HOMOMORPHIC TWO TIER REVERSIBLE DATA HIDING IN ENCRYPTED 3D OBJECTS

Bianca Jansen van Rensburg[⋆†] *Pauline Puteaux*[⋆] *William Puech*[⋆] *Jean-Pierre Pedeboy*[†]

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

{bianca.jansen-van-rensburg, pauline.puteaux, william.puech}@lirmm.fr, jp.pedeboy@cadwin.com

ABSTRACT

Today, 3D objects are an increasingly popular form of media. It has become necessary to secure them during their transmission or archiving. In this paper, we propose a two tier reversible data hiding method for 3D objects in the encrypted domain. Based on the homomorphic properties of the Paillier cryptosystem, our proposed method embeds a first tier message in the encrypted domain which can be extracted in either the encrypted domain or the clear domain. Indeed, our method produces a marked 3D object which is visually very similar to the original object. It seeks to be format compliant and to preserve the original size of the data, without the need for an auxiliary file. Moreover, large keys are used, rending our method secure for real life applications.

***Index Terms*—** Multimedia security, reversible data hiding, 3D object security, homomorphic encryption, signal processing in the encrypted domain.

1. INTRODUCTION

Over the last decade, the cloud has become a popular way of storing and transferring multimedia such as images, videos and 3D objects. The need for multimedia security has become significant. Encryption methods serve to secure the multimedia file by converting its content to unintelligible ciphertext. Once the media is encrypted and located in the cloud, a user, whether it be the original owner of the media or a third party, may wish to analyse or to embed data in the encrypted media. The advantage of reversible data hiding in the encrypted domain (RDH-ED) is that it allows third party users to embed data into the cover media, without knowledge of the original content and therefore without the need to compromise the confidentiality of the cover media.

RDH-ED methods can be broken down into two main categories: Reserving Room Before Encryption (RRBE) [1–4], and Vacating Room After Encryption (VRAE) [5–7]. In RRBE methods, the content owner liberates space for the data in the media in a preprocessing step. While in VRAE methods, the media is first encrypted by the owner and the data hider can then embed the data by modifying the encrypted media.

In particular, several methods based on public key homomorphic cryptosystems for image security have been proposed. These methods can be divided into two categories: those based on the Paillier cryptosystem [8–13], and those which use a post-quantic cryptosystem and exploit the Learning With Error (LWE) problem [14, 15]. Homomorphic cryptosystems are beneficial in signal processing as they translate a mathematical operation in the clear domain to another operation in the encrypted domain. Note that they are also probabilistic.

Recently, the popularity of 3D objects has greatly increased and with it, the need to secure 3D objects. Despite the development of applications for 3D data hiding in the encrypted domain, it remains a relatively unexplored research area. To our knowledge, there exists very few RDH-ED methods for 3D objects. In 2018, Jiang *et al.* proposed a RDH-ED method for 3D objects where data is embedded in encrypted vertices designated for embedding [16]. This was later improved by Yin *et al.* [17] in 2019, who suggested using an error prediction protocol to designate the vertices to be embedded before the encryption. In 2018, Shah *et al.* proposed a two tier RDH-ED for 3D objects using the Paillier cryptosystem [18]. The first tier of data hiding is completed by using the Paillier cryptosystem's homomorphic properties to perform a histogram expansion and shifting in the encrypted domain. The second tier of data hiding is done by using the Paillier self-blinding property.

In this paper, we propose a two tier homomorphic RDH-ED method based on the Paillier cryptosystem for 3D objects. Our method preserves the original format of the 3D object and there is no size expansion, all without the need for an auxiliary file. In order to have a large key size, vertices are grouped into blocks without reducing the payload. After decryption, the reconstructed 3D object remains marked with the first tier message. It is also possible to recover the first tier message as a ciphertext in the encrypted domain. Note that a smaller second tier message can be embedded in the encrypted domain. Our method is reversible as we conserve the visual quality of the original 3D object.

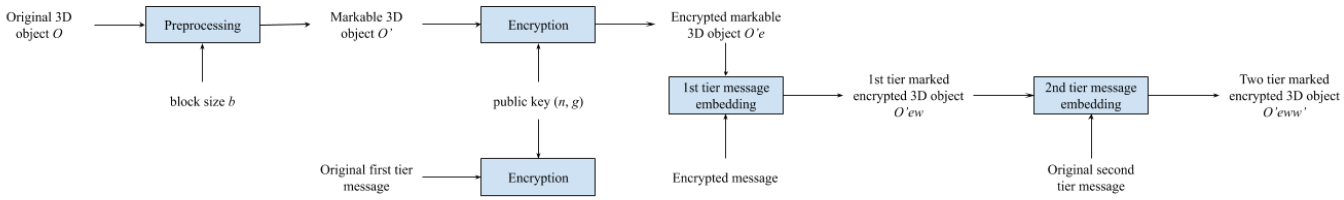


Fig. 1: Overview of the encoding phase of the proposed method.

2. PROPOSED METHOD

In this section, we describe our proposed method of homomorphic two tier reversible data hiding in encrypted 3D objects. Fig. 1 presents the overview of the encoding phase of the proposed method. The vertices are grouped into blocks, noted B and bits which we wish to use to embed the message are set to zero. The 3D object and the first tier message are both encrypted with the same public key and are multiplied in the encrypted domain in order to be equivalent to an addition in the clear domain, using the Paillier cryptosystem homomorphic property. A smaller second tier message can also be embedded.

We note the original 3D object O, which is represented is by a set of vertices. Each vertex consists of three coordinates x, y and z, where each of which can be represented by a 32-bit floating point fp, which consists of a sign s (1 bit), an exponent e (8 bits) and a mantissa $mant$ (23 bits) where:

$$fp = (-1)^s \times mant \times 2^{e-127}. \quad (1)$$

2.1. Preprocessing

The encryption is performed exclusively on the 23-bits of the mantissas of each coordinate, which are transformed into integers. This means that the part of each vertex v we want to encrypt is encoded with $23 \times 3 = 69$ bits.

In order to have a key sufficiently large to be secure, vertices are grouped into blocks B of size b vertices per block. Each block therefore consists of $69b$ bits. A block of vertices is then constructed by first grouping the MSB-0 of each vertex coordinate, then the MSB-1, until finally the LSB. To avoid a size expansion of the encrypted vertex block in relation to the clear vertex block, we encrypt only k MSB among the $2k + 1$ bits of the vertex block.

Fig. 2 illustrates the preprocessing, the encryption and the decryption of a vertex block. We note α the payload in bits per block. To avoid a bit overflow when we embed a segment of a message in a block B, as illustrated in Fig. 2, α bits of the block B are set to zero in the clear domain. If k is the number of bits to encrypt in a block B, then the α LSB among the k MSB are set to zero, as illustrated in Fig. 2. We note B' the markable vertex block and O' the corresponding markable 3D object.

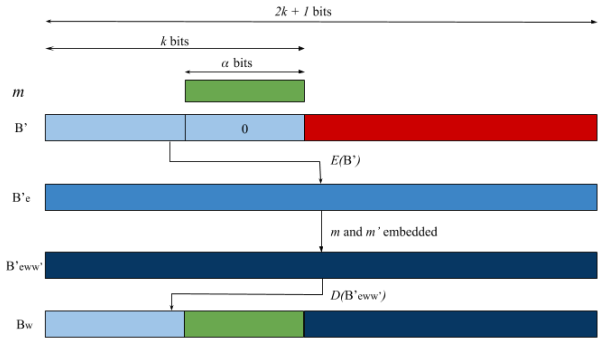


Fig. 2: Preprocessing, encryption and decryption of a vertex block B.

2.2. Encryption

We set the size of the encrypted vertex block $69b = 2k + 1$ bits and the block size b has to be odd. To encrypt the k MSB of the block B', which we note $B'_{k_{MSB}}$, we use:

$$\mathcal{E}(B'_{k_{MSB}}) = g^{B'_{k_{MSB}}} \times r^n \bmod n^2, \quad (2)$$

where (n, g) is the public key, r randomly generated, where $r \in (\mathbb{Z}/n\mathbb{Z})^*$, and $\mathcal{E}(\cdot)$ the Paillier encryption function.

We then obtain the $2k + 1$ encrypted bits which substitute all the bits of B', as illustrated in Fig. 2. We note B'_e the encrypted markable vertex block and O'_e the corresponding encrypted markable 3D object.

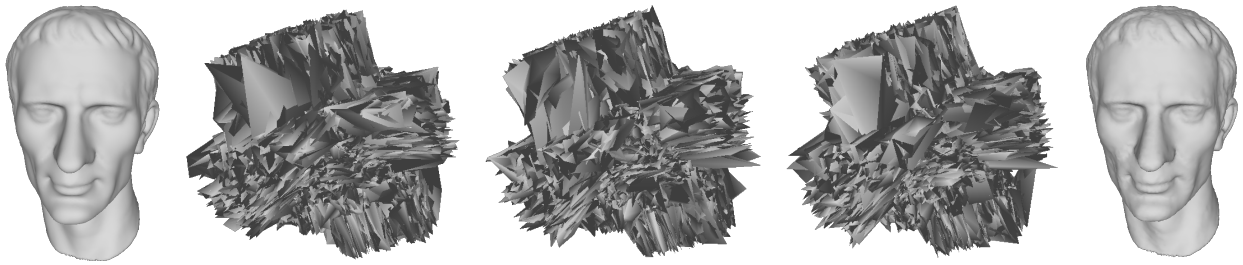
2.3. Data hiding in the encrypted domain

In order to embed a message m in each block B'_e of the encrypted markable 3D object O'_e, we use the Paillier additive homomorphic property, which indicates that a multiplication in the encrypted domain is equivalent to an addition in the clear domain. Therefore, to embed the message segment m, we have:

$$B'_{ew} = \mathcal{E}(B'_{k_{MSB}}) \times \mathcal{E}(m) \bmod n^2, \quad (3)$$

where B'_{ew} is the first tier marked encrypted block, $\mathcal{E}(\cdot)$ is the Paillier encryption function and $\mathcal{E}(B'_{k_{MSB}}) = B'_e$.

We note O'_{ew} the corresponding first tier marked encrypted 3D object. Note that since this multiplication in the encrypted domain is equivalent to an addition in the clear



(a) Original 3D object O (b) Encrypted markable 3D object O'_e (c) First tier marked encrypted 3D object O'_{ew} (d) Two tier marked encrypted 3D object $O'_{eww'}$ (e) Reconstructed marked 3D object O_w

Fig. 3: Obtained results on the 3D object *Caesar*, with a payload of 13.603 $(13.5 + 0.103)$ bpv.

domain, and since we have already cleared space for m by setting the α bits of the payload to 0, this operation is equivalent to an α LSB substitution in the clear domain:

$$\mathcal{D}(\mathcal{E}(B'_{k_{MSB}}) \times \mathcal{E}(m) \bmod n^2) = B' + m. \quad (4)$$

In order to preserve the visual quality of the original 3D object, Beugnon *et al.* showed that we need to conserve at least $23 - 16 = 7$ useful bits per coordinate (u), which results in $3u = 21$ MSB per vertex [19]. By respecting this, we do not compromise the visual quality of the decrypted 3D object. Therefore, α, the payload of a block B'_{ew} in bits is:

$$\alpha = k - 3u \times b \text{ bits}. \quad (5)$$

This results in a payload p, in bits per vertex (bpv) of:

$$p = \frac{\alpha}{b}\ bpv. \quad (6)$$

With our proposed approach it is also possible to embed a second tier message m' of up to 3 bits per vertex block, which exists only in the encrypted domain. The reconstructed marked 3D object in the clear domain remains unchanged by the second tier message. We note $O_{eww'}$ the corresponding two tier marked encrypted 3D object.

2.4. Data extraction and decryption

We note $B'_{eww'}$ the two tier marked encrypted vertex block. To extract the first tier message m in the encrypted domain, we multiply $B'_{eww'}$ by the multiplicative modular inverse of B'_e, corresponding to the encrypted block markable by data hiding and since we have already cleared space for m:

$$\mathcal{D}(B'_{eww'} \times {B'_e}^{-1} \bmod n^2) = m. \quad (7)$$

We specify that in this case the private key (μ, λ) is needed in order to retrieve m. The two tier marked encrypted 3D object $O'_{eww'}$ is decrypted using the private key (μ, λ):

$$\mathcal{D}(B'_{eww'}) = L({B'_{eww'}}^{\lambda} \bmod n^2) \times \mu \bmod n, \quad (8)$$

where $\mathcal{D}(\cdot)$ is the Paillier decryption function and $L(x) = \frac{x-1}{n}$, where $x \in \mathbb{N}^*$.

The decryption of the $2k + 1$ bits of the block $B'_{eww'}$ results in the original k MSB of the block B', as illustrated in Fig. 2. These bits replace the k MSB in the encrypted vertex block to construct B_w. This gives us the reconstructed first tier marked 3D object O_w. The first tier message can then be extracted from O_w in the clear domain.

3. EXPERIMENTAL RESULTS

3.1. Performance on a large dataset

We tested our method on the Princeton dataset [20] which consists of 380 different 3D objects. In order to be secure and for real life applications, we need a public key (n, g) where the size of n is at least an estimated 1000 bits. Therefore, we group the vertices into blocks of size $b = 29$ vertices per block, which gives us a key size of 1001 bits. Fig. 3 represents the 3D object *Caesar* after encryption, the first and second tier of data hiding and decryption, where the Hausdorff distances are 0.5073 for O/O'_e, 0.6478 for O/O'_{ew}, and $4.157\ 10^{-3}$ for O/O_w. With blocks of size $b = 29$ vertices, we obtain a first tier payload of 13.5 bpv and in order to limit the complexity we set the second tier payload to 3 bits per block, corresponding to a total payload of 13.603 bpv.

Princeton	O/O'_e	O/O'_{ew}	O/O_w
Mean	0.4677	0.4686	$3.769\ 10^{-3}$
Median	0.4833	0.4830	$3.744\ 10^{-3}$
St. Deviation	0.1101	0.1100	$0.443\ 10^{-3}$

Table 1: Hausdorff distances obtained when our method is applied to the 380 objects of the Princeton dataset [20].

Table 1 presents the Hausdorff distances when we compare the original 3D object O with the encrypted 3D object O'_e, the marked encrypted 3D object O'_{ew} and finally the marked decrypted 3D object O_w.

We observe that O/O'_e and O/O'_{ew} have very similar Hausdorff distances, represented in Table 1. Therefore we

Methods	Features					
	Encryption	Size expansion	Auxiliary file	Payload (bpv)	Data error	Marked 3D object
Jiang *et al.* [16]	Exclusive-or	No	No	0.37	Yes	No
Shah *et al.* [18]	Paillier cryptosystem	Yes	No	6 (3+3)	No	Yes
Yin *et al.* [17]	Exclusive-or	No	Yes	16.25	No	No
Proposed	**Paillier cryptosystem**	**No**	**No**	**{1-13.5} + {0-3}**	**No**	**Yes**

Table 2: Feature comparison between our proposed method and other existing state-of-the-art methods.

Methods	Encrypted domain payload (bpv)	Clear domain payload (bpv)	Mean HD (10^{-3})
Jiang *et al.* [16]	0.37 ± 0.05	0	1.01 ± 0.046
Shah *et al.* [18]	6 (3+3)	**3**	0.209 ± 0.176
Yin *et al.* [17]	$\mathbf{16.25 \pm 1.62}$	0	$(7.325 \pm 1.93)\ 10^{-3}$
Proposed	{1 - 4} (1 + {1 - 3 })	1	0.280 ± 0.219
Proposed	10 (7 + 3)	**7**	1.15 ± 0.911
Proposed	**16 (13 + 3)**	**13**	3.94 ± 2.43

Table 3: Comparison of the payload in both encrypted and clear domains, and of the distortion between our method and three significant current state-of-the-art approaches for the four 3D objects *Beetle*, *Mushroom*, *Mannequin* and *Elephant*.

can conclude that the content of the 3D object remains secure independently of whether there is an embedded message or not. Moreover, the median Hausdorff distance of O/O_w is $3.744\ 10^{-3}$, which indicates that the resulting marked 3D object O_w is very similar to the original 3D object O. We note that the mean distance is similar to the median distance.

3.2. Comparisons with previous work

Table 2 and Table 3 present comparisons between our proposed method and three existing state-of-the-art methods [16–18]. In particular, Table 2 shows that our proposed method is the only one to avoid size expansion, an auxiliary file and data error. Note also that our method is able to generate a marked 3D object in the clear domain. We note that the payloads of the methods of Jiang *et al.* [16] and Yin *et al.* [17] are the average payloads of the four 3D objects, as the payloads of these methods depend on the number of vertices eligible for embedding. The payloads of our proposed method and of Shah *et al.* are both divided into the payload in the clear domain and the possible payload in the encrypted domain. While both the proposed method and the method of Shah *et al.* [18] produce a marked 3D object in the clear domain, the proposed method has no size expansion and achieves a significantly higher first tier payload.

Table 3 shows comparisons in terms of Hausdorff distance and payloads in the encrypted domain and in the clear domain when applied to four 3D objects *Beetle*, *Mushroom*, *Mannequin* and *Elephant*. For this experiment, in order to be comparable with state-of-the-art methods, we encrypt these four 3D objects vertex by vertex. We note that the method of Yin *et al.* [17] has the best performance in terms of Hausdorff distance, but this is at the cost of an auxiliary file and a reconstructed 3D object without a message. While the methods of Yin *et al.* [17] and Jiang *et al.* [16] seek to reconstruct the original 3D object, the method of Shah *et al.* [18] and the proposed method generate a reconstructed marked 3D object and therefore do not seek to be statistically identical to the original 3D object. With our method, note that the reconstructed marked 3D object remains visually identical to the original 3D object. Our method is the only one to conserve a high payload in the clear domain. Once the 3D object is reconstructed, it remains marked with the first tier message of up to $13.5\ bpv$.

4. CONCLUSION

In this paper, we proposed a new high capacity two tier RDH-ED for 3D objects based on the Paillier cryptosystem. We describe a method which conserves the original format and avoids both size expansion and the use of an auxiliary file, while maintaining the visual quality of the 3D object. Our method uses a large key size, which makes it suitable for real life applications. Most importantly, our approach is a two tier method in which the first tier message can be extracted in either the encrypted domain or in the clear domain, producing a reconstructed 3D object marked with up to **13.5 *bpv***. The second tier message could be used as a flag in the case of multi-embedding.

In future work, the proposed method could be further improved by ordering the coordinates within the vertex block B according to the ascending order of the three exponents e of the vertex coordinates in Eq. 1. This would lead to less distortion in the case where the same number of bits are not encrypted in every coordinate.

5. REFERENCES

[1] K. Ma, W. Zhang, X. Zhao, N. Yu, and F. Li, "Reversible data hiding in encrypted images by reserving room before encryption," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 3, pp. 553–562, 2013.

[2] X. Cao, L. Du, X. Wei, D. Meng, and X. Guo, "High capacity reversible data hiding in encrypted images by patch-level sparse representation," *IEEE Transactions on Cybernetics*, vol. 46, no. 5, pp. 1132–1143, 2016.

[3] P. Puteaux and W. Puech, "An efficient MSB prediction-based method for high-capacity reversible data hiding in encrypted images," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 7, pp. 1670–1681, 2018.

[4] Y. Qiu, Q. Ying, X. Lin, Y. Zhang, and Z. Qian, "Reversible data hiding in encrypted images with dual data embedding," *IEEE Access*, vol. 8, pp. 23209–23220, 2020.

[5] W. Puech, M. Chaumont, and O. Strauss, "A reversible data hiding method for encrypted images," *Proceedings of SPIE - The International Society for Optical Engineering*, vol. 6819, 2008.

[6] W. Hong, T. Chen, and H.-Y. Wu, "An improved reversible data hiding in encrypted images using side match," *IEEE Signal Processing Letters*, vol. 19, pp. 199–202, 2012.

[7] X. Zhang, "Reversible data hiding with optimal value transfer," *IEEE Transactions on Multimedia*, vol. 15, no. 2, pp. 316–325, 2012.

[8] Y.-C. Chen, C.-W. Shiu, and G. Horng, "Encrypted signal-based reversible data hiding with public key cryptosystem," *Journal of Visual Communication and Image Representation*, vol. 25, no. 5, pp. 1164–1170, 2014.

[9] C.-W. Shiu, Y.-C. Chen, and W. Hong, "Encrypted image-based reversible data hiding with public key cryptography from difference expansion," *Signal Processing: Image Communication*, vol. 39, pp. 226–233, 2015.

[10] S. Xiang and X. Luo, "Reversible data hiding in homomorphic encrypted domain by mirroring ciphertext group," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 28, no. 11, pp. 3099–3110, 2018.

[11] X. Zhang, J. Long, Z. Wang, and H. Cheng, "Lossless and reversible data hiding in encrypted images with public-key cryptography," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 26, no. 9, pp. 1622–1631, 2015.

[12] S. Zheng, Y. Wang, and D. Hu, "Lossless data hiding based on homomorphic cryptosystem," *IEEE Transactions on Dependable and Secure Computing*, 2019.

[13] P. Puteaux, M. Vialle, and W. Puech, "Homomorphic encryption-based LSB substitution for high capacity data hiding in the encrypted domain," *IEEE Access*, vol. 8, pp. 108655–108663, 2020.

[14] Y. Ke, M. Zhang, and J. Liu, "Separable multiple bits reversible data hiding in encrypted domain," 02 2017, vol. 10082, pp. 470–484.

[15] L. Xiong, D. Dong, Z. Xia, and X. Chen, "High-capacity reversible data hiding for encrypted multimedia data with somewhat homomorphic encryption," *IEEE Access*, vol. PP, pp. 1–1, 10 2018.

[16] R. Jiang, H. Zhou, W. Zhang, and N. Yu, "Reversible data hiding in encrypted three-dimensional mesh models," *IEEE Transactions on Multimedia*, vol. 20, no. 1, pp. 55–67, 2018.

[17] Z. Yin, N. Xu, and F. Wang, "Separable reversible data hiding based on integer mapping and multi-MSB prediction for encrypted 3D mesh models," *arXiv*, pp. arXiv–1908, 2019.

[18] M. Shah, W. Zhang, H. Hu, H. Zhou, and T. Mahmood, "Homomorphic encryption-based reversible data hiding for 3D mesh models," *Arabian Journal for Science and Engineering*, vol. 43, no. 12, pp. 8145–8157, 2018.

[19] S. Beugnon, W. Puech, and J.-P. Pedeboy, "From visual confidentiality to transparent format-compliant selective encryption of 3D objects," in *2018 IEEE International Conference on Multimedia & Expo Workshops (ICMEW)*. IEEE, 2018, pp. 1–6.

[20] P. Shilane, P. Min, M. Kazhdan, and T. Funkhouser, "The Princeton shape benchmark," in *Proceedings Shape Modeling Applications, 2004.* IEEE, 2004, pp. 167–178.