6D Hyperchaotic Encryption Model for Ensuring Security to 3D Printed Models and Medical Images

Siju John [1,2] and S. N. Kumar [3,*]

[1] Marian Research Center, Marian College Kuttikanam (Autonomous), Lincoln University College, Wisma Lincoln, Malaysia
[2] Department of Computer Science and Engineering, Amal Jyothi College of Engineering, Kanjirappally, India
[3] Department of Electrical and Electronics Engineering, Amal Jyothi College of Engineering, APJ Abdul Kalam Technological University, Kerala, India
Email: sjohn@lincoln.edu.my (S.J.); appu123kumar@gmail.com (S.N.K.)
*Corresponding author

***Abstract*—In the 6G era, where ultra-fast and reliable communication is expected to be ubiquitous, encryption shall continue to play a crucial role in ensuring the security and privacy of data. Encryption and decryption of medical images and 3D printed models using 6D hyperchaotic function is proposed in this research work for ensuring security in data transfer. Here we envisage using a six-dimensional hyperchaotic system for encryption purposes which shall offer a high level of security due to its complex and unpredictable dynamics with multiple positive Lyapunov exponents. This system can potentially enhance the encryption process for 3D objects and medical images, ensuring the protection of sensitive data and preventing unauthorized access. A hyperchaotic system is a type of dynamical system characterized by exhibiting more than one positive Lyapunov exponent, which indicates strong sensitivity to initial conditions. These systems have more degrees of freedom and complex and intricate dynamics compared to standard chaotic systems. The security of the encryption scheme depends on the complexity of the hyperchaotic system and the randomness of the secret key. The parameters of a 6D hyperchaotic system shall be used as an encryption key with six dimensions, each with its range of values, and shall provide many possible keys. In this work, we implemented a 6D hyperchaotic system for the encryption of the 3D printed model and medical images. The performance evaluation was done by metrics entropy, correlation, Number of Pixels Change Rate (NPCR), and Unified Averaged Changed Intensity (UACI) which revealed the robustness of the encryption model in ensuring security. Hyperchaotic systems can be efficiently implemented in parallel computing architectures, which allow faster encryption and decryption processes.**

***Keywords*—image encryption, hyperchaotic system, 3D printing, medical image processing**

I. Introduction

Encrypting 3D-printed model images involves protecting the model's digital design from unauthorized access or modification. It is necessary to protect the intellectual property and confidential information contained within the designs. With the increasing popularity and accessibility of 3D printing technology, it has become easier for anyone to create and reproduce 3D models. Encryption also adds an extra layer of security to digital files, making it more difficult for hackers or malicious actors to access and modify the design files. This is especially important for sensitive designs, such as those used in the defense, medical, or aerospace industries. Image encryption using hyperchaotic systems is a popular technique for protecting the confidentiality and integrity of digital images. Steganography is the practice of hiding a secret message or information within another image, message, or video in a way that the existence of the hidden information is not obvious. In the healthcare sector, steganography is used for various purposes. Steganography is used to protect patient data and maintain confidentiality in the healthcare sector, particularly in telemedicine applications [1]. Patient data can be embedded within medical images or videos, which can then be securely transmitted without the fear of being intercepted by unauthorized users. Also, Medical images can be authenticated using steganography techniques. Digital watermarking techniques can be used to embed a unique signature within the image, which is used to verify the authenticity of the image. Steganography is used to embed hidden information within medical images or videos, which can aid in diagnosis and treatment [2].

Hyperchaotic systems are characterized by complex and unpredictable dynamics. This makes them potentially more secure than classical encryption methods, which rely on mathematical algorithms that may have known

Manuscript received September 4, 2023; revised November 6, 2023; accepted November 23, 2023; published April 10, 2024.

vulnerabilities. Classical encryption algorithms can be susceptible to statistical attacks, where an attacker analyzes patterns in the ciphertext to gain information about the plaintext. The proposed method is shown to be robust to common attacks and improves the quality of decrypted models compared to existing methods. The proposed method is shown to be robust to common attacks and improves the quality of decrypted models compared to existing methods.

II. Related Works

There have been several papers in the literature that deal with steganography techniques for 3D models in the health sector. Early detection of diseases affecting humans is critical for preserving human health, and medical imaging has an inevitable role in the diagnostic and treatment process. However, ensuring the privacy and security of medical images is just as important to patients as the diagnosis and treatment itself, as it prevents tampering or attacks on the images. In previous study, an approach was proposed that combines chaotic Henon maps and advanced encryption methods with an S-box to create a hybrid encryption system that is both highly secure and efficient for processing voluminous multidimensional 3D images [3]. The researchers were able to increase the security of medical images against a variety of attacks—including algebraic attacks—while retaining quick encryption/decryption speeds and manageable processing overheads by utilizing this hybrid approach. A method for encrypting 3D models in the metaverse using a 2D chaotic system, which generates an unpredictable keystream suitable for cryptography [4]. The proposed algorithm applies XOR and Semi-Tensor Product (STP) processing to the fractional and integer parts of the 3D model, respectively, to obtain a ciphertext model. 2D-LAIC produces the keystream needed for processing. The study demonstrates that 2D-LAIC offers superior security and efficiency for 3D model encryption and exhibits better dynamical behavior than conventional chaotic systems.

The issue of protecting 3D printing models was addressed from unauthorized access and theft by proposing a random encryption algorithm. The algorithm involves distorting each facet of the 3D model using a geometric transformation and randomly each vertex of each facet using a secret key [5]. Then, to create the encrypted 3D printing model, a 3×3 matrix is created using the distorted vertices, and the matrix parameters are encrypted using the random integers of another matrix. The experimental results demonstrated that the algorithm is highly effective, providing better security than previously reported methods. The algorithm completely modifies the 3D triangular mesh, ensuring that the encrypted model is protected from illegal copying. An encryption system for 3D mesh graphical models was proposed using the 3D Arnold cat map, another chaos-based encryption system [6]. The encryption is performed separately on vertices and faces using shuffling and substitution, and the results are combined to form the encrypted model. The model provides confusion and diffusion, making the system more secure. Simulation findings demonstrated that the suggested method was effective and resistant to a variety of attacks. The system has potential applications in the encryption of 3D multimedia content in the emerging Virtual Reality era.

As multimedia applications continue to develop, the security of 3D models has become a pressing concern. Due to their complex spatial structures, previous attempts at encrypting 3D models directly have been tedious and time-consuming. To address this issue, an encryption method based on chaos theory is suggested in previous study [7]. A study was proposed for encrypting 3D polygon mesh models using a 3D Lorenz Chaotic map to modify the vertices values of the model [8]. The proposed scheme was tested on various 3D models and achieved good encryption results, as demonstrated by the Hausdorff Distance and histogram metrics. The results show that the original and extracted models are nearly identical, indicating that the proposed scheme provides strong encryption.

To prevent unauthorized copying and access during storage and transmission, Pham *et al.* [9] presented an encryption technique for 3D printing models using the frequency domain of Discrete Cosine Transform (DCT). The facet data is extracted to create a 3×3 matrix, which is then transformed to the frequency domain of DCT. The approach creates an encrypted 3D printing model by encrypting the discrete cosine transform's DC coefficients for the facet's matrixes in the frequency domain. Experimental findings demonstrated that this strategy is quite successful for 3D printed models and provides better security than previous methods. The encryption process completely altered the entire 3D printing model. As 3D printing becomes more prevalent in various industries, it is increasingly vulnerable to unauthorized copying and distribution. To prevent this, 3D printing models should be encrypted during transmission and storage. A perceptual encryption algorithm was introduced [10]. Three control points, an interpolating vector, and curvature coefficients, are used by the algorithm to produce a degree 2 spline curve from a facet of the 3D printed model. These parameters are then encrypted using a secret key. Inverse interpolation and geometric distortion are employed to derive the encrypted 3D printing model using the encrypted characteristics of the spline curve.

An encryption technique using 3D Lu chaotic mapping for 3D textured models was proposed to ensure the security and privacy of 3D content in the emerging AR/VR era [11]. The technique uses 3D Lu chaotic mapping for separately encrypting the vertices, textures of 3D models, and polygons before combining them to create the final encrypted model, algorithm proposed was found to resist attacks. The issue of unauthorized distribution and theft of 3D printing models was discussed, and the authors proposed a selective encryption algorithm to address this problem [12]. The algorithm involved clustering and the use of discrete cosine transform to encrypt specific coefficients in the frequency domain of the 3D printing model. The proposed algorithm was effective in altering the entire 3D printing model and provided better security compared to previous methods. Results demonstrated that

the algorithm has zero decrypting error and is highly effective in encrypting 3D printing models.

A new encryption method called three-dimensional Steerable Cosine Number Transform (3D-SCNT) was introduced, is obtained by rotating the basis vectors of the 3D-CNT using a finite field rotation operator [13]. The 3D-SCNT is applied in a proposed medical image encryption scheme, where the rotation angles are used as secret parameters. The scheme is tested against cryptographic attacks using computer experiments, and it is found to be resilient against them. A method was proposed that used an optimized asymmetric encryption method to protect 3D mesh models, which are commonly used in design, computer graphics, engineering, and entertainment [14]. The method addresses the challenge of preserving the privacy of these models, which are generated in large quantities due to the availability of acquisition equipment and sensors.

Shah *et al.* [15] proposed a framework for reversible data hiding using the homomorphic Paillier cryptosystem in encrypted 3D mesh models. Cloud data management and End-to-end authentication are provided by the framework using two homomorphic characteristics of the cryptosystem. The proposed framework was implemented on different 3D mesh models, producing high-quality decrypted meshes with high embedding rates and error-free extraction of information bits. Choi *et al.* [16] suggest a color image encryption algorithm for medical images that uses a pseudorandom number generator called Nonlinear Cellular Automaton (NCA) and a generalized 3D chaotic cat map.

A chaotic image encryption scheme which is a single round for secure transmission of medical images in telemedicine was proposed by Kumar *et al.* [17]. The proposed scheme uses a Combined Chaotic Key Generator (CCKG) to produce initial seeds for the permutation and diffusion processes. First, Zigzag Transform (ZT) scanning is used to permute the plain image block by block under the impact of the Lorenz System (LS) and Fractional Order Chaotic System (FOCS). The entire permuted image is then split into even and odd portions, and these portions are diffused individually by random pixel matrices produced by FOCS and LS. The dispersed odd and even bits are combined to create the cipher image. The proposed scheme is tested and found to be effective, robust, and competent for secure medical image transmission.

Kok *et al.* [18] investigated the potential of using secure remote 3D printing in telemedicine to produce personalized medications based on electronic prescriptions. The use of 3D printing in telemedicine faces challenges such as cyber risks associated with transferring CAD files to the printer and ensuring the reproducibility of the final product. To address these challenges, the study uses DEFEND 3D technology for enhanced cybersecurity and intellectual property protection. The study confirms the feasibility of remote 3D printing of solid dosage forms using model polymers with good reproducibility and quality, indicating the potential for advancements in telemedicine and digital pharmacies. Further research is necessary to investigate the use of pharmaceutically relevant polymers in 3D printing.

An overview of the current state of 3D digital watermarking was provided and its potential for protecting the Intellectual Property Rights (IPR) of printed 3D models against attacks such as 3D printing and scanning [19]. A robust reversible watermarking method for 3D models was proposed based on homomorphic encryption, which can protect the privacy and copyright of 3D models transmitted over the internet [20].

In 6G, Internet of Things (IoT), and Edge Computing, encryption remains a critical component for securing data and communications [21]. With the advent of quantum computing, there's a growing need for encryption algorithms that can resist attacks from quantum computers. 6G is expected to incorporate post-quantum cryptographic techniques to ensure long-term security. Many IoT devices have limited processing power and memory, which requires lightweight encryption protocols like ECC (Elliptic Curve Cryptography) or symmetric key encryption optimized for IoT environments [22]. Edge computing brings computation closer to data sources [23]. This proximity allows for tighter control and encryption of data since it stays within a defined geographic area, reducing exposure to external threats.

Security plays a vital role in the health care and defense sector in data storage and transfer. This research work proposes a 6D hyperchaotic model for the encryption and decryption of medical data and 3D printed model images, thereby ensuring security. Section II focuses on the hyperchaotic function, and its properties followed by the 6D hyperchaotic function-based image encryption, Section III highlights the results of the encryption model for 3D printed model real-time 2D images and 2D medical images, validated by performance metrics, and finally, the conclusion is drawn in Section IV.

III. Detailed Methodology

A. Hyperchaotic Function and Its Features

Chaotic and hyperchaotic systems are mathematical models that exhibit highly complex and unpredictable behavior. These systems are characterized by their sensitivity to initial conditions, meaning that even tiny changes in the starting conditions can lead to dramatically different outcomes over time. The main difference between chaotic and hyperchaotic systems lies in the number of variables involved and the level of complexity. Hyperchaotic systems are a subset of chaotic systems that involve four or more variables. Compared to chaotic systems, hyperchaotic systems exhibit an even higher level of complexity and unpredictability. They are characterized by multiple positive Lyapunov exponents, which indicate the rate of exponential phase space divergence of neighboring trajectories.

The mathematical modeling of hyperchaotic systems is an important area of research in nonlinear dynamics and chaos theory. Hyperchaotic systems are characterized by multiple chaotic attractors, and their behavior is highly complex and difficult to predict. Using a set of differential equations, the behavior of hyperchaotic systems can be

represented. These equations typically involve a set of state variables that represent the system's internal state and a set of parameters that determine the system's dynamics. The equations are usually nonlinear and may involve higher-order terms, making it difficult to solve them analytically. As a result, numerical methods are often used to simulate the system's behavior and to analyze its properties. One popular numerical method for studying hyperchaotic systems is the Runge-Kutta method, which is a family of algorithms for solving ordinary differential equations. The Lyapunov exponent is a different strategy that assesses the rate of phase space divergence of nearby trajectories and gauges the system's sensitivity to beginning conditions. Many hyperchaotic systems have been studied extensively in the literature, which include the Lorenz-like hyperchaotic system, the Rössler hyperchaotic system, the Chen hyperchaotic system, and the Liu hyperchaotic system. Each of these systems exhibits unique properties and has applications in various fields, including cryptography, signal processing, and chaos-based communication systems. The flow diagram of the proposed methodology is depicted in Fig. 1.

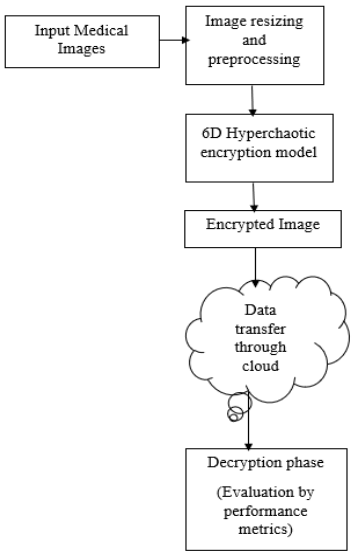

Fig. 1. Flow diagram of the proposed methodology.

Some examples of hyperchaotic systems and their corresponding mathematical formulas are given below.

Lorenz hyperchaotic system [21]: By adding more nonlinear components to the initial system, the Lorenz hyperchaotic system expands the original system and creates higher-dimensional chaotic dynamics. Compared to the original Lorenz system, it is distinguished by having more variables and equations.

$$\frac{dp}{dt} = a \times (q - p) + b \times r + c \times s \quad (1)$$

$$\frac{dq}{dt} = -p + q + d \times r + c \times s \quad (2)$$

$$\frac{dr}{dt} = p + q + s \quad (3)$$

$$\frac{ds}{dt} = -b \times p - d \times q + r + c \times s \quad (4)$$

Rossler hyperchaotic system [22]: The Rossler hyperchaotic system is an extension of the Rossler system which displays intricate attractors with numerous unstable equilibrium points and delicate beginning condition dependence. The attractors produced by this system have complicated structures and can show high-dimensional chaotic patterns.

$$\frac{dp}{dt} = -q - r \quad (5)$$

$$\frac{dq}{dt} = p + aq \quad (6)$$

$$\frac{dr}{dt} = b + r(p - c) \quad (7)$$

Chen hyperchaotic system [23]: The Chen hyperchaotic system is a higher-dimensional extension of the Chen system which introduced additional nonlinear terms and variables, resulting in higher-dimensional chaotic dynamics compared to the original Chen system. With several unstable equilibrium points and complicated attractors, the Chen hyperchaotic system displays chaotic and hyperchaotic patterns. The attractors produced by this system can have complicated, multi-dimensional shapes.

$$\frac{dp}{dt} = a(q - p) + d \times r \times s \quad (8)$$

$$\frac{dq}{dt} = c \times p - q \times r \quad (9)$$

$$\frac{dr}{dt} = x \times q - b \times r \quad (10)$$

$$\frac{ds}{dt} = e \times p - f \times s \quad (11)$$

Lu hyperchaotic system [24]: A transition from one system to another is accomplished via the Lu system, which connects the Lorenz and Chen systems. It is also among the unified chaotic system's simplest chaotic attractors.

$$\frac{dp}{dt} = a \times (q - p) + b \times q \times r \quad (12)$$

$$\frac{dq}{dt} = c \times p + q - p \times r \quad (13)$$

$$\frac{dr}{dt} = d \times p \times q - e \times r \quad (14)$$

$$\frac{ds}{dt} = f \times p - g \times t \quad (15)$$

In these formulas, *p*, *q*, *r*, and *s* represent the state variables of the hyperchaotic system, and a, b, and c are parameters that determine the system's dynamics. The exact values of these parameters can greatly influence the dynamics and complexity of the hyperchaotic system. These equations are typically nonlinear and involve higher-order terms, making it difficult to solve them analytically. Numerical methods, such as the Runge-Kutta method, are often used to simulate the system's behavior and to analyze its properties. In a nutshell, the mathematical formulas for hyperchaotic systems are complex and exhibit a rich variety of dynamics, which makes them useful for a wide range of applications in various fields.

In a hyperchaotic system, the Lyapunov exponent plays a crucial role in characterizing the system's sensitivity to

initial conditions. The Lyapunov exponents quantify the exponential rate of convergence or divergence of nearby trajectories in the system's phase space. In a hyperchaotic system, there are multiple positive Lyapunov exponents, indicating that the system exhibits more complex and intricate dynamics compared to standard chaotic systems. Each positive Lyapunov exponent corresponds to a specific direction in the phase space along which nearby trajectories diverge exponentially. The largest positive Lyapunov exponent is particularly important as it determines the overall rate of divergence of nearby trajectories and indicates the system's level of chaotic behavior. If this exponent is positive, it implies that the system is chaotic and exhibits sensitive dependence on initial conditions. However, in a hyperchaotic system, there are additional positive Lyapunov exponents that describe the divergence along other directions in phase space. The presence of multiple positive Lyapunov exponents in a hyperchaotic system suggests that it has more degrees of freedom and a higher-dimensional phase space. Consequently, the system's behavior becomes even more complex and unpredictable. The Lyapunov exponents are calculated using numerical methods, such as the Wolf algorithm or the Rosenstein algorithm, which involve tracking the evolution of nearby trajectories in the phase space and computing the logarithmic rate of their separation. The resulting set of Lyapunov exponents provided valuable insights into the dynamics and chaotic properties of the hyperchaotic system.

B. 6D Hyperchaotic Function-Based Encryption Model

In our proposed system, we implemented a 6D hyperchaotic system using the 2D image of 3D printed models obtained from our IDEA lab research laboratory [25]. A 6D hyperchaotic system refers to a dynamical system with six dimensions that exhibits hyperchaotic behavior. Hyperchaos is a phenomenon in which a system demonstrates both chaotic behavior and a high number of positive Lyapunov exponents, indicating complex and unpredictable dynamics [26–28]. The system has six state variables, represented by the vector $x = [x1, x2, x3, x4, x5, x6]$, and one-time variable t. The parameters a, b, c, d, e, and r, are constants that affect the behavior of the system. To simulate the behavior of this hyperchaotic system, we need to provide initial conditions for the state variables x and specific values for the parameters. Here the values of the parameters are set to $a = 20$, $b = 8/3$, $c = 28$, $d = -1$, $e = 8$, $r = 3$, and two positive Lyapunov coefficients are used. We then used numerical integration methods, i.e., the fourth-order Runge-Kutta method, to solve these equations and to obtain the evolution of the system over time.

$$x(1) = a \times \big(x(2) - (x1)\big) + x4 - x5 - x(6) \quad (16)$$

$$x(2) = c \times x(1) - x(2) - x(1) \times x(3) \quad (17)$$

$$x(3) = -b \times x(3) + x(1) \times x(2) \quad (18)$$

$$x(4) = d \times x(4) - x(2) \times x(3) \quad (19)$$

$$x(5) = e \times x(6) + x(3) \times x(2) \quad (20)$$

$$x(6) = r \times x(1) \quad (21)$$

The different steps in the implementation of image encryption algorithm using the 6D hyperchaotic algorithm is given below and is depicted in Fig. 2.

(1) Get the size of the input image I and store the dimensions in variables M and N;
(2) Convert the input image I into a column vector P of doubles;
(3) Generate chaotic initial conditions x using a logistic map;
(4) Define the system of differential equations L that represents a hyperchaotic system;
(5) Set the time interval [N0, MN3] for solving the differential equations using the ode45 solver. Solve the system of differential equations and obtain the solution trajectory in the form of a matrix Y;
(6) Extract a portion of the solution trajectory Y and reshape it to obtain the vector L. Sort the elements of L and store the sorting indices in S.
(7) Rearrange the pixel values of the input image I according to the sorting indices S and store the rearranged image in R. Reshape R back to the original image dimensions.
(8) Perform a matrix multiplication of 2×2 blocks in image R with a fixed matrix A to obtain the encrypted image C.
(9) Take the modulus of the elements of C with 256 to ensure the pixel values are within the valid range.
(10) Repeat the above steps for a specified number of rounds, encrypting the image iteratively.
(11) Store the final encrypted image I as I_enc, which is of type unit 8.

The above algorithm applies a hyperchaotic system to encrypt an input image by sorting and rearranging its pixel values. The image is then divided into 2×2 blocks, and each block is multiplied by a fixed matrix. The resulting encrypted image is obtained after multiple rounds of encryption. The steps in the decryption phase are the reverse of the encryption phase.

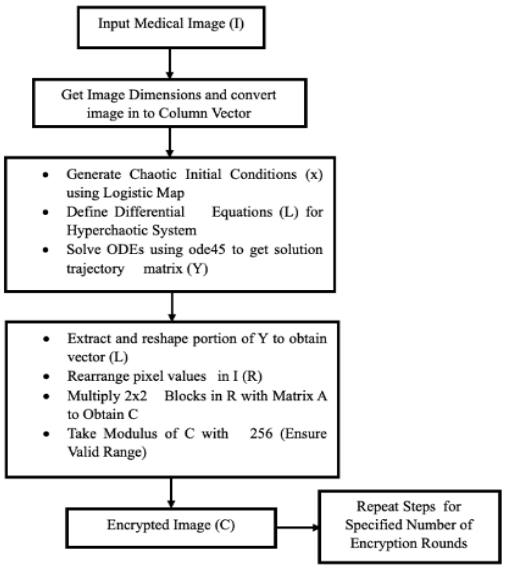

Fig. 2. Flow diagram of the steps of the proposed encryption model.

IV. Simulation Results and Discussion

We implemented our method in MATLAB 2020a and analyzed the different parameters discussed below using 2D slices of 3D printed models generated from our IDEA lab research laboratory. The medical images utilized in this research work are obtained from Mar Sleeva Medicity Hospital, Kerala, prior permission was obtained for using the images. Fig. 3 shows the 3D-printed model of a piston head. Fig. 3(a) shows the original object, Fig. 3(b) shows the encrypted object and Fig. 3(c) shows the decrypted object.

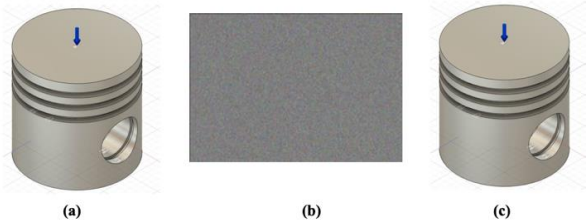

Fig. 3. Encryption and decryption of 3D object-D1 (Piston head) (a) original object (b) encrypted object (c) decrypted object.

Fig. 4 shows the histogram of the original object (piston head) while Fig. 5 shows the histogram of the object after encryption. Comparing the histograms of the objects before and after encryption provides insights into the effects of encryption. It is observed that Encryption introduced a shift in pixel intensities, resulting in a histogram that is shifted towards higher intensity. The encryption process also broadens the histogram, expanding the range of pixel intensities. Also, fine details and subtle variations in the original image may be lost or smoothed in the encrypted image, leading to a flatter histogram. Additionally, certain encryption techniques aim to spread pixel intensities uniformly, resulting in a more uniform histogram in the encrypted image.

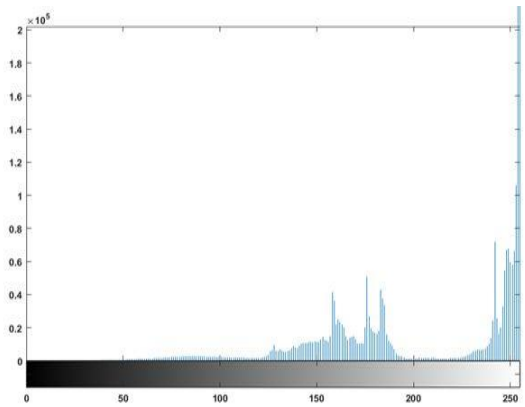

Fig. 4. Histogram of the original 3D object-D1 (Piston head).

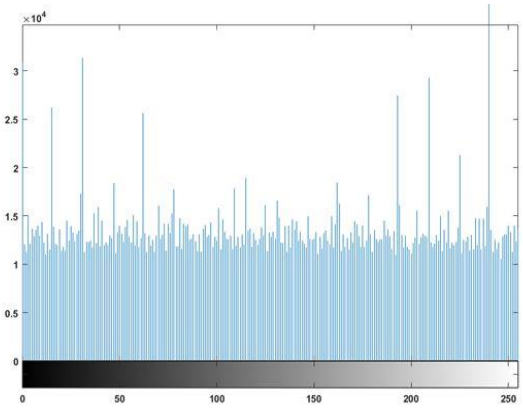

Fig. 5. Histogram of the encrypted 3D object-D1 (Piston head).

The correlation coefficient is another parameter used for measuring the similarity or relationship between two images. It is often applied to compare the corresponding pixel values of two images and assess how they vary together. Figs. 6 and 7 show the horizontal, vertical, and diagonal correlation coefficients of the same 3D object-D1, before and after encryption.

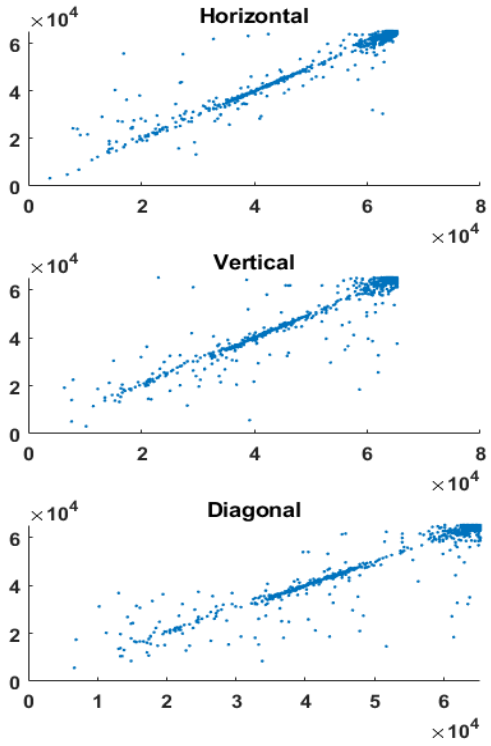

Fig. 6. Correlation coefficient plot of the original 3D object-D1 prior to encryption.

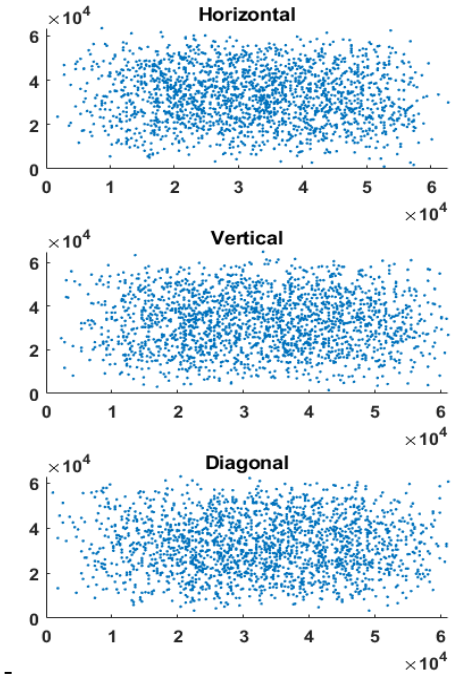

Fig. 7. Correlation coefficient plot of the original 3D object-D1 after encryption.

The proposed encryption model was tested on 2D slices of 3D object models and 2D medical images (Figs. 8 and 9). Tables I and II show the horizontal and vertical correlation coefficients of the various input images. Tables III and IV show the horizontal and vertical correlation coefficients of the various images after encryption. The horizontal and vertical correlation values of the input and encrypted images reveal the proficiency of the encryption model. The correlation of the input images is high, while the correlation value of the encrypted images is low.

TABLE I. CORRELATION COEFFICIENTS OF INPUT 3D OBJECT IMAGES

Position	3D Object-D1 (Input)	3D Object-D2 (Input)	3D Object-D3 (Input)	3D Object-D4 (Input)
Horizontal	0.9764	0.9270	0.9921	0.9769
Vertical	0.8033	0.7822	0.7717	0.7718

TABLE II. CORRELATION COEFFICIENTS OF INPUT MEDICAL IMAGES

Position	Medical Image-M1 (Input)	Medical Image-M2 (Input)	Medical Image-M3 (Input)	Medical Image-M4 (Input)
Horizontal	0.9993	0.9763	0.9759	0.9962
Vertical	0.9984	0.9670	0.9800	0.9984

TABLE III. CORRELATION COEFFICIENTS OF ENCRYPTED 3D OBJECT IMAGES

Position	3D Object-D1 (Encrypted)	3D Object-D2 (Encrypted)	3D Object-D3 (Encrypted)	3D Object-D4 (Encrypted)
Horizontal	−0.0190	−0.0141	−0.0154	−0.0150
Vertical	0.0356	−0.0401	0.0421	−0.0315

TABLE IV. CORRELATION COEFFICIENTS OF ENCRYPTED MEDICAL IMAGES

Position	Medical Image-M1 (Encrypted)	Medical Image-M2 (Encrypted)	Medical Image-M3 (Encrypted)	Medical Image-M4 (Encrypted)
Horizontal	−0.0007	−0.0008	−0.0041	−0.0177
Vertical	0.0006	0.0046	0.0048	0.0003

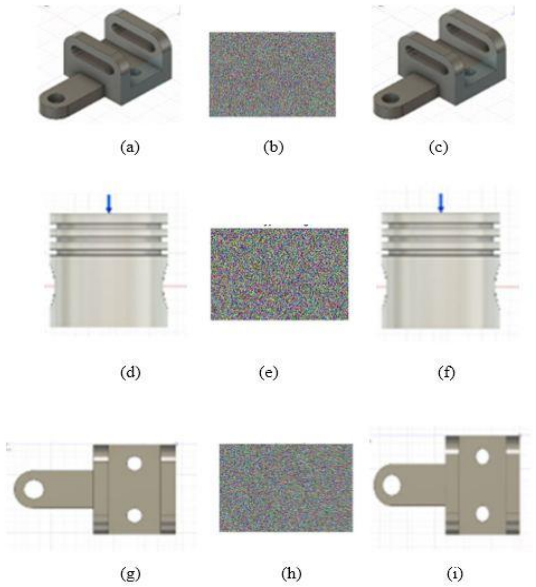

Fig. 8. (a), (d) and (g) represent the input images, (b), (e) and (h) represent the encrypted output and (c), (f) and (i) represent the decrypted outputs corresponding to 3D objects D2, D3 and D4.

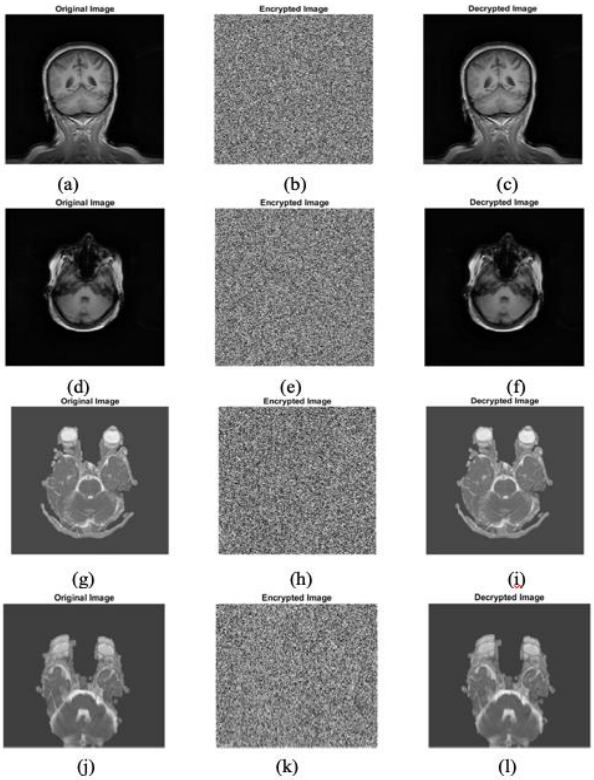

Fig. 9. (a), (d), (g) and (j) represent the input images, (b), (e), (h) and (k) represents the encrypted output, and (c), (f), (i) and (l) represent the decrypted outputs corresponding to medical images.

The entropy of an image refers to the amount of information or uncertainty contained in the image. It is a measure of the average amount of information needed to encode each pixel in the image. Mathematically, the entropy of an image is calculated using the probability distribution of pixel intensities. Let's assume we have a grayscale image with pixel intensities ranging from 0 to 255. The entropy H is given by Eq. (22):

$$H = -\sum p(i) \times log_2((p(i)) \quad (22)$$

where $p(i)$ is the probability of a pixel having intensity i, and the summation is performed over all possible intensities.

The entropy value is measured in bits per pixel (bpp). The entropy of an encrypted image and a normal (unencrypted) image differ significantly. In a normal image, entropy represents the amount of information or randomness in the pixel intensities. A high-entropy image typically contains a wide range of intensities and exhibits complex patterns, while a low-entropy image tends to be more uniform or predictable. On the other hand, an encrypted image is designed to appear randomly and contain no discernible patterns or structure. The encryption process introduces randomness and obscures any meaningful information. As a result, the entropy of an encrypted image is generally expected to be high, closer to the maximum possible entropy. However, it's important to note that encryption does not directly affect the entropy calculation. Entropy is computed based on the pixel intensities themselves and their probability distribution. So, if the encryption algorithm preserves the statistical properties of the image, the entropy may remain like the original image. Ultimately, the specific encryption algorithm used, and the quality of encryption implementation can impact the entropy of the encrypted image. Some encryption methods may introduce additional steps that intentionally increase entropy to enhance security. Table V shows the entropy values of the original 3D object, entropy after encryption, and after decryption. The entropy of the encrypted image is closer to 8, indicating the efficiency of the encryption model.

TABLE V. ENTROPY VALUES OF THE ORIGINAL IMAGES, AFTER ENCRYPTION AND AFTER DECRYPTION

Image Details	Entropy of input 3D model	Entropy of encrypted 3D model	Entropy of decrypted 3D model
3D Object-D1	5.050	7.967	5.050
3D Object-D2	4.124	7.876	4.124
3D Object-D3	4.704	7.961	4.704
3D Object-D4	3.554	7.855	3.554
Medical image-M1	6.794	7.997	6.794
Medical image-M2	6.562	7.993	6.562
Medical image-M3	6.368	7.996	6.368
Medical image-M4	6.996	7.999	6.996

The encryption and decryption time obtained for the different 3D objects are given below in Table VI.

TABLE VI. ENCRYPTION AND DECRYPTION TIME FOR VARIOUS IMAGES

Image Details	Encryption time(s)	Decryption time(s)
3D Object-D1	9.898973	1.742406
3D Object-D2	7.262983	1.771650
3D Object-D3	6.978551	1.904733
3D Object-D4	7.666405	1.955614
Medical image-M1	6.371	1.762
Medical image-M2	0.642	0.114
Medical image-M3	1.028	0.172
Medical image-M4	2.944	0.742

The NPCR value indicates the percentage of differing pixels between x and y. It is commonly used as a measure of the dissimilarity or change between two images or matrices. A higher NPCR value indicates a greater level of change between the two matrices. The NPCR values obtained for the 10 different 3D object models under consideration are tabulated in Tables VII and VIII.

TABLE VII. NPCR VALUES FOR DIFFERENT 3D MODELS

Metric	3D Object-D1	3D Object-D2	3D Object-D3	3D Object-D4
NPCR	99.4999	99.4916	99.4916	99.4907

TABLE VIII. NPCR VALUES FOR MEDICAL IMAGES

Metric	Medical Image-M1	Medical Image-M2	Medical Image-M3	Medical Image-M4
NPCR	99.734	96.219	98.854	99.3438

Universal Image Quality Index (UACI) is a metric used for evaluating the quality of an image by comparing a reference image to a distorted or processed image. UACI measures the visual similarity between the original and distorted images.

The formula to calculate UACI is as follows:

$$UACI = (1/N) \times \sum \sqrt{\left(r(i) - d(i)\right)^2 + \left(c(i) - d(i)\right)^2} \quad (23)$$

Where N is the total number of pixels in the image. $r(i)$ represents the pixel intensity value of the original image at pixel i. $d(i)$ represents the pixel intensity value of the decrypted image at pixel i.

The UACI value ranges from 0 to infinity. A lower UACI value indicates higher similarity and better quality between the reference and distorted images. The UACI values obtained for our proposed system are given in Tables IX and X.

TABLE IX. UACI VALUES FOR VARIOUS 3D OBJECT MODELS

Metric	3D Object-D1	3D Object-D2	3D Object-D3	3D Object-D4
UACI	24.1933	24.2435	24.2250	24.2369

TABLE X. UACI VALUES FOR MEDICAL IMAGES

Metric	Medical Image-M1	Medical Image-M2	Medical Image-M3	Medical Image-M4
UACI	35.308	29.421	35.264	26.239

The inferences from the results are as follows:

Low Correlation: When the encrypted images have little statistical similarity to the original images, it indicates that the encryption model is effective in transforming the data in such a way that it becomes difficult to discern any patterns or similarities between the original and encrypted data. This lack of correlation is a positive sign for the security of the encryption model, as it suggests that it is challenging for an attacker to derive any meaningful information about the original image from the encrypted version.

High Entropy: High entropy in encrypted images means that the data is highly random and contains a large amount of information. This randomness makes it difficult for an attacker to predict or analyze the encrypted data, thereby enhancing the security of the encryption model. High entropy ensures that the encrypted data appears as random noise to anyone who attempts to analyze it without the proper decryption key.

High NPCR and Low UACI: NPCR and UACI are metrics used to evaluate the robustness of an encryption model against small changes in the input image. A high NPCR value suggests that a small change in the plaintext image results in a significant change in the encrypted image. Similarly, a low UACI value implies that the average intensity of the pixels in the encrypted image does not change much when the original image is modified slightly. These characteristics are essential for security, as they indicate that the encrypted data remains largely unaffected by minor alterations in the input image, making it more challenging for attackers to manipulate the encrypted data to retrieve meaningful information. Table XI represents the performance of the proposed encryption model in contrast with the existing works.

TABLE XI. PERFORMANCE OF THE PROPOSED ENCRYPTION MODEL IN CONTRAST WITH THE EXISTING WORKS

Reference details	Algorithms used	Inferences
Ref. [29]	2D Schaffer map hyperchaotic model	Tested on benchmark images and validated in terms of entropy and correlation. The average entropy value is 7.99945 and the correlation value ranges -92×10^{-7} and 18×10^{-5}.
Ref. [30]	3D memristive neuron model-based encryption model	2D and 3D image encryption using chaotic function, validated in terms of correlation, entropy, NPCR value of 99.6199, and UACI value of 33.4661.
Ref. [31]	Hyperchaotic model based on Cascade Modulation Couple (CMC) and two 1D-chaotic map.	Teste on benchmark 2D images, validated in terms of correlation, entropy, UACI, and NPCR
Proposed Methodology	6D hyperchaotic function encryption model	Tested on medical and 3D printed model images, validated in terms of correlation, entropy, NPCR, and UACI. Performance was found to be robust when compared with the existing works [29–31].

Overall, considering these characteristics collectively can help assess the robustness and security of an image encryption model. They provide insights into how well the encryption process protects the original data from unauthorized access and ensures the confidentiality and integrity of the information.

Implementing and solving 6D hyperchaotic systems can be computationally expensive, especially in real-time applications or on resource-constrained devices. Hyperchaotic systems, especially in higher dimensions, may not have well-established hardware implementations. Implementing them efficiently in real-world applications could be challenging.

V. CONCLUSION

The outcome of this research work finds its applications in healthcare and the 3D printing industry for secure data transfer. A 6D hyperchaotic system operates in a six-dimensional phase space. This high dimensionality provides a large parameter space, making it more challenging for attackers to predict and reverse-engineer the encryption process. Hyperchaotic systems are characterized by highly nonlinear differential equations. This nonlinearity adds an extra layer of complexity to the encryption process, making it more resistant to standard cryptanalysis techniques. The randomness and unpredictability of hyperchaotic systems make them resistant to various statistical attacks, such as frequency analysis or correlation attacks.

As we have seen from this work, a six-dimensional hyperchaotic system characterized by multiple positive Lyapunov exponents, indicating highly complex and unpredictable dynamics was used for the encryption of the 3D object and medical images. This 6D hyperchaotic system had a higher level of complexity and intricacy in its behavior, making it valuable for studying nonlinear dynamics and complex systems. The unpredictable nature of hyperchaotic systems is advantageous for information security applications, such as cryptography, as it makes it difficult for adversaries to decipher encrypted information. Also, the larger parameter space of a 6D hyperchaotic system provides more flexibility and control in shaping the system's behavior. The performance validation by metrics revealed the proficiency of the 6D hyperchaotic encryption model.

We will be focusing on the hardware implementation of the hyperchaotic encryption model as the next step forward. Deep learning model coupled with the 6D hyperchaotic model yields proficient results.

CONFLICT OF INTEREST

The authors declare no conflict of interest.

AUTHOR CONTRIBUTIONS

S.N Kumar formulated the algorithm and collected the data set and Siju John performed the algorithm development and evaluated the results. All authors had approved the final version.

ACKNOWLEDGMENT

The authors acknowledge the support provided by AICTE IDEA lab at Amal Jyothi College of Engineering, Kottayam, Kerala, India for Computer Aided Modelling and Data collection pertaining to the models used in this work and special thanks to Dr. Vishal John Mathai (Mar Sleeva Medicity Hospital, Pala, Kerala, India) for the support provided in data collection.

REFERENCES

[1] H. Sajedi and S. R. Yaghobi, "Information hiding methods for E-healthcare," *Smart health*, vol. 15, 100104, 2020.

[2] I. J. Kadhim, P. Premaratne, P. J. Vial, and B. Halloran, "A comprehensive survey of image steganography: Techniques, evaluations, and trends in future research," *Neurocomputing*, vol. 335, pp. 299–326, 2019.

[3] K. C. Shankar and S. P. Shyry, "A novel hybrid encryption method using S-box and Henon maps for multidimensional 3D medical images," *Soft Computing*, pp. 1–11, 2023.

[4] S. Gao, R. Wu, X. Wang, J. Wang, Q. Li, C. Wang, and X. Tang, "A 3D model encryption scheme based on a cascaded chaotic system," *Signal Processing*, vol. 202, 108745, 2023.

[5] N. G. Pham, S. H. Lee, O. H. Kwon, and K. R. Kwon, "3D printing model random encryption based on geometric transformation," *International Journal of Machine Learning and Computing*, vol. 8, no. 2, pp. 186–190, 2018.

[6] B. Raj, L. J. Anbarasi, M. Narendra, and V. J. Subashini, "A new transformation of 3D models using chaotic encryption based on arnold cat map," in *Porc. the 7th International Conference on Emerging Internet, Data and Web Technologies*, 2019, pp. 322–332.

[7] X. Wang, M. Xu, and Y. Li, "Fast encryption scheme for 3D models based on chaos system," *Multimedia Tools and Applications*, vol. 78, pp. 33865–33884, 2019.

[8] N. A. Ali, A. M. S. Rahma, and S. H. Shaker, "3D polygon mesh encryption based on 3D Lorenz chaotic map," *iJIM*, vol. 15, no. 15, 2021.

[9] N. G. Pham, K. S. Moon, S. H. Lee, and K. R. Kwon, "An effective encryption algorithm for 3D printing model based on discrete cosine transform," *Journal of Korea Multimedia Society*, vol. 21, no. 1, pp. 61–68, 2018.

[10] G. N. Pham, S. H. Lee, and K. R. Kwon, "Interpolating spline curve-based perceptual encryption for 3D printing models," *Applied Sciences*, vol. 8, no. 2, 242, 2018.

[11] X. Jin, S. Zhu, C. Xiao, H. Sun, X. Li, G. Zhao, and S. Ge, "3D textured model encryption via 3D Lu chaotic mapping," *Science China Information Sciences*, vol. 60, pp. 1–9, 2017.

[12] G. N. Pham, K. R. Kwon, E. J. Lee, and S. H. Lee, "Selective encryption algorithm for 3D printing model based on clustering and DCT domain," *Journal of Computing Science and Engineering*, vol. 11, no. 4, pp. 152–159, 2017.

[13] V. S. Lima, F. Madeiro, and J. B. Lima, "Encryption of 3D medical images based on a novel multiparameter cosine number transform," *Computers in Biology and Medicine*, vol. 121, 103772, 2020.

[14] Y. Liang, F. He, and H. Li, "An asymmetric and optimized encryption method to protect the confidentiality of the 3D mesh model," *Advanced Engineering Informatics*, vol. 42, 100963, 2019.

[15] M. Shah, W. Zhang, H. Hu, H. Zhou, and T. Mahmood, "Homomorphic encryption-based reversible data hiding for 3D mesh models," *Arabian Journal for Science and Engineering*, vol. 43, pp. 8145–8157, 2018.

[16] U. S. Choi, S. J. Cho, and S. W. Kang, "Color medical image encryption using 3D chaotic cat map and NCA," in *Proc. 2019 10th IFIP International Conference on New Technologies, Mobility, and Security (NTMS)*, 2019, pp. 1–5.

[17] D. Kumar, V. K. Sudha, and R. Ranjithkumar, "A one-round medical image encryption algorithm based on a combined chaotic key generator," *Medical & Biological Engineering & Computing*, vol. 61, no. 1, pp. 205–227, 2023.

[18] X. W. Kok, A. Singh, and B. T. Raimi-Abraham, "A design approach to optimise secure remote three-dimensional (3D) printing: A proof-of-concept study towards advancement in telemedicine," *Healthcare*, vol. 10, no. 6, 1114, 2022.

[19] B. Macq, P. R. Alface, and M. Montanola, "Applicability of watermarking for intellectual property rights protection in a 3D printing scenario," in *Proc. the 20th International Conference on 3D Web Technology*, 2015, pp. 89–95.

[20] L. Li, S. Wang, S. Zhang, T. Luo, and C. C. Chang, "Homomorphic encryption-based robust reversible watermarking for 3D model," *Symmetry*, vol. 12, no. 3, 347, 2020.

[21] Q. V. Khanh, A. Chehri, N. M. Quy, N. D. Han, and N. T. Ban, "Innovative trends in the 6G era: A comprehensive survey of architecture, applications, technologies, and challenges," *IEEE Access*, 2023.

[22] S. R. Masadeh, "A new encryption system for IoT devices using embedded key cryptosystem," *International Journal of Electronic Security and Digital Forensics*, vol. 15, no. 1, pp. 56–65, 2023.

[23] J. Liu, Y. Zhang, and B. Gong, "A data compression and encryption method for green edge computing," *Cluster Computing*, vol. 6, pp. 1–9, 2023.

[24] R. Lin and S. Li, "An image encryption scheme based on lorenz hyperchaotic system and RSA algorithm," *Security and Communication Networks*, pp. 1–18, 2021.

[25] W. Huang, D. Jiang, Y. An, L. Liu, and X. Wang, "A novel double-image encryption algorithm based on Rossler hyperchaotic system and compressive sensing," *IEEE Access*, vol. 9, pp. 41704–41716, 2021.

[26] A. A. K. Javan, M. Jafari, A. Shoeibi, A. Zare, M. Khodatars, N. Ghassemi, and J. M. Gorriz, "Medical images encryption based on adaptive-robust multi-mode synchronization of chen hyper-chaotic systems," *Sensors*, vol. 21, no. 11, 3925, 2021.

[27] S. Wang, X. Wang, Y. Zhou, and B. Han, "A memristor-based hyperchaotic complex Lu system and its adaptive complex generalized synchronization," *Entropy*, vol. 18, no. 2, 58, 2016.

[28] K. M. Hosny, S. T. Kamal, M. M. Darwish, and G. A. Papakostas, "New image encryption algorithm using hyperchaotic system and fibonacci q-matrix," *Electronics*, vol. 10, no. 9, 1066, 2021.

[29] U. Erkan, A. Toktas, and Q. Lai, "2D hyperchaotic system based on Schaffer function for image encryption," *Expert Systems with Applications*. vol. 213, 119076, 2023.

[30] X. Gao, M. Miao, and X. Chen, "Multi-image encryption algorithm for 2D and 3D images based on chaotic system," *Frontiers in Physics*. vol. 10, 901800, 2022.

[31] J. Sun, "2D-SCMCI hyperchaotic map for image encryption algorithm," *IEEE Access*, vol. 9, pp. 59313–59327, 2021.