

3D Polygon Mesh Encryption Based on 3D Lorenz Chaotic Map

<https://doi.org/10.3991/ijim.v15i15.24177>

Nashwan Alsalam Ali¹(✉), Abdul Monem S. Rahma², Shaimaa H. Shaker²

¹University of Baghdad, Baghdad, Iraq

²University of Technology, Baghdad, Iraq

nashwan_alsalam60@coeduw.uobaghdad.edu.iq

Abstract—The multimedia application developments in recent years lead to the widespread of 3D model applications. It becomes more popular in various fields as well as exchanging it over the internet. The security of the 3D models is a very important issue now a day, so the scheme for encrypting the 3D model will be proposed in this work. In this proposed scheme, the 3D polygon mesh model will be protected through the encrypting process based on a 3D Lorenz Chaotic map where the vertices value of the 3D polygon mesh model will be modified using 3D keys generated by 3D Lorenz Chaotic Map, which has excellent property and provides a good diffusion. The proposed scheme was implemented on various 3D models, which have a different number of vertices and faces. The experimental results show that the proposed scheme has good encryption results, which were noted through completely deforming and changing the whole shape of the 3D models. The Hausdorff Distance (HD) and histogram metrics are adopted to calculate the matching degree between the original and extracted model. The results show that the original and extracted model are identical through the values of HD, where they are approximately zero, and the histogram visually is identical.

Keywords—3D polygon mesh model, vertices, 3D Lorenz chaotic map

1 Introduction

Recently, information technology security became a very important issue where the transmission of digital data through an unsecured channel such as the internet will lead to security threats and attacks on data. Various encryption algorithm types are proposed to convert data into unrecognized forms and prevent unauthorized user access [1–5]. The 3D model applications now days are developed and become more popular such as virtual reality, Computer-Aided Design (CAD), 3D printing, and digital visualization, so providing security for 3D model becomes an important matter and must provide a high level of confidentiality, integrity, and protection against unauthorized access for data, so the problem of the thread must be solved [6, 7]. There are many proposed encryption schemes some of them have been adopted and standardized in the world; however, they are not suitable for a 3D model such as Advanced Encryption Standard

(AES) and Data Encryption Standard (DES) because the problem of 3D model encryption due to the application requirements and the data structure such as format compliance, content usability, complexity, security level and real-time performance [8], to overcome these problems, various encryption methods based on chaotic cryptography have been implemented. Chaotic systems are attracted and adopted in cryptosystems by the researcher because they have excellent properties such as sensitivity to initial condition and control parameter, ergodicity, randomness, deterministic, and periodicity [9–11]. In this paper, the encryption algorithm of the 3D model will be introduced based on the key generated from the chaotic map.

2 Related work

Benson Raj et al. in 2020 [1] proposed an encryption system that uses a 3D Arnold cat map to encrypt the 3D mesh model. The 3D mesh model encrypted using substitution and shuffling based on Arnold cat map where the vertices and faces are substituted and shuffled separately in the proposed cryptosystem. Then, they are composed together to constitute the final encrypted model. The 3D Arnold map generated confusion and diffusion that would be done through each round in which a good substitution and shuffling are performed. More security will be achieved in the 3D mesh model through chaotic function by using substitution and shuffling. The results of the encryption system show that the 3D models were resisted various attacks.

Xingyuan Wang et al. in 2019 [7] proposed the scheme in which the 3D object is converted into 2D objects as the same as of image format to perform encryption on it. The encryption scheme is performed via two phases: the confusion phase and diffusion phase. During the confusion phase, the authors have introduced random points. During the diffusion phase, the authors divided the floating-point data into two parts: the integer and decimal parts. The integer part was encrypted using XOR operation, and the decimal part was scrambled only. The security analysis has shown that the scheme is highly secured and resistant to common attacks.

Chaochuan Jia et al. in 2019 [12], the authors proposed two schemes for encrypting the 3D point cloud using a chaotic cat map. In the first scheme, permutation using 2D Cat Map(P2DCM), which has time complexity is $O(3N^2)$, the authors used a 2D cat map to perform permutation for each coordinate (x, y, z) in every point cloud. In the second scheme, Random Transformation Matrix using 3D Cat Map (RTM3DCM), which has a time complexity is $O(6M)$, the authors used a 3D cat map to generate a random transformation matrix that was used to transform a point in 3D space to a different position.

Ji Xu, Chen Zhao, and Jun Mon in 2020 [13] proposed a novel 3D image encryption algorithm. They proposed an algorithm based on a new discrete chaotic maps system. Novel chaotic system characteristics are analyzed by Lyapunov exponent, phase diagram, and bifurcation diagram. The encryption scheme is destined for 3D image file through the analysis results firstly: the initial condition of the discrete system is changed using the SHA-256 hash function, which produced a hash value that used to change the initial condition of the system, second: used the chaotic sequences to scramble and spread 3D image file coordinate value using diffusion algorithm of Arnold

matrix and DNA. The proposed encryption algorithm for 3D image files has higher security to maintain the resistance for conventional attacks.

Najlaa Hamza et al. in 2019 [14], the authors proposed a method for encrypting the 3D object model using the Transformation, Substitution, Folding, and Shifting (TSFS) algorithm. The encryption method takes the vertices of the 3D model and inputs them to the TSFS algorithm. The four stages in TSFS based on three keys wherein transformation step, the position of the vertex will be changed, in substitution step, each component of the data matrix will be altered with another element, in folding step, the elements of the matrix are folded in a diagonal, horizontal and vertical manner and in shifting step which is the last step of TSFS it uses of element 16 in a set of numeric digits for replacing the code with another one. The experimental results show that the proposed method succeeded in encryption the 3D model where the system has achieved effective and strong security.

3 Chaotic system and cryptography

There are many requirements for protecting data, the most important requirements including confidentiality and security. The proportionate mixture of chaotic mathematical theory and the science of cryptography is called cryptography. The chaotic system consists of the dynamic equation that varies with time. When the dynamic system satisfies the three conditions below, it will be considered as chaotic.

- a) Sensitive to initial conditions.
- b) Topological mixing.
- c) The density of periodic orbits.

Cryptosystem and chaotic systems have a relationship between them; however, the main variation between chaotic and cryptographic systems is that the chaos is valid in an infinite domain while cryptography operates on a finite domain [10, 15]. The relationship between cryptography and chaotic systems makes cryptography-based chaos a normal candidate for cryptography and secure communication. Similar properties have been shared between chaotic systems and cryptographic such as control parameters, sensitivity to the initial conditions, unstable periodic orbits with long periods, and random behavior. Due to the random behavior, the system output seems random in the attacker views, whereas it appears as defied in the receiver views, and decryption is possible [16–18]. In Table 1, the comparison between chaotic systems and cryptography will be illustrated.

Table 1. Comparison between chaotic system and cryptography

Chaotic Property	Cryptography Property
Sensitive to initial condition	Diffusion
Ergodicity	Diffusion
Structure complexity	Algorithm complexity
System parameter	Key
Deterministic dynamics	Deterministic pseudo-randomness

4 3D Lorenz chaotic map

The 3D Lorenz is a chaotic map of a three-dimension. It was developed by the scientist Edward Lorenz by a combined differential equation. The Lorenz chaos sequences generated attractors, which is the deck of chaotic solutions for the Lorenz system. The 3D Lorenz chaotic formula is depicted by equations (1), (2), and (3).

$$\frac{dx}{dt} = a(y - x) \tag{1}$$

$$\frac{dy}{dt} = rx - y - xz \tag{2}$$

$$\frac{dz}{dt} = xy - bz \tag{3}$$

The control parameters r and b are the parameters where the system depending on them. When the parameters value $a=10$, $r=28$, and $b=8/3$. The x , y , and z solution curves for these equations circle two equilibrium points and the projections of its phase portrait. The initial values of (x, y, z) are the bases of the 3D Lorenz chaotic trajectory framework, representing the secret key for performing the permutation process [19, 20].

5 The 3D polygon mesh

The 3D model surface is represented by 3D polygon mesh. The polygons are straight-sided shapes that can be triangles when they have three sides or quadrilaterals when having four sides; the typical structure is the 3D triangular mesh. An individual polygon is called a face, and when connecting many faces, they create a network of faces called polygon mesh. The representation of the polygon mesh can be represented as $M = \{G, C\}$, where G represents geometry information and C represents topological information. The geometry information is denoted as $G = \{V, E, F\}$, where V is the vertices of the mesh, E is the straight lines that connect vertices, and F is the facets information. The topological information, including the connectivity data between the geometry elements that specify which vertices belong to each polygon [21–24]. Figure 1 illustrates the triangle and quadrilaterals representation.

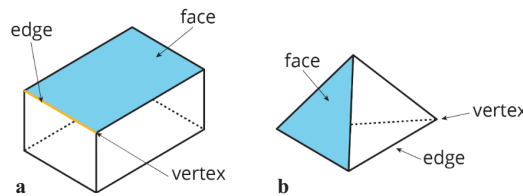


Fig. 1. (a) quadrilaterals representation, (b) triangle representation

6 Proposed method of 3D model encryption

In this section, the main steps of encryption and decryption will be described. The 3D model contains vertices and faces, each vertex composes of (v_x, v_y, v_z) . The encryption process is performed by changing the vertices values. The vertices in the 3D model are listed as an array V .

$$V = \{(v_{x1}, v_{y1}, v_{z1}), (v_{x2}, v_{y2}, v_{z2}), \dots, (v_{xn}, v_{yn}, v_{zn})\}$$

Where n is the number of vertices in the model, Figure 2 shows the girl 3D model and a close view of its triangle mesh.

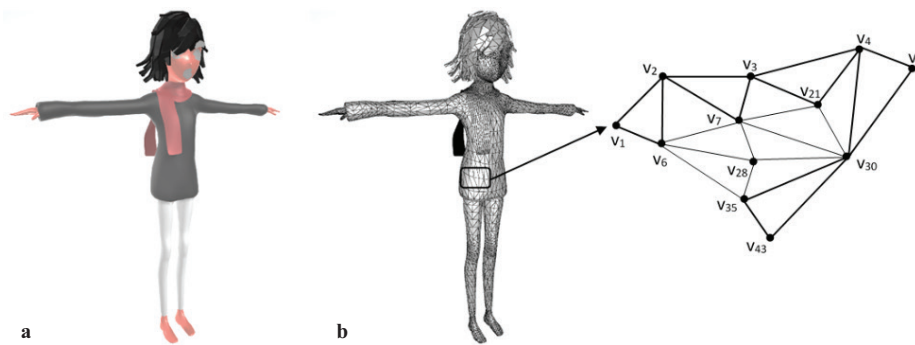


Fig. 2. (a) 3D model of girl, (b) 3D polygon triangle mesh and close view of it

The vertices and faces structures in the ‘.obj’ file are shown in Table 2, where the vertices and the faces are represented by a list of indices to reduce the size needed in memory.

Table 2. Vertices and faces structure representation

Vertices List Information				Faces List Information	
Index of vertex	x-coordinate	y-coordinate	z-coordinate	Index of face	Vertices index in each face
1	V1,x	V1,y	V1,z	1	(2,6,7)
2	V2,x	V2,y	V2,z	2	(6,28,7)
3	V3,x	V3,y	V3,z	3	(7,28,30)
4	V4,x	V4,y	V4,z	4	(7,30,21)
.....	5	(7,21,3)
32	V32,x	V32,y	V32,z
33	V33,x	V33,y	V33,z	12	(35,30,28)
34	V34,x	V34,y	V34,z	13	(35,43,30)
.....

The 3D Lorenz chaotic map is used in the proposed scheme to generate random keys for each vertex in the model, such that

$$K = \{(K_{x_1}, K_{y_1}, K_{z_1}), \dots, (K_{x_n}, K_{y_n}, K_{z_n})\}$$

where the K is a key generating for each vertex in the model.

In the following, the main steps of the encryption process are described:

Input: 3D model in ‘.obj’ format.

Output: 3D encrypted model.

Step1: Read 3D mesh model, store vertices in an array V and faces in an array F.

Step2: For each vertex in the 3D model, do the following.

Step3: Apply 3D Lorenz map to generate three keys for each vertex, key for x, key for y, and key for z, store in K.

Step4: Apply the encryption process using equation 4 to modify the values of vertices.

$$V' (x,y,z) = V(x,y,z)*W + K(x,y,z) \tag{4}$$

Where V' is the encrypted vertex, V is the original vertex in the 3D model, K is the key generated by 3D Lorenz map, W is the weight to preserve the dimensionality, stability, and size, the value is chosen by trial and test, the best value is 0.5.

Step5: End for

Step6: Save the new vertices and faces as a new file.

The block diagram in Figure 3 illustrates the encryption process of vertices in a 3D polygon mesh.

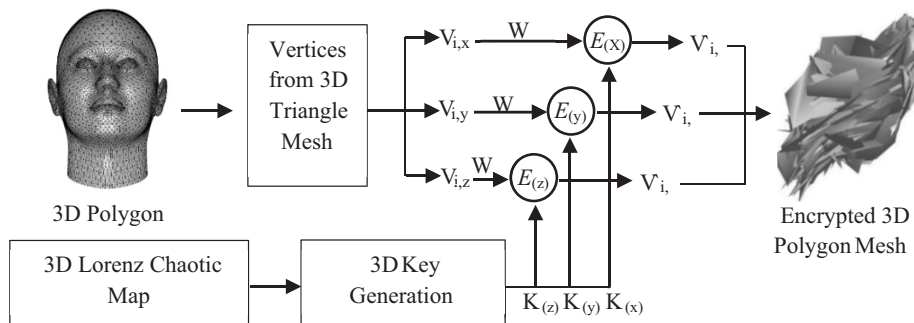


Fig. 3. Block diagram for 3D polygon mesh encryption process

The steps of the decryption process are similar to the encryption process but in reverse order, which is illustrated in Figure 4.

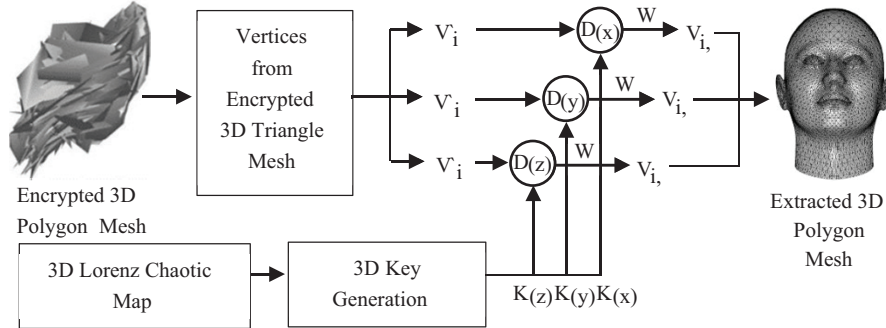


Fig. 4. Block diagram for 3D polygon mesh decryption process

The various types of 3D models may contain a single part of 3D polygon mesh or more than one part, and each part contains a different group of vertices and faces, as shown in Figure 5, which describe the different parts of the teapot 3D model.

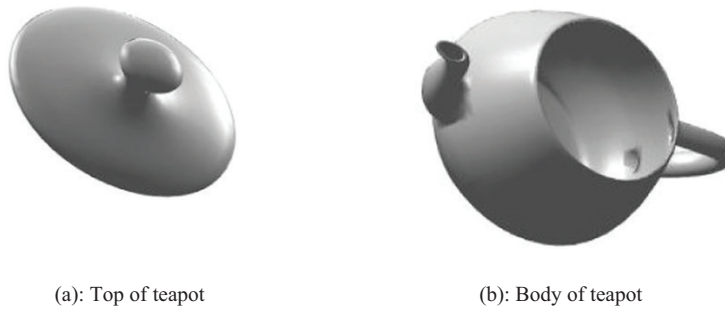

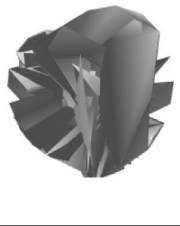

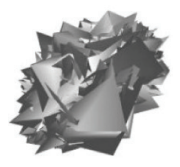

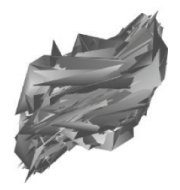

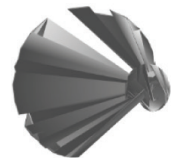




Fig. 5. Teapot 3D model parts, (a) Top of teapot and (b): Body of teapot

7 Simulation results

The efficiency of the proposed encryption algorithm was tested using different 3D models of type '.obj' file format (Girl, Teapot, Face Man, Butterfly, Knife). These models with a different number of vertices and faces. The original model and the encryption for each model are shown in Table 3. As shown in the Table, the encryption time required is based on the number of vertices and faces.

Table 3. Information for the 3D model encryption process

Model Name	No. of Vertices	No. of Faces	Elapsed Time in Sec.	Model Before Encryption	Model After Encryption
Girl	54570	18190	13.969		
Teapot	47112	15704	10.819		
Face man	36522	12174	8.123		
Butterfly	8328	2776	3.512		
Knife	3555	1185	0.976		

The experimental results are shown in Table 3, and the encrypted models are completely different from the original model, where the vertices values are changed.

8 Statistical tests

The statistical tests Hausdorff Distance (HD) and histograms are applied to evaluate the quality of the proposed encryption scheme. Table (4) illustrates the values of HD between the original and encrypted 3D model. The HD is the measurement tool used to measure the dissimilarity between two point sets. HD is used in various domains like pattern matching, 3D comparison, and image processing. The HD between two sets of points is defined as the maximum distance of a set to the nearest point in the other set.

Table 4. The results of Hausdorff

Model Name	Hausdorff After Encryption	Hausdorff After Decryption
Face Man	124.5836	0.000016
Teapot	71.0325	0.000017
Girl	106.2076	0.000016
Butterfly	106.5517	0.000057
Knife	106.5528	0.000015

This distance is used to assess the degree of resemblance between two superimposed objects on one another. The purpose of using the HD in the proposed scheme is to reveal the degree of dissimilarity between the original model (A) and the decrypted model (B).

$$h(A, B) = \max_{a \in A} \left\{ \min_{b \in B} \{d(a, b)\} \right\} \tag{5}$$

Where A and B are the two meshes and d (a, b) is the Euclidean distance between a and b in the 3D space [25, 26]. If the HD nears zero, this means there is no difference between them and vice versa.

Figure 6 shows a complete example for encryption and decryption steps for the teapot 3D model. From Figure 6, the histogram can see for the original and encrypted model, and the difference is clear for eyes; this means the algorithm is resistant to statistical attack and completely identical between the histogram of the original and decryption model.

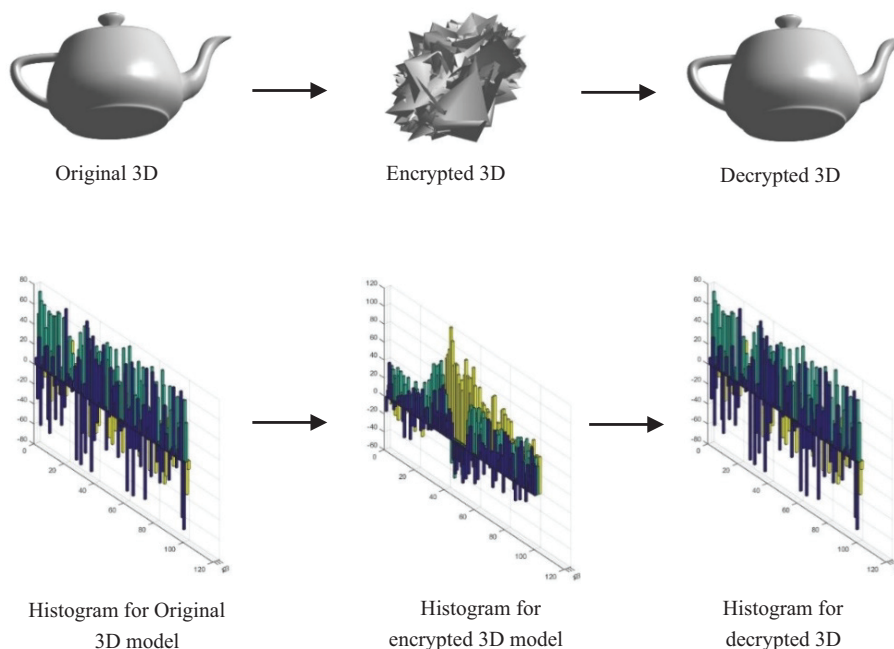


Fig. 6. The complete example of teapot encryption and decryption with histogram

9 Security analysis

Security analysis can be used in encryption system by:

- **Keyspace:** the keyspace must be large enough to resist the various attacks, such as brute-force attacks. The precision of 64-bit double data is 10^{-15} , in addition to initial conditions by 3D Lorenz are (6), as a result, the keyspace size $(10^{-15})^6$.
- **Secret key sensitivity:** Several experiments for secret key sensitivity are done. Any change in the initial condition value will lead to the wrong decryption process and diffused the error almost to all vertices, so unable to extract the original 3D model.

10 Time complexity analysis

The 3D polygon mesh encryption algorithm is implemented by Matlab 2018 on a laptop computer with Core i7 CPU, Ram 16 G DDR4, and graphical card 4G, where the time needs for encryption and decryption are varying according to the number of vertices in a 3D polygon mesh. The larger number of vertices leads to spending more time and vice versa, as described in Table 3.

11 Conclusion

In this paper, the proposed algorithm was encrypting a different testing number of 3D polygon mesh models based on keys generated by 3D Lorenz map, where a different number of the 3D models are used to check the efficiency of the algorithm, firstly the XOR function is applied for the encryption process, but this process shows that the results did not maintain the dimensionality and spatial stability of encrypted results so proposed another mathematical encryption process based on weight factor (w) is adopted. The proposed algorithm completely deforms the 3D mesh model with maintaining the dimensionality and spatial stability achieved through the weight factor (w) value. The results are analyzed based on Hausdorff and histogram, which show that the encrypted 3D model is completely different from the original model, and the extracted model is identical to the original model through HD and histogram metrics, the large key space of the 3D Lorenz map makes the algorithm more resistant to brute-force attacks.

12 References

- [1] B. Raj, L. Jani Anbarasi, M. Narendra, and V. J. Subashini, "A New Transformation of 3D Models Using Chaotic Encryption Based on Arnold Cat Map," in *Lecture Notes on Data Engineering and Communications Technologies*, vol. 29, pp. 322–332, 2019. https://doi.org/10.1007/978-3-030-12839-5_29
- [2] S. M. Kareem and A. M. S. Rahma, "A novel approach for the development of the Twofish algorithm based on multi-level key space," *J. Inf. Secur. Appl.*, vol. 50, p. 102410, 2020. <https://doi.org/10.1016/j.jisa.2019.102410>

- [3] S. M. Kareem and A. M. S. Rahma, "A Modification on Key Stream Generator for RC4 Algorithm," *Eng. Technol. J.*, vol. 38, no. 2B, pp. 54–60, 2020. <https://doi.org/10.30684/etj.v38i2B.404>
- [4] I. A. Aljazaery, H. T. S. Alrikabi, and M. R. Aziz, "Combination of hiding and encryption for data security," *Int. J. Interact. Mob. Technol.*, vol. 14, no. 9, pp. 34–47, 2020. <https://doi.org/10.3991/ijim.v14i09.14173>
- [5] H. A. Naman, N. A. Hussien, M. L. Al-dabag, and H. T. S. Alrikabi, "Encryption System for Hiding Information Based on Internet of Things," *Int. J. Interact. Mob. Technol.*, vol. 15, no. 2, pp. 172–183, 2021. <https://doi.org/10.3991/ijim.v15i02.19869>
- [6] X. Jin et al., "Multi-Level Chaotic Maps for 3D Textured Model Encryption," in 2nd EAI International Conference on Robotic Sensor Networks, pp. 107–117, 2020. https://doi.org/10.1007/978-3-030-17763-8_10
- [7] X. Wang, M. Xu, and Y. Li, "Fast encryption scheme for 3D models based on chaos system," *Multimed. Tools Appl.*, vol. 78, no. 23, pp. 33865–33884, 2019. <https://doi.org/10.1007/s11042-019-08171-2>
- [8] A. Jolfaei, X. W. Wu, and V. Muthukkumarasamy, "A secure lightweight texture encryption scheme," in *Lecture Notes in Computer Science*, vol. 9555, pp. 344–356, 2016. https://doi.org/10.1007/978-3-319-30285-0_28
- [9] H. Najm, H. K. Hoomod, and R. Hassan, "A New WoT Cryptography Algorithm Based on GOST and Novel 5d Chaotic System," *Int. J. Interact. Mob. Technol.*, vol. 15, no. 2, pp. 184–199, 2021. <https://doi.org/10.3991/ijim.v15i02.19961>
- [10] J. G. Sekar and C. Arun, "Comparative performance analysis of chaos based image encryption techniques," *J. Crit. Rev.*, vol. 7, no. 9, pp. 1138–1143, 2020. <https://doi.org/10.31838/jcr.07.09.209>
- [11] L. Xu, Z. Li, J. Li, and W. Hua, "A novel bit-level image encryption algorithm based on chaotic maps," *Opt. Lasers Eng.*, vol. 78, pp. 17–25, 2016. <https://doi.org/10.1016/j.optlaseng.2015.09.007>
- [12] 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, 2019. <https://doi.org/10.1007/s13319-018-0212-9>
- [13] J. Xu, C. Zhao, and J. Mou, "A 3D Image Encryption Algorithm Based on the Chaotic System and the Image Segmentation," *IEEE Access*, vol. 8, pp. 145995–146005, 2020. <https://doi.org/10.1109/ACCESS.2020.3005925>
- [14] N. A. Hamza, S. H. Jafeer, and A. E. Ali, "Encrypt 3D Model Using Transposition, Substitution, Folding, and Shifting (TSFS)," in *SCCS 2nd Scientific Conference of Computer Sciences*, pp. 126–131, 2019. <https://doi.org/10.1109/SCCS.2019.8852600>
- [15] H. A. Abdullah and H. N. Abdullah, "Secure Image Transmission Based on a Proposed Chaotic Maps," in *Multimedia Security Using Chaotic Maps : Principles and Methodologies*, K. M. Hosny, Ed. Springer Nature, pp. 81–109, 2020. https://doi.org/10.1007/978-3-030-38700-6_4
- [16] P. R. Sankpal and P. A. Vijaya, "Image encryption using chaotic maps: A survey," in *Proceedings - 2014 5th International Conference on Signal and Image Processing, ICSIP*, pp. 102–107, 2014. <https://doi.org/10.1109/ICSIP.2014.80>
- [17] Y. H. Ail and Z. A. H. Alobaidy, "Images Encryption Using Chaos and Random Generation," *Eng. Technol. J.*, vol. 34, no. 1 Part (B) Scientific, pp. 172–179, 2016.
- [18] A. S. Hamad and A. K. Farhan, "Image Encryption Algorithm Based on Substitution Principle and Shuffling Scheme," *Eng. Technol. J.*, vol. 38, no. 3B, pp. 98–103, 2020. <https://doi.org/10.30684/etj.v38i3B.433>
- [19] F. Masood, J. Ahmad, S. A. Shah, S. S. Jamal, and I. Hussain, "A novel hybrid secure image encryption based on Julia set of fractals and 3D Lorenz chaotic map," *Entropy*, vol. 22, no. 3, 2020. <https://doi.org/10.3390/e22030274>

- [20] P. Rakheja, R. Vig, and P. Singh, “Double image encryption using 3D Lorenz chaotic system, 2D non-separable linear canonical transform and QR decomposition,” *Opt. Quantum Electron.*, vol. 52, no. 2, 2020. <https://doi.org/10.1007/s11082-020-2219-8>
- [21] J. Alireza, “Robust Encryption Schemes for 3D Content Protection,” Thesis (Ph.D. Doctorate) Griffith University, 2016.
- [22] R. Jiang, H. Zhou, W. Zhang, and N. Yu, “Reversible data hiding in encrypted three-dimensional mesh models,” *IEEE Trans. Multimed.*, vol. 20, no. 1, pp. 55–67, 2018. <https://doi.org/10.1109/TMM.2017.2723244>
- [23] S. Borah and B. Borah, “Three-Dimensional (3D) Polygon Mesh Authentication Using Sequential Bit Substitution Strategy,” in *Advances in Intelligent Systems and Computing*, vol. 990, pp. 617–627, 2020. https://doi.org/10.1007/978-981-13-8676-3_52
- [24] Z. N. Al-Qudsy, S. H. Shaker, and N. S. Abdulrazzque, “Robust Blind Digital 3D Model Watermarking Algorithm Using Mean Curvature,” in *Third International Conference, New Trends in Information and Communications Technology Applications*, pp. 110–125, 2018. https://doi.org/10.1007/978-3-030-01653-1_7
- [25] A. A. Taha and A. Hanbury, “An Efficient Algorithm for Calculating the Exact Hausdorff Distance,” *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 37, no. 11, pp. 2153–2163, 2015. <https://doi.org/10.1109/TPAMI.2015.2408351>
- [26] D. Karimi and S. E. Salcudean, “Reducing the Hausdorff Distance in Medical Image Segmentation with Convolutional Neural Networks,” *IEEE Trans. Med. Imaging*, vol. 39, no. 2, pp. 499–513, 2020. <https://doi.org/10.1109/TMI.2019.2930068>

13 Authors

Nashwan Alsalam Ali is presently one of the college faculty of education for women, computer science department, University of Baghdad, Iraq. He received his B.Sc. degree in Computer Science in 2003 from Technology University in Baghdad, Iraq, his M.Sc. degree in Computer Science focusing on Multimedia Security from Iraqi Commission for Computers and Informatics from Baghdad, Iraq. He is currently a Ph.D. student in Computer Science, Technology University in Baghdad, Iraq. Contact: +9647706572872. E-mail: nashwan_alsalam60@coeduw.uobaghdad.edu.iq

Prof. Dr. Abdul Monem S. Rahma received his B.Sc. degree in Mathematics, Al- Mustansiriya University, Baghdad, Iraq, in 1977. His M.Sc. in Numerical Analysis, Brunel University, the United Kingdom in 1982. His Ph.D. in Computer Science, Loughborough University, the United Kingdom in 1984. He is presently one of the faculty computer science department, Technology University, Baghdad, Iraq. His research interests focus on Image and Video Processing, Pattern Recognition, and Information security. E-mail: 110003@uotechnology.edu.iq

Assist. Professor Dr. Shaimaa H. Shaker earned her bachelor’s and master’s degree in Computer Science from the Department of Computer Science at the University of Technology-Baghdad-Iraq. Her Ph.D. in Computer science from the Department of Computer Science at the University of Technology-Baghdad-Iraq since 2006. She presently is the head of the networks management branch since 2017-till until now. Her research interested focuses on image processing, pattern recognition, and security visual cryptography systems. E-mail: Shaimaa.h.shaker@uotechnology.edu.iq

Article submitted 2021-05-12. Resubmitted 2021-06-03. Final acceptance 2021-06-04. Final version published as submitted by the authors.