Research Article

Asmaa Hasan Alrubaie*, Maisa' A. Abid Ali Khodher, and Ahmed Talib Abdulameer

Modification of the 5D Lorenz chaotic map with fuzzy numbers for video encryption in cloud computing

https://doi.org/10.1515/eng-2024-0051
received March 16, 2024; accepted May 17, 2024

Abstract: As surveillance cameras have proliferated in usage, their widespread deployment has raised privacy concerns. We introduce an inventive strategy to safeguard privacy in surveillance videos to address these concerns. This article designs a secure system for detecting and encrypting regions of interest (ROIs) that depict multiple individuals within video footage. The suggested system is composed of three phases, with the initial phase incorporating an object detection model to efficiently detect individuals in video frames with the You Only Look Once version 7 architecture. The second stage encrypts ROIs with our unique algorithm, which represents a novel technique derived from combining triple DNA with the modification of the 5D Lorenz chaotic map using fuzzy triangular numbers, which are utilized in key generation. The reverse of this process is a decryption that obtains the original video. The third stage combines all encrypted ROIs from the reconstructed video frames to be securely stored as encrypted video in the cloud. Evaluation results show that the utmost value of the unified averaged changed intensity and the number of changing pixel rate stand at 33.8000 and 99.8934%, respectively, with encryption and decryption speeds up to 7.06 and 6.72 s, respectively.

Keywords: object detection, object encryption, YOLOv7, 5D Lorenz chaotic map, 3DNA coding

*** Corresponding author: Asmaa Hasan Alrubaie,** Computer Sciences Department, University of Technology Iraq, Baghdad, Iraq, e-mail: cs.20.41@grad.uotechnology.edu.iq
Maisa' A. Abid Ali Khodher: Computer Engineering Department, University of Technology-Iraq, Baghdad, Iraq
Ahmed Talib Abdulameer: IT Department, Middle Technical University, Baghdad, Iraq

1 Introduction

In recent years, there has been a surge of interest in object encryption, largely spurred by an escalating transfer of videos over networks. Ensuring the security of these videos is imperative to thwart unauthorized access and to safeguard sensitive information, which has prompted significant research efforts in academic and practical domains. Video surveillance systems that are frequently deployed in high-security environments have been pivotal in driving the evolution of object detection methods for encryption [1].

Surveillance video encryption offers a promising approach to enhancing the privacy and security of video recordings. Two strategies exist for applying encryption techniques to surveillance videos: encrypting the complete video and selectively encrypting solely the regions of interest (ROIs) containing confidential data. Encrypting the entire video [2], as previously discussed, may not always be warranted, especially in the case of public areas where the data is not considered sensitive. Comprehensive encryption can also require substantial computational resources and time. Consequently, a more efficient approach involves encrypting only the ROIs, while leaving non-ROI regions unencrypted [3] to optimize the production of protected surveillance videos.

DNA cryptography suggests an interesting potential for enhancing object encryption in surveillance videos transmitted over networks. With its computational power and the intricate dynamics rooted in chaos theory, the approach can be a valuable resource in the field of cryptography. Specifically, DNA cryptography can produce pseudo-random sequences to serve as encryption keys. This encryption process encompasses the two key steps of scrambling and diffusion. In scrambling, pixel positions across video frames are adjusted based on the encryption key, while diffusion alters pixel values. These two operations work synergistically to generate a novel encoded structure that differs from the original video [4].

In this article, we introduce a novel video encryption approach that combines triple DNA with the modification of the 5D Lorenz chaotic map using fuzzy triangular numbers. The incorporation elevates the level of security and improves video encryption effectiveness by harnessing high diffusion achieved through a scrambling operation and the incorporation of DNA coding within the chaotic system. The noteworthy outcomes of this research include:

- Presents a fresh surveillance video. An encryption and decryption scheme is proposed, aiming for reduced time and memory requirements alongside heightened efficiency. The design emphasizes enhanced security, ensuring reduced correlation coefficients among neighboring pixels in the encrypted video.
- Proposes a novel method to perform video encryption that combines a triple DNA and anew 5D Lorenzo chaotic system. These methods are compared with recent approaches as baselines.
- Generates an exceptionally sensitive key for encrypting and decrypting videos through the proposed 5D Lorenzo map system with fuzzy number, which are utilized in keys generation. This system presents additional benefits compared to a basic chaotic system, including a broader parameter space, increased randomization, and a multitude of chaotic sequences.
- The keys generated by the modified 5D Lorenzo map pass all 15 tests in the National Institute of Standards and Technology (NIST) statistical test suite. These produced keys are then utilized for video encryption. The resulting encrypted video undergoes a security analysis using methods such as histogram analysis, correlation, and information entropy.

The remainder of the article consists of sections covering the literature review, theoretical background, research method, experiment process, and results and discussion, followed by our summary and conclusions.

2 Literature review

In their 2018 work, Zhang *et al.* proposed using DNA sequences for privacy protection in surveillance videos, specifically focusing on safeguarding RoI within the videos. Instead of encrypting the entire video, they advocate for only the areas containing sensitive information. This is a more efficient approach to reduce computational costs and meet real-time video transmission requirements. While conventional cryptographic technologies like AES and RSA are commonly used for privacy protection, they may not be well-suited to the specific needs of surveillance videos. Hence, researchers have explored alternative methods, including the unique approach of utilizing DNA sequences for video encryption, which has shown effectiveness beyond traditional cryptographic technologies in this context [5].

In 2020, Shao proposed an image encryption algorithm for torsional components of generators based on a complex chaotic model. This method involves extracting the RGB torsional vibration component of the image for discrete cosine transform transformation; it is then rotated and fused to complete the initial encryption of the image information. In order to further enhance the security of image information, the image information complex, chaotic encryption model is constructed according to the coding result, so as to eliminate the strong correlation between the adjacent pixels. Particle swarm optimization is used to co-ordinate and optimize the parameters of the compound chaotic encryption model to improve the encryption performance of the model. Experimental results show that the pixel has low correlation, high security, and strong ability to resist attacks after encrypting with this algorithm [6].

In a study published in 2020, Darwich *et al.* suggested using cloud storage for storing videos intended for specific audiences. Cloud computing, known for its processing power, extensive storage capacity, and fast computation speed, has gained popularity among various entities. However, it also raises security concerns, including confidentiality, data integrity, and availability. Ensuring authentication and authorization for data access is crucial, given that cloud storage comprises distributed supercomputers worldwide [7].

3 Theoretical background

3.1 You Only Look Once version 7 (YOLOv7) algorithm

The latest advancement in architecture for object detection is YOLOv7, which is within the You Only Look Once series. Anticipated to establish itself as the industry norm for object detection [8,9]. YOLOv7 architecture consists of three main components, as shown in Figure 1.

1. Backbone: A convolutional neural network generates image features.
2. Neck: An assemblage of neural network layers that blends and integrates features before forwarding them to the subsequent stage for prediction.
3. Head: Utilizes features from the bottleneck to generate prediction outputs.

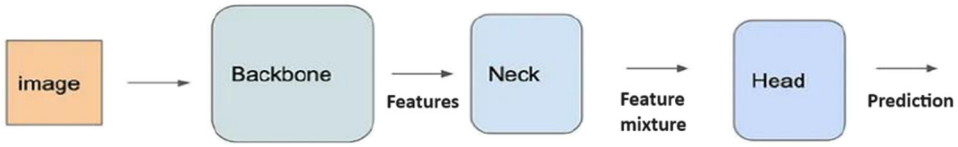

Figure 1: YOLOv7 architecture [10].

3.2 Fuzzy numbers

In this section, we provide some introductory information on fuzzy numbers, although there are slight variations in the definitions of fuzzy numbers. In this work, we define a fuzzy number as a function f: $X \to [0,1]$, where X is a set within the real numbers ($\mathbb{R}$), with the following characteristics:

- It is a regular fuzzy set, implying the existence of at least one $x \in X$ such that $f(x) = 1$.
- The function f is piecewise continuous.

It is worth noting that in certain studies, fuzzy numbers are defined with a unique x_0, such that $f(x_0) = 1$. However, the fuzzy numbers under consideration in this context are defined as f: $[0, 1] \to [0, 1]$ and take on a triangular form:

$$f_z(x) = \begin{cases} \dfrac{x}{z}, & 0 \le x \le z \\ \dfrac{1-x}{1-z}, & z \le x \le 1. \end{cases} \tag{1}$$

In this context, z denotes the peak of the triangular fuzzy number. Figure 2 provides examples for different values of z [11,12].

3.3 Lorenz chaotic mapping

Chaotic maps play a significant role in the study of dynamic nonlinear systems. The Lorenz mapping is a typical example of chaotic mapping in chaotic systems, and it is described by the system's dynamic equations:

$$x = a(y - x), \tag{2}$$

$$y = xz + \beta x - y, \tag{3}$$

$$z = xy - \gamma z. \tag{4}$$

Incorporated into the mapping are system parameters, commonly assigned values of 10, 28, and 8/3. Should these values remain unchanged, the system undergoes collapse once the criterion of 24.74 is satisfied. The Lorenz system produces chaotic sequences characterized by a more intricate system structure compared to low-dimensional ones. This complexity allows for the generation of chaotic sequences involving either a single variable or multiple variables, showcasing a high degree of flexibility in sequence design [13].

3.4 DNA encoding

Understanding DNA sequences is indispensable in fundamental biological research and practical applications across various fields such as diagnostic, forensic, biotechnological, and biological systematics. A DNA sequence consists of four different nucleic acids: thymine (T), adenine (A), guanine (G), and cytosine (C). These nucleic acids adhere to specific base pairing rules, where purine adenine (A) consistently pairs with pyrimidine thymine (T), and pyrimidine cytosine

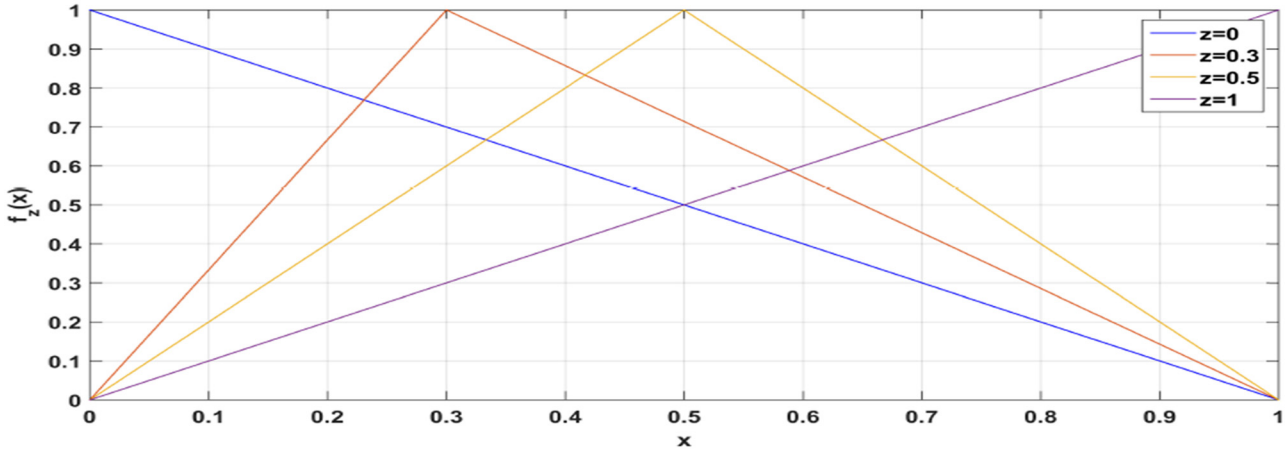

Figure 2: Illustrations of fuzzy trigonometric numbers for z = 0, 0.3, 0.5, 1 [11].

Figure 3: A simple DNA structure [13].

(C) consistently pairs with purine guanine (G) [14]. This complementary base pairing is illustrated in the basic structure of DNA depicted in Figure 3 [15].

The connections between these bases are referred to as the Watson–Crick base pairing rules, named in honor of the scientists who uncovered their structural basis. Analogous to the complementary nature of 0 and 1 in the binary system, 01 and 10 can also be observed to be complementary, just as 00 and 11 are. Table 1 presents the rules for decoding and coding mapping in the specific context of a DNA series employed within this research. Conversely, Table 2 illustrates the XOR procedure applied to DNA arrangements to conform to the Watson–Crick base pairing rules [15].

4 Research method

In this section, the provided approach is outlined, elucidating each sequential step. The initial stage employs YOLOv7 to process the video surveillance, identifying the ROIs within every frame. After pinpointing each ROI, they undergo encryption to secure the sensitive data they encapsulate using a new 5D Lorenzo chaotic system. In the next stage, the coded ROIs are seamlessly reintegrated back to their original positions within the frames of the video. Finally, the encrypted video is uploaded to the cloud for storage and subsequent access. A visual overview of the entire process is illustrated in Figure 4.

Table 2: XOR operations for the DNA sequence pairing rules

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

4.1 Object detection process

The proposed approach presents an effective strategy to minimize the processing time necessary for object detection in videos by utilizing YOLOv7 and incorporating the “remove duplicate frames” method. This method leverages zero difference approaches (ZDAs) to detect and remove frames that contain identical content, thereby eliminating those frames with a difference of zero. After implementing ZDA, the proposed method continues with the YOLOv7 algorithm, resulting in object detection denoted by bounding boxes around the identified objects.

4.2 Encryption process

The suggested video encryption scheme is outlined in a step-by-step manner in Figure 5.

4.2.1 ROIs scrambling algorithm

To enhance the security of the encryption technique, image scrambling operations are employed to disrupt the correlation between adjacent pixels. Specifically, the scrambling process is applied to an ROI denoted as I, with dimensions ($M \times N$). In this context, M denotes the height, and N denotes the width of the ROI. Algorithm 1 outlines the procedure for creating a scrambled ROI, denoted as I', by utilizing a chaotic key (k) that serves as an arbitrary matrix.

Table 1: Rules for mapping the encoding and decoding of DNA

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

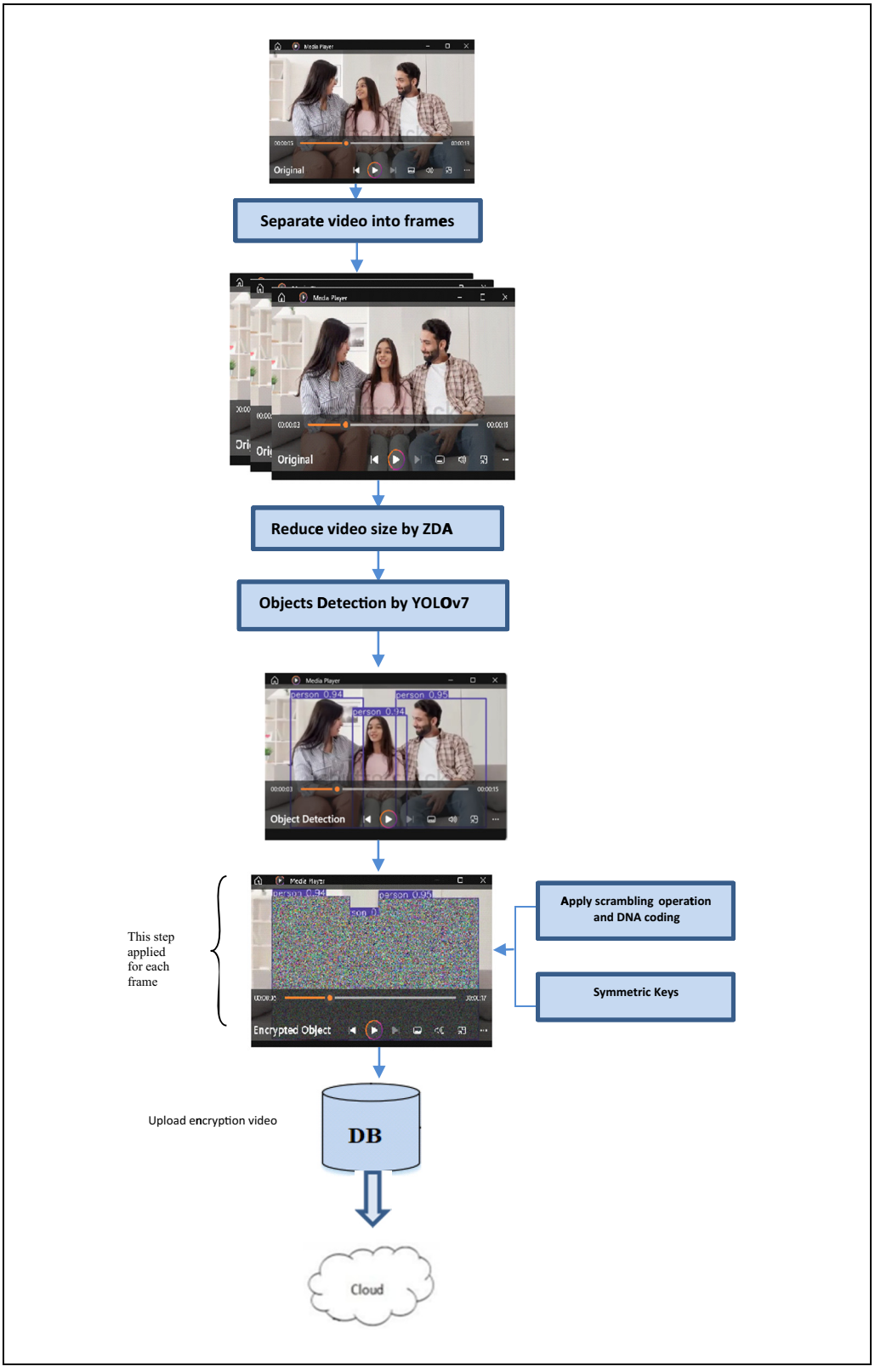

Figure 4: The general framework of the proposed method to detect and encrypt ROIs [16].

Algorithm 1: The Scrambling Pixels Algorithm

Input: I (i, j), ROI of video with dimension ($M \times N$), scrambling key (k).
Output: I' (i, j), the scrambled ROI.
Begin:
Step 1: Generate chaotic sequence K with a random function. The sequence length is $K0 = M \times N$.
Step 2: Transform the digital ROI matrix I, with dimensions $M \times N$, into a one-dimensional sequence P with a length of $M \times N$. $P = (p(1), p(2), \ldots, p(MN))$.
Step 3: Organize the chaotic sequence K in ascending order to derive the index sequence B. Consequently, the size of B, along with its updated index sequences, becomes $1 \times MN$.
Step 4: Shuffle the array P based on the index sequence B to generate a new array Q, where $Q(i) = P(B(i))$, for $i = 1, 2, 3, \ldots, M \times N$.
Step 5: Transform the one-dimensional array Q into an ROI matrix I' with dimensions $M \times N$.
Step 6: Repeat steps 2 through 5 until all ROIs across all video frames are scrambled.
End.

4.2.2 ROIs video triple DNA encoding

The subsequent phase involves the application of 3DNA coding to the permutation outcome obtained in the preceding step. The RGB-scrambled ROI is divided into its

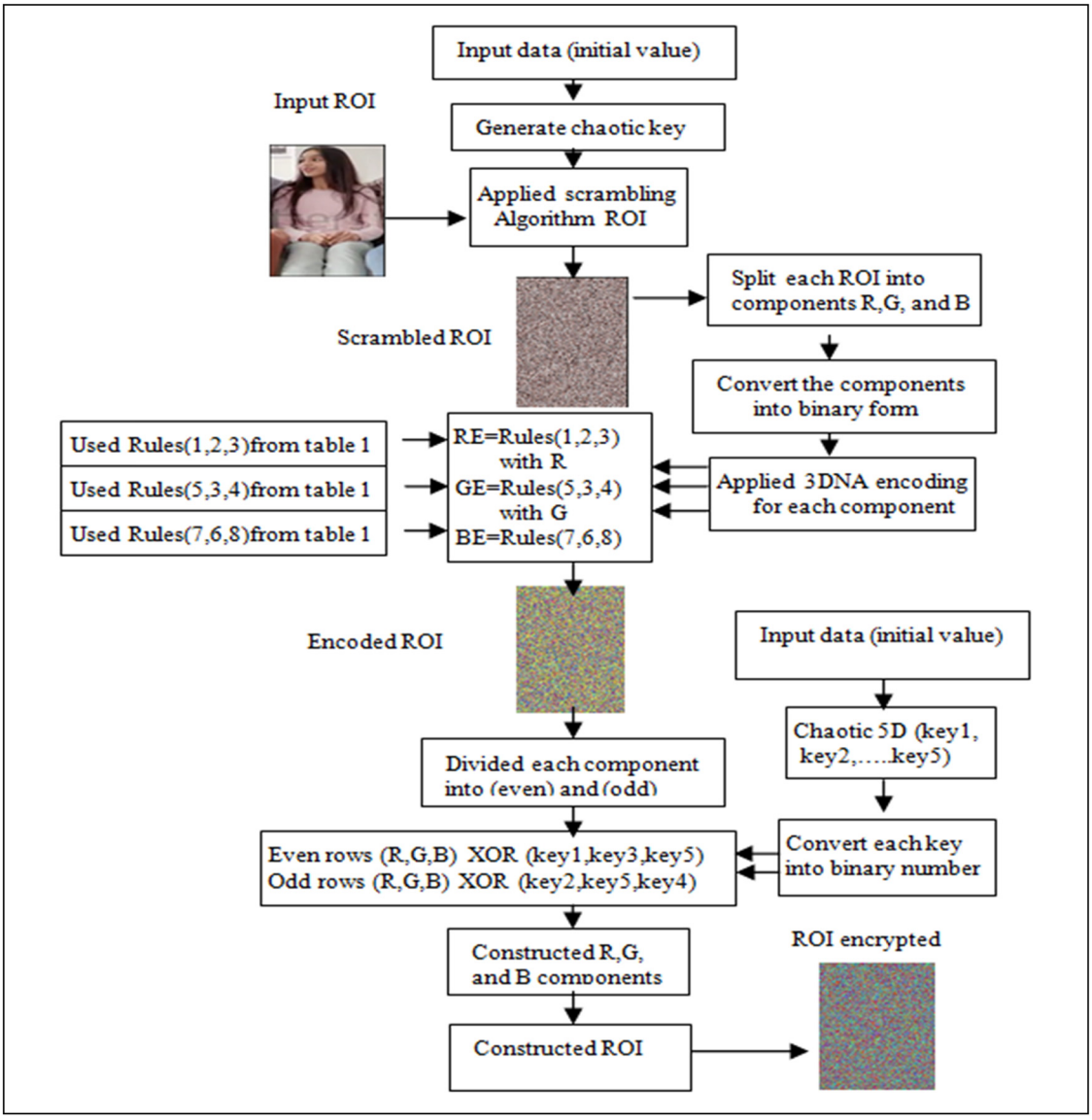

Figure 5: A workflow visualization for the general steps of the encryption process [16].

three constituent parts: R (red), G (green), and B (blue). Each component is individually converted into binary numbers, where each pair of bits is mapped to any of the DNA symbols: A, C, G, or T, following the randomly selected rules listed in Table 1. This transformation adheres to rules (1, 5, 7) outlined in Table 1, yielding the three encoding elements of Rc, Gc, and Bc. Following, the second round of Rc, Gc, and Bc components is encoded based on rules (2, 3, 6). This step produces three additional encoding components: Rcc, Gcc, and Bcc.

In another subsequent phase, a third round of Rcc, Gcc, and Bcc components are encoded based on rules (3, 4, 8). This step generates three more encoding components of Rccc, Gccc, and Bccc. Finally, these three encoding components are combined to create a unified ROI representing the encoded ROI.

4.2.3 Generating keys through a new 5D Lorenzo chaotic system

A novel 5D chaotic system with fuzzy numbers incorporating differential dynamic equations has been introduced to explore chaotic properties and produce a series of numerical output sequences. Figure 6 displays the chaotic attractors in each plane of the 5D Lorenz chaotic map.

$$X[i+1] = f_z(x[i] + (-s \times x[i] + y[i] \times k[i] - r \times p[i])) \times \mathrm{d}t, \tag{5}$$

$$Y[i+1] = y[i] + f_z(-y[i] - x[i] \times z[i] + r \times x[i] - u \times p[i]) \times \mathrm{d}t, \tag{6}$$

$$Z[i+1] = z[i] + (z[i] \times x[i] \times y[i] - 1.5 \times f_z(s \times p[i] - k[i])) \times \mathrm{d}t, \tag{7}$$

$$K[i+1] = k[i] + (s \times x[i] + f_z(u \times y[i] - r \times k[i])) \times \mathrm{d}t, \tag{8}$$

$$P[i+1] = p[i] + f_z(b \times (x[i] + k[i])/z[i] + y[i]) \times \mathrm{d}t. \tag{9}$$

In the chaos parameter set, b, r, s, u, and $\mathrm{d}t$ are involved, while x, y, z, k, and p constitute the starting conditions for the chaotic map. The recently introduced 5D chaotic system was implemented and evaluated, and the Lyapunov exponents for both the initial conditions and parameters were computed. At maximum Lyapunov values (x = 2.1, y = 0.5, z = 1.1, k = 1.1, and p = 0.1) and system parameter (b = 0.01, r = 0.5, s = 0.95, u = 1.1, and $\mathrm{d}t$ = 0.01), f_z denotes the fuzzy triangular function described above, centered at z. The proposed 5D chaotic system demonstrates Lyapunov values indicative of super chaos, featuring five values that are positive. The chaos keys generated (K1, K2, ..., K5) from all proposed systems successfully undergo statistical tests conducted by the NIST before being effectively employed in video encryption. Figure 6 displays the chaotic attractors in each plane of the 5D Lorenz chaotic map.

4.2.4 ROIs video encryption

The set of five chaotic sequences generated by equations (5)–(9) within the proposed method. These sequences are

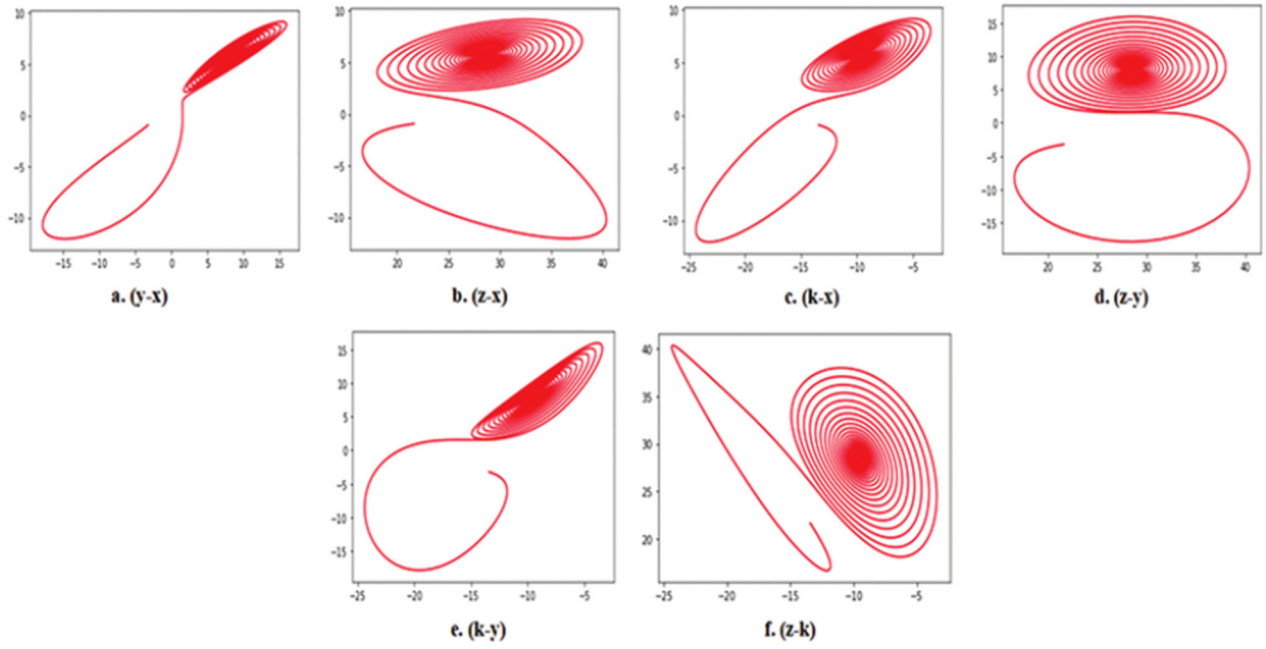

Figure 6: Chaotic attractors found in every plane of the 5D Lorenz chaotic map onto different spaces (a) y-x , (b) z-x, (c) k-x, (d) z-y, (e) k-y, and (f) z-k.

then converted into five vectors, identified as key1, key2, key3, key4, and key5. The creation of these vectors depends on the 5D chaotic Lorenz map, characterized by specific parameters and starting conditions. Each vector has a dimensionality corresponding to the original image ($h \times w$). During this phase, the encoded ROI that is split into even and odd arrays is organized into the R, G, and B components. The pixels in the even array of the ROI with key1, key3, and key5 undergo the DNA-XOR procedure, as outlined in Table 2, to obtain the even ROI encryption. Conversely, the pixels in the odd array of the ROI with key2, key5, and key4 undergo the DNA-XOR operation to obtain the odd ROI encryption. Combining these two 2D arrays from the XOR operations yields the encrypted ROI.

In summary, this process ensures ROI encryption by utilizing chaotic sequences and performing XOR operations, as shown in Equations (10)–(15).

$$\text{REeven} = \text{Reven XOR key1}, \tag{10}$$

$$\text{Geeven} = \text{Geven XOR key3}, \tag{11}$$

$$\text{Beeven} = \text{Beven XOR key5}, \tag{12}$$

$$\text{Reodd} = \text{Rodd XOR key2}, \tag{13}$$

$$\text{Geodd} = \text{Godd XOR key5}, \tag{14}$$

$$\text{Beodd} = \text{Bodd XOR key4}. \tag{15}$$

4.2.5 Decryption process

For decryption, the original ROIs from the encrypted surveillance video are recovered by reversing the encryption steps. This entails identifying the positions of the encrypted ROIs and the keys employed in the encryption process, as depicted in Figure 7. In other words, the decryption stage retraces the stages of the encryption phase by following the opposite order. Figure 8 illustrates a visual representation of the suggested object decryption method.

4.3 Uploading encrypted video to the cloud

The cloud upload of videos is important for organizations today because of its efficiency and cost-effectiveness. For uploading videos to the cloud, an organization must establish an end-to-end system that ensures the safety and security of videos [17,18]. The software for such a system should be easy to use and maintain as it is expected to be

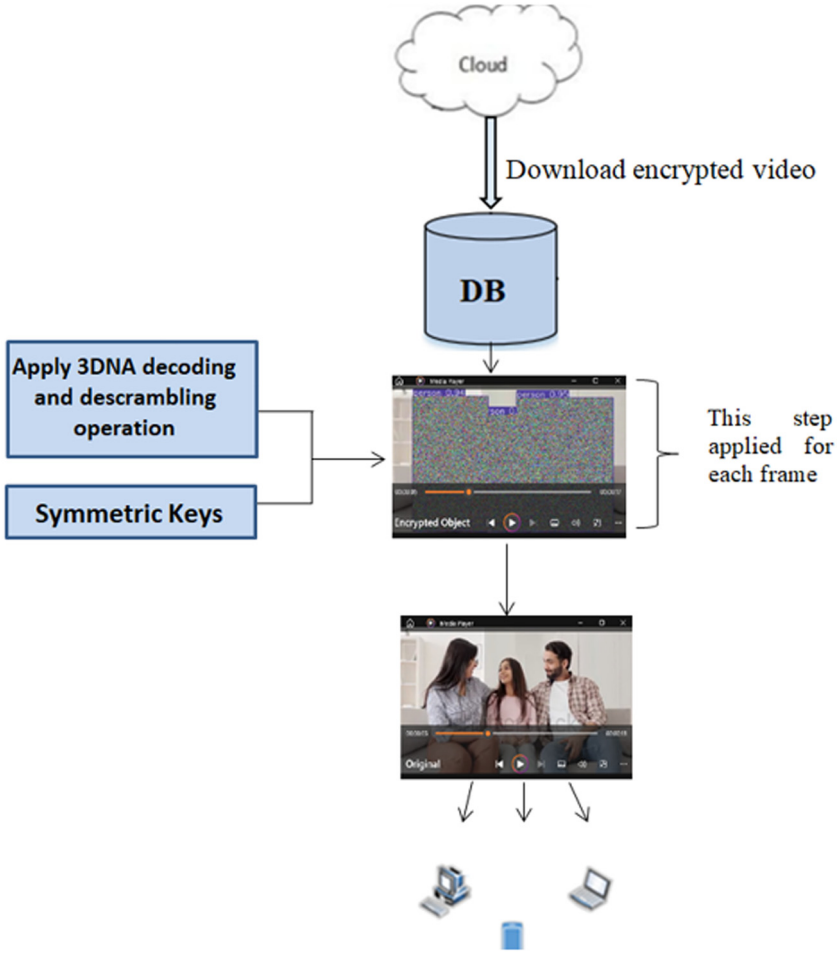

Figure 7: Overview of the basic stages involved in the decryption procedure [16].

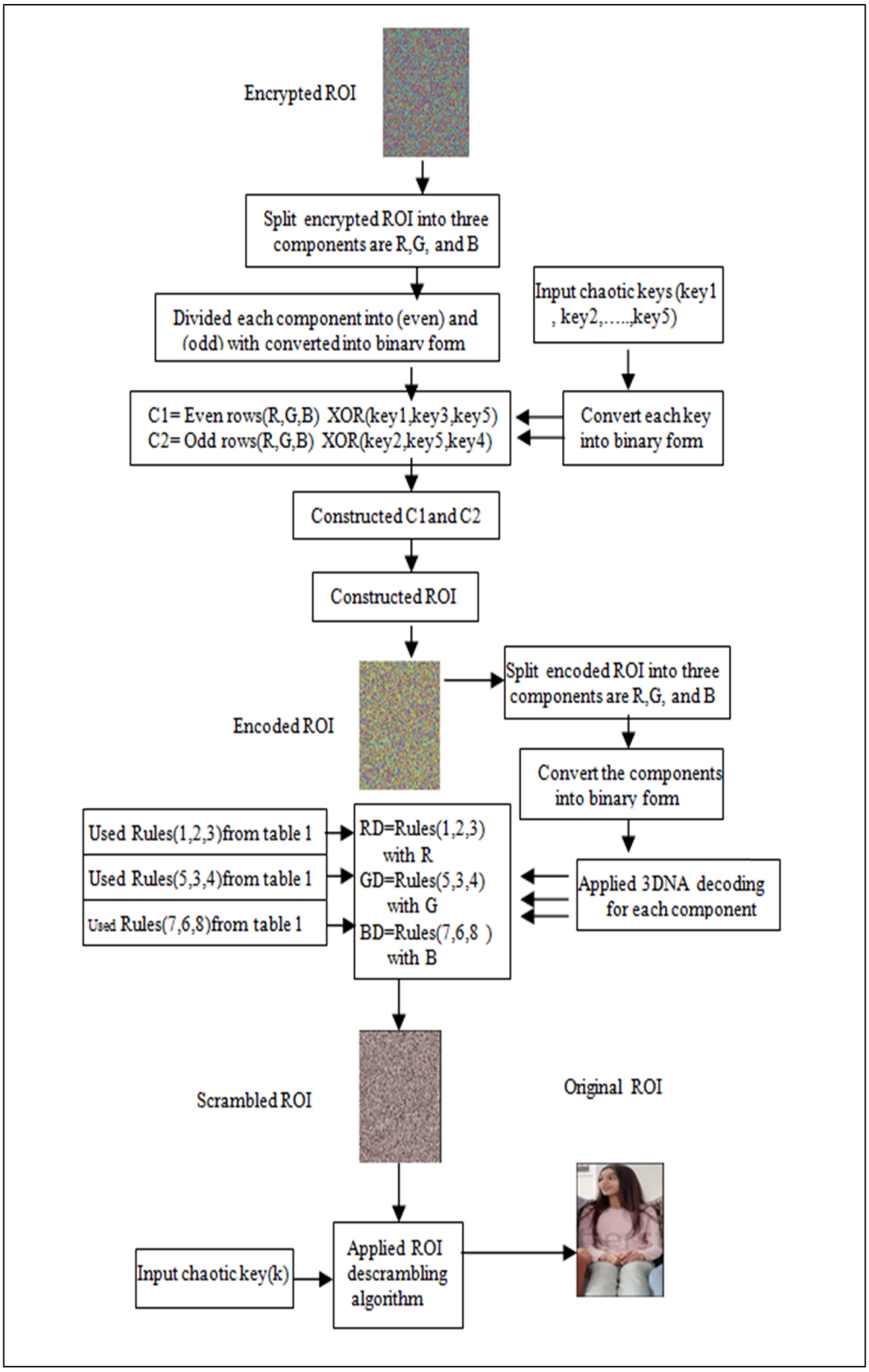

Figure 8: A workflow visualization for the general steps of the decryption process [16].

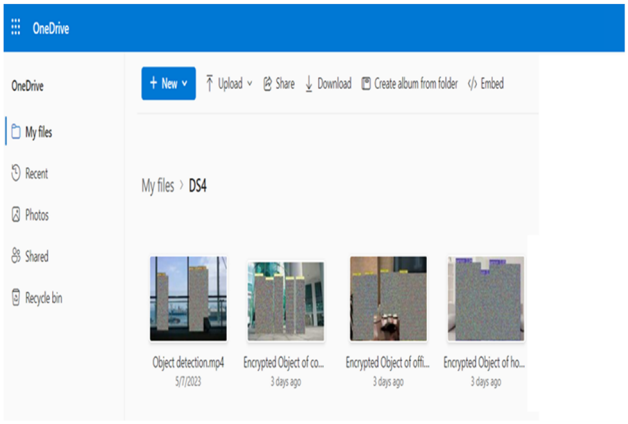

Figure 9: Screenshot of uploaded encrypted videos in the OneDrive cloud.

used by multiple individuals who may not be tech-savvy and require user-friendly interfaces. This proposed work utilizes the OneDrive cloud as the interface tool for managing encrypted videos, as illustrated in Figure 9.

5 Experimental process

This section provides details about the experimental setup for evaluating the performance of the proposed image encryption algorithms. The experiments were performed using Python 3.10 on a computer with an 8th Gen Core i7 CPU operating at 2.20 GHz and 8 GB of memory. The surveillance videos in Figure 10 are used as tested videos from [16], that includes the original, objects detected, encrypted, and decrypted versions. The findings outlined demonstrate that all encrypted videos appear utterly distorted, suggesting the efficiency of the proposed method.

6 Results and discussion

In this section, we evaluate the efficiency of the proposed encryption algorithm with a variety of tests, including analyzing the key space entropy and conducting an analysis of differential attacks, histogram examination, evaluation of video quality, correlation analysis, and time assessment. The tests are further explained in the following.

6.1 Analysis of key space and sensitivity

The key space metric is essential for evaluating encryption systems as it measures the system's susceptibility to minimal alterations in the secret key used for encryption and decryption. As depicted in Figure 11, the proposed approach exhibits a high level of sensitivity, making it highly responsive to even the most minor changes in the secret key [19].

6.2 Entropy

In the context of this study, entropy quantifies the amount of information contained within a dataset and can show the distribution of grayscale pixel values in the ROIs of the video frames. Entropy is a constant positive value, and a higher value indicates that a variable contains a greater amount of information such that

$$H_{(s)} = \sum_{i=0}^{n-1} -p(s_i)\log_2 p(s_i), \tag{16}$$

where $p(s_i)$ denotes the probability of grayscale s_i, and n represents the total count of grayscale pixels. In this experiment, a house test video is utilized, and Table 3 lists the calculated entropy for the initial and encrypted ROIs representing the individuals on the left, middle, and right appearing in frame number 100 of the test video. These results imply that the information entropy of the encrypted ROIs is near 8, demonstrating the system's ability to withstand attacks [20].

6.3 Differential attack analysis

The unified averaged changed intensity (UACI) and the number of changing pixel rate (NPCR) are metrics capable of identifying factors associated with differential attacks and highlighting crucial image information. The equations for each metric are defined in the following:

$$\text{NPCR} = \sum_{i-0}^{W}\sum_{j=0}^{H} D(i,j) \times 100\%, \tag{17}$$

where H and W denote the columns and rows for ROI, in each case, and D is approximated by

$$D(i,j) = \begin{Bmatrix} 0 & \text{if } C_1(i,j) = C_2(i,j) \\ 1 & \text{if } C_1(i,j) \neq C_2(i,j) \end{Bmatrix}, \tag{18}$$

where $C_1(i, j)$ and $C_2(i, j)$ depict pixel values within the ciphered ROIs, and L indicates the quantity of gray levels. Then, the UACI is expressed as

$$\text{UACI} = \frac{1}{W \times H}\left[\sum_{i=0}^{W}\sum_{j-0}^{H}\frac{C_1(i,j) - C_2(i,j)}{2^L - 1}\right] \times 100\%. \tag{19}$$

Figure 10: Sample output of the experimental process to test encrypting and decrypting ROIs in videos with the proposed method [16].

Table 4 lists the calculated metric values after a series of ROIs for the same left, middle, and right elements in video frame 100, which were tested using the suggested system [21]. The results of NPCR and UCAI are relatively good, so the reconstructed ROIs seem plausibly similar to the original pixel distributions compared to other methods.

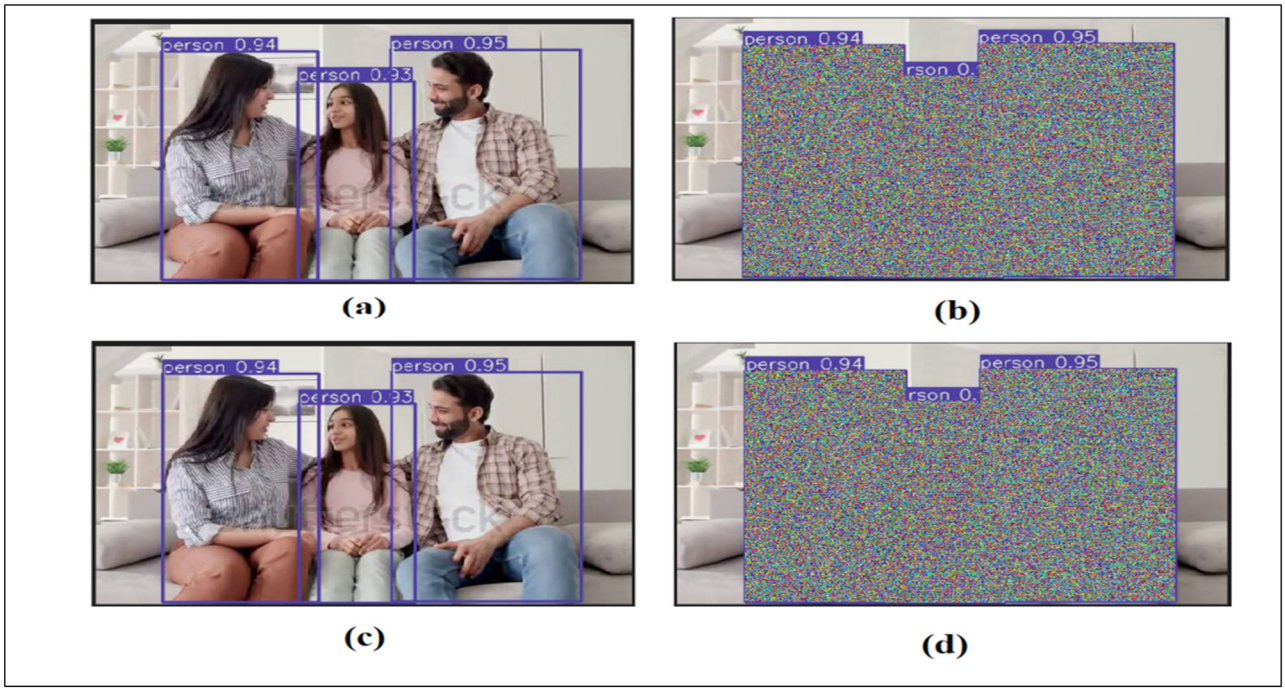

Figure 11: Illustration of how the encryption process is affected by variations in the secret key parameter. (a) Original of house frame. (b) Encrypted of house frame. (c) Decrypted of house frame by r = 1.19. (d) Decrypted of house frame by r = 1.12000001 [16].

6.4 Histogram analysis

For an encryption algorithm to be considered effective, the histograms of the encrypted video frames are anticipated to exhibit uniformity. Figure 12 displays the pixel value histograms per color channel for both the original and encrypted ROIs. The results indicate that the suggested algorithm has the potential to thwart statistical attacks [25].

$$\text{PSNR} = 10\ \log_{10}\left(\frac{(255)^2}{\text{MSE}}\right)\text{d}B, \tag{20}$$

$$\text{MSE} = \frac{1}{W \times H}\sum_{i-0}^{W}\sum_{j=0}^{H}(p(i,j) - C(i,j))^2. \tag{21}$$

Values for our test frame are calculated in Table 5, with the results for MSE and PSNR being relatively good.

6.5 Video quality

A standard requirement for the ROIs of video frame encryption methods is that the encrypted ROIs deviate significantly from the initial ROIs. The two criteria of the PSNR and MSE can compare the original and encrypted ROIs generated by the proposed algorithm. These metrics are defined as [26]

6.6 Correlation coefficient

The correlation coefficient gauges the linear relationship in terms of range and trend between two random variables. The correlation coefficient approaches 1 when two variables, x and y, are closely linked, while a value near 0

Table 3: Calculated entropy of the ROIs in the initial and corresponding encrypted video frames

Video object	Left ROI	Middle ROI	Right ROI
Original ROI	7.8600	7.7322	7.6532
Encrypted ROI	7.9967	7.9948	7.9902
Decrypted ROI	7.8525	7.7271	7.6532

Table 4: Calculated NPCR and UCAI metrics for the test video frame

ROIs test	NPCR	UCAI
Left ROI	99.1298	32.8111
Middle ROI	99.0945	31.9025
Right ROI	99.8734	33.8000
[22]	99.6097	33.4557
[23]	99.6130	33.6100
[24]	99.5800	28.4800

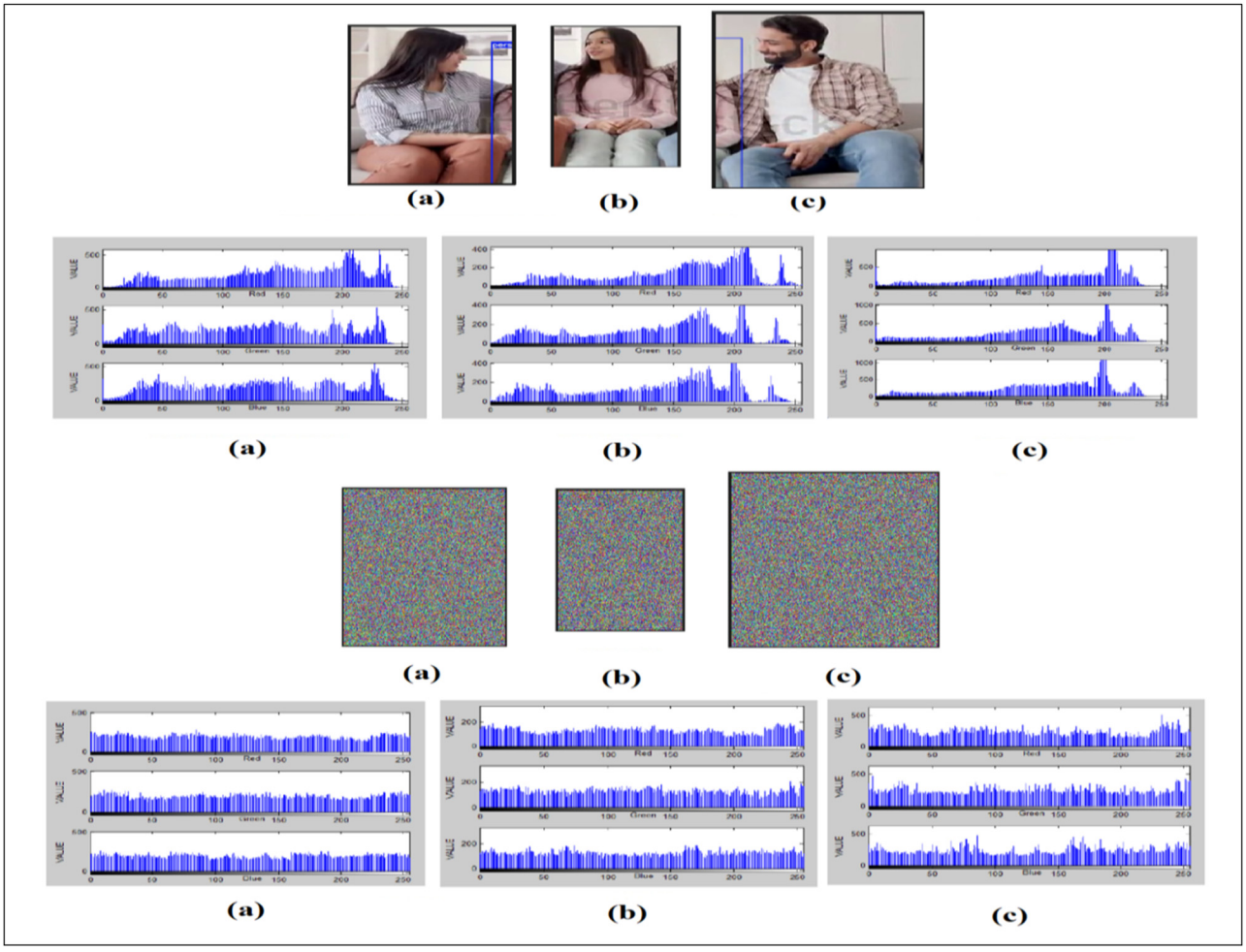

Figure 12: Histogram comparison analysis for the (a) original and encrypted left ROI of the test video frame, (b) original and encrypted middle ROI, and (c) original and encrypted right ROI [16].

indicates that these variables are considered unrelated. Equation (22) can be employed for calculating the correlation coefficient as follows:

$$C = \frac{\sum_i (x_i - x_m)(y_i - y_m)}{\sum_i \sqrt{\sum_i (x_i - x_m)^2} \sqrt{\sum_i (y_i - y_m)^2}}. \quad (22)$$

These coefficients are calculated for our test video frames in Table 6, which indicates a range for the original ROIs between 0.9689 and 0.9313 and the range for the encrypted ROIs between −0.0184 and −0.0296. The correlation coefficients between the initial and encrypted ROIs are different, as illustrated in Figure 13, which suggests a robust algorithm [27].

6.7 Time analysis

The assessment criterion involves the duration it takes for the cryptographic strategy to execute the encryption and

Table 5: MSE and PSNR tests

ROIs test	PSNR	MSE
Left ROI	13.3894	3238.5398
Middle ROI	12.7382	3287.9376
Right ROI	13.1092	3236.8273
[25]	7.4130	1179.2310
[23]	10.1948	6217.3002

Table 6: Correlation coefficients calculated on the test video frame between the original and corresponding encrypted ROIs

Video name	Left ROI	Middle ROI	Right ROI
Original ROIs	0.9313	0.9689	0.9513
Encrypted ROIs	−0.0184	−0.0296	−0.0261

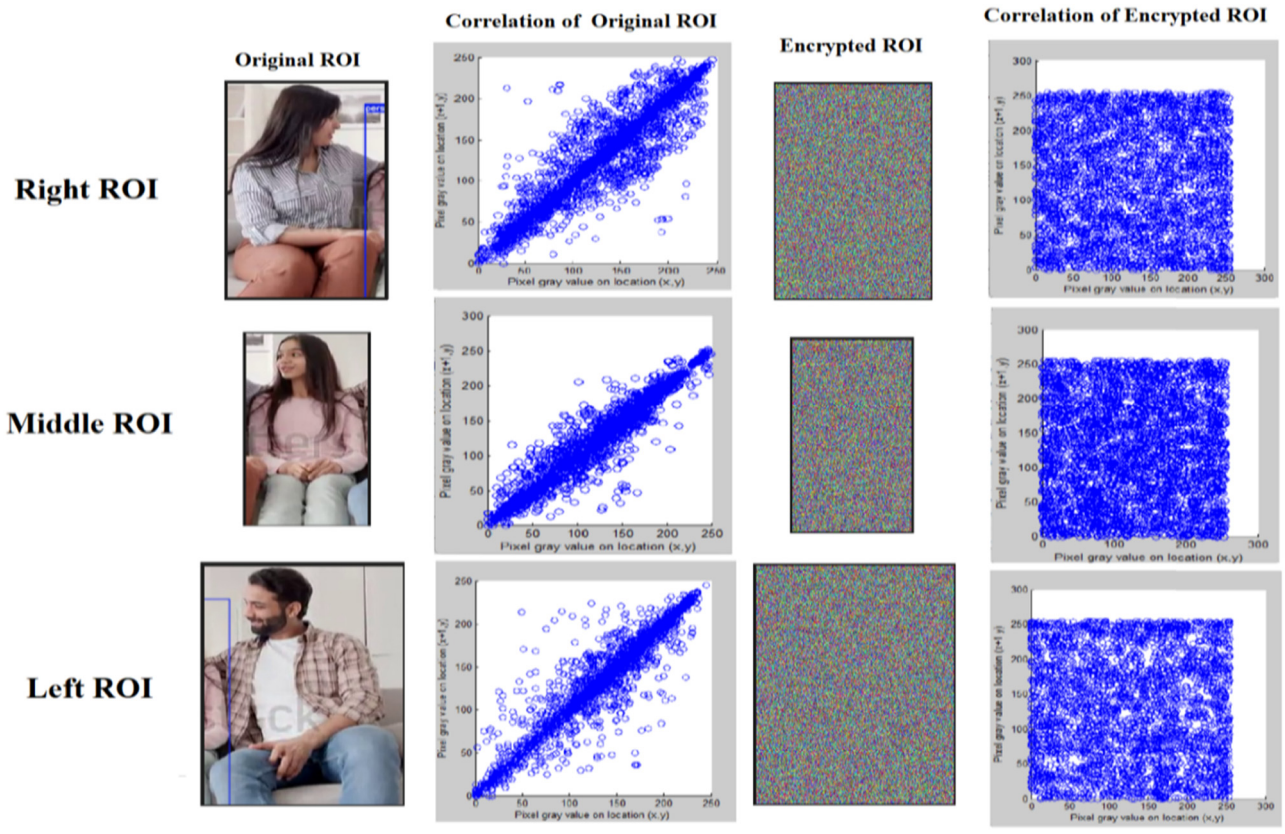

Figure 13: Correlation analysis of the ROIs in both the original frames and their corresponding encrypted frames in the test video indicates a notable distinction in the pixel value distributions [16].

decryption algorithms for any video. Our experiment shows a slight difference between encryption and decryption times. As a result, encrypting the frames with our proposed approach takes longer than decrypting them, as compared in Table 7 with existing ROI encryption methods. However, our method requires a shorter overall time for execution in comparison to existing approaches.

Table 7: Average encryption and decryption times

Video name	Max ROIs per frame	Time of encryption (s)	Time of decryption (s)
House	3	10.16	9.15
Airport	4	9.71	9.11
Company	5	7.06	6.72
Street	14	11.95	10.99
Reception	2	10.2	10.1
Office	5	8.76	8.02
[28]	12	34.28	—
[28]	3	42.88	—
[28]	1	50.61	—
[29]	Color (512 × 512)	4.60.58	—
[29]	Color (256 × 256)	3.61.75	—
[30]	Color (512 × 512)	14.81.19	—

6.8 NIST analyses

The NIST outlined guidelines for ensuring data security that includes fifteen tests designed to assess the randomness and strength of encryption algorithms. Table 8 provides benchmarked performance data for our proposed system with these tests, indicating a successful evaluation for each. We compare our results with those from random number generators proposed in [31], as shown in Table 9.

6.9 Energy consumption analysis

The selective encryption algorithm is faster than the full encryption algorithm since it encrypts the partial data

Table 8: NIST assessment test results of dynamic random key1,... key5

ID	NIST test	*P*_value of key1	*P*_value of key2	*P*_value of key3	*P*_value of key4	*P*_value of key5	*P*_value >0.01
1	Frequency	0.8596	0.8734	0.4398	0.8495	0.5489	Pass
2	Frequency within a block	0.8596	0.7834	0.7645	0.2384	0.5478	Pass
3	Runs	0.3781	0.7638	0.7643	0.6378	0.4578	Pass
4	Longest run of ones	0.8354	0.8384	0.7839	0.7864	0.5784	Pass
5	Rank	0.4765	0.6384	0.1274	0.489	0.5478	Pass
6	Spectral	0.3303	0.3789	0.8634	0.6749	0.5478	Pass
7	Non-overlapping T.M.	0.9999	0.4873	0.3672	0.9749	0.9840	Pass
8	Overlapping T.M.	0.9432	0.2174	0.7523	0.6738	0.5494	Pass
9	Maurer's universal	0.6548	0.4837	0.9734	0.5498	0.4873	Pass
10	Linear complexity	0.5678	0.9483	0.3456	0.8495	0.1298	Pass
11	Serial	0.4989	0.5647	0.8673	0.8493	0.8459	Pass
12	Approximate entropy	1.0000	0.7483	0.2371	0.9293	0.5489	Pass
13	Cumulative sums	0.9492	0.9743	0.8943	0.1278	0.4563	Pass
14	Random excursions	0.4584	0.8743	0.7485	0.6478	0.9743	Pass
15	Random excursions variant	0.2327	0.7489	0.8438	0.8493	0.8493	Pass

Table 9: NIST assessment test results of static random key in [31]

ID	NIST test	*P*_value	*P*_value >0.01
1	Frequency	0.3291	Pass
2	Frequency within a block	0.1792	Pass
3	Runs	0.0887	Pass
4	Longest run of ones	0.0620	Pass
5	Rank	0.0283	Pass
6	Spectral	0.0000	Fail
7	Non-overlapping T.M	0.9986	Pass
8	Overlapping T.M.	0.7500	Pass
9	Universal	0.8847	Pass
10	Linear complexity	0.1760	Pass
11	Serial	0.3040	Pass
12	Approximate entropy	0.3114	Pass
13	Cumulative sums	0.2869	Pass
14	Random excursions	0.1276	Pass
15	Random excursions variant	0.2624	Pass

instead of the total video clip [32]. Contrary to popular belief, our experiments show that the energy overhead of selective video encryption is insignificant compared to the energy consumed for full video encryption. In terms of energy, the selective algorithm consumes about 40% of relative energy. energy analysis on the video encryption algorithms as summarized in Table 10.

7 Conclusions

In this work, the 5D Lorenz map underwent modification by incorporating triangular fuzzy numbers, resulting in a newly modified 5D Lorenz map that demonstrates a broad spectrum of chaos-related phenomena across different parameter settings. It was illustrated that the altered 5D Lorenz map achieves an elevated Lyapunov exponent in comparison to the original Lorenz map. The 5D Lorenzo map is employed in the generation of keys, which are then used to encrypt ROIs symbolizing individuals. The identification of these (ROIs) through YOLOv7, indicating effective object detection, streamlines the process of identifying pertinent areas within surveillance videos. After this, triple DNA encoding is applied, resulting in the encoded ROI. This triple-encoded ROI is further fortified through encryption using a chaotic 5D Lorenzo map to enhance video security during transmission. The decryption process reverses the

Table 10: Comparison of energy consumption of video encryption algorithms

ID	Method	Algorithms	Security	Size	Speed	Relative energy (%)
1	[32]	Naive	High	No change	Slow	100
2	[32]	Selective	Moderate	No change	Fast	59
3	Our proposed	Encrypted ROIs	High	Change	Fast	40

encryption operation. Finally, the encrypted video is uploaded to the cloud for persistent storage. A simulation experiment is conducted to assess the effectiveness of the proposed approach with an evaluation of various metrics, like entropy and the analysis of differential attacks, analysis of histograms, assessment of sensitivity, exploration of key space, and evaluation of video quality. The experimental findings suggest the algorithm's robust security performance and ability to effectively withstand various threats.

Funding information: The authors state no funding involved.

Author contributions: All authors have accepted responsibility for the entire content of this manuscript and consented to its submission to the journal, reviewed all the results and approved the final version of the manuscript. MAAK conceived of the presented idea. AHA developed the theory, performed the computations, and verified the analytical methods. ATA helped supervise the project. All authors discussed the results and contributed to the final manuscript.

Conflicts of interest: Authors state no conflict of interest.

Data availability statement: Most datasets generated and analyzed in this study are comprised in this submitted manuscript. The other datasets are available on reasonable request from the corresponding author with the attached information.

References

[1] Zuxuan W, Ting Y, Yanwei F, Yu-Gang J. Deep learning for video classification and captioning. In Frontiers of multimedia research. New York; Vol. 2. 2017 Feb. p. 3–29.
[2] Xiaodong L, Haoyang Y, Hongyu Z, Xin J, Hongbo S, Jing L. Video encryption based on hyperchaotic system. Multimed Tools Appl. 2022 Jun;79:23995–4011.
[3] Shifa A, Asghar MN, Fleury M, Kanwal N, Ansari MS, Lee B, et al. MuLViS: Multi-level encryption based security system for surveillance videos. IEEE Access. 2020;8:177131–55.
[4] Alem F, Yu C, Sencun Z. Lightweight frame scrambling mechanisms for end-to-end privacy in edge smart surveillance. IET Smart Cities. 2022;4(1):17–35.
[5] Zhang X, Seo SH, Wang C. A lightweight encryption method for privacy protection in surveillance videos. IEEE Access. 2018 Apr;6:18074–87.
[6] Shao Y. Image encryption algorithm for torsional components of generator based on compound chaotic model. Therm Sci. 2020;24(3 Part A):1473–80.
[7] Darwich M, Ismail Y, Darwich T, Bayoumi M. Cost-efficient storage for on-demand video streaming on cloud. In 2020 IEEE 6th World Forum on Internet of Things (WF-IoT). IEEE; 2020 Jun. p. 1–4.
[8] Jiang K, Xie T, Yan R, Wen X, Li D, Jiang H, et al. An attention mechanism-improved YOLOv7 object detection algorithm for hemp duck count estimation. Agriculture. 2020;12(10):1–18.
[9] Muhammad H, Hussain A, Muhammad M, Richard H, Tariq A. Domain feature mapping with YOLOv7 for automated edge-based pallet racking inspections. Sensors. 2022;22(18):1–13.
[10] Chien YW, Alexey B, Hong YM. YOLOv7: Trainable bag-of-freebies sets new state-of-the-art for real-time object detectors. arXiv Prepr. arXiv2207.02696. 2022 Jul;1–15.
[11] Lazaros M, Christos V, Sajad J, Jesus M, Jacques K, Karthike YR, et al. Modification of the Logistic Map Using Fuzzy Numbers with Application to Pseudorandom Number Generation and Image Encryption. Entropy. 2020 April;1:20.
[12] Lefta FA, Hamdan AN. Integrated fuzzy logic and multicriteria decision model methods for selecting suitable sites for wastewater treatment plant: A case study in the center of Basrah, Iraq. Open Eng. 2024;14:1–21.
[13] Rawia AM, Maisa'a AA, Ashwak A. A novel lightweight image encryption scheme. Comput Mater Continua. 2023;75:1–17.
[14] He JH. Mysterious pi and a possible link to DNA sequencing. Int J Nonlinear Sci Numer Simul. 2004 Sep;5(3):263–74.
[15] Wei W, Dongming P, Honggang W, Hamid S, Hsiao H. Energy -constrained quality optimization for secure image transmission in wireless sensor networks. Adv Multimed. 2007;2027:1–10.
[16] https://www.shutterstock.com/royalty-free/people-videos.
[17] Emre E, Santiago O. Multimedia storage in the cloud using Amazon web services: implications for online education. arXiv Prepr. arXiv1608.07085. 2016;1–16.
[18] Sergei V, Yuriy A, Daniil T. Templet Web: the use of volunteer computing approach in PaaS-style cloud. Open Eng. 2018;8:1–7.
[19] Xiaoqiang Z, Zhiwei L, Xiaochang Y. Design of artificial intelligence image encryption algorithm based on hyperchaos. Ain Shams Eng J. 2023;14(3):1–8.
[20] Huda G, Maisa'a A. Comparison of three proposal methods in steganography encryption secret message using PVD and MapReduce. IRAQI J Comput Commun Control Syst Eng. 2021;21(2):1–17.
[21] Yousef A, Arslan M, Jawa A. A lightweight image encryption algorithm based on chaotic map and random substitution. Entropy. 2022;24(10):1–25.
[22] Hui L, Jianwen Z, Linquan H, Yifan L. A lightweight image encryption algorithm based on message passing and chaotic map. Secur Commun Netw. 2020;2020:1–12.
[23] Azhaar K, Alaa K. A new image encryption algorithm based on multi chaotic system. Iraqi J Sci. 2022;63(1):324–37.
[24] Manish G, Kamlesh K, Piyush K. Session key based fast, secure and lightweight image encryption algorithm. Multimed Tools Appl. 2020;80(7):10391–416.
[25] Simin D, Guodong Y. IWT and RSA based asymmetric image encryption algorithm. Alex Eng J. 2023;66:979–91.
[26] Sally A, Maisa'a A. An improved method for combine (LSB and MSB) based on color image RGB. Eng Technol J. 2021;39(1B):231–42.
[27] Gao S, Wu R, Wang X, Wang J, Li Q, Wang C, et al. A 3D model encryption scheme based on a cascaded chaotic system. Signal Process. 2023;202:108745.
[28] Khalid M, Mohamed A, Hanaa M, Mostafa M, Nabil A. Privacy protection in surveillance videos using block scrambling-based

encryption and DCNN-based face detection. IEEE Access. 2022;10:106750–69.
[29] Shuting C, Linqing H, Xuesong C, Xiaoming X. A symmetric plaintext-related color image encryption system based on bit permutation. Entropy. 2018;20(4):282.
[30] Xiaolin W, Bin Z, Yutong H, Yamei R. A novel color image encryption scheme using rectangular transform-enhanced chaotic tent maps. IEEE Access. 2017;5:6429–36.
[31] Chih H, Guo H, Jie S, Jun J, Kuang H. Novel design of cryptosystems for video/audio streaming via dynamic synchronized chaos-based random keys. Multimed Syst. 2022;28(5):1793–808.
[32] Lee K, Dutt N, Venkatasubramanian N. An experimental study on energy consumption of video encryption for mobile handheld devices. In 2005 IEEE International Conference on Multimedia and Expo. IEEE; 2005 Jul. p. 1424–7.