Survey on 3D Content Encryption

https://doi.org/10.3991/ijim.v15i15.24179

Nashwan Alsalam Ali[1](✉), Abdul Monem S. Rahma[2], Shaimaa H. Shaker[2]
[1]University of Baghdad, Baghdad, Iraq
[2]University of Technology, Baghdad, Iraq
nashwan_alsalam60@coeduw.uobaghdad.edu.iq

Abstract—The rapidly growing 3D content exchange over the internet makes securing 3D content became a very important issue. The solution for this issue is to encrypting data of 3D content, which included two main parts texture map and 3D models. The standard encryption methods such as AES and DES are not a suitable solution for 3D applications due to the structure of 3D content, which must maintain dimensionality and spatial stability. So, these problems are overcome by using chaotic maps in cryptography, which provide confusion and diffusion by providing uncorrelated numbers and randomness. Various works have been applied in the field of 3D content-encryption based on the chaotic system. This survey will attempt to review the approaches and aspects of the structure used for 3D content encryption methods for different papers. It found the methods that used chaotic maps with large keyspace are more robust to various attacks than other methods that used encryption schemes without chaotic maps. The methods that encrypting texture, polygon, and vertices for 3D content provide full protection than another method that provides partial protection.

Keywords—3D content, chaotic system, 3D model

1 Introduction

Dealing with data over the communication network such as video and images is increasingly used in our daily lives. In addition to videos and images, 3D content is widespread nowadays in various applications and technologies, including virtual reality and augmented reality technology, industry, medical and military, so protecting 3D content from unauthorized use is necessary. The encryption process is applied to achieve a high level of confidentiality, integrity, and security for 3D content when transmitted via unsafe channels [1–3]. 3D content is classified into two types: 3D surface model and 3D solid model, the 3D surface model representing the shell/boundary of the object model, and the 3D solid model representing the volume of the physical object model, the 3D surface including vertices (point cloud), polygon, and textures [4]. There are many proposed encryption schemes some of them have been adopted and standardized in the world; however, they are not suitable for 3D content, such as Advanced Encryption Standard (AES) and Data Encryption Standard (DES), because the problem of encrypting 3D content due to the application requirement and the data structure such as format compliance, content usability, complexity, real-time performance, and

security level [5]. Chaotic systems are attracted and adopted by the researcher in cryptosystems because they have excellent properties such as sensitivity to the initial condition, control parameter, ergodicity, randomness, deterministic, periodicity, and high speed [6,7].

search have been proposed to develop robust 3D content encryption schemes. This survey focused on and interested in the schemes that encrypted 3D content using chaotic maps and found some papers [4,18–23] are used chaotic maps in encrypting 3D content, and the remaining other papers [5,16,17] are used encryption schemes without chaotic maps.

2 3D content

The 3D content is a data representation in three dimensions which is embodied by a 3D object and a material in a virtual space. The 3D object illustrates the geometry representation of 3D content where it is represented by 3D modeling; hence it is characterized by a material. The object surface physical characteristics are defined by the material, which is represented by a texture map. The texture is a wrapper upon geometry. The 3D content structural elements, including

- Texture map: The texture map is a 2D image that overlaid upon the geometry of a 3D model that improves surface details to add realism to computer graphics. It consists of an array of elements representing texture space where each element in the array is called Texel, texture element, or texture pixel. Each Texel is assigned to a vertex of the 3D object; it maps pixels from a texture to a 3D surface (wrapping the image around the 3D object), as shown in Figure 1.

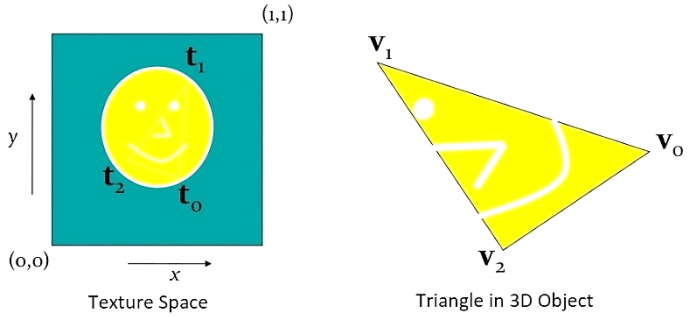

Fig. 1. Concept of texture mapping

- 3D models: The 3D model is a mathematical representation of a 3D object in digital space; it included four main 3D representations, which are
  a) Point cloud: is a set of vertices represented by x, y, and z coordinates. These vertices are used to demonstrate the external surface of an object.
  b) Polygon meshes: it consists of vertices, edges, and facets.

c) Volumetric model: is a set of volumetric elements (voxels) which demonstrate a value on a regular grid in a three-dimensional space.
d) Parametric surface: is specified by a parametric equation with two parameters. [8, 9].

3 3D content encryption approaches

3D content encryption can be classified into two main parts texture map encryption and 3D model encryption. In texture map encryption, the 2D image, which represents the surface details and the wrapper of the geometry 3D model will be encrypted. In 3D model encryption, the mathematical representation of the 3D object will be encrypted in a three-dimensional Cartesian space R3 [8].

4 Cryptography based chaos theory

The proportionate mixture of chaotic mathematical theory and the science of cryptography is called chaotic cryptography. The chaotic system consists of dynamic equations that vary with time. When the dynamic system satisfies the flowing three conditions, it will be considered as chaotic.

- Sensitive to initial conditions.
- Topological mixing.
- The density of periodic orbits [7].

The relationship between cryptography and the chaotic system makes a cryptography base chaos 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's view, whereas it appears as defined in the receiver's view and decryption is possible [10–12].

The chaotic system is applied in a cipher system using two ways.

a) A chaotic system is used to generate a pseudorandom keystream.
b) Use the secret keys or plaintext as the control parameters and initial conditions.

The chaotic system and cryptography have similarities and differences that are illustrated in Table 1.

Table 1. Similarities and differences between chaotic systems and cryptography systems [10]

Chaotic System	Cryptography System
Phase space: a set of a real number	Phase space: a set of an integer number
Use iterations	Use Rounds
Parameters	Key
Sensitive to initial condition and control parameter.	Diffusion

5 Chaos based data cryptosystem architecture

The chaos-based data cryptosystem architecture consists of two main stages: the confusion and diffusion stages. Diffusion means spreading out of the influence of a single plain text digit over many ciphertext digits to hide the statistical structure of the plain text. To achieve confusion and diffusion robust key sequence must be generated [13]. Figure 2 illustrates the architecture of the two stages.

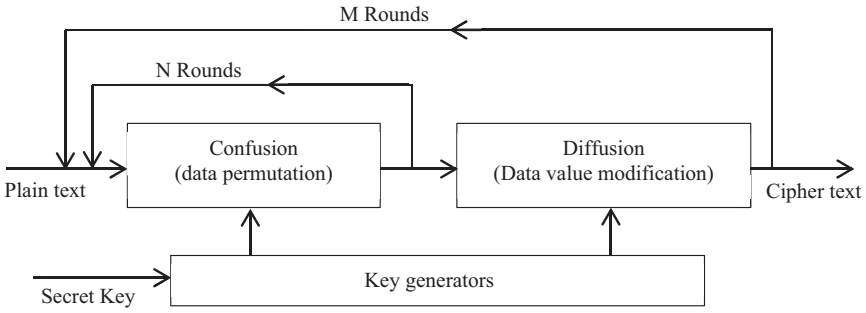

Fig. 2. The architecture of chaos-based data cryptosystem

In the confusion stage, the data values are permutated where just the position of the data is scrambled without changing the data value, so the data will be unrecognizable but performing just confusion stages on the data make it not very secure because the attack may be breaking it, so to increase the data security and enhance the security level the second stage (diffusion) must be applied, wherein this stage the data values will be modified using the sequence generated by the chaotic system. To satisfy a good security level, the confusion and diffusion round must be repeated several times [7,14,15].

6 Insight into different 3D encryption techniques

Alireza Jolfaei et al. in 2016 [5] proposed a novel texture encryption scheme where they used fast stream cipher Salsa20/12 to encrypting texture images by using permutation and bit masking operation. The encryption process involves scrambling the lower nibble-image using zigzag permutation and using Salsa20/12 to encrypt the upper nibble-image. The proposed scheme has satisfied security requirements, and it is lightweight and protects the texture from partially leaked. The encryption speed of the scheme has a better speed profile than encryption by 128-bit AES. The 500 sample texture images are used to implement and test the proposed scheme. The implementation scheme results show that the scheme is better than 128 bit AES in encryption performance.

Ngoc-Giao Pham et al. in 2018 [16], the authors presented a random encryption method for encrypting 3D printing models (3D triangle mesh). After the geometric transformation process, the proposed method encrypted the vertices of each distorted facet randomly using a secret key produced from the Hash function. The geometric transformation, including shear transformation, destroyed each facet of the 3D printing

model and 3*3 vertices matrix constructed from the vertices of each destroyed facet. The constructed matrix coefficients are encrypted randomly using the random numbers of another matrix so that the encrypted 3D printing model will be generated. After the encryption process, the entire 3D triangle mesh is altered. The experimental result shows that the proposed method is highly efficient and has high security for 3D printing models.

Najlaa Hamza et al. in 2019 [17], 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 the substitution step, each component of the data matrix will be altered with another element, in the 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 encrypting the 3D model where the system has achieved effective and strong security.

Xin Jin et al. in 2016 [18], the authors encrypting the 3D point clouds using a method based on chaotic maps, they proposed two methods for encrypting 3D point clouds the first method is: using Logistic chaotic mapping to generate three random sequences Random Vector (RV). Each 3D point clouds coordinate is shuffled randomly by each random vector; the second method is using the logistic mapping to generate 3*1 translate vector Random Transformation Matrix (RTM) and random invertible rotation 3*3 matrix, then the translate vector and random rotation matrix are used to project each 3D point to another random place in the homogenous coordinate. The authors used different 3D point clouds to test the above two encryption methods of the 3D point cloud, and they evaluated the encryption results using the VFH (Viewpoint Feature Histogram).

Xin Jin et al. in 2017 [19] focused on the 3D textured from the 3D content to provide security and privacy for 3D content. The authors encrypted 3D textured models using proposed 3D Lu chaotic maps. They used the 3D Lu chaotic map for encrypting textures, vertices, and polygon, then gathering these encrypted content to form the final encrypted 3D texture model. The experimental results show that the proposed method can correctly encrypt the 3D textured model and resisting to brute- force attacks.

Ji Xu, Chen Zhao, and Jun Mon in 2020 [20] proposed a novel 3D image encryption 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 the conventional attack.

Benson Raj et al. in 2020 [21], the authors proposed an encryption system that uses a 3D Arnold cat map to encrypting 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 [22] 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 results are close to the ideal value, leading the scheme to be highly secured and resist common attacks.

Chaochuan Jia et al. in 2019 [23], 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(3N2), the authors used 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) with time complexity is O(6M), the authors used a 3D cat map to generate a random transformation matrix to transform a point in 3D space into a different position.

Xin Jin et al. in 2020 [4], the authors proposed an encryption method that encrypts point cloud, polygon, and textures using multi-level chaotic maps; for vertices, the authors encrypt them by using a high-level 3D Lu chaotic map. The authors use a 1D Logistic map and DNA coding to encrypt textures and use 2D Arnolds's cat map to encrypt polygons. The experimental results illustrate that the proposed method has a similar performance with other methods using the same multi-level chaotic maps for vertices, polygons, and textures, but the proposed method has less execution time. The proposed method also can resist more attacks such as correlation attacks, brute force attacks, and statistic attacks.

7 Security analysis of the encryption schemes

A good 3D model encryption scheme should resist all kinds of known attacks, such as various brute-force attacks and statistical attacks [4,10].

7.1 Resistance to brute-force attack

- Key Space Analysis: The decryption key can be found by checking all possible keys by several tries; this refers to a keyspace. The 3D model encryption scheme should have a large keyspace to resist various attack types. If keyspace is not large enough, it will be broken down by exhaustive search and will obtain the secret encryption key.
- Key Sensitivity Analysis: The good encryption scheme must be sensitive to the secret key used, so a small change in the secret key must produce a large different encrypted or decrypted 3D model. A Chaotic system is sensitive to the initial value

and system parameter. When a light difference has been made, this will lead to a failure decryption process. So, using Chaotic systems in encrypting the 3D model will increase the security of the encryption scheme.

7.2 Resistant to the statistical attack

- Histogram analysis: The viewpoint feature histogram (VFH) represents point clusters for cluster identification. The VFH is used to evaluate 3D vertex encryption. When the VFH of the encryption process different from the VFH of the decryption process. So, the statistical attack will be impossible [4].
- Distribution of occupied positions: The 3D vertices occupied positions are analyses by computing the distribution occupied position 3D vertices for normal 3D vertices and encrypted 3D vertices.

8 Comparative analysis

This section will be explaining the comparative between the encryption methods on 3D content based on the main aspect (Type of 3D content encryption, Method based and Characteristics). Table 2 shows a comparative analysis for the methods explained in the section above.

Table 2. The comparison between methods

Authors	Type of 3D Content Encryption	Method Based	Characteristics	Limitations
Alireza Jolfaei et al. [5]	Texture Encryption	• Selective AES. • Full AES. • Salsa20/12 stream cipher (Salsa dance). • Bit masking and permutation.	• Salsa20/12 lightweight encryption. • Salsa20/12 has better speed than selective AES and full AES.	• Encrypting texture only. • Partial protection for 3D content.
Ngoc-Giao Pham et al. [16]	3D Triangle mesh (Set of facets)	• Key from Hash function. • Geometric Transformation. • (Shear facets Transformation).	• High efficient. • High Security. • Speed depends on the number of facets.	• Encrypting facets only by the shear process. • Partial protection for 3D content.
Najlaa A. Hamza et al. [17]	Vertices of the 3D model.	• Three keys are generated from a random number generator. • Transposition, Substitution, Folding, and Shifting (TSFS) Algorithm for vertices.	• High security. • Speed depends on the number of vertices.	• Encrypting vertices only. • Partial protection for 3D content.

(Continued)

Table 2. The comparison between methods *(Continued)*

Authors	Type of 3D Content Encryption	Method Based	Characteristics	Limitations
Xin Jin et al. [18]	3D point cloud	• Logistic chaotic mapping • Random Vector(RV) shuffle point clouds. • Random Transformation matrix(RTM) shuffle point clouds.	• Resistant to brute-force attack because keyspace is large. • Speed depends on the number of points in the cloud.	• Encrypting points in the cloud only. • Partial protection for 3D content.
Xin Jin et al. [19]	3D textured model	• 3D Lu Chaotic mapping.	• Resistant to brute-force attacks and statistical attacks because the keyspace is large. • Speed depends on the number of vertices.	• Non
Jixu, Chen Zhao and Jun Mon et al. [20]	Vertices of the 3D model	• SHA 256 hash value • Chaotic System. • Arnold matrix and DNA Algorithm.	• Resistant to conventional attack. • High-security features.	• Encrypting vertices only. • Partial protection for 3D content.
Benson Raj et al. [21]	3D mesh model	• 2D Arnold cat map. • 3D Arnold cat map. • Permutation and substitution for vertices and faces.	• Resistant to various attacks. • Large keyspace.	• Encrypting vertices and facets only. • Partial protection for 3D content.
Xingyuan Wang et al. [22]	3D triangle model	• Uses Hash-256 to generate the 256-bit key. • 1D Logistic map to generate a sequence. • Use sequence for permutation and scramble plain text. • Encryption using XOR and scrambling.	• Resistant to brute-force attacks and statistical attack • It has high security.	• Encrypting points of triangular facets only. • Partial protection for 3D content.
Chaochuan Jia et al. [23]	3D point cloud	• Permutation using 2D Cat Map (P2DCM). • Random Transformation Matrix using 3D Cat Map (RTM3DCM).	• Resistant to brute-force attacks and statistical attacks because the keyspace is large. • Speed depends on the number of points in the cloud.	• Encrypting points in the cloud only. • Partial protection for 3D content.
Xin Jin et al. [4]	3D textured model (vertices, Polygons, and textures)	• 1D Logistic map and DNA coding for encryption textures. • 2D Arnold cat map for encryption polygons. • 3D Lu chaotic for encryption vertices.	• Resistant to Brute-force attacks, statistical attack, and correlation attack. • Speed depends on the number of vertices.	• Non

9 Conclusion

In recent years, the security of 3D content has become a very important issue, especially when data exchanging over an open network and internet. This paper studies and reviews the methods of encrypting 3D content. Many encryption methods are compared and published in 2016–2020. The review paper includes most encryption methods based on chaotic map systems to encrypt vertices, polygon, and texture based on confusion and diffusion, thereby increasing its resistance to various attacks such as brute-force attacks and statistical attacks. This survey found that the methods that used chaotic maps with large keyspace are more robust to various attacks than other methods which are used encryption methods without chaotic maps and the methods which encrypting texture, polygon, and vertices for 3D content provide full protection than another method which encrypting some part of 3D content, so they provide partial protection.

10 References

[1] 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

[2] 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

[3] 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

[4] 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

[5] 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

[6] 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

[7] 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

[8] A. Jolfaei, "Robust encryption schemes for 3D content protection", Thesis (Ph.D. Doctorate), Griffith University, 2016.

[9] L. F. Jalil and M.M. Laftah, "Text Hiding in 3D Object", Engineering and Technology Journal, vol. 34, Part (B), no. 5, 2016.

[10] 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

[11] Y. H. Ali and Z. A. H. Alobaidy, "Images Encryption Using Chaos and Random Generation," Engineering and Technology Journal, vol. 34, Part (B), no. 1, 2016.

[12] A. S. Hamad and A. K. Farhan, "Image Encryption Algorithm Based on Substitution Principle and Shuffling Scheme," Engineering and Technology Journal, Vol. 38, Part B, No. 03, pp. 98-103, 2020. https://doi.org/10.30684/etj.v38i3B.433
[13] A. Karim and S. Mahmoud, "Image Encryption Based on Hyperchaotic Liu system Algorithm," Engineering and Technology Journal, vol. 33, Part (B), no. 2, 2015.
[14] S. Sheela and S. V. Sathyanarayana, "Application of chaos theory in data security-a survey," Accent. Trans. Inf. Secur., vol. 2, no. 5, pp. 1–15, 2017. https://doi.org/10.19101/TIS.2017.25001
[15] L. P. Gagnani and S. Varjani, "Survey of 3D Chaotic Map Techniques for Image Encryption," Int. J. Sci. Res., vol. 4, no. 12, pp. 1000–1004, 2015. https://doi.org/10.21275/v4i12.NOV152193
[16] N. G. Pham, S. H. Lee, O. H. Kwon, and K. R. Kwon, "3D printing model random encryption based on geometric transformation," Int. J. Mach. Learn. Comput., vol. 8, no. 2, pp. 186–190, 2018. https://doi.org/10.18178/ijmlc.2018.8.2.685
[17] N. A. Hamza, S. H. Jafeer, and A. E. Ali, "Encrypt 3D Model Using Transposition, Substitution, Folding, and Shifting (TSFS)", 2nd Scientific Conference of Computer Sciences, pp. 126–131, 2019. https://doi.org/10.1109/SCCS.2019.8852600
[18] X. Jin, Z. Wu, C. Song, C. Zhang, and X. Li, "3D point cloud encryption through chaotic mapping," in 17th Pacific Rim Conference on Advances in Multimedia Information Processing, vol. 9916 LNCS, pp. 119–129, 2016. https://doi.org/10.1007/978-3-319-48890-5_12
[19] X. Jin et al., "3D textured model encryption via 3D Lu chaotic mapping," Sci. China Inf. Sci., vol. 60, no. 12, pp. 1–9, 2017. https://doi.org/10.1007/s11432-017-9266-1
[20] 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
[21] 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
[22] 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
[23] 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

11 Authors

Nashwan Alsalam Ali is presently one of the faculty college of education for women, computer science department, Baghdad University in 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 focused on Multimedia Security from Iraqi Commission for Computers and Informatics in 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. Contact: +9647712890216. 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 2021-05-10. Resubmitted 2021-06-04. Final acceptance 2021-06-04. Final version published as submitted by the authors.