International Journal of Safety and Security Engineering
Vol. 16, No. 2, February, 2026, pp. 373-381
Journal homepage: http://iieta.org/journals/ijsse

Video Encryption Using 7D Hyperchaotic System with Two-Level Discrete Wavelet Transform and Rubik's Cube Scrambling

Ashwaq A. Kadhim[1*], Sadiq A. Mehdi[2], Duaa F. Al Edhary[1]

[1] Faculty of Physical Education and Sports Sciences, University of Kufa, Najaf 54001, Iraq
[2] Department of Computer Science, College of Education, University of Almustansirya, Baghdad 10001, Iraq

Corresponding Author Email: ashwaka.kadhim@uokufa.edu.iq

https://doi.org/10.18280/ijsse.160212

Received: 11 December 2025
Revised: 4 February 2026
Accepted: 13 February 2026
Available online: 28 February 2026

Keywords:
video encryption, 7D hyperchaotic system, Discrete Wavelet Transform, Rubik's Cube, Number of Pixels Change Rate, Unified Average Changing Intensity, Peak Signal-to-Noise Ratio, Structural Similarity Index

ABSTRACT

Securing visual data has become crucial, particularly following the advancement of hacking techniques. This research presents a new video encryption method based on integrating a 7D hyperchaotic system, second-level Discrete Wavelet Transform (DWT), and Rubik's Cube-based scrambling, with parallel YCbCr channel processing and dynamic inter-frame key updating. The system's efficiency was tested using a set of metrics, including Number of Pixels Change Rate (NPCR), Unified Average Changing Intensity (UACI), Peak Signal-to-Noise Ratio (PSNR), and Structural Similarity Index (SSIM), where results demonstrated the effectiveness of the proposed system, achieving NPCR = 99.69%, UACI = 33.46%, entropy ≈ 8, PSNR = ∞ (MSE = 0), and SSIM = 1.0, exhibiting high resistance against various analytical and differential attacks and showing perfect matching between the original and decrypted video. The method demonstrated an execution time of 0.031 s per frame with theoretical security guarantees against known-plaintext, chosen-plaintext, and temporal correlation attacks through dynamic inter-frame key updating.

1. INTRODUCTION

In the era of the digital revolution and advanced communications, the use of digital visual content has witnessed tremendous growth across various fields, where videos are employed in medical applications, military communications, distance education platforms, and social media, requiring considerable attention to security and privacy issues. This rapid growth has been accompanied by an accelerating increase in security risks, cyber threats, and electronic attacks, as attack methods have evolved to include advanced techniques such as sophisticated statistical analysis, differential attacks, and brute force attacks enhanced by artificial intelligence [1]. This reality necessitates the development of more robust and complex encryption systems capable of confronting these advanced threats while maintaining operational efficiency [2].

Traditional cryptographic methods, such as AES and DES, are computationally demanding even though they offer strong security and can theoretically encrypt video data. When used directly on large-scale, high-resolution video streams, they can result in enormous processing costs and considerable latency. As a result, different strategies have been investigated to better strike a compromise between processing speed and good security [3]. Digital video possesses unique characteristics, including massive data volume, strong correlation between spatially and temporally adjacent pixels, the need for instant processing in live applications, and the necessity of maintaining compression quality to conserve storage space and transmission capacity. These particular challenges require innovative solutions that consider the statistical and structural properties of visual content [4]. Therefore, recent research focuses on developing hybrid systems that combine different techniques to provide advanced encryption solutions that unite superior security with efficiency. Chaotic systems represent one of the most prominent of these techniques, possessing unique properties that make them ideal for generating strong encryption keys. These systems are characterized by exhibiting seemingly random behavior despite their deterministic nature and providing regular distribution of generated values [5]. Nevertheless, the literature on cryptanalysis has revealed recognized flaws in traditional low-dimensional chaos-based cryptosystems. They frequently experience dynamical degradation when implemented on finite-precision digital devices, resulting in short cycle durations and susceptibilities to phase-space reconstruction attacks [6, 7]. This study uses a high-dimensional (7D) hyperchaotic system, which offers much more complex dynamics, more positive Lyapunov exponents, and a considerably wider key space, to overcome these intrinsic vulnerabilities and successfully fend off conventional cryptanalytic attacks. Conversely, the Discrete Wavelet Transform (DWT) establishes a rigorous mathematical framework for analyzing and representing visual data in the frequency domain. Through signal decomposition, DWT effectively separates high-frequency components (fine details) from low-frequency components (general structural features). This decomposition facilitates the application of multiple

encryption levels specifically designed for each frequency sub-band. Additionally, employing second-level DWT enhances analysis precision and enables a more accurate and robust encryption process [8].

The Rubik's Cube technique has proven its effectiveness as a powerful tool for scrambling data in a complex and organized manner [9], where this technique applies multiple and diverse operations such as row and column rotation, inversion, and diagonal transposition, resulting in a sophisticated scrambling mechanism capable of breaking statistical patterns in a nonlinear fashion while ensuring complete reversibility [10]. This latter characteristic guarantees precise recovery of original data after decryption.

This research presents a novel hybrid video encryption method that combines three advanced techniques: a 7D chaotic system, second-level DWT, and Rubik's Cube algorithm. A sophisticated methodology is developed for processing all color channels in YCbCr space in a parallel and specialized manner, ensuring comprehensive and effective protection of the entire visual content. It also achieves advanced encryption performance that combines high security and efficiency, rendering the method capable of confronting current and future cyber threats.

Main Contributions: (1) Integration of a 7D hyperchaotic system with two-level DWT and Rubik's Cube for comprehensive video encryption, (2) parallel YCbCr channel processing with specialized chaotic keys, (3) dynamic inter-frame key updating, preventing temporal attacks, and (4) fast execution suitable for real-time applications.

Section 2 reviews previous studies. Section 3 presents theoretical foundations. Section 4 describes the proposed method. Section 5 reports experimental results and analysis. Section 6 concludes.

2. PREVIOUS STUDIES

The field of video encryption is witnessing rapid growth in research and development, as researchers seek to develop methods capable of addressing the unique challenges posed by moving video data, particularly its large volume and the high spatial and temporal correlation between successive frames. Khudair et al. [11] conducted a comparative study between the CAST-128 and RSA encryption algorithms for video frame encryption, relying on the entropy value as an evaluation criterion. The results demonstrated the superiority of CAST-128 using an adaptive key extracted from the main diagonal of each frame. However, both algorithms treat each frame as a generic data block similar to text, ignoring the high spatial correlation among its pixels. This results in detectable statistical patterns in the encrypted histogram, a well-documented weakness of block cipher applications to multimedia data, where inter-pixel spatial correlation is not accounted for.

To accelerate the encryption process, other studies have turned to chaotic systems. Jiang et al. [12] proposed a strategy based on multi-threaded parallel computing with low-dimensional chaotic maps (1D and 2D), achieving an encryption time of less than 42 milliseconds through five rounds of confusion and diffusion. Nevertheless, this approach requires high-performance multi-core processors, which restricts its application in resource-constrained environments, such as embedded systems and mobile broadcasting applications.

Similarly, Hilal and Al-Azawi [13] proposed a selective encryption system for compressed video based on the H.266/VVC standard, using a 2D chaotic map (2D-SCLM). The study focused on encrypting reference frames (I-frames) and motion vectors. Despite the reduced encryption time and its compatibility with the compression standard, relying solely on selective encryption is insufficient; the unencrypted frames (P-frames and B-frames) expose motion vectors, which can be exploited to achieve an approximate reconstruction of the content via temporal inference attacks.

Furthermore, Rajaonarison and Randriamitantsoa [14] presented a video encryption algorithm based on discrete 2D chaotic maps, such as the Tinkerbell map, to generate encryption keys through three cascading schemes that combine confusion and diffusion phases to encrypt both the frames and the audio track. However, the algorithm generates a static chaotic sequence applied uniformly across all frames without any mechanism to update the diffusion key between successive frames. Consequently, two visually identical frames will produce identical ciphertext—a well-known vulnerability in static-key chaotic encryption systems that facilitates known-plaintext attacks and temporal correlation analysis.

El Kinani et al. [15] proposed a hybrid scheme combining DWT for compression and hybrid encryption, Advanced Encryption Standard-Elliptic Curve Cryptography (AES-ECC) in an Internet of Things (IoT) environment. However, relying on a single-level DWT concentrates most of the signal's energy into the single LL1 subband. Thus, recovering this subband alone is sufficient to reconstruct the majority of the visual content. This structural concentration of energy in a single subband represents an inherent limitation absent in multi-level decomposition approaches, which distribute the energy across a greater number of frequency bands. An encryption approach based on composite chaotic maps (Tent and Arnold) was proposed by Tu et al. [16] to jumble RGB channels and encrypt them using the XOR operation, resulting in a correlation coefficient between neighboring pixels that is nearly zero. Nonetheless, a strong color association between the three channels is preserved when using the RGB color space. Studies have demonstrated that this association gives attackers more information, allowing them to examine cross-channel variations in order to deduce the key. By using the YCbCr color space, which fully distinguishes luminance from chrominance, this flaw is completely removed.

Murari et al. [17] introduced a technique for the selective encryption of RGB channels using the One-Time Pad algorithm and permutation techniques, applied to only 25% to 50% of the frames. This approach combines three overlapping limitations: First, selective encryption leaves between 50% and 75% of the frames exposed, allowing temporal inference attacks to exploit unencrypted frames to reconstruct adjacent encrypted ones. Second, the reliance on the RGB color space retains a high color correlation among its channels. Third, the key lacks any plaintext-dependent updating mechanism, meaning that two visually identical frames will produce identical ciphertext, enabling pattern-based cryptanalysis.

Based on the aforementioned review, current approaches exhibit six major drawbacks: (1) Because they ignore the strong spatial correlation between pixels in a single frame, standard block ciphers are insufficient for video data. (2) Some systems require high-performance computing infrastructure, which limits their use on devices with limited resources. (3) When using a single-level wavelet transform, there may be

residual correlation between pixels due to the restricted frequency separation. (4) Selective encryption is insufficient for offering complete security, making unencrypted frames susceptible to partial reconstruction and temporal inference attacks. (5) Relying on the RGB color space is less effective in color decorrelation than the YCbCr color space created especially for video data. (6) The lack of a plaintext-dependent key updating mechanism allows temporal analysis attacks to take advantage of the diffusion key's static nature over subsequent frames by producing identical ciphertext from two visually identical frames.

The current study addresses these limitations collectively through an integrated encryption system. To address the first two limitations, a 7D hyperchaotic system is employed, providing a key space of approximately 2^{884} with a computational complexity that allows it to run on mid-range devices without requiring specialized processors. To address the third limitation, a two-level DWT is used, producing seven sub-bands instead of four, thus ensuring deeper frequency separation and more comprehensive pixel decorrelation. To address the fourth limitation, the entire video is encrypted without selectivity, closing the security gaps left by partial encryption. To address the fifth limitation, the video is converted to the YCbCr space with a separate chaotic key applied to each channel in parallel. Finally, to address the sixth limitation, the proposed system uniquely employs a plaintext-dependent key updating mechanism that links the diffusion key to the content of each frame, ensuring that two visually identical frames will produce completely different ciphertexts and breaking the temporal correlation between all successive frames.

3. THEORETICAL FOUNDATIONS

3.1 Chaotic systems

Chaos is a widespread phenomenon in nature that is widely used in diverse applications in many fields of study, such as physics, engineering, mathematics, biology, secure communications, high-performance circuit design for telecommunications, and information processing. It has a behavior similar to noise and is present in nonlinear dynamical systems. The sequences generated by chaotic systems are highly sensitive to their initial conditions, unpredictable, have long periodicities, and have a spread spectrum. Highly chaotic systems tend to have very complex dynamics. A highly chaotic system is often defined as one with more than one positive Lyapunov exponent, meaning the number of propagation directions is greater than one, resulting in the system exhibiting chaotic behavior and high randomness [18]. Therefore, the more chaotic a chaotic system is, the more complex it is and therefore unpredictable for long periods.

In this research, we use a 7D hyperchaotic system [19], which has more complex dynamic properties than low-dimensional chaotic systems. This system is obtained as follows:

$$\begin{aligned} \frac{dx}{dt} &= -\sigma x + \rho y + \delta w - \eta v \\ \frac{dy}{dt} &= \Omega x - \Psi xz - \mu y \\ \frac{dz}{dt} &= -\phi z + xy + \eta v \\ \frac{dw}{dt} &= -w - \mho yz - \phi vp \\ \frac{dv}{dt} &= yp + \beta xp - \eta z - v \\ \frac{du}{dt} &= \omega u - \mu zwp + \Omega xp \\ \frac{dp}{dt} &= -\alpha p + xy + \eta v \end{aligned} \tag{1}$$

This system has states x, y, z, u, v, w, p, and t, which are positive numbers. Its parameters include σ, ρ, δ, Ψ, ϕ, ℧, β, ω, μ, α, η, and Ω. The system exhibits chaotic behavior and a strange attractor when these parameters are set to specific values: σ = 14, ρ = 11, δ = 0.4, η = 0.5, Ω = 30, Ψ = 2.5, ϕ = 5, ℧ = 3, β = 2, ω = 15, μ = 4, and α = 13. This chaotic nature is further demonstrated with the initial conditions: x(0) = 0.1, y(0) = 0.5, z(0) = 3.5, w(0) = 0.6, u(0) = 0.4, v(0) = 0.1, and p(0) = 0.6.

In the present work, the 7D hyperchaotic system (Eq. (1)) is numerically integrated using the fourth-order Runge-Kutta (RK4) method with a fixed step size of h = 0.01. The system exhibits fully developed hyperchaotic behavior from the specified initial conditions, as evidenced by three positive Lyapunov exponents (L1 = 0.929593, L2 = 0.327552, L3 = 0.001271) [17, 18] and confirmed through NIST statistical randomness tests [18]. Accordingly, the chaotic sequences used for key generation are derived directly from these initial conditions without discarding transient samples.

3.2 Discrete Wavelet Transform

DWT is an advanced mathematical technique that analyzes a signal into different frequency components while preserving both spatial and temporal information. This makes it an ideal tool for representing visual data in the frequency domain [20]. DWT offers multi-resolution analysis capabilities, which are particularly useful for various image processing tasks, including denoising, compression, enhancement, and feature extraction. Within the context of encryption, DWT provides unique features that make it an optimal choice for advanced security applications [21].

The 2-D DWT can be used in visual processing to decompose an image into four sub-bands. It effectively separates high-frequency information (fine details) from low-frequency information (general image properties). A second-level DWT, which involves applying the transform twice, provides a deeper level of frequency analysis. The first level produces four sub-matrices: LL1 (approximation coefficients), LH1 (horizontal details), HL1 (vertical details), and HH1 (diagonal details). The second level then applies the transform only to the LL1 matrix, yielding more precise coefficients: LL2, LH2, HL2, and HH2 [22].

The primary advantages of using DWT for encryption include: Energy Compaction—Most of the important information is concentrated into a few coefficients, allowing for selective and efficient encryption. Multi-resolution Representation—This provides exceptional flexibility for applying different, graded levels of encryption to various image details. Noise Robustness—Encrypting in the frequency domain is less affected by minor noise and slight distortions [8].

3.3 Rubik's Cube

The Rubik's Cube is a 3D (3 × 3 × 3) puzzle of six faces. Each side has nine stickers, which come in six different base colors spread evenly across the cube. Any of the faces can be rotated 90 degrees, clockwise or counter-clockwise. The cube has three middle layers, hence there are 18 quarter-turns possible in a single step. The step is defined by the Face-Turn Metric, which takes a quarter-turn of one face as a step. In contrast, the Alternative Quarter-Turn Metric takes a half-turn as two steps [23]. Complexity and States: The total possibilities for states of a 3 × 3 × 3 Rubik's Cube are:

$$\frac{(8! \times 3^7) \times (12! \times 2^{11})}{2} \approx 4.3 \times 10^{19}$$

There are around 4.3×10^{19} possible combinations, which is about 43 quintillion. The incredible number of permutations demonstrates just how complex the Rubik's Cube is. No wonder then that this puzzle is helping inspire scrambling techniques and encryptions [24].

4. THE PROPOSED METHOD

The proposed method processes each video frame independently using dynamically updated keys to ensure maximum security. Figure 1 illustrates the flow chart of the proposed method.

1. Initially, chaotic sequences are generated using a chaotic system in (Eq. (1)), where the system is initialized with specific initial conditions and system parameters. The chaotic equations are solved using the fourth-order Runge-Kutta method with a fixed step of h = 0.01. These sequences are employed to generate seven encryption keys: three keys for the color channels, three additional keys for the XOR operation, and one key for the Rubik's Cube operations.

2. For each frame in the video, it is read from the original file and converted from RGB to the YCbCr color space. This conversion enables specialized processing for each component. The Y channel contains luminance information and essential details, while the Cb and Cr channels contain chrominance information. This separation provides flexibility in applying encryption levels according to the importance of each component.

3. The DWT is applied at two successive levels. At the first level, the data for each channel is decomposed into four components representing details in different directions using the Haar wavelet, where the LL1 component contains the fundamental information, while the other components (LH1, HL1, HH1) contain edge details in various directions. At the second level, the wavelet transform is applied exclusively to the LL1 component, yielding four additional components (LL2, LH2, HL2, HH2). This multi-level analysis provides an optimal representation of the data in the frequency domain, resulting in seven subcomponents. DWT is applied prior to Rubik's Cube scrambling so that encryption operates on frequency-domain coefficients rather than raw pixel values, enabling independent and targeted scrambling of subbands that carry structurally distinct information. The intermediate IDWT after second-level scrambling is a necessary reconstruction step: since LL1 was decomposed into four second-level subbands, it must be rebuilt from its encrypted components before the complete first-level reconstruction can proceed.

4. All these components undergo encryption using techniques inspired by the Rubik's Cube. This process involves a series of complex geometric operations such as row and column rotations, diagonal permutations, and reflections. The number and sequence of these operations are determined by the chaotic keys, ensuring that each component undergoes a unique and complex shuffling pattern. The scrambling process applies n operations determined by:

$$n = max(50, floor(\sum |k_i|))$$

where, $k_i \in$ chaotic_key. Each operation type $t \in \{1,2, \ldots ,8\}$ is selected by:

$$t = (floor(|k_i| \times 1000) \, mod \, 8) + 1$$

corresponding to row rotation, column rotation, row flip, column flip, 90° rotation, 180° rotation, 270° rotation, and diagonal swap. The two-level DWT decomposes each channel into $4^L = 4^2 = 16$ subbands (where L = 2 is the decomposition level), enabling fine-grained frequency-domain scrambling superior to single-level approaches ($4^1 = 4$ subbands).

5. Upon completion of the second-level encryption, the first level is reconstructed using the Inverse Discrete Wavelet Transform (IDWT). Subsequently, the first-level coefficients undergo encryption using the same techniques. The complete frame is then reconstructed from all encrypted coefficients.

6. In the final encryption stage, an XOR operation is applied using a chaotic key with unique values for each color channel. The XOR operation applies bit-level diffusion:

$$E(x,y) = D(x,y) \oplus K_{chaotic}(x,y)$$

where, $K_{chaotic}$ is derived from unique segments of the 7D sequence for each channel, ensuring non-repetitive keys across frames and channels.

7. After completing the encryption of the three channels independently, they are merged to form a complete encrypted frame, which is then converted from YCbCr to RGB color space and saved in the encrypted video file.

8. Before processing each frame, keys are updated through a dual-level dynamic mechanism derived exclusively from the 7D hyperchaotic sequence without re-initializing its initial condition, which is a deliberate design choice to avoid the periodicity vulnerabilities associated with repeated chaotic seeding. At the spatial scrambling level, the Rubik's Cube key for each frame is re-derived by selecting a frame-index-dependent segment from the chaotic trajectory of the seventh state variable (p) of the 7D system:

$$\text{offset}_{\text{rubik}}(n) = \text{mod}(\text{n} \times \text{C} \times 7919, \text{L-16}) + 1$$

where, n is the frame index, C is a channel-specific constant derived from the ASCII encoding of the channel label (C = 89 for Y, C = 165 for Cb, C = 181 for Cr), L is the total chaotic sequence length, and 7919 is a prime number selected to eliminate periodicity in offset distribution across frames. At the diffusion level, a plaintext-dependent key updating mechanism integrates each frame's pixel statistics into the XOR key to determine a unique offset into the chaotic sequence:

$$K_{\text{dynamic}}(n) = \mathrm{K}_{\text{xor}}(n) + \text{mod}\,(\sum P_n(\mathrm{x,y}), 256)$$

$$\text{offset}_{\text{xor}}(n) = \text{mod}(\left\lfloor \sum K_{\text{dynamic}}(n) \times 1000 \right\rfloor, \text{L-P}) + 1$$

The XOR key is then updated for the subsequent frame as:

$$K_{\text{xor}}(\mathrm{n+1}) = \text{mod}\,(K_{\text{xor}}(n) + \frac{\text{mod}\,(\sum p_n, 256)}{256} + \delta_c, 1)$$

where, δ_c is a channel-specific constant ($\delta_Y = 0.0155$, $\delta_{Cb} = \delta_{Cr} = 0.0135$). This ensures that each frame is encrypted using a unique content-dependent segment of the 7D chaotic trajectory, completely eliminating inter-frame temporal correlation.

9. Steps 2-8 repeat for all frames. After processing all frames, the encrypted video is saved.

Decryption applies inverse operations (inverse XOR, inverse Rubik's, IDWT) using identical chaotic keys, achieving perfect reconstruction.

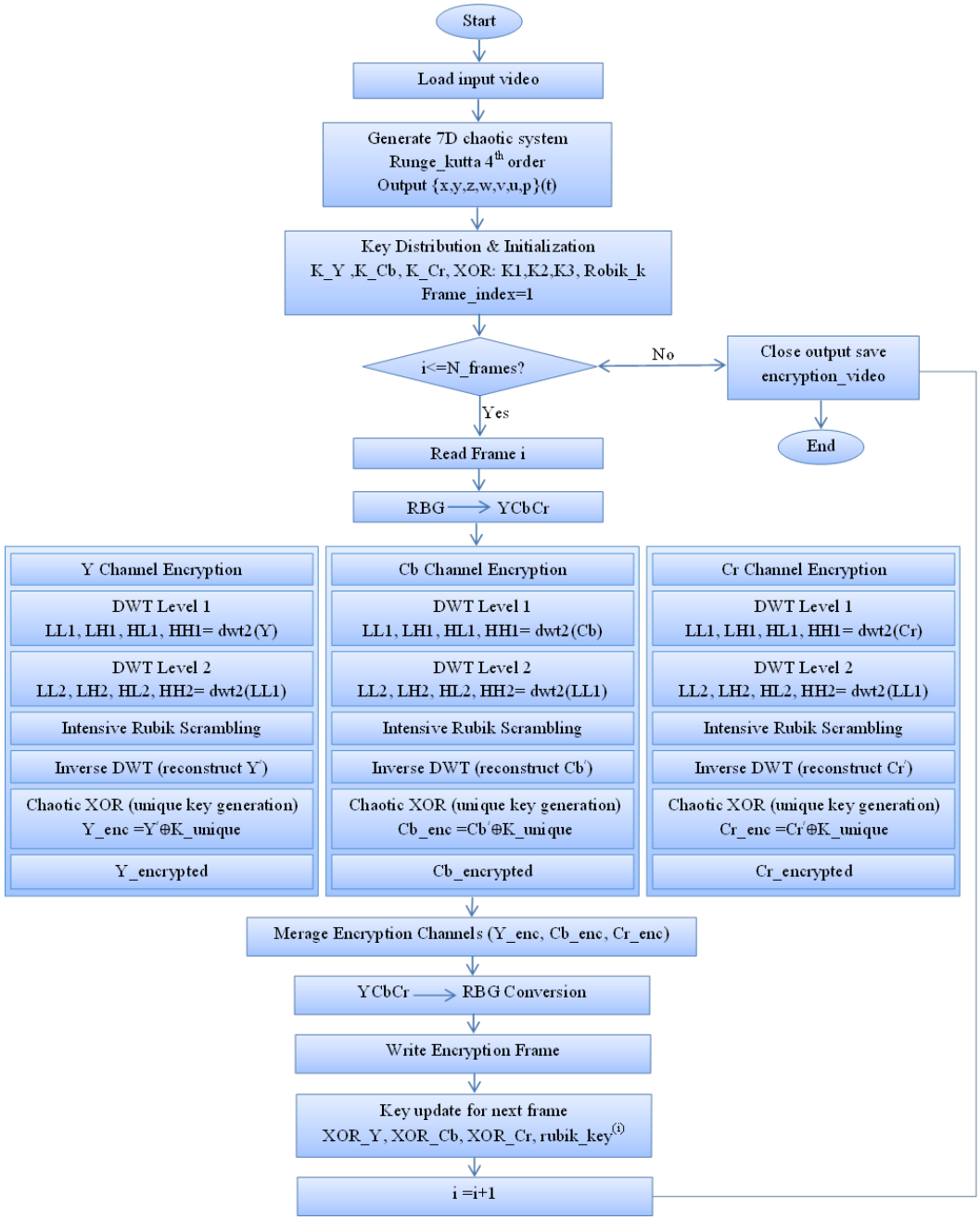


Figure 1. Flowchart of the proposed method

5. EXPERIMENTAL ANALYSIS AND RESULTS

This section presents a series of experimental tests that demonstrate the efficiency of the proposed method and its resistance to various attacks. The method was applied to a diverse set of color videos of different types and sizes. All experiments were conducted using MATLAB R2025a on an Intel Core i5 processor with 8 GB RAM. Table 1 illustrates a selection of these samples.

5.1 Key space analysis

A fundamental requirement for any robust encryption method is its resistance to brute-force attacks. These attacks

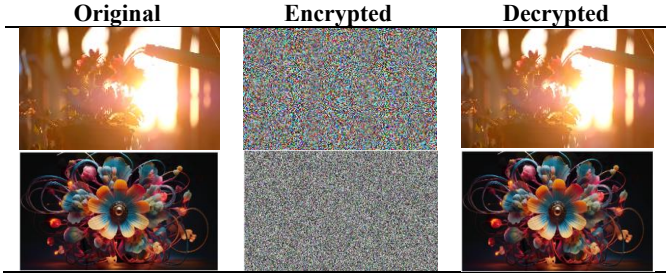
involve systematically attempting all possible keys within the key space. To ensure a high level of security, a key space of at least 2^{128} is recommended to prevent it from being broken within a reasonable timeframe.

In our proposed method, the encryption key is composed of 19 variables, including the initial conditions and parameters of the chaotic system. Given that the precision for each variable is 10^{-14}, the total size of the key space is estimated to be approximately 10^{266}, which is roughly equivalent to 2^{884}. This immense size far exceeds the recommended standard, making our method highly effective against brute-force attacks [18].

5.2 Histogram analysis

A histogram is an essential tool for video analysis, providing a description of the distribution of pixel values in each frame. To mitigate analytical attacks targeting histograms, the pixel distribution in the encrypted video must be completely uniform so that it does not reveal any patterns or statistical information about the original video. This uniformity ensures that no data about the relationship between the two videos is leaked [25]. As shown in Figure 2, the histogram of the encrypted video exhibits a quasi-uniform distribution.

Table 1. Sample frames

Original	Encrypted	Decrypted
		

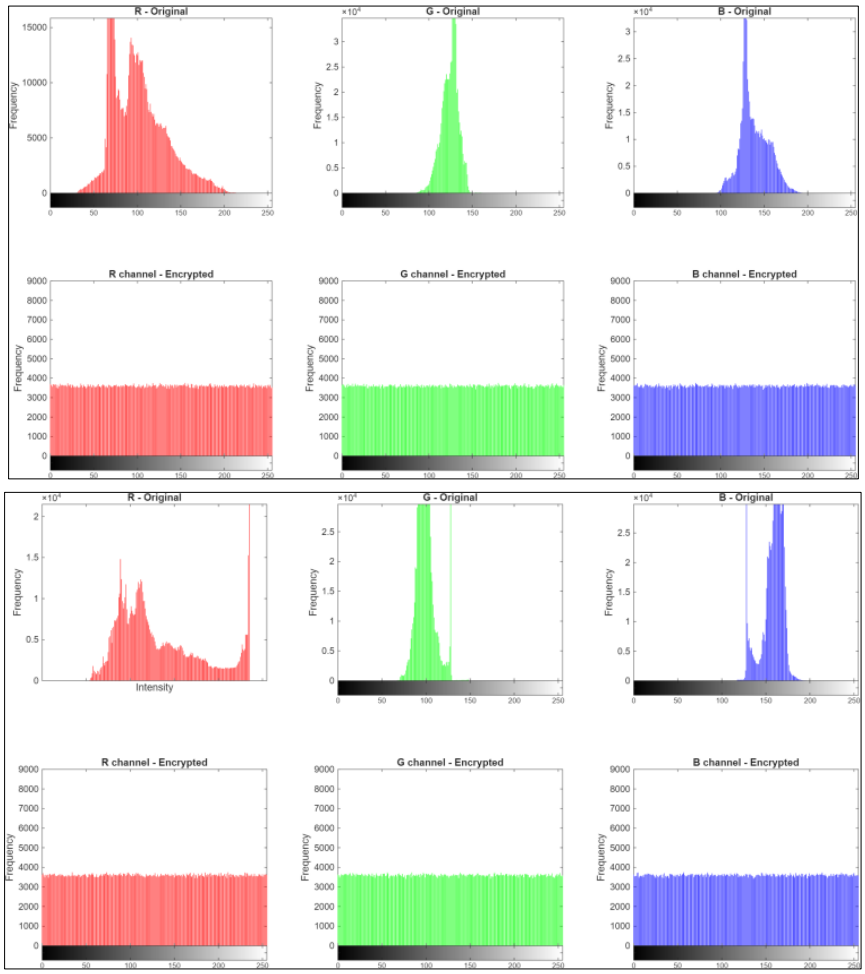


Figure 2. Histogram analysis

This result proves that the encrypted video is completely different from the original video in terms of visual and statistical distribution, as there is no statistical similarity between the two histograms.

5.3 Information entropy analysis

Information entropy is a fundamental mathematical property used to evaluate the unpredictability and randomness of an information source. To ensure an effective encryption system, the entropy of the encrypted video should ideally be 8. A value lower than 8 suggests that the source is not sufficiently random, introducing a degree of predictability that compromises its security [13].

$$H(m) = -\sum_{i=0}^{N-1} P(s_i) \log_2 \left[P(s_i) \right] \tag{2}$$

where, S is the information source, s_i represents intensity

levels (0-255) for each color channel, and $p(s_i)$ is the probability of occurrence of s_i.

The information entropy was calculated for several original videos and their corresponding encrypted versions. As shown in Table 2, the obtained entropy values are very close to the theoretical value of 8. This result demonstrates that no statistical information was leaked during the encryption process, confirming that the proposed method is secure against entropy analysis attacks.

Table 2. Entropy values

Video	Frame No	Original	Encrypted
	1	5.673807	7.999921
	60	5.748788	7.999916
	150	5.426651	7.999951
	90	5.668431	7.999893
	211	5.668431	7.999963
	302	5.652542	7.999928

5.4 Differential attacks

Differential attacks are a technique for cracking an encryption method by analyzing the differences between two encrypted versions of the same material. To measure the impact of a small change in a single pixel within the original video frame on the encrypted video, metrics such as the Number of Pixels Change Rate (NPCR) and the Unified Average Changing Intensity (UACI) are used. These metrics are calculated by encrypting the original video, then randomly changing the value of a single pixel in a given frame and re-encrypting it [26].

$$NPCR = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} D\,(i.j)}{M \times N} \times 100 \tag{3}$$

$$UACI = \frac{\sum_{i=1}^{M}\sum_{J=1}^{N} \frac{|C_1(i.j) - C_2(i.j)|}{255}}{M \times N} \times 100 \tag{4}$$

where, D(i,j) = 0 if C1(i,j) = C2(i,j), else D(i,j) = 1, and C1, C2 are two encrypted frames of size M × N. Table 3 presents the NPCR and UACI values evaluated across 5 frames from multiple test videos.

Table 3. Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI) values

Frame	NPCR (%)	UACI (%)
Frame 1	99.6852	33.4582
Frame 2	99.6978	33.4638
Frame 3	99.6546	33.4825
Frame 4	99.6904	33.4611
Frame 5	99.6983	33.4236
Mean	99.6853	33.4578
Std	0.0180	0.0214

The results confirm that both metrics remain consistently close to their ideal values, with a mean NPCR of 99.6853% (std = 0.0180%) and a mean UACI of 33.4578% (std = 0.0214%), demonstrating stable differential sensitivity independent of frame content or video type.

5.5 Correlation coefficient

A strong correlation between adjacent pixels is a key characteristic of unencrypted video. The correlation coefficient reflects the similarity between adjacent pixel values, whether horizontally, vertically, or diagonally. Therefore, any effective encryption system must significantly reduce this correlation, making the encrypted video appear as random data or "noise," to avoid any statistical attacks [14].

$$r_{xy} = \frac{cov(x,y)}{\sqrt{D(y)}\sqrt{D(x)}} \tag{5}$$

$$cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)) \tag{6}$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i\,, D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \tag{7}$$

where, x and y represent intensity values of two adjacent pixels (horizontal, vertical, or diagonal); N is the total number of pixel pairs sampled; cov(x,y) is the covariance; D(x) is the variance; and E(x) is the mean. The results in Table 4 show that the correlation coefficients in the original video are very high (approximately 1).

Table 4. Correlation coefficients

Frame	Direction	Original	Encrypted
Frame 1	Horizontal	0.9960903609	-0.0000070602
	Vertical	0.9926687693	-0.0000052627
	Diagonal	0.9906144258	0.0000114866
Frame 2	Horizontal	0.9908544405	0.0000222284
	Vertical	0.9848133695	-0.000383073
	Diagonal	0.9814575550	0.00000151785

However, these values decrease significantly after encryption, becoming close to zero. This decrease indicates that the encryption method has successfully removed statistical relationships between pixels, which enhances the resistance of the encrypted video to analytical attacks and makes it more difficult to exploit.

5.6 Mean Squared Error, Peak Signal to Noise Ratio, and Structural Similarity Index analysis

The Peak Signal to Noise Ratio (PSNR) is a commonly used metric for measuring the quality of video after decryption. In addition to this matter, Mean Squared Error (MSE) is also another useful metric for assessing the decoded video quality. MSE determines the average difference between the original video frames and the frames after processing, while PSNR indicates the quality of reconstruction. Seeing as the decrypted frames are identical to the original frames, the MSE becomes zero, so we can say that the PSNR becomes infinite. The pioneer measure of assessing the quality of video is the Structural Similarity Index (SSIM) [27]. This assessment process compares the structural features of video samples. The parameters, such as brightness, contrast, etc., are compared in this assessment between the original video and the decrypted video.

$$MSE = \frac{1}{M \times N} \sum_{i} \sum_{j} [I(i,j) - K(i,j)]^2 \quad (8)$$

$$PSNR = 20 \times log_{10} \left(\frac{255}{\sqrt{MSE}} \right) dB \quad (9)$$

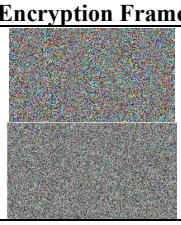
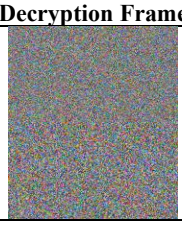
$$SSIM(X,Y) = \frac{(2\mu_x\mu_y + C_1)(2\delta_{xy} + C_2)}{(\mu_X^2\mu_Y^2 + C_1)(\delta_x^2\delta_y^2 + C_2)} \quad (10)$$

where, μ_x, μy are mean intensities, σx^2, σy^2 are variances, σ_{xy} is covariance, and C_1, C_2 are stability constants. According to our test results, the SSIM value is 1. It should be mentioned that obtaining a PSNR of ∞ and an SSIM of 1 for our symmetric encryption strategy are expected outcomes that are presented only to verify the precise and lossless nature of the decryption process, not as cryptographic security metrics. The proposed encryption system is capable of full decryption; the video is recovered without the loss of any information.

5.7 Sensitivity analysis

A robust encryption system must exhibit high sensitivity to any perturbation in the secret keys, whereby even infinitesimal modifications to the initial conditions of the chaotic system yield entirely different key sequences. To evaluate this key sensitivity, one of the initial condition parameters was altered, z(0), from 3.5 to 3.50000000000001, and the subsequently generated keys were employed in an attempt to decrypt the video frame. The decryption results using the altered key are presented in Table 5.

Table 5. Key sensitivity test

Original Frame	Encryption Frame	Decryption Frame
		

The decryption attempt using the slightly perturbed key failed completely, and the original frame could not be reconstructed. This result confirms that even minor deviations in the secret key lead to complete decryption failure, thereby demonstrating the method's strong resistance against brute-force and key-guessing attacks.

5.8 Security model and resistance analysis

Threat model: We consider an adversary with the following capabilities: (1) Known-plaintext attack: access to plaintext-ciphertext pairs. (2) Chosen-plaintext attack: ability to encrypt chosen frames. (3) Temporal analysis: exploiting inter-frame correlations. (4) Statistical analysis: histogram, entropy, and correlation attacks. (5) Brute-force attack: exhaustive key search.

Resistance analysis: (1) Brute-force: Key space of $10^{266} \approx 2^{884}$ makes exhaustive search computationally infeasible. (2) Known/Chosen-plaintext: Dynamic key updating between frames prevents pattern extraction. (3) Temporal attacks: plaintext-dependent key updating ensures unique chaotic keys per frame, completely eliminating inter-frame temporal correlation. (4) Statistical attacks: Quasi-uniform histogram distribution, entropy ≈ 8, and near-zero correlation coefficients demonstrate strong resistance to analytical attacks. (5) Differential attacks: NPCR = 99.69% and UACI = 33.46% confirm complete diffusion satisfying the avalanche criterion.

6. CONCLUSION

This research has presented a novel video encryption system based on a 7D chaotic system, DWT, and Rubik's Cube. Experimental results demonstrated the superiority of the proposed system across all metrics, where correlation coefficient values were close to zero. Regarding differential sensitivity, NPCR and UACI recorded values very close to the ideal values (99.61% and 33.46%, respectively). The average entropy was also very close to the ideal value (8). Regarding retrieval, the system achieved distinguished performance, where the MSE value was zero, and consequently, the PSNR value reached infinity, while SSIM attained a value of 1 after decryption. The average processing time was 0.031 seconds per frame (≈ 32 FPS) for 1280 × 720 resolution video, measured on MATLAB R2025a with an Intel Core i5 processor and 8 GB RAM, including I/O operations, confirming suitability for real-time video encryption applications. These results confirm a favorable trade-off between the added computational complexity of the multi-layer encryption approach and the security gains achieved, demonstrating that high security and real-time efficiency are simultaneously achievable. Future work will investigate resistance against deep learning-based attacks, hardware implementation, and extension to high-resolution formats.

REFERENCES

[1] Liu, H., Kadir, A., Niu, Y. (2014). Chaos-based color image block encryption scheme using S-box. AEU-International Journal of Electronics and Communications, 68(8): 676-686. https://doi.org/10.1016/j.aeue.2014.02.002

[2] Jasem, N.N., Mehdi, S.A. (2023). Multiple random keys for image encryption based on sensitivity of a new 6D chaotic system. International Journal of Intelligent Engineering and Systems, 16(5): 576-584. https://doi.org/10.22266/ijies2023.1031.49

[3] Huo, M., Zheng, Y., Huang, J. (2025). Enhancing AES image encryption with a three-dimensional hyperchaotic system for increased security and efficiency. PLOS One, 20(7): e0328297. https://doi.org/10.1371/journal.pone.0328297

[4] Wang, X., Teng, L. (2012). A novel colour image encryption algorithm based on chaos. Signal Processing, 92(4): 1101-1108. https://doi.org/10.1016/j.sigpro.2011.10.023

[5] Shakir, H.R., Mehdi, S.A., Hattab, A.A. (2022). A dynamic S-box generation based on a hybrid method of new chaotic system and DNA computing. TELKOMNIKA Telecommunication Computing Electronics and Control, 20(6): 1230-1238. https://doi.org/10.12928/TELKOMNIKA.v20i6.23449

[6] Luo, Y., Liu, Y., Liu, J., Tang, S., Harkin, J., Cao, Y. (2021). Counteracting dynamical degradation of a class of digital chaotic systems via unscented Kalman filter

and perturbation. Information Sciences, 556: 49-66. https://doi.org/10.1016/j.ins.2020.12.065

[7] Liu, L., Miao, S. (2016). A new image encryption algorithm based on logistic chaotic map with varying parameter. SpringerPlus, 5(1): 289. https://doi.org/10.1186/s40064-016-1959-1

[8] Mallat, S.G. (1989). A theory for multiresolution signal decomposition: The wavelet representation. IEEE Transactions on Pattern Analysis and Machine Intelligence, 11(7): 674-693. https://doi.org/10.1109/34.192463

[9] Hua, Z., Jin, F., Xu, B., Huang, H. (2018). 2D logistic-sine-coupling map for image encryption. Signal Processing, 149: 148-161. https://doi.org/10.1016/j.sigpro.2018.03.010

[10] Ahmad, J., Khan, M.A., Hwang, S.O., Khan, J.S. (2017). A compression sensing and noise-tolerant image encryption scheme based on chaotic maps and orthogonal matrices. Neural Computing and Applications, 28(Suppl 1): 953-967. https://doi.org/10.1007/s00521-016-2405-6

[11] Khudair, E.T., Naser, E.F., Mazher, A.N. (2022). Comparison between RSA and CAST-128 with adaptive key for video frames encryption with highest average entropy. Baghdad Science Journal, 19(6): 11. https://doi.org/10.21123/bsj.2022.6398

[12] Jiang, D., Chen, T., Yuan, Z., Li, W., Wang, H., Lu, L. (2024). Real-time chaotic video encryption based on multi-threaded parallel confusion and diffusion. Information Sciences, 666: 120420. https://doi.org/10.1016/j.ins.2024.120420

[13] Hilal, A.H., Al-Azawi, M.K. (2025). Selective chaotic video encryption for versatile video compression H.266/VVC standard. Journal Européen des Systèmes Automatisés, 58(9): 1899-1909. https://doi.org/10.18280/jesa.580912

[14] Rajaonarison, T.R., Randriamitantsoa, P.A. (2022). Performances study of a new chaos-based video encryption algorithm. International Journal of Computer Trends and Technology, 70(6): 30-43. https://doi.org/10.14445/22312803/IJCTT-V70I6P104

[15] El Kinani, K., Bendaoud, S., Amounas, F. (2023). A novel compression-encryption scheme based on DWT and ECC for securing the transmission of multimedia data in IoT environment. International Research Journal of Advanced Engineering and Science, 8(1): 216-221. https://irjaes.com/wp-content/uploads/2023/02/IRJAES-V8N1P218Y23.pdf.

[16] Tu, L., Liu, Z., Wang, Y., Yang, G. (2024). A new digital video encryption algorithm based on composite chaotic mapping. In International Conference on Optical Communication and Optoelectronic Technology (OCOT 2024), Hangzhou, China, pp. 26-32. https://doi.org/10.1117/12.3045748

[17] Murari, T.V., KC, R., ME, R. (2024). Selective encryption of video frames using the one-time random key algorithm and permutation techniques for secure transmission over the content delivery network. Multimedia Tools and Applications, 83(35): 82303-82342. https://doi.org/10.1007/s11042-024-18613-1

[18] Zghair, H.K., Mehdi, S.A., Sadkhan, S.B. (2021). Speech scrambler based on discrete cosine transform and novel seven-dimension hyper chaotic system. Journal of Physics: Conference Series, 1804(1): 012048. https://doi.org/10.1088/1742-6596/1804/1/012048

[19] Zghair, H.K., Mehdi, S.A., Sadkhan, S.B. (2020). Design and analytic of a novel seven-dimension hyper chaotic systems. In 2020 1st Information Technology to Enhance e-learning and Other Application (IT-ELA), Baghdad, Iraq, pp. 77-81. https://doi.org/10.1109/IICETA50496.2020.9318940

[20] Daubechies, I. (1992). Ten Lectures on Wavelets. https://epubs.siam.org/terms-privacy.

[21] Vetterli, M., Kovačević, J. (1995). Wavelets and Subband Coding. Prentice-Hall. http://waveletsandsubbandcoding.org/Repository/VetterliKovacevic95_Manuscript.pdf.

[22] Wang, W., Tan, H., Pang, Y., Li, Z., Ran, P., Wu, J. (2016). A novel encryption algorithm based on DWT and multichaos mapping. Journal of Sensors, 2016(1): 2646205. https://doi.org/10.1155/2016/2646205

[23] Kunkle, D., Cooperman, G. (2007). Twenty-six moves suffice for Rubik's cube. In Proceedings of the 2007 International Symposium on Symbolic and Algebraic Computation, Waterloo, Ontario, Canada, pp. 235-242. https://doi.org/10.1145/1277548.1277581

[24] Zhang, L., Tian, X., Xia, S. (2011). A scrambling algorithm of image encryption based on Rubik's cube rotation and logistic sequence. In 2011 International Conference on Multimedia and Signal Processing, Guilin, China, pp. 312-315. https://doi.org/10.1109/CMSP.2011.69

[25] Rehman, M.U., Shafique, A., Khan, M.S., Driss, M., et al. (2024). A novel medical image data protection scheme for smart healthcare system. CAAI Transactions on Intelligence Technology, 9(4): 821-836. https://doi.org/10.1049/cit2.12292

[26] Wu, Y., Noonan, J.P., Agaian, S. (2011). NPCR and UACI randomness tests for image encryption. Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications, 1(2): 31-38. http://www.cyberjournals.com/Papers/Apr2011/05.pdf.

[27] Horé, A., Ziou, D. (2010). Image quality metrics: PSNR vs. SSIM. In 20th International Conference on Pattern Recognition (ICPR), Istanbul, Turkey, pp. 2366-2369. https://doi.org/10.1109/ICPR.2010.579