IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received June 10, 2020, accepted July 7, 2020, date of publication July 13, 2020, date of current version July 23, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3008644

A Novel Hybrid Cryptosystem for Secure Streaming of High Efficiency H.265 Compressed Videos in IoT Multimedia Applications

ABDULAZIZ ALARIFI[1], SYAM SANKAR[2], TORKI ALTAMEEM[1], K. C. JITHIN[2], MOHAMMED AMOON[1], AND WALID EL-SHAFAI[3]

[1]Department of Computer Science, Community College, King Saud University, Riyadh 11437, Saudi Arabia
[2]Department of Computer Science and Engineering, NSS College of Engineering, Palakkad 678008, India
[3]Department of Electronics and Electrical Communications Engineering, Faculty of Electronic Engineering, Menoufia University, Menouf 32952, Egypt

Corresponding author: Abdulaziz Alarifi (abdulazizalarifi@ksu.edu.sa)

The authors extend their appreciation to the Deanship of Scientific Research at King Saud University for funding this work through Research Group No (RG-1440-039).

ABSTRACT In this modernistic age of innovative technologies like big data processing, cloud computing, and Internet of things, the utilization of multimedia information is growing daily. In contrast to other forms of multimedia, videos are extensively utilized and streamed over the Internet and communication networks in numerous Internet of Multimedia Things (IoMT) applications. Consequently, there is an immense necessity to achieve secure video transmission over modern communication networks due to the third-party exploitation and falsification of transmitted and stored digital multimedia data. The present methods for secure communication of multimedia content between clouds and mobile devices have constraints in terms of processing load, memory support, data size, and battery power. These methods are not the optimum solutions for large-sized multimedia content and are not appropriate for the restricted resources of mobile devices and clouds. The High-Efficiency Video Coding (HEVC) is the latest and modern video codec standard introduced for efficiently storing and streaming of high-resolution videos with suitable size and higher quality. In this paper, a novel hybrid cryptosystem combining DNA (Deoxyribonucleic Acid) sequences, Arnold chaotic map, and Mandelbrot sets is suggested for secure streaming of compressed HEVC streams. Firstly, the high-resolution videos are encoded using the H.265/HEVC codec to achieve efficient compression performance. Subsequently, the suggested Arnold chaotic map ciphering process is employed individually on three channels (Y, U, and V) of the compressed HEVC frame. Then, the DNA encoding sequences are established on the primary encrypted frames resulted from the previous chaotic ciphering process. After that, a modified Mandelbrot set-based conditional shift process is presented to effectively introduce confusion features on the Y, U, and V channels of the resulted ciphered frames. Massive simulation results and security analysis are performed to substantiate that the suggested HEVC cryptosystem reveals astonishing robustness and security accomplishment in contrast to the literature cryptosystems.

INDEX TERMS Video cryptography, H.265-HEVC, DNA, Mandelbrot sets, IoMT, Arnold chaotic map.

I. INTRODUCTION

Internet of Things (IoT) systems have enormous computation and processing costs, and deliver massive amounts of multimedia data, specifically upon storage utilizing cloud systems [1]. Therefore, the new expansion in the processing resources of smart devices has developed intelligent IoT services, supporting the connection of distributed nodes to analyze, perceive and collect essential multimedia data from the surrounding environment [2]. Wireless multimedia networks are part of these IoT-supported services, which comprises visual sensors (cameras) that monitor certain actions from

The associate editor coordinating the review of this manuscript and approving it for publication was Parul Garg.

various intersecting observations by continuously gaining video frames, thus creating a huge amount of multimedia data with considerable redundancy. It is commonly approved in the research community of multimedia communication applications and services that the collected multimedia data should be pre-processed to obtain the important and informative content before multimedia streaming [3]. So, it is unpreferable to transmit the visual data through the communication channels without processing (e.g. compression), this is unrealistic due to energy and bandwidth limitations. Therefore, there is a mandatory need for an efficient compression process for multimedia data before their streaming over bandwidth-limited communication channels. The standard of HEVC is the most modern video codec [4], which is utilized for compressing videos, especially high-resolution videos. Thus, it can offer sufficient characteristics customized to various IoT multimedia services and applications. In contrast with its antecedent H.264/AVC (Advanced Video Coding) video codec, the HEVC codec accomplishes 50% compression ratio with great bit rate reduction by exploiting its improved prediction features of temporal and spatial estimation processes [5].

The rapid improvement of communication networks and Internet technologies produces further digital multimedia content. Thus, the privacy and security of the multimedia data are of utmost prominence with the growth in veracity, volume, and velocity of the developed multimedia services and applications. The cryptography process conventionally acts as a vital and essential role to protect multimedia data [6]–[10]. In the cryptography process, multimedia data are ciphered to be converted from an intelligible form to an unintelligible one. Therefore, after the ciphering process, multimedia data become worthless for adversaries and intruders, and consequently, they are maintained and protected [11], [12]. In preceding years, numerous cryptography schemes have been suggested, however, most of them have some restrictions. Some schemes are extremely robust but have high processing and computational cost, and some schemes are energy efficient and extraordinarily uncomplicated but do not deliver adequate security performance [13]–[23].

Digital images and video frames have a high relationship and correlation amongst neighboring pixels. Therefore, the preceding introduced traditional cryptography schemes, like AES (Advanced Encryption Standard), DES (Data Encryption Standard), and RSA (Rivest–Shamir–Adleman) [6], [9], are not appropriate for achieving multimedia ciphering with great security efficiency and robustness performance. Lately, various categories of multimedia ciphering schemes based on cellular automata, optical transform, Fourier transform, chaotic systems, magic cube, wavelet transform, etc. have been examined and researched [7], [8], [10], [17], [19], [22], [23]. These cryptosystem categories are divided into two classes of cryptography algorithms based on the methodology employed to model the ciphering and deciphering procedures.

A chaotic cryptosystem is the application of the arithmetic and statistical principles of chaos maps to generate the chaotic sequences that are employed and exploited in cryptography schemes. The chaotic-based multimedia ciphering principally comprises two phases: the confusion (permutation) phase and the diffusion phase [9]. In the permutation phase, the pixel locations are arbitrarily substituted without modifying the authentic values of pixels. So, this phase creates an undetectable video frame for intruders. But the video frame is not incredibly secure with only performing this permutation phase since it may be retrieved by the intruders and adversaries if they repeatedly attempt. So, to enhance privacy, the diffusion phase is urgently required. It principally aims to exchange the pixel values in the whole video frame with other values. Also, the diffusion process can be carried out through certain functions on the pixels of the video frame to sequentially modify their values through some random values of chaotic sequences generated from the utilized chaotic maps. For further achieving trustworthy security and privacy, the confusion and diffusion phases are iterated a specific number of times. The randomness feature of the chaotic maps makes it proper and recommended for the services and applications of multimedia cryptosystems [6], [8], [10].

The utilization of chaos principles in the cryptography process is firstly researched by Robert Matthews in 1989, they have gained much attention, but long-time interests about their execution speed and security continue to restrict their implementation issues. Several chaos-based video and image ciphering techniques have been suggested by numerous researchers all over the world [13], [15], [16], [21]–[30]. Hamidouche *et al.* [24] suggested a real-time selective HEVC cryptography approach based on the chaos map. In the proposed approach, two distinct chaotic maps are employed named the STM (Skew Tent Map) and the PWLCM (Piecewise Linear Chaotic Map). The presented approach scrambles a group of sensitive parameters in HEVC frames with a lower complexity and delay overheads. Also, it accomplishes both formats conforming video ciphering needs and constant bitrate. Valli and Ganesan [25] introduced a chaos-based video cryptography scheme utilizing Ikeda time-delay system and chaotic maps. The proposed cryptography scheme comprises two chaos-based video ciphering methods. The first one is the superior-dimensional 12D chaos map and the second one is chaos-based Ikeda DDE (Delay Differential Equation) which is appropriate for constructing a real-time reliable and secure symmetric video ciphering process. So, recently, the chaos-based cryptography algorithms get extra attention among researchers. They are effective in accomplishing increased speed and extremely guaranteed multimedia ciphering because of its wonderful characteristics, such as ergodicity, mixing, randomness, and higher sensitivity to control factors and preliminary conditions.

The DNA-based cryptosystem is an additional area of cryptography promising with the analysis of DNA encoding rules for creating secure image and video ciphering systems with low processing and long encryption key.

Maniyath and Kaiselvan [26] presented a DNA-based cryptosystem for multimedia communication over insecure channels. In the presented cryptosystem, successive XORed operations with DNA calculations are employed to attain more robustness and security. Zhang *et al.* [27] suggested a coupled map lattices and DNA-based cryptography scheme based on the spatio-temporal chaos cryptographic features and characteristics. The DNA computing policy and one-time pad ciphering strategy are exploited to improve the sensitivity performance against differential, plaintext, statistical, and brute-force attacks. Wang *et al.* [28] suggested a Lorenz map and DNA permutations-based image ciphering algorithm. In the presented algorithm, the chaos pseudo-random sequences generated from the 3D Lorenz map are utilized for the ciphering process with long and more secret keys. Also, the DNA subtraction/addition and permutation operations are introduced to completely break pixels correlations and bit planes of the original image to achieve higher sensitivity and resistance against brute-force, differential, and statistical attacks. Consequently, DNA encoding-based cryptography procedure has many attractive characteristics for multimedia cryptosystems like massive storage, vast parallelism, and extreme-minimal power consumption. Lots of scientists and researchers have merged the merits of DNA encoding and chaos algorithms to extremely improve the privacy and security of multimedia communication and streaming [30].

In this paper, a novel cost-effective HEVC cryptosystem combining DNA encoding sequences, Arnold chaotic map, and modified Mandelbrot sets is introduced. The key achievement of this paper is to build a DNA based chaos HEVC cryptosystem, which can resist the whole categories of conventional kinds of multimedia attacks. Also, the suggested cryptosystem enhances the whole of the assessment security parameters so that the compressed HEVC frames can be streamed efficiently having no possibility of being exposed/deciphered by the intruders and adversaries. Furthermore, the suggested cryptosystem has a large keyspace, so it is robust against brute-force attacks. Moreover, one of the main features of the introduced cryptosystem that it can encrypt any size of HEVC frames.

The rest of the article is coordinated as follows. Section II explains a variety of related works and its vulnerabilities. The preliminary works related to the suggested cryptosystem are discussed in section III. Section IV presents the suggested HEVC cryptosystem. Comparison analysis and experimental security results are investigated in section V. Section VI depicts the conclusions and future suggestions work.

II. REVIEW OF RELATED WORKS

Cryptography algorithms such as IDEA (International Data Encryption Algorithm), DES, AES, and RSA are not appropriate for multimedia ciphering due to two main considerations: (1) superfluous pixel values and (2) high relationship and correlation amongst pixels in images and video frames [31]. Therefore, numerous cryptography algorithms utilizing DNA encoding and chaotic maps aiming to encrypt images and videos securely and robustly are introduced by several academicians and researchers. A summary of the most recent image and video ciphering techniques is provided in this section.

In [32], the authors suggested an enhanced hybrid data hiding and ciphering approach for information protection of HEVC streams. The proposed hybrid approach exploits the syntax elements of the sign of motion vector difference (MVD), the sign of quantized transform coefficient (QTC), and the magnitude of MVD of the compressed HEVC streams for data hiding and ciphering processes. The main advantage of the suggested approach is that it saves the format compliance of the transmitted bitstreams and keeping the video bit rate unaffected. Also, it introduces higher embedding capacity with efficient extraction of embedded and encrypted information. In [33], an efficient HEVC ciphering scheme for scalable video transmission is introduced. The introduced scheme encrypts the content-adaptive binary arithmetic coding (CABAC) parameters of the coded block flag, macro-block types, transform coefficient (TCs), delta quantization parameters (dQPs) and MVD of the compressed HEVC streams. A simple Exclusive OR process based on pseudo-random number generator is employed for encryption purposes. The suggested ciphering scheme has the merit of reducing the bandwidth and ciphering latency.

Tew *et al.* [34] suggested region-of-interest-based three different types of ciphering schemes for the significant values of the binary bin symbols, suffixes in chosen coding tree unit (CTU), and skip transforms signals of the encoded slices of the HEVC streams. The suggested schemes are employed without introducing parsing overhead throughout the encryption and decryption procedures. Yang *et al.* [35] introduced improved format compliance ciphering technique to encrypt the compressed bitstreams of the HEVC sequences. The suggested technique chooses the highly important syntax elements (cu_qp_de/ta_abs, mvd_sign_flag, the suffix of abs_mvd_minus2, and the coeff_sign_flag) of the HEVC bitstreams to be encrypted utilizing the advanced encryption standard (AES) algorithm. The suggested technique presented acceptable security parameters with relatively low complexity. Ma *et al.* [36] introduced a security-maintaining motion estimation scheme for HEVC streams. Both compression and ciphering processes are employed to save the format compliance of the transmitted HEVC data, where the ciphered data have an identical bit rate as the original encoded HEVC data. The major properties of the suggested encoding-ciphering technique are achieving higher encoding ratio desirable and lower processing complexity.

Thiyagarajan *et al.* [37] presented a low overhead and energy-concerned ciphering for HEVC communication in IoMT to secure and scramble the structural video syntax elements of intra-prediction modes, the texture video syntax elements of transform coefficients and the motion video syntax elements of the motion associated codewords. The presented IoMT-based HEVC ciphering algorithm modifies and adapts the choice of the aforesaid video syntaxes to be

encoded corresponding to the motion energy, texture, and structure present in every HEVC frame. So, the suggested algorithm adapts between two cases of high and low energy levels of the frames in HEVC sequences based on an adaptive and estimated threshold. In the case of a high-energy video frame, the proposed ciphering algorithm encrypts the completely HEVC syntax components. In the case of a low-energy video frame, the proposed ciphering algorithm encrypts alternative HEVC syntax components for accomplishing minimal ciphering overhead. The extensive simulation results proved that the suggested IoMT-based ciphering algorithm powerfully decreases the ciphering overhead with an acceptable security degree.

In [38], a real-time end-to-end region-of-interest (ROI)-based HEVC ciphering algorithm is introduced. The suggested ciphering algorithm divides the input HEVC frame into discrete rectangular regions to obtain ROI areas from the background of the video frame, and only these extracted ROI regions are ciphered. The selective HEVC ciphering algorithm encrypts a set of syntax video components that maintains the format compliant of the HEVC codec. Consequently, the ciphered video bit-streams can be deciphered with a typical HEVC decoder with only the knowledge of a secret key to decrypt the ROI regions. The obtained results demonstrated that the presented ROI-based HEVC ciphering algorithm can be performed for real-time security applications with achieving miniature complexity expenses and transmission bitrate.

In [39], a lightweight IoMT-based selective encryption algorithm for H.264 video communication is proposed. This algorithm encrypts the chosen syntax video components with the exclusive OR (XOR) based on an extended permutation process. The results confirmed that the suggested H.264 selective ciphering algorithm delivered considerable privacy with a little complexity and an insignificant bitrate overhead of the ciphering process, which validated that this presented security algorithm is an appropriate option for energy-constrained mobile devices in an IoMT ecosystem. In [40], a lightweight ciphering-based safeguard information sharing and storage utilizing public clouds and HEVC is introduced. The presented ciphering procedure is based on the AES algorithm and it is suggested for the information communication between the media clouds and mobile users. The suggested algorithm encrypts the intra-unsliced-encoded bit streams of the input HEVC videos to sustain power-conserving limitation and real-time computational processing. The simulation outcomes indicated that the suggested algorithm provided minimal processing time and transmission bitrate to be readily employed for real-time video transmission in cloud services.

More chaos and DNA-based image cryptography algorithms are introduced in the literature works. These algorithms can be exploited and adapted for HEVC-based cryptosystems. Chai *et al.* [6] suggested a new hybrid image ciphering technique based on DNA encoding, row-by-row diffusion process, and wave-based permutation process. This technique achieves great privacy and confidentiality results and can withstand several multimedia attacks like chosen-plaintext attacks and more. In [11], a novel image cryptography algorithm of DNA encoding, pixel permutation, and two-dimensional Henon-sine map has been presented and implemented to achieve an efficient diffusion process on the values of image pixels. The ciphering technique introduced in [41] employed DNA functions and a hamming distance approach in scrambling digital images to increase the cryptosystem capability to survive chosen and known-plaintext attacks. Although these aforementioned image cryptosystems further enhanced assessment security factors, their keyspace is relatively inadequate. Also, these ciphering algorithms presented in [6], [11], [41] are implemented only for gray digital images. Therefore, before employing the cryptography process, there is an additional encumbrance of transforming color digital images and other kinds of information to the consistent form of gray digital images.

The authors in [42] introduced a hybrid cryptography algorithm of DNA sequence procedure and cellular automata to encipher multiple digital images. This algorithm has an improvement in enhancing performance computational time, however, it can be employed only for gray digital images and no considerable variations in the obtained values of assessment security factors have been detected while competing with the previous cryptography algorithms. Numerous chaos-based procedures in digital image cryptography [43]–[47] are inadequate to withstand the conventional known-plaintext and chosen-plaintext attacks [31]. It is noticed that the preliminary conditions employed in chaotic maps play a crucial task in determining the chaotic performance. In [48], the authors implemented the DNA encoding and Message-Digest hash algorithm (MD5) to generate primary conditions of the employed chaotic maps. In [49], the authors suggested a joint cryptography algorithm based on cellular neural network and DNA encoding to generate chaotic sequences. These sequences are exploited to break the extreme correlations amongst neighboring pixels of a digital image.

For robust multimedia cryptosystems, it is very significantly necessary to have any designed cryptography process not only based on the secret keys but as well on the input original video frame or image. In [12], a robust image cryptography algorithm is suggested in which the employed key streams for the ciphering process are produced from the input plain image and a secret key creating the cryptosystem to work in a different way for every input digital image. It is proved that this cryptography algorithm withstands chosen and known-plaintext multimedia attacks, although the obtained entropy values are comparatively low when contrasted to other cryptography algorithms. The suggested work in [8] is developed for the gray image ciphering process based on a hybrid of DNA operations, cellular automata, and hyper-chaotic schemes. This presented cryptosystem seems computationally complex, however, it can avoid the known and chosen-plaintext multimedia attacks. The operations of DNA XOR, subtractions, and additions are employed in the

majority of the cryptosystems explaining image and video ciphering utilizing DNA sequences [7]. In several cryptosystems such as in [7], [50], the Hash functions based on secure Hash algorithm-256 are even utilized to control the preliminary conditions employed for producing secret key streams.

The principal and major vulnerabilities recognized in the related multimedia cryptosystems are as follows:

- The related chaos-based cryptosystems have not indicated the followed criteria for the choice of the employed chaotic map.
- Most of the related cryptosystems merely are only based on secret key streams.
- No meaningful improvement is discovered in the estimated Shannon information entropy (the most important security property in any cryptography science) even in modern related cryptosystems.
- Nearly all related research papers assess their presented work based on an upper limit of five to six test videos or images for investigation and evaluation purposes.
- Almost related cryptosystems are not investigating the effect of different kinds of noises on the analysis of the security performance of the designed system.
- The running speed and computational complexity of almost related cryptosystems have not been considered and examined.
- All security metrics and extensive privacy analyses are not discussed and investigated in detail in almost related cryptosystems.
- Almost related cryptosystems have minimal sensitivity concerning the modification in plaintext (avalanche effect property) and secret key (key sensitivity property).
- Almost related cryptosystems are not achieved both diffusion and confusion properties.

Therefore, most of the related cryptosystems have critical shortcomings, in terms of surplus memory and energy consumption, higher delay and computational cost, and not delivering an adequate degree of confidentiality and privacy, due to their simplicity. Motivated by the preceding debates, to tackle such drawbacks, this paper introduces a novel hybrid HEVC cryptosystem amalgamating Arnold chaotic map, DNA functions, and modified Mandelbrot set. The first step in the proposed cryptosystem is the generation of key streams using the Arnold chaotic map. Then, these generated key streams are encoded with the help of DNA sequences. After that, the calculation of Hamming distance amongst the generated key streams and the Y-U-V compressed video components is performed, then the DNA sequences are used to encode the result of hamming distance step. Finally, an important mechanism that encompasses both confusion and diffusion procedures based on DNA encoding is employed. The XOR operation is exploited to perform the diffusion procedure, while a novel suggested conditional shift scheme is employed to accomplish the confusion procedure of pixel values. The Mandelbrot set is exploited in our proposed cryptosystem to generate the input of the conditional shift scheme, and finally, once again a diffusion process is carried out to obtain the encrypted HEVC frames.

III. PRELIMINARIES

In this section, the basic concepts of the DNA encoding procedure and Mandelbrot sets that are exploited in our proposed HEVC cryptosystem are described.

A. DNA ENCODING PROCEDURE

The procedure of DNA encoding is the operation utilized to map binary values series into DNA bases of thymine (T), adenine (A), cytosine (C), and guanine (G). The structure of genetic code blocks can be constructed from these DNA bases. The choice of T, A, C, and G is achieved with a rule of DNA encoding strategy [14]. Two binary digits at any time can be exploited to employ the encoding process. The available rules of DNA encoding process that can be performed to encode 01, 00, 11, and 10 are 24 forms of rules. There are only eight of these rules that fulfill the complementary rule of Watson-Crick [10], as demonstrated in Table 1.

TABLE 1. The main rules of DNA encoding process.

Rule	1	2	3	4	5	6	7	8
A	00	00	01	01	10	10	11	11
T	11	11	10	10	01	01	00	00
C	01	10	00	11	00	11	01	10
G	10	01	11	01	10	00	10	01

In this paper, to encode the binary sequences, rule 01 is employed for the DNA encoding process. Therefore, this DNA encoding rule is exploited to encode video frames by replacing their binary values of the pixels with the congruous DNA sequences. If we suppose that the $DNAEncode(\cdot)$ is the utilized function for the DNA encoding process. So, for example, if we have a pixel value of 120 with an 8-bit form of (01,111,0 0 0), its DNA encoded structure can be acquired as "CTGA". If we suppose that the $DNADecode(\cdot)$ is the utilized function for the DNA decoding process. So, for example, for a sequence with a DNA form of "TGAC", its decoded binary structure corresponding to the employed DNA rule 01 is given by (11,10 0,0 01) (equals 255 in a decimal manner).

Moreover, the DNA-based XOR function is used in this paper for encoding sequences. Because there are eight DNA rules that fulfill the complementary rule of Watson-Crick [10], so there are eight forms of rules for the DNA-based XOR function that can be utilized in this paper. Thus, the DNA-based XOR function of the employed DNA rule 01 is demonstrated in Table 2. For instance, the result of

TABLE 2. The DNA-based XOR function.

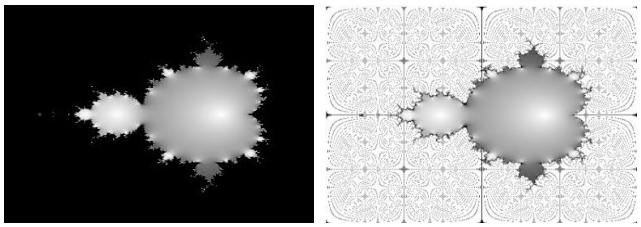
XOR	A	G	C	T
A	A	G	C	T
G	G	A	T	C
C	C	T	A	G
T	T	C	G	A

the DNA-based XOR operation of the two sequences in DNA forms of TGAC and CTGA can be found as GCGC.

B. MANDELBROT SET

The basic idea of the Mandelbrot set (M set) is that it is a collection of points that can be represented in the complex plane. Each point in this plane can be depicted utilizing a complex number $c \in C$ described on the way of $c = x + jy$, where both $x, y \in R$. Figure 1(a) shows an example of the supposed Mandelbrot set structure of the points of a colored video frame in a grey format. Due to the great advantages of the Mandelbrot set [51], we exploited the generated values resulted from this set in the shifting process in our proposed cryptosystem. So, the M set is employed in our work for the purpose that it has convoluted arrangements emerging from a simple characterization, and a minor shift of the control parameter can implement the M set structure. The typical definition of the M set is given in Eq. (1) [51], where $Z_0 = 0$ and C is a constant value that is selected to have a value of 10^{14} in our proposed cryptosystem.

$$\lim_{m\to\infty} Z_{m+1} = Z_m^2 + C \tag{1}$$



(a) M set structure. (b) Modified M set structure.

FIGURE 1. The images of the M set structure and its modified version.

To shuffle off the group of the whole zero values of the black pixels in Figure 1(a), a simple modified M set generation procedure described in Algorithm 1 is suggested. This algorithm is exploited to get a modified version of the Mandelbrot set as given in Figure 1(b), it is noticed that its boundary forms a fractal.

Algorithm 1 Modified M Set Generation Process

input: the image of M set structure (Figure 1(a)).
if *p(m, n)* equals 0 ***then***
  // *p(m, n)* signifies the pixel value at a location *(m, n)* in Figure 1(a).
  p(m, n) = [(m × n) + C] mod 256
end
output: the image of modified M set structure (Figure 1(b)).

IV. PROPOSED HYBRID HEVC CRYPTOSYSTEM

Figure 2 illustrates the structure diagram of the suggested cryptographic procedure. The deciphering process can be constructed by reversing the steps of the encryption process. The suggested HEVC cryptosystem consists of three main phases: (1) Chaotic map sequences-based keystream generation, (2) DNA sequences encoding, and (3) Diffusion-confusion process. This hybrid HEVC cryptosystem is suggested to generate a highly ciphered form of the plain compressed HEVC frame indestructible by the invaders while HEVC streaming in IoMT applications. The ciphering process can be utilized for any HEVC frames whichever size with whatever their content characteristics.

The suggested HEVC cryptographic procedure can be performed using three different phases as shown in Figure 2, and in-detail description of these three phases is given as follows.

A. PHASE (1): CHAOTIC SECRET KEY GENERATION

A proper map choice is one of the essential phases in the ciphering process. The chaotic feature of the secret sequences generated by the chosen map improves the privacy and precludes the ciphered video frames from being divulged or violated by the aggressors. Thus, the choice of the chaotic map controls on the ciphering quality so that the original information pattern of the video frame is hidden in a superior manner. In the suggested cryptography procedure, the Arnold chaotic map is selected to be employed for the ciphering process. We tested the ciphering quality of the Arnold chaotic map compared to other chaotic maps: Logistic map, Henon map, Duffing (Holmes) map, Baker map, Gauss-iterated map, Lorenz map, Tinkerbell map, and Tent map. So, the map selection algorithm introduced in [13] is exploited in our proposed cryptosystem to find the best chaotic map based on the estimated entropy value which is the most important security property in any cryptography science. So, the motivation for choosing entropy value as the benchmark metric is that an efficient ciphering technique should get the information entropy lean to a value of 8 [30], and consequently, the pattern of video frame information is obscured in a safer direction. Thence, the choice of an appropriate map which eventually results in better information entropy value is very advantageous. After extensive tests, it has been proved and identified that the Arnold chaotic map is the most excellent chaotic map for cryptography compared to other types of chaotic maps. It achieves the best value of average information entropy of 7.96 compared to other tested chaotic maps. Therefore, our suggested HEVC cryptosystem utilizes it for the aid of secret key streams generation. This phase of chaotic secret key generation encompasses the following two steps (1 and 2).

Step (1): Generate the three secret key streams (K_1, K_2, and K_3) produced from the three chaotic sequences (S_1, S_2, and S_3) created via the employed Arnold chaotic map (Repeat the Arnold chaotic map t times and generate K_m through Eq. (2)).

$$K_m = Mod((S_m \times 10^{10}), 256) \quad (\text{for } m = 1, 2, \text{and } 3) \tag{2}$$

Step (2): Employ the DNA sequences encoding process on the obtained K_1, K_2, and K_3 using the function

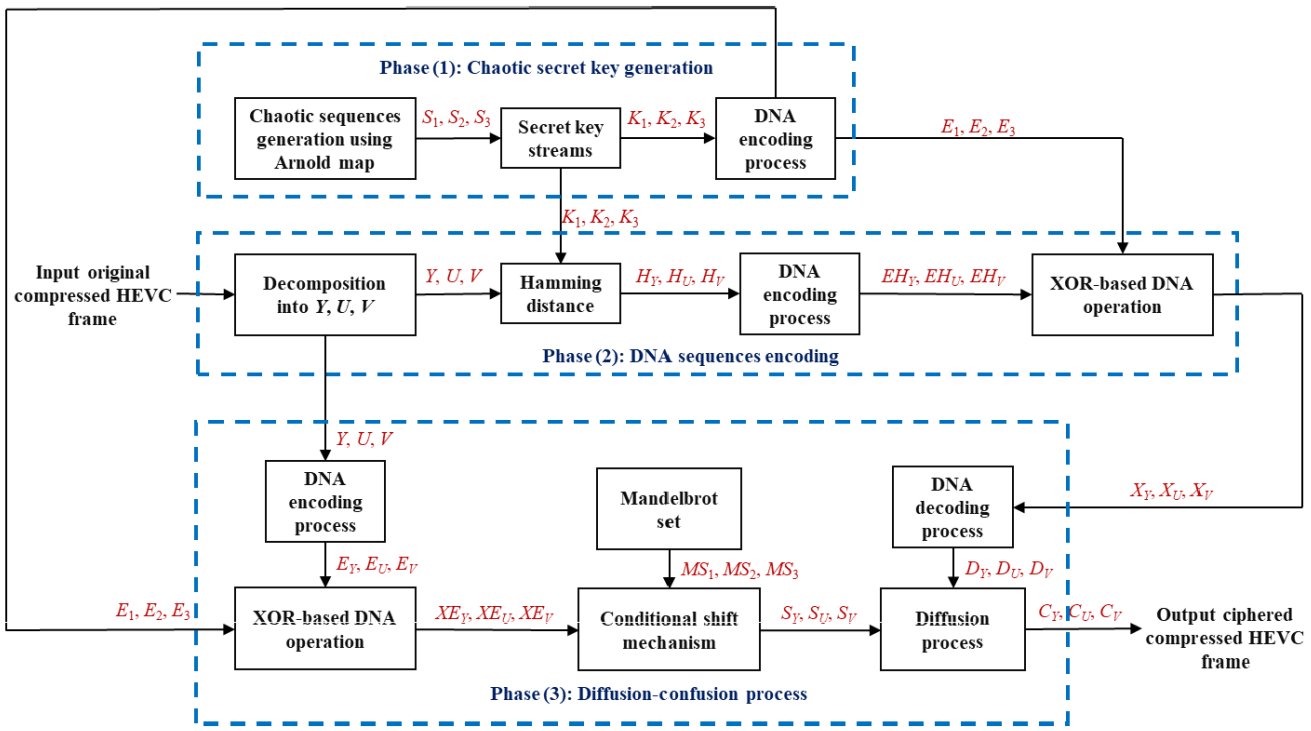


FIGURE 2. Structure diagram of the suggested hybrid HEVC cryptography procedure.

DNAEncode(·), to obtain the bases of the DNA sequences (E_1, E_2, and E_3) with a size of the same size of the input HEVC frame, as shown in Eq. (3).

$$E_i = DNAEncode(K_i) \tag{3}$$

where each one of K_i is transformed into its binary format before employing the DNA sequences encoding process (*DNAEncode*(·)).

B. PHASE (2): DNA SEQUENCES ENCODING

This phase consists of the subsequent four steps (3 to 6).

Step (3): Separate the three main Y, U, and V components of the input compressed HEVC frame.

Step (4): Estimate the value of Hamming distance between the generated key streams (K_i) and the three decomposed Y, U, and V matrices, as given in Eqs. (4) to (6).

$$H_Y(m,n) = HM(Y(m,n), K_1(m,n)) \tag{4}$$
$$H_U(m,n) = HM(U(m,n), K_2(m,n)) \tag{5}$$
$$H_V(m,n) = HM(V(m,n), K_3(m,n)) \tag{6}$$

where $HM(\cdot)$ refers to the hamming distance function which reverts the number of bits which are distinct at identical location in the inputs of this function.

The objective from the utilization of the estimation of the hamming distance between the generated key streams and the three decomposed Y, U, and V matrices of the video frame is to avoid the drawbacks that may be resulted from the employed Arnold map. It is known that the state resulted from the Arnold map may be periodic after a number of iterations. Therefore, the suggested cryptography procedure can survive this shortcoming in such a manner that the generated secret key streams are not employed immediately to the video frames. As an alternative, the estimation of hamming-distance amongst the generated secret key streams and video frame components is performed, followed by the DNA sequences encoding which can abolish this impact. Therefore, the step of hamming-distance estimation is established decisively due to the occurrence of periodic secret key streams produced from the employed Arnold map after several iterations.

Step (5): Employ the strategy of DNA encoding on the H_Y, H_U, and H_V to produce the matrices of DNA sequences: EH_Y, EH_U, and EH_V, as given in Eqs. (7) to (9).

$$EH_Y = DNAEncode(H_Y) \tag{7}$$
$$EH_U = DNAEncode(H_U) \tag{8}$$
$$EH_V = DNAEncode(H_V) \tag{9}$$

Step (6): Perform XOR function between generated DNA sequences of key streams given in (3) and the estimated matrices of encoded DNA sequences as given in (7) to (9).

$$X_Y = XOR(EH_Y, E_1) \tag{10}$$
$$X_U = XOR(EH_U, E_2) \tag{11}$$
$$X_V = XOR(EH_V, E_3) \tag{12}$$

C. PHASE (3): DIFFUSION-CONFUSION PROCESS

The actual ciphering process begins from this phase of the diffusion and confusion mechanisms. The objective of the confusion mechanism necessitates reordering or rearranging the values of the pixels without adjusting their values. While the objective of the diffusion mechanism aims to adjust the values of the pixels. Therefore, these two mechanisms are the two key steps tracked in every ciphering process. So, they are essential for suppressing the main information in the plain video frame from the aggressors. These two mechanisms can be accomplished in any way such that the plain video frame must be regained through the deciphering process. Thus, these two mechanisms have to be reversible as well. In the suggested cryptographic algorithm, a conditional shift mechanism described in Algorithm (2) is established to encounter the requirement of the confusing process and a Bit XOR process captures the responsibility of the diffusion process. The confusion and diffusion processes in this phase can be described as in step 7.

Step (7): Employ the confusion-diffusion process based on the following sub-steps, to produce the video frame components C_Y, C_U, and C_V that are concatenated to generate the final ciphered compressed HEVC frame. The main confusion-diffusion procedure steps are described as follows:

1. Obtain the estimated values of the encoded DNA sequences of the Y, U, and V components of the input compressed HEVC frame, as given in Eqs. (13) to (15).

$$E_Y = DNAEncode(Y) \tag{13}$$
$$E_U = DNAEncode(U) \tag{14}$$
$$E_V = DNAEncode(V) \tag{15}$$

2. Receive the encoded DNA sequences of the secret key streams as E_1, E_2, and E_3.
3. Employ the XOR-based DNA process between the encoded DNA sequences of the key streams and the encoded DNA sequences of the YUV components, as given in Eqs. (16) to (18).

$$XE_Y(m) = DNAXor(E_Y(m), E_1(m)) \tag{16}$$
$$XE_U(m) = DNAXor(E_U(m), E_2(m)) \tag{17}$$
$$XE_V(m) = DNAXor(E_V(m), E_3(m)) \tag{18}$$

4. Employ the proposed conditional shift mechanism as described in the steps of Algorithm (2), on the obtained XE_Y, XE_U, and XE_V to produce the keys of S_Y, S_U, and S_V.
5. Employ the DNA decoding process on the outcome delivered by the phase (2) of the DNA sequences encoding, as given in Eqs. (19) to (21).

$$D_Y = DNADecode(X_Y) \tag{19}$$
$$D_U = DNADecode(X_U) \tag{20}$$
$$D_V = DNADecode(X_V) \tag{21}$$

6. Execute the diffusion process based on the Bit XOR process to get the ciphered video frame components C_Y, C_U, and C_V that are merged to obtain the final ciphered compressed HEVC frame, as given in Eqs. (22) to (24).

$$C_Y(m) = (BitXor(S_Y(m), D_Y(m))) \bmod 256 \tag{22}$$
$$C_U(m) = (BitXor(S_U(m), D_U(m))) \bmod 256 \tag{23}$$
$$C_V(m) = (BitXor(S_V(m), D_V(m))) \bmod 256 \tag{24}$$

V. SIMULATION RESULTS AND SECURITY ANALYSIS

To entirely validate the benefits of the suggested HEVC cryptosystem, more standard video streams (Balloons, Bospharous, Dancer, Flamenco, Forest, Lovebird, Mobcal, Newspaper, PoznanHall, and Race) [52] that have different intensity values, resolutions, and spatial-temporal features are selected and tested. The reference HEVC Test Model (HM) codec [4] is firstly employed to encode the tested H.265 video streams to generate the compressed HEVC frames that will be considered as the input for the suggested HEVC cryptosystem. The samples of the tested video frames are exhibited in Figure 3. The implementation tests of the suggested HEVC cryptosystem are executed utilizing a laptop which has the subsequent hardware environment: 8 GB memory, Intel(R) Core(TM) i7-4500 CPU @ 1.80GHz and 2.40GHz, and Windows 10 execution system. The compiling Visual Studio 2019 and MATLAB R2019a software are employed for the performed experiments.

A. VISUAL ANALYSIS

More and comprehensive evaluations have been carried out for the purpose of security analysis of the suggested cryptosystem. The visual inspection is the first and main evaluation metric that is used to assess the ciphering/deciphering performance of the suggested HEVC cryptosystem. Figure 3 indicates the encryption-decryption results of the tested compressed HEVC frames. From the offered results, it is observed the great advantage of the suggested cryptosystem in disappearing and hiding the main details within the tested video frames, while the suggested cryptosystem can efficiently and successfully decrypt and recover the video frames with superior performance at the receiver side.

B. HISTOGRAM ANALYSIS

The distribution of the pixel strength rates of a video frame can be demonstrated by the histogram, it can also deliver certain statistical knowledge of the video frame. A protected and secure video cryptosystem can make the ciphered video frame has a histogram with a uniform distribution to withstand any type of statistical channel attacks [16]. Figure 4 indicates the histograms of the tested original, ciphered, and deciphered video frames. The original video frame distribution varies appreciably from the ciphered video frame distribution. Consequently, it is observed that our suggested HEVC cryptosystem has introduced a uniform pixel distribution on the ciphered video frame with obscuring the actual pattern of the tested video frames. Thus, it is noticed from the histograms that there are no patterns/sequences of any observable nature

Algorithm 2 The Steps of the Pseudocode of the Suggested Conditional Shift Algorithm

Input: the MS_1, MS_2, MS_3 and the XE_Y, XE_U, XE_V.
- suppose that M relates to the modified Mandelbrot set video frame matrix illustrated in Figure 1(b).

while $j = 1$ *to c,* ***do*** *// c signifies the overall columns number in M.*
- Estimate the maximum value of j^{th} row elements of XE_Y, XE_U, XE_V and signify them as max_{yj}, max_{uj}, and max_{vj}, respectively.
- Estimate the maximum value of j^{th} column elements of M and signifies it as max_j.
- Employ shifting operation as follows.

Case 1 do if $(max_j \leq max_{yj})$ ***then***
| j^{th} row elements of XE_Y are confused by employing left cyclic shift max_j times.
else
| j^{th} row elements of XE_Y are confused by employing right cyclic shift max_j times.
end if

Case 2 do if $(max_j \leq max_{uj})$ ***then***
| j^{th} row elements of XE_U are confused by employing left cyclic shift max_j times.
else
| j^{th} row elements of XE_U are confused by employing right cyclic shift max_j times.
end if

Case 3 do if $(max_j \leq max_{vj})$ ***then***
| j^{th} row elements of XE_V are confused by employing left cyclic shift max_j times.
else
| j^{th} row elements of XE_V are confused by employing right cyclic shift max_j times.
end if

end while

Output: the final shifted S_Y, S_U, S_V matrices equivalent to the XE_Y, XE_U, XE_V, respectively.

in the corresponding ciphered video frames. Moreover, it is clear that the histograms of the decrypted video frames are similar to the histograms of the original video frames, so the suggested cryptosystem can effectively and profitably recover the video frame histograms with better functionality. These histograms results corroborated the soundness of the suggested HEVC cryptosystem.

C. CORRELATION ANALYSIS

In each video frame, there are a certain amount of relationships are sustained amongst each pair of neighboring pixels. Excellent cryptography techniques are anticipated to prevent or conceal such relationships between pixels to defend the video content from various channel attacks [20]. To realize and investigate the relationships amongst the pairs of video frame pixels, it is required to choose specific adjoining pixels of the input video frame along with the three vertical (V), horizontal (H), and diagonal (D) directions. The pixel pairs correlation can be determined as given in Eq. (25).

$$r_{xy} = \frac{N^2.cov(x,y)}{\sum_{i=1}^{N}(x_i - E_x)^2.\sum_{i=1}^{N}(y_i - E_y)^2} \tag{25}$$

where $E_x = \frac{\sum_{i=1}^{N} x_i}{N}$ and $cov(x,y) = E((x - E_x)(y - E_y))$.
where the two sequences of neighboring pixels of the vertical, horizontal, or diagonal are denoted by (x, y), and N signifies the video frame size.

Figures from 5 to 14 illustrate the results of the vertical, horizontal, and diagonal correlation distributions of each pair neighboring pixels for the tested original video frames and their corresponding distributions of the ciphered frames. The related vertical, horizontal, and diagonal correlation coefficients values of the whole tested original, ciphered, and deciphered frames are presented in Table 3. It is apparent from Table 3 that all the three V, H, and D directions of correlation values among each adjacent pair pixels of the whole ciphered video frames are extremely low. Therefore, it is established that all structures of pattern in the ciphered video frames have been hidden that making them are indestructible by the intruders and attackers.

D. ENTROPY ANALYSIS

The entropy is a definition which is utilized to describe the intensity of a video frame or an image. So, it refers to the information or data amount which is concealed in a video frame utilizing any form of technique. The Shannon entropy defines a degree of unpredictability of a video frame [23]. Shannon entropy for an 8-bit video frame is determined as presented in Eq. (26).

$$H(m) = -\sum_{i=0}^{255} P(x_i) \times \log P(x_i) \tag{26}$$

where the i^{th} grey value in a video frame is given by x_i and the probability of x_i in a video frame is denoted by $P(x_i)$. A good cryptography technique should have an

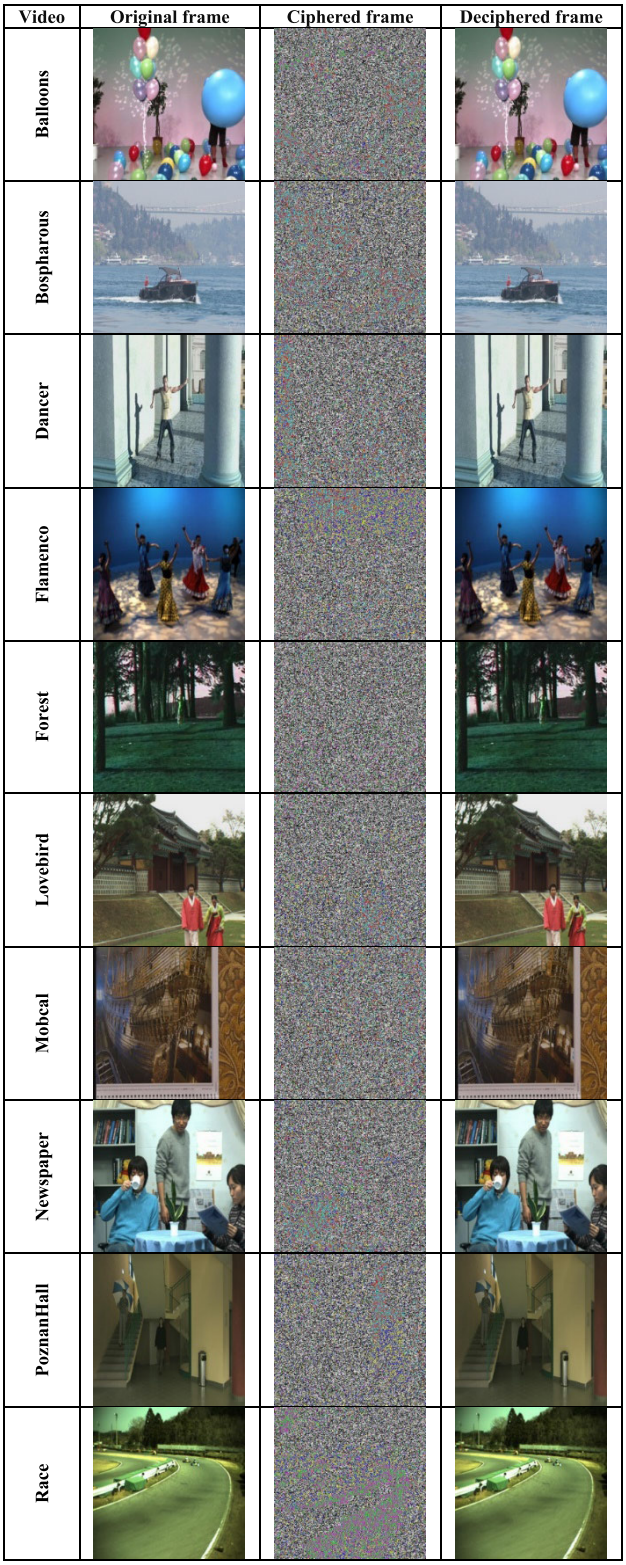


FIGURE 3. Subjective results of the original frames, ciphered frames, and deciphered frames of the tested compressed HEVC videos.

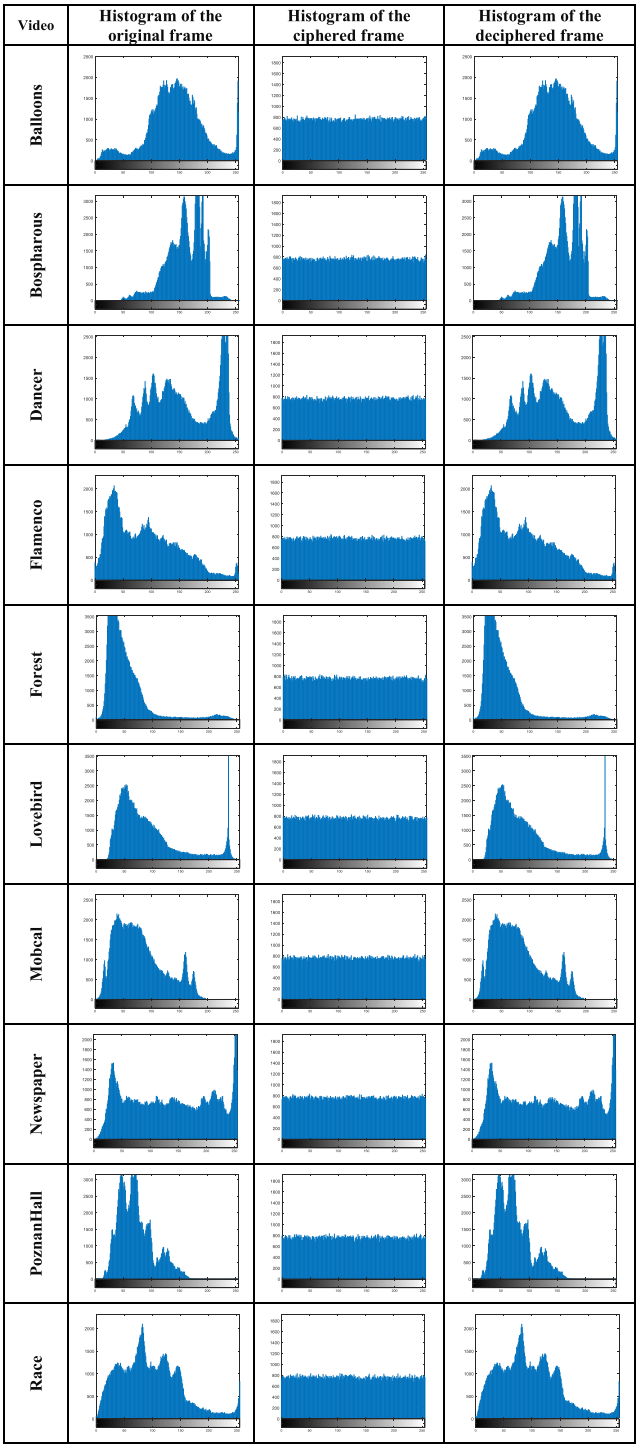
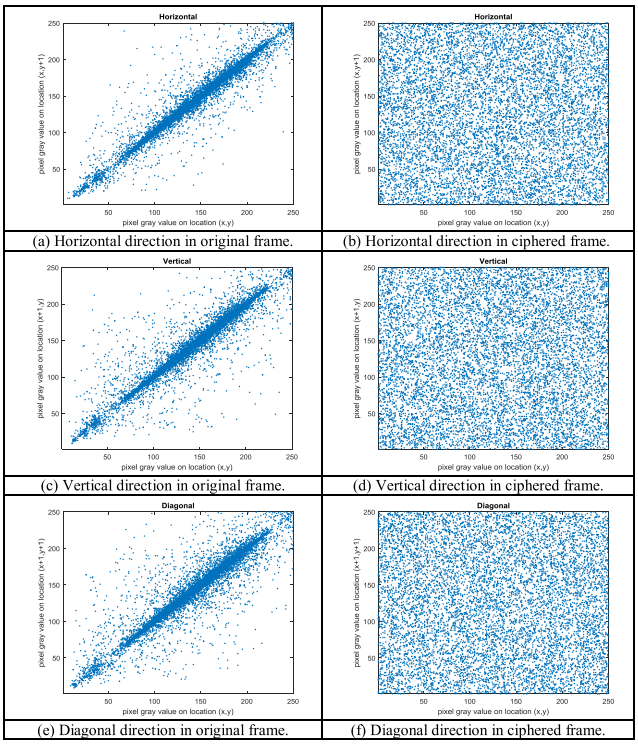


FIGURE 4. Histrogram results of the original frames, ciphered frames, and deciphered frames of the tested compressed HEVC videos.

estimated value of Shannon entropy close enough to 8. Table 4 presents the information entropies of the tested original, ciphered, and deciphered frames of the tested compressed HEVC sequences. It is observed that our HEVC cryptosystem provides the ultimate values of the Shannon entropy which characterizes ideal values for a variety of video frames with different features. This indicates that the information leakage in the ciphering may be overlooked. Subsequently, the suggested cryptosystem is robust and secure alongside entropy attacks.

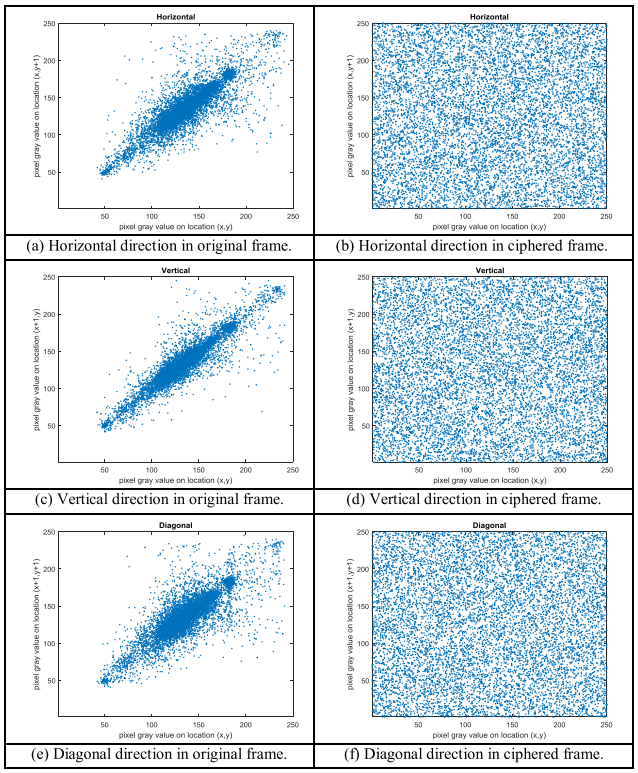
TABLE 3. Correlation coefficients of two adjacent pixels in the original, ciphered, and deciphered frames of the tested compressed HEVC sequences.

Video	Original frame			Ciphered frame			Deciphered frame		
	H	V	D	H	V	D	H	V	D
Balloons	0.9372	0.9635	0.9151	0.0184	-0.0357	0.0333	0.9372	0.9635	0.9151
Bospharous	0.9485	0.8769	0.8415	-0.0102	0.0263	-0.0012	0.9485	0.8769	0.8415
Dancer	0.9185	0.9820	0.8965	0.0144	0.0718	-0.0064	0.9185	0.9820	0.8965
Flamenco	0.9749	0.9825	0.9724	-0.0777	0.0158	-0.0087	0.9749	0.9825	0.9724
Forest	0.9147	0.9237	0.8731	0.0256	-0.0481	0.0080	0.9147	09237	0.8731
Lovebird	0.9605	0.9561	0.9472	0.0538	0.0624	-0.0430	0.9605	0.9561	0.9472
Mobcal	0.8818	0.9338	0.7879	-0.0277	0.0227	-0.0013	0.8818	0.9338	0.7879
Newspaper	0.9731	0.9698	0.9519	0.0608	-0.0191	-0.0473	0.9731	0.9698	0.9519
PoznanHall	0.9447	0.9876	0.9372	-0.0199	-0.0070	-0.0129	0.9447	0.9876	0.9372
Race	0.9721	0.9394	0.9079	0.0448	-0.0358	0.0295	0.9721	0.9394	0.9079



(a) Horizontal direction in original frame. (b) Horizontal direction in ciphered frame.
(c) Vertical direction in original frame. (d) Vertical direction in ciphered frame.
(e) Diagonal direction in original frame. (f) Diagonal direction in ciphered frame.

FIGURE 5. The horizontal, vertical, and diagonal correlation results of two adjacent pixels in the original and ciphered frames of the tested Balloons sequence.



(a) Horizontal direction in original frame. (b) Horizontal direction in ciphered frame.
(c) Vertical direction in original frame. (d) Vertical direction in ciphered frame.
(e) Diagonal direction in original frame. (f) Diagonal direction in ciphered frame.

FIGURE 6. The horizontal, vertical, and diagonal correlation results of two adjacent pixels in the original and ciphered frames of the tested Bospharous sequence.

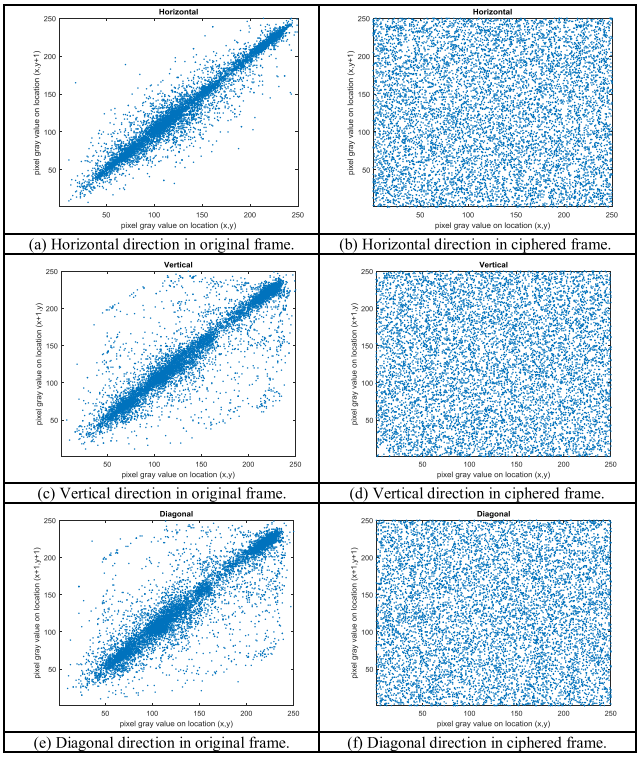
E. SSIM, FSIM, AND PSNR ANALYSIS

The SSIM (structural similarity) index, FSIM (feature similarity), and PSNR (Peak Signal-to-Noise Ratio) metrics are used to assess the quality performance of the ciphering and deciphering processes. In our simulation tests, we evaluated the SSIM, FSIM, and PSNR values between the original video frames and ciphered video frames that must be given with low values for the efficient ciphering process. Also, we estimated the SSIM, FSIM, and PSNR values between the original video frames and decrypted video frames, that must be given with high values for the efficient decrypting process.

The SSIM is a metric that is used for determining the relationship between two video frames. The video frame pixels have strong and great inter-dependencies particularly when they are spatially close together, this can be estimated and determined by the concept of structural information [12]. These inter-dependencies convey valuable information about the structure of the objects in the visual video frame. The decimal value of the SSIM index is between -1 and 1. The SSIM metric can be estimated as given in Eq. (27).

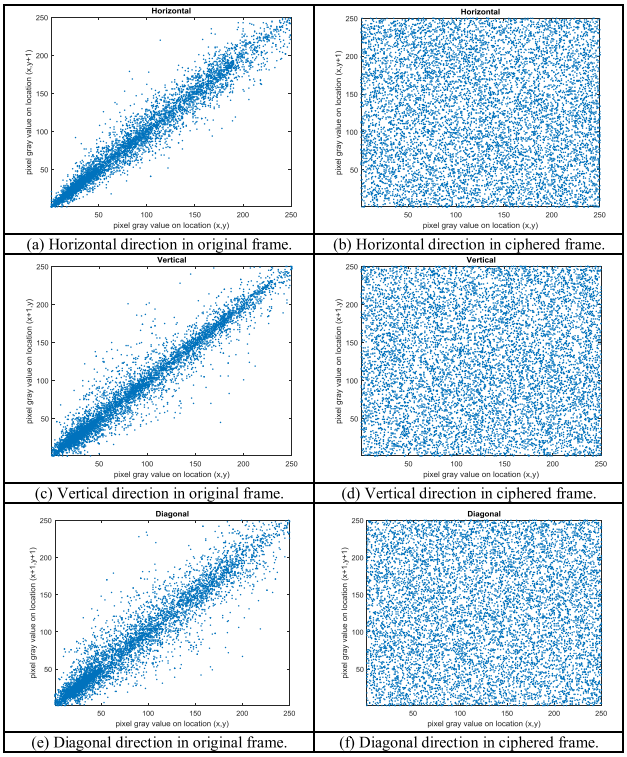
$$SSIM(x, y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)} \tag{27}$$

where μ_x and μ_y are the average values of x and y, respectively. σ_x^2 and σ_y^2 are the variance values of x and y, respectively. σ_{xy} is the covariance value of x and y.



(a) Horizontal direction in original frame. (b) Horizontal direction in ciphered frame.
(c) Vertical direction in original frame. (d) Vertical direction in ciphered frame.
(e) Diagonal direction in original frame. (f) Diagonal direction in ciphered frame.

FIGURE 7. The horizontal, vertical, and diagonal correlation results of two adjacent pixels in the original and ciphered frames of the tested Dancer sequence.



(a) Horizontal direction in original frame. (b) Horizontal direction in ciphered frame.
(c) Vertical direction in original frame. (d) Vertical direction in ciphered frame.
(e) Diagonal direction in original frame. (f) Diagonal direction in ciphered frame.

FIGURE 8. The horizontal, vertical, and diagonal correlation results of two adjacent pixels in the original and ciphered frames of the tested Flamenco sequence.

TABLE 4. Information entropies of the tested original, ciphered, and deciphered frames of the tested compressed HEVC sequences.

Video	Original frame	Ciphered frame	Deciphered frame
Balloons	7.4840	7.9991	7.4840
Bospharous	6.8658	7.99914	6.8658
Dancer	7.4728	7.9992	7.4728
Flamenco	7.6719	7.9990	7.6719
Forest	6.6811	7.99908	6.6811
Lovebird	7.0787	7.99917	7.0787
Mobcal	7.2652	7.99925	7.2652
Newspaper	7.8578	7.9996	7.8578
PoznanHall	6.8273	7.9989	6.8273
Race	7.6291	7.99905	7.6291

TABLE 5. The PSNR, SSIM, and FSIM results between the original and ciphered frames of the tested compressed HEVC sequences.

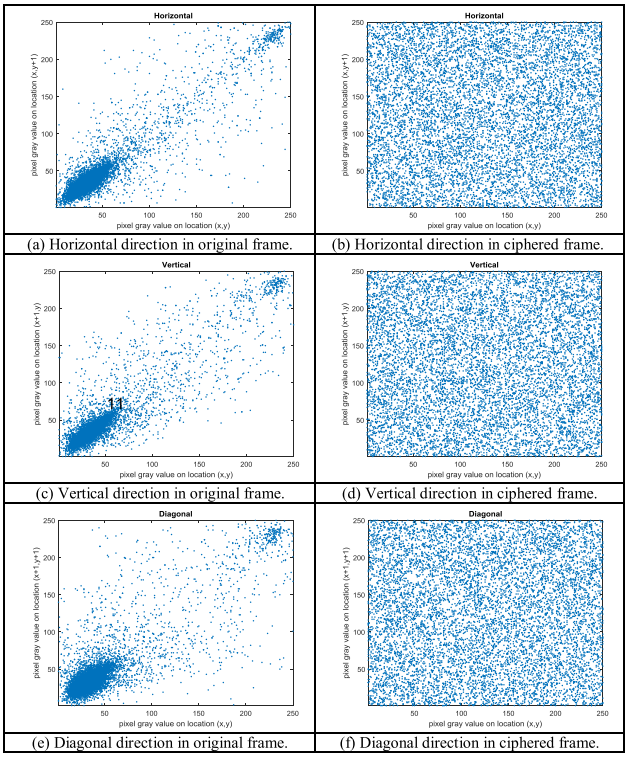
Video	PSNR (dB)	SSIM	FSIM
Balloons	9.0961	0.0031	0.3790
Bospharous	9.3885	0.0033	0.3826
Dancer	8.3470	0.0025	0.3350
Flamenco	8.0253	0.0043	0.3750
Forest	7.1476	0.0044	0.3680
Lovebird	8.0243	0.0046	0.4086
Mobcal	8.3462	0.0048	0.4203
Newspaper	7.7268	0.0044	0.3923
PoznanHall	8.4139	0.0035	0.2343
Race	8.4655	0.0048	0.3743

$C_1 = (K_1L)^2$ and $C_2 = (K_2L)^2$ are two constant variables that are used to alleviate the division process with a low denominator, where L is the pixel-values dynamic range. The value of K_1 and K_2 are ordinarily selected to be 0.01 and 0.03, respectively.

Table 5 illustrates the SSIM results between the original and ciphered frames of the tested videos. For a well-ciphering process, it is recommended to get lower values for the SSIM results between the original and ciphered frames. Table 6 demonstrates the SSIM results between the original and deciphered frames of the tested videos. For a well-deciphering process, it is recommended to get higher values for the SSIM results between the original and deciphered frames. It is observed from Tables 5 and 6 that the HEVC cryptosystem provides SSIM results that are near to the target and optimum values.

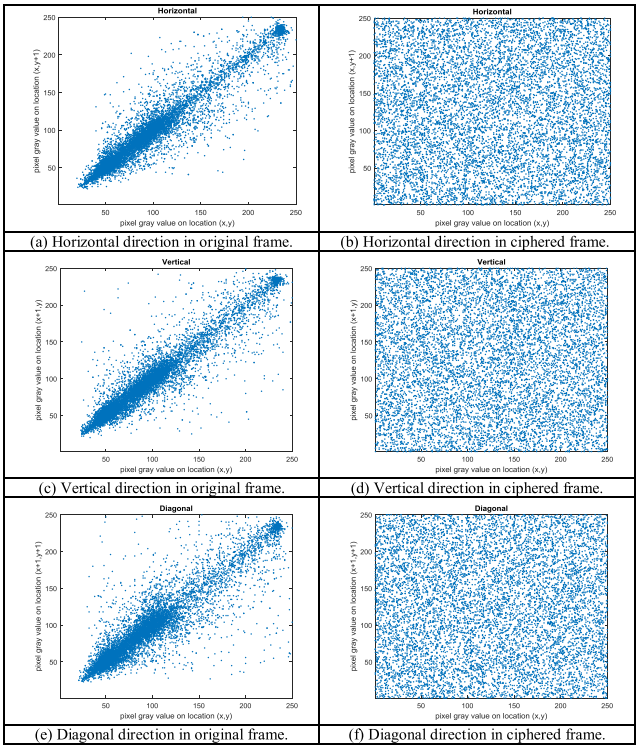
The FSIM is a metric that is utilized for examining the ciphering-deciphering proficiency of the suggested HEVC cryptosystem. It estimates the local similarity value amongst two different video frames. We tested this metric between the original and ciphered frames, and between the original and deciphered frames. The decimal value of the FSIM index is between -1 and 1. The FSIM metric can be estimated as given in Eq. (28).

$$FSIM = \frac{\sum_{x\in\Omega} S_L(x).PC_m(x)}{\sum_{x\in\Omega} PC_m(x)} \tag{28}$$



(a) Horizontal direction in original frame. (b) Horizontal direction in ciphered frame.
(c) Vertical direction in original frame. (d) Vertical direction in ciphered frame.
(e) Diagonal direction in original frame. (f) Diagonal direction in ciphered frame.

FIGURE 9. The horizontal, vertical, and diagonal correlation results of two adjacent pixels in the original and ciphered frames of the tested Forest sequence.



(a) Horizontal direction in original frame. (b) Horizontal direction in ciphered frame.
(c) Vertical direction in original frame. (d) Vertical direction in ciphered frame.
(e) Diagonal direction in original frame. (f) Diagonal direction in ciphered frame.

FIGURE 10. The horizontal, vertical, and diagonal correlation results of two adjacent pixels in the original and ciphered frames of the tested Lovebird sequence.

TABLE 6. The PSNR, SSIM, and FSIM results between the original and deciphered frames of the tested compressed HEVC sequences.

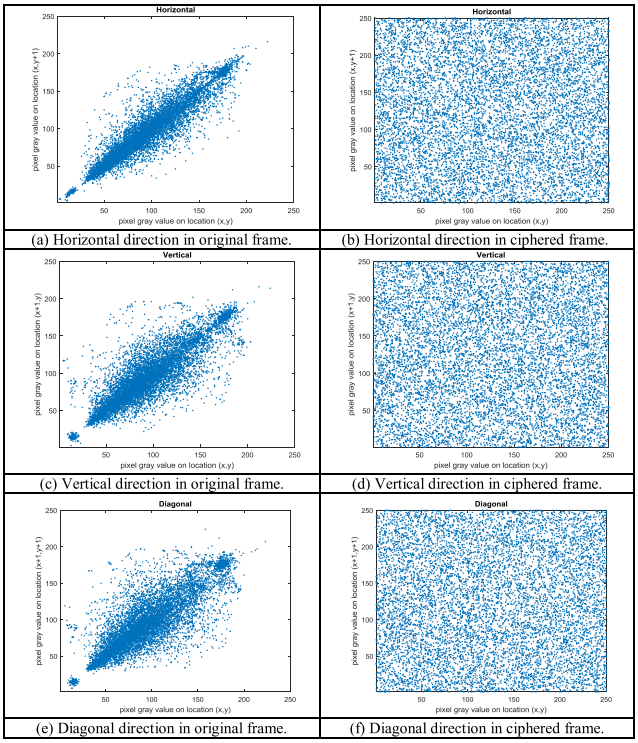
Video	PSNR (dB)	SSIM	FSIM
Balloons	Inf.	1	1
Bospharous	Inf.	1	1
Dancer	Inf.	1	1
Flamenco	Inf.	1	1
Forest	Inf.	1	1
Lovebird	Inf.	1	1
Mobcal	Inf.	1	1
Newspaper	Inf.	1	1
PoznanHall	Inf.	1	1
Race	Inf.	1	1

where Ω is the spatial domain of the video frame, $S_L(x)$ signifies to the overall anticipated similarity amongst two video frames, and $PC_m(x)$ refers to the expected value of phase congruency. Table 5 illustrates the FSIM results between the original and ciphered frames of the tested videos. For a well-ciphering process, it is recommended to get lower values for the FSIM results between the original and ciphered frames. Table 6 demonstrates the FSIM results between the original and deciphered frames of the tested videos. For a well-deciphering process, it is recommended to get higher values for the FSIM results between the original and deciphered frames. It is observed from Tables 5 and 6 that the HEVC cryptosystem provides FSIM results that are near to the target and optimum values.

The PSNR is another important metric that is utilized for analyzing the ciphering-deciphering performance of the suggested HEVC cryptosystem. The PSNR metric is estimated as the percentage between the highest possible signal power and the power of falsifying noise. Therefore, it is preferable to get higher values for the efficient deciphering process (between original and deciphered frames) and lower values for the efficient ciphering process (between original and ciphered frames) [17].

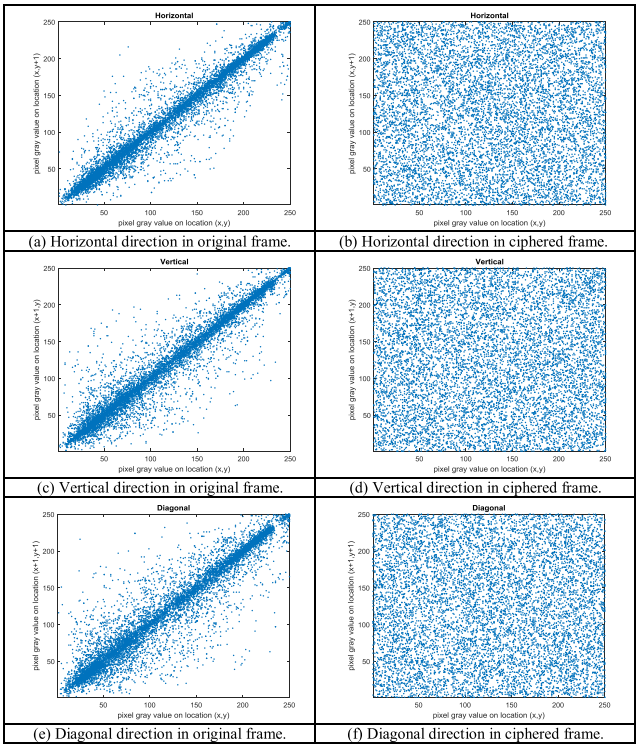
For a greyscale video frame, the PSNR metric is calculated as in Eq. (29). Due to a very broad dynamic range of many different signals, the PSNR is typically expressed in terms of the logarithmic decibel scale (dB). Table 5 illustrates the PSNR results between the original and ciphered frames of the tested videos. For a well-ciphering process, it is recommended to get lower values for the PSNR results between the original and ciphered frames. Table 6 demonstrates the PSNR results between the original and deciphered frames of the tested videos. For a well-deciphering process, it is recommended to get higher values for the PSNR results between the original and deciphered frames. It is observed from Tables 5 and 6 that the HEVC cryptosystem provides PSNR results that are near to the target and optimum values.

$$PSNR = 10 \log \frac{255 \times 255}{MSE} \tag{29}$$



(a) Horizontal direction in original frame. (b) Horizontal direction in ciphered frame.
(c) Vertical direction in original frame. (d) Vertical direction in ciphered frame.
(e) Diagonal direction in original frame. (f) Diagonal direction in ciphered frame.

FIGURE 11. Horizontal, vertical, and diagonal correlation results of two adjacent pixels in the original and ciphered frames of the tested Mobcal sequence.



(a) Horizontal direction in original frame. (b) Horizontal direction in ciphered frame.
(c) Vertical direction in original frame. (d) Vertical direction in ciphered frame.
(e) Diagonal direction in original frame. (f) Diagonal direction in ciphered frame.

FIGURE 12. The horizontal, vertical, and diagonal correlation results of two adjacent pixels in the original and ciphered frames of the tested Newspaper sequence.

where the *MSE* is the value of mean square error that is described as in Eq. (30).

$$MSE = \frac{1}{m \times n} \sum_{i=1}^{m} \sum_{j=1}^{n} [V_1(i,j) - V_2(i,j)]^2 \tag{30}$$

where $V_1(i, j)$ refers to the original video frame and $V_2(i, j)$ signifies to the corresponding ciphered or deciphered video frame.

F. DIFFERENTIAL ATTACK ANALYSIS

Occasionally, an adversary may attempt to produce a little variation in the original video frame which is utilized for ciphering and examine the variation in ciphering outcomes (that is, the cipher video frame of the plain frame and the cipher video frame of plan frame with a little variation). In this manner, the adversary follows the relationship amongst the plain video frame and the two ciphered video frames [44]. The differential cryptanalysis is a procedure that eases in deciphering a video frame. Therefore, it is evident that our HEVC cryptosystem should be anti-differential, which requires that it must be complicated for the aggressors to recognize how the original video frame is associated with the ciphered video frame. The NPCR (Number of Changing Pixel Rate) and UACI (Unified Averaged Changed Intensity) are the two main indicators utilized for this aim. These evaluation indicators are well-defined as in Eqs. (31) and (32).

$$NPCR(C_1, C_2) = \frac{\sum_{i=1}^{m} \sum_{j=1}^{n} D(i,j)}{m \times n} \times 100 \tag{31}$$

$$UACI(C_1, C_2) = \frac{1}{255 \times m \times n} \left[\sum_{i=1}^{m} \sum_{j=1}^{n} [C_1(i,j) - C_2(i,j)] \right] \times 100 \tag{32}$$

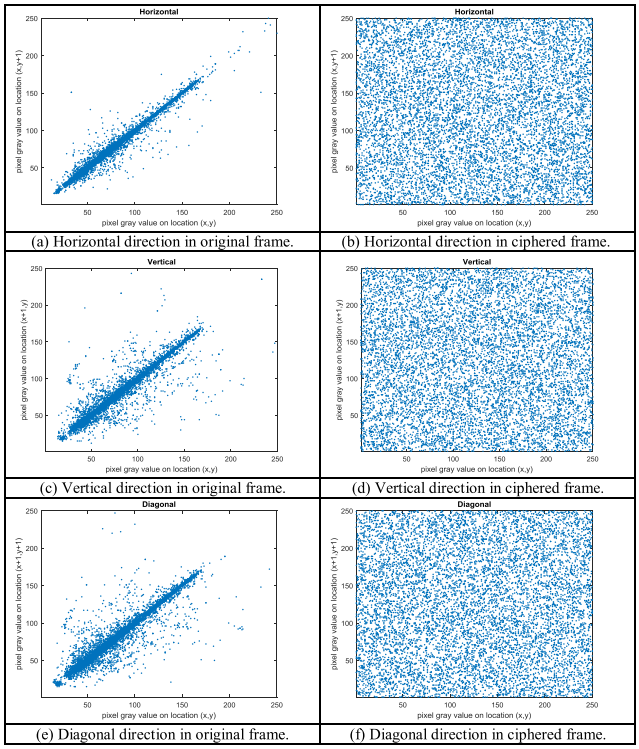
where $C_1(i, j)$ and $C_2(i, j)$ are the two encrypted video frames equivalent to the original video frame before and after a little adjustment, respectively. The m and n values refer to the video frame size (width and height). $D(i, j) = 1$, if $C_1(i, j) \neq C_2(i, j)$, and $D(i, j) = 0$, if $C_1(i, j) = C_2(i, j)$.

The proven estimated values of the UACI and NPCR metrics are approximately 0.33 and 0.996, respectively [9]. By obtaining these optimum values, it will be indicated that the ciphering process is highly vulnerable to the input video frame, and hence the suggested cryptosystem will survive the differential channel attack to a significant amount. Table 7 demonstrates the UACI and NPCR outcomes of the tested video frames. It is remarked that all obtained values are exceedingly close to the theoretical ideal values.

G. CIPHERING QUALITY ANALYSIS

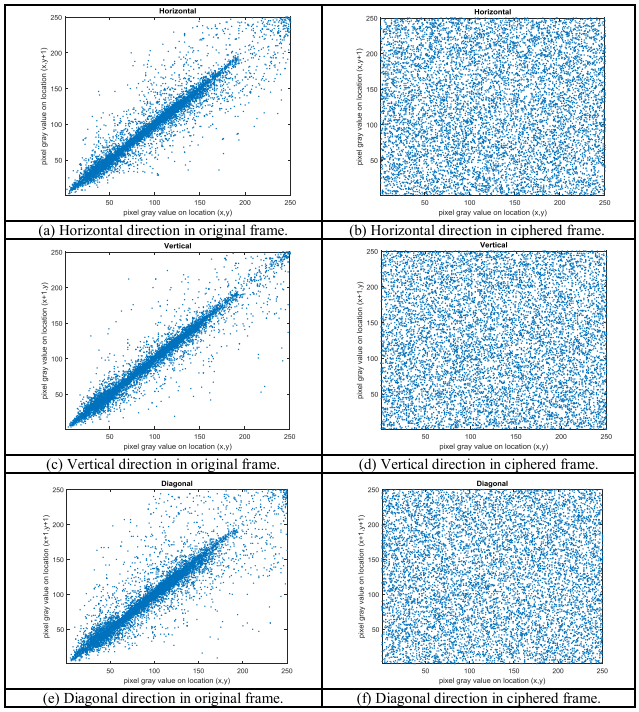
1) HISTOGRAM DEVIATION (D_H)

The maximum quantity of deviation amongst the histograms of the original and ciphered video frames [53] can be



(a) Horizontal direction in original frame. (b) Horizontal direction in ciphered frame.
(c) Vertical direction in original frame. (d) Vertical direction in ciphered frame.
(e) Diagonal direction in original frame. (f) Diagonal direction in ciphered frame.

FIGURE 13. The horizontal, vertical, and diagonal correlation results of two adjacent pixels in the original and ciphered frames of the tested PoznanHall sequence.



(a) Horizontal direction in original frame. (b) Horizontal direction in ciphered frame.
(c) Vertical direction in original frame. (d) Vertical direction in ciphered frame.
(e) Diagonal direction in original frame. (f) Diagonal direction in ciphered frame.

FIGURE 14. The horizontal, vertical, and diagonal correlation results of two adjacent pixels in the original and ciphered frames of the tested Race sequence.

estimated by utilizing the metric of histogram deviation to appraise the ciphering quality performance of the suggested HEVC cryptosystem. This metric can be estimated

TABLE 7. The NPCR and UACI results of the tested compressed HEVC sequences.

Video	NPCR	UACI
Balloons	0.99609	0.336935
Bospharous	0.99617	0.338132
Dancer	0.99621	0.335638
Flamenco	0.99641	0.334613
Forest	0.99685	0.339197
Lovebird	0.99628	0.334120
Mobcal	0.99608	0.332606
Newspaper	0.99627	0.335141
PoznanHall	0.99631	0.330626
Race	0.99686	0.338957

TABLE 8. The histogram and irregular deviations results of the ciphered frames of the tested compressed HEVC sequences.

Video	Histogram Deviation (H_D)	Irregular Deviation (D_I)
Balloons	2.28641	0.006958
Bospharous	3.24257	0.007476
Dancer	2.95392	0.005981
Flamenco	2.58000	0.005157
Forest	3.57416	0.007446
Lovebird	2.69461	0.006958
Mobcal	2.39603	0.006225
Newspaper	2.72638	0.004211
PoznanHall	3.18804	0.006988
Race	2.82735	0.006744

as in Eq. (33). It is observed that the outcomes of the D_H values are low as shown in Table 8. Consequently, the original and ciphered video frames are uncorrelated which proves the high-quality performance of the suggested HEVC cryptosystem.

$$D_H = \frac{(\frac{d_0+d_{255}}{2} + \sum_{i=1}^{254} d_i)}{m \times n} \tag{33}$$

where d_i is the amplitude of the absolute difference at the gray level i. The m and n values refer to the video frame size (width and height).

2) IRREGULAR DEVIATION (D_I)

The maximum quantity of irregular deviation caused in the ciphered video frame from the ciphering procedure on the plain video frame [53] can be estimated by utilizing the metric of irregular deviation to appraise the ciphering quality performance of the suggested HEVC cryptosystem. This metric can be calculated as in Eq. (34). The outcomes of D_I values are introduced in Table 8. It is observed that the outcomes of the D_I values are low. As a result, the original and ciphered video frames are uncorrelated which proves the high-quality performance of the suggested HEVC cryptosystem.

$$D_I = \frac{\sum_{i=0}^{255} |H(i) - M_H|}{m \times n} \tag{34}$$

where H is the histogram of the difference resulted from video frame, m and n values refer to the video frame size (width and height), and M_H is the value of the histogram.

H. KEY SPACE AND SENSITIVITY ANALYSIS

1) KEY SPACE ANALYSIS

To withstand the critical brute force attack, it is recommended that the employed cryptography technique must have a secret key with a large space [13]. Therefore, the keyspace should be large enough to build a robust and secure cryptosystem. To prevent the brute-force attacks of the transmitted video frames, the keyspace should have at least a value of 2^{100}. In our HEVC cryptosystem, different initial values of the employed Arnold map and hamming distance matrix are utilized to obtain the secret keys. For the Arnold map, the initials values of X_0 and Y_0 are utilized to produce secret sequences of each Y, U, and V channels with allowed values: [0, 1] with an iteration value of t. For the hamming distance matrix for each Y, U, and V channels: H_Y, H_U, H_V, it is assumed that each one of this matrix of hamming distance has a size of 256×256 for the input video frame with a size of 256×256.

Therefore, the number of various values feasible for each initial value of X_0 and Y_0 is around $(2 \times 10^{15})^3$, and the equivalent for the iteration counter t is supposed to be10^2. Also, each generated matrix has a total number of elements equals 65,536, where each element position with the matric can have possible various values of 256 (0–255). Thus, the total number of possible various values for the three H_Y, H_U, H_V matrices is about $256^{(65,536\times3)}$. Therefore, the final value of keyspace is about $(256)^{(65,536\times3)} \times 10^2 \times (2 \times 10^{15})^3$, which is decidedly larger than 2^{100}, this confirms that the suggested HEVC cryptosystem will be greatly robust against brute-force channel attacks.

2) KEY SENSITIVITY ANALYSIS

The ciphering algorithm should be susceptible to the preliminary and constraint values of the employed chaotic map [17]. So, the cryptosystem must generate distinct output result for a minor variation in the secret keys. Thus, to demonstrate that if there is any small alteration in the input main boundaries and control values, it will create a considerable modification at the output, and subsequently, the original video frame persists unrecoverable and the ciphered video frames cannot be deciphered accurately. Figure 15 illustrates the investigation of key sensitivity analysis for the tested video frames. Consequently, for examining the key sensitivity execution of the suggested HEVC cryptosystem, the ciphered video frames, deciphered video frames, and their histogram representations are exhibited in Figure 15 for all tested video frames at right and wrong values of secret keys. After utilizing ciphering on the test video frames with the right keys (*keyset*1) with $X_0 = 0.105795019$, $Y_0 = 0.2685999$, we marginally modify one of the preliminary control values of the employed Arnold map (the X_0 value is adjusted to be equals $X_0 = 0.105795020$) to form a *keyset*2, and then we tried to decipher the video frames with the altered *keyset*2.

From the findings, it is observed the extreme key sensitivity efficiency of the suggested cryptosystem in the case of a minor adjustment in the secret keyset values. It is indicated that the deciphered frames acquired with the modified keys (*keyset*2) are fairly distinct, not the actual video frame delivered though a tiny alteration is employed to secret keys. This proves that our suggested cryptosystem has wonderful sensitivity to the secret keys and thus averting it from numerous channel attacks.

I. EDGES DETECTION ANALYSIS

The suggested HEVC cryptosystem must guarantee the protection of the edge's information in the transmitted video frames from the channel attacks. Consequently, the visual misrepresentation for the ciphered video frames exploiting the suggested HEVC cryptosystem can be quantified by the distortion offered at video frames edges. The metric of EDR (Edge Differential Ratio) is utilized to estimate the edge distortion, it is formulated as in Eq. (35) [24].

$$EDR = \frac{\sum_{i,j=1}^{K} \left| P(i,j) - \overline{P}(i,j) \right|}{\sum_{i,j=1}^{K} \left| P(i,j) + \overline{P}(i,j) \right|} \tag{35}$$

where the pixel value in the detected edges inside the binary form of the original video frame can be estimated by $P(i,j)$, and the related pixel value in the binary detected edges in the ciphered video frame can be calculated by $\overline{P}(i,j)$. Table 9 exposes that the EDR outcomes amongst the ciphered and plain video frames are close to 1 that guarantees that the ciphered and plain video frames are extremely dissimilar. Figure 16 offers the visual Laplacian description of Gaussian binary edge detection for the original, ciphered, and deciphered video frames. From the offered results, it is observed that there is a great difference in edges between original and ciphered frames. This proves the wonderful advantage of the suggested cryptosystem in disappearing and hiding the main details within the tested video frames, while it can efficiently restore the video frames with superior performance.

TABLE 9. The EDR values of the ciphered frames of the tested compressed HEVC sequences.

Video	EDR
Balloons	0.89905
Bospharous	0.87453
Dancer	0.89982
Flamenco	0.88151
Forest	090418
Lovebird	0.88665
Mobcal	0.85124
Newspaper	0.88944
PoznanHall	0.90556
Race	0.90380

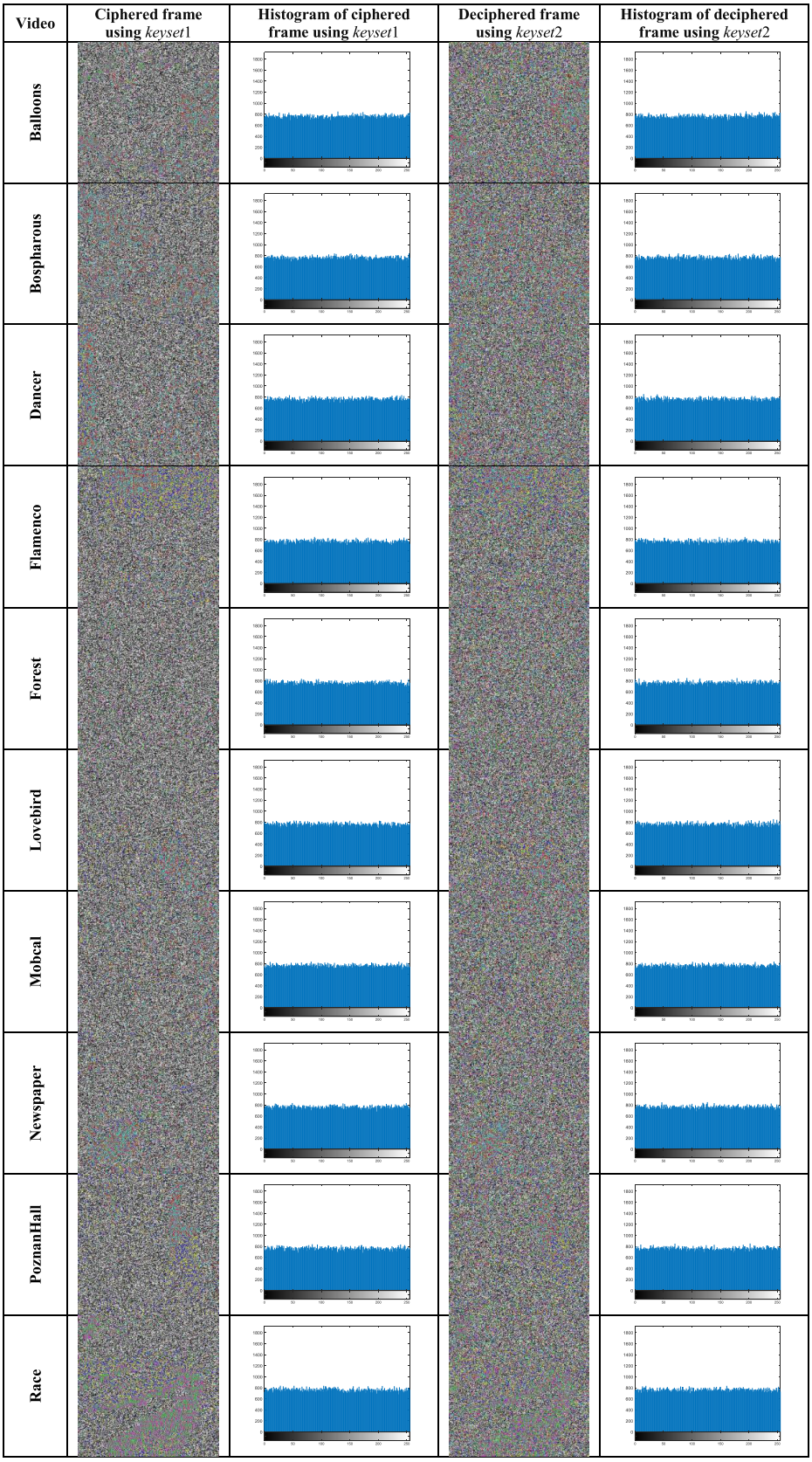


FIGURE 15. Key sensitivity analysis results for the tested compressed HEVC videos.

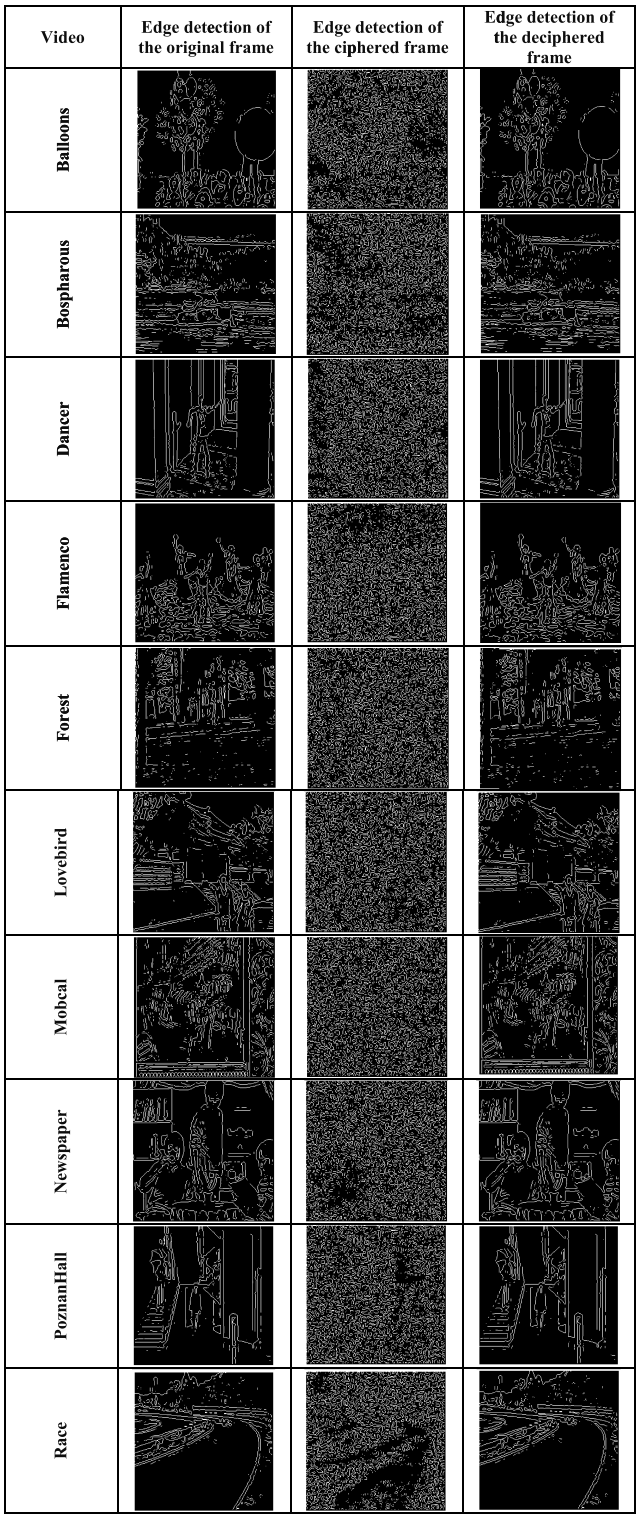


FIGURE 16. Laplacian of Gaussian edge detection results of the original, ciphered, and deciphered frames of the tested compressed HEVC videos.

J. CHANNEL NOISES ATTACK ANALYSIS

In this section, we investigate how the suggested ciphering-deciphering procedures perform with channel noises. The communication medium continually comprises several kinds of noise. Throughout communication, the video frame in the ciphered form will firmly be seriously influenced by these channel noises. Therefore, our deciphering procedure must be able to survive the channel noise in such a manner that the deciphered video frames should be comprehensible or in a human-understandable shape even if they are infected with channel noise during video streaming. Thus, we must verify that the suggested cryptosystem is effective enough to produce the identifiable and noticeable video frame from the ciphered video frame comprising channel noise. Different types of channel noises (Gaussian, Poisson, Salt and Pepper, and speckle) are considered in our analysis.

1) GAUSSIAN NOISE ANALYSIS

In digital images and videos, Gaussian noise mainly results during the acquisition process. The utilized sensor in the imaging system has an ingrained noise as a consequence of the illumination level and its specific temperature. Also, there is another source of electronic circuit noise injected to the sensor which is coming from the electronic circuits associated with the imaging sensor [14]. A conventional model of image or video frame noise is independent, additive, and gaussian at each value of pixels, and it is independent of the intensity of the signal. Figure 17 presents the results of ciphered and deciphered frames of the Gaussian noise analysis for all tested video frames affected with Gaussian noise has a zero mean and different variance values of 0.001, 0.003, and 0.005. It is observed that the deciphered video frames are identifiable and detectable even if the related ciphered video frames are influenced by different patterns of Gaussian noises. So, the suggested cryptosystem has a terrific benefit in resisting the effect of Gaussian noise attack.

2) SHOT/POISSON NOISE ANALYSIS

The Poisson noise typically results from the statistical quantum oscillations of the imaging sensor, its effect appears in the darker sections of a video frame or an image. This noise is considered as a change in the number of sensed photons at a certain exposure level [42], so it may be named as a shot photon noise. It has a value of root mean square which is proportional to the square root of the intensity of the video frame, and the number of noises at distinct pixels are independent of each other. So, the distribution of the shot noise is considered a Poisson distribution. Figure 18 presents the results of ciphered and deciphered frames of the Poisson noise analysis for all tested video frames affected by Poisson noise. It is clearly noticed that the deciphered video frames are detectable and identifiable even if the related ciphered video frames are influenced by Poisson noise. This proves the great advantage of the suggested cryptosystem in withstanding the effect of the Poisson noise attack.

3) SALT AND PEPPER NOISE ANALYSIS

The Salt-and-Pepper noise has different names of Fat-tail distributed noise, or impulsive noise, or spike noise [47]. The effect of salt-and-pepper noise on the digital image or video frame results in bright pixels in dark areas and dark

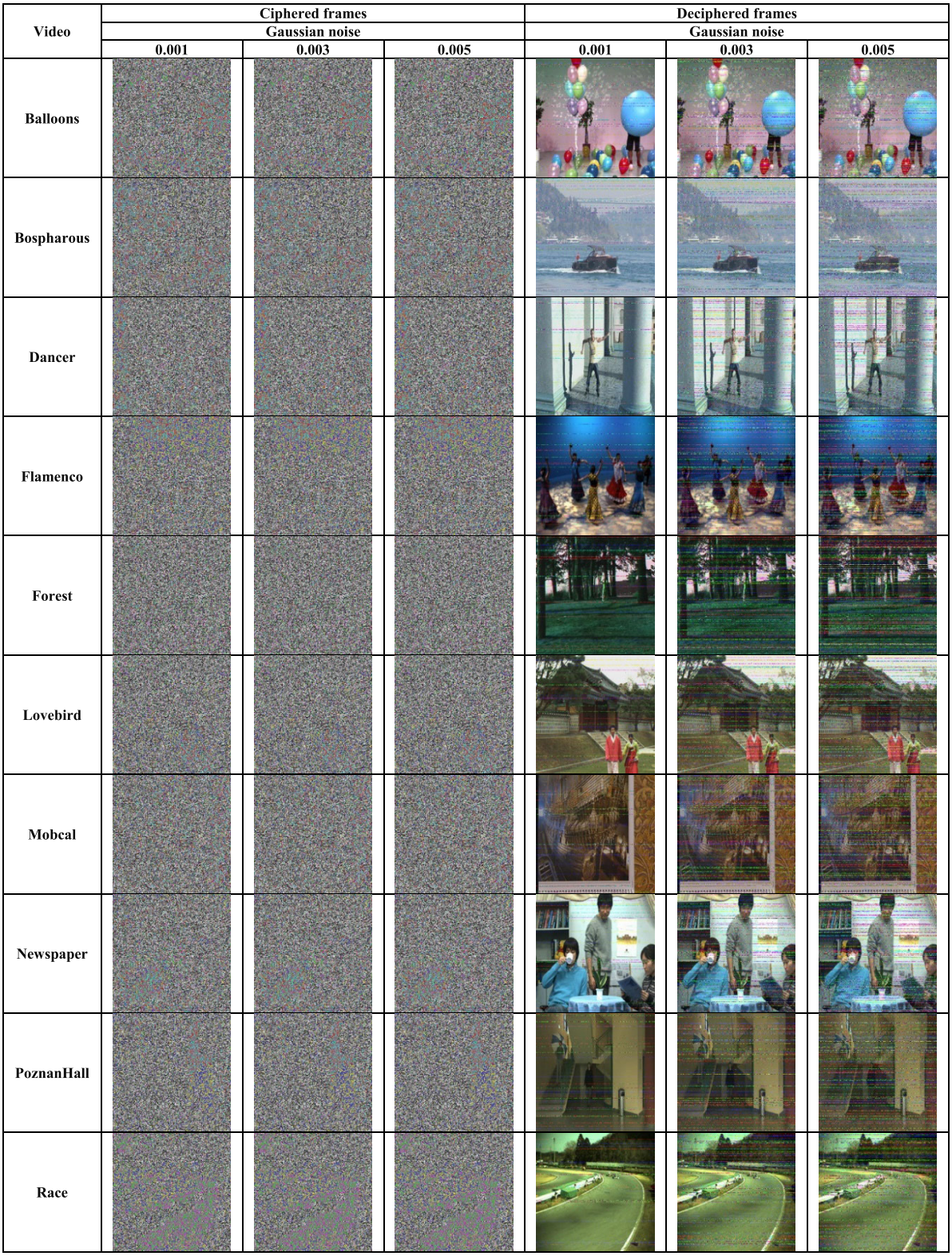


FIGURE 17. The ciphered and deciphered video frames in the existence of Gaussian noise with various noise variances on the ciphered frames of the tested compressed HEVC sequences.

pixels in bright areas. This kind of noise may be produced by bit errors in transmission, errors from analog-to-digital conversion, etc. It can be mainly reduced by utilizing median filtering, dark frame subtraction, interpolation of bright and

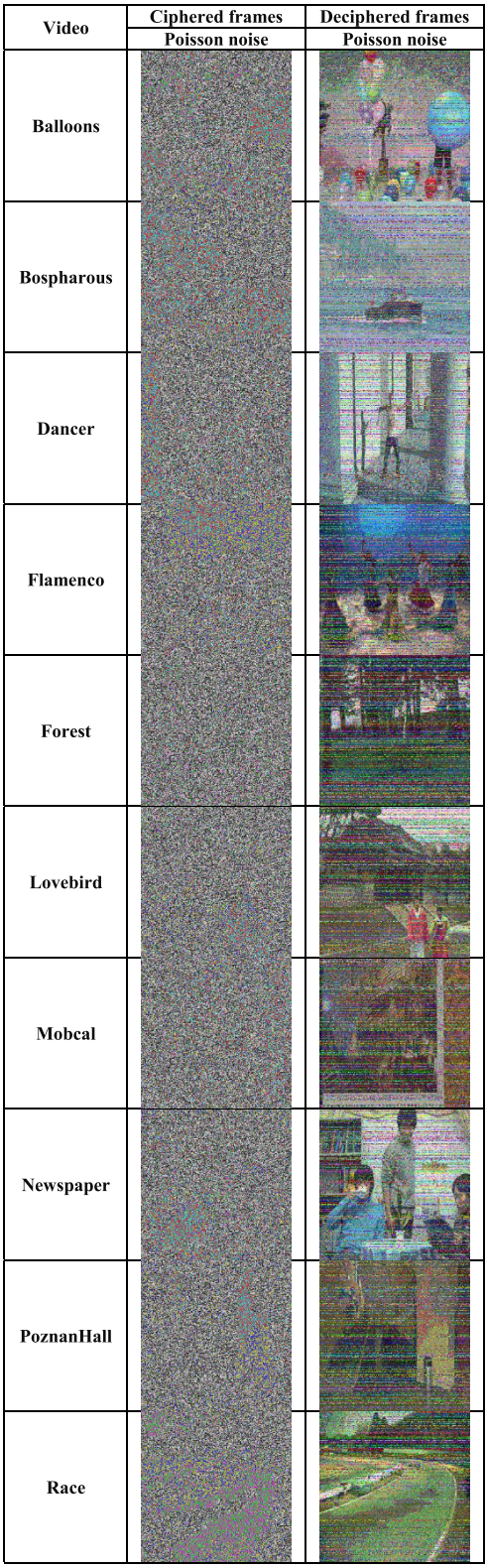


FIGURE 18. The ciphered and deciphered frames in the existence of Poisson noise on the ciphered frames of the tested compressed HEVC sequences.

dark pixels, and a hybrid of median and mean filtering. Figure 19 introduces the outcomes of ciphered and deciphered frames of the Salt and Pepper noise analysis for all tested video frames affected with Salt and Pepper noise at different variance values of 0.001, 0.003, and 0.005. It is noticed that the deciphered video frames are discernible and demonstrable even if the associated ciphered video frames are influenced by various patterns of Salt and Pepper noises. Consequently, the suggested cryptosystem has a tremendous advantage in combating the impact of Salt and Pepper noise attack.

4) SPECKLE NOISE ANALYSIS

The speckle noise emanates from the models of destructive and constructive interference exhibited as dark and bright dots in the video frame [22]. Figure 20 demonstrates the results of ciphered and deciphered frames of the speckle noise analysis for all tested video frames affected with speckle noise at different variance values of 0.001, 0.003, and 0.005. It is observed that the deciphered video frames are noticeable and discernable even if the concomitant ciphered video frames are affected by numerous patterns of speckle noises. So, the suggested cryptosystem has an immense gain in lessening the influence of speckle noise attack.

K. OCCLUSION ATTACK ANALYSIS

During the transmission and streaming of video sequences through the Internet and communication networks, some video frames may be dropped as a result of malicious destruction or congestion in the network [6]. In this section, the occlusion attack analysis is investigated to assess the capability of recovering original video frames from ciphered video frames in the case of some portion of it has been occluded or lost. The results of the occlusion attack analysis of all tested video frames are displayed in Figure 21. It is observed that the video frames can be deciphered in a comprehensible or plausible manner even if certain pieces of ciphered video frames are lost in different regions during the video streaming. This proves the capability of our suggested HEVC cryptosystem for resisting the probable occurrence of occlusion attack.

L. COMPUTATIONAL PROCESSING ANALYSIS

A good cryptography technique is anticipated to have a rapid execution speed to achieve lower computations of processing. Different video frames with various sizes have been utilized as examples to evaluate the ciphering/deciphering running time of the suggested HEVC cryptosystem. Our implementation testes have been carried out on a personal laptop with 8 GB RAM, 1TB hard drive, and Intel(R) Core(TM) i7-4500 CPU @ 1.80GHz and 2.40GHz. The execution system is Microsoft Windows 10, while the computational platform is MATLAB R2019a. The results of the average ciphering/deciphering time taken by the suggested cryptosystem algorithm for processing the tested video frames are presented in Table 10. It is observed that these achieved running speeds are acceptable by considering its tremendous level of privacy and security for video streaming in IoT multimedia applications.

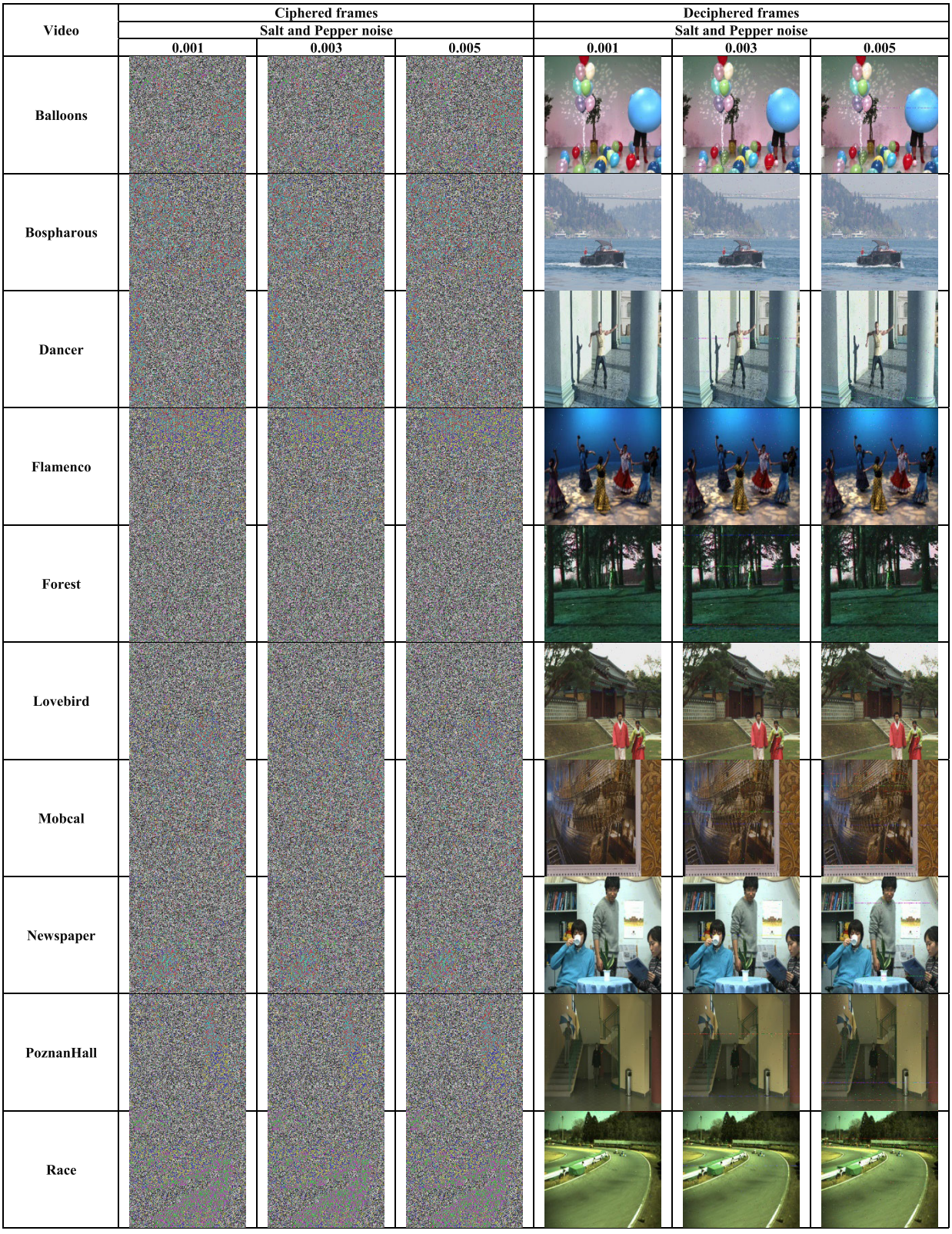


FIGURE 19. The ciphered and deciphered frames in the existence of Salt and Pepper noise with various noise variances on the ciphered frames of the tested compressed HEVC sequences.

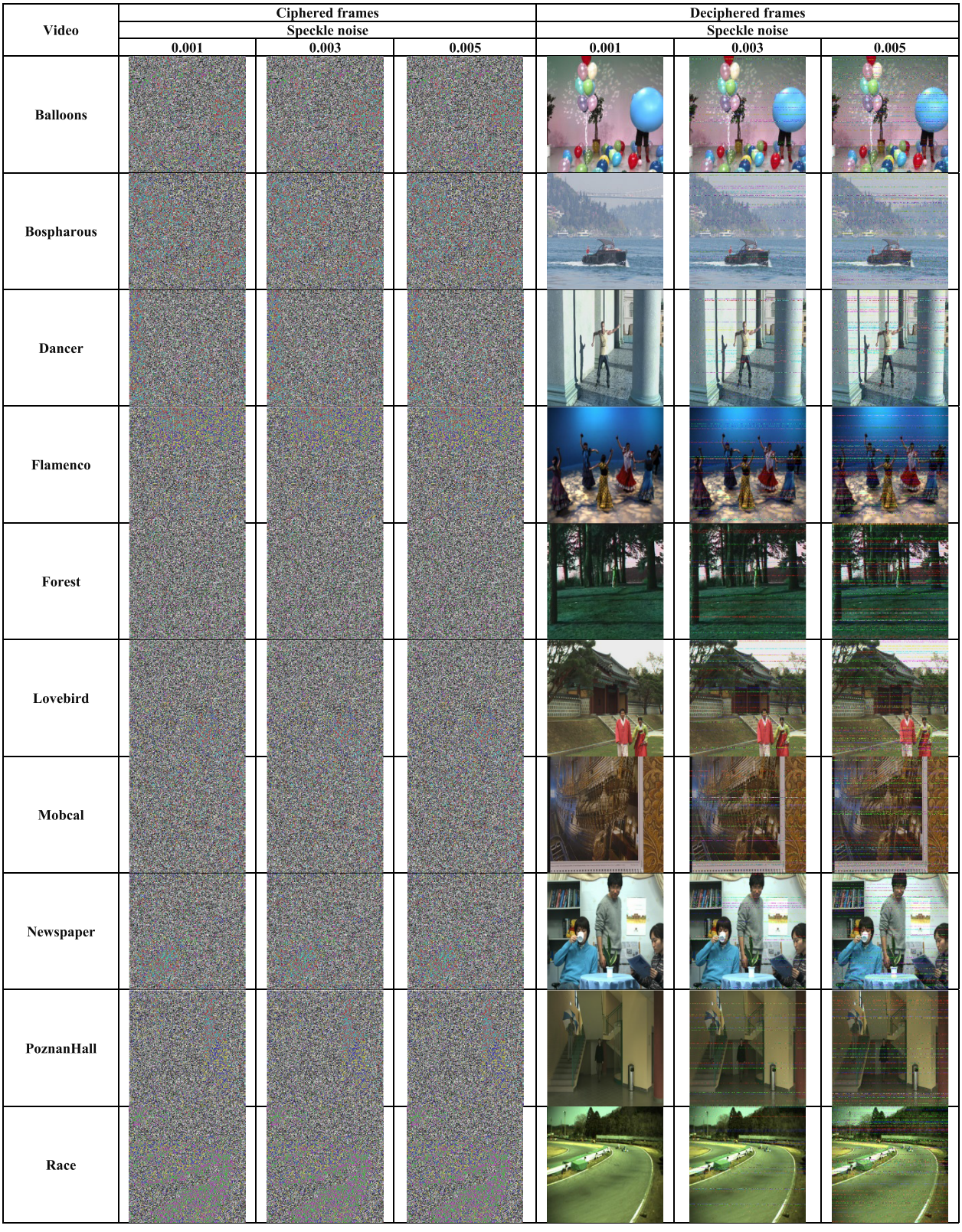


FIGURE 20. The ciphered and deciphered frames in the existence of Speckle noise with various noise variances on the ciphered frames of the tested compressed HEVC sequences.

TABLE 10. The average computational processing time values of the tested compressed HEVC sequences.

Video	Time (sec)
Balloons	5.83
Bospharous	5.23
Dancer	6.04
Flamenco	5.49
Forest	5.68
Lovebird	6.57
Mobcal	5.93
Newspaper	5.87
PoznanHall	6.13
Race	4.98

M. DISCUSSION OF CLASSICAL CATEGORIES OF ATTACKS ANALYSIS

It is known that every designed ciphering-deciphering system will be released publicly and accessible at the end. Therefore, under the public domain, the attackers might be able to investigate the designed cryptosystem steps as they are accessible, except the secret keys distributed amongst the transmitter and receiver side to execute the ciphering or deciphering process. It is recognized that there are four conventional categories of multimedia attacks: known-plaintext, chosen-ciphertext, chosen-plaintext, and ciphertext only. It is definitely apparent that the chosen-plaintext attack is the extremely horrible or crucial attack as the attacker someway has attained provisional access to the setting of the ciphering and deciphering procedures, thus in this case, the attacker might be able to create the equivalent ciphertext for a chosen-plaintext. If our HEVC cryptosystem has the ability to beat the chosen plaintext attacks, it will be surely and defeat and avoid the remaining three categories of attacks.

It is definitely proved in sections (H.1 and H.2) that our suggested HEVC cryptosystem is highly sensitive to the constant values (or control parameters) and the preliminary values utilized with the employed Arnold map. Also, the suggested cryptosystem is sensitive to the constant initial values utilized with the employed Mandelbrot set. There is a most important step in the ciphering process in our cryptosystem which is the calculation of the Hamming distance step, which determines the hamming distance value amongst the plain video frame components and the corresponding secret key sequences. Consequently, the step of hamming distance matrix calculation plays the main role in the advance processing of our HEVC cryptosystem. Therefore, our suggested cryptosystem not simply depends on the employed secret keys but as well on the original video frame. The key-value of the iteration count t can be set to various random values for each input plain video frame. Hence, there are entirely different generated outputs from the utilized Arnold cat map when it changes the value of the iteration count. Thus, if we definitively presume that even the adversary is capable to acquire some patterns of plain-cipher video frame pairs, our suggested HEVC cryptosystem is adequate and enough to survive the chosen plain-text critical attack. And as a result, it will surely resist the other three types of attacks. Therefore, the hamming distance calculation step is one of our main

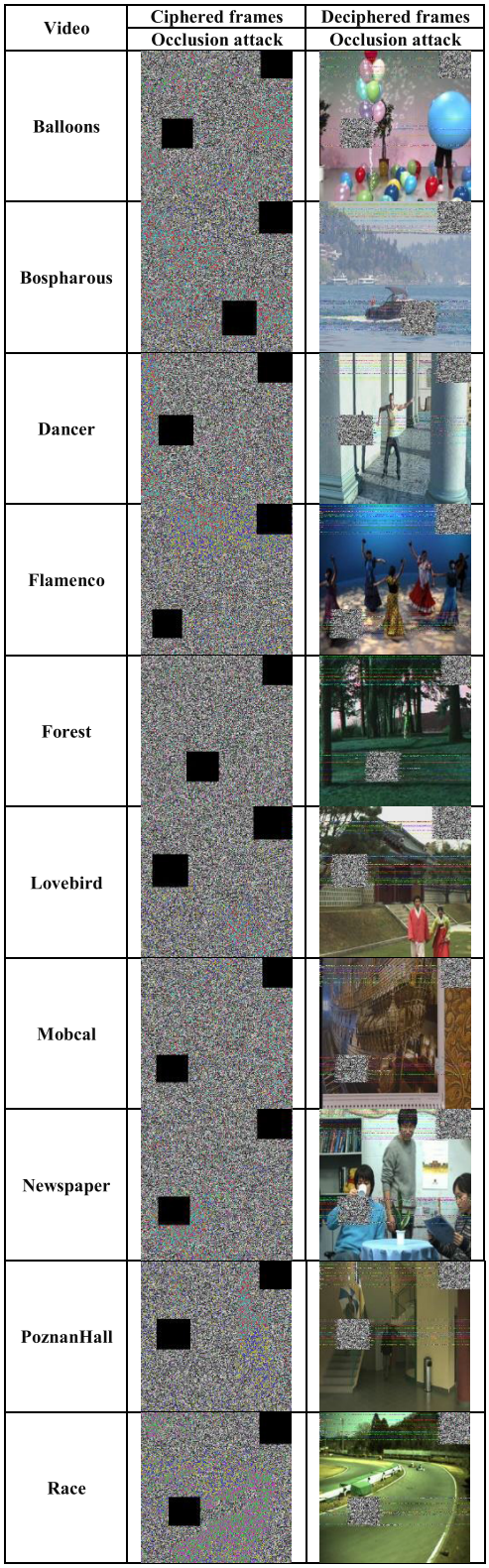


FIGURE 21. The ciphered and deciphered frames in the existence of occlusion attack on the ciphered frames of the tested compressed HEVC sequences.

contributions in this work for building a robust and secure video streaming system.

N. COMPARATIVE ANALYSIS WITH RECENT RELATED WORKS

This section examines how appropriately the numerous assessment parameters of our HEVC cryptosystem are superior compared to the latest related works. Therefore, to further confirm the suggested cryptosystem effectiveness for reliable HEVC communication over untrustworthy channels, a comparison study has been investigated to evaluate the security efficiency of the suggested cryptosystem compared to the preceding cryptography works [24], [29], [32]–[34], [37]–[39], [54], [55] in terms of average values of SSIM and PSNR outcomes. The average SSIM and PSNR outcomes for the ciphered videos of the comparison study between the suggested cryptosystem and the preceding works in [24], [29], [32]–[34], [37]–[39], [54], [55] are displayed in Table 11. The accomplished comparison study ensures and confirms that the suggested cryptosystem provides adequate average lower PSNRs and SSIMs for the encrypted videos compared to the preceding cryptography algorithms.

TABLE 11. The average SSIM and PSNR results of the ciphered video frames for the suggested cryptosystem and the related cryptography algorithms in [24], [29], [32]–[34], [37]–[39], [54], [55].

Method	PSNR (dB)	SSIM
Proposed	9.38	0.032
[24]	11.82	0.153
[29]	19.47	0.432
[32]	12.23	0.218
[33]	14.92	0.232
[34]	10.84	0.321
[37]	11.42	0.237
[38]	11.31	0.241
[39]	11.64	0.183
[54]	10.68	0.218
[55]	12.31	0.203

Because of our suggested cryptosystem can be tested and applied to any multimedia content like digital images ciphering, as we already tested it for the ciphering of streamed video frames. So, to further confirm the performance efficiency of the suggested cryptosystem, we analyzed its execution on an ordinary digital color image (Lena) to compare its security performance to a wide range of recent related image cryptography techniques [6]–[23]. Tables 12 presents the comparison study of the suggested cryptosystem with recent preceding image cryptography works in [6]–[23] in terms of entropy, PSNR, correlation, NPCR, and UACI. It is observed from this comparative analysis that all assessment parameters are superior compared to the preceding related algorithms. So, it is proved from all introduced results that the suggested cryptosystem has great sensitivity to the plain images and video frames, and it can survive the known/chosen-plaintext attacks, confirming that our cryptosystem is better robust and secure than other related cryptosystems.

TABLE 12. Comparison analysis of the suggested cryptosystem with recent related cryptography algorithms in [6]–[23].

Method	PSNR (dB)	NPCR	UACI	Entropy	Correlation
Proposed	36.07	0.9957	0.3381	7.9992	-0.00116
[6]	32.42	0.9928	0.3325	7.9893	0.0053
[7]	33.57	0.9961	0.3347	7.9896	0.0023
[8]	32.31	0.9961	0.3342	7.9971	0.0130
[9]	33.87	0.9951	0.3358	7.9975	0.0011
[10]	------	0.9963	0.3360	7.9972	-0.0025
[11]	------	0.9952	0.3368	7.9984	0.0032
[12]	30.50	0.9967	0.3346	7.9896	0.0004
[13]	------	0.9975	0.3345	7.9980	0.0000327
[14]	31.57	0.9954	0.3311	7.9983	0.04267
[15]	30.84	0.9960	0.3357	7.9973	0.0088
[16]	------	------	------	7.9909	0.0025
[17]	------	0.9946	0.3341	7.9972	0.0116
[18]	------	0.9941	0.3397	7.9878	0.0578
[19]	------	------	------	7.9952	0.0069
[20]	------	0.9963	0.3347	7.9895	0.003768
[21]	------	0.9959	0.3351	7.9927	0.0037
[22]	------	0.9962	0.3352	7.9970	0.0042
[23]	------	0.9925	0.3330	7.9987	0.0011

VI. CONCLUSIONS AND FUTURE WORK

In this work, a hybrid secure and robust HEVC cryptosystem based on DNA sequences, chaotic maps, and Mandelbrot sets is suggested. The Arnold map has been selected as the most excellent map to be employed with our cryptosystem due to its great security performance, where a straightforward and appropriate strategy for the chaotic map selection is devised to choose the most proper chaotic map. In the suggested cryptosystem, the ciphering process is employed independently on each of the three video frame channels to further boost privacy and security efficiency. The suggested cryptosystem proved its superior performance for the security of video streaming. The ciphered video frames engendered by our suggested cryptosystem are not possible to be deciphered by the attackers as the ciphering process is performed utilizing the arbitrarily created secret sequences and keys from chaotic maps. Also, the advantage of large keyspace of the suggested cryptosystem eradicates the impact of brute-force attacks. Extensive security analysis is investigated for the suggested cryptosystem which includes visual analysis, histogram analysis, quality analysis, correlation analysis, noise effect analysis, differential analysis, attack analysis, entropy analysis, etc. These assessment indicators which are studied and examined provide superior values than the preceding related works. Additionally, it has been proved that the suggested cryptosystem yields a greater robust and secure way to communicate different types of multimedia content like images and videos. In the future, we can incorporate the parallel diffusion and permutation concepts to further enhance the computation speed of the suggested cryptosystem. Also, we intend to design a multilevel security system for reliable HEVC communication by merging the watermarking, and steganography algorithms for achieving further security of video streaming in IoT multimedia applications. Moreover, we aim to develop

a smart and secure video streaming security system based on the new trends of deep learning techniques.

REFERENCES

[1] A. Rego, A. Canovas, J. M. Jimenez, and J. Lloret, "An intelligent system for video surveillance in IoT environments," *IEEE Access*, vol. 6, pp. 31580–31598, 2018.
[2] A. Kumari, S. Tanwar, S. Tyagi, N. Kumar, M. Maasberg, and K.-K.-R. Choo, "Multimedia big data computing and Internet of Things applications: A taxonomy and process model," *J. Netw. Comput. Appl.*, vol. 124, pp. 169–195, Dec. 2018.
[3] R. Herrero, "Analysis of IoT mechanisms for media streaming," *Internet Things*, vol. 9, Mar. 2020, Art. no. 100168.
[4] *High Efficiency Video Coding (HEVC) Codec*. Accessed: May 15, 2020. [Online]. Available: https://hevc.hhi.fraunhofer.de/
[5] D. Jun and H. Y. Kim, "Low complexity based ultra-high quality video compression method for multimedia-centric Internet of Things (IoT) services," *Multimedia Tools Appl.*, vol. 77, no. 4, pp. 4661–4675, Feb. 2018.
[6] X. Chai, Y. Chen, and L. Broyde, "A novel chaos-based image encryption algorithm using DNA sequence operations," *Opt. Lasers Eng.*, vol. 88, pp. 197–213, Jan. 2017.
[7] X. Wu, K. Wang, X. Wang, H. Kan, and J. Kurths, "Color image DNA encryption using NCA map-based CML and one-time keys," *Signal Process.*, vol. 148, pp. 272–287, Jul. 2018.
[8] X. Chai, Z. Gan, K. Yang, Y. Chen, and X. Liu, "An image encryption algorithm based on the memristive hyperchaotic system, cellular automata and DNA sequence operations," *Signal Process., Image Commun.*, vol. 52, pp. 6–19, Mar. 2017.
[9] R. Enayatifar, A. H. Abdullah, I. F. Isnin, A. Altameem, and M. Lee, "Image encryption using a synchronous permutation-diffusion technique," *Opt. Lasers Eng.*, vol. 90, pp. 146–154, Mar. 2017.
[10] X.-Y. Wang, H.-L. Zhang, and X.-M. Bao, "Color image encryption scheme using CML and DNA sequence operations," *Biosystems*, vol. 144, pp. 18–26, Jun. 2016.
[11] J. Wu, X. Liao, and B. Yang, "Image encryption using 2D Hénon-sine map and DNA approach," *Signal Process.*, vol. 153, pp. 11–23, Dec. 2018.
[12] X. Wu, H. Kan, and J. Kurths, "A new color image encryption scheme based on DNA sequences and multiple improved 1D chaotic maps," *Appl. Soft Comput.*, vol. 37, pp. 24–39, Dec. 2015.
[13] P. S. Sneha, S. Sankar, and A. S. Kumar, "A chaotic colour image encryption scheme combining Walsh–Hadamard transform and Arnold–Tent maps," *J. Ambient Intell. Humanized Comput.*, vol. 11, no. 3, pp. 1289–1308, Mar. 2020.
[14] J. Kalpana and P. Murali, "An improved color image encryption based on multiple DNA sequence operations with DNA synthetic image and chaos," *Optik*, vol. 126, no. 24, pp. 5703–5709, Dec. 2015.
[15] X. Chai, K. Yang, and Z. Gan, "A new chaos-based image encryption algorithm with dynamic key selection mechanisms," *Multimedia Tools Appl.*, vol. 76, no. 7, pp. 9907–9927, Apr. 2017.
[16] C. Li, G. Luo, K. Qin, and C. Li, "An image encryption scheme based on chaotic tent map," *Nonlinear Dyn.*, vol. 87, no. 1, pp. 127–133, Jan. 2017.
[17] A. Y. Niyat, M. H. Moattar, and M. N. Torshiz, "Color image encryption based on hybrid hyper-chaotic system and cellular automata," *Opt. Lasers Eng.*, vol. 90, pp. 225–237, Mar. 2017.
[18] H. Liu and X. Wang, "Color image encryption using spatial bit-level permutation and high-dimension chaotic system," *Opt. Commun.*, vol. 284, nos. 16–17, pp. 3895–3903, Aug. 2011.
[19] K. M. Faraoun, "Fast encryption of RGB color digital images using a tweakable cellular automaton based schema," *Opt. Laser Technol.*, vol. 64, pp. 145–155, Dec. 2014.
[20] H. Liu and A. Kadir, "Asymmetric color image encryption scheme using 2D discrete-time map," *Signal Process.*, vol. 113, pp. 104–112, Aug. 2015.
[21] X. Wang, Y. Zhao, H. Zhang, and K. Guo, "A novel color image encryption scheme using alternate chaotic mapping structure," *Opt. Lasers Eng.*, vol. 82, pp. 79–86, Jul. 2016.
[22] X. Wang and H.-L. Zhang, "A color image encryption with heterogeneous bit-permutation and correlated chaos," *Opt. Commun.*, vol. 342, pp. 51–60, May 2015.
[23] W. Auyporn and S. Vongpradhip, "A robust image encryption method based on bit plane decomposition and multiple chaotic maps," *Int. J. Signal Process. Syst.*, vol. 3, no. 1, pp. 8–13, 2014.
[24] W. Hamidouche, M. Farajallah, N. Sidaty, S. E. Assad, and O. Deforges, "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] D. Valli and K. Ganesan, "Chaos based video encryption using maps and Ikeda time delay system," *Eur. Phys. J. Plus*, vol. 132, no. 12, p. 542, Dec. 2017.
[26] S. R. Maniyath and T. V. Kaiselvan, "A novel DNA based encryption algorithm for multimedia information," *Compusoft*, vol. 5, no. 1, p. 2036, 2016.
[27] Y.-Q. Zhang, X.-Y. Wang, J. Liu, and Z.-L. Chi, "An image encryption scheme based on the MLNCML system using DNA sequences," *Opt. Lasers Eng.*, vol. 82, pp. 95–103, Jul. 2016.
[28] X.-Y. Wang, P. Li, Y.-Q. Zhang, L.-Y. Liu, H. Zhang, and X. Wang, "A novel color image encryption scheme using DNA permutation based on the Lorenz system," *Multimedia Tools Appl.*, vol. 77, no. 5, pp. 6243–6265, Mar. 2018.
[29] 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.
[30] X. Zhang and X. Wang, "Multiple-image encryption algorithm based on DNA encoding and chaotic system," *Multimedia Tools Appl.*, vol. 78, no. 6, pp. 7841–7869, Mar. 2019.
[31] B. Norouzi, S. M. Seyedzadeh, S. Mirzakuchaki, and M. R. Mosavi, "A novel image encryption based on row-column, masking and main diffusion processes with hyper chaos," *Multimedia Tools Appl.*, vol. 74, no. 3, pp. 781–811, Feb. 2015.
[32] 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.
[33] 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.
[34] 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.
[35] M. Yang, L. Zhuo, J. Zhang, and X. Li, "An efficient format compliant video encryption scheme for HEVC bitstream," in *Proc. IEEE Int. Conf. Prog. Informat. Comput. (PIC)*, Dec. 2015, pp. 374–378.
[36] X. Ma, B. Zhu, T. Zhang, S. Cao, H. Jin, and D. Zou, "Efficient privacy-preserving motion detection for HEVC compressed video in cloud video surveillance," in *Proc. IEEE INFOCOM-IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, Apr. 2018, pp. 813–818.
[37] 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.
[38] 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.
[39] A. Shifa, M. 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, Mar. 2019.
[40] M. Usman, M. A. Jan, and X. He, "Cryptography-based secure data storage and sharing using HEVC and public clouds," *Inf. Sci.*, vol. 387, pp. 90–102, May 2017.
[41] X.-Y. Wang, Y.-Q. Zhang, and X.-M. Bao, "A novel chaotic image encryption scheme using DNA sequence operations," *Opt. Lasers Eng.*, vol. 73, pp. 53–61, Oct. 2015.
[42] R. Enayatifar, F. G. Guimarães, and P. Siarry, "Index-based permutation-diffusion in multiple-image encryption using DNA sequence," *Opt. Lasers Eng.*, vol. 115, no. 3, pp. 131–140, 2019.
[43] C. Li, Y. Liu, T. Xie, and M. Z. Q. Chen, "Breaking a novel image encryption scheme based on improved hyperchaotic sequences," *Nonlinear Dyn.*, vol. 73, no. 3, pp. 2083–2089, 2013.
[44] T. Gao and Z. Chen, "A new image encryption algorithm based on hyper-chaos," *Phys. Lett. A*, vol. 372, no. 4, pp. 394–400, Jan. 2008.
[45] V. Patidar, N. K. Pareek, and K. K. Sud, "A new substitution–diffusion based image cipher using chaotic standard and logistic maps," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 14, no. 7, pp. 3056–3075, 2009.

[46] C. Li, S. Li, and K.-T. Lo, "Breaking a modified substitution-diffusion image cipher based on chaotic standard and logistic maps," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 16, no. 2, pp. 837–843, 2011.
[47] S. Lian, "Efficient image or video encryption based on spatiotemporal chaos system," *Chaos, Solitons Fractals*, vol. 40, no. 5, pp. 2509–2519, 2009.
[48] H. Liu, X. Wang, and A. Kadir, "Image encryption using DNA complementary rule and chaotic maps," *Appl. Soft Comput.*, vol. 12, no. 5, pp. 1457–1466, May 2012.
[49] B. Norouzi and S. Mirzakuchaki, "An image encryption algorithm based on DNA sequence operations and cellular neural network," *Multimedia Tools Appl.*, vol. 76, no. 11, pp. 13681–13701, Jun. 2017.
[50] A. U. Rehman, X. Liao, R. Ashraf, S. Ullah, and H. Wang, "A color image encryption technique using exclusive-OR with DNA complementary rules based on chaos theory and SHA-2," *Optik*, vol. 159, pp. 348–367, Apr. 2018.
[51] Y.-Y. Sun, R.-Q. Kong, X.-Y. Wang, and L.-C. Bi, "An image encryption algorithm utilizing Mandelbrot set," in *Proc. Int. Workshop Chaos-Fractal Theories Appl.*, Oct. 2010, pp. 170–173.
[52] *YUV Video Sequences*. Accessed: May 15, 2020. [Online]. Available: http://trace.eas.asu.edu/yuv/
[53] R. Guesmi, M. A. B. Farah, A. Kachouri, and M. Samet, "A novel chaos-based image encryption using DNA sequence operation and secure hash algorithm SHA-2," *Nonlinear Dyn.*, vol. 83, no. 3, pp. 1123–1136, Feb. 2016.
[54] 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.*, early access, Jun. 26, 2019, doi: 10.1109/TCSVT.2019.2924910.
[55] 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.

ABDULAZIZ ALARIFI received the Ph.D. degree in information security from the University of Wollongong, Australia. He is currently an Assistant Professor with the Department of Computer Science, Community College, King Saud University (KSU), Saudi Arabia. He is also the Head of the Research Unit, Community College, KSU. His main research interests include information security, information technology management, cloud computing, big data, information privacy, risk assessment and management, e-governance, and mobile applications.

SYAM SANKAR received the B.Tech. degree in computer science and engineering and the M.Tech. degree in computer and information science from the Cochin University of Science and Technology, Kerala, in 2013 and 2015, respectively. He is currently working as an Assistant Professor with the Department of Computer Science and Engineering, NSS College of Engineering, Palakkad, Kerala. His research interests include image encryption and chaotic cryptography. He has authored several articles in the area of secure image transmission and got published in top journals. He has been acting as a reviewer of several international journals published by Elsevier and IEEE.

TORKI ALTAMEEM received the B.S. degree from the Faculty of Computers and Information Sciences, King Saud University, in 2003, and the M.S. and Ph.D. degrees from Pronel University, U.K., in 2004 and 2007, respectively. He is currently a Professor with the Department of Computer Science, King Saud University. His research interests include e-commerce, high-performance computing, distributed computing, image processing, and computer vision.

K. C. JITHIN received the B.Tech. degree in computer science and engineering from the University of Calicut, Kerala, in 2017, and the M.Tech. degree in computer science and engineering from APJ Abdul Kalam Technological University, Kerala, in 2019. His research interests include image encryption, chaotic cryptography, MEMS application, and mobile application development. He has authored several articles in these areas and got published in top journals.

MOHAMMED AMOON received the B.Sc. degree in electronic engineering and the M.Sc. and Ph.D. degrees in computer science and engineering from Menoufia University, in 1996, 2001, and 2006, respectively. He is currently a Professor of computer science and engineering with the Department of Computer Science and Engineering, Menoufia University. He is also a Professor of computer science with the Department of Computer Science, King Saud University. His research interests include agent-based systems, fault tolerance techniques, scheduling algorithms, green computing, distributed computing, grid computing, cloud computing, fog computing, and the Internet of Things (IoT).

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 FEE, Menoufia University, in 2019. He is currently working as a Lecturer and an Assistant professor with the 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, and deep learning in signal processing and communication systems applications.