A Format-compliant Selective Secret 3D Object Sharing Scheme Based on Shamir's Scheme

Sebastien Beugnon, William Puech, Jean-Pierre Pedeboy

A FORMAT-COMPLIANT SELECTIVE SECRET 3D OBJECT SHARING SCHEME BASED ON SHAMIR'S SCHEME

Sébastien BEUGNON[⋆,†] *William PUECH*[⋆] *Jean-Pierre PEDEBOY*[†]

[⋆] LIRMM, Univ Montpellier, CNRS, Montpellier, France
[†] STRATEGIES S.A., Rungis, France

ABSTRACT

New issues have arisen in the creation of 3D objects linked to collaboration in 3D workflows. In this kind of usage it may be necessary to allow access and to share a lower quality file of a 3D object for some collaborators. In this paper, we present a Format-Compliant Selective Secret 3D Object Sharing (FCSS3DOS) scheme, which visually protects the content using geometrical distortions by selectively sharing bits of a 3D object's geometry using Shamir's Secret Sharing scheme. The degradation level D is selected before the sharing process and determines how much geometrical distortions are induced into n generated shared 3D objects which are given to n participants. When at least k or more participants agree to combine their own shared 3D objects, then the secret 3D object can be recovered without distortion. The value of k can vary between 2 and n. In experimental results, we analyze the degradation level D that influences the geometrical distortions induced into shared 3D objects.

Index Terms— 3D Object, Selective 3D Encryption, Visual Secret Sharing, Content Protection.

1. INTRODUCTION

3D objects are the new digital art of this decade. Through virtual reality, simulations, 3D scans or 3D printing, 3D objects play a key role in cutting-edge technologies. In order to prevent piracy and illegal access to 3D content, crypto-security applications for 3D objects and graphics have become a hot topic. Many ways exist to protect 3D objects, such as using classic encryption methods, but they handle them as binary files which breaks the compliance of their format.

Secret Sharing (SS) aims to find a way to safely distribute a secret among a group by giving its members "shares" of this secret. In 1979, Shamir [1] and Blakley [2] independently developed the first (k, n)-threshold schemes using polynomial interpolation and hyperplane geometry, respectively. To reconstruct a secret shared using their methods, it requires combining at least k or more shares among n. In the last few decades, the SS concept has been applied to 2D images in order to preserve format-compliance. Secret Image Sharing (SIS) is a field of research particularly well studied [3, 4, 5]. Secret 3D Object Sharing (S3DOS) has been proposed by applying SS schemes directly without taking into account format compliance [6, 7], whereas other previous work proposed to use SS to recover low quality 3D objects or to hasten transmission of multiple 3D objects using data hiding [8, 9]. Furthermore, progressive or selective encryption methods for 3D objects has also received some interests [10, 11, 12].

In this paper, we propose a new (k, n, D) scheme to share 3D objects, called Format-Compliant Selective Secret 3D Object Sharing scheme (FCSS3DOS) where $k \in [\![2\ ;\ n]\!]$ and D the degradation level, which is chosen at the beginning of the sharing process. This approach makes a selection of bits within the coordinates of all vertices of the secret 3D object, then generates n binary words for each vertex using Shamir's scheme. These information blocks substitute the original selected bits in the shared 3D objects. Each of these shared 3D objects can be visualized in a 3D environment, but its content is visually protected by geometrical distortions due to the sharing process.

The rest of this paper is organized as follows. Section 2 details the proposed FCSS3DOS scheme. Section 3 provides experimental results of our proposed method and comparisons with other S3DOS schemes. Finally, Section 4 concludes this paper and offers directions for future work.

2. OUR PROPOSED FCSS3DOS SCHEME

In this section, the proposed FCSS3DOS (k, n, D) scheme based on Shamir's SS approach is explained. The proposed method shares a secret 3D object, which is defined by a set of 3D vertices V and a set of polygons T, into a set of n 3D objects with geometrical distortions, called shared 3D objects. As illustrated in Fig. 1, this scheme independently shares the vertices by selecting bits of coordinates. Thereafter, the selected bits are shared as a secret, using Shamir's SS scheme to obtain n binary words for each of the n participants per vertex. Then, these binary words substitute the selected bits of the secret 3D object as shared 3D objects. This method takes control over geometrical distortions induced by sharing selected bits from vertices of the secret 3D object as a function of the degradation level D as illustrated in Fig. 1. Along with the secret 3D object M, the method requires three parameters: k, the number of required participants to reconstruct the

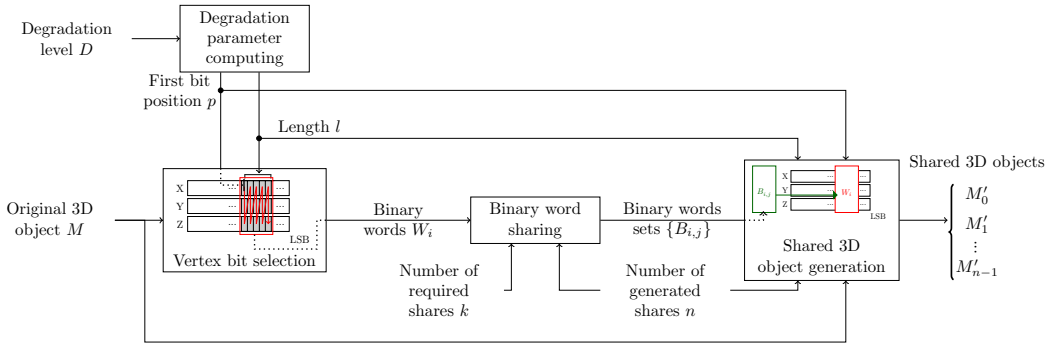


Fig. 1: Sharing process overview.

secret 3D object, n, the total number of wanted shared 3D objects and D the desired degradation level.

2.1. Shamir's SS scheme

The scheme proposed by Shamir is a (k, n)-threshold scheme which means that any group with k or more shares among the n generated, can reconstruct the secret S [1]. With less than k shares, participants cannot acquire information about the secret. Note that generated shares are irrelevant independently. This scheme is based on a polynomial interpolation and in the sharing process a $(k-1)$-degree polynomial is produced over a finite field noted $\mathbb{F}_p$ where p is prime and coefficients $A = \{a_1, ..., a_{k-1}\}$ are randomly chosen from $\mathbb{F}_p$:

$$f(x) = \sum_{i=0}^{k-1} a_i \times x^i \bmod p. \tag{1}$$

The secret S, but also k and n have to be in $\mathbb{F}_p$. Then, the secret S is the value $f(0)$ which means that $a_0 = S$. Thus, each participant receives a share $f(x_i)$. At the reconstruction step, at least k or more shares are required in order to reconstruct the secret S. Therefore, participants can cooperate to recover the coefficients of $f(x)$ using Lagrange's interpolation:

$$f(x) = \sum_{i=1}^{k} \prod_{j=1, i\neq j}^{k} \frac{x - x_j}{x_i - x_j} \times f(x_i). \tag{2}$$

2.2. Vertex bit selection

Coordinates of a vertex in a 3D object can be defined by symbol sequences, binary floating or quantified values. In our proposed method, we select bits of these representations and share them using Shamir's SS scheme. As illustrated in Fig. 1, the degradation level D determines which range of bits is selected and consists of two variables:

$$D =< p, l >, \tag{3}$$

where p is the position of the first selected bit from the least significant one and l is the range of bits to protect from p to the less significant bits.

The selected sequence of bits is recovered as a binary word noted W_i, where i is the vertex index and $|W_i| = 3 \times l$. The binary word W_i is built by reading bits and by interleaving bits of coordinates v_i^x, v_i^y and v_i^z as shown in the vertex bit selection step illustrated in Fig. 1.

2.3. Binary word sharing

During this step, for each vertex v_i, n binary words $B_{i,j}$, where $j \in [\![0\ ;\ n[\![$, are generated by sharing the previously created binary word W_i with Shamir's SS scheme. To insure the method can properly substitute selected bits by $B_{i,j}$ and reconstruct W_i, it is required to have $|B_{i,j}| = |W_i|$. Thus, we compute over the Galois field $GF(2^{(3\times l)})$ to restrain the size of $B_{i,j}$ and to insure that the reconstruction W_i will be lossless as proposed by Yang *et al.* [13] for their SIS scheme. Furthermore, this also allows us to increase the number of participants and the computational complexity of the scheme as a function of the degradation level D. The greater the parameter l from degradation level D, the safer the scheme. The method starts the sharing process from Shamir's SS scheme by attributing a distinct x_j for each participant and their respective shared 3D object as:

$$\begin{cases} x_j \in GF(2^{(3\times l)}), \\ x_j \neq 0, \\ \forall j, t \in [\![0\ ;\ n[\![, j \neq t \Leftrightarrow x_j \neq x_t. \end{cases} \tag{4}$$

The value of x_j is used for all vertices of the 3D object. Coefficient a_0 is assigned the value of W_i. Then, the method builds n results noted $B_{i,j}$ using Eq.(1) for each vertex v_i. For each vertex, coefficients of A are rebuilt with new random values.

2.4. Shared 3D object generation

As illustrated in Fig. 1, after generating the n binary words $B_{i,j}$ with Shamir's SS scheme for each vertex, the proposed method substitutes the selected bits of coordinates in the secret 3D object with the binary words to generate n shared 3D objects, noted M'_j. Then, the n M'_j are transmitted to the n participants. Coordinates generated by the substitution of W_i

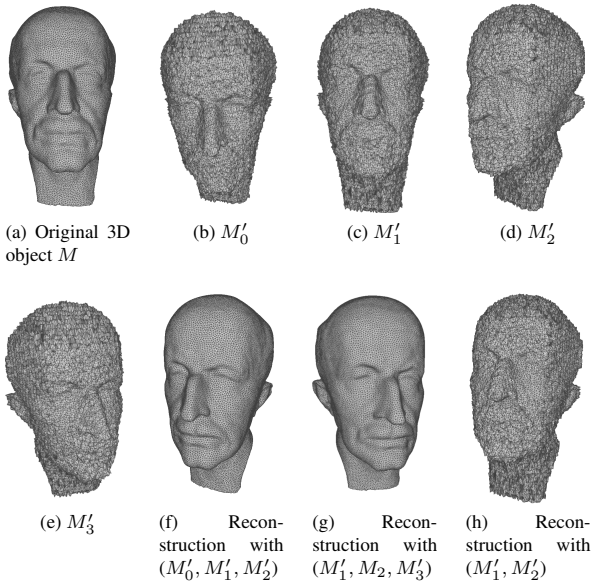
by binary words $B_{i,j}$ become different from those of the secret 3D object. Indeed, geometrical distortions appear in the shared 3D objects as a function of the degradation level D.

2.5. 3D object reconstruction

The reconstruction of the secret 3D object can only be achieved when at least k or more shared 3D objects are present. Instead of extracting one binary words, the reconstruction method recovers k binary words $B'_{i,j}$ for each vertex v_i of k shared 3D objects M'_j. Therefore, the method applies the reconstruction process of Shamir's SS scheme (Eq. (2)) using $B'_{i,j}$. The returned secret by Shamir's reconstruction is the original binary word W_i. Finally, the method, for all vertices, substitutes bits from the selected area in one (it does not matter which) of the k shared 3D objects by bits of W_i using the degradation level D.

3. EXPERIMENTAL RESULTS

In this section, we present experimental results of our proposed FCSS3DOS (k, n, D) scheme based on Shamir's SS scheme and analyze statistically its results and its security. We implemented our method for 3D objects based on the IEEE 754 norm to represent vertex coordinates [14]. We decided to only protect the mantissa field of this representation. Thus, the degradation level D parameters are defined as $p \in [\![0\ ;\ 22]\!]$ and $l \in [\![1\ ;\ p+1]\!]$ where the last bit of the sequence is the last significant bit when using the big-endian rule. Fig. 2



(a) Original 3D object M (b) M'_0 (c) M'_1 (d) M'_2

(e) M'_3 (f) Reconstruction with (M'_0, M'_1, M'_2) (g) Reconstruction with (M'_1, M_2, M'_3) (h) Reconstruction with (M'_1, M'_2)

Fig. 2: Sharing of a 3D object M with parameters $k = 3$, $n = 4$ $D =< 18, 19 >$ using Shamir's SS scheme.

presents results of our method with parameters $k = 3$, $n = 4$ and $D =< 18, 19 >$ applied on a secret 3D object illustrated Fig. 2.a. Fig. 2.b-e are 4 generated shared 3D objects given to participants at the end of the sharing process. These shared 3D objects have the same number of vertices as the original 3D object, but their geometry is distorted. However, they still remain usable for their integration in 3D environments depending on the desired degradation level, for example in an animation application. Fig. 2.f and Fig. 2.g illustrate that any group of 3 shared 3D objects can perfectly reconstruct the secret 3D object. Fig. 2.h presents a "reconstructed" 3D object with only 2 shared 3D objects instead of 3, this remains as distorted as the used shared 3D objects because the threshold k is not reached.

3.1. Large dataset quantitative analysis

From the Princeton mesh segmentation dataset [15], we analyzed the geometrical distortions of generated shared 3D objects from 400 original secret 3D objects.

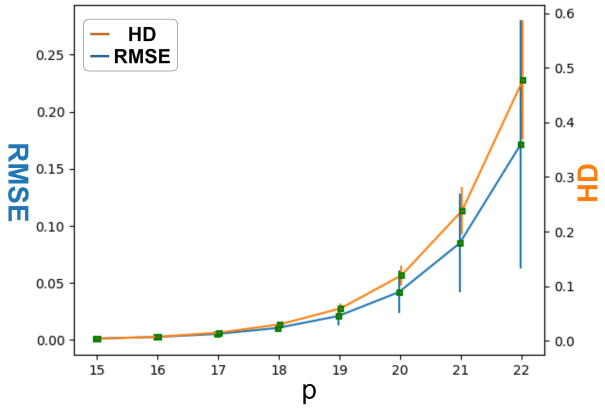


Fig. 3: Mean and standard deviation of the RMSE (blue curve) and the HD (orange curve) on the Princeton mesh segmentation dataset [15] as a function of the degradation level ($D =< p, p+1 >$).

Fig. 3 illustrates the mean and the standard deviation of the Root Mean Square Error (RMSE) [16] and the Hausdorff Distance (HD) [17] on shared 3D objects generated from the dataset as a function of degradation level D. We observe that, the higher the degradation level, the stronger the geometrical distortions. The HD reveals pretty much the same pattern as the RMSE. From Fig. 2 and Fig. 3, we note that, from $p \geq 18$, the proposed method allows us to visually protect all the 3D objects from this dataset in the same way by adding sufficient geometrical distortions.

3.2. Security analysis

In this section, we discuss the robustness of our scheme to attacks. Since our scheme overrides selected bits in the mantissa of coordinates for each vertex, it can be less robust to attacks looking to recover the content rather than the secret key, as described in [18] for selectively encrypted images. As previously explained, the degradation level D directly determines the geometrical distortions induced in shared 3D objects. An adversary is able to preserve the unencrypted part of

information of shared data to build targeted attacks in order to sufficiently reconstruct the content. Instead of trying a naive brute-force attack, which requires finding the right combination among $2^{3\times|V|}$ for each protected bit, an adversary can try to put each protected bit to zero, we call this a *zero-bit* attack. Also, since our method preserves parts of the original coordinates of each vertex, 3D object processing techniques such as smoothing methods [19, 20] or even reconstruction approaches [21], are another way to slightly improve the quality of a shared 3D object.

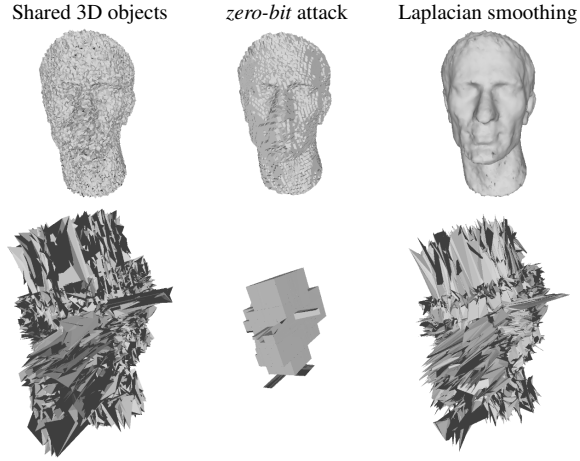


Fig. 4: *zero-bit* attack and Laplacian smoothing on shared 3D objects depending on the degradation level: $D =< 18, 1 >$ (up row) and $D =< 22, 1 >$ (bottom row).

Fig. 4 illustrates how shared 3D objects respond to attacks depending on their degradation level $D =< 18, 1 >$ and $D =< 22, 1 >$. For zero-bit attacks, we observe that it does not allow the adversary to recover an improved version of the 3D object. Indeed, the recovered 3D object contains defects, such as discretization artifacts, self-intersecting triangles and overlaps. No high quality features are present in these levels of degradation. Meanwhile for a Laplacian smoothing attack, such as in Fig. 4, for the degradation level $D =< 18, 1 >$ the general shape of the secret 3D object is preserved, but high quality features are still protected by our scheme. Whereas for a higher degradation level, the shape is also protected by geometrical distortions. An adversary can only hope to try to improve the quality of an intercepted shared 3D object. Note that the metrics we used to evaluate the quality of the shared 3D objects, are with full reference, which means that it is necessary to have the original secret 3D object to make comparisons. But since the adversaries do not have access to the original 3D object, they cannot use these metrics to recover the secret content.

3.3. Comparison with previous work

Table 1 presents comparisons of our FCSS3DOS scheme with previous work on S3DOS schemes [6, 7, 22, 8, 9].

The proposed method stands out thanks to its improved functionality. The property **meaningful** means that when shares are not just considered random noise data. Our proposed method generates shared 3D objects representing the secret 3D object in low quality, meanwhile [8, 9] embed their sharing data in host 3D objects to enhance the confidentiality. The property **lossless** is attributed to methods where the reconstruction is lossless, which is the case of our proposed scheme and [22, 8]. The property **multiple** defines methods sharing multiple secrets simultaneously, only [7, 22, 9] proposed this property. The property **non expansive** defines the inconvenience of some secret sharing schemes where the shares are bigger in size than the secret message. Our FCSS3DOS scheme preserves the size of the 3D object, whereas other schemes resample their host 3D objects, in order to ease their embedding process [8, 9] or generate public information [7]. The property **Format-compliant** means that schemes return the same type of file as it was given in input, in our case 3D objects like [22, 8, 9]. The property **selective** consists of using a selective encryption approach in order to encrypt transparently, sufficiently or with total visual confidentiality, explained in [12]. We note that our method is the only one that is meaningful, lossless, non-expansive, format-compliant and selective.

Table 1: Comparison of our scheme with previous work.

Scheme	[6]	[7]	[22]	[8]	[9]	**Proposed**
Meaningful	No	No	No	Yes	Yes	**Yes**
Lossless	No	No	Yes	Yes	No	**Yes**
Multiple	No	Yes	Yes	No	Yes	**No**
Non expansive	Yes	No	Yes	No	No	**Yes**
Format-compliant	No	No	Yes	Yes	Yes	**Yes**
Selective	No	No	No	No	No	**Yes**

4. CONCLUSION

In this paper, a FCSS3DOS (k, n, D) scheme to visually protect 3D objects by creating n shared 3D objects with geometrical distortions is proposed. When at least k of the n generated shared 3D objects are combined, the secret 3D object is reconstructed without degradation. The distortions are controlled at the beginning of the sharing process by the degradation level D which indicates how many bits of vertices and where they are selected to be shared. Each vertex is shared independently by forming a binary word with selected bits using Shamir's SS scheme. The degradation level also controls the used Galois field and can increase the number of generated shared 3D objects and set the computational complexity of our scheme. Shared 3D objects preserve the original size of the secret 3D object, have the same level of geometrical distortions between them and can be rendered in 3D environments. Experimental results and analyses of our method prove that it is efficient. In future studies, we would like to offer new properties from other SIS schemes based on Shamir's SS scheme such as a hierarchical system.

5. REFERENCES

[1] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[2] G. R. Blakley, "Safeguarding cryptographic keys," in *Proceedings of the National Computer Conference*, 1979, vol. 48, pp. 313–317.

[3] C.C. Thien and J.C. Lin, "Secret image sharing," *Computers & Graphics*, vol. 26, no. 5, pp. 765–770, 2002.

[4] M.H. Tsai and C.C. Chen, "A study on secret image sharing," in *Proceedings of the 6th International Workshop on Image Media Quality and its Applications, Tokyo, Japan*. Citeseer, 2013.

[5] S. Beugnon, W. Puech, and J.-P. Pedeboy, "An efficient lossless (2, n) secret image sharing based on blakleys scheme," in *IEEE 19th International Workshop on Multimedia Signal Processing (MMSP)*, 2017.

[6] E. Elsheh and A. B. Hamza, "Secret sharing approaches for 3D object encryption," *Expert Systems with Applications*, vol. 38, no. 11, pp. 13906–13911, 2011.

[7] L. J. Anbarasi and GS A. Mala, "Verifiable multi secret sharing scheme for 3D models.," *International Arab Journal of Information Technology*, vol. 12, no. 6, pp. 708–713, 2015.

[8] Y.-Y. Tsai, "A secret 3D model sharing scheme with reversible data hiding based on space subdivision," *3D Research*, vol. 7, no. 1, pp. 1, 2016.

[9] S.-S. Lee, Y.-J. Huang, and J.-C. Lin, "Protection of 3D models using cross recovery," *Multimedia Tools and Applications*, vol. 76, no. 1, pp. 243–264, 2017.

[10] Michael Gschwandtner and Andreas Uhl, *Protected Progressive Meshes*, Springer, 2009.

[11] M. Éluard, Y. Maetz, and G. Doërr, "Impact of geometry-preserving encryption on rendering time," in *IEEE International Conference on Image Processing (ICIP)*. 2014, IEEE.

[12] S. Beugnon, W. Puech, and J.-P. Pedeboy, "Format compliant selective encryption of 3D objects," in *2018 IEEE International Conference on Multimedia and Expo (ICME)*, 2018.

[13] C.-N. Yang, T.-S. Chen, K. H. Yu, and C.-C. Wang, "Improvements of image sharing with steganography and authentication," *Journal of Systems and software*, vol. 80, no. 7, pp. 1070–1076, 2007.

[14] IEEE, "Ieee standard for floating-point arithmetic," *IEEE Std 754-2008*, pp. 1–70, Aug 2008.

[15] X. Chen, A. Golovinskiy, and T. Funkhouser, "A benchmark for 3D mesh segmentation," *ACM Transactions on Graphics (TOG)*, vol. 28, no. 3, pp. 73, Aug. 2009.

[16] P. Cignoni, C. Rocchini, and R. Scopigno, "Metro: Measuring error on simplified surfaces," in *Computer Graphics Forum*. Wiley Online Library, 1998, vol. 17, pp. 167–174.

[17] N. Aspert, D. Santa-Cruz, and T. Ebrahimi, "Mesh: Measuring errors between surfaces using the hausdorff distance," in *Proceedings of the 2002 IEEE International Conference on Multimedia and Expo, ICME 2002, Lausanne, Switzerland. August 26-29, 2002. Volume I*. IEEE, 2002, vol. 1, pp. 705–708.

[18] A. Said, "Measuring the strength of partial encryption schemes," in *IEEE International Conference on Image Processing (ICIP)*. IEEE, 2005, vol. 2, pp. II–1126.

[19] L. R. Herrmann, "Laplacian-isoparametric grid generation scheme," *Journal of the Engineering Mechanics Division*, vol. 102, no. 5, pp. 749–907, 1976.

[20] G. Taubin, "Curve and surface smoothing without shrinkage," in *Computer Vision, 1995. Proceedings., Fifth International Conference on*. IEEE, 1995, pp. 852–857.

[21] W. E. Lorensen and H. E. Cline, "Marching cubes: A high resolution 3D surface construction algorithm," *SIGGRAPH Computer Graphics*, vol. 21, no. 4, pp. 163–169, Aug. 1987.

[22] A. Martín del Rey, "A multi-secret sharing scheme for 3D solid objects," *Expert Systems with Applications*, vol. 42, no. 4, pp. 2114 – 2120, 2015.