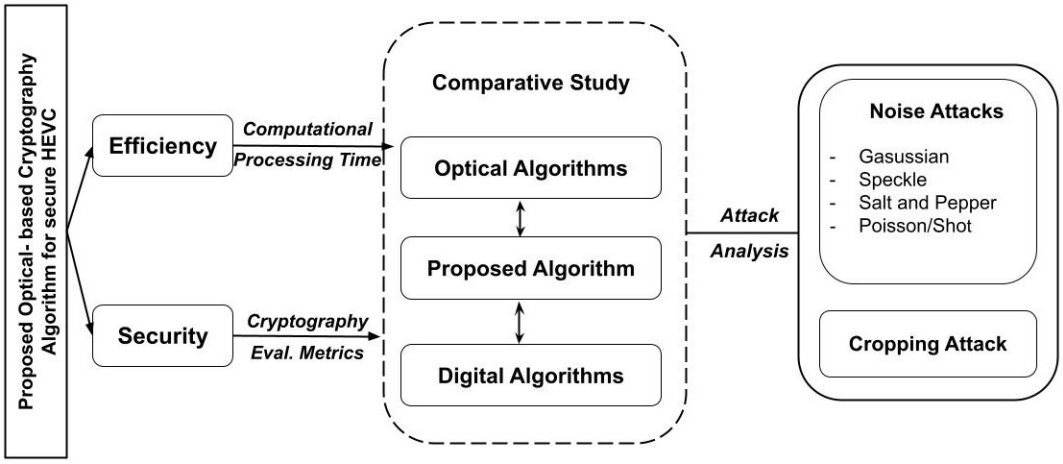


FIGURE 3. The proposed evaluation framework.

corresponding to an arbitrary permutation matrix, in the 3D-JST cube.

The HEVC frame bit-planes are dense of complex layers, where each layer incorporates a specific range of the gray-scale intensity of the input video frame. Subsequently, the overall number of divided blocks will be $N = [M \times M]/[m \times n]$, and thus the totals of probable 3D-JST permutations are determined by $N!$. So, the utilization of the rotated 3D-JST for encryption or transformation improves the security degree of the proposed cryptography algorithm and minimizes the chance of blind deciphering using attackers, where every block is positioned in a separated bit-plane that has four probable alignments to alter its position.

Additional discussions, details, equations, and definitions about the 3D-JST are presented in [34], [37], [41]. Subsequently, the produced jigsaw transformed bit-planes are combined to generate the decomposed HEVC frame. After that, this resulted HEVC frame is ciphered with the first stage of the 2D-FrFT. Then, the obtained output of the first stage of the 2D-FrFT is multiplied with an arbitrary phase mask $R(m, n)$. Ultimately, the subsequent ciphered HEVC frame is further ciphered with an additional ciphering stage of 2D-FrFT to obtain the final ciphered HEVC frame. The two stages parameters of the 2D-FrFT encryption algorithm, the arbitrary phase mask, and the 3D-JST index create the secret keys for HEVC ciphering. This increases the security and robustness of the proposed optical HEVC cryptography algorithm by numerous orders of significance.

V. EVALUATION FRAMEWORK

This section presents the framework applied to evaluate the proposed cryptography algorithm to achieve efficient and secure communication for HEVC. As shown in Fig. 3, the proposed algorithm was heavily examined against several metrics to ensure the secrecy of the transmitted video with high efficiency.

In terms of security, many cryptographic-based metrics were measured and analyzed. These metrics are listed in Fig. 4. The security metrics were classified into main three groups: (a) Visual based metrics that provide the visual analysis for the encryption and decryption processes, histogram and attacks analysis, in addition to the key sensitivity, (b) Diffusion and the Quality metrics that provide deep performance analysis of the proposed algorithm when comparing the original multimedia frames, enciphered and the deciphered frames all together, and (c) Avalanche effect metrics to test how minor changes in the original frame or the used key will cause major change in the enciphered frame.

Whereas the efficiency of the proposed algorithm was assessed in terms of computational processing time. More details will be provided in the following section. Moreover, the proposed algorithm was compared with related work whether optical-based or digital-based to provide a comprehensive evaluation of its performance. Not only that, several attacks were implemented to test their impacts on the behaviour of the proposed algorithm. These attacks include different types of noise attacks in addition to the cropping attack.

In the following sections, the simulation environment is presented, experiments' results per each metric in all categories are revealed and analyzed. Also, the comparisons with related work are shown and discussed. The impact of different security attacks is also highlighted.

VI. EXPERIMENT RESULTS AND ANALYSIS

To completely corroborate the advantage and the best features of the proposed optical HEVC cryptography algorithm, different and standard HEVC sequences were chosen and examined. These sequences include BasketBallDrive, BQMall, BQSquare, FourPeople, PartyScene, and Traffic[1] that have diverse resolutions, spatial-temporal features, and intensity values. The standard HEVC (HM) reference software codec[2] is primarily utilized to compress the examined video sequences to produce the encoded HEVC frames that

[1]YUV Video Sequences, Available at http://trace.eas.asu.edu/yuv/
[2]HEVC Codec, Available at https://hevc.hhi.fraunhofer.de/

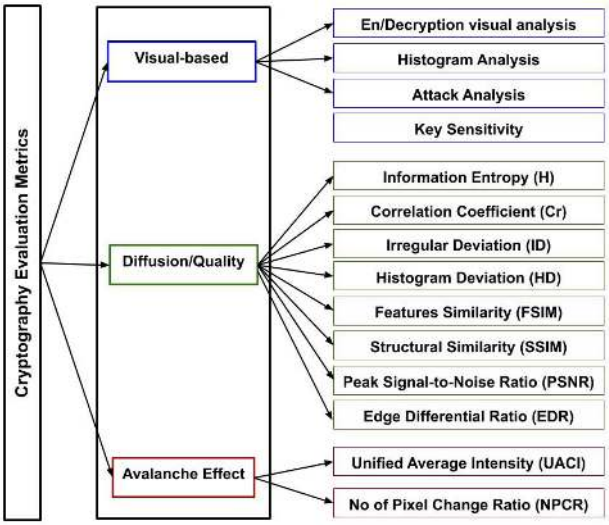


FIGURE 4. The applied evaluation metrics.

are then forwarded to be the input of the suggested optical HEVC cryptography algorithm. The examined HEVC frames are displayed in Fig. 5. The simulation experiments of the suggested optical HEVC cryptography algorithm were performed using a computer machine with: Windows 10, Intel-Core(R-TM) i7-5200 CPU @ 2.4 GHz, and 8 GB RAM. Whereas, the utilized compiling software programs were MATLAB R2020b and Visual Studio 2019.

As explained in section V, the proposed cryptography algorithm were examined against different metrics to test its security and efficiency. Moreover, the impact of different attacks were analyzed; in addition to its key sensitivity. For a complete evaluation of the proposed work, it was compared with recent related works whether optics-based or digital based.

A. VISUAL ANALYSIS

This section provides visual analysis of different evaluation metrics including the analysis of: the encryption and decryption processes, the histogram, the attacks impact, and the key sensitivity.

1) ENCRYPTION/DECRYPTION VISUAL ANALYSIS

For the objective of robustness and security examination of the suggested optical HEVC algorithm, comprehensive and supplementary assessments have been performed. The visual encryption/decryption analysis is one of the most important metrics utilized to assess the cryptography algorithm's robustness efficacy. Figure 5 demonstrates the ciphering/deciphering findings of the examined HEVC frames. It is depicted from the obtainable visual findings the excellent performance of the suggested optical cryptography algorithm in hiding and disappearing the main information inside the examined HEVC frames. In contrast, the suggested optical cryptography algorithm can successfully and efficiently recover and decipher the HEVC frames with high efficiency.

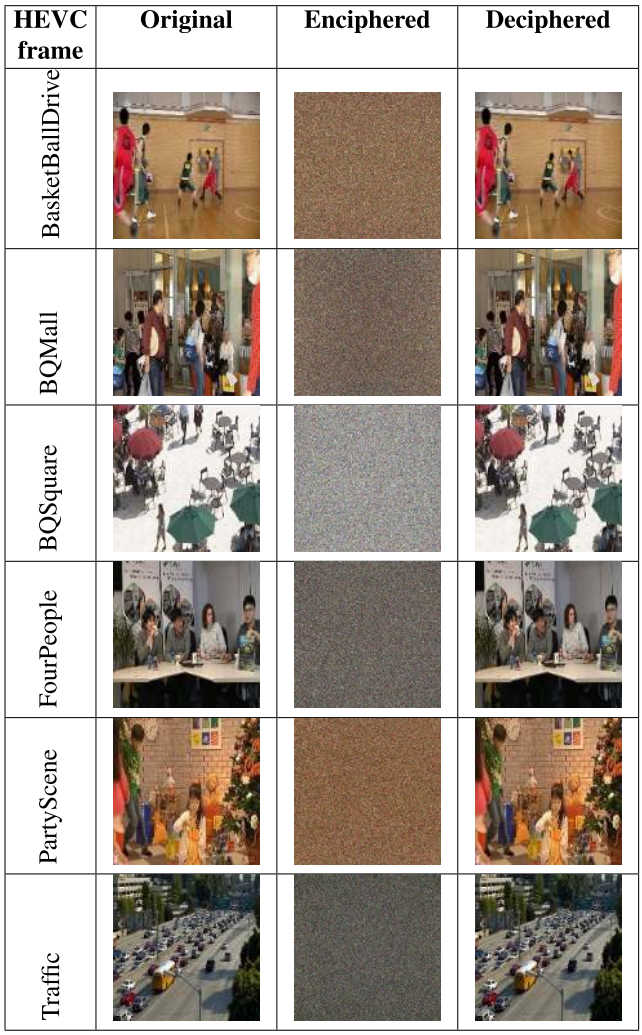


FIGURE 5. Encryption/decryption outcomes of the tested HEVC frames.

2) HISTOGRAM SECURITY ANALYSIS

The histogram can be employed to demonstrate the pixel strength distribution and rates of an HEVC frame, where it can provide a specific statistical security understanding of the encrypted/decrypted HEVC frame. A secure and efficient HEVC cryptography algorithm provides an encrypted HEVC frame histogram which is completely different from the original HEVC frame histogram to survive several types of channel statistical outbreaks [11]. Figure 6 implies the histogram security analysis of the examined HEVC frames. It demonstrates that the histogram distribution of the original HEVC frames fluctuates significantly from the distribution of the ciphered HEVC stream with concealing the tangible form of the examined HEVC streams. Consequently, it is observed from the histogram distributions that there are no arrangements/shapes of a little discernable description in the consistent encrypted HEVC frames. Additionally, it is noticed that the histogram distributions of the deciphered HEVC streams are completely analogous to the histogram distributions of the original HEVC frames. Thus, the optical HEVC cryptography algorithm can successfully and

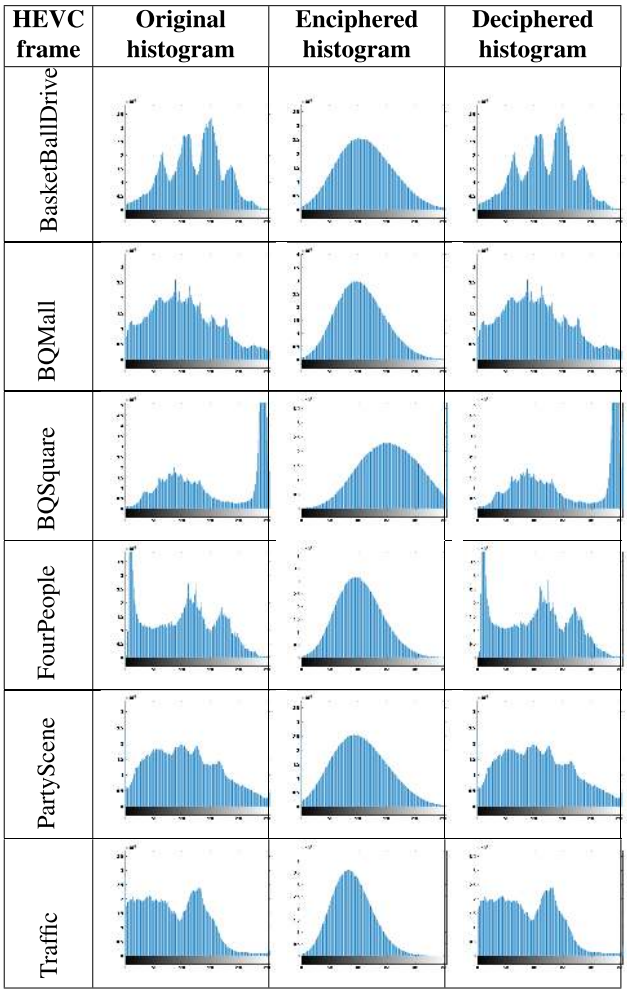


FIGURE 6. Histogram distributions of the original, enciphered, and deciphered HEVC frames.

gainfully retrieve the histogram distribution of the HEVC frame with improved quality. Therefore, these histogram distribution outcomes substantiated the trustworthiness of the suggested optical cryptography algorithm.

3) EFFECT OF CHANNEL NOISE ANALYSIS

This section investigates the effect of different noises on the performance of the proposed enciphering-deciphering processes. The transmission channel frequently encompasses numerous classes of noise. Through video streaming, the HEVC frame in the enciphered arrangement will decisively be extremely predisposed by these transmission noises. Consequently, the proposed optical decryption process should survive these noises' effects so that the decrypted HEVC streams must be understandable or in a human-comprehensible form even if they are infested with a streaming noise attack. Hence, the proposed optical HEVC cryptography algorithm's efficacy must be verified enough to create the noticeable and identifiable HEVC frame from the noisy enciphered HEVC frame. In the noise effect study, various transmission noises (Salt and Pepper, Speckle, Poisson, and Gaussian) are studied.

a: GAUSSIAN NOISE ANALYSIS

In the imaging system, the Gaussian noise is principally resulting throughout the digital videos or images acquisition procedure due to the illumination and temperature effect of the employed camera sensor. It can also be generated from the electronic circuit interruptions of the imaging sensor [24]. Figure 7 offers the outcomes of deciphered and enciphered HEVC frames of the Gaussian noise study with diverse variance rates of 0.02, 0.04, and 0.06. Table 2 presents the PSNR/SSIM outcomes of the deciphered HEVC frames of the Gaussian noise study with diverse variance rates of 0.02, 0.04, and 0.06. It is remarked that the decrypted HEVC streams are still recognizable and demonstrable with good quality performance of acceptable PSNR and SSIM values if various Gaussian noise patterns inspire the associated enciphered HEVC streams. Thus, the suggested optical HEVC cryptography algorithm has a tremendous advantage in fighting against the Gaussian noise effect.

b: SPECKLE NOISE ANALYSIS

The outlines of destructive and constructive obstruction displayed as dark and bright dots in digital videos and images have resulted from the effect of the speckle noise [29]. Figure 8 illustrates the outcomes of enciphered and deciphered HEVC frames of the speckle noise study with diverse variance rates of 0.02, 0.04, and 0.06. Table 2 presents the PSNR/SSIM outcomes of the deciphered HEVC frames of the speckle noise study with diverse variance rates of 0.02, 0.04, and 0.06. It is remarked that the decrypted HEVC streams are still demonstrable and recognizable with good quality performance of acceptable PSNR and SSIM values if the associated enciphered HEVC streams are injected by various speckle-noise patterns. Thus, the suggested optical HEVC cryptography algorithm has a remarkable advantage in preventing the speckle noise effect.

c: SALT AND PEPPER NOISE ANALYSIS

The effect of this noise on digital videos or images is coming from bright areas with dark pixels and dark areas with bright pixels. Figure 9 presents the outcomes of enciphered and deciphered HEVC frames of the Salt-and-Pepper noise study with diverse variance rates of 0.02, 0.04, and 0.06. Table 2 presents the PSNR/SSIM outcomes of the deciphered HEVC frames of the Salt-and-Pepper noise study with diverse variance rates of 0.02, 0.04, and 0.06. It is remarked that the decrypted HEVC streams are still detectable and identifiable with good quality performance of acceptable PSNR and SSIM values if the corresponding enciphered HEVC streams are infected by various Salt-and-Pepper noise patterns. Thus, the optical HEVC cryptography algorithm has marvelous merit in tolerating the noise effect.

d: POISSON/SHOT NOISE ANALYSIS

The noise of Poisson is predictably resulting from the imaging sensor's statistical quantum fluctuations. The outcome of

TABLE 2. The PSNR and SSIM results for the deciphered HEVC frames in the presence of noise attacks.

HEVC frame	PSNR (dB)/SSIM									
	Gaussian			Salt-and-pepper noise			Speckle noise			Poisson noise
	0.02	0.04	0.06	0.02	0.04	0.06	0.02	0.04	0.06	
BasketBall Drive	37.3862/ 0.9576	36.1972/ 0.9358	35.1864/ 0.9109	39.9283/ 0.9785	38.3892/ 0.9527	37.2067/ 0.9398	36.7056/ 0.9683	35.4053/ 0.9472	34.4712/ 0.9287	39.4975/ 0.9698
BQMall	36.4532/ 0.9682	35.3975/ 0.9358	34.4387/ 0.9207	41.7105/ 0.9820	40.4271/ 0.9607	39.6071/ 0.9507	36.7986/ 0.9762	35.6782/ 0.9528	34.7895/ 0.9385	38.5008/ 0.9763
BQSquare	36.9627/ 0.9538	35.7256/ 0.9358	34.5876/ 0.9180	39.6743/ 0.9839	39.1935/ 0.9662	38.1938/ 0.9497	35.5134/ 0.9558	34.1245/ 0.9427	33.2130/ 0.9294	39.4998/ 0.9689
FourPeople	38.7682/ 0.9258	37.8496/ 0.9102	36.9042/ 0.9018	40.2730/ 0.9811	39.7923/ 0.9598	38.6002/ 0.9410	35.4452/ 0.9632	34.2046/ 0.9471	33.1976/ 0.9236	37.1056/ 0.9587
PartyScene	37.4035/ 0.9762	36.1342/ 0.9489	35.2008/ 0.9287	38.4203/ 0.9756	37.1830/ 0.9587	36.4873/ 0.9378	34.7952/ 0.9486	33.4973/ 0.9306	32.1986/ 0.9289	38.6987/ 0.9387
Traffic	37.3352/ 0.9357	36.1178/ 0.9138	35.2791/ 0.9087	37.7958/ 0.9592	36.8409/ 0.9403	35.2194/ 0.9289	35.7986/ 0.9587	34.5137/ 0.9338	33.2011/ 0.9247	36.5097/ 0.9738

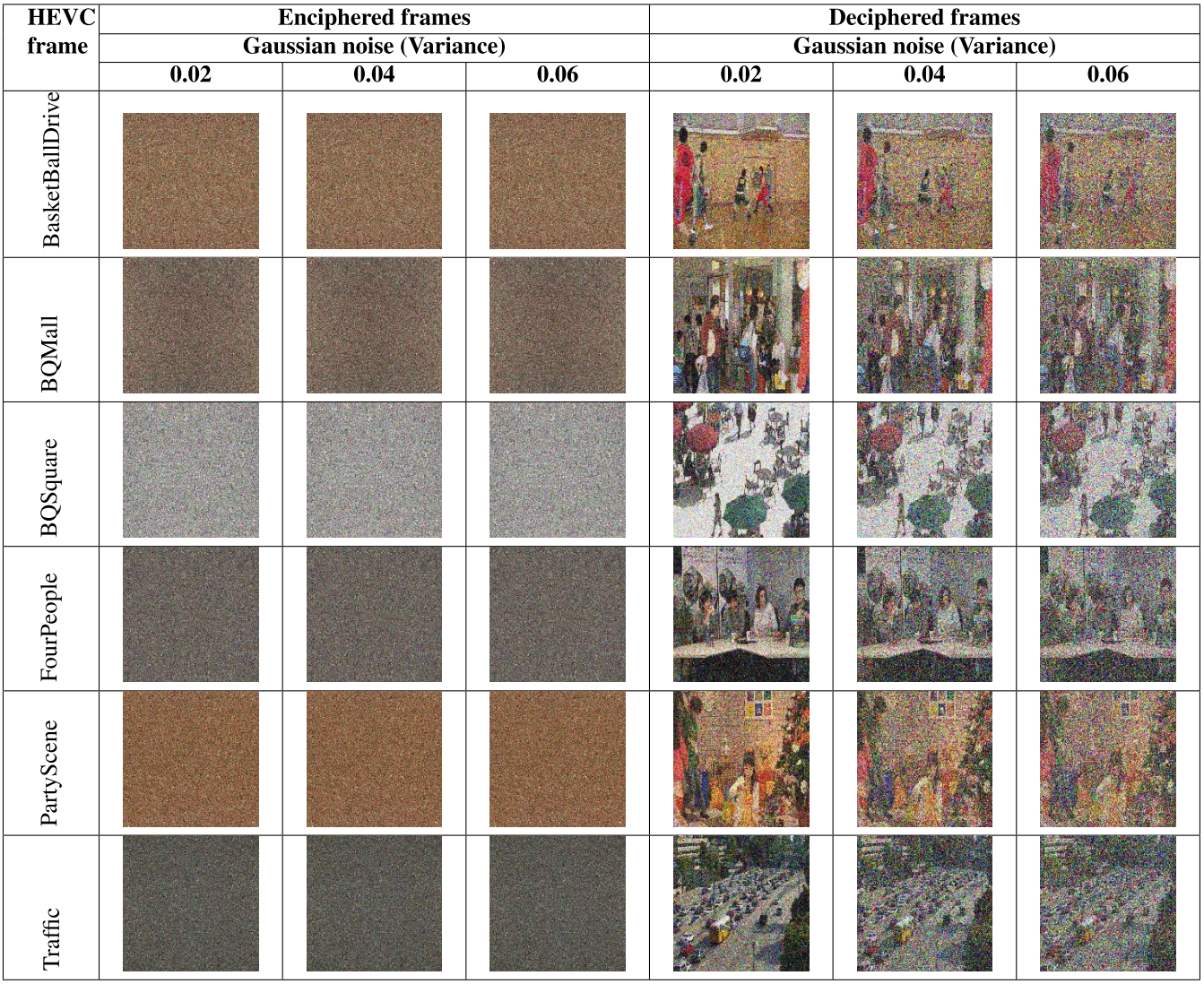


FIGURE 7. The enciphered and decrypted HEVC streams in the occurrence of Gaussian noise with different variances on the enciphered HEVC streams.

this noise is observed in the darker segments of an HEVC stream or a digital image. So, it is studied as a variation in the sensed photons number at a particular exposure degree [11]; thus it might be identified as a photon shot noise. Therefore, it follows the distribution of Poisson. Figure 10 introduces the outcomes of deciphered and enciphered HEVC streams of the

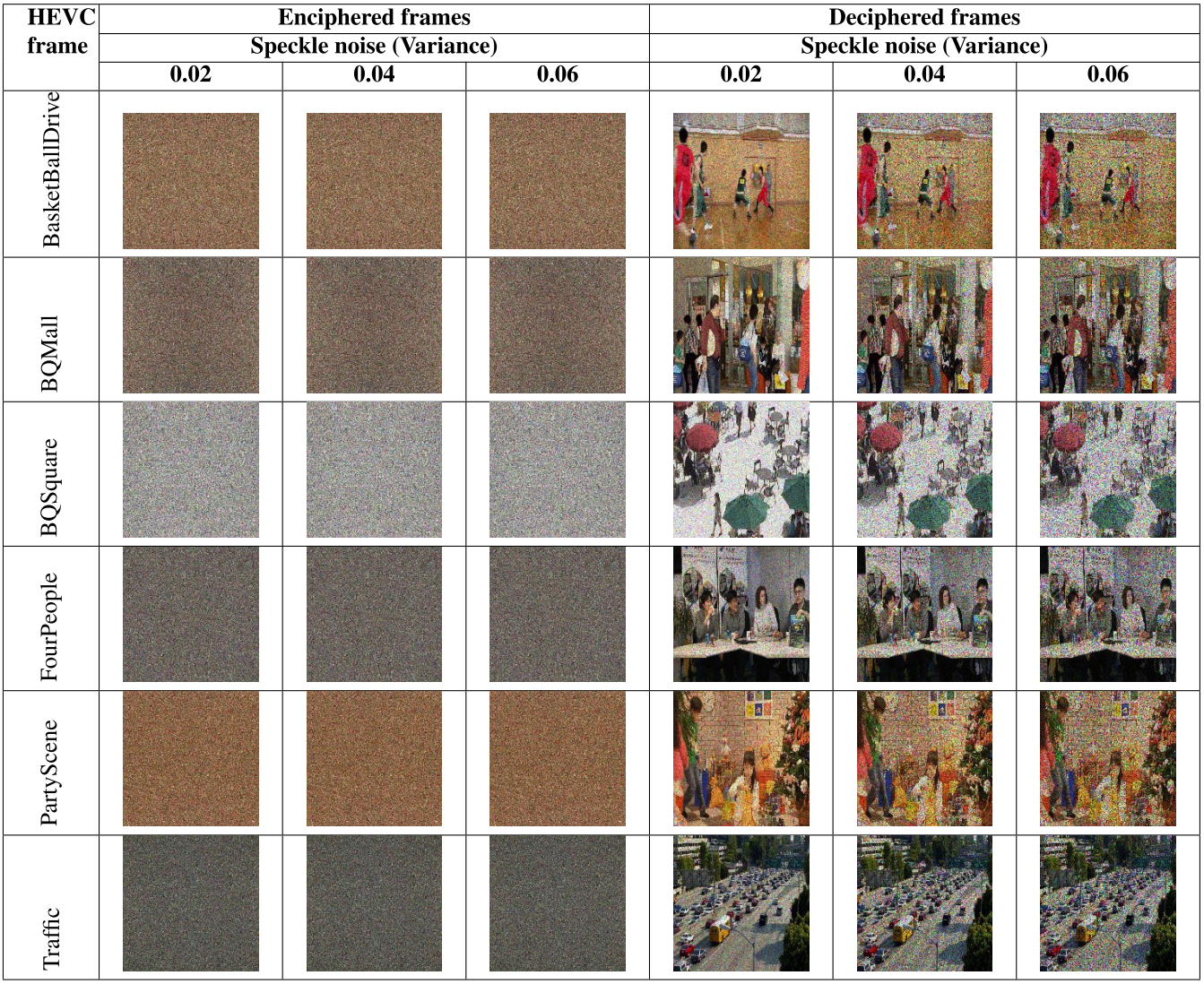


FIGURE 8. The enciphered and deciphered HEVC streams in the state of Speckle noise with different variances on the enciphered streams.

Poisson noise study. Table 2 presents the PSNR/SSIM outcomes of the deciphered HEVC frames of the Poisson noise study. It is obviously remarked that the decrypted HEVC frames are still noticeable and recognizable with good quality performance of acceptable PSNR and SSIM values if the associated enciphered HEVC streams are injected by various Poisson patterns. Thus, the suggested optical HEVC cryptography algorithm has performed well against the Poisson noise effect.

4) CROPPING ATTACK SECURITY ANALYSIS

Through the streaming and transmission of HEVC frames over the communication networks and the Internet, some HEVC frames might be slumped due to mischievous congestion or destruction in the transmission network [10]. The cropping attack study is examined in this section to evaluate the potential of restoring and decoding original HEVC frames from enciphered HEVC frames in the state of a certain percentage if it has been vanished or obstructed. The cropping security study outcomes of the whole examined HEVC streams are demonstrated in Fig. 11. It can be observed that the HEVC streams can be decrypted in a plausible or comprehensible form even if some parts of enciphered HEVC streams are cropped in distinct and separate localities throughout the HEVC communication. This confirms the proposed optical HEVC cryptography algorithm's ability to withstand the plausible incidence of cropping attacks.

5) KEY SENSITIVITY SECURITY ANALYSIS

The employed cryptosystem must be vulnerable to the control and preliminary values of the utilized cryptography scheme [22]. So, the cryptography algorithm should produce distinctive outputs for slight alterations in the secret control keys. Consequently, to reveal that if there is a little variation in the input control values and margins, it will build a substantial

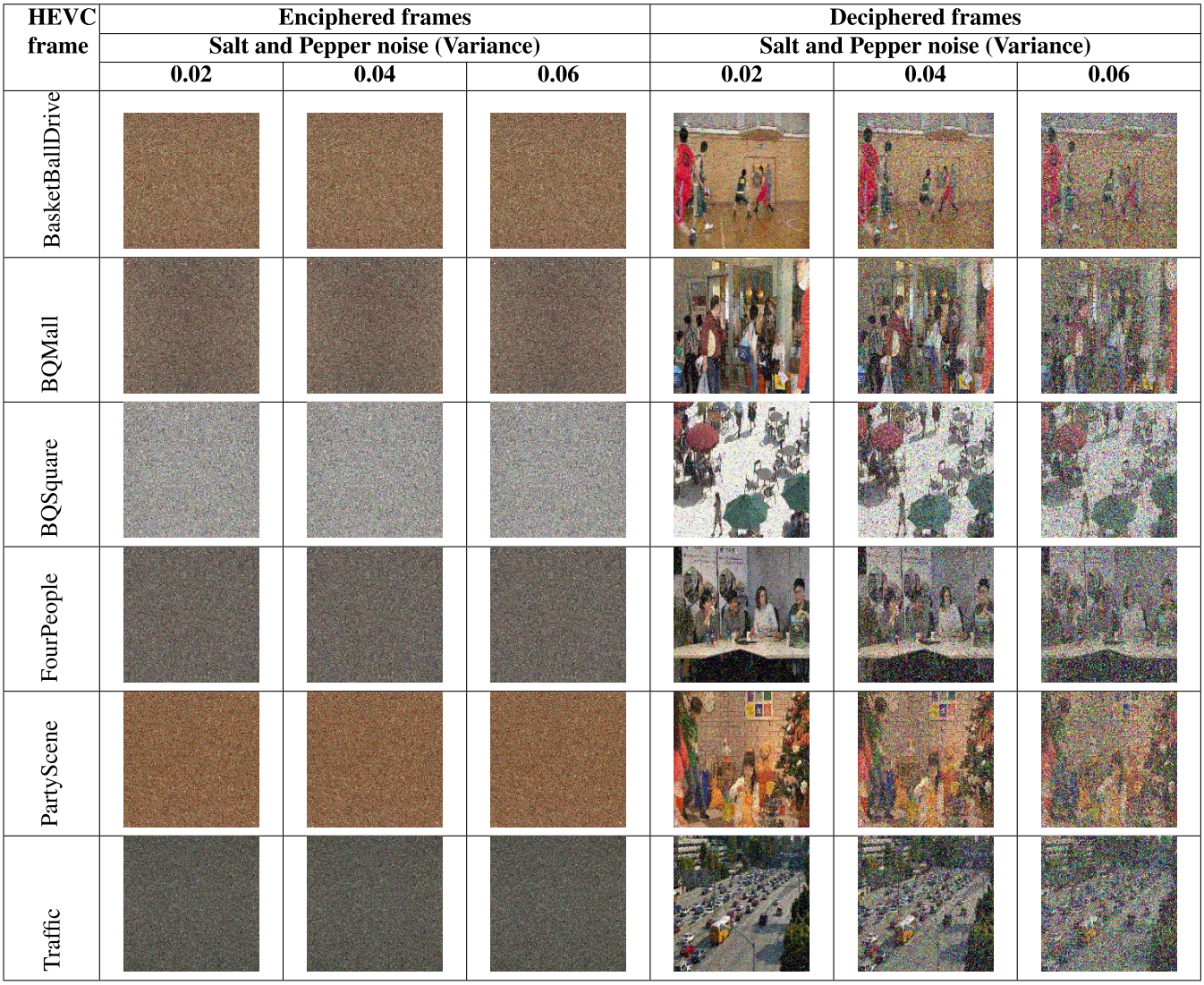


FIGURE 9. The enciphered and deciphered HEVC streams in the occurrence of Salt and Pepper noise with different variances on the enciphered HEVC streams.

adjustment at the output result. Thus, the plain HEVC stream perseveres irrecoverable and the enciphered HEVC frame cannot be decrypted perfectly. Figure 12 demonstrates the security analysis of key sensitivity study for the examined HEVC streams. Therefore, for studying the key sensitivity accomplishment of the proposed optical HEVC cryptography algorithm, the enciphered HEVC streams, decrypted HEVC streams, and their histogram distributions are revealed in Fig. 12 for the whole examined HEVC frames at correct (K_1) and incorrect (K_2) values of secret control keys.

From the obtained outcomes, it is noticed the extremity key sensitivity efficacy of the proposed optical HEVC cryptography algorithm in the state of a slight modification in the values of the secret control keys. It is revealed that the decrypted HEVC frames obtained with the changed control key (K_2) are relatively distinctive, not the real HEVC frame provided even if a little modification is hired to the secret control keys. This confirms that our suggested optical HEVC cryptography algorithm has magnificent sensitivity to the secret control keys and hence diverting it from several channel multimedia assaults.

B. DIFFUSION AND QUALITY ANALYSIS

This subsection presents the results of the metrics that assess the diffusion and the quality characteristics of the proposed algorithms which includes eight different metrics as illustrated below:

1) ENTROPY SECURITY ANALYSIS

The amount of data or information intensity in an HEVC frame can be measured using the entropy metric. The Shannon entropy describes an unpredictability degree of an HEVC frame [30]. It is known that an 8-bit HEVC frame has a Shannon entropy, which is formulated as given in Eq. (14) [42].

$$H(m) = -\sum_{j=0}^{255} P\left(m_j\right) \times \log P\left(m_j\right) \tag{14}$$

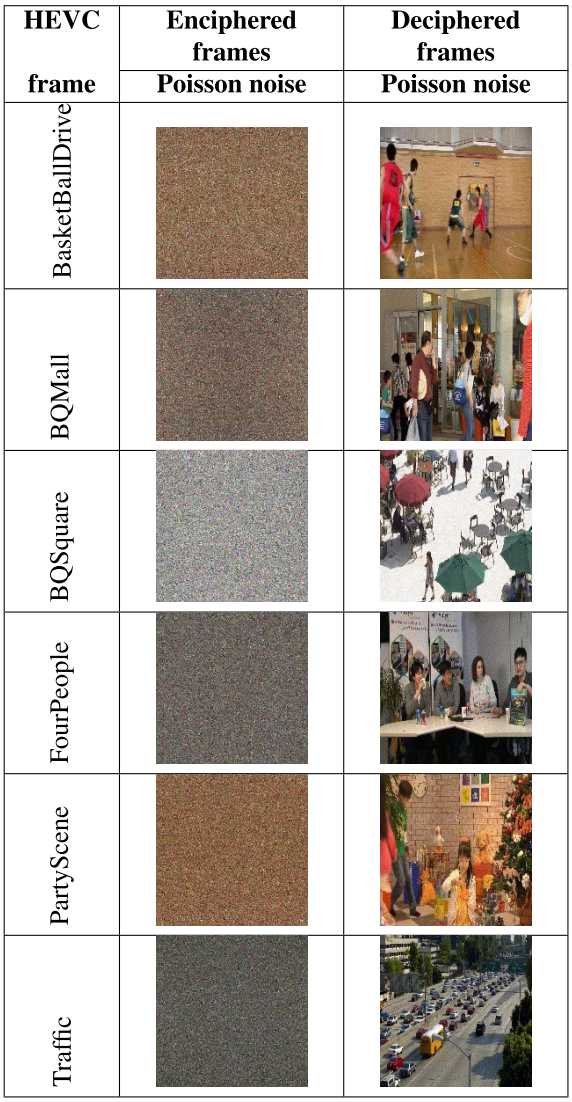


FIGURE 10. The enciphered and deciphered HEVC streams in the occurrence of Poisson noise on the enciphered HEVC streams.

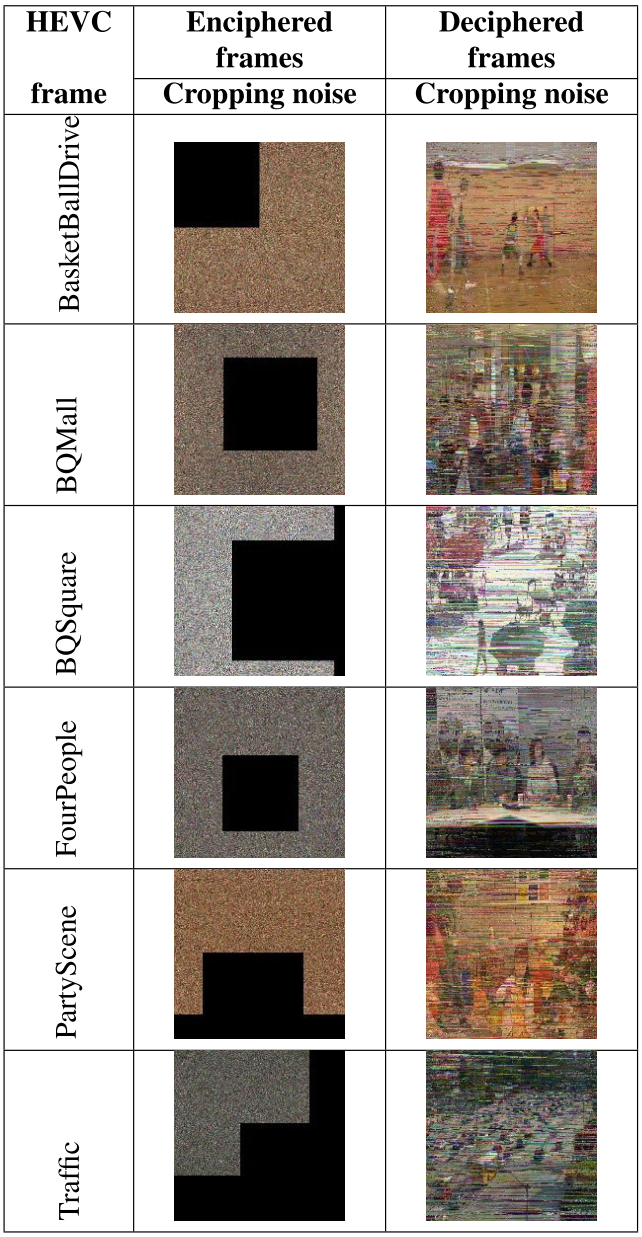


FIGURE 11. The enciphered and deciphered HEVC streams in the presence of copping attack on the enciphered HEVC streams.

where m_j is the j^{th} grey amount in an HEVC frame, while $P(m_j)$ is the probability of m_j in an HEVC frame. It is well known that a terrific cipher algorithm should provide an optimum value close enough to 8 for the estimated Shannon entropy. Table 3 offers the Shannon estimated entropies of the examined HEVC frames. It is shown that the suggested optical HEVC cryptography algorithm delivers appreciated values that are close to the optimum and ideal Shannon entropies of HEVC streams with various attributes. This implies that the data leakage in the encryption might be unnoticed. Consequently, the proposed optical HEVC cryptography algorithm is forceful and safeguard in conjunction with statistical entropy strikes.

TABLE 3. Entropy results of the examined HEVC steams.

HEVC frame	Original	Enciphered	Deciphered
BasketBallDrive	7.5592	7.9687	7.5592
BQMall	7.6924	7.9867	7.6924
BQSquare	7.5371	7.9384	7.5371
FourPeople	7.6824	7.9907	7.6824
PartyScene	7.3287	7.9837	7.3287
Traffic	7.0946	7.9794	7.0946

2) CORRELATION SECURITY ANALYSIS

There is a specific relationship in each HEVC frame, which is persistent along with every set of adjoining pixels. Outstanding cryptography algorithms are expected to preclude or suppress such relations amongst video pixels to bolster the HEVC frame content from a variety of statistical channel outbreaks [27]. To investigate and realize the relations between the couples of pixels in an HEVC frame, it is necessary to choose particular contiguous video pixels of the

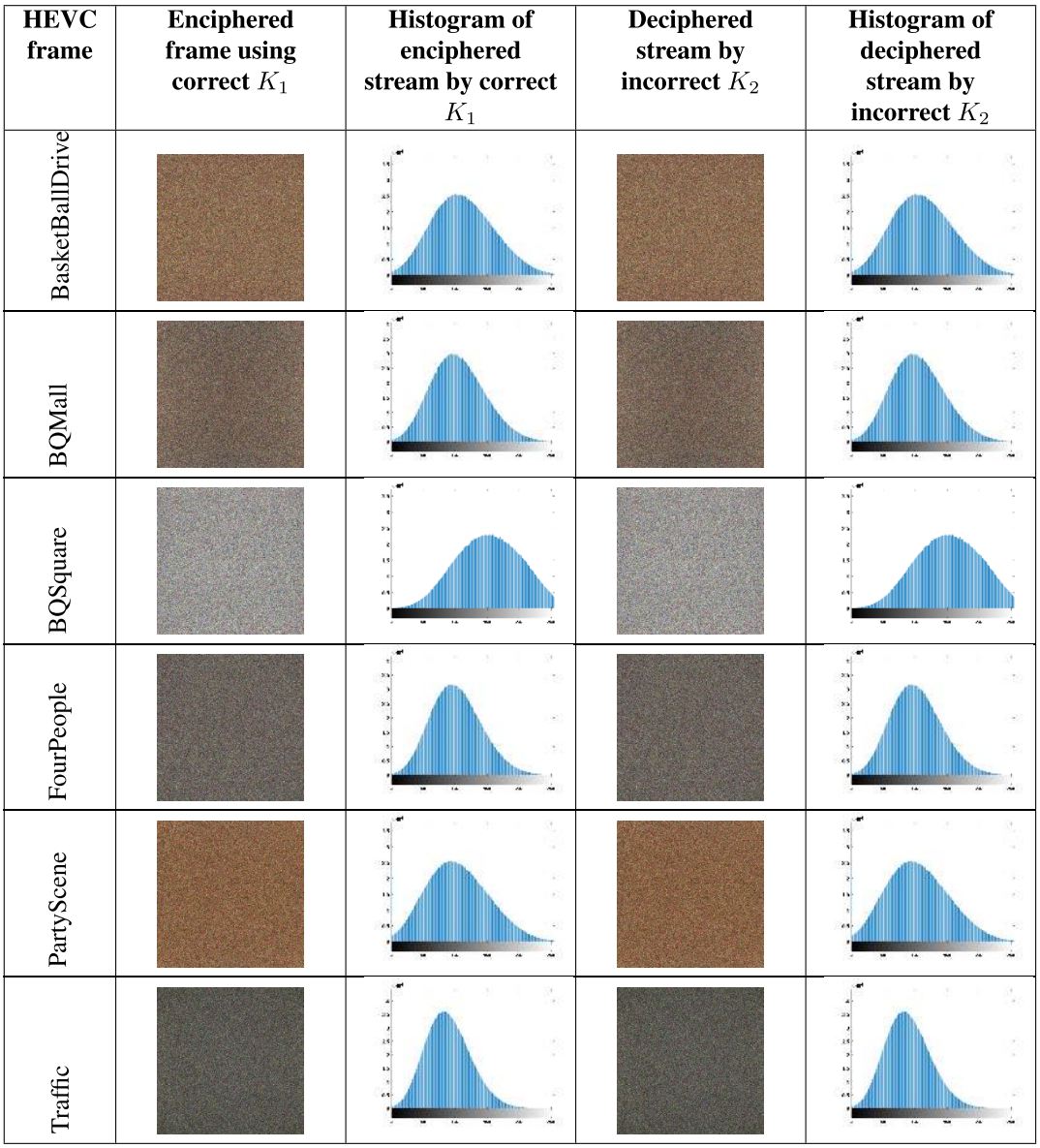


FIGURE 12. Results of the key sensitivity security investigation for the examined HEVC streams.

original HEVC frame in conjunction with the three different directions of vertical (V), diagonal (D), and horizontal (H). The amount of correlation within two pixels of a video frame can be defined as provided in Eq. (15) [43].

$$C_r = \frac{N^2 \cdot \mathrm{cov}(m,n)}{\sum_{j=1}^{N}(m_i - E_m)^2 \cdot \sum_{j=1}^{N}\left(n_j - E_n\right)^2} \tag{15}$$

where $cov(m,n) = E((m-E_m)(n-E_n))$, $E_m = \frac{\sum_{j=1}^{N} m_j}{N}$ and $E_n = \frac{\sum_{j=1}^{N} n_j}{N}$. The two progressions of adjoining video pixels are signified by (m,n), and N denotes the frame size of the HEVC stream.

Figures 13 to 18 demonstrate the diagonal, horizontal, and vertical results of the correlation distributions of every couple of adjoining video pixels for the examined original HEVC streams and their consistent correlations of the enciphered HEVC streams. The associated diagonal, horizontal, and vertical correlation measures of the examined original, enciphered, and decrypted HEVC frames are offered in Table 4. It is obvious from the obtained correlation values that the three estimated correlation values of D, H, and V directions amongst each adjoining couple of video pixels of all enciphered HEVC streams are tremendously low. Consequently, it is recognized that all shape formations in the enciphered HEVC streams have been concealed, rendering them robust and secure against attackers and intruders.

3) ANALYSIS OF IRREGULAR DEVIATION (I_D)

The greatest amount of irregular deviation produced in the enciphered HEVC stream from the enciphering process

TABLE 4. Correlation coefficients outcomes of the examined HEVC streams.

HEVC frame	Original frame			Enciphered frame			Deciphered frame		
	H	V	D	H	V	D	H	V	D
BasketBallDrive	0.9949	0.9701	0.959	0.0729	0.1289	0.1038	0.9949	0.9701	0.959
BQMall	0.8677	0.9592	0.8372	0.0743	0.074	0.1202	0.8677	0.9592	0.8372
BQSquare	0.9661	0.9808	0.9536	0.098	0.0452	0.0228	0.9661	0.9808	0.9536
FourPeople	0.9696	0.9952	0.952	0.0691	0.1024	0.0843	0.9696	0.9952	0.952
PartyScene	0.9482	0.9797	0.9418	0.1338	0.0522	0.0452	0.9482	0.9797	0.9418
Traffic	0.9169	0.9697	0.8972	0.0538	0.034	0.0684	0.9169	0.9697	0.8972

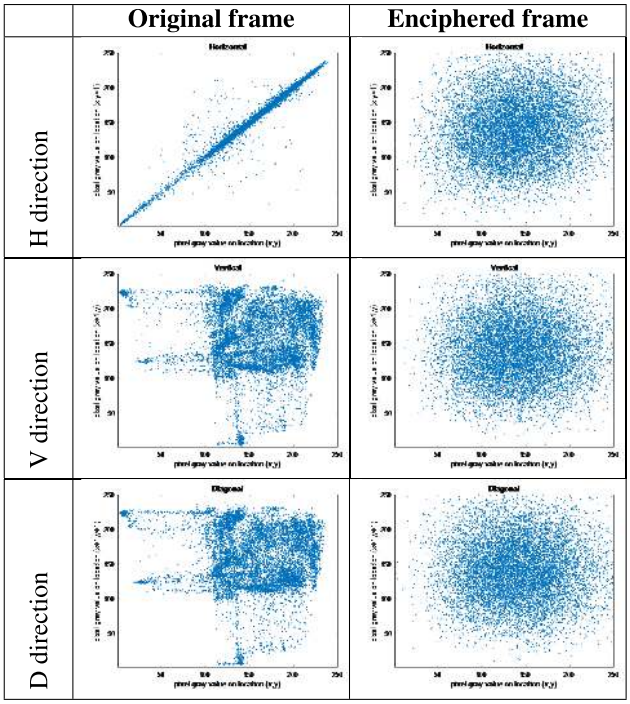


FIGURE 13. The diagonal, vertical, and horizontal correlations in the original and enciphered HEVC frames of the examined BasketBallDrive video.

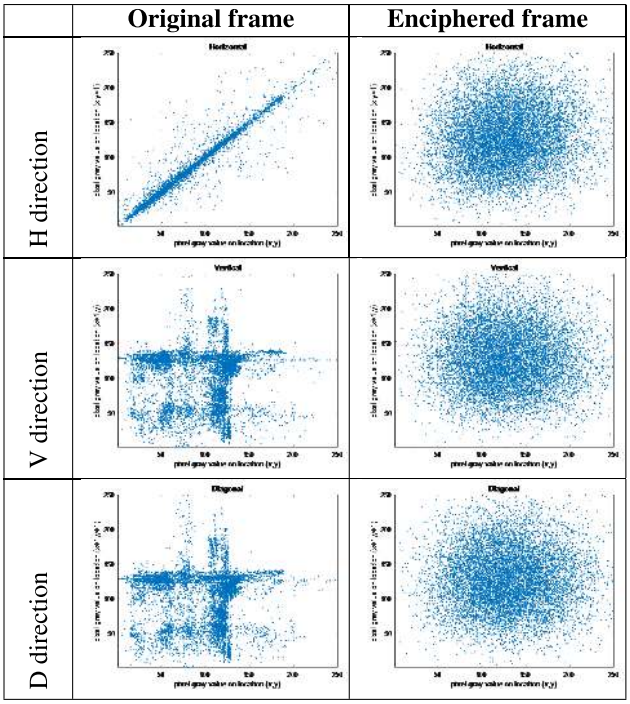


FIGURE 14. The diagonal, vertical, and horizontal correlations in the original and enciphered HEVC frames of the examined BQMall video.

on the original HEVC stream [11] can be anticipated by employing the deviation irregularity (I_D) metric to measure the superiority assessment and encryption efficiency of the suggested optical HEVC cryptography algorithm. The I_D can be assessed as in Eq. (16) [44]. It is remarked that the I_D findings are small as demonstrated in Table 5. Therefore, the enciphered and original HEVC streams are uncorrelated which confirms the superior execution of the proposed optical HEVC cryptography algorithm.

$$I_D = \frac{\sum_{j=0}^{255} |M_H - H(j)|}{m \times n} \tag{16}$$

where the difference in histogram caused by HEVC stream is given by $H(j)$, n and m indexes denote to the frame size (height and width) of the HEVC stream, the histogram amount is estimated as M_H, and the values of n and m belong to the width and height (size) of the HEVC frame.

4) ANALYSIS OF HISTOGRAM DEVIATION (H_D)

The greatest amount of divergence between the histogram distributions of the enciphered and original HEVC frames [11] can be anticipated by exploiting the histogram deviation (H_D) metric to measure the superiority assessment and encryption efficiency of the suggested optical HEVC cryptography algorithm. The H_D can be assessed as in Eq. (17) [45]. It is remarked that the H_D findings are small as demonstrated in Table 5. Therefore, the enciphered and original HEVC streams are uncorrelated which confirms the superior execution of the proposed optical HEVC cryptography algorithm.

$$H_D = \frac{\left(\sum_{j=1}^{254} d_j + \frac{d_0 + d_{255}}{2}\right)}{m \times n} \tag{17}$$

where at the gray level j, the absolute difference amplitude is given by d_j. The values of n and m belong to the width and height (size) of the HEVC frame.

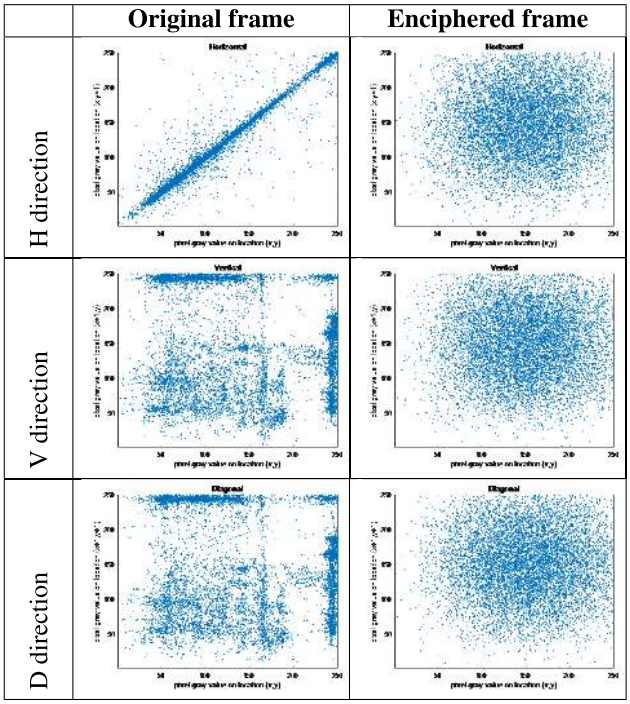


FIGURE 15. The diagonal, vertical, and horizontal correlations in the original and enciphered HEVC frames of the examined BQSquare video.

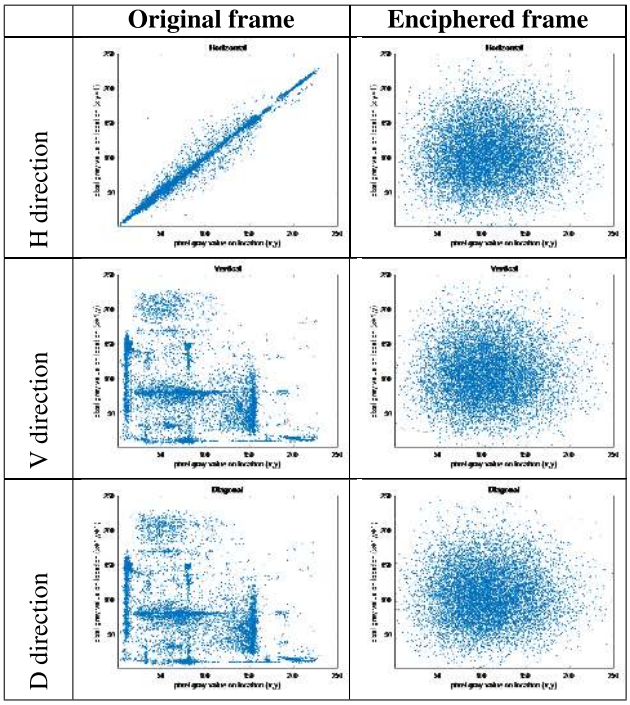


FIGURE 16. The diagonal, vertical, and horizontal correlations in the original and enciphered HEVC frames of the examined FourPeople video.

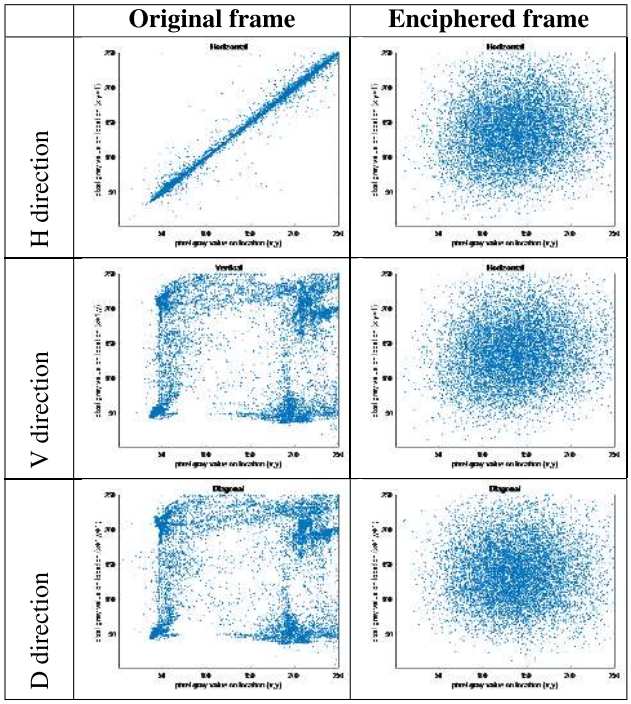


FIGURE 17. The diagonal, vertical, and horizontal correlations in the original and enciphered HEVC frames of the examined PartyScene video.

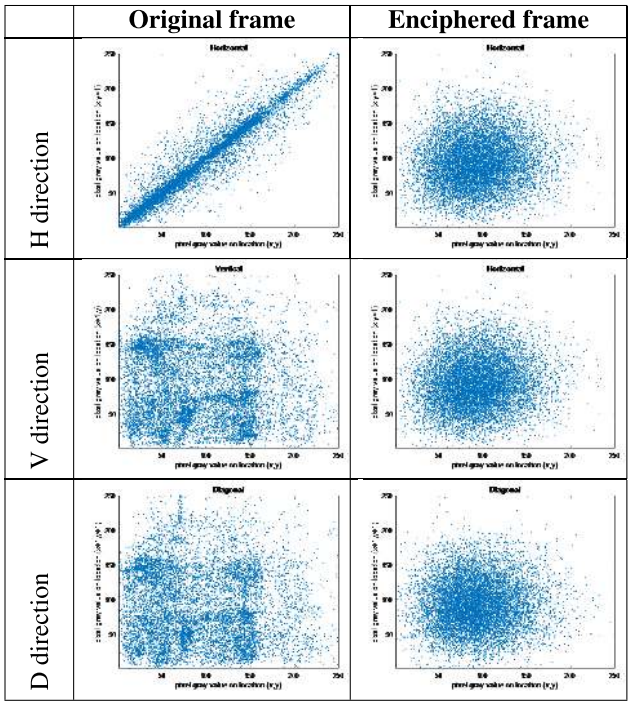


FIGURE 18. The diagonal, vertical, and horizontal correlations in the original and enciphered HEVC streams of the examined Traffic video.

5) FSIM, SSIM, AND PSNR SECURITY ANALYSIS

The metrics of PSNR (peak signal-to-noise ratio), FSIM (feature similarity), and SSIM (structural similarity) are utilized to measure the superiority efficiency of the deciphering and enciphering procedures. In our examination assessments, the values of FSIM, SSIM, and PSNR metrics are measured amongst the enciphered and original HEVC frames that should be offered with low rates for an effective enciphering procedure. Additionally, the values of FSIM, SSIM, and PSNR metrics are measured amongst the deciphered and

TABLE 5. The irregular and histogram deviations values of the enciphered HEVC frames.

HEVC frame	I_D	H_D
BasketBallDrive	0.009324	1.6283
BQMall	0.008647	3.6284
BQSquare	0.003628	2.4637
FourPeople	0.005329	2.4362
PartyScene	0.007332	3.0624
Traffic	0.006382	2.9823

original HEVC frames that should be offered with high rates for an effective deciphering procedure.

The FSIM statistical metric is employed for analyzing the encryption/ decryption competence of the proposed optical HEVC cryptography algorithm [11]. It determines the value of local similarity among two distinct HEVC frames. In the studied security analysis, it is tested amongst the enciphered and original HEVC frames, and amongst the deciphered and original HEVC streams. The quantity of the FSIM metric is in the decimal range of -1 and 1. The index of FSIM can be formulated as provided in Eq. (18) [10], [11], [46].

$$FSIM = \frac{\sum_{x\in\Omega} PC_m(x) \cdot S_L(x)}{\sum_{x\in\Omega} PC_m(x)} \tag{18}$$

where the HEVC frame spatial domain is given by Ω, $PC_m(x)$ denotes the expected phase congruency value, and the whole projected similarity among two HEVC frames is indicated to the $S_L(x)$. Table 6 demonstrates the FSIM findings amongst the enciphered and original HEVC frames. For a perfectly enciphering procedure, it is advised to obtain lower FSIM values amongst the enciphered and original HEVC frames [11]. Table 7 reveals the FSIM findings amongst the deciphered and original HEVC frames. For a perfectly decryption procedure, it is advised to obtain superior FSIM values amongst the deciphered and original HEVC frames. It is viewed from these outcomes in Table 6 and 7 that the suggested optical HEVC cryptography algorithm delivers FSIM calculations that are in close proximity to the optimum and recommended values.

The SSIM statistical metric is utilized for defining the association amongst two different HEVC frames. It is also employed for analyzing the encryption/decryption competence of the proposed optical HEVC cryptography algorithm. The pixels of an HEVC frame have great and robust interdependencies, particularly when they are close together in the spatial domain. This can be determined and estimated by the theory of physical data [18]. Thus, the SSIM metric determines the value of local similarity among two distinct HEVC frames. In the studied security analysis, it is tested amongst the enciphered and original HEVC frames, and amongst the deciphered and original HEVC frames. The quantity of the SSIM metric is in the decimal range of -1 and 1. The SSIM index can be formulated as provided in Eq. (19) [18], [46].

$$\mathrm{SSIM}(m,n) = \frac{(2\mu_m\mu_n + K_1)(2\sigma_{mn} + K_2)}{(\mu_m^2 + \mu_n^2 + K_1)(\sigma_m^2 + \sigma_n^2 + K_2)} \tag{19}$$

TABLE 6. The FSIM, SSIM, and PSNR findings amongst the enciphered and original HEVC frames.

HEVC frame	FSIM	SSIM	PSNR (dB)
BasketBallDrive	0.3534	0.0027	10.3628
BQMall	0.3846	0.0039	9.9857
BQSquare	0.3462	0.0038	9.6247
FourPeople	0.3732	0.0059	9.8957
PartyScene	0.3385	0.0019	10.2385
Traffic	0.3824	0.0035	9.9986

TABLE 7. The FSIM, SSIM, and PSNR findings amongst the deciphered and original HEVC frames.

HEVC frame	FSIM	SSIM	PSNR (dB)
BasketBallDrive	1	1	Inf.
BQMall	1	1	Inf.
BQSquare	1	1	Inf.
FourPeople	1	1	Inf.
PartyScene	1	1	Inf.
Traffic	1	1	Inf.

where μ_m and μ_n are the average estimated quantities of m and n, consistently. σ_m^2 and σ_n^2 are the variances assessed quantities of m and n, correspondingly. σ_{mn} is the covariance estimated value of m and n. $K_1 = (C_1L)^2$ and $K_2 = (C_2L)^2$ are constant quantities that are utilized to lighten the partition procedure with a little denominator, where, the C_2 and C_1 quantities are typically chosen to be 0.03 and 0.01, correspondingly, and the dynamic pixel-values range is given by L.

Table 6 demonstrates the SSIM findings amongst the enciphered and original HEVC frames. For a perfectly enciphering procedure, it is advised to obtain lower SSIM values amongst the enciphered and original HEVC frames [11]. Table 7 reveals the SSIM findings amongst the deciphered and original HEVC frames. A perfectly decryption procedure is advised to obtain superior SSIM quantities amongst the deciphered and original HEVC frames. It is viewed from the results in Tables 6 and 7 that the suggested optical HEVC cryptography algorithm delivers SSIM calculations that are in close proximity to the optimum and recommended quantities.

The PSNR is an extra valuable measure employed for examining the encryption/decryption competence of the proposed optical HEVC cryptography algorithm. It is assessed as the ratio between the greatest achievable signal power and the falsifying noise power. Consequently, it is desirable to obtain greater values for the effective deciphering procedure (amongst deciphered and original HEVC frames) and smaller values for the effective enciphering procedure (amongst enciphered and original HEVC frames) [22].

For an HEVC frame, the metric of the PSNR is determined as in Eq. (20) [46] that is predictably expressed in a dB scale. Table 6 demonstrates the PSNR findings amongst the enciphered and original HEVC streams. For a perfectly enciphering procedure, it is advised to obtain lower PSNR values amongst the enciphered and original HEVC frames [10]. Table 7 reveals the SSIM findings amongst the deciphered and original HEVC frames. For a perfectly

decryption procedure, it is advised to obtain higher PSNR values amongst the deciphered and original HEVC frames [11]. It is shown from the results in Tables 6 and 7 that the suggested optical HEVC cryptography algorithm delivers PSNR ratios that are close to the optimum and recommended quantities.

$$PSNR = 10 \log \frac{255 \times 255}{MSE} \tag{20}$$

where the mean square error is denoted as MSE that is defined as in Eq. (21) [10].

$$MSE = \frac{1}{m \times n} \sum_{a=1}^{m} \sum_{b=1}^{n} [F_1(a, b) - F_2(a, b)]^2 \tag{21}$$

where $F_1(a, b)$ and $F_2(a, b)$ relate to the original and enciphered/deciphered HEVC frames, respectively.

6) EDR SECURITY ANALYSIS

The suggested optical HEVC cryptography algorithm should ensure safeguarding the edge's data in the streamed HEVC streams from the channel manipulations. Subsequently, the graphical falsification for the enciphered HEVC streams developing the proposed optical algorithm can be computed by the misrepresentation presented at the edges of the HEVC frames. The EDR (Edge Differential Ratio) metric is employed to assess the distortions in video frame edges, it is expressed as in Eq. (22) [11], [47].

$$EDR = \frac{\sum_{a,b=1}^{K} |\bar{P}(a, b) - P(a, b)|}{\sum_{a,b=1}^{K} |\bar{P}(a, b) + P(a, b)|} \tag{22}$$

where the $P(a, b)$ is the value of a binary pixel of the detected original HEVC frame edges, and the $\bar{P}(a, b)$ is the value of an associated binary pixel the detected enciphered HEVC frame edges.

Table 8 shows that the EDR results between the enciphered and original HEVC streams that are near to 1, which ensures that the enciphered and original HEVC frames are exceedingly contradictory. Figure 19 presents the graphical Laplacian Gaussian EDR results of the deciphered, enciphered, and original HEVC frames. It is noticed for the obtained findings that there is a significant discrepancy in observed edges amongst enciphered and original HEVC frames. This confirms the advantage of the suggested optical HEVC cryptography algorithm in hiding and disappearing the most important elements inside the examined HEVC frames, whilst it can competently recover the HEVC frames with excellent quality and high efficiency.

C. AVALANCHE EFFECT ANALYSIS

Sometimes, an opponent or attacker may try to create a slight alteration in the plain HEVC stream which is employed for encryption and investigate the dissimilarity in encryption consequences (that is, the enciphered HEVC stream of the original HEVC stream and the enciphered HEVC stream of plain HEVC frame with a slight alteration). In this way,

TABLE 8. The EDR quantities of the enciphered HEVC streams.

HEVC frame	EDR
BasketBallDrive	0.9538
BQMall	0.9486
BQSquare	0.9647
FourPeople	0.9348
PartyScene	0.9534
Traffic	0.9462

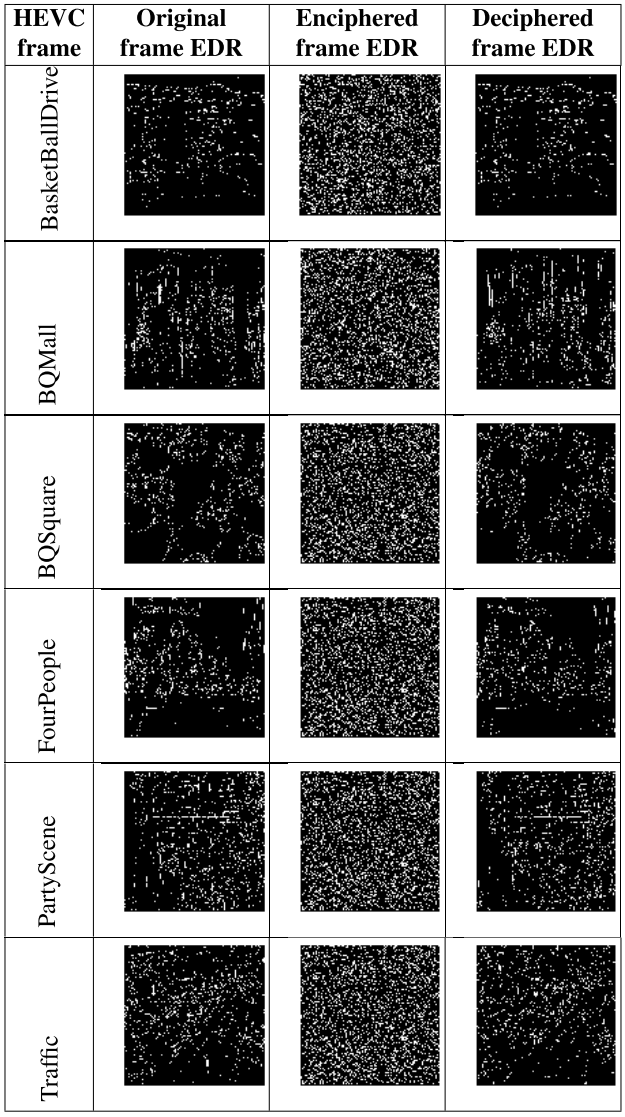


FIGURE 19. Laplacian Gaussian EDR findings of the original, enciphered, and deciphered HEVC frames.

the opponent sees the correlation and relation among the two enciphered HEVC frames and the original HEVC frame [30]. The differential security cryptanalytics is a process that helps in decoding an HEVC frame. Consequently, it is obvious that the suggested optical HEVC cryptography algorithm should be against differential attempts, which necessitates that it must be convoluted for the assailants to realize how the plain HEVC frames are correlated with the enciphered HEVC frames. The Unified Averaged Changed Intensity (UACI)

TABLE 9. The UACIs and NPCRs of the examined HEVC frames.

HEVC frame	UACI	NPCR
BasketBallDrive	0.334934	0.99617
BQMall	0.338381	0.99607
BQSquare	0.334382	0.99632
FourPeople	0.334592	0.99639
PartyScene	0.338773	0.99678
Traffic	0.332834	0.99637

TABLE 10. The execution times of the enciphered/deciphered HEVC frames.

HEVC frame	Time (sec)
BasketBallDrive	5.52
BQMall	5.88
BQSquare	6.16
FourPeople	5.72
PartyScene	6.98
Traffic	7.94

and Number of Changing Pixel Rate (NPCR) are the two most important statistics developed for this objective [30]. These assessment statistics are formulated as in Eqs. (23) and (24) [48].

$$UACI\,(E_1, E_2) = \frac{1}{255 \times m \times n}\left[\sum_{a=1}^{m}\sum_{b=1}^{n}[E_1(a,b) - E_2(a,b)]\right] \times 100 \tag{23}$$

$$NPCR\,(E_1, E_2) = \frac{\sum_{a=1}^{m}\sum_{b=1}^{n} D(a,b)}{m \times n} \times 100 \tag{24}$$

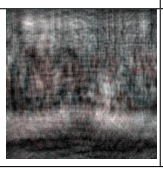
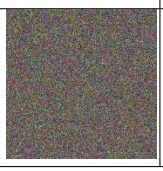
where $E_2(a, b)$ and $E_1(a, b)$ are the two enciphered HEVC frames corresponding to the plain HEVC frame after and before a slight modification, correspondingly. The n and m values relate to the height and width (size) of the HEVC frame. When $E_2(a, b) \neq E_1(a, b)$, the $D(a, b) = 1$, and when $E_2(a, b) = E_1(a, b)$, the $D(a, b) = 0$.

The substantiated and anticipated optimum NPCR and UACI values are roughly 0.33 and 0.996, correspondingly [12]. With achieving these optimal quantities, it will be implied that the enciphering procedure is extremely susceptible to the original HEVC stream, and therefore the proposed cryptography algorithm will be robust and secure against the statistical differential attacks. Table 9 reveals the NPCR and UACI findings of the examined HEVC streams. It is observed that the whole achieved results are extraordinarily near to the theoretic optimum results.

D. COMPUTATIONAL PROCESSING ANALYSIS

The good quality of any employed cryptosystem is predicted to have a speedy implementation rate to accomplish lower processing computations. Various HEVC frames have been employed as samples to assess the decryption/enciphering implementation time of the proposed optical HEVC cryptography algorithm. The outcomes of the average decryption/enciphering time exploited in the proposed optical HEVC cryptography system for processing the examined HEVC streams are depicted in Table 10. It is remarked that these accomplished execution speeds are satisfactory by contemplating its incredible security and confidentiality level for HEVC communication services.

TABLE 11. The average outcomes of the enciphered HEVC FourPeople streams for the proposed optical cryptography algorithm compared to the related algorithms.

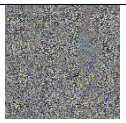
Metric	Algorithm		
	OSH [49], [50]	DRPE [12], [51]	Proposed
Entropy	7.621	7.8391	7.9907
Correlation	0.1624	0.1037	0.0691
ID	0.09234	0.09685	0.005329
HD	3.9657	2.9648	2.4362
UACI	0.34268	0.339658	0.334592
NPCR	0.98795	0.99325	0.99639
FSIM	0.4837	0.4012	0.3732
SSIM	0.1306	0.04382	0.0059
PSNR (dB)	12.8347	11.5381	9.8957
EDR	0.8964	0.9234	0.9348
Time (sec) encipher-ing/deciphering	3.86	7.58	5.72
Visual			

E. COMPARATIVE STUDY AGAINST RELATED WORK

This section investigates how properly the several evaluation considerations of the proposed optical HEVC cryptography algorithm are better contrasted to the most modern related studies whether digital or optical cryptography techniques. Consequently, to supplementary approve the effective performance of the proposed optical cryptography algorithm for secure and efficient HEVC transmission over deceitful communication mediums, a security assessment analysis has been examined to appraise the security and privacy competence of the proposed optical cryptography algorithm contrasted to the two most common optical cryptography algorithms. So, the proposed optical cryptography algorithm is compared to the optical DRPE (Double Random Phase Encoding) algorithm and the OSH (optical Scanning Holography) algorithm [12], [49]–[51]. The outcomes of the average values of several runs of the experiments of the statistical security analyses for the enciphered/deciphered frames of the HEVC FourPeople sequence are demonstrated in Table 11. From this comparative study, it is substantiated that the proposed optical cryptography algorithm affords satisfactory statistical security outcomes for the ciphered HEVC frames in contrast to the recent preceding related optical DRPE and OSH ciphering procedures.

Also, the proposed optical cryptography algorithm is compared to the recent related digital-based cryptosystem in [11];

TABLE 12. Comparison investigation between the proposed optical-based encryption work and the related digital-based cryptosystem in [11].

Metric	Ref. [11]		Proposed work	
	PoznanHall	FourPeople	PoznanHall	FourPeople
Entropy	7.9989	7.999	7.99596	7.9907
Correlation (H)	-0.0199	0.04164	0.02476	0.0691
Correlation (V)	-0.007	0.09352	0.037547	0.1024
Correlation (D)	-0.0129	0.07525	0.02373	0.0843
ID	0.006988	0.0048	0.00496	0.005329
HD	3.18804	1.4777	4.83472	2.4362
UACI	0.330626	0.320761	0.334635	0.334592
NPCR	0.99631	0.995936	0.996093	0.99639
FSIM	0.2343	0.38868	0.2683	0.3732
SSIM	0.0035	0.0062	0.0048	0.0059
PSNR (dB)	8.4139	8.7924	9.3274	9.8957
EDR	0.90556	0.8792	0.9507	0.9348
Time (sec) enciphering/deciphering	12.26	11.48	5.9	5.72
Visual				

to additionally confirm the efficacy of the proposed optical cryptography algorithm for HEVC communication in comparison with the digital-based encryption algorithms. The outcomes of the average values of the statistical security analyses and visual findings for the enciphered/deciphered frames of the HEVC PoznanHall and FourPeople sequences are demonstrated in Table 12. From this comparison, it is validated that the proposed optical cryptography algorithm offers reasonable statistical security findings for the ciphered HEVC frames in contrast to the digital-based encryption algorithms, especially in terms of the processing time. This is due to the great advantages of the proposed optical-based encryption algorithm compared to digital-based encryption algorithms in terms of computational processing, parallelism, and security. Therefore, the obtained lower computational processing time of the proposed optical cryptography algorithm encourages its utilization for real-time video streaming applications.

VII. CONCLUSION AND FUTURE DIRECTIONS

This paper introduced an optical HEVC cryptography algorithm for efficient and secure multimedia communication applications, which is more safeguard in contrast to intruders and attackers. The foremost involvement and impact of this research work is the utilization of the 2D-FrFT ciphering process with the 3D-JST for developing an efficient and secure optical HEVC cryptography algorithm. Therefore, the proposed cryptography algorithm combines more diffusion and permutation to the ciphered HEVC frames, simultaneously. The proposed algorithm was heavily examined against several evaluation metrics to prove its security and efficiency. The simulation results revealed the high performance of the proposed optical cryptography in almost all tested metrics and in comparisons with related work to effectively ciphering the streamed HEVC frames. Consequently, it is more suitable for securing video communication in contrast to conventional cryptography algorithms.

The future research strategy can incorporate the realization of a cascaded multimedia security algorithm with the utilization of various watermarking, ciphering, and steganography procedures for further reliable and robust streaming of HEVC data over insecure communication channels. Additionally, we plan to employ the optimization and deep learning technologies for cryptography algorithms of secure video transmission.

ACKNOWLEDGMENT

The authors would like to thank the support of Prince Sultan University for paying the Article Processing Charges (APC) of this publication.

REFERENCES

[1] W. El-Shafai, S. El-Rabaie, M. M. El-Halawany, and F. E. A. El-Samie, "Security of 3D-HEVC transmission based on fusion and watermarking techniques," *Multimedia Tools Appl.*, vol. 78, no. 19, pp. 27211–27244, Oct. 2019.

[2] M. Al-Akhras, H. Zedan, R. John, and I. ALMomani, "Non-intrusive speech quality prediction in VoIP networks using a neural network approach," *Neurocomputing*, vol. 72, nos. 10–12, pp. 2595–2608, Jun. 2009.

[3] W. El-Shafai, S. El-Rabaie, M. M. El-Halawany, and F. E. A. El-Samie, "Efficient hybrid watermarking schemes for robust and secure 3D-MVC communication," *Int. J. Commun. Syst.*, vol. 31, no. 4, p. e3478, Mar. 2018.

[4] M. Al-Akhras, I. Almomani, and A. Sleit, "An improved e-model using artificial neural network VoIP quality predictor," *Neural Netw. World*, vol. 21, no. 1, pp. 3–26, 2011.

[5] W. El-Shafai, "Pixel-level matching based multi-hypothesis error concealment modes for wireless 3d h. 264/mvc communication," *3D Res.*, vol. 6, no. 3, p. 31, 2015.

[6] W. El-Shafai, S. El-Rabaie, M. M. El-Halawany, and F. E. A. El-Samie, "Encoder-independent decoder-dependent depth-assisted error concealment algorithm for wireless 3D video communication," *Multimedia Tools Appl.*, vol. 77, no. 11, pp. 13145–13172, Jun. 2018.

[7] W. El-Shafai, "Joint adaptive pre-processing resilience and post-processing concealment schemes for 3D video transmission," *3D Res.*, vol. 6, no. 1, p. 10, Mar. 2015.

[8] K. A. Al-Afandy, W. El-Shafai, E.-S.-M. El-Rabaie, F. E. Abd El-Samie, O. S. Faragallah, A. El-Mhalaway, A. M. Shehata, G. M. El-Banby, and M. M. El-Halawany, "Robust hybrid watermarking techniques for different color imaging systems," *Multimedia Tools Appl.*, vol. 77, no. 19, pp. 25709–25759, Oct. 2018.

[9] I. Almomani and M. Al-Akhras, "Statistical speech quality prediction in voip networks," in *Proc. Int. Conf. Commun. Comput.*, vol. 2, 2008, pp. 146–152.

[10] N. F. Soliman, M. Khalil, A. D. Algarni, S. Ismail, R. Marzouk, and W. El-Shafai, "Efficient HEVC steganography approach based on audio compression and encryption in QFFT domain for secure multimedia communication," *Multimedia Tools Appl.*, vol. 80, no. 3, pp. 4789–4823, 2020.

[11] A. Alarifi, S. Sankar, T. Altameem, K. Jithin, M. Amoon, and W. El-Shafai, "A novel hybrid cryptosystem for secure streaming of high efficiency h. 265 compressed videos in IoT multimedia applications," *IEEE Access*, vol. 8, pp. 128548–128573, 2020.

[12] O. S. Faragallah, M. A. Alzain, H. S. El-Sayed, J. F. Al-Amri, W. El-Shafai, A. Afifi, E. A. Naeem, and B. Soh, "Block-based optical color image encryption based on double random phase encoding," *IEEE Access*, vol. 7, pp. 4184–4194, 2019.

[13] O. S. Faragallah, M. A. AlZain, H. S. El-Sayed, J. F. Al-Amri, W. El-Shafai, A. Afifi, E. A. Naeem, and B. Soh, "Secure color image cryptosystem based on chaotic logistic in the FrFT domain," *Multimedia Tools Appl.*, vol. 79, nos. 3–4, pp. 2495–2519, Jan. 2020.

[14] G. Ye, K. Jiao, H. Wu, C. Pan, and X. Huang, "An asymmetric image encryption algorithm based on a fractional-order chaotic system and the RSA public-key cryptosystem," *Int. J. Bifurcation Chaos*, vol. 30, no. 15, Dec. 2020, Art. no. 2050233.

[15] I. Almomani, "Investigating the use of encryption techniques and different speech coders with multimedia streaming," *Int. J. Comput. Sci. Inf. Secur.*, vol. 14, no. 9, pp. 454–460, 2016.

[16] J. Zhou, N.-R. Zhou, and L.-H. Gong, "Fast color image encryption scheme based on 3D orthogonal latin squares and matching matrix," *Opt. Laser Technol.*, vol. 131, Nov. 2020, Art. no. 106437.

[17] W. El-Shafai, E.-S.-M. El-Rabaie, M. El-Halawany, and F. E. A. El-Samie, "Efficient multi-level security for robust 3D color-plus-depth HEVC," *Multimedia Tools Appl.*, vol. 77, no. 23, pp. 30911–30937, Dec. 2018.

[18] 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. A. El-Samie, "Investigation of chaotic image encryption in spatial and FrFT domains for cybersecurity applications," *IEEE Access*, vol. 8, pp. 42491–42503, 2020.

[19] M. N. Asghar, R. Kousar, H. Majid, and M. Fleury, "Transparent encryption with scalable video communication: lower-latency, CABAC-based schemes," *J. Vis. Commun. Image Represent.*, vol. 45, pp. 122–136, May 2017.

[20] K. Go, I.-G. Lee, S. Kang, and M. Kim, "Secure video transmission framework for battery-powered video devices," *IEEE Trans. Dependable Secure Comput.*, early access, Mar. 13, 2020, doi: 10.1109/TDSC.2020.2980256.

[21] B. Guan, D. Xu, and Q. Li, "An efficient commutative encryption and data hiding scheme for HEVC video," *IEEE Access*, vol. 8, pp. 60232–60245, 2020.

[22] R. Kousar, H. Majid, M. N. Asghar, and M. Fleury, "Effective transparent encryption scheme with scalable video communication," in *Proc. 6th Int. Conf. Innov. Comput. Technol. (INTECH)*, Aug. 2016, pp. 556–560.

[23] O. S. Faragallah, A. Afifi, H. S. El-Sayed, M. A. Alzain, J. F. Al-Amri, F. E. A. El-Samie, and W. El-Shafai, "Efficient HEVC integrity verification scheme for multimedia cybersecurity applications," *IEEE Access*, vol. 8, pp. 167069–167089, 2020.

[24] W. Hamidouche, M. Farajallah, N. Sidaty, S. E. Assad, and O. Déforges, "Real-time selective video encryption based on the chaos system in scalable HEVC extension," *Signal Process., Image Commun.*, vol. 58, pp. 73–86, Oct. 2017.

[25] Y. Tew, K. Wong, and R. C.-W. Phan, "Region-of-interest encryption in HEVC compressed video," in *Proc. IEEE Int. Conf. Consum. Electron.-Taiwan (ICCE-TW)*, May 2016, pp. 1–2.

[26] K. Thiyagarajan, R. Lu, K. El-Sankary, and H. Zhu, "Energy-aware encryption for securing video transmission in Internet of multimedia things," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 29, no. 3, pp. 610–624, Mar. 2019.

[27] M. A. Taha, N. Sidaty, W. Hamidouche, O. Dforges, J. Vanne, and M. Viitanen, "End-to-End real-time ROI-based encryption in HEVC videos," in *Proc. 26th Eur. Signal Process. Conf. (EUSIPCO)*, Sep. 2018, pp. 171–175.

[28] A. Shifa, M. N. Asghar, S. Noor, N. Gohar, and M. Fleury, "Lightweight cipher for H.264 videos in the Internet of multimedia things with encryption space ratio diagnostics," *Sensors*, vol. 19, no. 5, p. 1228, 2019.

[29] F. Peng, X. Zhang, Z.-X. Lin, and M. Long, "A tunable selective encryption scheme for H.265/HEVC based on chroma IPM and coefficient scrambling," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 30, no. 8, pp. 2765–2780, Aug. 2020.

[30] Z. Shahid and W. Puech, "Visual protection of HEVC video by selective encryption of CABAC binstrings," *IEEE Trans. Multimedia*, vol. 16, no. 1, pp. 24–36, Jan. 2014.

[31] M. Abu Taha, W. Hamidouche, N. Sidaty, M. Viitanen, J. Vanne, S. El Assad, and O. Deforges, "Privacy protection in real time HEVC standard using chaotic system," *Cryptography*, vol. 4, no. 2, p. 18, Jun. 2020.

[32] H. Xu, X. Tong, Z. Wang, M. Zhang, Y. Liu, and J. Ma, "Robust video encryption for H.264 compressed bitstream based on cross-coupled chaotic cipher," *Multimedia Syst.*, vol. 26, pp. 363–381, Feb. 2020.

[33] J. He, Y. Xu, W. Luo, S. Tang, and J. Huang, "A novel selective encryption scheme for H.264/AVC video with improved visual security," *Signal Process., Image Commun.*, vol. 89, Nov. 2020, Art. no. 115994.

[34] A. Sinha, "Image encryption by using fractional Fourier transform and jigsaw transform in image bit planes," *Opt. Eng.*, vol. 44, no. 5, May 2005, Art. no. 057001.

[35] J. M. Vilardy O., L. Barba J., and C. O. Torres M., "Image encryption and decryption systems using the jigsaw transform and the iterative finite field cosine transform," *Photonics*, vol. 6, no. 4, p. 121, Nov. 2019.

[36] P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," *Opt. Lett.*, vol. 20, no. 7, pp. 767–769, 1995.

[37] S. Ibrahim, S. Ibrahim, M. G. Egila, H. Shawky, M. K. H. Elsaid, W. El-Shafai, and F. E. A. El-Samie, "Cancelable face and fingerprint recognition based on the 3D jigsaw transform and optical encryption," *Multimedia Tools Appl.*, vol. 79, pp. 14053–14078, Feb. 2020.

[38] Z. Ma and S. Sun, "Research on HEVC screen content coding and video transmission technology based on machine learning," *Ad Hoc Netw.*, vol. 107, Oct. 2020, Art. no. 102257.

[39] A. S. Y. Irawan, A. F. El Ramdhani, M. Jordi, R. S. Mahdi, and T. Al Mudzakir, "Implementasi algoritma advanced encryption standard (aes) untuk mengamankan file video," *Systematics*, vol. 2, no. 1, pp. 28–32, 2020.

[40] A. Ajmera, M. Divecha, S. S. Ghosh, I. Raval, and R. Chaturvedi, "Video steganography: Using scrambling-AES encryption and DCT, DST steganography," in *Proc. IEEE Pune Sect. Int. Conf. (PuneCon)*, Dec. 2019, pp. 1–7.

[41] P. Kumar, J. Joseph, and K. Singh, "Optical image encryption using a jigsaw transform for silhouette removal in interference-based methods and decryption with a single spatial light modulator," *Appl. Opt.*, vol. 50, no. 13, pp. 1805–1811, 2011.

[42] M. Borda, *Fundamentals in Information Theory and Coding*. Cham, Switzerland: Springer, 2011.

[43] J. Taylor, *Introduction to Error Analysis, the Study of Uncertainties in Physical Measurements*. New York, NY, USA: Univ. Science Books, 1997.

[44] C. J. Stone, "An asymptotically optimal histogram selection rule," in *Proc. Berkeley Conf. Honor Jerzy Neyman Jack Kiefer*, vol. 2. Belmont, CA, USA: Wadsworth, 1984, pp. 513–520.

[45] D. W. Scott, "On optimal and data-based histograms," *Biometrika*, vol. 66, no. 3, pp. 605–610, 1979.

[46] S. E. Umbaugh, *Digital Image Processing and Analysis: Human and Computer Vision Applications With CVIPtools*. Boca Raton, FL, USA: CRC Press, 2010.

[47] D. Ziou and S. Tabbone, "Edge detection techniques—An overview," *Pattern Recognit. Image Anal. C/C Raspoznavaniye Obrazov I Analiz Izobrazhenii*, vol. 8, pp. 537–559, Dec. 1998.

[48] D. Coppersmith, "The data encryption standard (DES) and its strength against attacks," *IBM J. Res. Develop.*, vol. 38, no. 3, pp. 243–250, May 1994.

[49] P. W. M. Tsang, A. Yan, T.-C. Poon, and H. Lam, "Asymmetrical and biometric encrypted optical scanning holography (ABE-OSH)," *IEEE Trans. Ind. Informat.*, vol. 16, no. 2, pp. 1094–1101, Feb. 2020.

[50] L.-Z. Zhang, X. Zhou, D. Wang, N.-N. Li, X. Bai, and Q.-H. Wang, "Multiple-image encryption based on optical scanning holography using orthogonal compressive sensing and random phase mask," *Opt. Eng.*, vol. 59, no. 10, p. 102411, 2020.

[51] J. M. Vilardy, M. S. Millán, and E. Pérez-Cabré, "Experimental optical encryption scheme for the double random phase encoding using a nonlinear joint transform correlator," *Optik*, vol. 217, Sep. 2020, Art. no. 164653.

WALID EL-SHAFAI was born in Alexandria, Egypt. He received the B.Sc. degree (Hons.) in electronics and electrical communication engineering from the Faculty of Electronic Engineering (FEE), Menoufia University, Menouf, Egypt, in 2008, the M.Sc. degree from the Egypt-Japan University of Science and Technology (E-JUST), in 2012, and the Ph.D. degree from the Faculty of Electronic Engineering, Menoufia University, in 2019. Since January 2021, he has been joined as a Postdoctoral Research Fellow at the Security Engineering Lab (SEL), Prince Sultan University (PSU), Riyadh, Saudi Arabia. He is currently working as a Lecturer and an Assistant Professor with the Electronics and Communication Engineering (ECE) Department, FEE, Menoufia University. His research interests include wireless mobile and multimedia communications systems, image and video signal processing, efficient 2D video/3D multi-view video coding, multi-view video plus depth coding, 3D multi-view video coding and transmission, quality of service and experience, digital communication techniques, cognitive radio networks, adaptive filters design, 3D video watermarking, steganography, and encryption, error resilience and concealment algorithms for H.264/AVC, H.264/MVC, and H.265/HEVC video codecs standards, cognitive cryptography, medical image processing, speech processing, security algorithms, software defined networks, the Internet of Things, medical diagnoses applications, FPGA implementations for signal processing algorithms and communication systems, cancellable biometrics and pattern recognition, image and video magnification, artificial intelligence for signal processing algorithms and communication systems, modulation identification and classification, image and video super-resolution and denoising, cybersecurity applications, deep learning in signal processing, and communication systems applications. He has several publications in the above research areas in several reputable international and local journals and conferences. Also, he serves as a reviewer for several international journals.

IMAN M. ALMOMANI (Senior Member, IEEE) received the bachelor's and master's degrees in computer science from UAE and Jordan, in 2000 and 2002, respectively, and the Ph.D. degree in wireless network security from De Montfort University, U.K., in 2007. She is currently an Associate Professor of Cybersecurity. She is also the Associate Director of the Research and Initiatives Centre (RIC) and also the Leader of the Security Engineering Lab (SEL), Prince Sultan University (PSU), Riyadh, Saudi Arabia. Before Joining Prince Sultan University, she worked as an Associate Professor and the Head of the Computer Science Department, The University of Jordan, Jordan. Her research interests include wireless networks and security, mainly wireless mobile ad hoc networks (WMANETs), wireless sensor networks (WSNs), multimedia networking (VoIP), and security issues in wireless networks. She is also interested in the area of electronic learning (e-learning) and mobile learning (m-learning). She has several publications in the above areas in a number of reputable international and local journals and conferences. She is in the organizing and technical committees for a number of local and international conferences. Also, she serves as a reviewer and a member of the editorial board in a number of international journals. She is also a Senior Member of IEEE WIE.

AALA ALKHAYER received the B.Eng. degree (Hons.) in information technology engineering from SVU University, Damascus, in 2017, and the bachelor's degree (Hons.) in software engineering from Prince Sultan University (PSU), Riyadh, Saudi Arabia, in 2018. She is currently pursuing the M.Sc. degree in computer science (big data systems) with Arizona State University, USA. She is also a Research Engineer with the Security Engineering Lab (SEL), PSU. Her research interests include software engineering, networks security, malware analysis, multimedia networking, and computer vision.