International Journal of Clinical & Medical Informatics

ISSN: 2582-2268 **Research** | Vol 1 Iss 1

Secured Watermarked Multi Secret Sharing Scheme of 3D Models

Modigari Narendra[1*], M L Valarmathi[2], and L Jani Anbarasi[3]

[1]Department of CSE, Sri Ramakrishna Institute of Technology, India

[2]Department of EEE, Alagappa Chettiar Government College of Engineering and Technology, India

[3]Department of CSE , Agni College of Technology, India

[*]**Corresponding author:** Modigari Narendra, Department of CSE, Sri Ramakrishna Institute of Technology/Anna University, Coimbatore, India, E-mail: modigarinarendra@gmail.com

Abstract

Visual Secret Sharing is a technique for securing secrets that involves the distribution of secret into many shadows. In this paper an efficient, secure, watermark based verifiable (t, n) secret sharing scheme using YCH model is proposed for multiple 3D models. 3D models are securely shared among 'n' participants such that less than 't' cannot reconstruct the original secret. Watermark is embedded into original 3D model after which secret sharing is performed. During reconstruction at least 't' shadows are pooled to reconstruct the multiple 3D models. Various experimental analyses were performed to detect the security measure of the 3D model. The feasibility of the watermark reconstruction is demonstrated for various 3D models. The simulation results show that the secrets and the watermark are retrieved from the shares without any loss.

Keywords: ***Visual secret sharing; 3D graphics; Cryptography***

Received Date: February 02, 2018; **Accepted Date:** March 15, 2018; **Published Date:** March 23, 2018

Introduction

One of the considerable difficulties in information security is to outline improvised and effective algorithm that are important to keep the framework secure, especially while exchanging information through untrusted systems, for example, the web. In standard encryption schemes, the encoded information is set in a single location. In any case, if a hacker finds the loop holes, it is very much easy to hack the data from a central storage which affects confidentiality and integrity of the data. The Secret sharing scheme does not experience the ill effects of these issues, in light of the fact that the secret image is changed over into "n" shadows and is put away at various different locations.

Secret sharing is the way towards partitioning a secret image into n shadows. A (t, n) secret sharing, shares the secret 3D model into n shadows, where at least "t" shadows are pooled to remake the secret. By examining less than t shadows, data about the secret cannot be obtained. Tremendous development in computer and information technology and data innovation organization needs the utilization for 3d models in different areas, similar to manufacturing, medical imaging, virtual reality, animations etc. The protection of these 3D models is highly essential since various studies says that people are willing to license their product

and could see how it works digitally, when it is not physically available for inspection.

Along these lines, various research works has been completed to design strong and secure 2D image protection schemes, yet 3D models have got less consideration. So far numerous 2D image protection schemes like Steganography and other encryption plans have been proposed. Shamir [2] secret sharing scheme is based on the Lagrange's Interpolation polynomial whereas Blakley [1] secret sharing scheme is based on the intersection of affine hyper planes. Various mathematical models have been proposed for numeric and text data encryption. These strategies are not best suited for multimedia related data because of the huge data and their pixel representation. Secret sharing scheme works good only for honest participants. To avoid the malpractice of the participants, watermarking is performed to the 3D models using wavelet transformation technique. This watermarked 3D model is securely shared among participants using YCH scheme.

In the most recent decade, different secret sharing techniques have been proposed in the literature [12-14]. The size of the created shadows is same as that of the secret. Thien and Lin proposed secret sharing technique where the shadow size is 1/t of that of secret, while Wang and Su decreased the extent of shadows size as 40% smaller than the Thien and Lin approach.

To avoid suspicious intruder most of the secret sharing techniques [14-17] uses steganography method which embeds the shadows into a host image. The stego images avoid the suspicion of intruders. Elsheh et al. [18] proposed the secret sharing technique which securely shares the single 3D model using Shamir and Blakely scheme. Verifiable multi secret sharing technique prevents cheating of a participant or a dealer [6,8-11]. Shao & Z. Cao [4] proposed a multi secret sharing verifiable method based on YCH scheme, where the shadows are distributed through a secure channel. Zhao [5] proposed a practical verifiable multi secret sharing scheme with the use of RSA and Diffie Hellman concepts, where the verification process is performed by both the dealer and the participants.

In this paper, secret sharing of multiple 3D objects, a practical verifiable watermarked multiple secret sharing scheme is imposed which is based on the YCH scheme. The RSA and Diffie Hellman key concepts, provides the verifiability property for both the participants and the dealer and furthermore stays away from the need of a secure channel. The reminder of the work is organized as follows. In Section 2, the traditional secret sharing techniques and watermarking technique is discussed. In Section 3, multiple 3D Secret Sharing models and the algorithms are explained. In Section 4, the simulation results for various 3D models are provided. The analysis and conclusion are given in Section 5.

Related Work

This section deals with traditional secret sharing schemes, such as Shamir's secret sharing, and multiple secret sharing techniques for 3D modeling and Discrete Wavelet Transform scheme are as follows:

Secret sharing schemes

Shamir and Blakley introduced secret sharing in the year 1979. To distribute a secret 'S' among 'n' number of participants, a (t,n) Secret sharing is used such that at least 't' participants could reconstruct the secret 'S', but less than 't' participants could not obtain it.

This plan is said to be immaculate just if participants less than 't' can't recover the secret. Shamir's secret sharing methodology utilizes a secret "S" and a prime number "m" to produce a $(t-1)^{th}$ degree polynomial, which is given underneath:

$$F(X) = S + C_1X^1 + \cdots + C_{t-1}X^{t-1} \bmod m \quad \text{……..(1)}$$

Where, $C_1, C_2 \ldots C_{t-1}$ are random integers Coefficients within the range [0, m-1].

The secret sharing shadows are calculated from equation (1) as follows:

$$Y_1 = F(K_1)\, Y_2 = F(K_2) \cdots Y_n = F(K_n)$$

Where $Y_{i(1\le 1\le n)}$ represents the shadow value, calculated using the secret key $K_{i(1\le 1\le n)}$ for each participant, and is securely issued to the participants by the owner. At least 't' participants pool their shadows, to reconstruct the secret and less than 't' shadows cannot retrieve the secrets. Lagrange interpolation technique uses the secret shadow and the participant's key to reconstruct the secret without loss is given as follows.

$$h(x) = \sum_{i=1}^{t} Y_i \prod_{j=1, i\neq j}^{t} \frac{x - k_j}{k_i - k_j} \bmod m$$

Multiple secret sharing schemes

Multi secret sharing scheme which is proposed by Yang et al. [19] has one way function *f(r, k)*. The function f*(r, k)* denotes any two variable one-way functions that map a secret key *k* and a random value r onto a bit string *f*(r, *k)* of a fixed length. If *r* and *k* are given it is easy to compute *f(r, k)*. However, it is hard to compute:

- *r*, given *k* and *f(r, k)*,
- *f(r, k)* for any r, without any knowledge of *k*,
- *k*, given *r* and *f(r, k)*

Let $S_1, S_2 \ldots S_P$ denotes P secrets to be shared among n participants. Initially, the dealer chooses n secret keys $k_1, k_2 \ldots k_n$ in a random manner, and issues them to n authenticated participants by a covert channel. Then the dealer performs the following steps:

- Case P ≤ t

1. Choose a prime m and construct $(t-1)^{th}$ degree polynomial h(x) mod m, where 0< S1, S2...Sp, c1, c2, ct-p < m as follows: $h(x) = S_1 + S_2x^1 + \cdots + S_px^{p-1} + C_1x^p + C_2x^{p+1} + \cdots C_{t-p}x^{t-1}$ ….(3)
2. Compute *Yi=h (f(r, ki))* mod m for i = 1, 2. . . n
3. Distribute (*r*, Yi) to the participants.

- Case *P >t*

1. Choose a prime m satisfying S1, S2...S_P < m, then construct the following $(P-1)^{th}$ degree polynomial h(x) mod m: $h(x) = S_1 + S_2x^1 + \cdots + S_px^{p-1}$ …..(4)
2. Compute $Y_i = h(f(r, k_i))$ mod m for i = 1, 2. . . n…
3. Compute h (i) mod m for i = 1, 2. . . P-t
4. Distribute (r, Y_i, h (i)) to the participants.

For a (t, n) threshold scheme, Atleast t participants' secret shadows are pooled to recover the P secrets $S_1, S_2 \ldots S_p$. The Polynomial h(x) mod m can be determined uniquely as follows:

- Case *P ≤ t*

$$h(x)=\sum_{i=1}^{t}Y_i\prod_{j=1,\ j\neq i}^{t}\frac{x-f(r,k_j)}{f(r,k_i)-f(r,k_j)}\bmod m$$

$$=S_1+S_2x^1+\cdots+S_px^{p-1}+C_1x^p+C_2x^{p+1}+\cdots C_{t-p}x^{t-1}\bmod m \qquad \ldots\ldots(5)$$

- Case P>T

$$h(x)=\sum_{i=1}^{t}Y_i\prod_{j=1,\ j\neq i}^{t}\frac{x-f(r,k_j)}{f(r,k_i)-f(r,k_j)}+\sum_{i=1}^{p-t}Y_i\prod_{j=1,\ j\neq i}^{p-t}\frac{x-j}{i-j}\bmod m=S_1+S_2x^1+\cdots+S_px^{p-1}\bmod m \qquad \ldots\ldots.(6)$$

3D Modelling

3D modelling is completely based on geometry, where it is partially concerned with spatial relationship, particularly analytical geometry, which expresses these relationships in terms of algebraic formulas. In 3D model each point has three coordinates, which are called as axes labelled (x, y, z), where x, y, z represent the height, length and breadth respectively. The values of x, y and z will be in the range corresponding to $0\le x\le H, 0\le y\le L, 0\le z\le B$, where H, L, and B are the maximum height, length and breadth respectively. Generally, 3D models are represented as a polygons or mesh. A mesh is a collection of edges, faces and vertices that describe the shape of a 3D object. A vertex represents a point in the 3D model. An edge is a straight line which connects any two vertices. A face is a flat surface enclosed by edges. A face is any of the polygons of the 3D model that makes up its boundaries. Meshes can be represented in different ways based on how the vertices' edge and face information are stored. The graphical model of a simple 3D mesh is shown in Figure 1.

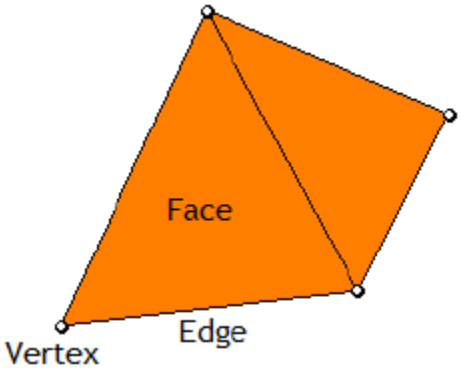


Figure 1: Graphical model.

Discrete wavelet transform

Watermark embedding in the wavelet domain plays a vital role in securing the ownership possession. Discrete Wavelet Transform is an orthogonal change which assumes a noteworthy part in different applications like feature extraction, speech recognition and biometric watermarking, and so forth. DWT breaks down the image progressively including both frequency and spatial segments of an image. Discrete Wavelet Transform segregates an image into vertical (LH), approximation (LL), horizontal (HL) and diagonal (HH) determination detail parts. The results which obtained through wavelet transform have great accuracy of Human Visual System (HVS) than FFT or DCT transformations. To improve the robustness of the watermark, watermarks with higher energy ratio can be performed in the low sensitive HVS regions.

Proposed 3D secret sharing scheme

This paper proposes a technique called (t, n) watermarked 3D secret sharing model with verifiability property, where all the 3D models are watermarked using DWT and are then shared among n number of participants. To reconstruct the multiple 3D models, t participants can pool their secret shadows whereas less than t participants cannot recover the 3D models. The number of vertices and faces should be same for all 3D models. These 3D models are watermarked in order to protect from the unauthorized and untrusted usage. Secret keys must be generated by both the participants and the dealer. The participants who choose their own private key should compute a secret value and provide it to the dealer. Using public key cryptosystem the dealer computes the secret key. By this secret key in an invertible polynomial, the shadows are generated and distributed to the participants. Shares have equal number of vertices and faces. Lagrange's interpolation technique is used for reconstruction of 3D models. The 3D objects are also authenticated by reconstructing the watermark after generating the original secret 3D model.

Generally, 3D models are represented as a mesh, defined as (V, F), where V denotes set of vertices and F denotes the set of faces.

$$\begin{bmatrix} V_1 \\ V_2 \\ \vdots \\ V_w \end{bmatrix} = \begin{pmatrix} v_{1x} & v_{1y} & v_{1z} \\ v_{2x} & v_{2y} & v_{2z} \\ \vdots & \vdots & \vdots \\ v_{wx} & v_{wy} & v_{wz} \end{pmatrix}$$

$$\begin{bmatrix} F_1 \\ F_2 \\ \vdots \\ F_m \end{bmatrix} = \begin{pmatrix} f_{1x} & f_{1y} & f_{1z} \\ f_{2x} & f_{2y} & f_{2z} \\ \vdots & \vdots & \vdots \\ f_{mx} & f_{my} & f_{mz} \end{pmatrix} \quad \ldots\ldots(7)$$

where $V = (v_1, v_2 \ldots v_w)$ be the set of vertices and $F = (f_1, f_2 \ldots f_m)$ be the set of faces.

Multiple 3D secret sharing using Shamir's Scheme

The proposed work includes 3 phases; the initialization and embedding phase, the secret share construction phase and the verification, reconstruction and extraction phase. The initialization phase is divided into two processes: Watermarking using DWT and secret key generation by both the participants and dealer. The secret shares are constructed using the YCH scheme, during reconstruction process the verification of participants and the dealer is performed to avoid cheating. Original 3D models are reconstructed by t shares of the participants, using equations (4) and (5). Watermark is also retrieved from the reconstructed model to prove the authenticity of the 3D model. The computations are performed using prime field F_p,. In this scheme, since the vertex coordinates have negative numbers, decimals and integers, it is very difficult to attack or predict the values. To avoid statistical attacks; a duplication of vertex number and the faces is performed.

Initialization and Embedding Phase

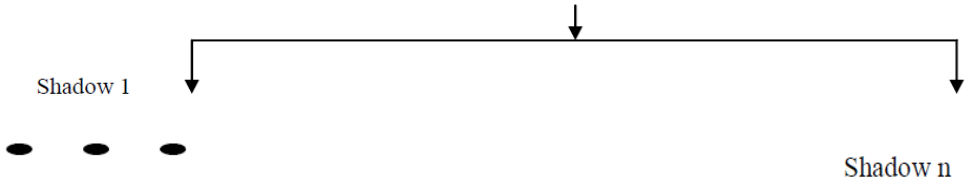
Initialization process deals with the sharing of keys for secret share construction. Large prime numbers B and Q are selected from which the product is computed as N.

An effective integer g is randomly chosen between $[N^{1/2}, N]$. {g, N} is distributed to the participants by the dealer.

K_i selected by the Participant U_i and computes,

$L_i = g^{K_i} \bmod N$

$$S_{i(1\le i\le p)} = \begin{bmatrix} V_{i1} \\ V_{i2} \\ \vdots \\ V_{iw} \\ F_{i1} \\ F_{i2} \\ \vdots \\ F_{i3} \end{bmatrix} = \begin{bmatrix} v_{i1x} & v_{i1y} & v_{i1z} \\ v_{i2x} & v_{i2y} & v_{i2z} \\ \vdots & \vdots & \vdots \\ v_{iwx} & v_{iwy} & v_{iwz} \\ \mathrm{f}_{iw+1x} & \mathrm{f}_{iw+1y} & \mathrm{f}_{iw+1z} \\ \mathrm{f}_{iw+2x} & \mathrm{f}_{iw+2y} & \mathrm{f}_{iw+2z} \\ \vdots & \vdots & \vdots \\ \mathrm{f}_{\mathrm{imx}} & \mathrm{f}_{\mathrm{imy}} & \mathrm{f}_{\mathrm{imz}} \end{bmatrix}$$



$$Y_1 = \begin{bmatrix} \gamma_1 \\ \gamma_2 \\ \vdots \\ \gamma_w \\ \gamma_{w+1} \\ \vdots \\ \gamma_m \end{bmatrix} = \begin{bmatrix} \gamma_{1x} & \gamma_{1y} & \gamma_{1z} \\ \gamma_{2x} & \gamma_{2y} & \gamma_{2z} \\ \vdots & \vdots & \vdots \\ \gamma_{wx} & \gamma_{wy} & \gamma_{wz} \\ \gamma_{w+1x} & \gamma_{w+1y} & \gamma_{w+1z} \\ \vdots & \vdots & \vdots \\ \gamma_{mx} & \gamma_{my} & \gamma_{mz} \end{bmatrix} \cdots Y_n = \begin{bmatrix} \gamma_1 \\ \gamma_2 \\ \vdots \\ \gamma_w \\ \gamma_{l+1} \\ \vdots \\ \gamma_{jm} \end{bmatrix} = \begin{bmatrix} \gamma_{1x} & \gamma_{1y} & \gamma_{1z} \\ \gamma_{2x} & \gamma_{2y} & \gamma_{2z} \\ \vdots & \vdots & \vdots \\ \gamma_{wx} & \gamma_{wy} & \gamma_{wz} \\ \gamma_{w+1x} & \gamma_{w+1y} & \gamma_{w+1z} \\ \vdots & \vdots & \vdots \\ \gamma_{mx} & \gamma_{my} & \gamma_{mz} \end{bmatrix}$$

Figure 2: Representation of secret shadow having w vertices and *m* faces.

Secret key Li and his identity Idi is provide by the participant to the dealer such that $L_i \neq L_j$ for $U_i \neq U_j$. Integer S_0 is chosen from the period [2, N], which is relatively prime to (B-1) and (Q-1). The dealer computes and distributes the $\{R_0, z\}$ to each participant.

$$S_0 \times z = 1 \bmod \phi(N) \qquad \ldots\ldots(8)$$

$$R_0 = g^{S_0} \bmod N \qquad \ldots\ldots(9)$$

$$I_i = L_i^{S_0} \bmod N \qquad \ldots\ldots(10)$$

where I = 1,2...n

where Φ (N) is the Euler's phi-function.

The chosen watermark is embedded into the vertices of the OBJ 3D model and the faces of the models are left unaltered. The vertices of the 3D models are decomposed into 1-level two dimensional DWT coefficients. The three high resolution bands

like LH, HL and HH are chosen. Embed the watermark sequence 'W' into the selected DWT sub bands with an amplification factor 'α'. The embedding is performed into the coefficient matrix V_i using the following equation.

$$E_{i,uv} = V_{i,uv} + \alpha W_{uv} \text{ where } uv \in \{LH, HL, HH\}$$

Otherwise

$$E_{i,uv} = V_{i,uv}$$

Shadow construction phase

Secret shares are constructed for the multiple 3D models for both the cases, like.

- The number of secret 3D models is less than or equal to the threshold $(P \leq t)$
- The number of secret 3D models is greater than the threshold $(P > t)$
- Case $(P \leq t)$, where the threshold is greater than or equal to the number of secrets

(1) Compute

$$h(x) = S_1 + S_2 x^1 + \cdots + S_p x^{p-1} + C_1 x^p + C_2 x^{p+1} + \cdots C_{t-p} x^{t-1} \bmod F_p \quad \ldots\ldots(11)$$

(1) Generate $Y_i(I_i) \bmod F_p$

(2) Distribute (R_0, z, Y_i)

- Case $(P > t)$ where the threshold is less than the number of secrets

(1) Generate $h(x) = S_1 + S_2 x^1 + \cdots + S_p x^{p-1} \bmod F_p$ ……(12)

(2) Compute $Y_i(I_i) \bmod F_p$ for i = 1,2…n

(3) Compute $h(i) \bmod F_p$ for i = 1,2…P-t

(4) Distribute the (R_0, z, Y_i, h(i))

Recovery phase

Pooled shadows are used to reconstruct the secret models using equations (4) and (5) for both the cases and less than that cannot retrieve any secrets. The participant and the dealer can are verified to check the authenticity of the.

1. Verification Process.

- Each U_i computes, $I_i^{'}$

$$I_i^{'} = R_o^{K_i} \bmod N \quad \ldots\ldots(13)$$

- Participants verify $I_i^{'} - if^{I_i^{'Z} = L_i \bmod N}$ then is true, $I_i^{'}$ otherwise is false and participant U_i may be a cheat, where the I_i is the secret value of the dealer.

2. Reconstruction of the secret model and the extraction of Watermark.

- The polynomial h(x) mod m can be uniquely determined for two cases as follows:

$$Case^{p \leq t}$$

$$h(x) = \sum_{i=1}^{t} Y_i \prod_{j=1,\, j \neq i}^{t} \frac{x - I_j^{'}}{I_i^{'} - I_j^{'}} \bmod F_p = = S_1 + S_2 x^1 + \cdots + S_p x^{p-1} + C_1 x^p + C_2 x^{p+1} + \cdots C_{t-p} x^{t-1} \bmod F_p$$

- $Case^{P>t}$

$$h(x)=\sum_{i=1}^{t} Y_i \prod_{j=1,\, j\neq i}^{t} \frac{x-I_j^{'}}{I_i^{'}-I_j^{'}}+\sum_{i=1}^{p-t} Y_i \prod_{j=1,\, j\neq i}^{p-t} \frac{x-j}{i-j} \bmod \mathrm{F}_p = S_1 + S_2 x^1 + \cdots + S_p x^{p-1} \bmod \mathrm{F}_p$$

The 3D models are reconstructed from the pooled shares without any loss. The watermark information is extracted from the 3D models without tampering. 1-level DWT is performed to the watermarked vertices of the 3D models. The watermarked sub band is chosen to retrieve the embedded watermark. The watermarked image W is regenerated using the seed 'α' which is used during the embedding process. The watermarked image and the 3D models are reconstructed successfully.

Experimental Results

Experimental analysis is shown for (4,6) scheme, for both the cases. Every model is chosen in such a way that its vertices and faces of the model are equal or else duplicated in order to have the same number of vertices and faces. Similarly the vertices are duplicated to achieve a prime vertices number. Figure 3a and Figure 3b show the original 3D model and the image used for watermarking.

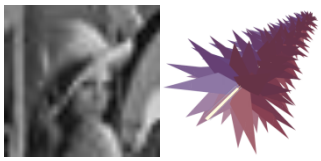


Figure 3: (a) Watermark Image (b) 3D model.

Figure 4 (a, b and c) shows the results for the case ($P \geq t$) embedded secret models and the generated six shadows along with the reconstructed secrets. Since the shares are unrecognizable and the secrets are also reconstructed without any loss.

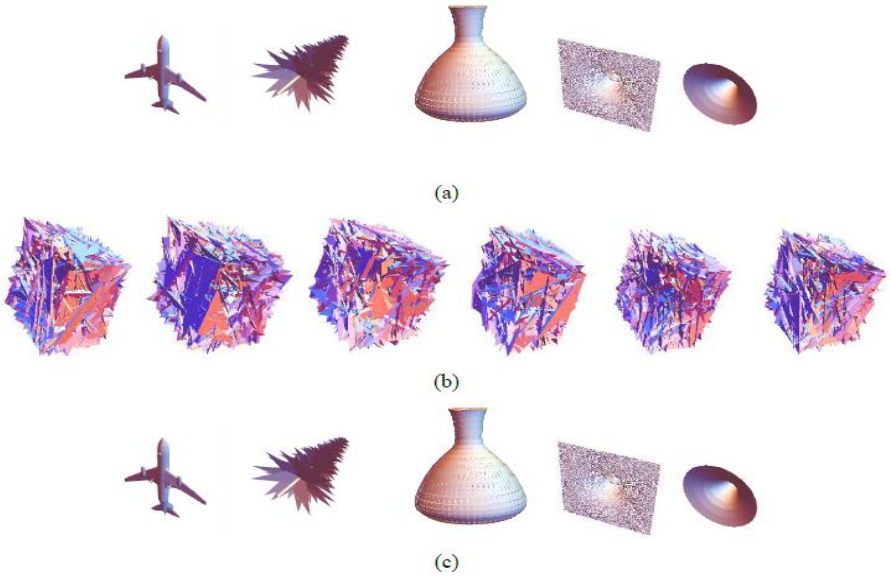


Figure 4: (a) Original embedded models and the (b) generated shares and the (c) reconstructed models for the case P>t.

Similarly the other case is also tested using 2 secret 3D models, for the case ($P \leq t$). Figure 5 (a, b and c) shows generated shares and the reconstructed secret. Figure 6 shows the extracted watermark image from these models.

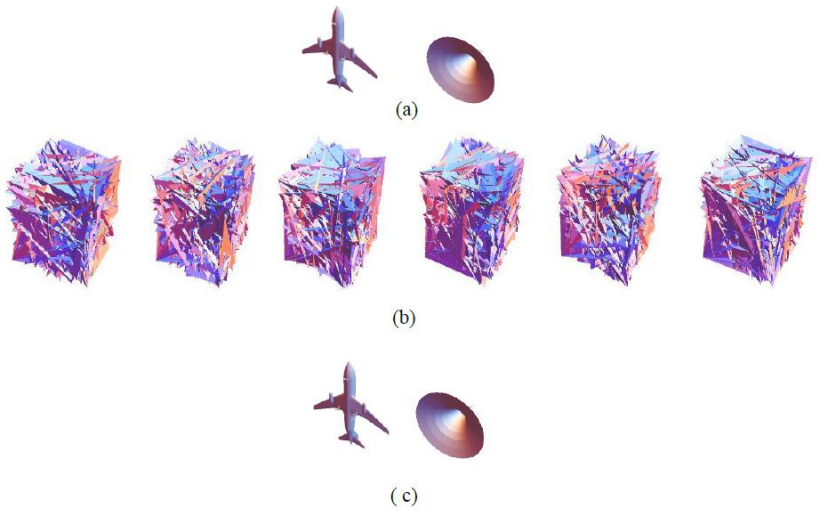


Figure 5: (a) Original embedded models and the (b) generated shares and the (c) reconstructed models for the case P ≤ t.

Figure 6: Retrieved watermark image.

Quality of the Watermarked 3D Models

Image distortion occurs when a watermark is embedded in to a model which affects the image quality by generating a degradation in the watermark model. When the value of α become 0.0001 then the watermark is invisible leading to a very less which is unnoticeable. To evaluate the watermarked 3D model quality the PSNR is calculated between original 3D model and the original 3D model as given in equation.

$$MSE(V,V_w) = \frac{1}{MxN}\sum_{x=1}^{M}\sum_{y=1}^{n}\left(V(x,y) - V_w(x,y)\right)^2$$

$$PSNR(V,V_w) = 10\log_{10}\left[\left(\frac{\left(2^p - 1\right)^2}{MSE}\right)\right]$$

Where, V and V_w are the original and the watermarked 3D models respectively.

3D Object Models	PSNR
Pinetree	61.4095
Plane	65.5917
Pot	65.788
Wizard	64.28
Hat	62.127

Table 1: PSNR values between original and watermarked 3D models.

Table 1 shows the correlation value between the original 3D model and the watermarked 3D model which shows that the quality of the watermarked 3D models are preserved.

Similarly the correlation among the watermark image and the retrieved watermark image is calculated and are shown in the Table 2.

Image	Correlation Vertical of Watermark Image	Correlation Vertical of Retrieved Image	Correlation Horizontal of Watermark Image	Correlation Horizontal of Retrieved Image
Lena	0.8889	0.8910	0.8899	0.8919

Table 2: Correlation values between original and retrieved watermark

Conclusion

The frame work for watermarking and secret sharing for multiple 3D models is proposed and its implementation and results are discussed in this paper. The proposed scheme makes use of the YCH algorithm for the secret sharing process. The verification property is implemented on both participants and the dealer to identify the duplicate shadow. Watermarking is performed to prove the integrity of the reconstructed model. The simulation results show that it is a perfect scheme and the feasibility is shown using different 3D models. Further, the size can be reduced by lossless compression techniques, such as the Huffman encoding and ZLIP.

References

1. Blakley G (1979) Safeguarding cryptography key, in: Proceedings of AFIPS National Computer Conference, 48: 313-317.
2. Shamir A (1979) How to share a secret. Communications of the ACM 22(11): 612-613.
3. Naor M and Shamir A (1994) May. Visual cryptography. In Workshop on the Theory and Application of Cryptographic Techniques (pp. 1-12). Springer, Berlin, Heidelberg.
4. Shao J and Cao Z (2005) A new efficient (t, n) verifiable multi-secret sharing (VMSS) based on YCH scheme. Applied Mathematics and Computation 168(1): 135-140.
5. Zhao J, Zhang J and Zhao R (2007) A practical verifiable multi-secret sharing scheme. Computer Standards & Interfaces 29(1): 138-141.
6. Fang WP (2007) November. Visual Cryptography in reversible style. In Intelligent Information Hiding and Multimedia Signal Processing, 2007. IIHMSP 2007. Third International Conference on (1: 519-524). IEEE.
7. Fang WP (2009) Non-expansion visual secret sharing in reversible style. International Journal of Computer Science and Network Security 9(2): 204-208.
8. Feng JB, Wu HC, Tsai CS, et al. (2008) Visual secret sharing for multiple secrets. Pattern Recognition 41(12): 3572-3581.
9. Jagannathan V, Mahadevan A, Hariharan R et al. (2007) February. Number theory based image compression encryption and application to image multiplexing. In Signal Processing, Communications and Networking, 2007. ICSCN'07. International Conference on (59-64). IEEE.
10. Shyu SJ, Huang SY, Lee YK, et al. (2007) Sharing multiple secrets in visual cryptography. Pattern Recognition 40(12): 3633-3651.
11. Ulutas G, Ulutas M and Nabiyev V (2011) Distortion free geometry based secret image sharing. Procedia Computer Science 3: 721-726.
12. Lin SJ and Lin JC (2007) VCPSS: A two-in-one two-decoding-options image sharing method combining visual cryptography (VC) and polynomial-style sharing (PSS) approaches. Pattern Recognition 40(12): 3652-3666.

13. Thien CC and Lin JC (2002) Secret image sharing. Computers & Graphics 26(5): 765-770.
14. Wang RZ and Su CH (2006) Secret image sharing with smaller shadow images. Pattern Recognition Letters 27(6): 551-555.
15. Chang CC, Hsieh YP and Lin CH (2008) Sharing secrets in stego images with authentication. Pattern Recognition 41(10): 3130-3137.
16. Lin CC and Tsai WH (2004) Secret image sharing with steganography and authentication. Journal of Systems and Software 73(3): 405-414.
17. Iftene S and Boureanu IC (2005) Weighted threshold secret sharing based on the Chinese remainder theorem. Scientific Annals of Cuza University 15(EPFL-ARTICLE-174320): 161-172.
18. Elsheh E and Hamza AB (2011) Secret sharing approaches for 3D object encryption. Expert Systems with Applications 38(11): 13906-13911.
19. Yang CC, Chang TY and Hwang MS (2004) A (t, n) multi-secret sharing scheme. Applied Mathematics and Computation 151(2): 483-490.