Secure Video Encryption Using Chaotic Map Modification and Encoding Techniques

Asmaa Hasan Alrubaie[1] and Maisa'a Abid Ali Khodher[2]
[1]*Department of Computer Science, University of Technology, 10066 Baghdad, Iraq*
[2]*Department of Computer Engineering, University of Technology, 10066 Baghdad, Iraq*
cs.20.41@grad.uotechnology.edu.iq, Maisaa.A.Khodher@uotechnology.edu.iq

Keywords: Video Encryption, Video Scrambling, Fuzzy Triangular Numbers, 3D Lorenz Chaotic Map, 2DNA Encoding.

Abstract: As multimedia information continues to explode on the internet and in everyday life, the forms in how people access information have come in more varied forms. Video content has become an essential part of daily life and in usage at work. Nevertheless, the mass utilization of video data has also brought a list of security risks and challenges, and the concern about video security issues is increasing. In the current paper, various algorithms have been incorporated in order to attain high degree of security. The proposed approach integrates a simplified three-dimensional (3D) Lorenz chaotic map using fuzzy triangular numbers in generating keys with 2DNA encoding to increase video encryption. First, the video is broken down to single frames. The given approach further involves three key steps. The first stage consists of a scrambling operation on the pixels of each frame which is determined by a position key. In the second step, the scrambled frames are encoded (scrambled) with 2DNA, based on many encoding rules in accordance with the concepts of DNA cryptography to generate coded frames. At the last stage, coded frames are encrypted by XOR operation with chaotic keys calculated based on modified 3D Lorenz chaotic map. Lastly, reconstructing of all encrypted frames is used to produce the completely encrypted video. The performance of the proposed scheme is confirmed by the results of the experiments, and the highest UACI and NPCR values were 33.6100% and 99.6130, respectively.

1 INTRODUCTION

The security of the information and upholding privacy are among the gravest issues in the modern digital systems, irrespective of whether the information is in the form of images, text, video, or audio data. As multimedia technologies rapidly develop, video data, which is distinguished by the abundance of information, has become popular in many areas, such as surveillance systems, medical applications, legal investigations, and many others [1]. Encryption is one of the surest methods of protecting confidential data. Extensive research has therefore been done to come up with encryption schemes that offer high security and great computation efficiency especially when dealing with image and video data [2]. Prior to the transmission of data through the unsecured communication channels, the data are encrypted so that the original message is converted into the unintelligible version that cannot be decoded by the unauthorized individuals. The opposite process returning the encrypted information to its original readable form is called decryption [3]. Chaos theory, which can be referred to as the science of unpredictable behavior, concerns nonlinear dynamic systems, the development of which is highly sensitive and cannot be controlled or predicted. Chaos theory has also found extensive application in other scientific and engineering fields because of its capacity to predict the behavior of complex systems. It is especially suitable in cryptography due to its sensitive to initial conditions and positive Lyapunov exponents; it is ergodic, and it can be viewed as stochastic [4]. The randomized systems are capable of generating pseudo-random numbers which can be utilized suitably as encryption keys. Chaotic encryption schemes in most cases have two fundamental operations that include scrambling and diffusion. Scrambling varies the arrangement of the pixels in each image of the video as per some secret key and diffusion modifies the pixel values of the intensity such that small changes are spread out over

the entire frame. Through these two processes, an encoded frame is generated, which is much different than the original frame, thus improving security [5]. In the biological systems, information that is passed to the next generation is genetic through deoxyribonucleic acid (DNA). The basic nucleotides of DNA are four, which are thymine (T), guanine (G), cytosine (C), and adenine (A). These nucleotides can be introduced into cryptography by following binary-to-DNA mapping principles (usually the [0,1] encoding scheme) [6]. One common method of multimedia encryption is the DNA coding, which encodes pixel values of plain video images in DNA sequences upon fixed rules of encodings. Owing to its high storage density, inherent parallelism, and computational advantages, DNA-based encoding has emerged as an effective encryption mechanism. Consequently, numerous cryptographic schemes have been proposed that rely on DNA computing principles. Moreover, DNA-based techniques generate encrypted video data that differ substantially from the original plain video, further improving resistance against attacks [7].

Chaotic encryption coupled with the use of DNA coding enjoy the benefits of the two methods together. The outcome of this hybridization is a very secure encryption structure having high-entropy and high complexity, and thus extremely challenging to attackers to crack the system [8]. In the proposed method, pixel scrambling is first applied to video frames, followed by Double DNA (2DNA) encoding using multiple encoding rules, as listed in Table 1. The resulting encoded frames are subsequently coded alongside the use of a modified three-dimensional (3D) Lorenz chaotic map that is based on the application of fuzzy triangular numbers applied in generation of chaotic keys. The 3D Lorenz map has more intricate and unforeseeable dynamics compared to the one-dimensional (1D) systems of chaos. This holistic approach is very resistant to the differential, statistical, and brute type of attacks. This part of the paper is followed by the following structure. Section 2 reviews related work in the field of video encryption. Section 3 presents the theoretical background. In Section 4 the details of the proposed encryption scheme are described. Experimental results are discussed in Section 5, while the security analysis is presented in Section 6. Finally, conclusions are drawn in Section 7.

2 RELATED WORKS

Presented a video encryption system using chaotic based systems which utilizes two-dimensional distortion models to provide a very secure transmission of video. Their methodology emphasizes the increasing prevalence of chaos-based encryption methods in the current video cryptography over the traditional methods. The suggested scheme incorporates various chaotic maps into a perturbation-based encryption scheme to increase the diffusion and confusion processes. Tests that were conducted experimentally revealed that the method is of high encryption quality, key sensitivity, and low residual visual information. In addition, comprehensive security and differentiation testing was performed to make the scheme sound against various attacks. Besides, extensive security and differentiation tests were done to ensure the soundness of the scheme when faced with different attacks. The given framework can also effectively manage redundancy of frame level data without compromising on the acceptable computational complexity and encryption stability; thus, it can be applied in secure video communication systems [9]. Suggested a video encryption method that performs on a hyperchaotic system, to counter the rising security issues relating to the proliferation of video in both personal and work environments. The video stream is split into color frames displayed in the Y, Cb, Cr color space in their approach. The color components are encrypted with Arnold transformations together with DNA coding. As shown by experimental evidence, the suggested encryption scheme can be assessed as the scheme with high security performance, as well as with high encryption efficiency, which proves its applicability in securing video content [10]. Introduced an innovative encryption model that can be used to ensure color video data security in heterogeneous networks. The algorithm will start with video frame extraction and decoding into red, green, and blue (RGB) color, and then it will be zero-padded to homogenize frame sizes. The color blocks are then broken down into blocks of different sizes which in turn are scrambled through zigzag scanning, block rotation, and random block permutation. Lastly a secret key that is derived out of a chaotic map is used to encrypt the scrambled portions. It was demonstrated in the experimental work that the suggested solution has good encryption performance and can offer a high level of protection against the unauthorized access [11].

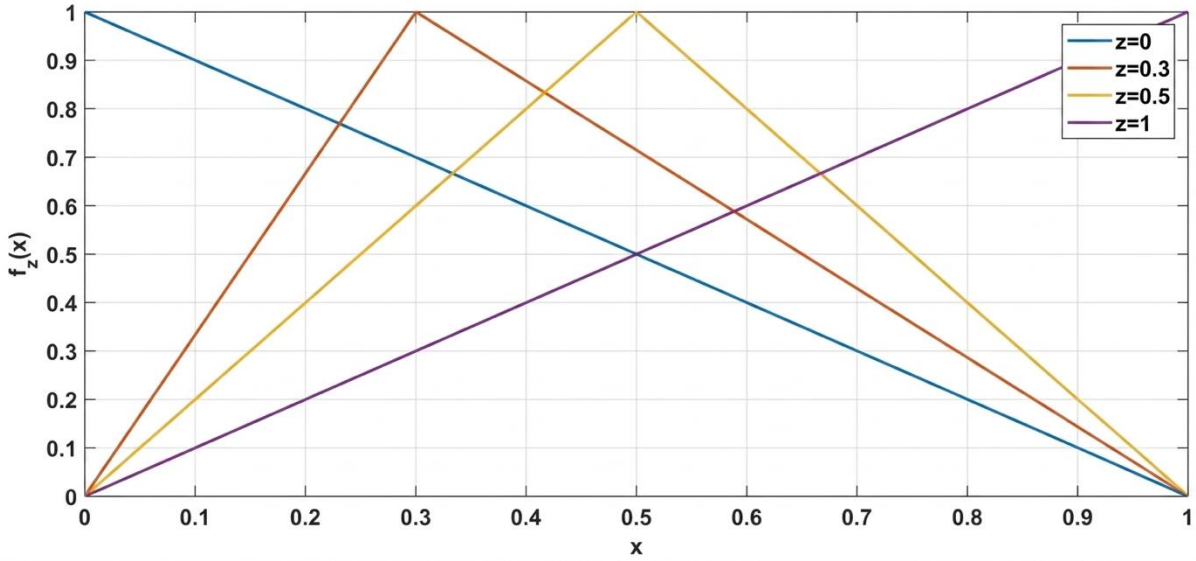

Figure 1: Illustrations of fuzzy trigonometric numbers for z=0,0.3,0.5, z = 0, 0.3, 0.5,z=0,0.3,0.5, and 111 [12].

3 THEORETICAL BACKGROUNDS

3.1 Fuzzy Number

This section presents preliminary concepts related to fuzzy numbers. Although the literature contains several slightly different definitions, in this study a fuzzy number is described as a mapping f:X→[0,1], where X⊆ ℝ. This mapping satisfies specific properties. First, it represents a normalized fuzzy set, meaning that there exists at least one element x Є X for which f (x) = 1. Second, the membership function f is assumed to be piecewise continuous over its domain.

It is necessary to mention that there are previous works that place a more strict requirement by demanding a special element x_0 so that f (x_0) = 1. Conversely, the fuzzy figures dealt with, and this work are characterized as functions f: [0,1] - [0,1] and are limited to a triangular membership framework [12].

$$f_z(x) = \begin{cases} 0 \le x \le z\frac{x}{z} \\ z \le x \le 1, \quad \frac{1-x}{1-z}. \end{cases} \qquad (1)$$

In this case, z is the maximum of the triangular fuzzy number. The Figure 1 presents the examples of different values of z. [12].

Chaotic maps are fundamental tools in the analysis of nonlinear dynamical systems. Among them, the Lorenz map is a well-known example that exhibits chaotic behavior and is governed by a set of nonlinear dynamic equations [13]. Compared to one-dimensional chaotic maps, three-dimensional Lorenz maps demonstrate more intricate and richer chaotic dynamics. The mathematical formulation of the three-dimensional Lorenz chaotic system is presented in equations (2)-(4), [14].

3.2 Chaotic 3D Lorenzo Maps

It is evident that the resulting phase portrait is consistent with the mathematical formulation of the three-dimensional Lorenz chaotic map for the parameter values for a = 10, r = 28, and b = 8/3. The solution trajectories of the variables x, y and z revolve around two equilibrium points, as observed in both the phase portrait and its projections. The initial conditions (x, y, z) form the foundation of the 3D Lorenz chaotic trajectories; therefore, this system can be effectively employed as a pseudo-random number generator for cryptographic applications [14].

$$\frac{dx}{dt} = a\,(y - x). \qquad (2)$$

$$\frac{dy}{dt} = (rx - y - xz). \qquad (3)$$

$$\frac{dz}{dt} = (xy - bz). \qquad (4)$$

3.3 Two DNA Encoding

Fundamental biological research and many areas of application require knowledge of DNA sequences,

including medical diagnostics, forensic science, biotechnology, and biological systematics. A DNA sequence is composed of four nucleotide bases: adenine (A), thymine (T), guanine (G), and cytosine (C). According to the principle of complementary base pairing, adenine pairs with thymine, while guanine pairs with cytosine. The basic structure of DNA is illustrated in Figure. 2. From this pairing mechanism, it can be inferred that the bases form two complementary groups, namely A-T and C-G [15].

These pairings are referred to as the Watson-Crick base-pairing rules after the names of scientists who introduced the structural basis of DNA. In a similar manner, the binary system exhibits complementary behavior between the digits 0 and 1. Consequently, the binary pairs 01 and 10 can be regarded as complementary, as can the pairs 00 and 11. In this study, the DNA sequences are encoded according to these complementary principles. Table1 shows the rules of coding and decoding of DNA, whereas Table 2 demonstrates the XOR operation that is used on the DNA sequences in a manner that does not violate the Watson Crick complementarity requirements [16].

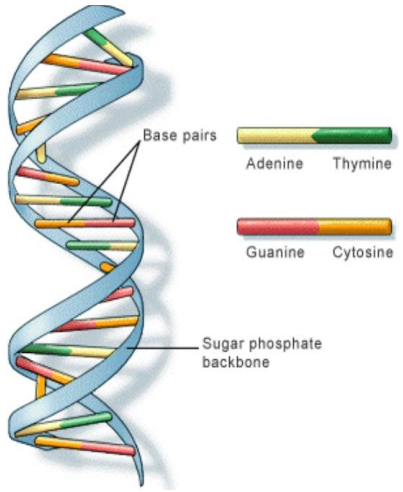

Figure 2: Simple DNA structure [15].

Table 1: Decoding and encoding map.

Rules	A	T	C	G
Rule1	00	11	10	01
Rule2	00	11	01	10
Rule3	11	00	10	01
Rule4	11	00	01	10
Rule5	10	01	00	11
Rule6	01	10	00	11
Rule7	10	01	11	00
Rule8	01	10	11	00

Table 2: The sequences of DNA used XOR operation.

⊕	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 METHODOLOGY

This work proposes a video encryption and decryption scheme intended to ensure secure video transmission over insecure communication channels. The theory is based on the fact that mathematical functions on a three-dimensional chaotic system and a two-dimensional DNA encoding system are combined to give the proposed method. The scheme operates through two primary phases: encryption and decryption. During the decryption phase, the same operations applied in the encryption stage are executed in reverse order to recover the original video content. The overall architecture of the proposed encryption-decryption framework is illustrated in Figure 3.

4.1 Encryption Stage

In the initial stage, the input video is decomposed into a sequence of individual frames, which are subsequently utilized in the scrambling process. Following frame extraction, a series of encryption operations is applied to each frame, as illustrated in Figure 4.

4.1.1 Frame Video Scrambling Algorithm

The use of scrambling operations is aimed at increasing the level of security of the proposed encryption method. Scrambling algorithm is executed at this stage to every video frame of (M x N) size where M and N denote and represent the frame height and frame width respectively. To generate a scrambled frame (as shown in Algorithm 1) the original frame is rearranged using position key (k) i = 0,1,2, 3, etc. and j = 0,1,2, etc. M-1 and N-1 respectively. The position key (k) is randomly selected. This key indicates new spatial positions of pixels of the scrambled frame I'. The scrambling algorithm is used to do pixel permutation where the items in the random matrix are the new pixel indices

and permitting swapping of the elements in the random matrix based on a symmetric key. Consequently, the spatial correlation between the neighboring pixels is largely diminished benefiting the encryption strength as a whole.

4.1.2 Two Encoding Frames Video

The DNA encoding process of the permuted frames obtained at the previous stage is subjected to the double random phase (DRP) encoding process. Initially, each scrambled RGB frame is decomposed into its three-color components, namely red (R), green (G), and blue (B). Each component is then independently converted into a binary representation, where every two-bit sequence is mapped to a DNA symbol (A, C, G, or T) according to Rule 1, Rule 3, and Rule 6 listed in Table 1. This step generates three DNA-encoded components, denoted as Rc, Gc, and Bc. Subsequently, a second encoding phase is performed using different DNA encoding rules selected randomly from Table 1 to further enhance security. During this step, Rc, Gc, and Bc components are re-encoded with Rule 2, Rule 5 and Rule 8 respectively to generate three components that are doubly encoded, namely Rcc, Gcc, and Bcc. These elements are, lastly, assembled to create one encoded frame, which is known as the DNA-encoded frame.

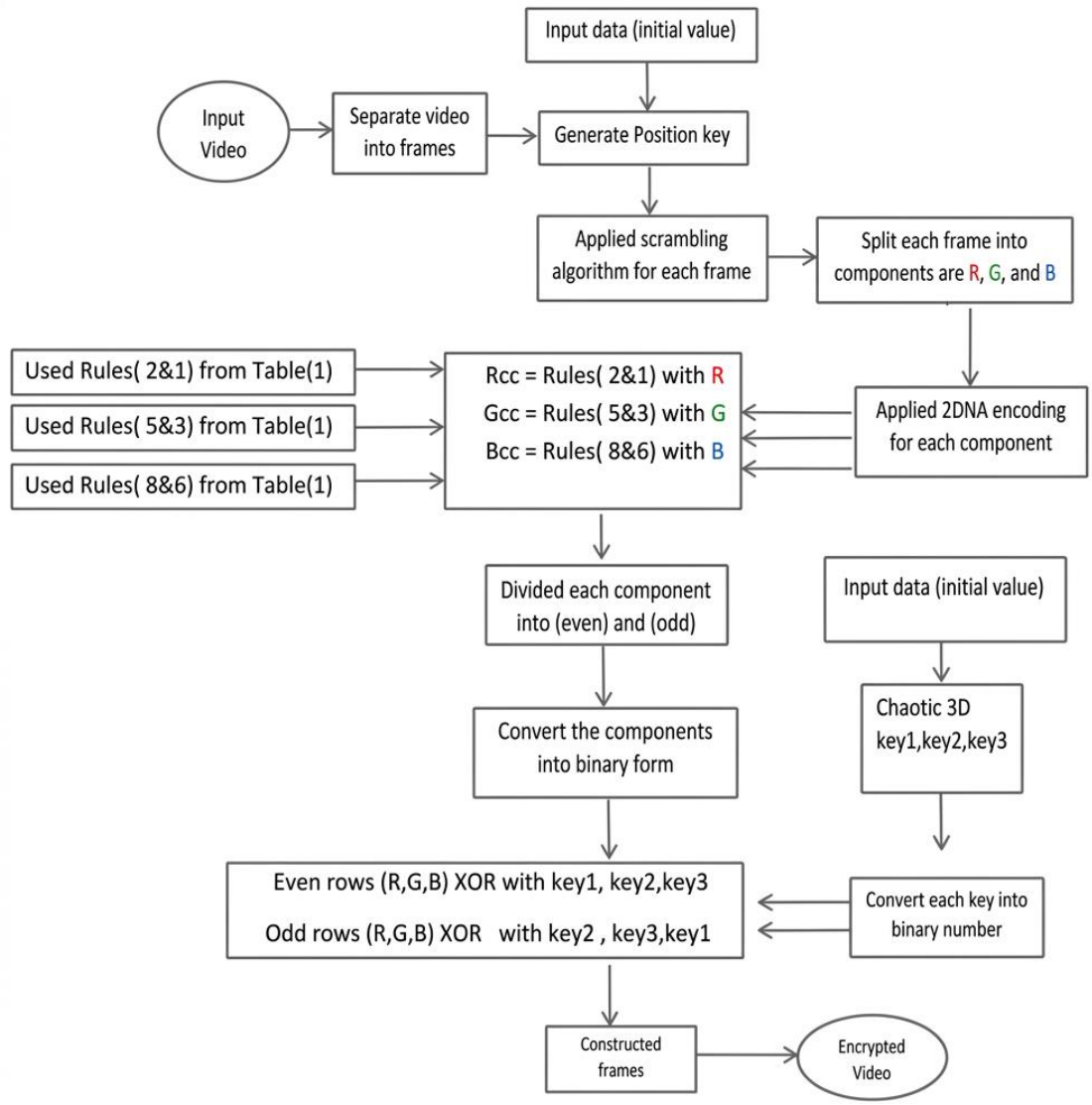

Figure 3: Schematic representation of the proposed video encryption and decryption framework.

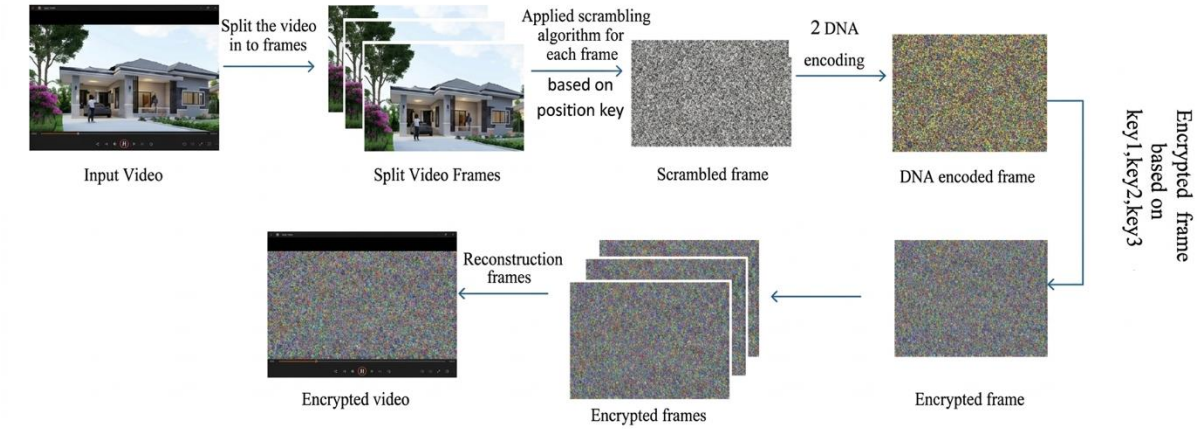

Figure 4: Overall scheme of the encryption process proposed.

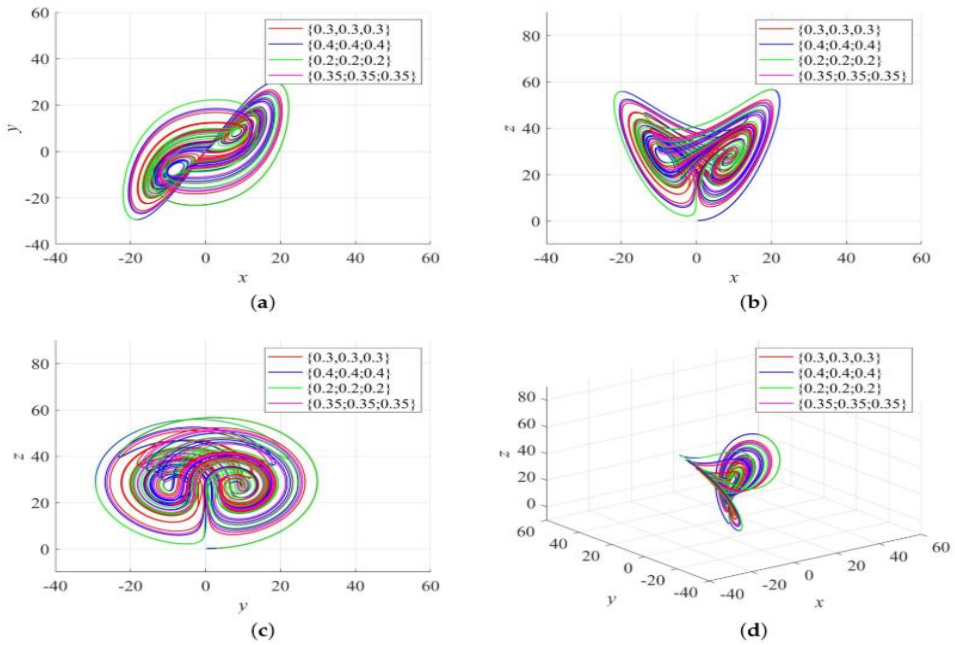

Figure 5: The fractional-order 3D Lorenz system with different initial: a) x-y plane, b) x-z plane, c) y-z plane, d).

Algorithm 1: The algorithm of Scattered operations.
Input: Position key (K), Video frame I (i,j) .
Output: I' (i,j) the scrambled frame.
Step 1: Start.
Step 2: Read all pixels on frame based on pixel locations(i,j).

```
width, height = img.size
        scr = []
        for i in range(width):
            for j in range(height):
              scr.append(img.getpix((i, j)))
              // scr   matrix used  to  store
              pixels of frame.
        exc =  ScatteredIndex(scr)
```

Step 3: Define ScatteredIndex (scr)

```
        exc = list(range(len(scr)))
        random.shuffle(exc)
        return  exc
```

Step 4: Determine ScatteredPixels(scr, exc)

```
        for each pixel scr do
              exc (i,j) = scr (i, j)
        end for
```

Step 5: Determine Store Pixels(img.size, scr)

```
        outImge = Imag.new("RGB", size)
        width, height = size
        pinter = inter(scr)
```

```
        // pinter, inter(scr)   are parameters.
        for x in range(width):
           for y in range(height):
              outImge.putpix((x, y), next(pinter))
        outImge.save(path of scattered frame)
```

Step 6: Repeat the steps from (step2 to step6) video is scattered until it is scattered.

Step 7: End.

4.1.3 Generation of Keys Using a New Lorenzo Chaotic System

To address the research question of chaotic behavior, a three-dimensional chaotic system with fuzzy numbers integrated in a system of equations of the dynamical process is presented as a novel three-dimensional chaotic system and produced the numbers in the form of numerical outputs. The proposed system is derived from the classical Lorenz chaotic system presented in equations (2)-(4) [17] and is based on a modified three-dimensional Lorenz chaotic map that integrates fuzzy numbers, as expressed by the following formulation:

$$\frac{dx}{dt} = \text{fz}\ (a\ (y - x)). \quad (5)$$

$$\frac{dy}{dt} = \text{fz}\ (rx - y - xz). \quad (6)$$

$$\frac{dz}{dt} = \text{fz}\ (xy - bz). \quad (7)$$

It is evident that the obtained phase portraits are consistent with the mathematical formulation of the proposed three-dimensional Lorenz chaotic map, where fz represents the triangular fuzzy function described previously. The chaotic keys generated from the proposed system, namely (K1, K2, K3), successfully passed the statistical randomness tests specified by the National Institute of Standards and Technology (NIST) prior to their utilization in the video encryption process. Figure 5 shows chaotic attractors of all the planes of the three-dimensional Lorenz chaotic map [17].

4.1.4 Encryption Process of Frames Video

The equations that are used to create three real-valued chaos series in the proposed approach are (5)-(7), which are then created to create three key vectors, i.e. (key1, key2, key3). These keys are based on the three-dimensional Lorenz chaotic map through making the right system parameters and the initial conditions. The length of each individual key vector is equal to the sum of the pixels in the original frame i.e. hxw.

At this point, the DNA-encoded frame is split in even-indexed and odd-indexed arrays and subsequently arranged in the R, G and B color positions. The pixel values in the even-indexed arrays are then concatenated with the (key1, key2, key3) and the DNA-XOR operation which is described in Table 2 to get the encrypted even array. The same is done on odd-indexed arrays with (key2, key3, key1) to obtain the encrypted odd array. The final encrypted frame is obtained by merging the two resulting two-dimensional arrays. This encryption process is applied iteratively to all video frames to produce the fully encrypted video sequence.

3.4 Decryption Stage

The decryption is implemented, which is the reverse of the encryption procedure. In this step the encrypted video image is initially divided into individual frames that are then used in the DNA decoding algorithm that is two dimensional in nature. Thereafter, a sequence of decryption operations is applied to each frame, as illustrated in Figure 6.

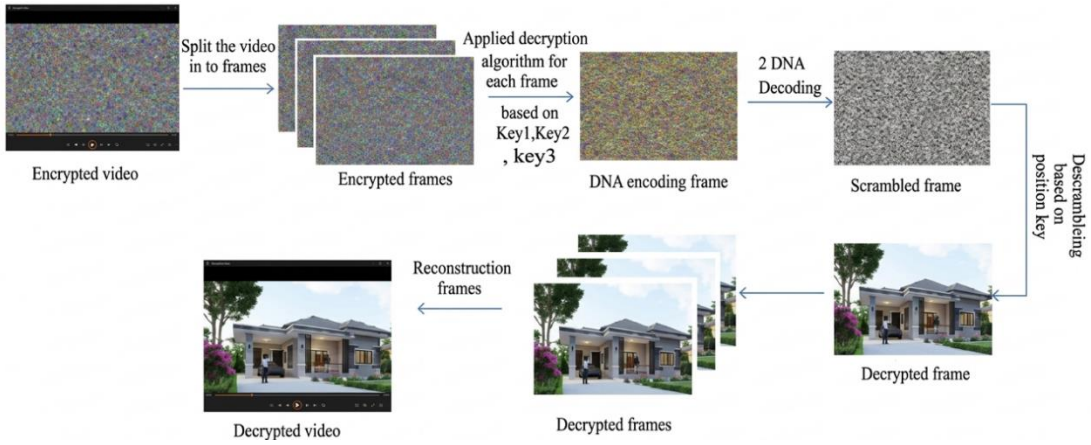

Figure 6: General workflow of the proposed decryption procedure.

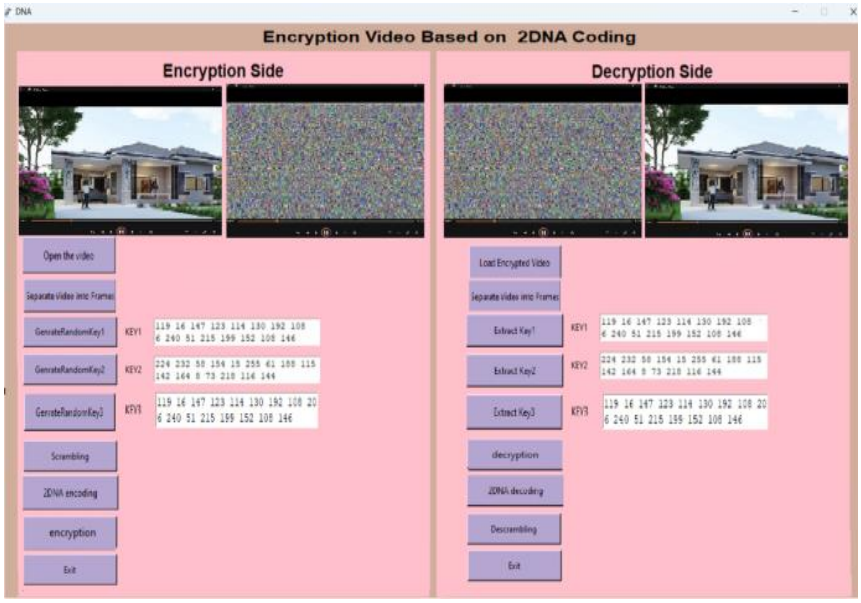

Figure 7: The result of the encrypting and decrypting.

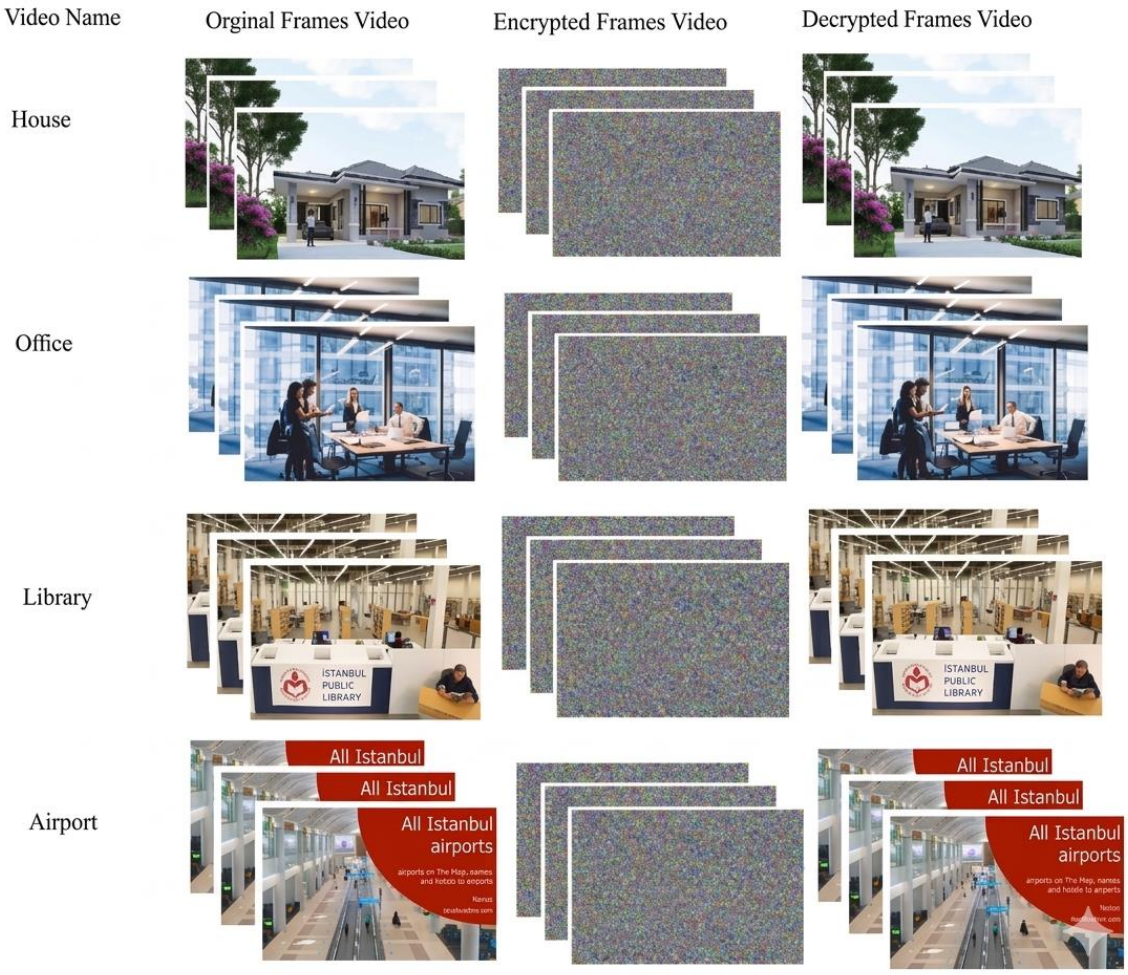

Figure 8: Comparison of original, encrypted and decrypted videos using the proposed scheme.

5 EXPERIMENTAL PROCESS

The experimental results acquired to assess the effectiveness of the suggested video encryption system are presented in this section. A common video sequence called House was chosen and utilized as the test input to conduct the research. The spatial resolution of the video is 1280 × 720 pixels.

Python 3.10 was used for all experimental simulations on a PC with an Intel Core i7 (8th generation) processor running at 2.20 GHz and supported by 8 GB of RAM. Step-by-step implementation and verification of the entire encryption and decryption procedure took place in this environment. Figure 7 shows the general layout of the encryption and decryption process.

Figure 8 shows the original and the respective encrypted video sequences. As it can be seen, the encrypted videos cannot be visually distinguished with random noise, which substantiates the validity of the suggested encryption scheme.

6 RESULTS AND DISCUSSION

To determine whether the proposed encryption method is effective or not, several performance analyses are conducted. They are key space evaluation, correlation analysis and histogram evaluation. Experimental validation is done by a sequence of color video frames. More specifically, four frames are randomly selected among four different videos; a frame is taken out of each video prior to and after encryption process as an attempt to offer the usual examples. The selected frames would provide a suitable and demonstrative evaluation of the performance of the algorithm since it would need much processing time and energy to analyze all the video frames. The results of such tests are presented in the subsequent sections.

6.1 Key Space and Sensitivity Analysis

One of the most critical measurements of the assessment of the envisaged encryption systems may be regarded as the key sensitivity since it evaluates the sensitivity of the system to the tiniest change in the secret key which gets utilized in the encryption and decryption processes. The suggested approach utilizes the Lorenz chaotic map, which is a three-dimensional map when creating the secret keys. As it is illustrated in Figure 9, even a small change in the secret key leaves behind a decrypted video that bears no resemblance to the original video. This fact establishes that the encryption scheme proposed has a high level of key sensitivity which increases its resistance to cryptographic attacks [18].

Figure 9: Encryption process sensitivity to the secret key.

6.2 Entropy

Entropy is a statistical value of information contained in the data set which is a statistical definition of the grayscale intensity values in a video frame, and its value is never negative. In this research, the entropy of the encrypted frames is calculated using equations (8), which can be a valuable method of estimating the level of security of the proposed system [19].

$$H(S) = \sum_{i=0}^{n-1} -P(Si) \log 2\ P(Si). \qquad (8)$$

P(Si) =(Si) = probability of Si, Si the gray scale and n the number of the gray scale in total. Table 3 and Figure 10 have provided the result of entropy test of the video of frames. According to the findings, the entropy of the information of the encryption frames is very near to 8, and it suggests that the system is capable of withstanding the entropy attacks [20].

Table 3: Entropy of original frames and the encrypted ones.

Frames video	House	Office	Library	Airport
The frames of original video	7.8734675	7.5342876	7.8963784	7.2309675
The frames of encrypted video	7.9953457	7.7896542	7.8977698	7.8998543

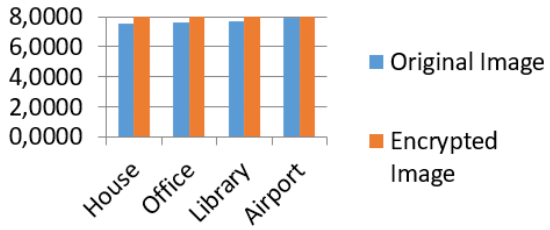

Figure 10: Entropy of original frames and those that have been encrypted.

6.3 Differential Attack Analysis

The detecting factors of the differential attacks are the normalized mean change intensity (UACI) and pixel change rate (NPCR). They play an important role as frame of video information indicators. NPCR is an abbreviation that means percentage of pixels in the encrypted picture that have altered upon the arbitrary fluctuating of a pixel value in the original picture. UACI represents the pixel value change in the encrypted frame following the comparison of the pixel value of the original frame which has already been modified randomly. In the instance where the change in pixels in relation to the original frame is small and the difference between the encrypted frame and the original encrypted frame is vast, the encryption algorithm would effectively be resistant to the differential attacks. The equation is as follows:

$$\text{NPCR} = \frac{D(i,j)}{W*H} * 100\% \quad (9)$$

Where H and W are row and column in frame, respectively and D is estimated by the following formula [20].

$$D(i,j) = \begin{cases} 0 & \text{if original}_{\text{frame}(i,j)} = \text{decryption}_{\text{frame(i,j)}} \\ 1 & \text{otherwise} \end{cases} \quad (10)$$

$$\text{UACI} = \frac{1}{W*H}\left[\sum_{i,j} \frac{C(i,j)-C2(i,j)}{2^{L-1}}\right] * 100\ \% \quad (11)$$

C1(i, j), C2(i, j) are pixel values of the video of cipher frames L is the number of gray levels and H and W are the column and the row respectively of the frame. Table 4 illustrates all the values obtained after the measurement of each value was conducted in order to studies a sequence of frames video with the assistance of the proposed system [21]. The results of NPCR and UCAI are quite acceptable therefore the reconstructed frames resemble a possibility just as the original one does compared to the other techniques.

Table 4: The NPCR and UCAI test.

Frames Test	NPCR	UCAI
House	99.4734	31.2873
Office	99.1928	32.6387
Library	99.4738	33.3894
Airport	99.2784	32.1874
[22]	99.6097	31.4557
[23]	99.6130	30.6100
[24]	99.5800	29.4800

6.4 Histogram Analysis

The encrypted video must have a histogram that is smooth in order to have an efficient encryption algorithm. As it is illustrated in Figure 11, which was entered in MATLAB in 2013, is the color histogram of four video frames prior to the encryption and after the encryption. The color frame histogram of the encrypted frame distribution is evenly distributed in comparison with plaintext frame with the interval distribution probability also being more or less even. As a result, the attackers can hardly make predictions about the frame they were originally generated using the statistical analysis process. The results confirm that the algorithm was able to defeat statistical attacks [25].

6.5 Video Quality

The ability of a video encryption algorithm to produce encrypted frames that are visually distinct from the similar original frames is an important element of its effectiveness. The proposed approach relies on two commonly used quantitative measures the mean squared error (MSE) and the peak signal-to-noise ratio (PSNR) to objectively estimate this difference. Table 5 presents a numerical comparison of the original and encrypted frames using these indicators. While the overall performance is still on par with or better than that of current encryption techniques, the observed MSE and PSNR values verify that the decrypted frames retain the crucial visual information of the original video. Equations (12) and (13) define the analytical expressions of the evaluation metrics [26].

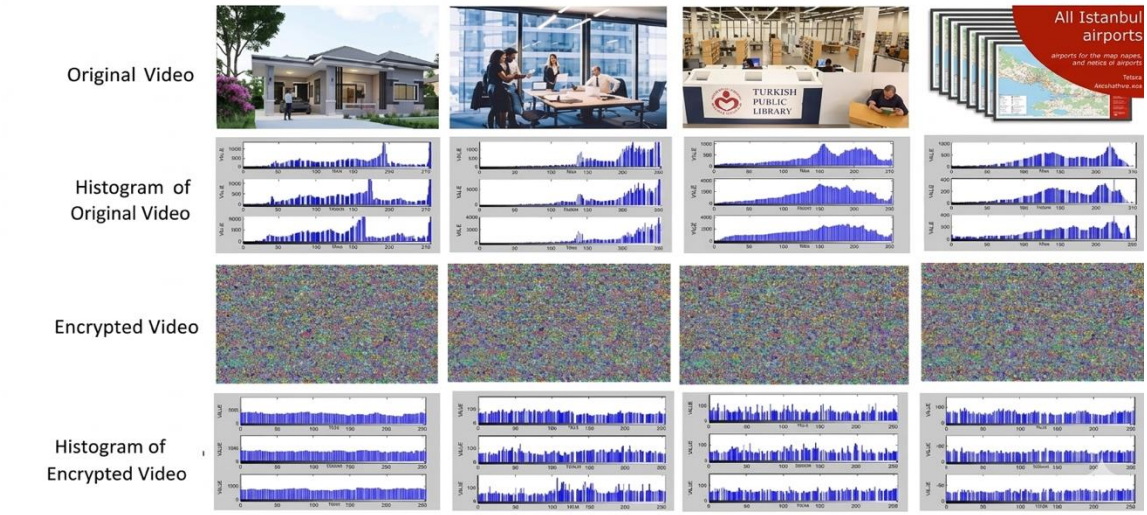

Figure 11: The histogram view of proposed method.

$$\text{PSNR} = 20\ log_{10}\ (\frac{255}{\sqrt{MSE}})\ \text{dB} \quad (12)$$

$$\text{MSE} = \frac{1}{M \times N}\ \sum_{i,j}(p0(i.j) - p1(i.j))^2 \quad (13)$$

Table 5: PSNR and MSE tests.

Frames Test	PSNR	MSE
House	11.8733	3238.6473
Office	13.8945	3875.9584
Library	12.7837	3746.5783
Airport	13.6728	3827.4678
[27]	7.4130	1179.2310
[28]	10.1948	6217.3002

6.6 Correlation Coefficient

The linear group is based on the range and the trend of the two random variables, which is determined by the correlation coefficient, c. When two variables have a strong relationship, the correlation coefficient is precisely equal to 1. If the coefficient is equal to 0, then the two variables are unrelated [28]. The coefficient c can be calculated using (14):

$$c = \frac{\sum_i (x_i - x_m)(y_i - y_m)}{\sum_i \sqrt{\sum_i (x_i - x_m)^2} \sqrt{\sum_i (y_i - y_m)^2}}. \quad (14)$$

The correlation coefficient is an important value that tends to take a value of 1 as the value of the correlation coefficient is close to 0. This correlation coefficient is large since it applies a 3D-chaos way of encrypting the frame and a 2DNA encoding. The range of the value correlation coefficient of the four initial tests reported in Table 6 and Figure 12 suggests that the range was within 0.9937-0.9194 when the encryption frame was within 0.0138-0.0487. Encryption and original frames are not equal in the correlation coefficient and they are shown in Figure 13. A very strong system was a manifestation of this status [28], [29].

As explained in section 7, one can see that the outcome of the integrated 2DNA coding and 3D Lorenz chaos approach of encrypted videos delivers acceptable performance and can be useful in getting around multiple threats. Such scheme is associated with the scattering of the pixels and is typically focused on processes like scrambling. This scheme was designed to be highly efficient in encryption, resistant to a range of attacks with an adequate execution time, reduce the amount of memory, and reduce complexity.

Table 6: The original end encrypted frame Correlation test.

Video frame	House	Office	Library	Airport
Original Frame	0.9245	0.9937	0.9847	0.9194
Encrypted	0.0382	0.0138	0.0245	0.0487

Figure 12: The Correlation test of original end encrypted frames.

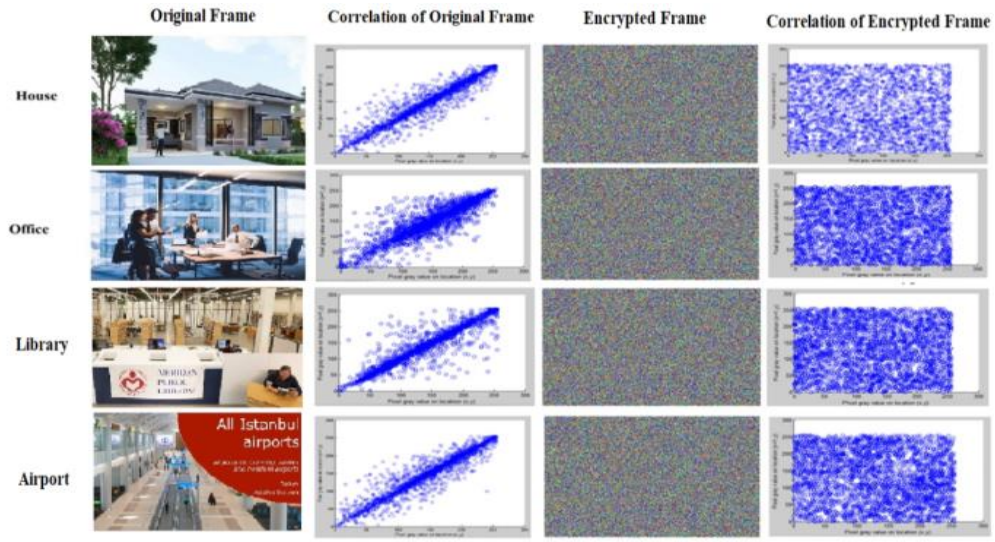

Figure 13: The correlation test of original and encrypted frames of proposed method.

6.7 NIST Analyses

The National Institute of Standards and Technology (NIST) offers fifteen statistical tests that are used to test the randomness and strength of encryption algorithms. Results of the proposed scheme are presented in Tables 7 and 8, with majority of the tests obtaining p-values exceeding 0.01 which is a satisfactory value of randomness in order to have a secure video encryption. The experiment was done on two dynamic keys produced by the chaotic system with stream length of 128 bits, and the output of the experiment indicates that dynamic key. compared to the fixed-key graph, encryption has more randomness [30].

Table 7: Dynamic random key1 NIST test results.

ID	NIST Test	P_value	P_value >0.01
1	Approximate entropy	0.8382	Pass
2	Cumulative sums	0.4285	Pass
3	Non-overlapping T.M	0.8934	Pass
4	Longest run of ones	0.1456	Pass
5	Frequency within a block	0.9345	Pass
6	Serial	0.5937	Pass
7	Spectral	0.2985	Pass
8	Runs	0.1825	Pass
9	Frequency within a block	0.9345	Pass

Table 8: NIST test result of dynamic random key2.

ID	NIST Test	P_value	P_value >0.01
1	Frequency	0.7384	Pass
2	Frequency within a block	0.9387	Pass
3	Runs	0.2839	Pass
4	Longest run of ones	0.9387	Pass
5	Spectral	0.2849	Pass
6	Cumulative sums	0.8937	Pass
7	Serial	0.7387	Pass
8	Approximate entropy	1.1839	Pass
9	Non-overlapping T.M	0.8398	Pass

Table 9: Encryption time (average).

Name of Video	Maxmum ROIs of Frame	Time of Encryption (sec.)
House	4	9.20
Airport	5	8.48
Company	6	8.17
Street	15	12.01
Reception	3	11.02
Office	6	7.84

6.8 Time Consuming

An efficient encryption algorithm must have high speed of execution in order to be practicable. As presented in Table 9, the proposed ROI-based approach has the advantage of low average encryption time on the various test videos which proves to be an efficient way of processing and can be used in real-time surveillance [31].

7 CONCLUSIONS

In this study, a robust video encryption and decryption scheme has been proposed. To enhance security, the input video is first scrambled using multiple techniques prior to the application of two-dimensional DNA (2DNA) encoding. Subsequently, the encryption process is carried out by integrating fuzzy triangular numbers into a modified three-dimensional Lorenz chaotic map, which is employed for secret key generation, resulting in an encrypted video stream. Decryption is achieved by applying the inverse operations of the encryption process.

To validate the effectiveness of the proposed method, extensive simulation experiments were conducted, including entropy evaluation, differential attack analysis, histogram analysis, key sensitivity and key space assessment, as well as video quality analysis. The results of the experiment indicate that the offered algorithm has high security performance and can be effectively used to withstand different cryptographic attacks. Furthermore, the obtained results indicate that the proposed scheme is competitive with existing chaotic video encryption approaches and satisfies essential requirements for secure video transmission.

REFERENCES

[1] T. H. Obaida, A. S. Jamil, and N. F. Hassan, "A review: Video encryption techniques, advantages and disadvantages," Webology, vol. 19, no. 1, 2022.

[2] M. Samiullah, W. Aslam, H. Nazir, M. I. Lali, B. Shahzad, M. R. Mufti, and H. Afzal, "An image encryption scheme based on DNA computing and multiple chaotic systems," IEEE Access, vol. 8, pp. 25650-25663, 2020.

[3] S. Pronika and S. Tyagi, "Performance analysis of encryption and decryption algorithm," Indonesian Journal of Electrical Engineering and Computer Science, vol. 23, no. 2, pp. 1030-1038, 2021.

[4] S. Bhattacharjee, S. Bhattacharya, A. Chatterjee, S. Bansal, and S. Shukla, "A Method for Securely Transmitting Large Video Files Using Chaotic Compression and Encryption," arXiv, May 2026, [Online]. Available: https://doi.org/10.48550/arXiv.2605.16563.

[5] Fitwi, Y. Chen, and S. Zhu, "Lightweight frame scrambling mechanisms for end-to-end privacy in edge smart surveillance," IET Smart Cities, vol. 4, no. 1, pp. 17-35, 2022.

[6] P. Mukherjee, H. Garg, C. Pradhan, S. Ghosh, S. Chowdhury, and G. Srivastava, "Best fit DNA-based cryptographic keys: the genetic algorithm approach," Sensors, vol. 22, no. 19, p. 7332, 2022.

[7] S. Zhou, Y. Wei, Y. Zhang, and L. Teng, "Novel chaotic image cryptosystem using dynamic DNA coding," International Journal of Modern Physics C, vol. 35, no. 06, p. 2450068, 2024.

[8] V. Patidar and G. Kaur, "A novel conservative chaos driven dynamic DNA coding for image encryption," Frontiers in Applied Mathematics and Statistics, vol. 8, p. 1100839, 2023.

[9] Yasser, M. A. Mohamed, A. S. Samra, and F. Khalifa, "A chaotic-based encryption/decryption framework for secure multimedia communications," Entropy, vol. 22, no. 11, p. 1253, 2020.

[10] X. Li, H. Yu, H. Zhang, X. Jin, H. Sun, and J. Liu, "Video encryption based on hyperchaotic system," Multimedia Tools and Applications, vol. 79, no. 33, pp. 23995-24011, 2020.

[11] K. M. Hosny, M. A. Zaki, N. A. Lashin, and H. M. Hamza, "Fast colored video encryption using block scrambling and multi-key generation," The Visual Computer, vol. 39, no. 12, pp. 6041-6072, 2023.

[12] L. Moysis, C. Volos, S. Jafari, J. M. Munoz-Pacheco, J. Kengne, K. Rajagopal, and I. Stouboulos, "Modification of the logistic map using fuzzy numbers with application to pseudorandom number generation and image encryption," Entropy, vol. 22, no. 4, p. 474, 2020.

[13] S. A. Hadi, S. A. Ali, and M. J. Jawad, "Binary image encryption, chaotic and DNA encoding," in Next Generation Internet of Things 2021, Singapore: Springer Singapore, 2021, pp. 295-312.

[14] N. A. Ali, A. M. S. Rahma, and S. H. Shaker, "3D Polygon Mesh Messages Encryption by 3D Lorenz Chaotic Map," Int. J. Interact. Mob. Technol., vol. 15, no. 15, p. 103, 2021.

[15] N. R. Manihira and A. K. Dauda, "Chaotic map image encryption and DNA encoding," International Journal of Engineering Research and Technology, vol. 10, no. 11, pp. 1-5, 2022.

[16] H. Wen, Z. Liu, H. Lai, C. Zhang, L. Liu, J. Yang, Y. Lin, Y. Li, Y. Liao, L. Ma, and Z. Chen, "Secure DNA-coding image optical communication using non-degenerate hyperchaos and dynamic secret-key," Mathematics, vol. 10, no. 17, p. 3180, 2022.

[17] M. Dua, D. Makhija, P. Y. L. Manasa, and P. Mishra, "3D chaotic map-cosine transformation based approach to video encryption and decryption," Open Computer Science, vol. 12, no. 1, pp. 37-56, 2022.

[18] D. Xu, G. Li, W. Xu, and C. Wei, "Design of artificial intelligence image encryption algorithm based on hyperchaos," Ain Shams Engineering Journal, vol. 14, no. 3, p. 101891, 2023.

[19] S. Du and G. Ye, "IWT and RSA based asymmetric image encryption algorithm," Alexandria Engineering Journal, vol. 66, pp. 979-991, 2023.

[20] S. J. Al-Saeed and A. S. Mahmood, "Securing videos using chaotic maps in a parallel processing environment," AIP Conference Proceedings, vol. 3282, no. 1, p. 030010, Apr. 2025, [Online]. Available: https://doi.org/10.1063/5.0265404.

[21] Y. Alghamdi, A. Munir, and J. Ahmad, "A lightweight image encryption algorithm based on chaotic map and random substitution," Entropy, vol. 24, no. 10, p. 1344, 2022.

[22] H. Liu, B. Zhao, J. Zou, L. Huang, and Y. Liu, "A lightweight image encryption algorithm based on message passing and chaotic map," Security and Communication Networks, vol. 2020, no. 1, p. 7151836, 2020.

[23] A. A. Abdallah and A. K. Farhan, "A new image encryption algorithm based on multi chaotic system," Iraqi Journal of Science, pp. 324-337, 2022.

[24] M. Gupta, K. K. Gupta, and P. K. Shukla, "Session key based fast, secure and lightweight image encryption algorithm," Multimedia Tools and Applications, vol. 80, no. 7, pp. 10391-10416, 2021.

[25] M. A. A. K. Al-Dabbas, A. Alabaichi, and A. S. Abbas, "Dual method cryptography image by two force secure and steganography secret message in IoT," TELKOMNIKA (Telecommunication Computing Electronics and Control), vol. 18, no. 6, pp. 2928-2938, 2020.

[26] W. Alexan, N. H. E. Shabasy, N. Ehab, et al., "A secure and efficient image encryption scheme based on chaotic systems and nonlinear transformations," Scientific Reports, vol. 15, p. 31246, 2025, [Online]. Available: https://doi.org/10.1038/s41598-025-15794-z.

[27] S. M. Hameed, H. A. Sa'adoon, and M. Al-Ani, "Image encryption using DNA encoding and RC4 algorithm," Iraqi Journal of Science, pp. 434-446, 2018.

[28] P. Tian and R. Su, "A novel virtual optical image encryption scheme created by combining chaotic S-Box with double random phase encoding," Sensors, vol. 22, no. 14, p. 5325, 2022.

[29] D. Jiang, Z. Yuan, W.-X. Li, and L.-L. Lu, "Real-time chaotic video encryption based on multithreaded parallel confusion and diffusion," Information Sciences, vol. 666, p. 120420, 2024, doi: 10.1016/j.ins.2024.120420.

[30] H. Lin, G. H. Hu, J. S. Chen, J. J. Yan, and K. H. Tang, "New design of cryptosystems video/audio streaming with dynamic synchronized chaos-based random keys," Multimedia Systems, vol. 28, no. 5, pp. 1793-1808, 2022.

[31] S. Cai, L. Huang, X. Chen, and X. Xiong, "Symmetric plaintext-related color image encryption system, which is founded on bit permutation," Entropy, vol. 20, no. 4, p. 282, 2018.