Iraqi Journal of Science, 2023, Vol. 64, No. 5, pp: 2521-2532
DOI: 10.24996/ijs.2023.64.5.35

ISSN: 0067-2904

3D Content Encryption Using Multi-Level Chaotic Maps

Nashwan Alsalam Ali[1*], Abdul Monem S. Rahma[2], Shaimaa H. Shaker[3]
[1]*Computer Department, College of Education for Women, University of Baghdad, Baghdad, Iraq*
[2]*Computer Sciences Department, Al-Maarif University College, Anbar, Iraq*
[3]*Computer Science Department, University of Technology, Baghdad, Iraq*

Received: 24/1/2022 Accepted: 16/9/2022 Published: 30/5/2023

Abstract

Nowadays, 3D content is becoming an essential part of multimedia applications, when the 3D content is not protected, hackers may attack and steal it. This paper introduces a proposed scheme that provides high protection for 3D content by implementing multiple levels of security with preserving the original size using weight factor (w). First level of security is implemented by encrypting the texture map based on a 2D Logistic chaotic map. Second level is implemented by shuffling vertices (confusion) based on a 1D Tent chaotic map. Third level is implemented by modifying the vertices values (diffusion) based on a 3D Lorenz chaotic map. Results illustrate that the proposed scheme is completely deform the entire 3D content according to Hausdorff Distance (HD) approximately around 100 after the encryption process. It provides a high security against brute force attack because it has large key space equal to 10^{165} and secret key sensitivity using NPCR near 99:6% and UACI near 33:4%. The histogram and HD indicate the decrypted 3D content is identical to the origin where HD values approximate zero.

Keywords: 3D content, 2D Logistic map, 3D Lorenz map, chaotic map, 1D Tent map

تشفير المحتوى ثلاثي الابعاد بأستخدام عدة مستويات من الخرائق الفوضوية

نشوان السلام علي[1]*, عبد المنعم صالح رحمة[2], شيماء حميد شاكر[3]
[1] قسم الحاسوب, كلية التربية للبنات, جامعة بغداد, بغداد, العراق
[2] قسم علوم الحاسوب, كلية المعارف الجامعة, أنبار, العراق
[3] قسم علوم الحاسوب, الجامعة التكنولوجية, بغداد, العراق

الخلاصة

في الوقت الحاضر ، أصبح المحتوى ثلاثي الأبعاد جزءًا أساسيًا من تطبيقات الوسائط المتعددة ، عندما لا يكون المحتوى ثلاثي الأبعاد محميًا ، قد يهاجمه المتسللون ويسرقوه. هذا البحث قدم طريقة مقترحة لتوفير حماية عالية للمحتوى ثلاثي الأبعاد من خلال تنفيذ مستويات متعددة من الأمان مع المحافظة على الحجم الاصلي للجسم المشفر باستعمال معامل (w). يتم تنفيذ المستوى الأول من الأمان عن طريق تشفير النسيج بناءً على الخريطة الفوضوية لوجستك ثنائية الأبعاد. يتم تنفيذ المستوى الثاني عن طريق تبديل النقاط (ارباك)

*Email: nashwan_alsalam60@coeduw.uobaghdad.edu.iq

بناءً على الخريطة الفوضوية Tentذات البعد الواحد. يتم تنفيذ المستوى الثالث من خلال تغييرقيم الرؤوس (الانتشار) بناءً على الخريطة الفوضوية ثلاثية الأبعاد Lorenz. توضح النتائج أن المخطط المقترح يشوه تمامًا المحتوى ثلاثي الأبعاد بالكامل وفقًا لمقياس Hausdorff (HD) تقريبًا حتى 100 بعد عملية التشفير ويوفر أمانًا عاليًا ضد هجوم brute force لأنه يحتوي على عدد كبير من مفتاح يساوي 10^{165} وحساسية المفتاح السري باستخدام NPCR تقريبا 99:6% و UACI تقريبا 33:4%. يشير الرسم البياني و HD إلى أن المحتوى ثلاثي الأبعاد الذي تم فك تشفيره متطابق مع الأصل حيث قيم HD تقريبًا صفر .

1. Introduction

Digital media development in the Internet, multimedia applications, transmitting digital data over the unsecured channel, and widespread use of personal computers allow users to protect the digital data from threats and attacks [1]. Cryptography is applied for protecting digital data by performing encryption process, which is a good tool for encoding operation. Encryption process is based on key generation that defines how data are coded so it can be accessed by the authorized person [2]. Many algorithms for encryption are suggested to transform data into unidentifiable formats and prevent illegal access by users [3,4]. Presently, 3D content has become an increasingly significant aspect of multimedia content; as their applications grow in popularity, there is a need for protecting these 3D contents; As a result, the thread problem must be resolved [5,6]. Several recommended encryption techniques have been established and adopted as a standardized method, but they are not appropriate to encrypt a 3D content, such as Data Encryption Standard (DES) and Advanced Encryption Standard (AES), since the difficulty of the 3D content encryption is caused by the requirements of the application and data formats [7]. To solve that, various chaotic cryptography-based encryption methods have been implemented. The researcher is drawn to and uses chaotic systems in cryptosystems because they have desirable qualities [8,9]. In this paper, the proposed 3D content encryption method will be introduced, which provides a multi-level of security with preserving the original 3D content size (dimensionality), which is considered a main problem in 3D content encryption. Our contribution is encrypting the 3D content with preserving the dimensionality (original size) as the origin.

2. Previous Work

Xin Jin et al. in 2017 [10] apply the 3D encryption method depending on 3D Lu chaotic maps to encrypt 3D models with texture to achieve the main requirements of security for 3D content. They encrypted textures, vertices, and polygons using the same chaotic map. They used a colour image for texture and encrypted each band separately (Red, Green and Blue) using 3D Lu chaotic maps and combined them to get the final encrypted texture. After encryption was complete, merge the encrypted texture with the encrypted mesh model to obtain the final encrypted content mixing with texture. According to the testing results, the proposed method encrypts the 3D textured model with good results and good resist brute-force attacks.

Benson Raj et al. in 2019 [1] suggested a scheme for encrypting a 3D mesh model using a 3D Arnold cat map by translating the clear data to unobvious. The proposed cryptosystem encrypts the 3D mesh model but does not encrypt the texture by shuffling and substitution using the chaotic Arnold cat map, which shuffles and substitutes the vertices and faces individually. The final encrypted model is created by combining them. The 3D Arnold map achieves good diffusion and confusion at each round to increase the level of security. The encryption method exhibit that the 3D models were resistant to a wide range of attacks.

Xingyuan Wang et al. in 2019 [6] suggested a system for encrypting 3D objects by converting them to 2D objects in the same way as images are encoded. Confusion and diffusion are two steps that the encryption scheme is included: the first step Random key generated during the confusion phase, and during the diffusion phase, they separated the floating data into two parts: integer and decimal parts. XOR procedure is used to encrypt the integer part, whereas the decimal part was just jumbled. The scheme is very safe and resistant to common attacks, according to the security analysis.

Najlaa Hamza et al. in 2019 [11] recommended employing an encryption algorithm to encrypt a 3D mesh model without texture based on Transformation, Substitution, Folding, and Shifting (TSFS) to encrypt the 3D object. The 3D model vertices are fed into the TSFS algorithm through the encryption method. The four stages of TSFS depend on three keys: in transformation step, firstly, the vertices positions are altered; second step, data matrix component is replaced with a different element; in third step, folding the matrix elements diagonally, vertically, and horizontally; and in final step, to replace the code with another the TSFS using the element 16. Results demonstrated that the suggested technique effectively encrypts the 3D model, resulting in effective and resilient security for the system.

3. Cryptography and Chaotic System

Confidentiality and security are being the most crucial for data protection. Cryptography is defined as a proportionate mixing of chaotic mathematical theory and cryptography science. The chaotic system comprises a dynamic equation that evolves over time. Chaotic is defined as a dynamic system that meets all three characteristics (topological mixing, initial conditions sensitive and the density of periodic orbits).

The relationship between a cryptographic system and a chaotic system exists; however, the main distinction has been that chaos operates on an unlimited domain, whereas cryptography operates on a limited domain [8,12]. Cryptography-based chaos is a natural choice for cryptography and safe interaction because of the link between cryptography and chaotic systems [13]. Chaotic systems and cryptography share Periodic orbits with huge durations that are unstable, initial conditions sensitivity, control parameters, and unpredictable behavior. The attacker sees the system output as arbitrary due to unexpected behavior. But it appears predictable to the receiver, allowing decryption. [14,15].

4. Chaotic Maps

4.1 2D Logistic map

The emerging of the 2D Logistic map is developed from the 1D Logistic map, which represents the basis of the 2D Logistic map. 1D Logistic can be easily attacked due to its one control parameter, so it has smaller key space. The 1D Logistic map is a simple and demonstrated not sophisticated chaotic behavior. The 2D Logistic map is more sophisticated than the 1D Logistic map and has a larger key space; hence it is commonly used in cryptography. Equation (1) and (2) represents the 2D Logistic map mathematically, where x_i and y_i are the two pair points at the i^{th} iteration and r represents the control parameter.

$$x_{i+1} = r(3y_i + 1)x_i(1 - x_i) \quad (1)$$

$$y_{i+1} = r(3x_i + 1)y_i(1 - y_i) \quad (2)$$

The parameter r is confined to a limited range between 0 and 4 such that [0, 4], the two pair points x_i and y_i take the values within the range [0, 1], the iterations x_{i+1} and y_{i+1} are iterative sequences since they depend on the prior value of x_i and y_i, respectively. [16-19].

4.2 3D Lorenz chaotic map

Edward Lorenz developed a mixed differential equations and produced a three-dimensional chaotic map called the 3D Lorenz. The array containing chaotic solutions for the Lorenz system is called attractors, formed by the Lorenz chaos sequences. The Lorenz chaotic formula in three dimensions is shown by equations (3), (4), and (5).

$$\frac{dx}{dt} = a(y - x) \tag{3}$$

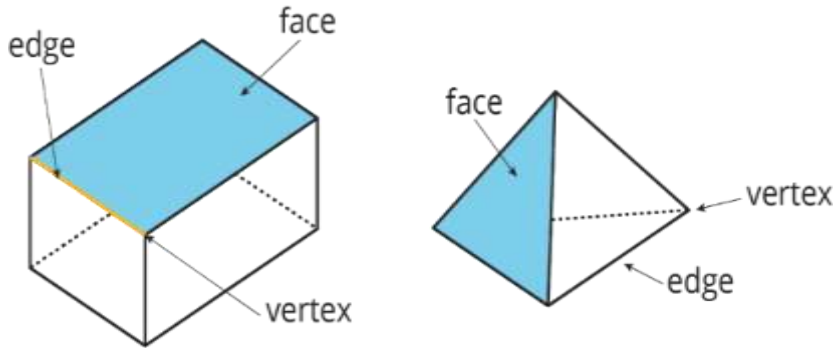
$$\frac{dy}{dt} = rx - y - xz \tag{4}$$

$$\frac{dz}{dt} = xy - bz \tag{5}$$

The main parameters to control the system are a, r, and b, representing the important ones the system relies on. The values of the parameter when equal to a=10, r=28, and b=8/3 are used, the x, y, and z are the equation solution curves. The starting values for (x, y, and z) are the basis of the trajectory of the 3D Lorenz, where they constitute the permutation process secret key. [20, 21].

5. Representation of 3D Content

The 3D model is expressed by a 3D polygon mesh; each polygon can be either triangle or quadrilaterals polygon depending on the sides. It can be triangles if three sides are available or quadrilaterals if four sides are there [22]. The mathematical structure of the polygon mesh is labelled as M= {G, C}, such that G denotes the data of geometry and C denotes the topological data. The geometry data is marked as G= {V, E, F}, such that V are the vertices list, E is the edge that connects between vertices in the model, and F is the data for faces. The topological data, which includes the geometry elements connection information. Figure 1 depicts the representation for quadrilaterals and triangle polygons.



(a) **(b)**

Figure 1: (a) Structure for Quadrilaterals, (b) Structure for Triangle [23]

The 3D model is visualized by its geometry which represents the 3D surface. The surface must be characterized by material to achieve the vision laid out by the notion artist using a texture map.

The texture map is the physical properties of the surface of a 3D model. It is a two-dimensional image linked to the geometry of a 3D model to improve the details of the surface and give computer visuals more realism. It is made up of an array containing elements, the individual element of which is referred to as a texel (wrapping around the 3D object) [24-26].

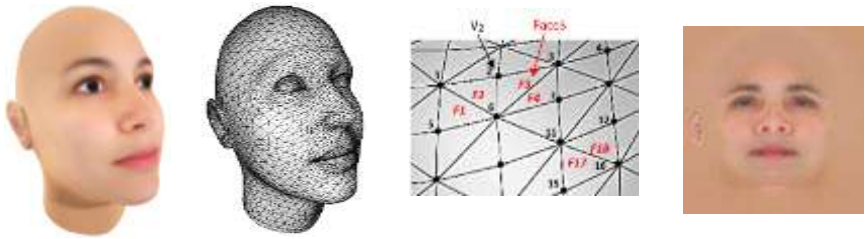
6. Proposed 3D Content Encryption Scheme

The fundamental phases of the encryption and decryption process for the proposed method will be described in this section. A 3D mesh model and texture map together comprise the 3D content surface; we'll encrypt both the mesh of the 3D model and texture map. The mesh has vertices and faces, with the vertices linking every three vertices to form faces. Each vertex has three coordinates (v_x, v_y, and v_z). The suggested encryption technique is made up of two basic processes including:

a) *Texture encrypting process*: The texture of the 3D content is encrypted in the first step of the encryption process using keys created by a 2D Logistic map with a length equal to the number of texels in the texture map.

b) *3D mesh model encrypting process*: The 3D mesh will be encrypting in this process and including two sub-processes firstly, applying permutation to the mesh vertices using a key obtained from a 1D tent chaotic map to shuffle the mesh vertices positions; secondly utilizing keys generated from a 3D Lorenz Chaotic map to change the mesh vertices values. When 3D Lorenz is applied, three keys are generated for each iteration (key_1, key_2, and key_3) representing the 3D key, where key_1 is in charge of altering the v_x value, key_2 is in charge of changing the v_y value, and key_3 is in charge of changing the v_z value, such that K = {(Kx_1, Ky_1, Kz_1), …… (Kx_n, Ky_n, Kz_n)}

The vertices of the model are stored in a list V, where V= {(v_{x1}, v_{y1}, v_{z1}), ……, (v_{xn}, v_{yn}, v_{zn})}, the number n denotes the vertices number in the 3D model. Figure 2 depict the Face Man 3D content and its 3D mesh representations.



(a) **(b)** **(c)** **(d)**

Figure 2: (a) Original 3D content, (b): 3D Mesh model, (c): Close-up of the mesh's triangles, (d) Texture map

Table 1 shows the structure of the ".obj" file where for reducing the memory size, the vertices and the faces are formed as an array of indices.

Table 1: The structure for vertices and faces for 3D mesh .

Vertices list Information					Faces list information	
Index of vertex	**x-coordinate**	**y-coordinate**	**z-coordinate**		**Index of face**	**Vertices index in each face**
1	$V_{1,x}$	$V_{1,y}$	$V_{1,z}$		1	(5,6,1)
2	$V_{2,x}$	$V_{2,y}$	$V_{2,z}$		2	(1,6,2)
3	$V_{3,x}$	$V_{3,y}$	$V_{3,z}$		3	(6,3,2)
….	….	….	….		….	….
15	$V_{15,x}$	$V_{15,y}$	$V_{15,z}$		17	(15,16,11)
16	$V_{16,x}$	$V_{16,y}$	$V_{16,z}$		18	(11,16,12)
….	….	….	….		….	….

The encryption algorithm below lists the essential steps for the suggested method.

Encryption Algorith

Input: 3D content in '. Obj' file format.
Output: Encrypted 3D content.
Step 1: Read 3D content, separate 3D model and texture map from 3D content, store texture map in *T* array and vertices of the 3D model in *V* array.
Step 2: For every texel in the *T* array:
generate a 2D key using a 2D Logistic chaotic map and apply equation (6) to conduct the encryption process.

$$T` = T \oplus k(x, y) \quad (6)$$

End for.
Step 3: For every vertex in *V* array, do:
Apply shuffling process (Confusion) on *V* using a 1D key generated by Tent chaotic map and resulting *V`*.
End for.
Step 4: For every vertex from *V`* in shuffled 3D mesh model:
- use 3D Lorenz map to produce 3D keys *K*, where $K = \{x, y, z\}$.
- Modify vertex value (Diffusion) from *V`* using equation (7) to resulting *V``*.

$$V``(x, y.z) = (\big(V`(x, y, z) + K(x, y, z)\big) * W \quad (7)$$

Where *V``* is the vertex encrypted, *W* is the weight factor to keep the spatial stability and dimensionality; End for.
Step 5: Combine encrypted textured map from step2 with encrypted 3D mesh model from step 3-step 4 to generate encrypted 3D content.
Step 6: Save the encrypted 3D content.

Some 3D content needs to multiply each dimension x, y, or z by different weight factors to preserve the exact size of the original 3D content. The 3D content encryption technique stages are depicted in Figure 3.

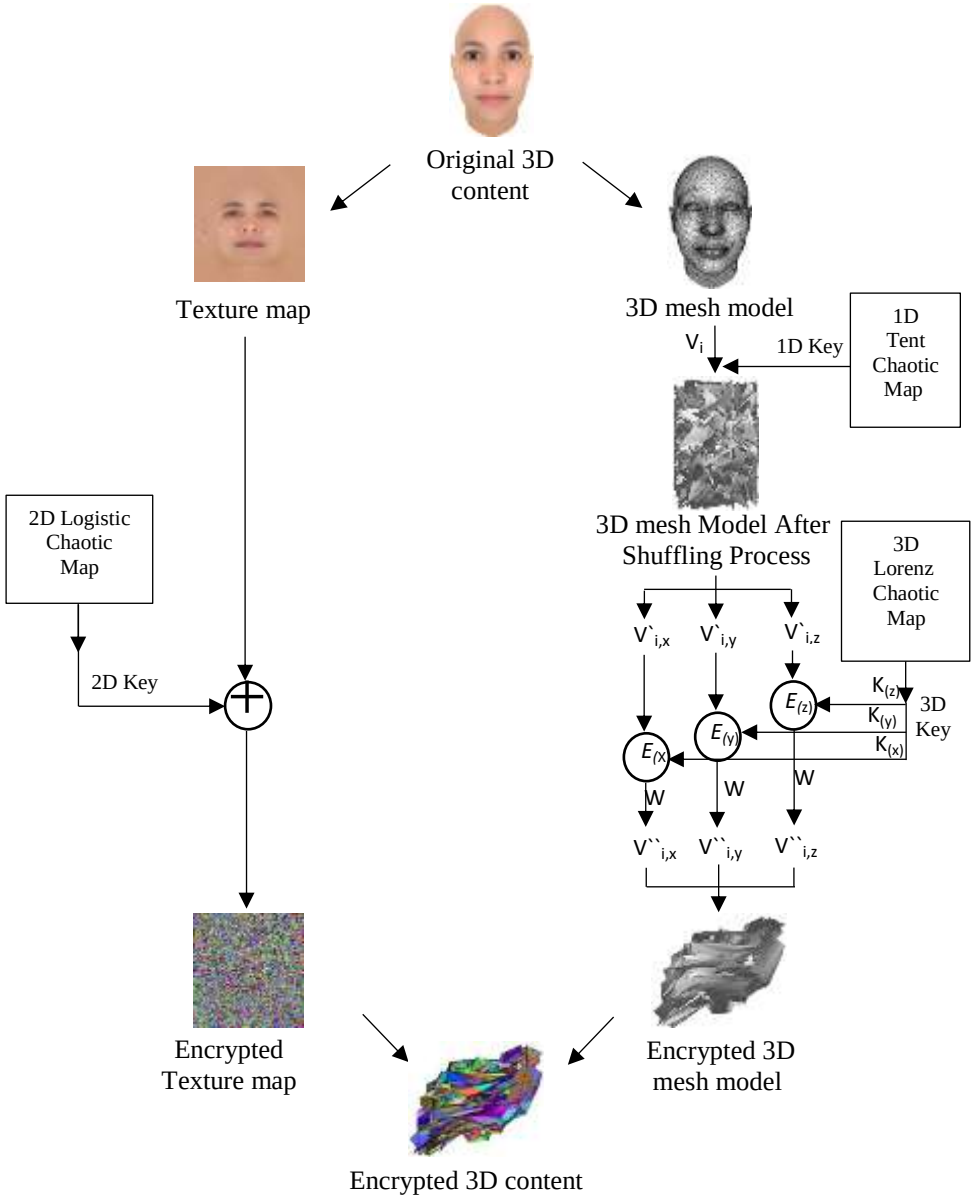


Figure :3 Encryption process of 3D content

The decryption process steps are identical to the encryption steps; however, they are performed in reverse order, except we will divide by the factor (w) instead of multiplication.

7. Simulation Results

Different 3D contents are used of type '.obj' file format to evaluate the efficiency and performance of the proposed encryption scheme (Girl, Heart, Knife, Hammer, and Vase), which are available at the Free3D website [27]. Free3D is a 3D content library that has more than nine thousand items. These 3D contents have various numbers of vertices and faces. Table 2 depicts the original 3D content and the encrypted 3D content; it also illustrates that the required time for the encryption process is based on the vertices number; it increases (more time) by increasing the vertices number included in the models.

Table 2: Information of the 3D content-encryption process

Model name	no. of Vertices	Elapsed time in sec.	Original 3D content	Encrypted 3D content
Girl	9417	27.0465		
Heart	5634	17.5150		
Knife	606	2.4133		
Hammer	314	1.2344		
Vasa	594	2.0868		

The testing results in Table 2 reveal that the encrypted 3D contents are entirely different from the original due to the texture map being encrypted first, and then the 3D mesh model of the 3D content being encrypted second.

8. Statistical Tests

The quality of the proposed encryption method is assessed using the measurements: histograms and Hausdorff Distance (HD). The HD calculates the degree of similarity between two points in two different sets of data, X and Y. The HD can represent the inaccuracy between two-point sets. For two-point sets X= $\{x_1, x_2, x_3, \ldots x_{nx}\}$ and Y= $\{y_1, y_2, y_3, \ldots y_{ny}\}$, the HD metric for a two-point sets can be defined as:

$$HD(Y,X) = max(hd(X,Y), hd(Y,X)) \quad (8)$$

where

$$hd(X,Y) = max_{x\epsilon X} min_{y\epsilon Y} \|x - y\| \quad (9)$$

$$hd(Y,X) = max_{y\epsilon Y} min_{x\epsilon X} \|y - x\| \quad (10)$$

In Equations (9) and (10), the directed Hausdorff Distance HD is used between two point sets X and Y is the biggest distance between each point $x\epsilon X$ to its closest neighbor $y\epsilon Y$; it takes the maximum distance. Directed Hausdorff distance which is represented in equations (9) and (10), used the Euclidean distance between point x and point y, which is denoted by the symbol $\| \ \|$. Undirected HD in Equation (8) is the basic form of HD used to measure the large dis-similarity degree between a two-point set. The greater the HD, is less similarity between the two-point set [28-30].

X and Y represent the two meshes in the 3D space, and $\| x - y \|$ is the Euclidean distance between two points in the two meshes. If the HD approaches zero, no difference exists between them, and inversely.

The values of HD of encrypted and decrypted 3D content are shown in Table 3.

Table 3: Hausdorff distance results

Model name	Hausdorff for encrypted 3D content	Hausdorff for decrypted 3D content
Vase	77.7203	0.0000
Hammer	106.1833	0.0000
Knife	106.5557	0.0000
Heart	84.6480	0.0000
Girl	106.2288	0.0000

Table 3 notes that the HD values for encrypted 3D content are very high, which means they are entirely different from the original models. In contrast, HD values for decrypted 3D content are near zero, which means they are identical to the original model.
Figure 4 depicts the encryption and decryption procedures for the spider 3D content

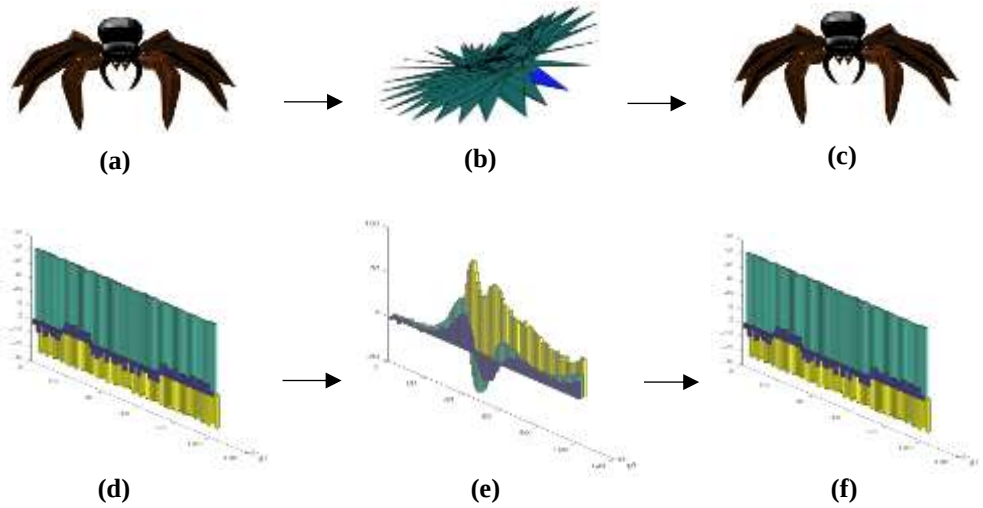


Figure 4: Example of spider 3D content encryption and decryption with histogram (a) Original 3D content (b) Encrypted 3D content (c) Decrypted 3D content (d) Original 3D content Histogram (e) Encrypted 3D content Histogram (f) Decrypted 3D content Histogram

The graphical representation in Figure 4 depicts that the original and encrypted 3D content histograms are obviously different to the eyes and totally identical between the original and decrypted 3D content histograms, so it indicates that the encryption method is immune to statistical attack.

9. Security Analysis

In an encryption system, security analysis can be used by:

– Key space: The key space must be large enough to withstand attacks like brute-force attacks. When the key space is small, it will lead to breaking the cipher text by exhaustive search. The precision of 64-bit data is 10^{15}, in addition to six parameters from the 3D Lorenz map, three parameters from the 2D Logistic map, and two parameters from the 1D Tent map resulting in the key space of size $(10^{15})^{11} = 10^{165}$. As a result, our suggested method is resistant to brute-force attacks due to its large key space.

– Secret key sensitivity: for providing high security to the encryption algorithm, the encryption algorithm must be sensitive to the initial secret key and the input data. A slight change (one bit) in the entered data or key will result in a massive change and significantly affect the encrypted data and the output-produced encryption keys. The Number of Pixels

Change Rate (NPCR) and Unified Average Changing Intensity (UACI) are used to achieve the key sensitivity and the effect of changing one pixel on the full cipher image where the randomization test may be used to assess the image robustness against various types of hackers [31-33]. Equations (11) and (12) evaluate the NPCR and UACI by the following formula.

$$NPCR = \frac{\sum_{i,j} D(i,j)}{M*N} * 100\% \quad (11)$$

$$UACI = \frac{1}{M*N}\left[\sum_{i,j} \frac{|c1(i,j)-c2(i,j)|}{255}\right] * 100\% \quad (12)$$

Where

$$D(i,j) = \begin{cases} 0 & if\ c1(i,j) = c2(i,j), \\ 1 & otherwise \end{cases}$$

M and N are the dimensions of the plain and encrypted images; c1 and c2 are the encrypted images before and after modifying one pixel in the plain image, respectively. NPCR and UACI have precise values of 99:6% and 33:4%, respectively. Table 4 shows the values of the NPCR and UACI of the tested 3D content by implementing the proposed algorithm. The values 99:63 and 33:52 of the NPCR and UACI are the most similar to the theoretical values. The results of Table 4 show that the proposed method is too sensitive to changes in the plain 3D content and that even small changes in the plain 3D content result in entirely different cipher 3D content. As a result, the proposed algorithm can withstand differential attacks. We concluded that if one bit of the key is wrong, that leads to impossibility of recovering the plain 3D content.

Several secret key sensitivity experiments have been conducted; if the initial condition of the chaotic map is changed, it will cause an erroneous decryption procedure to occur, spreading the error to practically all vertices, making it impossible to retrieve the original 3D content.

Table 4: The NPCR and UACI applied on the 3D content.

Model	NPCR	UACI
girl	0.99989	**0.33336**
heart	0.99982	**0.33339**
Knife	0.99835	**0.33388**
hammer	0.99682	**0.33439**
vasa	0.99831	**0.33389**

The 3D model was encrypted using confusion and diffusion process, the encryption algorithm in [10] only has the diffusion process and no confusion process, which means the cipher model can recover easily by rebuilding the 3D model.

10. Time Complexity Analysis

MATLAB 2018 was used to implement the encryption algorithm; it was applied using a computer that has a processor RIZEN 9, RTX graphics card and 16 G DDR4 RAM. The amount of time it takes to encrypt and decode a 3D model is based on the number of vertices in the mesh and the size of the texture map. As seen in Table 2, the girl 3D content having more vertices results in greater time spent, and the one which has less number of vertices will spend less time. Figure 5 shows the time spends for encryption each model (Vaza, Hammer, Knife, Heart and Girl) respectively.

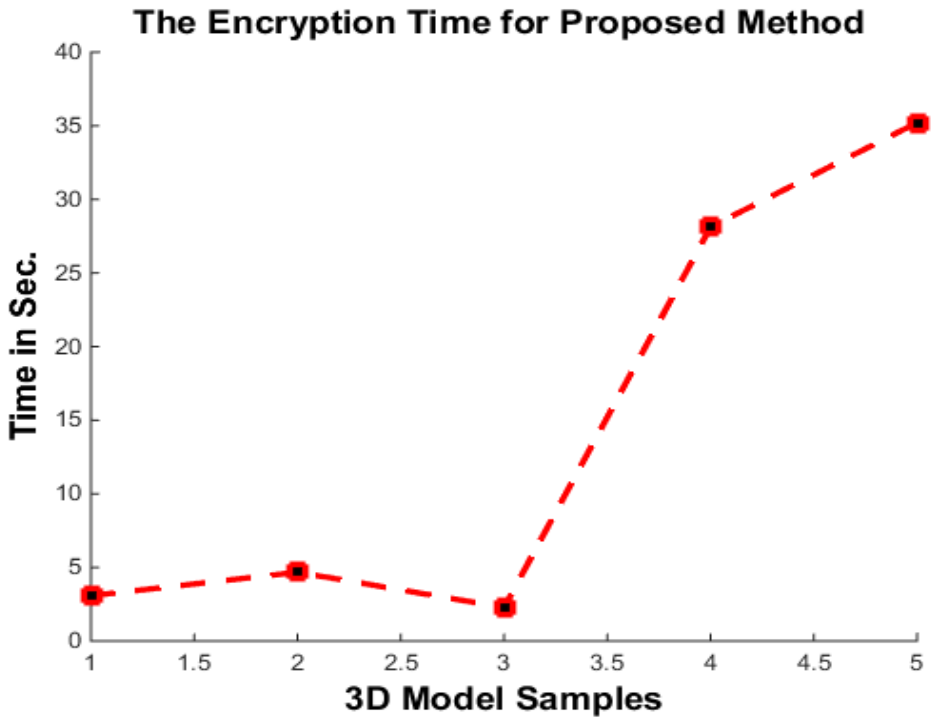


Figure 5: Shows the time for encryption each model.

11. Conclusion

In this paper, different 3D contents are encrypted based on two encryption stages; texture encryption stage and 3D model encryption stage. The results explained in the simulation results section conclude that the proposed scheme obtained good security by using different levels of encryption stages with different chaotic maps, which increased the complexity of the overall encryption scheme. Our proposed schemed also Resists brute-force attacks because it has a large key space equal to 10^{165} and maintains the original dimensions of the encrypted 3D content using the weight factor (w). The proposed scheme achieves secret key sensitivity according to the values of NPCR and UACI, up to 0.99989 and 0.33439 respectively.

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.

[2] M. A. A. J. A. Mizher, R. Sulaiman, A. M. A. Abdalla, and M. A. A. Mizher, "A simple flexible cryptosystem for meshed 3D objects and images," *J. King Saud Univ. - Comput. Inf. Sci.*, 2019.

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

[16] M. A. AlZain, "Efficient image cipher using 2D logistic mapping and singular value decomposition," *Int. J. Adv. Comput. Sci. Appl.*, vol. 9, no. 11, pp. 196–200, 2018.

[17] S. Harshitha, D. Ranjan, J. Madhushree, B, and L. Ashwini, "A Systematic Approach for Image Encryption Using Chaotic 2D Logistic Map Using MATLAB," *Int. J. Eng. Res. Technol.*, vol. 6, no. 13, pp. 1–4, 2018.

[18] M. Sharma, "Image encryption based on a new 2D logistic adjusted logistic map," *Multimed. Tools Appl.*, vol. 79, no. 1–2, pp. 355–374, 2020.

[19] X. Huang, L. Liu, X. Li, M. Yu, and Z. Wu, "A new two-dimensional mutual coupled logistic map and its application for pseudorandom number generator," *Math. Probl. Eng.*, vol. 2019, pp. 1–10, 2019.

[20] 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.

[21] 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.

[22] 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.

[23] https://favpng.com/png_view/three-dimensional-prism-triangle-polyhedron-face-vertex-line-segment-png/f2kevVAA, Accessed Jul., 2021.

[24] J. Alireza, "Robust Encryption Schemes for 3D Content Protection," Thesis (Ph.D. Doctorate), Griffith University, 2016.

[25] 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.

[26] 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.

[27] "Free3D," https://free3d.com/3d-models/obj, Accessed Feb., 2021.

[28] 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.

[29] M. M. Laftah, "3D Model Watermarking based on Wavelet Transform,". *Iraqi Journal of Science*, vol. 62, no. 12, pp.4999-5007, 2021.

[30] N. A. Ali, "Watermarking in 3D Models Using Depth Path,". *Iraqi Journal of Science*, vol. 60, no. 11, pp.2490-2496, 2019.

[31] M. Gafsi, M. A. Hajjaji, J. Malek, and A. Mtibaa, "Efficient Encryption System for Numerical Image Safe Transmission," *J. Electr. Comput. Eng.*, vol. 2020, 2020.

[32] B. Yousif, F. Khalifa, A. Makram, and A. Takieldeen, "A novel image encryption/decryption scheme based on integrating multiple chaotic maps," *AIP Adv.*, vol. 10, no. 7, 2020.

[33] A. Elghandour, A. Salah, and A. Karawia, "A new cryptographic algorithm via a two-dimensional chaotic map," *Ain Shams Eng. J.*, 2021.