IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 5 December 2022, accepted 18 December 2022, date of publication 26 December 2022,
date of current version 12 January 2023.

Digital Object Identifier 10.1109/ACCESS.2022.3232461

RESEARCH ARTICLE

Chaotic-Map Based Encryption for 3D Point and 3D Mesh Fog Data in Edge Computing

K. R. RAGHUNANDAN[1], RADHAKRISHNA DODMANE[1], K. BHAVYA[2], N. S. KRISHNARAJ RAO[3], AND ADITYA KUMAR SAHU[4]

[1]Department of Computer Science and Engineering, NMAM Institute of Technology, NITTE (Deemed to be University), Nitte, Karnataka 574110, India
[2]Department of Mathamatics, NMAM Institute of Technology, NITTE (Deemed to be University), Nitte, Karnataka 574110, India
[3]Department of Information Science and Engineering, NMAM Institute of Technology, NITTE (Deemed to be University), Nitte, Karnataka 574110, India
[4]Amrita School of Computing, Amaravati Campus, Amrita Vishwa Vidyapeetham, Amaravati, Andhra Pradesh 522503, India

Corresponding author: Aditya Kumar Sahu (adityasahu.cse@gmail.com)

This work was supported by the NMAM Institute of Technology, Nitte (Deemed to be University).

ABSTRACT Recent decades have seen dramatic development and adoption of digital technology. This technological advancement generates a large amount of critical data that must be safeguarded. The security of confidential data is one of the primary concerns in fog computing. As a result, achieving a reliable level of security in the fog computing environment is crucial. In this context, 3D point and mesh fog data are becoming increasingly popular among the various types of data stored in the fog. Data encryption using chaotic behavior is one of the preferred research areas due to its unique properties, such as randomness, determinism, sensitivity to initial conditions, and ergodicity. In this paper, we have taken advantage of this chaotic behavior to achieve higher security. This study presents a novel approach for protecting the privacy of 3D point and mesh fog data. Initially, the fog data coordinates are transformed using the sequence generated by the chaotic behavior. Then, bifurcation analysis is used to depict the enhanced scope of the proposed map. The quality of the proposed chaotic system is assessed using metrics such as the Lyapunov exponent and approximate entropy. Results show that the proposed encryption framework performs superior when subjected to brute-force and statistical attacks. Further, the designed framework produces better results than the prior literature.

INDEX TERMS Chaotic behavior, decryption, encryption, fog computing, 3D point fog, 3D mesh point.

I. INTRODUCTION

Fog computing, also known as fogging, is a type of cloud architecture that is placed in between data and the cloud. It is a distributed design in which fog nodes gather data from various edge devices. This enables faster data transmission, boosting overall network performance and efficiency. Using fog computing, data management and storage can be efficiently streamlined.

The architecture of the fog computing process is depicted in Figure 1. It is made up of three layers. The lowest layer is made up of edge devices such as sensors, actuators, vehicles, and data-generating apps. Fog nodes sit in the second layer above the edge devices, collecting data from multiple edge devices. Fog servers collect data from the edges via transport layer technologies such as WiFi or Bluetooth. They handle real-time edge requests and serve as a bidirectional gateway between the cloud and edge devices. Fog nodes are typically routers or base stations. The third layer is the cloud data center, which receives data from fog nodes.

With the growing popularity of web usage, 3D points and 3D cross-section [1] information depictions are commonly used for article portrayal. Applications like Autodesk123D capture images of articles from various points and send them to remote fog-based workers. This information is then used to create a 3D model of the articles, which is then sent to the clients. There are various desktop applications for altering the 3D point and cross-section fog information. Virtual Reality (VR) innovation has recently enabled clients to experience augmented reality 3D climate.

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

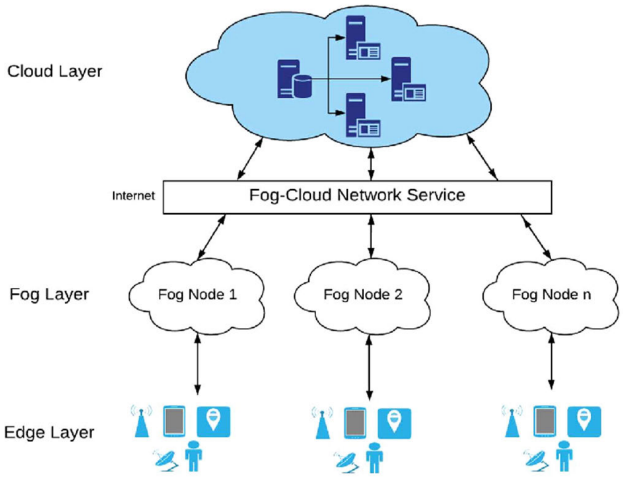

FIGURE 1. Layered architecture of fog computing process.

However, there have always been possible risks to cloud storage from numerous security vulnerabilities. The amount of data that each user has varied from GBs to TBs, and the local storage cannot keep up with this enormous demand on its own. Because of this, adopting a low-complexity, high-security cloud storage service is now a must in today's world [2]. In any case, the primary concern raised by these data is security, as they are stored in the fog. As a result, encryption of this information is an indispensable errand. The 3D information is enormous and multi-dimensional. Likewise, they have a high relationship among the focuses around them. Subsequently, conventional encryption techniques like Rivest, Shamir, and Adleman (RSA) [3], Advanced Encryption Standard (AES) [4], Data Encryption Standard (DES) [5], and blowfish [6], Two-fish [7], Elliptic Curve Cryptography (ECC) [8], El Gamal encryption [9], Diffie-Hellman key trade [10], and so on, may not be sufficient to meet the security issues of 3D information.

There are certain privacy and security issues to be concerned about 3D fog data, including limited network visibility, ineffective attack detection techniques, the lack of user-selective data collecting, problems with virtualization, and malicious fog node issues [11]. Several scholars and advert infrastructure implementers predict that fog platforms will be created and distributed in the coming years in a secure way to accommodate the ever-growing progress of connected computational devices. To create such secure systems, many researchers are following security-centric approaches. In this regard, this paper introduces a novel security framework for the protection of 3D point fog and 3D mesh fog data, which provides a solution to a fog computing environment.

The three main contributions of this paper are:

a) A new chaotic behavior generates a chaotic sequence for encryption.

b) A novel two-level framework for the encryption of 3D point fog and 3D mesh fog data.

c) Assessment of the proposed encryption scheme and comparison with existing frameworks.

The rest of the paper is organized as follows. Section II includes a thorough review of previous works in the field. Section III describes how to generate chaotic behavior sequences using the proposed chaotic behavior map. Section IV describes the proposed encryption method. The findings and discussion are presented in Section V. The work is concluded in Section VI.

II. LITERATURE SURVEY

Since fog computing is a recent innovation in today's world, managing the security issues associated with fog computing is most important. Chaos-based encryption algorithms have been widely used for image encryption due to their ease of implementation in comparison to more complex traditional cryptosystems such as AES and DES. Various researchers addressed the enhancement in the field of fog computing concerning security. Authors in [12] emphasize the benefits of fog computing in various fog applications, such as smart grids and smart traffic control systems. In [13], adaptive-thresholding sparsification and PCS techniques are used to develop a new visually secure image encryption scheme. An encryption method used in distributed computing was proposed in [14]. In this work, a patient-driven plan was proposed in which trait-based encryption was performed. This framework accomplished a serious level of safety by using multi-authority encryption. Intermediary-based encryption conspires for distributed storage was proposed in [15]. In this plan, an intermediary is approved by the sender for information encryption. This scrambled information is transferred to the fog. This structure depends on grid-based cryptography. The framework was demonstrated to accomplish protection from the acted-up fog workers. Homomorphic encryption is used in [16] to ensure the security of large amounts of data stored in the fog. Various fog notes were empowered and isolated in this study to perform computational analysis on numerous pieces of data. These hubs were designed to function independently. As a result, it was discovered that the presentation of this framework was superior to encryption using a single distributed computing hub. The work proposed in [17] describes another encryption scheme based on the confusion hypothesis. In this work, the compressive detecting hypothesis was used to achieve synchronous pressure and encryption. The estimation lattice, which is used for encryption, is a volatile strategic arrangement. A sigmoid capacity was used to measure the capacity. As a substitute for Discrete Cosine Change (DCT) premise work, a single round word reference was used. As a result, for each image, a unique word reference was created. This aided in the achievement of excellent encryption execution.

Encryption using hyper-chaotic behaviors was proposed in [18]. Here, it uses two types of encryption. The data was first encoded using block changes, then bit stages. Finally, security was upgraded by rearranging the bits at the bit level.

Encryption was accomplished using a hash value with a length of 256 bits. This paper proposes a scheme for encrypting 3D point fog data using two types of encryption strategies. The primary strategy was to use strategic tumultuous planning to determine the age of irregular successions and the later strategy was based on a change grid projection of the 3D fog information focuses' directions.

3D fog information encryption utilizing the arrangements produced from the chaotic behavior was proposed in [19]. Here, the succession produced by cat tumultuous guides was used for two kinds of encryptions. The main system depended on arranging the arrangements and rearranging the areas of the 3D information dependent on the arranged successions.

III. CHAOTIC BEHAVIOR SEQUENCE GENERATION

Authors Pacha et al. [20] revealed that data encryption systems generate hidden messages with chaotic behavior. Because of their inherent characteristics, chaotic systems have fascinated the interest of many researchers. The Lyapunov exponent and approximate entropy are two commonly used metrics for validating the chaotic behavior nature.

A. CHAOTIC BEHAVIOR OF LYAPUNOV EXPONENT (LE)

The Lyapunov exponent [21] is a widely used metric for quantifying chaos in a chaotic behavior. It computes the average divergence between two trajectories obtained with two different initial values that are close to each other. Lyapunov Exponent (LE) is mathematically defined as follows [22]:

$$\mathbf{LE} = \mathbf{lim_{n\to\infty}} \frac{\mathbf{1}}{\mathbf{N}} \sum_{\mathbf{n=1}}^{\mathbf{N}} \mathbf{log} \left| \frac{\mathbf{dx_{n+1}}}{\mathbf{dx_n}} \right| \tag{1}$$

A positive Lyapunov exponent indicates that the two trajectories generated by the map will diverge exponentially with time, while a negative value indicates that the two trajectories will overlap at some point in time. Furthermore, the greater the value of LE, the more chaotic behavior of the sequence produced by the map. The majority of chaotic systems in use today may have several drawbacks, such as discontinuous chaotic parameter ranges, a dearth of robust chaos, and a propensity for chaos degradation. To avoid the said limitations, a two-dimensional (2-D) parametric polynomial chaotic system (2D-PPCS) was proposed in [23]. High-dimensional chaotic maps have been extensively studied in recent years due to their more complex structures and advantageous dynamic properties when compared to low-dimensional chaotic maps. Customizing the number of positive LEs and their values is tricky when making high-dimensional chaotic maps because the complexity of a high-dimensional chaotic map can be reflected in its positive LEs [24]. Many high-dimensional chaotic maps with multiple positive LEs have been developed in recent work [25], [26]. In [27], an n-dimensional polynomial chaotic system that can generate nD chaotic maps with any desired LEs is proposed.

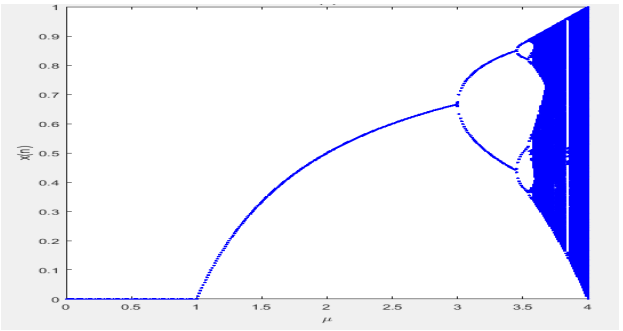

FIGURE 2. Bifurcation of the logistic map.

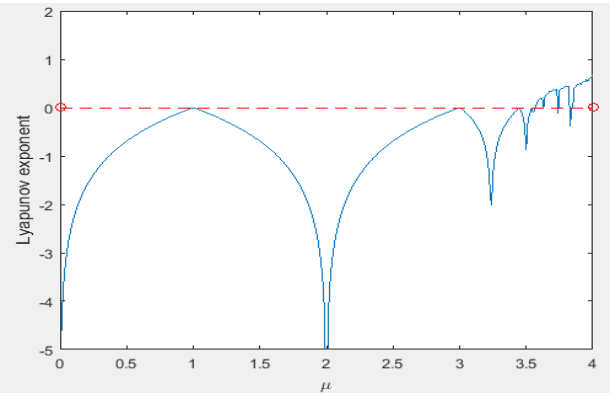

FIGURE 3. Lyapunov exponent of logistic map.

B. APPROXIMATE ENTROPY (AE)

Approximate entropy [28] is also used to represent the Chaotic behavior nature of Chaotic behaviors quantitatively by Pincus (1995). Higher AE values indicate that the Chaotic behavior sequence has a high level of complexity.

C. LOGISTIC MAP

The purpose of using the logistic map is to perform more complex pixel permutation, or better diffusion operation, by taking advantage of its well-known chaotic behavior. One function finds new positions for the pixels, while the other changes their intensities. The logistic map is defined as:

$$x_{n+1} = \mu x_n (1 - x_n) \tag{2}$$

where control parameter $\mu \in [0, 4]$ and initial condition $x_0 \in [0, 1]$. Here Chaotic behavior of x_{n+1} is completely reliant on the value μ. According to the bifurcation diagram of the Logistic Map given in Figure 2, it can be seen that the value of μ approaches in the range $\mu \in [3.57, 4]$.

Figure 3 depicts the logistic map's Lyapunov exponent to further illustrate the logistic map's chaotic behavior nature. The chaotic behavior region is represented by the positive region on the Lyapunov exponent graph.

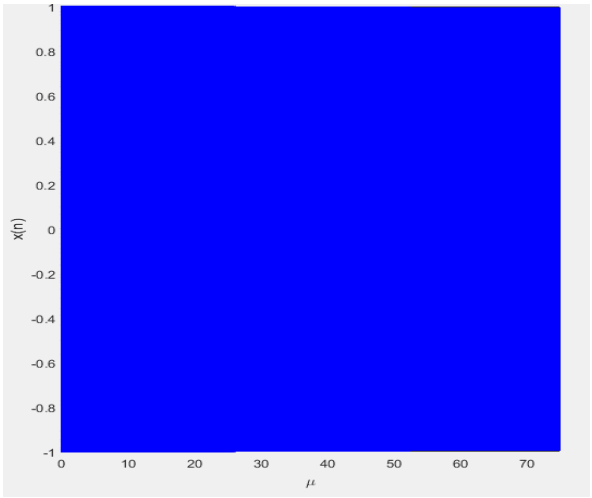

FIGURE 4. Bifurcation of proposed Chaotic Behavior.

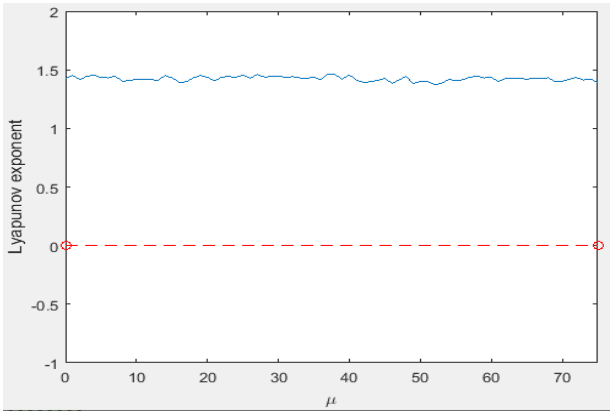

FIGURE 5. Lyapunov exponent of proposed chaotic behavior.

D. PROPOSED CHAOTIC BEHAVIOR

The proposed Chaotic Behavior is defined as:

$$x_{n+1} = ((7000 - \mu)/7000)sin(8\Pi x_n) \quad (3)$$

here $\mu \in [0, 75]$ is the control parameter and $x_0 \in [0, 1]$ is the initial condition. According to figure 4, the proposed map is chaotic behavior in the range. This range is significantly larger than the logistic map and logistic sine maps. The proposed map's sequences are used for the encryption and decryption of point fog and mesh fog data. Furthermore, the first 1000 values generated using a specific key are ignored to avoid the transient effect.

Figure 5 depicts the proposed chaos behavior of Lyapunov exponent, which is plotted similarly to the logistic map and logistic sine maps. As seen in Figure 5, the proposed map is completely chaotic behavior in the region $\mu \in [0, 75]$. However, the highest value of LE obtained is 1.2881 when $\mu = 75$.

Furthermore, the Lyapunov exponent and approximate entropy are evaluated and shown in Table 1 to quantitatively illustrate the chaotic behavior properties of the proposed map.

TABLE 1. Comparison of proposed Chaotic Behavior maps with logistic and logistic sine maps.

SL. NO.	MAP	MAP EQUATION	LE	AE
1	LOGISTIC	$x_{n+1} = \mu\, x_n(1 - x_n)$	0.5933	0.5142
2	LOGISTIC SINE MAP	$x_{n+1} = \mu\, x_n(1 - x_n) + \frac{4-\mu}{4} sin(\Pi x_n)$	0.5933	0.5142
3	PROPOSED MAP	$x_{n+1} = \frac{7000 - \mu}{7000} sin(8\Pi x_n)$	1.2881	1.6762

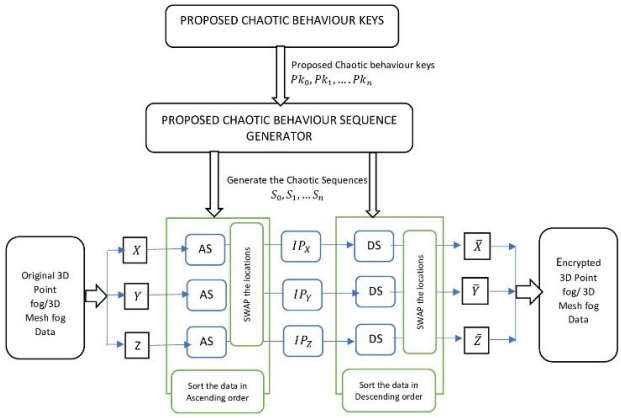

FIGURE 6. Proposed generalized process of two-level encryption schemes used for 3D point fog and 3D mesh fog data.

According to the tabulated values, the proposed map's LE and AE values are high when compared to other maps, indicating that the proposed map has better chaotic behavior than existing maps.

IV. PROPOSED METHODOLOGY

This section explains how the proposed chaotic behavior map generates a sequence for fog encryption. The encryption and decryption keys are securely transmitted between the sender and the receiver. Furthermore, because this technique only uses a few sets of keys, the risk of data leakage is reduced. Since two levels of encryption are used, the proposed scheme achieves an excessive level of security. In the first level, the sequences generated by chaotic behavior maps are sorted in ascending order to shuffle the coordinates of the fog data. In the second level, the sequences generated by chaotic behavior maps are sorted in descending order to further shuffle the coordinates of the fog data. Figure 6 illustrates the generalized process of two-level encryption schemes used for 3D point fog and 3D mesh fog data.

The process of decryption of 3D point fog is used to reverse the encryption effect and recover the original 3D point fog/3D mesh fog data from the encrypted data. Figure 7 illustrates the generalized process of two-level decryption schemes used for 3D point fog and 3D mesh fog data. The process of encryption and decryption process of the 3D point fog model and 3D

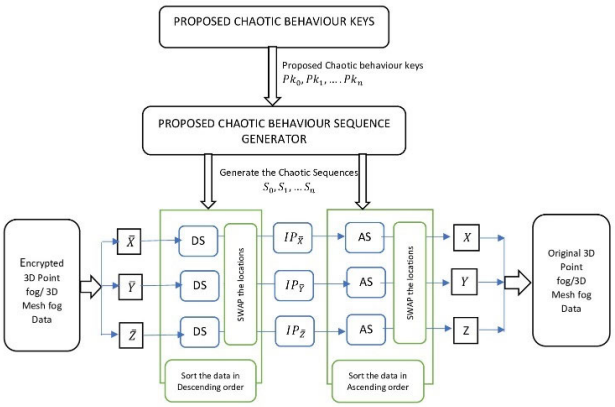

FIGURE 7. Proposed generalized process of two-level decryption schemes used for 3D point fog and 3D mesh fog data.

mesh fog data is illustrated using algorithms in the following subsections.

A. 3D POINT FOG MODEL

The data for the 3D point fog model is organized in a three-dimensional coordinate system i.e., each point is made up of three coordinates which are depicted in Figure 6. Furthermore, the proposed scheme employs a double encryption method. The proposed chaotic behavior map generates six random sequences to encrypt the information. These six sequences are made up of six chaotic behavior keys referred to as $Pk_1, Pk_2, \ldots .Pk_6$.

Encryption: The process of encryption of 3D point fog is used to convert the original data $P_1, P_2, \ldots P_n$ into the encrypted data $Ep_1, Ep_2 \ldots, Ep_n$. Algorithm 1 depicts the steps necessary to encrypt the 3D point fog model.

Algorithm 1 Encryption of 3D Point Fog

Input: Original point fog $P_1, P_2, \ldots P_n$ where $P_i = \{x_i, y_i.z_i\}$ and Chaotic keys $Pk_1, Pk_2, \ldots .Pk_6$ where $Pk_i = \{x_0, \mu_i\}$.
Output: Encrypted point fog $Ep_1, Ep_2 \ldots, Ep_n$ where $Ep_i = \{\bar{x}_i, \bar{y}_i, \bar{z}_i\}$.
Steps:

1: Using the chaotic behavior keys Pk_1, Pk_2, Pk_3 generate three chaotic behavior sequences S_1, S_2, S_3.
2: Sort the chaotic behavior sequences in ascending order and store the new location of each value.
3: Using the stored locations, swap the locations of the point fog data $P_1, P_2, \ldots P_n$ to obtain intermediate point fog data $IP_1, IP_2, \ldots IP_n$.
4: Now, using the chaotic behavior keys Pk_4, Pk_5, Pk_6 generate three new chaotic behavior sequences S_4, S_5, S_6.
5: Sort the new chaotic sequences in descending order and store the new location of each value.
6: Using the stored locations, swap the locations of the intermediate point fog data $IP_1, IP_2, \ldots IP_n$ to obtain encrypted point fog data $Ep_1, Ep_2 \ldots, Ep_n$.

Decryption: The process of decryption of 3D point fog is used to reverse the encryption effect and recover the original data $P_1, P_2, \ldots P_n$ from the encrypted data $p_1, Ep_2 \ldots, Ep_n$. The process of decrypting the 3D point fog model is illustrated using Algorithm 2.

Algorithm 2 Decryption of 3D Point Fog

Input: Encrypted point fog $Ep_1, Ep_2 \ldots, Ep_n$ chaotic behavior keys $Pk_1, Pk_2, \ldots .Pk_6$ where $Pk_i = \{x_0, \mu_i\}$.
Output: Original point fog data $P_1, P_2, \ldots P_n$.
Steps:

1: Using the chaotic behavior keys Pk_4, Pk_5, Pk_6 generate three chaotic behavior sequences S_4, S_5, S_6.
2: Sort the chaotic behavior sequences in descending order and store the new location of each value.
3: Using the stored locations, swap the locations of the point fog data $EP_1, EP_2, \ldots EP_n$ to obtain intermediate point fog data $IP_1, IP_2, \ldots IP_n$.
4: Now, using the chaotic behavior keys Pk_1, Pk_2, Pk_3 generate three new chaotic behavior sequences S_1, S_2, S_3.
5: Sort the new chaotic behavior sequences in ascending order and store the new location of each value.
6: Using the stored locations, swap the locations of the intermediate point fog data $IP_1, IP_2, \ldots IP_n$ to obtain original point fog data $p_1, p_2 \ldots, p_n$.

B. 3D MESH FOG MODEL

The 3D Mesh fog model uses the encryption process to convert the original mesh fog $M_1, M_2, \ldots .M_n$ using chaotic behavior keys $EM_1, EM_2, \ldots .EM_{18}$ and produces encrypted mesh fog $EM_1, EM_2, \ldots .EM_n$. Figure 6 illustrates the process of two-level encryption scheme for mesh fog data and the steps involved in the encryption of the 3D mesh fog model. The process of 3D Mesh fog data is explored using algorithms 3 and 4.

The decryption of 3D mesh fog is done to reverse the effect of encryption and to get back the original data $M_1, M_2, \ldots M_n$ from the encrypted data $EM_1, EM_2 \ldots, EM_n$. Figure 7 illustrates the process of the proposed decryption scheme using Mesh fog data. This process is illustrated using Algorithm 4.

V. RESULTS AND DISCUSSIONS

To assess the results of 3D point fog and 3D mesh fog data, the datasets from the Artec 3D [29], [30] and Stanford 3D scanning repository [30], [31] are used. Secret key sensitivity analysis, encryption speed analysis, entropy analysis, Asymmetry coefficient, and Differential analysis are used to assess the security of 3D point fog and 3D mesh fog data.

A. SENSITIVITY ANALYSIS OF SECRET KEYS OF 3D POINT AND 3D MESH FOG DATA

In order to be effective, an encryption system must be highly sensitive to encryption keys. There must be a complete

Algorithm 3 Encryption of 3D Mesh Fog

Input: Original mesh fog $M_1, M_2, \ldots M_n$ where $M_i = \{V_1^i, V_2^i.V_3^i\}$.
Here, $V_1^i = \{x_1^i, y_1^i.z_1^i\}$, $V_2^i = \{x_2^i, y_2^i.z_2^i\}$ $and V_3^i = \{x_3^i, y_3^i.z_3^i\}$ and Chaotic Behavior keys $Mk_1, Mk_2, \ldots .Mk_{18}$ where $Mk_i = \{x_0, \mu_i\}$.

Output: Encrypted Mesh fog $EM_1, EM_2 \ldots, EM_n$ where $EM_i = \{\bar{V_1^i}, \bar{V_{2i}^i}, \bar{V_3^i}\}$
Here $\bar{V_1^i} = \{\bar{x_1^i}, \bar{y_{1_i}^i}, \bar{z_1^i}\}$, $\bar{V_2^i} = \{\bar{x_2^i}, \bar{y_{2_i}^i}, \bar{z_2^i}\} and \bar{V_1^i} = \{\bar{x_3^i}, \bar{y_{3_i}^i}, \bar{z_3^i}\}$,

Steps:

1: Using the chaotic behavior keys $Mk_1, Mk_2, \ldots .Mk_9$ generate nine chaotic behavior sequences $S_1, S_2, \ldots S_9$.
2: Sort the chaotic behavior sequences in ascending order and store the new location of each value.
3: Using the stored locations, swap the locations of the point fog data $M_1, M_2, \ldots M_n$ to obtain intermediate point fog data $IM_1, IM_2, \ldots IM_n$.
4: Now, using the chaotic behavior keys $Mk_{10}, Mk_{11}, \ldots .Mk_{18}$ generate nine new chaotic behavior sequences $S_{10}, S_{11}, \ldots S_{18}$.
5: Sort the new chaotic behavior sequences in descending order and store the new location of each value.
6: Using the stored locations, swap the locations of the intermediate point fog data $IM_1, IM_2, \ldots IM_n$ to obtain encrypted point fog data $EM_1, EM_2 \ldots, EM_n$.

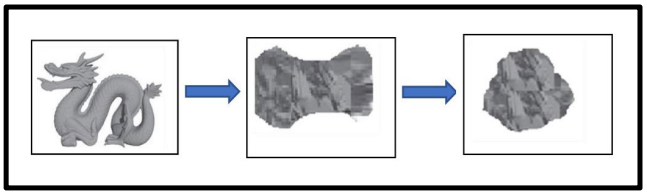

FIGURE 8. Results obtained using secret key sensitivity analysis of 3D point fog data.

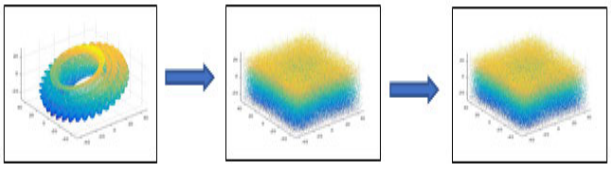

FIGURE 9. Results obtained using secret key sensitivity analysis of 3D Mesh fog data.

change in the cipher image for even small changes to the encryption keys. Figures 8 and 9 show the original data, encrypted data, and the result obtained after decryption with the new set of keys. The sensitivity analysis of the proposed methods is tested by changing the secret keys by $\Delta = 10^{-15}$. The decryption is then carried out with a new set of keys, $PK_i = \{x_0 + \Delta, \mu_i + \Delta\}$ and $i = 1, 2, \ldots, 6$ for 3D point and

Algorithm 4 Decryption of 3D Mesh Fog

Input: Encrypted Mesh fog $EM_1, EM_2 \ldots, EM_n$ where $EM_i = \left\{\bar{V_1^i}, \bar{V_{2_i}^i}, \bar{V_3^i}\right\}$
Here $\bar{V_1^i} = \{\bar{x_1^i}, \bar{y_{1_i}^i}, \bar{z_1^i}\}$, $\bar{V_2^i} = \left\{\bar{x_2^i}, \bar{y_{2_i}^i}, \bar{z_2^i}\right\}$ and $\bar{V_1^i} = \left\{\bar{x_3^i}, \bar{y_{3_i}^i}, \bar{z_3^i}\right\}$ and Chaotic Behavior keys $Mk_1, Mk_2, \ldots .Mk_{18}$ where $Mk_i = \{x_0, \mu_i.\}$

Output: Original Mesh fog $M_1, M_2, \ldots M_n$ where $M_i = \left\{V_1^i, V_2^i.V_3^i\right\}$. Here $V_1^i = \{x_1^i, y_1^i.z_1^i\}$, $V_2^i = \left\{x_2^i, y_2^i.z_2^i\right\}$ and $V_3^i = \left\{x_3^i, y_3^i.z_3^i\right\}$.

Steps:

1: Using the chaotic behavior keys $Mk_{10}, Mk_{11}, \ldots .Mk_{18}$ generate nine chaotic behavior sequences $S_{10}, S_{11}, \ldots S_{18}$.
2: Sort the chaotic behavior sequences in descending order and store the new location of each value.
3: Using the stored locations, swap the locations of the point fog data $EM_1, EM_2, \ldots EM_n$ to obtain intermediate point fog data $IM_1, IM_2, \ldots IM_n$.
4: Now, using the chaotic behavior keys $Mk_1, Mk_2, \ldots .Mk_9$ generate nine new chaotic behavior sequences $S_1, S_2, \ldots S_9$.
5: Sort the new chaotic behavior sequences in ascending order and store the new location of each value.
6: Using the stored locations, swap the locations of the intermediate mesh fog data $IM_1, IM_2, \ldots IM_n$ to obtain the original mesh fog data $M_1, M_2 \ldots, M_n$.

$PK_i = \{x_0 + \Delta, \mu_i + \Delta\}$ and $i = 1, 2, \ldots, 18$ in case of 3D Mesh fog data.

Figures 8 and 9 show that even minor changes in the key parameter values prevent the data from being retrieved. As a result, our proposed framework has extremely high secret key sensitivity. The sensitivity level is in the range of 10^{-15}, which is extremely low.

B. SPEED OF ENCRYPTION ANALYSIS

A good encryption algorithm must also be run-time efficient in addition to security. The proposed algorithm's encryption times are examined for images of various sizes and compared with those of previous works in Table 2. The proposed system was tested using MATLAB R2016b. Table 2 compares the encryption time analysis of point fog data with existing algorithms such as random variable (RV), random transformation matrix (RTM), and random reversible matrix (RRM) [32].

Based on the analysis presented in Table 2, the proposed encryption techniques require very less time compared to the existing methods specified. The randomness of the proposed techniques is further proved using the following subsection.

C. ENTROPY ANALYSIS

Entropy analysis is the best way to quantify the security of mesh encryption. This is because entropy measures the degree of uncertainty in a data source [33]. Entropy

TABLE 2. Encryption time analysis of proposed 3D point and 3D Mesh fog data.

Input data	Size	Time (s)				
		RV	RTM	RRM	Proposed 3D Point	Proposed 3D Mesh Fog
Bunny	8097	0.00533	0.00698	0.00817	0.000133	0.0002145
Happy Buddha	11061	0.00491	0.00428	0.00724	0.000121	0.0002111
Armadillo	33791	0.01331	0.03903	0.08754	0.000841	0.0009214
Thai statue	2332	0.03413	0.04346	0.06324	0.000234	0.0002114
Dragon	51341	0.07342	0.08432	0.04235	0.000148	0.0002245

TABLE 3. Comparison of Entropy analysis used for 3D point fog and 3D mesh fog data.

Input data	Entropy				
	Pham's	Marc's	Liang's	Proposed 3D Point Data	Proposed 3D Mesh Data
Bunny	7.54	7.65	7.44	7.92	7.904
Happy Budda	7.65	7.41	7.72	7.94	7.93
Dragon	7.81	7.72	7.79	7.91	7.90
Armadillo	7.77	7.69	7.73	7.97	7.95
Thai statue	7.82	7.70	7.75	7.94	7.92
Average	**7.718**	**7.634**	**7.686**	**7.936**	**7.920**

determines how difficult it is to retrieve the original mesh data without using the secret key. Below is its mathematical equation.

$$\mathbf{Z(r)} = \sum_{\mathbf{c=0}}^{\mathbf{2^n-1}} \mathbf{p\,(r_c)\log\frac{1}{p\,(r_c)}} \tag{4}$$

In this equation, $Z(r)$ is the information entropy of image r. p corresponds to the probability, and n refers to the total number of pixels in a given image r. For example, an image with 256 grayscale values will have a maximum value of 8 for this metric. In this case, an ideal case of $Z\,(r) = \log_2(255) \approx 8$. The higher the value of entropy, the higher the uncertainty and hence better the level of security against statistical attack. Table 3 shows the entropy analysis of the proposed techniques and compares the proposed scheme with existing techniques.

Based on the evidence of results in Table 3, it is clear that the entropy values of the proposed algorithms provide a randomness effect in the encryption. Even the average values of the entropy analysis for the five chosen images are also plausible. This indicates that the proposed algorithm is hard for the intruder to break against statistical attacks.

D. ASYMMETRY COEFFICIENT

The coefficient of skewness or asymmetry coefficient are terms used to describe the percentage of association between two 3D fog points [37]. It is explained using the following equation.

$$\mathbf{S} = \frac{\mathbf{(Q3 - 2Q2 + Q1)}}{\mathbf{(Q3 - Q1)}} \tag{5}$$

In these circumstances, S is the skewness, Q is the quartile, which designates the distribution of values. Table 4 shows the Asymmetry Skewness distribution of proposed Chaotic Behavior maps with existing Techniques.

TABLE 4. Comparison of the proposed Chaotic Behavior maps with existing Techniques.

Input data	RV	RTM	RRM	Proposed 3D point	Proposed 3D fog Mesh
Bunny	0.2935	0.2756	0.2759	0.36777	0.33172
Happy Budda	0.2756	0.2456	0.1895	0.36988	0.35673
Thai statue	0.2849	0.2415	0.2746	0.36888	0.37354
Armadillo	0.2844	0.2544	0.2345	0.3775	0.36732
Dragon	0.2655	0.2155	0.1457	0.3701	0.36352

The skewness results indicate that the proposed technique is above the axis of symmetry and parallel to the line of equality, with the skewness $S = 0.36$ in the case of 3D point and $S = 0.37$ in the case of 3D mesh fog data, respectively. As a result, this makes it difficult for intruders to employ various attacks to obtain fog data from the storage.

E. DIFFERENTIAL ATTACK

The attackers can obtain the secret key in a variety of ways. One of them is differential attack. This attack's mechanics are as follows. The attacker has two copies of the same image with only minor differences. In most cases, only a one-bit change is required between these two copies. The corresponding cipher images are then obtained by subjecting these two images to the corresponding encryption algorithm. Furthermore, a potential relationship between these two images is discovered, which has enormous implications for the discovery of the secret key. The cipher's resistance to differential attack is assessed using the evaluation metrics Unified Average Changing Intensity (UACI) and Number of Pixels Change Rate (NPCR). Their mathematical formulas are described as follows.

$$\mathrm{NPCR} = \frac{\sum_{\mathrm{e,k}} \mathrm{D(e,k)}}{\mathrm{G \times T}} \times 100\% \tag{6}$$

here G and T represent the width and height of the image, respectively. $D(e, k)$ can be defined by:

$$D\,(e,k) = \begin{cases} 1, if S(e,k) \neq S^{'}(e,k) \\ 0, if S\,(e,k) = S^{'}(e,k) \end{cases} \tag{7}$$

$$UACI = \frac{1}{G \times T}\left[\sum_{e,k} \frac{\left|S\,(e,k) - S^{'}(e,k)\right|}{255}\right] \times 100 \tag{8}$$

TABLE 5. Proposed encryption algorithm Results (NPCR and UACI) for the chosen images.

Input data	NPCR		UACI	
	Proposed 3D point fog data	Proposed 3D Mesh fog	Proposed 3D point fog data	Proposed 3D Mesh fog
Bunny	99.60512	99.6298	33.4292	33.06
Happy Budda	99.69142	99.6168	33.6303	33.62
Thai statue	99.54478	99.5912	33.4749	33.52
Armadillo	99.67112	99.6283	33.4212	33.55
Average	99.62811	99.6165	33.4889	33.4375

TABLE 6. Comparison of security metrics NPCR and UACI with existing schemes.

Algorithm	NPCR (%)	UACI (%)
Proposed 3D point fog data	99.62811	33.4889
Proposed 3D Mesh fog	99.6165	33.4375
Ref. [38]	99.6123	33.4178
Ref. [39]	99.6067	33.5000
Ref. [40]	99.6302	33.4277
Ref. [41]	99.5956	33.4588

here S and S' are, respectively, the ciphered images before and after one pixel of the plain image is changed. Table 5 shows the obtained values of NPCR and UACI for the proposed encryption scheme for the chosen input data. Table 6 draws the comparison of NPCR and UACI metrics for the proposed scheme with the existing schemes [38], [39], [40], [41].

From the results shown in Table 6, it is clear that the NPCR results of the proposed algorithm using 3D point fog data outperform the studies specified in [38], [39], and [41], and the algorithm using 3D mesh fog data outperforms the study specified in [38] and [41]. The results of the UACI of the proposed scheme using 3D point fog data are better than those [38], [40], [41], and the algorithm using 3D mesh fog data produces better results compared to the study specified in [38] and [40]. This result indicates that a minor change in the original data makes a maximum difference in the encrypted data. This feature leads to diffusion property, indicating immunity to cipher text-only attacks.

F. STATISTICAL RANDOMNESS ANALYSIS

Encrypted images in cryptographic applications must be immune to statistical attacks. As a result, the NIST statistical randomness test suite (National Institute of Standards and Technology) is used to evaluate the randomness of the resulting encrypted image [42]. To clear or accept the randomness of bit sequences, the test significance level should be greater than 0.01. Table 6 shows the NIST randomness test results for a Dragon greyscale image of size 512×512.

Tabulation results presented in Table 7 show that the proposed method cleared (✓) the randomness test under different tests carried under the NIST test suite.

TABLE 7. NIST encryption test results of Proposed 3d point fog data and 3d Mesh data.

Test name	Proposed 3D Point Data	Proposed 3D Mesh Data	Result
Frequency	0.147855	0.658924	✓
Block Frequency	0.539174	0.824597	✓
Approximate Entropy	0.410259	0.312451	✓
Random Excursions	0.622801	0.697458	✓
Random Excursions Variant	0.802513	0.598746	✓
Linear Complexity	0.314837	0.201478	✓

VI. CONCLUSION

The paper presented a novel method for encrypting 3D point fog and 3D mesh fog data. For encryption, the proposed method uses the sequences produced by chaotic behavior. The proposed chaos was demonstrated using bifurcation analysis, Lyapunov type, and approximation entropy. Through quantitative analysis, it has been shown that the proposed map has higher LE and AE values than other maps, demonstrating better chaotic behavior than other existing maps. Additionally, regarding security testing, the proposed multilevel encryption scheme conveyed outstanding results.

A variety of analyses, including secret key sensitivity analysis, encryption speed analysis, entropy analysis statistical randomness analysis, were performed to demonstrate the security and validity of the proposed algorithm. Results of the differential attack show that proposed techniques lead to diffusion property, indicating immunity to statistical attack. The result of the asymmetry coefficient shows that the proposed technique is above the axis of symmetry and parallel to the line of equality, with the skewness $\mathbf{S = 0.36}$ in the case of 3D point and $\mathbf{S = 0.37}$ in the case of 3D mesh fog data, respectively. This property makes it difficult for intruders to employ various attacks to obtain fog data from the storage.

Conflict of Interest: None of the authors have a conflict of interest to disclose

REFERENCES

[1] X. Xu, C. Liu, and Y. Zheng, "3D tooth segmentation and labeling using deep convolutional neural networks," *IEEE Trans. Vis. Comput. Graphics*, vol. 25, no. 7, pp. 2336–2348, Jul. 2019, doi: 10.1109/TVCG.2018.2839685.

[2] D. Xiao, M. Li, and H. Zheng, "Smart privacy protection for big video data storage based on hierarchical edge computing," *Sensors*, vol. 20, no. 5, p. 1517, Mar. 2020.

[3] K. R. Raghunandan, A. Ganesh, S. Surendra, and K. Bhavya, "Key generation using generalized Pell's equation in public key cryptography based on the prime fake modulus principle to image encryption and its security analysis," *Cybern. Inf. Technol.*, vol. 20, no. 3, pp. 86–101, Sep. 2020, doi: 10.2478/cait-2020-0030.

[4] K. Kumar, K. R. Ramkumar, and A. Kaur, "A design implementation and comparative analysis of advanced encryption standard (AES) algorithm on FPGA," in *Proc. 8th Int. Conf. Rel., Infocom Technol. Optim.*, Jun. 2020, pp. 182–185, doi: 10.1109/ICRITO48877.2020.9198033.

[5] O. Reyad, H. M. Mansour, M. Heshmat, and E. A. Zanaty, "Key-based enhancement of data encryption standard for text security," in *Proc. Nat. Comput. Colleges Conf. (NCCC)*, Mar. 2021, pp. 1–6, doi: 10.1109/NCCC49330.2021.9428818.

[6] T. Nie and T. Zhang, "A study of Desandblowfish encryption algorithm," in *Proc. IEEE Region Conf. (TENCON)*, Nov. 2009, pp. 1–4, doi: 10.1109/TENCON.2009.5396115.

[7] H. Dibas and K. E. Sabri, "A comprehensive performance empirical study of the symmetric algorithms: AES, 3DES, blowfish and twofish," in *Proc. Int. Conf. Inf. Technol. (ICIT)*, Jul. 2021, pp. 344–349, doi: 10.1109/ICIT52682.2021.9491644.

[8] J. R. Shaikh, M. Nenova, G. Iliev, and Z. Valkova-Jarvis, "Analysis of standard elliptic curves for the implementation of elliptic curve cryptography in resource-constrained E-commerce applications," in *Proc. IEEE Int. Conf. Microw., Antennas, Commun. Electron. Syst. (COMCAS)*, Nov. 2017, pp. 1–4, doi: 10.1109/COMCAS.2017.8244805.

[9] R. Kasodhan and N. Gupta, "A new approach of digital signature verification based on BioGamal algorithm," in *Proc. 3rd Int. Conf. Comput. Methodologies Commun. (ICCMC)*, Mar. 2019, pp. 10–15, doi: 10.1109/ICCMC.2019.8819710.

[10] F. Sun, S. He, X. Zhang, J. Zhang, Q. Li, and Y. He, "A fully authenticated Diffie–Hellman protocol and its application in WSNs," *IEEE Trans. Inf. Forensics Security*, vol. 17, pp. 1986–1999, 2022, doi: 10.1109/TIFS.2022.3173536.

[11] S. Khan, S. Parkinson, and Y. Qin, "Fog computing security: A review of current applications and security solutions," *J. Cloud Comput.*, vol. 6, no. 1, pp. 1–22, Dec. 2017, doi: 10.1186/s13677-017-0090-3.

[12] A. Alrawais, A. Alhothaily, C. Hu, X. Xing, and X. Cheng, "An attribute-based encryption scheme to secure fog communications," *IEEE Access*, vol. 5, pp. 9131–9138, 2017.

[13] Z. Hua, K. Zhang, Y. Li, and Y. Zhou, "Visually secure image encryption using adaptive-thresholding sparsification and parallel compressive sensing," *Signal Process.*, vol. 183, Jun. 2021, Art. no. 107998, doi: 10.1016/j.sigpro.2021.107998.

[14] K. Vohra and M. Dave, "Securing fog and cloud communication using attribute based access control and re-encryption," in *Proc. 2nd Int. Conf. Inventive Commun. Comput. Technol. (ICICCT)*, 2018, pp. 307–312, doi: 10.1109/ICICCT.2018.8473045.

[15] M. A. M. Ahsan, I. Ali, M. Imran, M. Y. I. B. Idris, S. Khan, and A. Khan, "A fog-centric secure cloud storage scheme," *IEEE Trans. Sustain. Comput.*, vol. 7, no. 2, pp. 250–262, Apr. 2022, doi: 10.1109/TSUSC.2019.2914954.

[16] L. N. Vijouyeh, M. Sabaei, J. Santos, T. Wauters, B. Volckaert, and F. De Turck, "Efficient application deployment in fog-enabled infrastructures," in *Proc. 16th Int. Conf. Netw. Service Manag. (CNSM)*, Nov. 2020, pp. 1–9, doi: 10.23919/CNSM50824.2020.9269052.

[17] A. S. Arumugam and D. K. Jothi, "Image encryption algorithm based on improved 3D chaotic cat map," in *Proc. IEEE Int. Conf. Comput. Intell. Comput. Res.*, Dec. 2010, pp. 1–4, doi: 10.1109/ICCIC.2010.5705910.

[18] C. X. Zhang, "Hyper-chaotic cat map and its application in image processing," *Appl. Mech. Mater.*, vols. 278–280, pp. 1392–1396, Jan. 2013, doi: 10.4028/www.scientific.net/amm.278-280.1392.

[19] C. Jia, T. Yang, C. Wang, B. Fan, and F. He, "Encryption of 3D point cloud using chaotic cat mapping," *3D Res.*, vol. 10, no. 1, pp. 1–13, Mar. 2019, doi: 10.1007/S13319-018-0212-9.

[20] A. A. Pacha, N. Hadj-Said, B. Belmeki, and A. Belgoraf, "Chaotic behavior for the secrete key of cryptographic system," *Chaos, Solitons Fractals*, vol. 23, no. 5, pp. 1549–1552, Mar. 2005, doi: 10.1016/j.chaos.2004.05.015.

[21] F. Meng, S. Shi, B. Zhang, M. Bai, and N. Lin, "Analysis for global characteristics of Lyapunov exponents in vehicle plane motion system," *Sci. Rep.*, vol. 12, no. 1, pp. 1–14, Jun. 2022, doi: 10.1038/s41598-022-13411-x.

[22] A. Wolf, J. Swift, H. L. Swinney, and J. A. Vastano, "Determining Lyapunov exponents from a time series," *Phys. D, Nonlinear Phenomena*, vol. 16, pp. 285–317, Jul. 1985, doi: 10.1016/0167-2789(85)90011-9.

[23] Z. Hua, Y. Chen, H. Bao, and Y. Zhou, "Two-dimensional parametric polynomial chaotic system," *IEEE Trans. Syst., Man, Cybern. Syst.*, vol. 52, no. 7, pp. 4402–4414, Jul. 2022, doi: 10.1109/TSMC.2021.3096967.

[24] C. Shen, S. Yu, J. Lü, and G. Chen, "Constructing hyperchaotic systems at will," *Int. J. Circuit Theory Appl.*, vol. 43, no. 12, pp. 2039–2056, 2015.

[25] Y. Chen and Q. Yang, "A new lorenz-type hyperchaotic system with a curve of equilibria," *Math. Comput. Simul.*, vol. 112, pp. 40–55, Jun. 2015.

[26] W. Liu, K. Sun, and S. He, "SF-SIMM high-dimensional hyperchaotic map and its performance analysis," *Nonlinear Dyn.*, vol. 89, no. 4, pp. 2521–2532, 2017.

[27] Z. Hua, Y. Zhang, H. Bao, H. Huang, and Y. Zhou, "N-dimensional polynomial chaotic system with applications," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 69, no. 2, pp. 784–797, Feb. 2022, doi: 10.1109/TCSI.2021.3117865.

[28] H. Zhang and S.-S. He, "Analysis and comparison of permutation entropy, approximate entropy and sample entropy," in *Proc. Int. Symp. Comput., Consum. Control (ISC)*, Dec. 2018, pp. 209–212, doi: 10.1109/IS3C.2018.00060.

[29] M.-L. Lam, B. Chen, K.-Y. Lam, and Y. Huang, "3D fog display using parallel linear motion platforms," in *Proc. Int. Conf. Virtual Syst. Multimedia (VSMM)*, Dec. 2014, pp. 234–237, doi: 10.1109/VSMM.2014.7136689.

[30] M. Malipatil and D. C. Shubhangi, "An efficient 3D watermarking algorithm for 3D mesh models," in *Proc. 4th Int. Conf. I-SMAC*, Oct. 2020, pp. 1–5, doi: 10.1109/I-SMAC49090.2020.9243381.

[31] R. Jiang, H. Zhou, W. Zhang, and N. Yu, "Reversible data hiding in encrypted three-dimensional mesh models," *IEEE Trans. Multimedia*, vol. 20, no. 1, pp. 55–67, Jan. 2018, doi: 10.1109/TMM.2017.2723244.

[32] Z. Wu, X. Jin, C. Song, C. Zhang, and X. Li, "Random reversible matrix based point fog encryption," *J. Syst. Simul.*, vol. 28, no. 10, pp. 2455–2459, 2016.

[33] K. R. Raghunandhan, S. Shetty, G. Aithal, and N. Rakshith, "Enhanced RSA algorithm using fake modulus and fake public key exponent," in *Proc. Int. Conf. Electr., Electron., Commun., Comput., Optim. Techn. (ICEECCOT)*, Dec. 2018, pp. 755–759, doi: 10.1109/ICEECCOT43722.2018.9001351.

[34] Y. Liang, F. He, and H. Li, "An asymmetric and optimized encryption method to protect the confidentiality of 3D mesh model," *Adv. Eng. Informat.*, vol. 42, Oct. 2019, Art. no. 100963.

[35] A. Q. Md, D. Agrawal, M. Mehta, A. K. Sivaraman, and K. F. Tee, "Time optimization of unmanned aerial vehicles using an augmented path," *Future Internet*, vol. 13, no. 12, p. 308, 2021.

[36] M. Eluard, Y. Maetz, G. Doerr, R. Technicolor, and D. France, "Geometry-preserving encryption for 3D meshes," in *Proc. Compress. Et Represent. Des Signaux Audiovisuels (CORESA)*, Nov. 2013, pp. 7–12.

[37] R. Raghunandan, A. Ganesh, S. Surendra, and K. Bhavya, "Image encryption scheme in public key cryptography based on cubic pells quadratic case," *Indonesian J. Electr. Eng. Comput. Sci.*, vol. 20, no. 1, p. 385, Oct. 2020, doi: 10.11591/ijeecs.v20.i1.pp385-394.

[38] Z. Guo and P. Sun, "Improved reverse zigzag transform and DNA diffusion chaotic image encryption method," *Multimedia Tools Appl.*, vol. 81, no. 8, pp. 11301–11323, Mar. 2022.

[39] X. Chai, X. Fu, Z. Gan, Y. Lu, and Y. Chen, "A color image cryptosystem based on dynamic DNA encryption and chaos," *Signal Process.*, vol. 155, pp. 44–62, Feb. 2019.

[40] I. Nadeem, M. Hanif, S. Abbas, M. A. Khan, and Z. U. Rehman, "Dynamic 3D scrambled image based RGB image encryption scheme using hyper-chaotic system and DNA encoding," *J. Inf. Secur. Appl.*, vol. 58, pp. 1–12, May 2021.

[41] W. Xingyuan, Y. Wang, X. Zhu, and C. Luo, "A novel chaotic algorithm for image encryption utilizing one-time pad based on pixel level and DNA level," *Opt. Lasers Eng.*, vol. 125, pp. 1–10, Feb. 2020.

[42] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, and E. Barker, "Test suite for random and pseudorandom number generators for cryptographic applications," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep. ADA393366, May 2010.

K. R. RAGHUNANDAN received the Ph.D. degree in public key cryptography from Visvesaraya Technological University. He is currently working as an Assistant Professor with the Department of Computer Science and Engineering, NMAM Institute of Technology, Affiliated to Nitte University, Nitte. He has published around 12 research articles in different international journals. His research interests include the cryptography, block chain technology, and cyber security and forensics. In addition, he is a reviewer for leading journals in the area of networking and cryptography.

RADHAKRISHNA DODMANE received the Ph.D. degree in cryptography from Visvesaraya Technological University. He is currently working as an Associate Professor with the Department of Computer Science and Engineering, NMAM Institute of Technology, Nitte Affiliated to Nitte University. He has published more than 14 research papers in different international journals and conferences. His research interests include cryptography, block chain technology, and cyber security and forensics.

K. BHAVYA received the B.Sc. degree in computers science and the M.Sc. degrees in mathematics from Mangalore University, India. She is currently pursuing the Ph.D. degree in graph theory with Nitte University, India. She is currently working as an Assistant Professor with the Department of Mathematics, NMAM Institute of Technology, Nitte Affiliated to Nitte University. Her research interests include number theory, graph theory, and cryptography.

N. S. KRISHNARAJ RAO is currently working as an Assistant Professor with the Department of Information Science and Engineering, NMAM Institute of Technology, Nitte Affiliated to Nitte University. His research interests include number theory, graph theory, and cryptography.

ADITYA KUMAR SAHU is currently working with the Amrita School of Computing, Amaravati Campus, Amrita Vishwa Vidyapeetham, Andhra Pradesh, India. His area of research interests include chaotic-map based tamper detection and localization, multimedia watermarking, data hiding, fog and edge computing, and machine learning techniques for optimal data hiding. He is serving as an Associate Editor for the *Journal of Electronic Imaging* (SPIE).