A Novel Method of 3D Image Steganography Using LZW Technique and Chaotic Neural Network

B. Geetha vani[1]

Research scholar, Dept. of CSE, JNTU Kakinada. AP, India.

E. V. Prasad[2]

Professor, Dept. of CSE & Rector JNTU Kakinada, AP, India

Abstract

In this paper a novel Image Steganography for 3D Images is proposed. As the volume for 3D images is high compared to 2D images, high capacity of Information can be embedded inside the 3D images. The proposed Steganography method is based on embedding the compressed encrypted secret text into spatial features of 3D images. The vertex information of 3D images is represented in real numbers. The mantissa part of the vertex representation is used for embedding the secret data. To provide high security to the information, the information is compressed using LZW technique and then encrypted using Chaotic Neural Network. The encryption data in unreadable form is embedded inside the 3D image. On the receiver side the extracted information is decrypted and then decompressed using LZW technique. The qualitative evaluation has resulted with high PSNR and Security values.

Keywords:

Steganography, Chaotic Neural Network, 3D images, LZW technique

1. Introduction

Information hiding has recently become an important research topic and has drawn a lot of attention. Information hiding encompasses a broad range of applications in which the messages are embedded into covert media for different purposes. The main types of information hiding are watermarking and Steganography. Both techniques are used to imperceptibly convey private information by embedding data into various digital media.

Watermarking focuses on ownership authentication or content protection, where as Steganography hides messages so that no one, apart from the sender and intended receiver, suspects the existence of a message. Compared with the cryptography, the advantage of Steganography is that messages do not attract attention to themselves. Cryptography protects the contents of a message, whereas Steganography protects both messages and communicating parties.

In general, secret information is hidden in another seemingly innocuous host to achieve covert communication in the network. To successfully conceal the existence of secret messages, the host medium is usually chosen in the manner of being nothing relation with the hidden information. With the development of 3D hardware, 3D computing or visualization has become very popular and has lead to widespread use of 3D models in various applications such as digital archives, entertainment and game industries. Thus, 3D models can act innocuous-looking hosts for hiding other types of digital content. The triangle mesh is commonly used in 3D model representation and is supported by various graphic packages and libraries. Usually, a 3D model is represented by elementary elements that include vertex coordinates, texture coordinates and connectivity information. This un-regular representation is highly different from typical sampling representation such as digital images or videos. Thus the information hiding schemes for traditional cover media are not suitable for 3D models.

In this paper, a novel three stage Steganography technique is proposed for embedding the data in 3D model. Compressing the message using LZW technique at the first stage, encrypting the compressed secret message data using Chaotic Neural Network at the second stage and embedding the encrypted data into the vertex positions of the 3D image at the third stage. Similarly on the receiver side, the secret text is extracted from the 3D image and then the extracted text is decrypted and then decompressed to obtain the secret message.

The rest of the paper is organized as follows. Section 2 contains the review of related work in the area. The proposed method is presented in section 3. Construction and Working of Proposed Algorithm is presented in section 4. The result analysis and conclusions are provided in sections 5 and 6 respectively.

2. Review of Literature

Many Steganography methods [3-5] and watermarking methods [8,14,15] have been proposed for 3D polygon models in the literature. Most of the Steganography techniques for 3D models are inspired by the well known concept of quantization index modulation (QIM) proposed by Chen and Wornell [19]. The basic idea of QIM is to split the host media into two states, that is, state ‘0’ and state ‘1’. The elementary elements of host media are

Manuscript received June 5, 2013
Manuscript revised June 20, 2013

quantized to the nearest state region according to the embedded messages. Cayre and Macq proposed a 3D data hiding scheme based on substitution procedure in the spatial domain [4]. Chao. et. al. Proposed a High Capacity steganography Scheme for 3D mesh model [3]. Chao's model is based on the multi layered embedded scheme to hide the secret message with low distortion. Wang and Chen presented a multi level embedding procedure for obtaining high capacity, with three levels of embedding called sliding, extending, and rotating based on slightly shifting vertex positions [5]. This paper presents a simple technique of altering the vertex information for embedding the data.

3. Proposed Method

This Paper proposes a novel method for high capacity information communication through the process of 3D Steganography using two different ways. One makes use of compression technique and the other chooses the 3D image as the cover media. The secret information is compressed using LZW technique [20,23] which is a lossless dictionary based technique where the size of the dictionary is based on the length of the information. The compressed information is encrypted using Chaotic Neural Network [17,18] and is embedded into the 3D image. The goal is to embed high capacity of information in the 3D image with less distortion and to make it easy to retrieve the secret information at receiver end by the right people. For a 3D image represented by M (v,c) , where v is the vertex set and c is the connectivity relationship of the image M, the secret information is embedded by inducing a small displacement on a subsets of v with a result to achieve M'(v',c'). A vertex v is denoted as v(x1, x2, x3) and v' (x1',x2',x3') before and after embedding the secret information.
The proposed algorithm can be better explained through the below process and through the flow charts given in Fig.1 and Fig.2.

Embedding Process

1. The subset of vertices v for embedding the secret information is identified and let W represents this subset.
2. Obtain the secret information and compress it using LZW technique.
3. Encrypt the compressed text using Chaotic Neural Network.
4. For all the vertices in W, embed the secret information by changing the mantissa part of the vertices to convert $v(x_1,x_2,x_3)$ to $v'(x_1',x_2',x_3')$.

Extraction Process

1. Obtain the subset of vertices v and extract the secret information from the mantissa of the vertex of the stego model.
2. Decrypt the secret information using Chaotic Neural network.
3. Decompress the decrypted information using LZW technique and obtain the information.

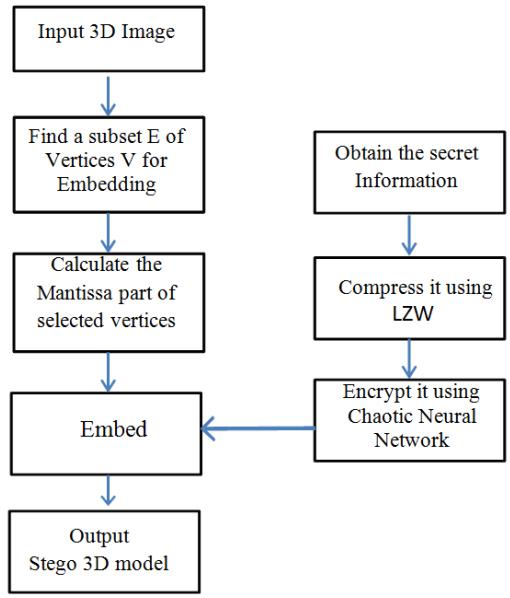

Fig.1 Flow chart of Embedding Process

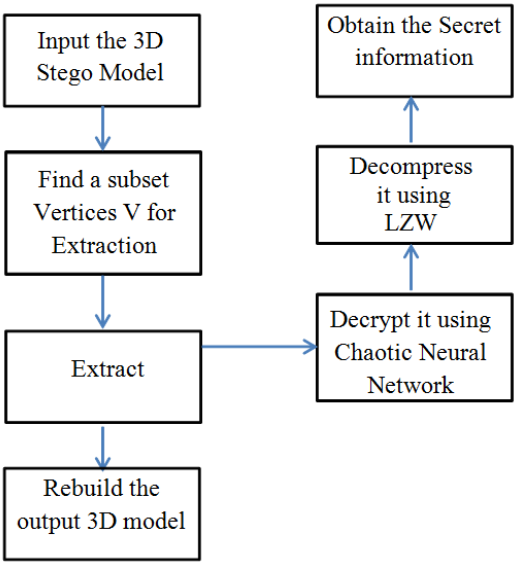

Fig.2 Flow chart of extraction Process

4. Construction and Working of Proposed Algorithm

The Proposed Algorithm can be explained using the below modules.

A. Lossless Compression and Decompression

In the proposed method, LZW technique is used for compression and decompression of information. LZW (Lempel-Ziv-Welch) is a general compression algorithm which works for any type of data. It belongs to LZ78 family of Lempel Ziv scheme [23]. LZW creates a dictionary which is a table of string which occurs commonly in the original plain text and replaces the re-occurring text with the reference of the existing data in the dictionary. This dictionary is formed during compression at the same time at which the data is encoded and during decompression at the same time the data is decoded. LZW technique is an adaptive compression algorithm which decompresses the data at the receiver side without the transmission of the dictionary generated during the compression to the receiver, thus reducing the complexity and time required.

B. Encryption and Decryption Module

In the proposed method, Encryption and Decryption is performed using Chaotic Neural Network [1]. Hopfield Chaotic Neural Network is a suitable environment for cryptography because of its interesting properties like ergodicity, sensitive dependence of initial conditions and control parameters and high speed of information transmission. Yu et al. [18] designed a delayed chaotic neural network based cryptosystem, which makes use of the chaotic trajectories of two neurons to generate basic binary sequences for encrypting plaintext. In Chaotic Neural Network, the weights and biases are determined by a chaotic sequence, and are used to mask or to scramble the original information. The encryption algorithm [1] is used for obtaining the cipher text. The use of Chaotic Neural Network is advantageous as it consumes less computational power and the sequence generated by using this is unpredictable leading to high security.

C. Embedding and Extraction Module

Data Embedding

The string that have to be embedded is S = N+ encrypted text, where N is the length of the encrypted string and the N is appended to the first position of string S. For a 3D model M (v, c), first, set all its vertices as fixed vertices, then traverse the whole model vertices starting from a predefined vertex, for example v1. The subset of vertices used for embedding E is the N+1 number of vertices starting from v1. In the proposed method, the data is hidden in the mantissa part starting from the Δ position of the mantissa part of the vertices. After embedding the data in the mantissa part, the vertices will adjust its position slightly but the relation with the neighboring vertices will be maintained. The vertices traversed for embedding are limited to the size of the compressed encrypted string.
For each vertex v in E, starting from Δ position of the mantissa part, the secret data in the real number form will be embedded as follows

For $\Delta = 1$

$$v'_i = \lfloor v_i \rfloor + S_i/1000 \quad \text{if} \quad v_i > 0$$
$$v'_i = \lfloor v_i \rfloor - S_i/1000 + 1 \quad \text{if} \quad v_i < 0$$

Where i=1, 2, 3... K; K=N+1 ------ Eq.1

To embed the data in the mantissa part, the mantissa truncation of the original vertices due to the limited precision of the vertices is required. For each vertex a 3 bit data is embedded into it.

Data Retrieval

To retrieve the embedded data, the reverse process of embedding is carried out. The mesh traversal for data extraction is ordered by the first vertex. The altered vertices alone are traversed for data extraction. The numbers of altered vertices are obtained from the first vertex data. The extraction of data from the vertex is done from the mantissa part of the altered vertex. The data is extracted using Eq.2.

$$S_i = (v'_i - \lfloor v'_i \rfloor) \times 1000 \quad \text{for} \quad v'_i > 0$$
$$A_i = | v'_i |$$
$$S_i = (A_i - \lfloor A_i \rfloor) \times 1000 \quad \text{for} \quad v'_i < 0$$

Where i=1, 2, 3…. K; K=N+1 -------- Eq.2

The process of steganography has been better explained in Figure 1 and Figure 2. It explains the process of creating the stego image from the plain text and retrieving the secret text from the stego image.

5. Results and Analysis

Experiments are performed to prove the efficiency of the proposed algorithm. A GUI was developed using Matlab 7.14.0.739. The Quantitative performance of the proposed algorithm is evaluated based on Peak signal to noise ratio

(PSNR) and Mean Square Error (MSE) of the vertices which is given in equations 3 and 4 respectively.

$$PSNR = 10\log_{10}\left(\frac{255^2}{MSE}\right) \quad \text{---------} \quad \text{Eq.3}$$

$$MSE = \frac{\sum_j (V'_j - V_j)2}{V} \quad \text{---------} \quad \text{Eq.4}$$

Where vj and vji refers to original vertex and changed vertex values, V is the size of Vertex set.

The qualitative performance of the proposed algorithm is tested on various 3D datasets obtained from [10,11] and the same is shown in Fig 9, Fig 10. These test models are with different numbers of vertices and different shapes and used in different applications. The secret text is of length 1000 bytes is taken for testing. Performance was calculated in terms of PSNR, MSE. Results are given in Table I. It is observed that the stego model is identical to the original model.

TABLE I COMPARISON OF PERFORMANCE OF PROPOSED ALGORITHM ON VARIOUS 3D NON-RIGID IMAGES WITHOUT TEXT COMPRESSION

Input image	Vertex	Faces	PSNR	MSE
Cat	3400	6774	62.8802	0.0338
Centaur	3400	6796	63.7005	0.0280
David	3400	6778	62.1852	0.0396
Dog	3400	6773	63.6628	0.0282
Gorilla	2046	3993	59.9295	0.0666
Horse	3400	6796	63.1663	0.0316
Lioness	3400	6189	62.3179	0.0384
Michael	3400	6783	62.5476	0.0365
Sea Horse	2194	4311	60.6730	0.0561
Victoria	3400	6767	62.3728	0.0379
Wolf	3400	6796	62.7359	0.0349

Table II COMPARISON OF PERFORMANCE OF PROPOSED ALGORITHM ON VARIOUS 3D RIGID IMAGES WITHOUT TEXT COMPRESSION

Input image	Vertex	Faces	PSNR	MSE
Bunny	34835	69666	72.7026	0.0035
Casting	5096	10224	63.5770	0.0288
Cow	2904	5804	61.8143	0.0432
Crank	50012	100056	74.2818	0.0024
Dragon	50000	100000	74.8691	0.0021
Elephant	24955	49918	70.5266	0.0058
Hand	36619	72958	72.1574	0.0040
Horse	112642	225280	78.7016	0.0008
Rabbit	70658	141312	76.1197	0.0016
Ramasses	826266	1652528	87.9863	0.0001
Venus	100759	201514	77.7970	0.0011

Table III COMPARISON OF PERFORMANCE OF PROPOSED ALGORITHM ON VARIOUS 3D NON-RIGID IMAGES WITH TEXT COMPRESSION

Input image	Vertex	Faces	PSNR	MSE
Cat	3400	6774	65.6257	0.0179
Centaur	3400	6796	66.5343	0.0146
David	3400	6778	64.5917	0.0228
Dog	3400	6773	67.8742	0.0107
Gorilla	2046	3993	62.4334	0.0374
Horse	3400	6796	66.3486	0.0152
Lioness	3400	6189	64.8500	0.0215
Michael	3400	6783	65.5863	0.0181
Sea Horse	2194	4311	63.6317	0.0284
Victoria	3400	6767	65.3874	0.0190
Wolf	3400	6796	65.3399	0.0192

Table IV COMPARISON OF PERFORMANCE OF PROPOSED ALGORITHM ON VARIOUS 3D RIGID IMAGES WITH TEXT COMPRESSION

Input image	Vertex	Faces	PSNR	MSE
Bunny	34835	69666	75.8580	0.001700
Casting	5096	10224	66.1694	0.015800
Cow	2904	5804	65.2920	0.019400
Crank	50012	100056	77.3987	0.001200
Dragon	50000	100000	77.4870	0.001200
Elephant	24955	49918	72.9979	0.003300
Hand	36619	72958	74.5891	0.002300
Horse	112642	225280	81.0190	0.0005183
Rabbit	70658	141312	78.4168	0.0009436
Ramasses	826266	1652528	90.9290	0.0005291
Venus	100759	201514	80.4316	0.0005933

TABLE V CPU TIME FOR THE PROPOSED ALGORITHM

Non-rigid images			Rigid images		
Input	**Without Compression**	**With Compression**	**Input**	**Without Compression**	**With Compression**
Cat	0.0312	2.3088	Bunny	0.0780	2.3244
Centaur	0.0312	2.5272	Casting	0.0312	2.3556
David	0.0312	1.6380	Cow	0.0156	2.4960
Dog	0.0312	1.6380	Crank	0.1404	2.0124
Gorilla	0.0156	2.4336	Dragon	0.1404	2.4336
Horse	0.0156	1.9188	Elephant	0.0936	2.5584
Lioness	0.0312	2.1528	Hand	0.0780	2.3244
Michael	0.0312	2.5584	Horse	0.2964	2.5584
Sea horse	0.0156	2.4492	Rabbit	0.2496	2.6832
Victoria	0.0312	2.4648	Ramasses	2.9796	5.4288
Wolf	0.0156	2.2776	Venus	0.2496	2.7768

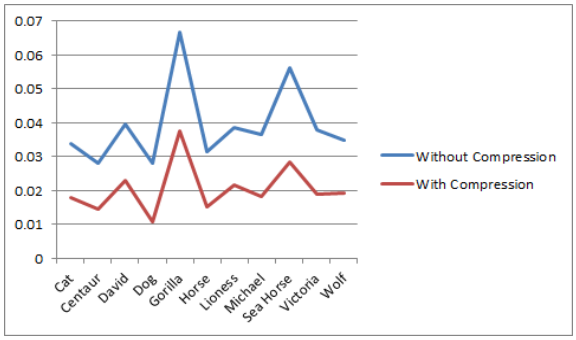

Fig.3 MSE of the stego model of the proposed algorithm with and without compression for 3D non-Rigid models

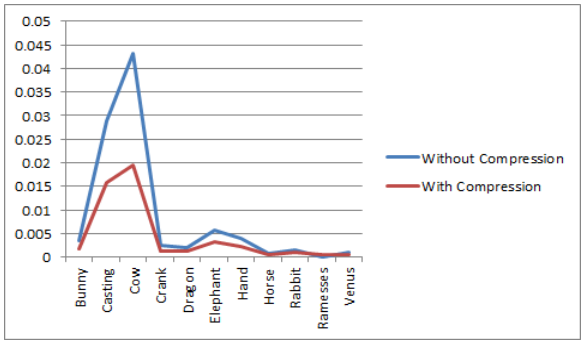

Fig.4 MSE of the stego model of the proposed algorithm with and without compression for 3D Rigid models

Figure 3 and Figure 4 shows the comparison of MSE of the 3D stego Model of the proposed algorithm with and without compression with the cover 3D model for various 3D Non Rigid Models and 3D Rigid Models. Figure 5 and Figure 6, shows the comparison of PSNR of the 3D stego Model of the proposed algorithm with and without the compression with the cover 3D model for various 3D Non Rigid Models and 3D rigid models.

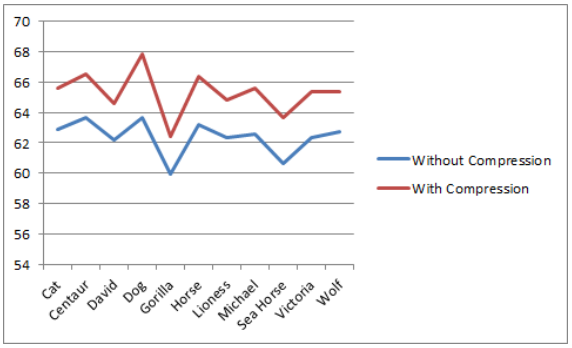

Fig.5 PSNR of the stego model of the proposed algorithm with and without compressionfor 3D non-Rigid models

The Images used for Qualitative Performance are shown below.

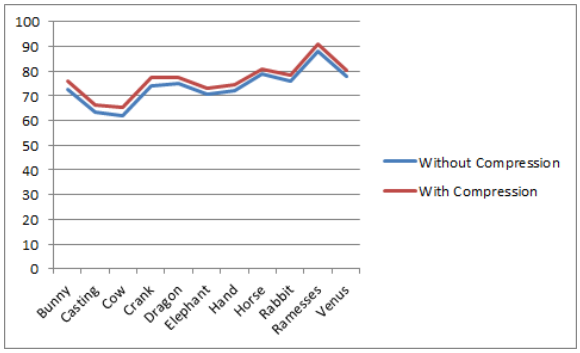

Fig.6 PSNR of the stego model of the proposed algorithm with and without compression for 3D Rigid models.

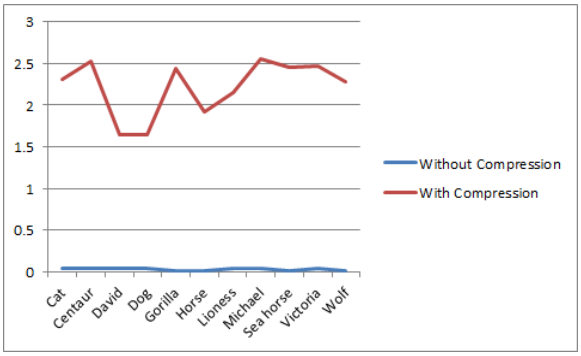

Fig.7 Processing time taken for the proposed algorithm with and without compression for 3D Non-Rigid models

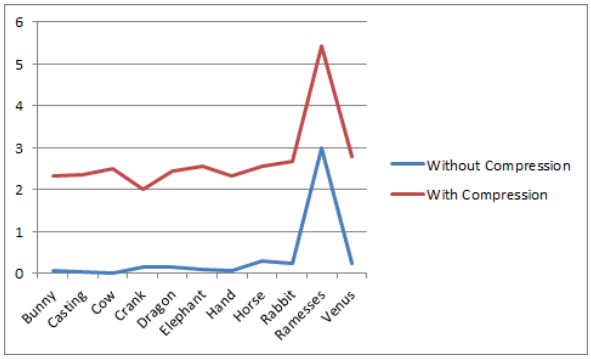

Fig.8 Processing time taken for the proposed algorithm with and without compression for 3D Rigid models

From the above graphs, better PSNR and low MSE is obtained for the proposed algorithm.

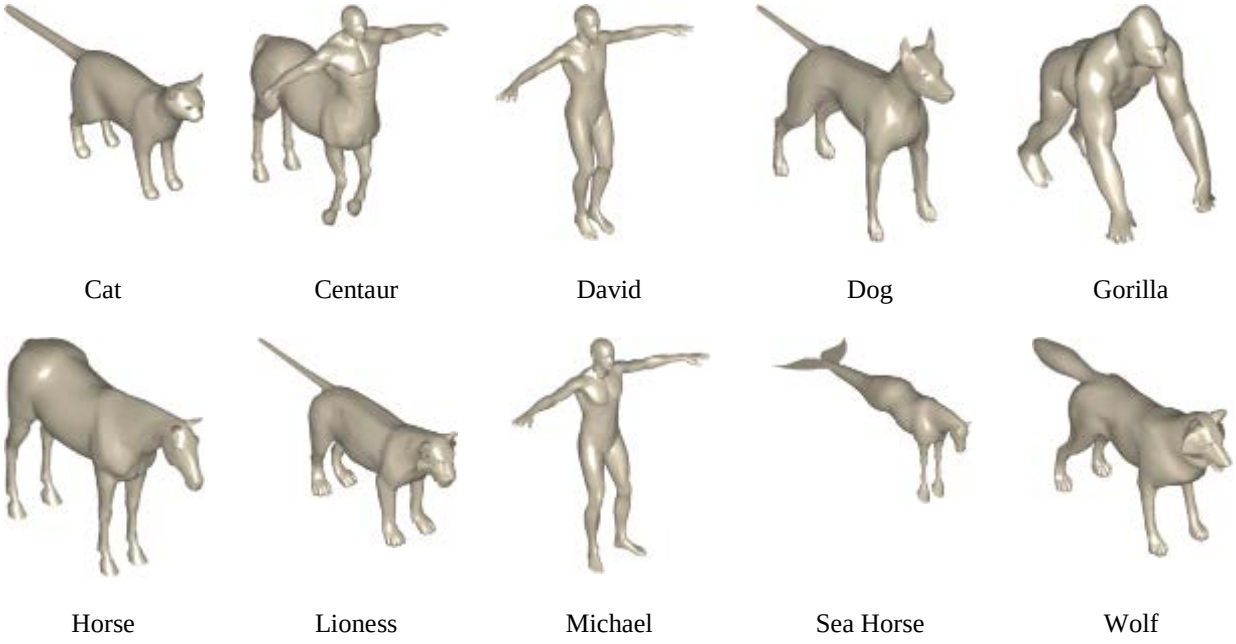

Fig.9 3D meshes used for Qualitative Performance for Non-Rigid models

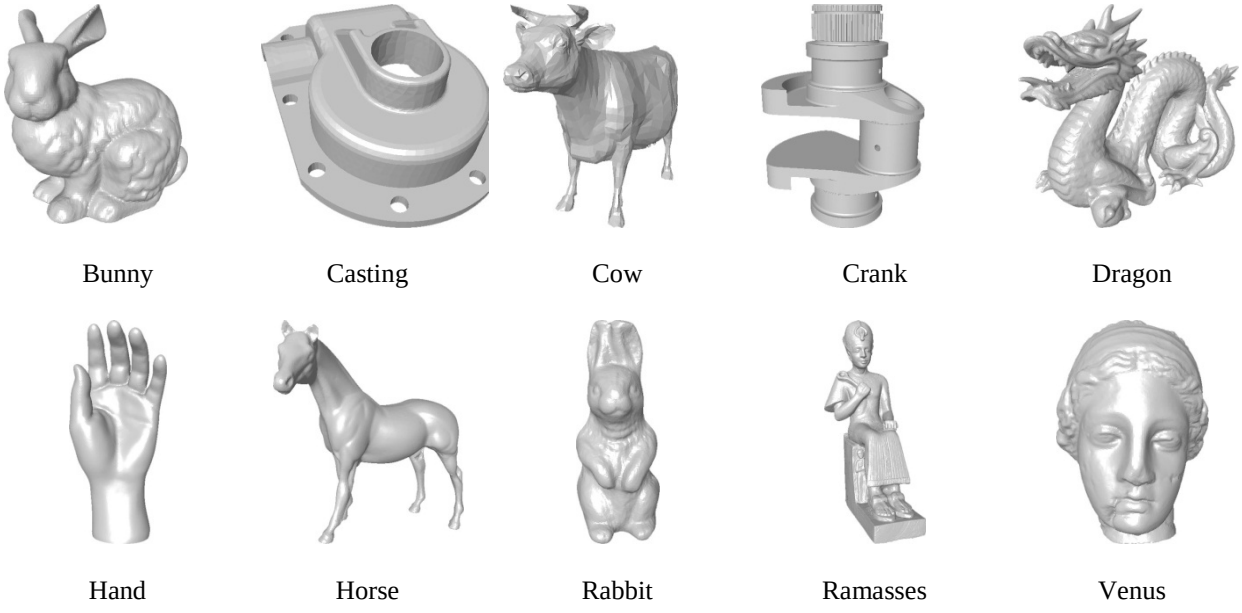

Fig.10 3D meshes used for Qualitative Performance for Rigid models

6. Conclusion

In this Paper, a novel method of 3D Image Steganography algorithm that makes use of spatial features is presented. Unlike other approaches, the proposed method uses simple vertex calculations for embedding the information. Here, Chaotic Neural Network and LZW techniques are used for encryption and compression of the information before embedding it into the 3D model. For a secret data of length 1000 bytes, experiments are conducted and the qualitative performance has been analyzed using PSNR and MSE. The PSNR and MSE values found to be dependent on the amount of data to be embedded and also on the size of the image. The CPU time required for embedding the information with compression and without compression is recorded. The Proposed system shows better performance in terms of both capacity and security. In future, it is proposed to extend the work for embedding the data in multiple layers of 3D model. Future research is also expected to explore and analyze the relationship between message length, visual effect, and the resulting robustness.

References

[1] B. Geetha vani, E. V. Prasad, "Scalable and Highly Secured Image Steganography based on Hopfield Chaotic Neural Network and Wavelet Transforms". *International Journal of Computer Science Issues*, Vol.10, No.3, pp 82-90, May 2013.

[2] W. Y. Hsu, "Application of competitive hopfield neural network to brain-computer interface systems", *International Journal of Neural Systems*, Vol.22, No.1, pp.51-62, 2012.

[3] Min-Wen Chao, Chao-hung Lin, Cheng-Wei Yu, Tong-Yee Lee, "A High Capacity 3D algorithm", *IEEE Transactions On Visualization And Computer Graphics*, Vol.15, No.2, pp. 274-284, April. 2009.

[4] F. Cayre, B. Macq, "Data hiding on 3-D triangle meshes", *IEEE Trans. Signal Processing*, Vol.51, No.4, pp.939-949, 2003.

[5] C. M. Wang, Y. M. Cheng, "An efficient information hiding algorithm for polygon models", *EU-ROGRAPHICS*, Vol.24, No.3, pp.591-600, 2005.

[6] Juneja M, Sandhu P.S, "Designing of robust image steganography technique based on LSB insertion and encryption", *Advances in Recent Technologies in Communication and Computing*, pp.302-305, Oct. 2009.

[7] Chen, T.S., Chang C.C., Hwang, M.S. "A virtual image cryptosystem based upon vector quantization", *IEEE transactions on Image Processing*, Vol.7, No.10, pp. 1485 – 1488, 1998.

[8] Kai Wang, Xiyan He, "A Benchmark for 3D Mesh Watermarking", *IEEE Shape Modeling International conference*, pp 231 -235, Oct. 2010.

[9] I-Ling Chung, Chang-Min Chou, Din-Chang Tseng, "A Reversible Steganography Scheme for 3D Mesh Models", *Proceedings of APSIPA Annual Summit and Conference, Sapporo, Japan*, pp 4 -7, Oct.2009.

[10] http://tosca.cs.technion.ac.il/book/resources_data.html

[11] http://liris.cnrs.fr/meshbenchmark/

[12] M. W. Chao, C. H. Lin, C. W. Yu ,T. Y. Lee, "A high capacity 3D Steganography algorithm", *IEEE Transactions on Visualization and Computer Graphics*, Vol.15, pp.274-284, 2009.

[13] Y. M. Cheng, C. M. Wang, "A high-capacity steganographic approach for 3D polygonal meshes", *The Visual Computer*, Vol.22, pp.845-855, 2006.

[14] Cho. J. W, Prost. R, Jung. H. Y, "An Oblivious watermarking for 3D Polygonal meshes using distribution of vertex norms", *IEEE Trans. Signal Processing*, Vol.55, No.1, pp.142-155, 2005.

[15] Zafeiriou.S, Tefas.A, Pitas.I, "Blind robust watermarking schemes for copyright protection of 3D mesh objects", *IEEE Transactions on Visualization and Computer Graphics*, Vol.11, No.5, pp.596-607, 2005.

[16] Qing Huang, S.S.Iyengar, Xin Li, "3D Surface Steganography using geometry images", *International conference on computer science and education(ICCSE2011), Singapore*, pp.866-870, Aug 3-5, 2011.

[17] Harpreet Kaur and Tripatjot Singh Panag, "cryptography using chaotic neural network", *International Journal of Information Technology and Knowledge Management*, Volume 4, No. 2, pp. 417-422, Jul-Dec 2011.

[18] Yu W, Cao J. "Cryptography based on delayed neural networks". *Physics Letter A*; pp.356:333, Aug. 2006

[19] A B. Chen and G. W. Wornell, "Quantization index modulation: A class of provably good methods for digital watermarking and information embedding", *IEEE Trans. Inf. Theory*, Vol.47, No.4, pp.1423-1443, 2001.

[20] Senthil Shanmugasundaram, Robert Lourdusamy, "A Comparative Study Of Text Compression Algorithms" *International Journal of Wisdom Based Computing*, Vol. 1, No.3, pp 68-76, Dec 2011.

[21] I-Ling chung, Chang Min Chou and Din Chang Tseng "A Reversible Steganography scheme for 3D mesh models", *Proceedings of APSIPA Annual Summit and Conference*, Sapporo, Japan, Oct 4-7 2009.

[22] Chao-Hung Lin, Min-Wen Chao, Jyun-Yuan Chen, Cheng-Wei Yu, and Wei-Yen Hsu, "High Capacity distortion free information hiding algorithm for 3D polygon models", *International Journal of Innovative Computing, Information and Control*, Vol.9, No.3, pp.1321-1335, Mar.2013.

[23] Haroon Altarawneh, Mohammad Altarawneh "Data compression techniques on text files: A comparison study", *International Journal of Computer Applications*, Vol.26, No.5, pp 1075-1087, Jul. 2011.

B. GeethaVani has received the B.Tech degree in Computer Science and Engineering from JNTU Hyderabad in 1993 and M. Tech degree in Computer Science and Engineering from JNTU Hyderabad in 2003. Currently pursuing Ph.D from JNTU Kakinada, India. Research interests include Theory of Computation, Artificial Neural Networks, Image Processing and Network Security.

Dr. E.V.Prasad has received Ph.D degree in Computer Science and Engineering from I.I.T, Roorke, India. He is having 34 years of experience in teaching. He joined in JNTU College of Engineering in the year 1979 and served in various positions like Head of the Department, Vice Principal, Principal, Director of IST**,** Registrar and presently he is the Rector, JNTU Kakinada, India. He has taught over 16 courses in CSE and has guided 7 Ph.D students successfully and presently supervising 9 Ph.D candidates. He is the Co author of six books and published more than 8 dozen papers in national and International journals and conferences. His research interests include Parallel Computing, Data Mining, and Information Security.