IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 20 September 2022, accepted 9 November 2022, date of publication 18 November 2022,
date of current version 30 November 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3223355

RESEARCH ARTICLE

Chaos Based Encryption Technique for Compressed H264/AVC Videos

M. A. EL-MOWAFY[1], S. M. GHARGHORY[1], M. A. ABO-ELSOUD[2], M. OBAYYA[2], AND M. I. FATH ALLAH[3]

[1]Electronics Research Institute, Cairo 12622, Egypt
[2]Department of Communications and Electronics, Mansoura University, Mansoura 35516, Egypt
[3]Department of Communications and Electronics, Delta Higher Institute for Engineering and Technology, Talkha 7623184, Egypt

Corresponding author: M. A. El-Mowafy (mohamedelmowafy@eri.sci.eg)

ABSTRACT Saving videos streaming from the unlawful users became an urgent claim. Cryptography and Steganography are the most important and indispensable processes to protect and embed the multimedia data during the transfer or storage process. Chaotic-based cryptography has been proposed to be an efficient encryption technique for multimedia applications and has played a vital role in information security. While the chaotic maps have a long history of researching as a nonlinear dynamic system, visual encryption is useful for concealing messages in videos and safeguarding private content from unauthorized intrusion. In this paper, two new proposed algorithms for compressed videos by the advanced H.264/AVC video coding are presented. First algorithm approach has been implemented by robust video encryption algorithm based on the chaos maps with random key to be tested under different attacks. The second algorithm approach has been implemented by using the hybrid of both steganography and cryptography based on chaotic maps for video frames. The proposed algorithms are conducted on luminance component Y of a set of different YUV video sequences with different resolution using MATLAB software. The simulation results of the proposed algorithms are evaluated using various performance metrics comparing to that with the state-of-art techniques. The suggested approaches have shown to be more resistant to many sorts of attacks and is recommended for future using in real-time applications.

INDEX TERMS H.264/AVC, YUV videos sequence, video encryption, chaotic map, video steganography.

I. INTRODUCTION

Nowadays, with great growth in the technology of information transmission and communications in general and technology of data compression and encryption in particular, the issue of information security has become one of the most important issues that must keep pace with this rapid development. This is to avoid the consequences of illegal access to confidential information [1].

H.264/AVC advanced video coding is one of the most recent video compression standards and is a popular format for coded video [2], [3]. One of the advantages of H.264/AVC is that it improves the efficiency of video compression, i.e., more flexibility with storing and transferring videos compared to Moving Picture Experts Groups MPEG-2 and MPEG-4. Concerning H264 video encryption techniques, the problem is how to design a secure and fast encoding system, where the encryption algorithm is incorporated into the encoding process which does not bring much additional computational burden with acceptable high-level security. One of the most important features of the incorporated system is that is able to generate totally syntax-compliant H264 videos. Therefore, relying on a simple encryption algorithm such as Data Encryption Standard DES or Advanced Encryption Standard AES negatively affects the security of the H264 videos. If there is a need to maintain the confidentiality of the information, the encryption technique should involve operations in which the information is not available without the use of the appropriate decryption key by the legitimate user [4], [5].

Cryptographic and Chaotic maps algorithms have some similar properties such as sensitivity to a change in initial

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

conditions and parameters and randomness-like behavior and unstable periodic orbits with long periods. Thus, the Chaotic map parameters have been representing a key to the encryption algorithm. As for the main difference between the two algorithms, cryptographic algorithm transformations are defined on finite sets while chaos has meaning only on real numbers [6], [7], [8], [9], [10], [11]. In steganography, hidden information is known only to the authorized sender and receiver and is considered more secure than cryptography where ciphertext attracts the intruder to decode the information. The most fundamental requirements for a successful steganography technique: are imperceptibility, the capacity to hide, and robustness. Video steganography is more secure and robust compared to images, because of the complex statistical video structure that is difficult to detect [12], [13], [14], [15], [16], [17].

Furthermore, many of these algorithms used the calculation of rate-distortion (RD) cost for the different prediction modes but this was at expense of high complexity due to many mathematical calculations utilized.

In 2015, The error propagation characteristic in an H.264 decoder was used by Yongwha Chung [18] to develop a selective encryption approach that encrypted just the DC/ACs of I-macroblocks and the motion vectors of P-macroblocks. According to experimental findings, the overall performance was improved and the burden associated with the entire encryption approach was reduced after examining the trade-off between visual level and processing speed and comparing it to conventional selective encryptions. In 2017, Wassim Hamidouche [19] suggested three encryption schemes for real-time selective video encryption solution in the scalable extension of High Efficiency Video Coding (HEVC) standard based on the chaos-based stream system. First scheme was encrypted the lowest layer of SHVC, and the second were encrypted only the highest layer, and the last scheme were encrypted all layers. The results showed that the encrypt of lower layer or all layers were a higher secure level than encrypt the highest layer.

In 2018, Saurabh Anand [20] proposed F5 algorithm and applied to after video compression by H.264 technique, in order to prevent statistical attacks and improving embedding efficiency. The proposed message hiding algorithm has given good results compared to traditional methods, and this is evident with the calculation of peak signal to noise ratio PSNR. Fatma K Tabash [21] proposed encryption algorithm based on Context-adaptive binary arithmetic coding (CABAC) in 2018. Where the bin-string of Intra-Prediction Mode was encrypted with chaotic signals and the sign of MVD was toggled randomly, in addition to that the sign of the AC coefficients were flipped randomly and the first value of DC coefficients was encrypted by XORing the bin-string with random stream ware generated with chaotic Logistic map. The proposed algorithm results had showed high time efficiency compared to traditional algorithms, because the technique not affecting on overall encoding process.

Jie Wang [22] proposed a novel video steganography in HEVC based on (IPM), by analyzes the probability distribution of 4×4 IPMs then cover selection method combined with the Coding Unit (CU) and Prediction Unit (PU) coding information in 2019.

In 2019, Dawen Xu [23] proposed a commutative encryption and data hiding scheme for HEVC videos, i.e. allowed to ciphering a steganographic video without interfering with the embedded signal or to perform steganography on an encrypted video while still allowing perfect decryption. The results showed that the achieved capacity was enough to embed a reliability proof as well as some other data and the video distortion caused by data hiding were very low. For Hassan Elkamchouchi [24], two video encryption schemes have been proposed with different types of chaotic maps to generate the key stream for encrypting the frames after video file was compressed the video sequence, and to improve the algorithms construction was used a Feistel structure in the substitution step. the study showed provide high level of security according to the increase of cost time compered to recent algorithms in 2020.

In 2020, Hui Xu [25] introduced a novel cross-coupled chaotic system as the key stream generation component, and the key stream has been closely related to the plaintext through the synchronization vector mechanism for the H.264 compressed video bitstream. And if part of the ciphertext stream was missed, the other parts could be decrypted normally. the proposed Algorithm had lower time overhead and did not cause a significant increase in bit rate. Lingyu Zhang [26] proposed H.264/AVC intra prediction video steganography algorithm based on (n, k) linear block code over ring Z4 in 2020. in additional, the property of adding abelian groups and multiplicative commutative semigroup was utilized to generate the steganography code that was applied to video steganography based on intra-prediction mode (IPM-based video steganography). Experimental results showed that the performance of the proposed scheme was superior to those of the former IPM-based schemes.

In 2021, Osama Fouad Abdel Wahab [27] proposed a hybrid data compression algorithm increases the input data to be encrypted by RSA (Rivest Shamir Adleman) cryptography technique to enhance the security level and it could be used in executing lossless and lossy compacting Steganography methods. After evaluated that algorithm on criteria such as percentage Savings percentage, Compression Ratio, Mean Squared Error, Bits per pixel, Compression Time, Structural Similarity Index, Peak Signal to Noise Ratio, and Compression Speed. The proposed algorithm was showed a high-level performance and system methodology compared to other algorithms that used the same methodology.

The results of the proposed algorithm have been more effective visual quality and storage capacity, and it has been highly security and acceptable durability against attacks than the existing techniques.

To meet the necessary requirements for information security and concealment, two techniques based on cryptography and steganography are proposed in this work for the compressed H264/AVC videos sequences. By employing various chaos maps with a particular key, multiplying and dividing it twice by the luminance component of the I-frame of the compressed sequences during the encryption process and doing the same during the decryption phase, chaos-based approaches were used to the compressed H264/AVC. The low-resolution video I-frame used in steganography is concealed inside a high-resolution video I-frame. Different metrics were employed to evaluate the suggested algorithms' performance using various chaos maps comparing to the performance of the present techniques. In comparison to other chaotic maps that were applied by the suggested algorithms and the current state-of-the-art algorithms, the logistic chaotic map achieves good results.

The remaining of this paper is organized as follows: Section II reviews fundamental concepts of H.264/AVC codec. in section III, reviews chaos maps for video encryption are presented. In section IV, measures used to assess the durability of a video encryption scheme are listed. The structures of the proposed algorithms based on chaos maps are proposed in section V. Simulation results and discussions of the proposed algorithms approach for optimal mode decisions are detailed in section VI. Finally, Section VII offers a conclusion.

II. FUNDAMENTAL CONCEPTS OF H.264/AVC CODEC

In general, Video coding is generally defined as a process of video compression and decompression H.264/AVC is an industry-standard and popular format for video coding. H.264 is defined as a block-oriented, compensation-based video compression standard that defines multiple profiles (tools) and levels (max bitrates and resolutions). Fig. 1 shows the encoding process which enables the conversion of video frames into bitstream, and the decoding enables the video to be retrieved after compression [2].

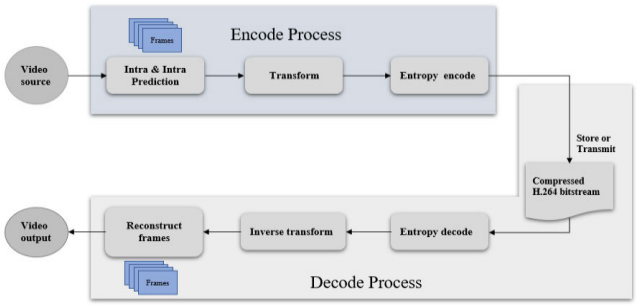


FIGURE 1. The H.264 video coding and decoding process.

The encoding process begins by dividing the video sequence into a group of frames. Next come is the prediction stage which aims to reduce redundancy. The prediction is divided into intra prediction (a spatial prediction) which formed from previously coded frame samples in the same frame, and inter prediction (a temporal prediction) which formed from previously coded frames.

For intra prediction luminance (Luma) component of I frame is divided into macroblocks (MBs) of size 16×16 or 4×4 or 8×8. While the two chrominance (Chroma) components of I frame are divided into blocks size of 8×8 and after that the prediction modes are applied to each block of, I frame components. Table 1 shows all possible prediction modes for MBs [28].

TABLE 1. Possible prediction modes of Intra prediction block size.

Intra prediction block size	The number of possible prediction modes	Mode
16×16	Four prediction modes are utilized to predict each block P in the Luma component.	- Vertical - Horizontal - DC - Plan
4×4	Nine possible modes are utilized to predict each block P in the Luma component.	- Vertical - Horizontal - DC - Vertical right - Vertical left - Horizontal up - Horizontal down - Diagonal left - Diagonal right
8×8	Four prediction modes are utilized to predict each block P in the Luma or Chroma component.	- Vertical - Horizontal - DC - Plan

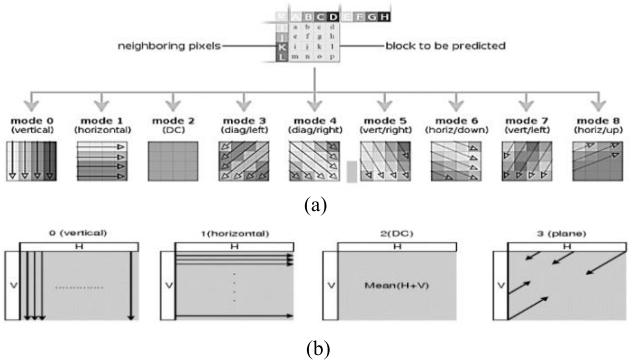


FIGURE 2. (a) Nine different modes for intraframe prediction of 4×4 luminance MBs. (b) Four different modes for intraframe prediction of 16×16 luminance MBs and 8×8 chrominance MBs.

Fig 2. (a) and (b) demonstrate the nine prediction modes as well as the four prediction modes used for encoding the luminance and chrominance components with block sizes of 4×4 or 16×16 or 8×8 respectively. (b), where acapital letters from A to M on the top left of the block to be predicted shown in fig. 2. (a) are used to encode the block. The DC mode is calculated by the average luminance values of the 12 pixels from A to L around the coding MB [29].

There are many structures of inter-prediction, as there are many options for choosing a reference frame. Multiple reference frames are one of the most popular structures in which all the previously coded slices are available as reference frames as show in Fig. 3 [2].

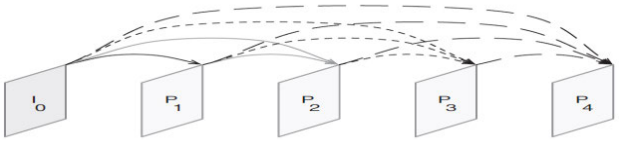


FIGURE 3. IPPP . . . with multiple reference pictures.

Blocks of residual data in a macroblock are transformed and quantized following the prediction process, with the number of transformations depending on the type of transformation. One of the types of transformation used with H.264/AVC is integer transform, a scaled approximation to the Discrete Cosine Transform, DCT, and these transform coefficients are scaled and quantized. After that, quantized transform coefficients, prediction parameters, header parameters, and motion vectors are converted into a compressed bitstream. H.264/AVC encoder using Exponential Golomb codes for some syntax elements and a custom-designed Context Adaptive Variable Length Coding CAVLC algorithm for residual blocks, or a Context Adaptive Binary Arithmetic Coder CABAC.

The decoder receives the coded compressed H.264 bitstream, macroblocks have been decoded, re-scaled, and inverse transformed to form a decoded residual to generate the same macroblocks prediction that was created and added to the residual to produce decoded macroblocks to recreate a sequence of video frames [2], [3].

III. CHAOS-BASED VIDEO ENCRYPTION

It is possible to encrypt the raw data entirely without taking the region-of-interest into consideration and to take the region-of-interest into consideration only partially or selectively. The raw video data is encrypted directly with chaotic maps before or after the compression process.

The capacity of chaotic maps to produce seemingly random sequences that are extremely sensitive to the original seed point is one of its most crucial characteristics [30], [31]. There are different kinds of chaotic maps, and three of them will be discussed in the following section besides the implementation of the suggested algorithms based on both of them are examined:

A. IKEDA CHOAS MAP

The Ikeda map is a complex map that was introduced by Kensuke Ikedain in 1987. Ikeda map can be described by the Maxwell-Bloch equations which consist of a set of difference-differential equations without involving the spatial coordinate under the appropriate conditions. 2D Ikeda map can be represented by the following equations [32]:

$$x_{i+1} = 1 + m(x_i(\cos(t)) - y_i \sin(t)) \quad (1)$$

$$y_{i+1} = 1 + m(x_i(\sin(t)) + y_i \cos(t)) \quad (2)$$

where m is the external parameter. The graph of this map is show in in Fig. 4.

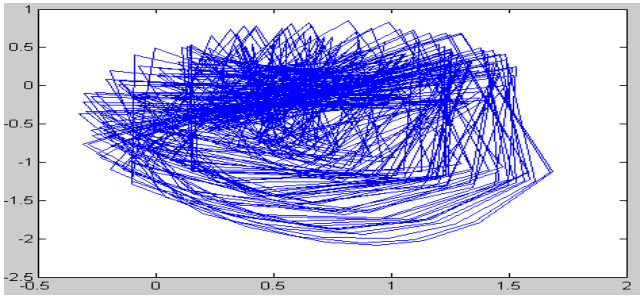


FIGURE 4. IKEDA map Graph.

B. HÉNON CHAOS MAP

Hénon shows how key structure area-preserving mappings may preserve the fundamental characteristics of dynamical systems that are described by differential equations. Hénon presented the well-known two-dimensional equations shown below [33], [34].

$$x_{n+1} = 1 - ax_n^2 + y_n \quad (3)$$

$$y_{n+1} = bx_n \quad (4)$$

where, a and b represent external control parameters. The graph of this map is shown in Fig. 5.

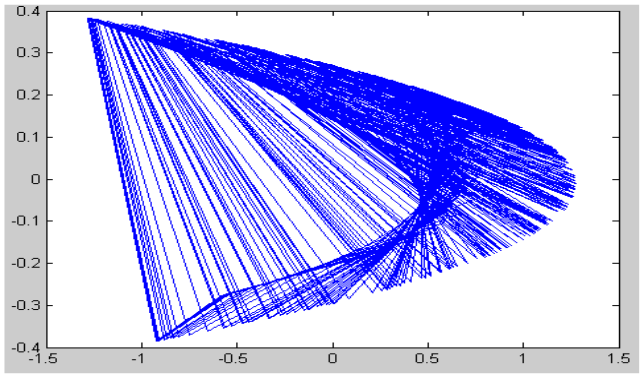


FIGURE 5. Hénon map Graph.

C. LOGISTIC CHAOS MAP

The logistic equation also called the ''Verhulst model'' is given by the equation:

$$x_{n+1} = k(1 - x_n) \quad (5)$$

where, K stands for the external control parameter, n is the running variable, and x_n is the variable at the nth iteration.

The logistic map is a non-invertible map i.e., the map can be iterated forward in time with each x_n leading to a unique subsequent value x_{n+1}, the reverse is not true. It is also called ''iterated map function''. The graph of this map is illustrated in Fig. 6 [31], [35].

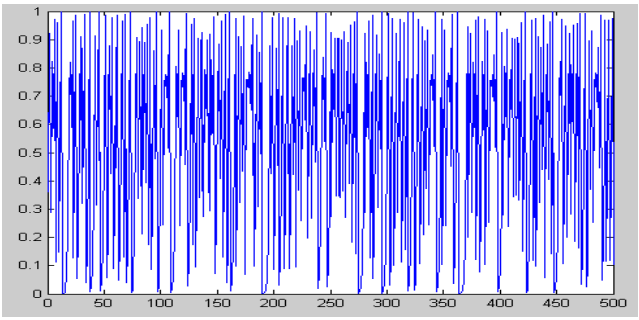


FIGURE 6. Logistic map graph.

IV. PERFORMANCE MEASURES AND ATTACKS MODELS

A. PERFORMANCE MEASURES

It's essential to evaluate the effectiveness of compressed video encryption methods in order to determine how robust they are against assaults. Numerous tests are run to evaluate the algorithm's quality:

1) MEAN SQUARED ERROR

The mean squared error between two video frames X and Y is defined as [24], [36]:

$$MSE = \frac{1}{M \times N \times f} \sum_{k=1}^{f} \sum_{i=1}^{M} \sum_{j=1}^{N} \times [OIF(i,j,k) - DIF(i,j,K)]^2 \quad (6)$$

where, M is the number of rows, N is the number of columns, f is the number of image frames, OIF is the original I-frame, and DIF is the decrypted I-Frame.

2) PEAK SIGNAL-TO-NOISE RATIO (PSNR)

The Peak Signal-to-Noise Ratio is used to measure the degradation between the plain and decrypted frames. It can be computed as in Eq. (7) [24]:

$$PSNR = 10 \log_{10} \left(\frac{max_{OIF}^2}{MSE} \right) dB \quad (7)$$

where, Max_{OIF} represents the maximum possible pixel value of the original I-Frame [].

3) CROSS CORRELATION COEFFICIENT (R)

The cross correlation between the original and decrypted images can be defined as in Eq. (4) [24]:

$$R = \frac{\sum_m \sum_n (OIF_{mn} - \bar{OIF})(DIF_{mn} - \bar{DIF}}{\sqrt{(\sum_m \sum_n (OIF_{mn} - \bar{OIF})^2)(\sum_m \sum_n (DIF_{mn} - \bar{DIF})^2)}} \quad (8)$$

where, m is the row number, n is the column number, OIF is the mean value of the pixels of original I-frame, and DIF is the mean value of the pixels of decrypted I-frame.

4) THE NUMBER OF PIXELS CHANGE RATE

The number of pixels change rate (NPCR) is used to measure the percentage of pixels that are different between two videoframes and is computed as follows [36]:

$$D(i,j) = \begin{cases} 0, & OIF(i,j) = DIF(i,j) \\ 1, & OIF(i,j) \neq DIF(i,j) \end{cases} \quad (9)$$

$$NPCR = \frac{1}{m \times n} \sum_{i=1}^{n} \sum_{j=1}^{m} D(i,j) \times 100\% \quad (10)$$

where *OIF* and *DIF* are the two video frames. This measure can be employed to assess how sensitive a video encryption algorithm is to slight variations in the plain video frame.

5) THE UNIFIED AVERAGE CHANGING INTENSITY (UACI)

The average intensity of absolute differences between two frames is determined according to the following equation [36]:

$$UACI = \frac{1}{m \times n} \sum_{i=1}^{n} \sum_{j=1}^{m} \frac{|OIF(i,j) - DIF(i,j)|}{255} \times 100\% \quad (11)$$

Again, OIF and DIF two mean value of the pixels of I-frames. It can be used to assess the sensitivity to slight changes in the plain video or key changes.

6) ELAPSED TIME

For each run of experiments, elapsed time has reflected the overall calculation time for encryption and decryption procedures in seconds [24], [36].

7) STRUCTURAL SIMILARITY INDEX METHOD (SSIM)

A video frame's degree of distortion as seen by the human visual system is measured using the SSIM metric. The range of SSIM's value is 0 to 1. The quality of the movie improves as the SSIM approaches 1.

$$SSIM(o,d) = \frac{(2\mu_o\mu_d + C_1)(2\sigma_{od} + C_2)}{(\mu_o^2 + \mu_d^2 + C_1)(\sigma_0^2 + \sigma_d^2 + C_2)} \quad (12)$$

where μ_o and μ_d, σ_o and σ_d, and σ_{od} are the local means, standard deviations and cross-covariance of original I-frame O and decrypted I-frame D, respectively. C_1, and C_2 are the regularization constants that have very small values to avoid the extreme small denominator [36].

B. ATTACKS MODELS

In addition to the aforementioned performance metrics, it was necessary to access the robustness of the suggested algorithms against different types of attacks. Therefore, the algorithms' robustness will be evaluated using the following attack tests: a cropping assault, a noise attack, and the key sensitivity [24].

In the cropping attack, one or more areas of the encrypted I-Frame of the video are deleted or cropped. The cropping attack will be applied with beside part from the I-frame. Concerning the noise attack, salt and pepper noise is applied to guarantee the robustness of the proposed scheme. Any encryption video algorithm must take key sensitivity into consideration. If a minor modification in a secrete key, it results in a completely different ciphered I-frame. The security level has a strongly relation to key sensitivity attacks.

Changes in the chaotic map parameters during the decryption process serve as the essential sensitivity test scenario.

V. PROPOSED ALGORITHMS

In this section, the two proposed video encryption algorithms are presented with their main steps and flow charts.

The first algorithm depends on using chaotic maps to produce randomization in the original video I-frames. The main flow chart of the proposed algorithm is shown in Fig. 7. Initially, the compressed YUV video sequence is split into frames with one luminance (Luma) and two chrominance (Chroma) components using the frame generator. The luma component of the I-frame is divided into sub-blocks of size 16×16 as shown in the right path. Then, the sub-blocks are multiplied by the candidate chaotic map and then the outputs from the preceding step are multiplied again by this chaotic map. All the presented chaotic maps for the suggested algorithms are applied with specific parameters and initial values. Finally, the outputs of the end stage are the encrypted YUV I-frames.

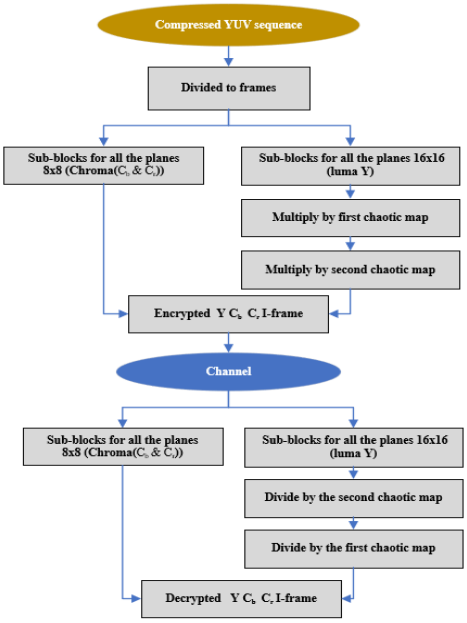


FIGURE 7. The proposed cryptography algorithm.

The decryption process has been started by divided the encrypted I-frame into Luma and two Chroma components then the luma is divided into sub-blocks of size 16×16. The sub-blocks are divided on the chaotic map used in encryption process and then follow by dividing the previous step output on this chaotic map again. All the chaotic maps used in the decryption process have the same specific parameters and initial values as in the encryption process to output the decrypted I-frame.

The following steps are the procedures for implementing out the proposed algorithm based on chaotic maps:

- Step1: Read YUV sequence.
- Step2: The sequence is divided into a group of frames.
- Step3: For the I-frame: Y is divided into (16×16) sub-blocks, andC_b and C_r are divided into (8×8) sub-blocks.
- Step4: Multiply the I-frame by tested chaotic map.
- Step5: Multiply the output I-frame from the previous step by the tested chaotic map.
- Step6: Encrypted YCbCr I-frame.
- Step7:transmit encrypted YCbCr I-fram through the channel.
- Step8: In decryption process; Y component of I-frame is divided into (16×16) sub-blocks, and C_b and C_r are divided into (8×8) sub-blocks.
- Step9: Divide the I-frame by the tested chaotic map.
- Step10: Divide the output I-Frame from previous step by the tested chaotic map.
- Step11: Decrypted YCbCr I-fram

In Fig. 8 The second approach is a hybrid algorithm combining both steganography and cryptography processes. In the first process, I-frame of the original video is hidden in I-frame of the cover video while the latter process is implemented by applying the chaotic map to the cover I-frame resulted from steganography process. Initially, the original I-frame is attached to the cover I-frame by replacing part of the cover I-frame with dimensions of the original I-frame. After that,

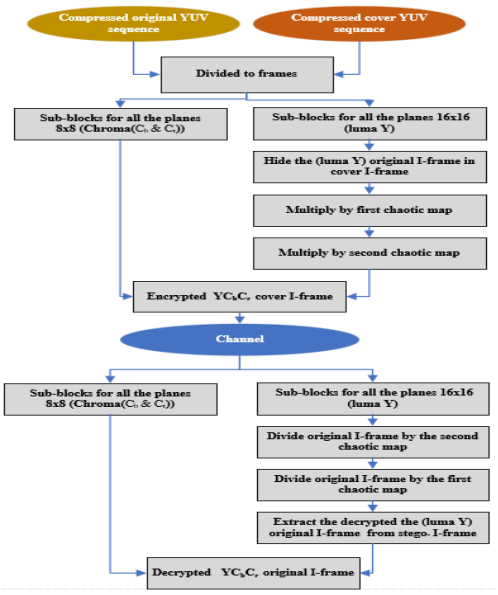


FIGURE 8. The proposed hybrid Steganography and cryptography algorithm.

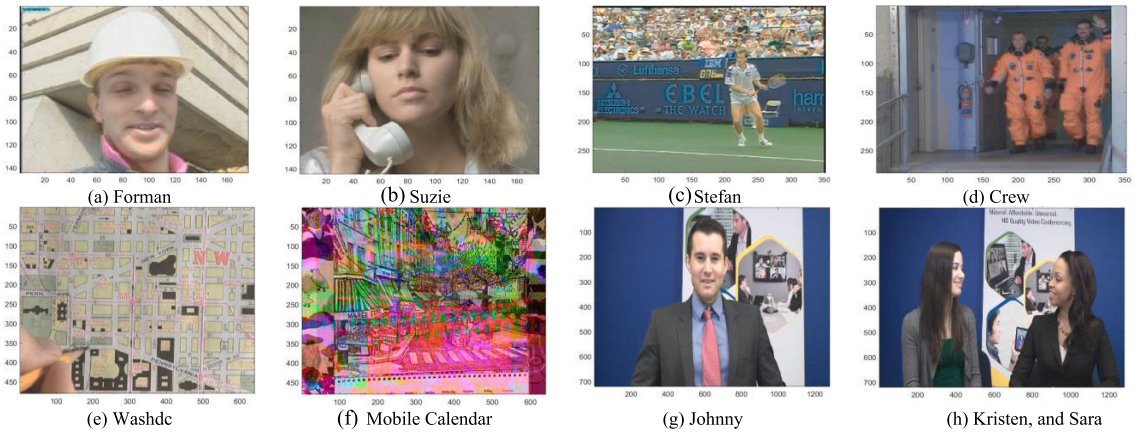


FIGURE 9. (a-h) The original I-Frames of different video sequences.

the steps of encryption and decryption processes of the first algorithm are implemented. In the final step of decryption process, the original I-frame is extracted from the cover I-frame by its subtraction from the cover I-frame.

The following steps are given for implementing the proposed approach, which uses the original and cover video sequences as input and produces the original I-Frame once it has been decrypted as an output. The pseudo code of the suggested hybrid algorithm is described as follow:

- Step1: Read original and cover YUV sequences.
- Step2: The sequences are divided into a group of frames.
- Step3: For the merged I-frames: Y is divided into (16×16) sub-blocks, and C_b and C_r are divided into (8×8) sub-blocks.
- Step4: Multiply the merged I-frame by tested chaotic map.
- Step5: Multiply the output merged I-frame from the previous step by the tested chaotic map.
- Step6: Encrypted YCbCr merged I-frame.
- Step7:transmit encrypted YCbCr merged I-frame through the channel.
- Step8: In decryption process; Y component of merged I-frame is divided into (16×16) sub-blocks, and C_b and C_r are divided into (8×8) sub-blocks.
- Step9: Divide the merged I-frame by the tested chaotic map.
- Step10: Divide the output I-Frame from previous step by the tested chaotic map.
- Step11: Decrypted YCbCr I-fram

VI. SIMULATION RESULTS AND DISCUSSIONS

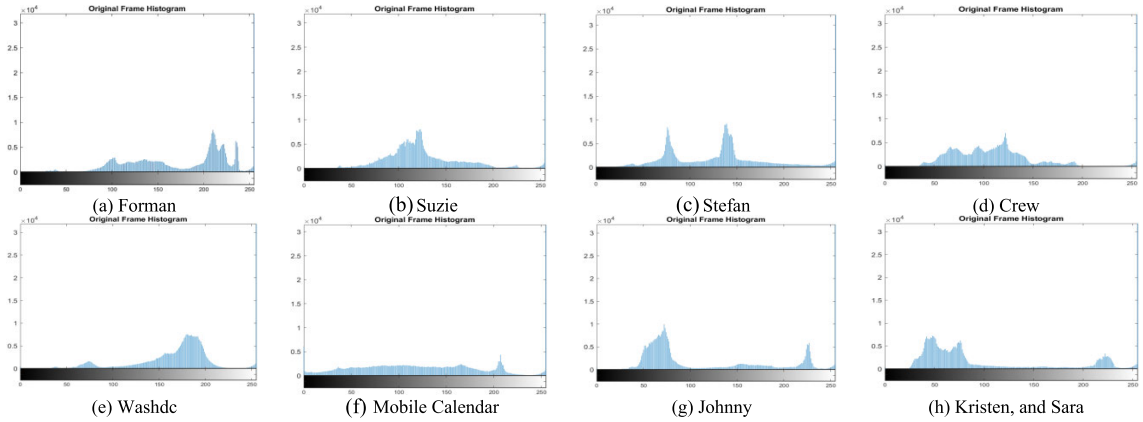
The suggested encryption algorithm is implemented on different video sequences with different resolutions which are: (two QCIF, two CIF, two Class C, and two 750p). Fig. 9 (a-h) shows the different YUV video sequences I-Frames with different resolutions, QCIF videos: (Forman, Suzie), CIF videos: (Stefan, Crew), class C videos: (Washdc, Mobile Calendar), 720p videos: (Johnny, Kristen, and Sara). Fig. 10 (a-h) shows the histogram of the different YUV video sequences I-Frames with different resolutions.

The setting parameters for applying the proposed algorithms on a sequence of test videos set using MATLAB are as follows:

- The compressed YUV videos sequences resolution is QCIF 176×144, CIF 352×288, CLASS C 832×480, and 720 P.
- The frames sequences are set to be III.....I.
- The encryption process of the proposed algorithm is implemented only on the luma component of the original I-frame while the two chroma components are combined to encrypt the luma.
- Both the encryption and decryption processes use a similar chaotic map.
- The setting parameters for the chaotic map are the same.
- the cover video sequence high resolution than the original video sequence resolution.
- Ikeda, Hénon, and Logistic chaotic maps were applied to the compressed video sequences.
- The frame rate of video sequences is 30 fps.

A. THE PROPOSED ENCRYPTION ALGORITHM FOR COMPRESSED H264 AVC SEQUENCES THAT DEPENDS ON USING CHAOTIC MAPS

Performance measurements are used assess and compare the simulation results of the proposed algorithms to those of other state-of-the-art encrypted video compression techniques. The following performance measures which are used for evaluation and the comparison are: MSE, PSNR (Original I-frame & Decrypted I-frame), PSNR (Original I-frame & Encrypted I-frame), Correlation coefficient, NPCR, UACI, and elapsed time. Table 2 displays the simulation results of the suggested approach that rely on employing different chaotic maps to randomise the original I-frame in addition to the results of the decryption process to I-frame of the following videos resolution: (two QCIF, two CIF, two Class C, and two 750p).



(a) Forman (b) Suzie (c) Stefan (d) Crew
(e) Washdc (f) Mobile Calendar (g) Johnny (h) Kristen, and Sara

FIGURE 10. (a-h) Histogram of the original I-Frames of different video sequences.

TABLE 2. Simulation Results of the proposed encryption algorithm for compressed H264 AVC sequences that depends on using chaotic maps.

Sequence type	sequence name	Chaotic map	Performance metrics						
			MSE	PSNR (Original I-frame & Decrypted I-frame)	PSNR (Original I-frame & Encrypted I-frame)	Correlation Coeffect	NPCR	UACI	Elapsed time (Sec)
QCIF	Foreman	Ikeda	1.45×10^3	16.532	8.8041	0.7894	0.0039	3.1904	3.80
		Hénon	2.22×10^3	14.6696	6.682	0.7233	0.0039	3.4889	3.82
		Logistic	4.67×10^2	21.4339	4.7107	0.9474	0.0039	3.1904	3.41
	Suzie	Ikeda	8.13×10^2	19.0324	8.2909	0.7622	0.0039	2.1469	4.02
		Hénon	1.28×10^3	17.0637	7.2028	0.6972	0.0039	3.4031	3.73
		Logistic	640.4779	20.0658	5.9011	0.8159	0.0039	2.1469	4.23
CIF	Stefan	Ikeda	5.44×10^2	20.7719	8.5944	0.8261	9.86×10^{-4}	1.7065	6.87
		Hénon	9.45×10^2	18.3763	7.8998	0.7437	9.86×10^{-4}	2.5375	6.57
		Logistic	1.26×10^2	27.1108	6.8691	0.9495	9.86×10^{-4}	4.0005	6.262
	Crew	Ikeda	8.54×10^2	18.8159	8.0143	0.8423	9.86×10^{-4}	2.3601	7.14
		Hénon	1.32×10^3	16.9186	6.9965	0.7874	9.86×10^{-4}	2.5912	6.87
		Logistic	128.4831	27.0423	5.7372	0.9746	9.86×10^{-4}	3.0211	6.55
C class	Washdc	Ikeda	1.31×10^3	16.9687	8.4616	0.6938	3.26×10^{-4}	2.8521	24.95
		Hénon	1.51×10^3	16.337	6.5717	0.6697	3.26×10^{-4}	2.781	22.42
		Logistic	3.87×10^1	32.2526	4.939	0.9853	3.26×10^{-4}	0.0697	22.60
	Mobile calendar	Ikeda	7.11×10^2	19.6119	7.1907	0.9079	3.26×10^{-4}	1.9651	25.72
		Hénon	858.6638	18.7926	6.5932	0.8945	3.26×10^{-4}	1.8729	21.83
		Logistic	36.0595	32.5606	5.783	0.9949	3.26×10^{-4}	2.5839	33.53
720p	Johnny	Ikeda	145.0234	26.5164	5.9486	0.9814	1.09×10^{-4}	0.405	189.56
		Hénon	858.783	18.792	5.0638	0.9014	1.09×10^{-4}	1.9122	185.73
		Logistic	9.41	38.3961	4.6773	0.9988	1.09×10^{-4}	3.334	183.03
	Kristen and Sara	Ikeda	128.2843	27.0491	5.8057	0.9836	1.09×10^{-4}	0.3624	188.42
		Hénon	724.2939	19.5317	5.0973	0.9153	1.09×10^{-4}	1.8075	220.83
		Logistic	9.2289	38.4793	4.7853	0.9988	1.09×10^{-4}	0.0171	160.86

From the simulation results given in table 2, the PSNR between the original I-frame and encrypted I-frame when the encrypted I-frame using the logistic chaotic map are averagely of 5.30 dB for the QCIF video sequences, 6.30 dB for the CIF video sequences, 5.36 dB for the C clas video sequences and 4.70 dB for the 720p video sequences. As it is evinced in this table, the value of PSNR between original I-frame and encrypted I-frame using the logistic chaotic map is less than that using Ikeda and Hénon chaotic maps. On the other hand, the value PSNR between the original I-frame & decrypted I-frame using the logistic chaotic map is the highest value compared to the PSNR between original I-frame and decrypted I-frame using Ikeda or Hénon chaotic maps, where PSNR between original I-frame and decrypted I-frame are averagely 20.74 dB for the QCIF video sequences, 27.07 d for the CIF video sequences, 32.40 dB for the C class video sequences and 38.84 dB for the 720p video sequences.

The results also show that the MSE metric when the logistic chaotic map was applied to the algorithm was less that when applying the Ikeda or Hénon chaotic maps. The MSE video sequences are averagely: 5.5×10^24 for QCIF, 1.5×10^27 for CIF, 37.384 for C class video sequences, and 9.31 for720p

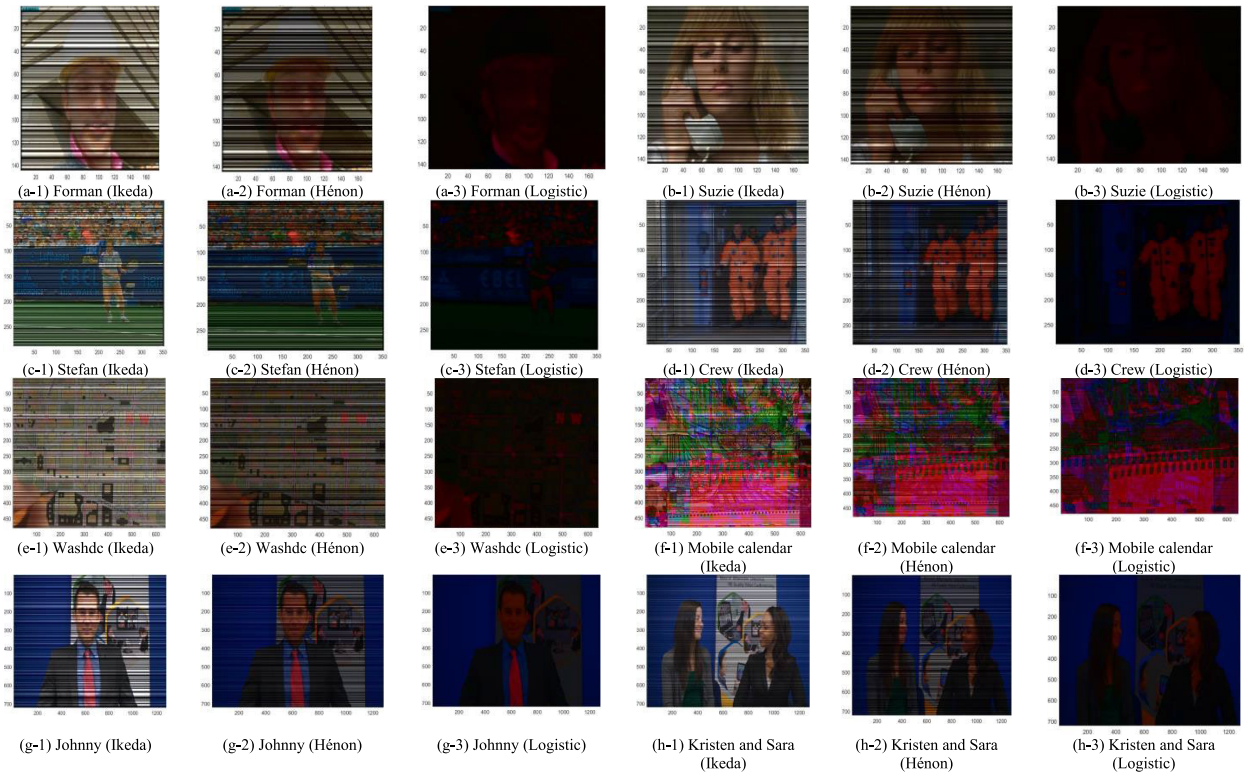


FIGURE 11. **((a-1) -(h-3)) The encrypted I-Frames of different video sequences by using the proposed cryptography algorithm based on different chaotic maps.**

video sequences averagely. For the correlation coefficient, the result of the logistic map is larger than the result of Ikeda and Hénon chaotic maps where the correlation coefficient for QCIF video sequences averagely 0.88, CIF video sequences averagely 0.96, C class video sequences averagely 0.98, and 720p video sequences averagely 0.99.

Fig. 11 (a-h) shows the encrypted I-Frames of different video sequences with different resolutions when using the different chaotic maps. Fig. 12 (a-h) shows the histogram of the encrypted I-Frames of different video sequences with different resolutions when using the different chaotic maps.

As visual in table 3, the proposed algorithm dependent on the logistic chaotic map produces encrypted videos sequences with lower PSNR values between them and their original videos frames comparing to other algorithms in literatures.

TABLE 3. **Performance evaluation results of the proposed algorithm in metric of PSNR compared to the existing state-of-the-art for different videos sequences resolutions.**

Algorithm / sequence	PSNR (dB)			
	QCIF	CIF	C class	720p
Proposed algorithm	5.30	6.30	5.36	4.73
Saurabh Anand [20]	-	13.38	14.73	-
Hassan Elkamchouchi [24]	14.00	-	-	-
Fatma K Tabash [21]	8.10	8.50	8.90	10.40
Hui Xu [25]	10.21	7.60	4.17	-

Different types of attacks are used to assess the robustness of the proposed encryption algorithm based on logistic chaotic map.

The performance measurements to the proposed cryptography algorithm based on logistic map under cropping and pepper and noise attacks are given in table 4 and table 5. As apparent in table 4, the cropping attacks has a negative impact on the quality of the decrypted different resolutions videos frames, in which the different decrypted videos after attack had lower values in metric of PSNR comparing to the results of decryption before attack.

The histograms analysis to different I-frames of various resolutions videos sequences after the decryption by the suggested algorithm dependent on logistic chaotic map under cropping attack are presented in Fig. 13. When the suggested technique was subjected to the cropping attack, the histogram analysis demonstrates flat distribution to the different encrypted videos sequences more than that before the results of different performance metrics to the proposed algorithm based on logistic chaotic map under salt and pepper noise attack are given in table. The results given in this table show that the MSE values between the original videos and the encrypted videos under attack is higher than those without any attack, and the PSNR values of the different decrypted videos are lower than those without attacked.

On the other hand, the histograms analysis of decrypted I-frames by the proposed algorithm for different resolution

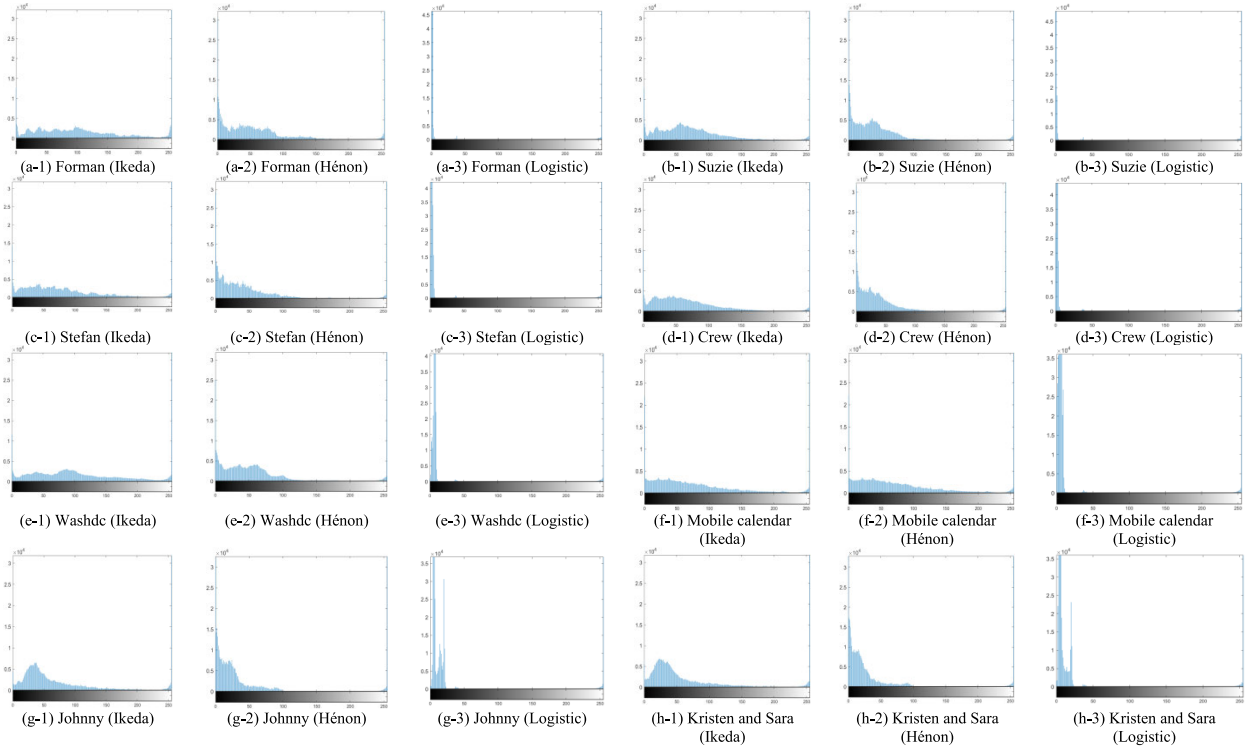


FIGURE 12. **((a-1) -(h-3)) Histogram of the encrypted I-Frames of different video sequences by applying different chaotic maps to the proposed algorithm.**

TABLE 4. **The results of different performance metrics to the proposed cryptography algorithm based on logistic map under cropping attack for different videos sequences.**

Performance metrics	video Sequencies/ name	QCIF		CIF		C Class		720p	
		Foreman	Suzie	Stefan	Crew	Washdc	Mobile calendar	Johnny	Kristen and Sara
MSE		5.15×10^3	7.29×10^3	8.09×10^3	7.61×10^3	5.67×10^3	1.12×10^4	1.51×10^4	1.41×10^4
PSNR (Original I-frame &Decrypted I-frame)		11.01	9.50	9.05	9.32	10.59	7.62	6.35	6.64
PSNR (Original I-frame &Encrypted I-frame)		8.09	7.85	7.77	8.00	7.92	6.94	5.23	5.59
Correlation Coeffect		0.3011	0.1214	0.1783	0.325	0.0075	0.0921	0.0382	-0.0287
NPCR		0.0039	0.0039	9.86×10^{-4}	9.86×10^{-4}	3.26×10^{-4}	3.26×10^{-4}	1.09×10^{-4}	1.09×10^{-4}
UACI		7.3963	14.808	14.234	17.332	-8.372	16.095	21.723	19.419
Elapsed time (sec)		5.04	4.50	7.46	7.62	23.86	23.22	159.57	165.67

video sequences which exposed to the salt and pepper assault are displayed in Fig. 14. The histograms analysis shows the difference when the salt and pepper attack were applied to the proposed algorithm, where it shows obvious deformation compared to proposed algorithm without any attack.

Another attack model conducted to the proposed algorithm is the key sensitivity. In table 6, The simulation results of the proposed algorithm based on a logistic chaotic map when the key parameters for the logistic chaotic map in the decryption process are different than those in the encryption process are given in table 6. The result shows the effect of the changed key parameters for a logistic chaotic map in the decryption process. The PSNR values of decrypted videos when using different key to the key used in encryption process are lower than the PSNR values of decrypted videos using the same key of encryption. Also, as the result of using different key, the MSE values were larger compared to those values when using the same encryption key. Fig.15 show the histogram analysis of decrypted I-frames for different resolution videos sequences using the proposed algorithm that depends on the logistic chaotic map when its key parameters for the decryption and encryption processes are not similar.

The simulation results show that the decrypted I-frames of QCIF video sequences using the proposed algorithm

TABLE 5. The results of different performance metrics to the proposed cryptography algorithm based on logistic map under salt and pepper noise attack for different videos sequences.

Performance metrics	video Sequencies/ name	QCIF		CIF		C Class		720p	
		Foreman	Suzie	Stefan	Crew	Washdc	Mobile calendar	Johnny	Kristen and Sara
MSE		3.29×10^3	5.43×10^3	6.45×10^3	6.39×10^3	4.14×10^3	9.85×10^3	1.28×10^4	1.37×10^4
PSNR (Original I-frame &Decrypted I-frame)		12.96	10.78	10.03	10.07	11.96	8.19	7.05	6.77
PSNR (Original I-frame &Encrypted I-frame)		4.759	5.95	5.84	6.98	5.14	5.97	4.95	5.01
Correlation Coefficient		0.398	0.148	0.227	0.354	0.0376	0.0932	-0.0116	0.057
NPCR		0.0039	0.0039	9.86×10^{-4}	9.86×10^{-4}	3.26×10^{-4}	3.26×10^{-4}	1.09×10^{-4}	1.09×10^{-4}
UACI		-7.264	-14.474	-14.80	-17.925	-9.497	-16.291	-18.127	-20.406
Elapsed time (sec)		4.89	4.00	6.51	6.51	42.52	22.06	200.76	166.60

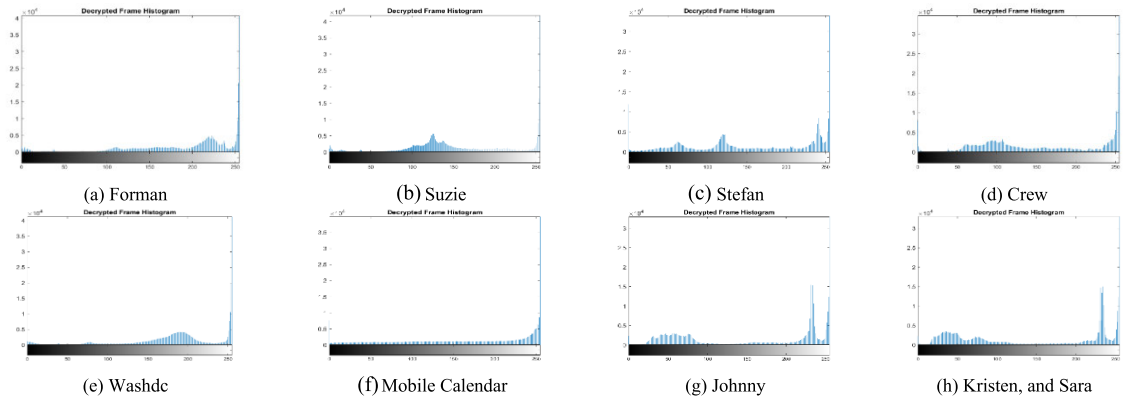


FIGURE 13. (a – n). Histogram of the encrypted I-Frames of different video sequences by applied logistic chaotic maps to the proposed algorithm with applying cropping attack.

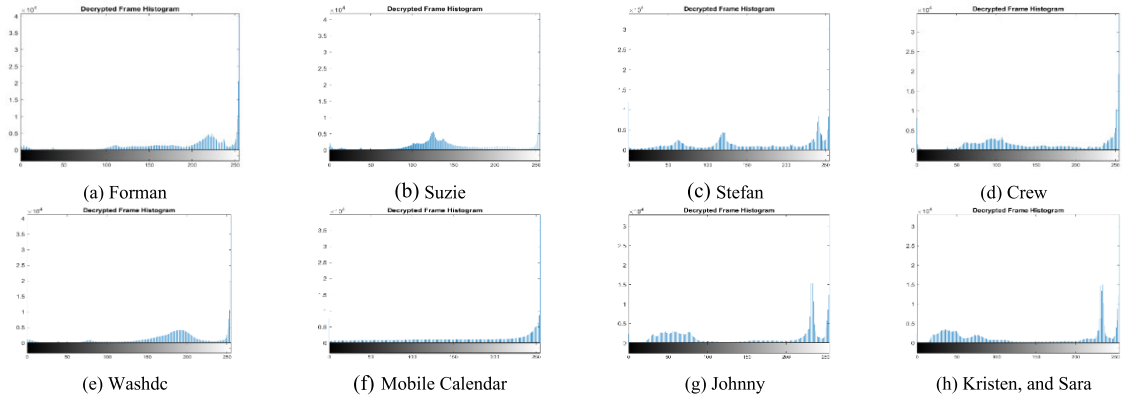


FIGURE 14. (a – h). Histogram of the encrypted I-Frames of different video sequences by applied logistic chaotic maps to the proposed algorithm with applying salt and pepper attack.

dependent on a logistic chaotic map in metric of PSNR are more sensitive to cropping and salt and pepper noise attacks compared to those of the decrypted I-frames of QCIF video sequences using by Hassan Elkamchouchi [24] algorithm. Where, the average PSNR of the decrypted I-frames using the proposed algorithm is smaller than that using the algorithm in literature [24] as depicted in table 7. Meanwhile, the proposed algorithm was more sensitive to changing the key parameters for the logistic chaotic map in the decryption process where the MSE is larger than that with the introduced algorithm in literature [24] for QCIF video sequences as given in table 8.

B. THE PROPOSED HYBRID ALGORITHM OF STEGANOGRAPHY AND CRYPTOGRAPHY BASED CHAOTIC MAPS

Table 9 demonstrates the simulation results of the proposed hybrid algorithm combined both cryptography and steganography that proceeds in two behaviors and its performance

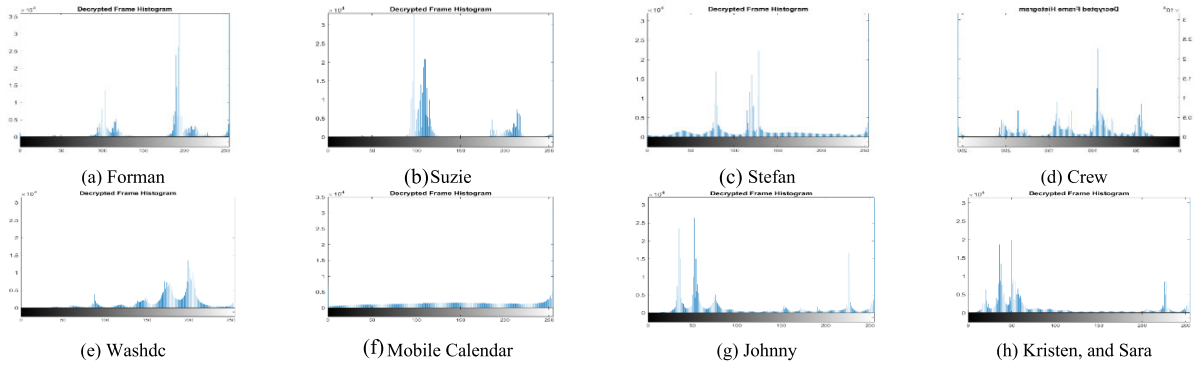


FIGURE 15. (a – h). Histogram of the encrypted I-Frames of different video sequences by using the proposed algorithm based on logistic chaotic map with different key than that used in the decryption process.

TABLE 6. The results of the encrypted I-Frames of different video sequences by using the proposed algorithm based on logistic chaotic map with different key than that used in the decryption process.

Performance metrics / video Sequences/ name	QCIF		CIF		C Class		720p	
	Foreman	Suzie	Stefan	Crew	Washdc	Mobile calendar	Johnny	Kristen and Sara
MSE	3.01×10^4	1.74×10^4	1.79×10^4	1.23×10^4	2.56×10^4	1.51×10^4	1.32×10^4	1.05×10^4
PSNR (Original I-frame &Decrypted I-frame)	3.34	6.25	5.60	7.23	4.04	6.34	6.93	7.90
PSNR (Original I-frame &Encrypted I-frame)	4.68	5.88	5.71	6.84	4.85	5.73	4.53	4.66
Correlation Coefficient	0.075	0.07	0.0647	0.072	0.960	0.98	0.996	0.996
NPCR	0.0039	0.0039	9.86×10^{-4}	9.86×10^{-4}	3.26×10^{-4}	3.26×10^{-4}	1.09×10^{-4}	1.09×10^{-4}
UACI	64.785	46.545	45.267	38.232	61.290	42.983	39.062	33.415
Elapsed time (sec)	3.86	3.98	6.34	6.72	24.25	22.76	161.20	159.89

TABLE 7. Performance evaluations to the proposed algorithm in metric of PSNR under the cropping attack and salt and pepper noise compared with the existing state-of-the-art for QCIF sequences.

algorithm / attack type	PSNR (dB)	
	Side cropping	salt and pepper noise
Hassan Elkamchouchi [24]	25.82	27.41
Proposed algorithm	10.25	11.87

TABLE 8. Performance evaluations to the proposed algorithm in metrics of average MSE, NPCR, and UACI under the key sensitivity attack compared with the existing state-of-the-art for QCIF sequences.

algorithm	measures		
	MSE	NPCR	UACI
Hassan Elkamchouchi [24]	2.32	0.0025	44.80
Proposed algorithm	2.38×10^4	0.0039	64.78

evaluation with the same metrics used in first proposed algorithm besides the SSIM metric. The first behavior is to hide I-frames video sequences of QCIF resolution inside I-frames video sequences of CIF resolution, and the second is to hide I-frames video sequences of C class resolution inside I-frames video sequences of 720 resolution. After that, the cryptography algorithm based on chaotic maps were conducted on the two behaviors.

As shown in table 9 the PSNR between Original I-frame & Decrypted I-frame by the two steganography behaviors and with using logistic chaotic map in encryption process is better than those when using the other chaotic maps. Where, the PSNR between Original I-frame & Decrypted I- frame is averagely 11.78dB to the first steganography behavior and averagely 9.39dB to the second behavior. while the PSNR between Original I-frame & Encrypted I-frame for first and second behaviors and with using the logistic chaotic map in encryption process is less than other chaotic maps where the PSNR between Original I-frame & encrypted I- frame is averagely 4.56dB to fist behavior and is averagely 5.57dB to the second behavior. The encrypted I-frames for the two steganography styles (QCIF is hidden in CIF) and (Class C is hidden in 720p) when the different chaotic maps were applied are show in Fig. 16. The encrypted I-frames based on the logistic chaotic map seem to be more distorted than those based on IKEDA and Hénon chaotic maps.

The comparison results of the proposed steganography algorithm with the competitive steganography algorithm of

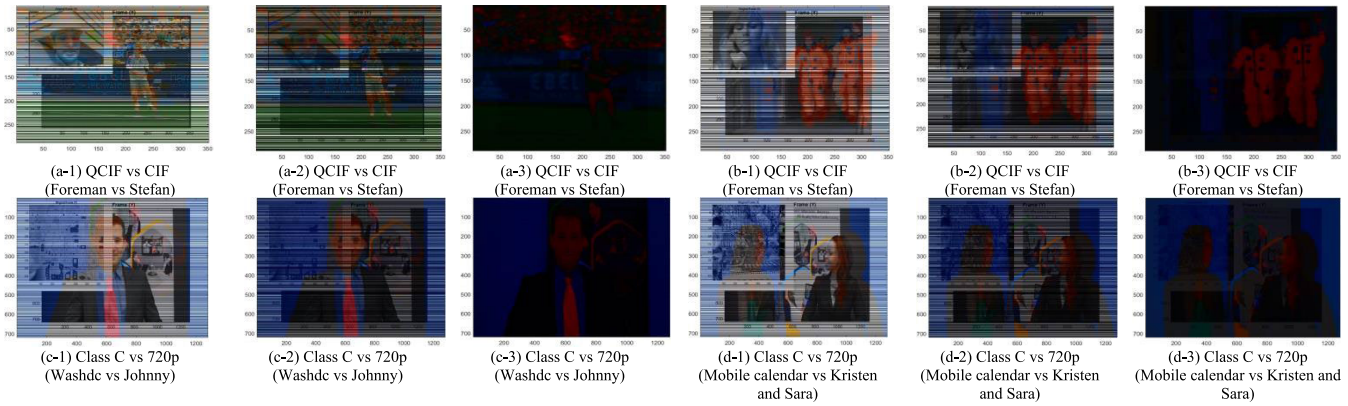


FIGURE 16. (a-1) – (c-3)). The encrypted low resolution I-Frames video sequences inside high resolution I-Frames video sequences by applied chaotic maps to the proposed algorithm.

TABLE 9. Simulation Results of the proposed hybrid algorithm combining steganography algorithm and the encryption algorithm based on different chaotic maps for the compressed H264 AVC videos sequence.

video sequence	Chaotic map	performance metrics	MSE	PSNR (Original I-frame & Decrypted I-frame)	PSNR (Original I-frame & Encrypted I-frame)	Correlation Confident	NPCR	SSIM	UACI	Elapsed time(sec)
QCIF vs CIF (Foreman vs Stefan)	Ikeda		3.87×10^{3}	11.25	8.83	0.4	0.0039	0.0611	-10.0176	6.58
	Hénon		4.33×10^{3}	11.76	6.83	0.37	0.0039	0.0516	-10.0115	6.80
	Logistic		5.03×10^{3}	12.12	4.69	0.35	0.0039	0.0345	-13.2743	6.37
QCIF vs CIF (Suzie vs Crew)	Ikeda		4.76×10^{3}	11.35	4.70	0.031	3.26×10^{-4}	1.64×10^{-2}	-11.9995	29.55
	Hénon		4.81×10^{3}	11.31	4.80	0.025	3.26×10^{-4}	1.58×10^{-2}	-11.6721	29.07
	Logistic		4.81×10^{3}	11.45	4.44	0.023	3.26×10^{-4}	1.46×10^{-2}	-12.248	29.46
Class C vs 720p (Washdc vs Johnny)	Ikeda		6.83×10^{3}	9.78	6.18	0.12	0.0039	0.032	-16.9595	6.21
	Hénon		7.24×10^{3}	9.54	4.68	0.13	0.0039	0.029	-16.7705	5.73
	Logistic		8.56×10^{3}	10.81	4.67	0.12	0.0039	0.017	-19.812	5.68
Class C vs 720p (Mobile calendar vs Kristen and Sara)	Ikeda		1.11×10^{4}	7.69	7.31	0.09	3.26×10^{-4}	4.58×10^{-2}	-18.918	34.85
	Hénon		1.12×10^{4}	7.65	8.83	0.09	3.26×10^{-4}	9.73×10^{-3}	-18.3382	30.64
	Logistic		1.11×10^{4}	7.97	6.83	0.09	3.26×10^{-4}	2.59×10^{-2}	-19.2082	29.13

TABLE 10. Performance evaluation of the proposed steganography algorithm compared with the existing state-of-the-art algorithm to CIF video sequences in metrics of average PSNR and SSIM values.

algorithm	sequence	CIF	
		PSNR	SSIM
Proposed algorithm		11.21	0.253
Dawen Xu [23]		11.3	0.024

Dawen Xu introduced in [23] are given in table 10. The results given in this table show that the value of PSNR of decrypted frames of the proposed steganography algorithm decrease than the average PSNR of the decrypted frames by the steganography algorithm introduced in [23] to CIF video sequences. The SSIM has the best result where the average value of SSIM of the proposed steganography algorithm to CIF video sequences is higher that SSIM value utilizing Dawen Xu [23] steganography method as debicted in table 10.

VII. CONCLUSION

In this paper, for steganography and cryptography processes of different I-frames with different resolutions of compressed videos sequences H.264/AVC, two methods of the Chaos-based encryption methodology are presented. The two suggested algorithms' implementation on the luminance component of the various test compressed video sequences was done using the MATLAB software. In comparison to IKEDA and Henon chaotic maps, the suggested technique that relies on employing a logistic chaotic map has the best average of various performance metrics values, and the strength of the proposed cryptographic algorithm was illustrated under the implementation of several attacks. With the comparison to state-of-the-art algorithms, the suggested steganography methodology demonstrated the best SSIM value.

REFERENCES

[1] Z. Su, S. Lian, G. Zhang, and J. Jiang, *Chaos-Based Cryptography: Theory, Algorithms and Applications* (Studies in Computational Intelligence), vol. 354. Berlin, Germany: Springer-Verlag, 2010, ch. 6, pp. 205–226.

[2] I. E. Richardson, *The H.264 Advanced Video Compression Standard*, 2nd ed. Aberdeen, U.K.: Vcodex, 2010, ch. 6, pp. 283–284.

[3] T. Stutz and A. Uhl, "A survey of H.264 AVC/SVC encryption," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 22, no. 3, pp. 325–339, Mar. 2012.

[4] X. Zhang, H. Deng, and L. Chen, "The video encryption scheme based on perceptual encryption algorithm in H.264 standards," in *Proc. 2nd Int. Conf. Syst. Eng. Modeling (ICSEM)*, 2013, pp. 148–152.

[5] B. Boyadjis, C. Bergeron, B. Pesquet-Popescu, and F. Dufaux, "Extended selective encryption of H.264/AVC (CABAC)- and HEVC-encoded video streams," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 27, no. 4, pp. 892–906, Apr. 2017.

[6] O.-Y. Lui and K.-W. Wong, "Chaos-based selective encryption for H.264/AVC," *J. Syst. Softw.*, vol. 86, no. 12, pp. 3183–3192, Dec. 2013.

[7] N. Kumar, D. Wadhwa, D. Tomer, and S. Vijayalakshmi, "Review on different chaotic based image encryption techniques," *Int. J. Inf. Comput. Technol.*, vol. 4, no. 2, pp. 197–206, 2014.

[8] S. Mohammadi, "A chaos-based video watermarking in wavelet domain," *Ciência Natura*, vol. 37, no. 6, pp. 364–370, 2015.

[9] N. Khlif, A. Masmoudi, F. Kammoun, and N. Masmoudi, "Secure chaotic dual encryption scheme for H.264/AVC video conferencing protection," *IET Image Process.*, vol. 12, no. 1, pp. 42–52, Jan. 2018.

[10] M. A. Taha, W. Hamidouche, N. Sidaty, M. Viitanen, J. Vanne, S. E. Assad, and O. Deforges, "Privacy protection in real time HEVC standard using chaotic system," *Cryptography*, vol. 4, no. 2, p. 8, Jun. 2020.

[11] Y. Hu and R. Tian, "Image encryption and decryption based on chaotic algorithm," *J. Appl. Math. Phys.*, vol. 8, no. 9, pp. 1814–1825, 2020.

[12] M. Hussain and M. Hussain, "A survey of image steganography techniques," *Int. J. Adv. Sci. Technol.*, vol. 54, pp. 1–12, May 2013.

[13] M. Dalal and M. Juneja, "H.264/AVC video steganography techniques: An overview," *Int. J. Comput. Sci. Eng.*, vol. 6, no. 5, pp. 297–303, May 2018.

[14] Y. Liu, S. Liu, Y. Wang, H. Zhao, and S. Liu, "Video steganography: A review," *Neurocomputing*, vol. 335, pp. 238–250, Mar. 2019.

[15] G. Xie, J. Ren, S. Marshall, H. Zhao, and H. Li, "A new cost function for spatial image steganography based on 2D-SSA and WMF," *IEEE Access*, vol. 9, pp. 30604–30614, 2021.

[16] Y.-H. Chuang, B.-S. Lin, Y.-X. Chen, and H.-J. Shiu, "Steganography in RGB images using adjacent mean," *IEEE Access*, vol. 9, pp. 164256–164274, 2021.

[17] M. Suresh and I. S. Sam, "Optimized interesting region identification for video steganography using fractional grey wolf optimization along with multi-objective cost function," *J. King Saud Univ., Comput. Inf. Sci.*, vol. 34, no. 6, pp. 3489–3496, Jun. 2022.

[18] Y. Chung, S. Lee, T. Jeon, and D. Park, "Fast video encryption using the H.264 error propagation property for smart mobile devices," *Sensors*, vol. 15, no. 4, pp. 7953–7968, Apr. 2015.

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

[20] S. Anand and A. S. Jalal, "An efficient steganographic approach for H.264/AVC compressed videos," *Int. J. Eng. Res. Comput. Sci. Eng.*, vol. 5, no. 2, pp. 344–348, Feb. 2018.

[21] F. K. Tabash and M. Izharuddin, "Efficient encryption technique for H.264/AVC videos based on CABAC and logistic map," *Int. J. Informat. Commun. Technol.*, vol. 7, no. 1, pp. 39–48, Apr. 2018.

[22] J. Wang, X. Jia, X. Kang, and Y.-Q. Shi, "A cover selection HEVC video steganography based on intra prediction mode," *IEEE Access*, vol. 7, pp. 119393–119402, 2019.

[23] D. Xu, "Commutative encryption and data hiding in HEVC video compression," *IEEE Access*, vol. 7, pp. 66028–66041, 2019.

[24] H. Elkamchouchi, W. M. Salama, and Y. Abouelseoud, "New video encryption schemes based on chaotic maps," *IET Image Process.*, vol. 14, no. 2, pp. 397–406, Jan. 2020.

[25] H. Xu, X. Tong, Z. Wang, M. Zhang, Y. Liu, and J. Ma, "Robust video encryption for H.264 compressed bitstream based on cross-coupled chaotic cipher," *Multimedia Syst.*, vol. 26, no. 4, pp. 363–381, 2020.

[26] L. Zhang and D. Chen, "The large capacity embedding algorithm for H.264/AVC intra-prediction mode video steganography based on linear block code over Z4," *Multimedia Tools Appl.*, vol. 79, pp. 12659–12677, Jan. 2020.

[27] O. F. A. Wahab, A. A. M. Khalaf, A. I. Hussein, and H. F. A. Hamed, "Hiding data using efficient combination of RSA cryptography, and compression steganography techniques," *IEEE Access*, vol. 9, pp. 31805–31815, 2021.

[28] J. Yang and A. Wei, "Fast mode decision algorithm for intra prediction in HEVC," in *Proc. IEEE 4th Inf. Technol., Netw., Electron. Automat. Control Conf. (ITNEC)*, Jun. 2020, p. 1018–1022.

[29] M. A. El-Mowafy, S. M. Gharghory, M. A. Abo-Elsoud, M. Obayya, and M. I. F. Allah, "Efficient mode decision scheme based on edge detection with Gaussian pulse for intra-prediction in H.264/AVC," *Alexandria Eng. J.*, vol. 61, no. 4, pp. 2709–2722, 2022.

[30] U. Sara, M. Akter, and M. S. Uddin, "Image quality assessment through FSIM, SSIM, MSE and PSNR—A comparative study," *J. Comput. Commun.*, vol. 7, no. 3, pp. 8–18, 2019.

[31] U. Zia, M. McCartney, B. Scotney, J. Martinez, M. AbuTair, J. Memon, and A. Sajjad, "Survey on image encryption techniques using chaotic maps in spatial, transform and spatiotemporal domains," *Int. J. Inf. Secur.*, vol. 21, no. 4, pp. 917–935, Aug. 2022.

[32] V. Aboites, D. Liceaga, A. Kiryanov, and M. Wilson, "Ikeda map and phase conjugated ring resonator chaotic dynamics," *Appl. Math. Inf. Sci.*, vol. 10, no. 6, pp. 2071–2076, Nov. 2016.

[33] R. Anandkumar and R. Kalpana, "Analyzing of chaos based encryption with Lorenz and Henon map," in *Proc. 2nd Int. Conf. I-SMAC (IoT Social, Mobile, Analytics Cloud) (I-SMAC)I-SMAC (IoT Social, Mobile, Analytics Cloud) (I-SMAC), 2nd Int. Conf.*, Aug. 2018, pp. 204–208.

[34] S. S. Hassan, Z. Iqbal, M. J. Ikram, and M. Ishaque, "Henon chaotic map-based image encryption scheme using bit-level circular shift," *J. Theor. Appl. Inf. Technol.*, vol. 100, no. 6, pp. 1960–1973, 2022.

[35] Y. Pourasad, R. Ranjbarzadeh, and A. Mardani, "A new algorithm for digital image encryption based on chaos theory," *Entropy*, vol. 23, no. 3, p. 341, Mar. 2021.

[36] M. Sharma, R. K. Ranjan, and V. Bharti, "Image encryption using chaotic maps: A survey," in *Soft Computing: Theories and Applications* (Lecture Notes in Networks and Systems), vol. 425. Berlin, Germany: Springer-Verlag, 2022, pp. 835–844.

M. A. EL-MOWAFY received the B.S. degree in electronics and communications engineering and the M.S. degree in signal processing engineering from the Faculty of Engineering, Mansoura University, Mansoura, Egypt, in 2008 and 2014, respectively. He is currently pursuing the Ph.D. degree in video signal processing with Mansoura University.

From 2008 to 2014, he was a Demonstrator with the Communications and Electronics Department, Faculty of Engineering, Mansoura University. Since 2014, he has been a Researcher Assistant with the Computers and Systems Department, Electronics Research Institute, Cairo, Egypt. His research interests include video signal processing and compression.

S. M. GHARGHORY received the B.S., M.Sc., and Ph.D. degrees in electronics and communications engineering from the Faculty of Engineering, Cairo University, Egypt.

She was an Associate Professor with the Computers and Systems Department, Electronics Research Institute, Dokki, Cairo, Egypt, in 2013. Her research interests include digital image and signal processing, digital image and video watermarking, pattern recognition and classification, artificial intelligence, and evolutionary computation, such as GA and fuzzy logic, swarm intelligence and natural inspired intelligence, intelligent control and robotics systems, fault detection, and identification and the application of convolution neural network for time series prediction and classification.

M. A. ABO-ELSOUD received the M.Sc. degree from the Electronics and Communication Engineering Department, Cairo University, Cairo, Egypt, in 1979, and the Ph.D. degree from the L'Institut National Polytechnique de Toulouze, Toulouze, France, in 1983.

He worked with the Technical Research Center (TRC), from 1970 to 1990. During 1984–1990, he was the Chairman with the Electronics Department, TRC. From 1991 to 1996, he was an Associate Professor at Mansoura University. He has been a Full Professor with the ECE Department, Mansoura University, since 1996. He has authored or coauthored more than 103 in international journals and conferences. His research interests include analog/digital VLSI and FPGA circuit design, sigma/delta A/D techniques, switched-resistor networks, and electronic systems for neural networks.

M. OBAYYA received the B.Sc. degree in electronics and communications engineering from the Faculty of Engineering, Mansoura University, Mansoura, Egypt, in 2001, and the M.Sc. and Ph.D. degrees from the Department of Electronics and Communications Engineering, Faculty of Engineering, Mansoura University, in 2005 and 2008, respectively.

She is currently an Associate Professor at the Electronics and Communications Engineering Department, Faculty of Engineering, Mansoura University. She is also the Director of the Communications Engineering Program, Electrical Engineering Department, Princess Nora bint Abdurrahman University, Riyadh, Saudi Arabia. She has several publications in the biomedical engineering, optimization, and intelligent machine learning. Her research interests include image processing, signal processing, optimization, and machine learning.

M. I. FATH ALLAH received the B.S. degree in electronics and communications engineering, the M.S. degree in optical communications, and the Ph.D. degree in optical encryption of images (development of optical encryption techniques) from the Faculty of Engineering, Mansoura University, Mansoura, Egypt, in 2007, 2012, and 2017, respectively.

From 2007 to 2010, he was a Demonstrator with the Communications and Electronics Department, Faculty of Engineering, Mansoura University. From 2010 to 2012, he worked as a Demonstrator with the Communications and Electronics Department, Delta Higher Institute for Engineering and Technology, Mansoura. From 2012 to 2017, he worked as an Assistant Lecturer with the Communications and Electronics Department, Delta Higher Institute for Engineering and Technology. Since 2017, he has been an Assistant Professor with the Communications and Electronics Department, Delta Higher Institute for Engineering and Technology. He has 12 publications in various international journals and conferences. His current research interests include multimedia processing, encryption, wireless communication systems, and field programmable gate array (FPGA) applications.