International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys. 9, No.4 (July-2020)

http://dx.doi.org/10.12785/ijcds/090403

A Comparative Study Among Different Mathematical Sequences in 3D Image Steganography

Wassim Alexan[1], Mazen El Beheiry[1] and Omar Gamal–Eldin[1]

[1] *Faculty of Information Engineering and Technology, The German University in Cairo, Cairo, Egypt*

Received 06 Mar. 2020, Revised 19 Apr. 2020, Accepted 24 Jun. 2020, Published 1 Jul. 2020

Abstract: This paper proposes a double–layer message security scheme. The message is first encrypted using AES-128 and is then embedded within a 3D image using least significant bit (LSB) substitution. The LSB substitution is carried out using multiple mathematical sequences and a comparison between the performance of each sequence is investigated. The proposed system is evaluated using a number of performance metrics including the mean square error (MSE), the peak signal to noise ratio (PSNR), the entropy, the mean structural similarity index measurement (MSSIM), the R measurement, the normalized cross correlation (NCC), the image fidelity (IF) and the image distance (ID). Furthermore, a comparison between the proposed schemes and other proposed works from the literature is performed to demonstrate its superiority.

Keywords: AES, LSB, steganography, arithmetic sequence, geometric sequence, Fibonacci sequence, N-bit gray code, PSNR

1. Introduction

Because of the advancements in the field of digital communications, the internet has become the world's most used communication channel. Thus, the securing of the data being transmitted over this channel has become one of the world's main concerns. Cryptography and steganography play great roles in the securing of said data. Cryptography is the science of using mathematical protocols to prevent unintended third parties or the public from reading private messages [1]. It encrypts data (to keep messages secured) by transforming a coherent message into unintelligible text [2]. Steganography on the other hand is the science of hiding the existence of communication to prevent undesired third parties from knowing that a message is being transmitted [3]. Therefore, a system that combines both techniques provides high data security over the communication channel. Modern cryptographic algorithms can be divided into two categories, symmetric key ciphers and asymmetric key ciphers [4]. Symmetric key ciphers use one private key (shared between the transmitter and the receiver) both for encryption and decryption while asymmetric key ciphers use a public key for encryption and a private key for decryption. An example of symmetric key ciphers is the advanced encryption standard (AES). AES, also known as the Rijndael cipher, was created in 1998 by Vincent Rijmen and Joan Daemen and was established in 2001 by the US National Institute of Standards and Technology (NIST) as the standard encryption algorithm [5]. As of today, no practical and time-efficient attack against standard AES algorithms (AES–128, AES–192, and AES–256) exists [6]. It is the most commonly used security protocol worldwide, and remains to be the preferred encryption standard for governments, banks and high security systems around the world. An example of steganography is image steganography where a secret message is hidden within a cover image [7]. One of the most widespread techniques of steganography is least significant bit (LSB) substitution. It is a powerful yet simple steganography method. Each pixel in a grayscale image is comprised of 1 byte (or 8 bits) and thus can take on 256 different color values or intensities. LSB embedding simply replaces the least significant bit of each pixel with a bit from the data one wishes to transmit [8]. A very small variation occurs in the pixel colour intensity when LSB substitution is performed. However, the change is very subtle and cannot be distinguished by the naked eye and therefore goes unnoticed, meaning that the data is successfully embedded [9].

As previously stated, in the field of digital communications, it is very important to secure the channels over which data is being transmitted in order to avoid personal data theft, identity theft and fraudulent

E-mail: wassim.alexan@ieee.org, mazen.elbeheiry@gmail.com, omar.i.gamal@gmail.com

financial transactions. A security scheme in which both steganography and cryptography are applied is more than adequate to prevent any data being sent over a digital communication channel from being intercepted by unauthorized third parties.

Steganography and cryptography have been fields of great interest over the past couple of decades and a subject of many research papers. The authors of [10] propose a method for secured image steganography using cryptographic techniques. Their scheme transforms an image into ciphertext by using a simplified version of the DES (S–DES) algorithm. The text is then embedded within an image using a form of LSB substitution. The authors used a modified version of LSB embedding since the regular version can be vulnerable to steganalysis; the secret data bits are exclusive–ORed with the second least significant bit of the carrier image and then the LSB of the carrier image is replaced with the resultant bit. A weakness of this paper is that it does not measure any performance metrics, it only relies on visual analysis to differentiate between the cover and stego images. In [11], the authors propose a double layer message security scheme in which the data is first encrypted using either: DES, CAST5, or Blowfish algorithms. The encrypted message is then hidden inside of a 2D cover image using LSB embedding. The embedding process uses Recamán's sequence to determine the order of bytes to embed in. The performance of the scheme is measured in terms of the maximum embedding capacity, the mean square error (MSE), the peak signal to noise ratio (PSNR), the structural similarity index measurement (SSIM) [12] as well as entropy measures and histogram analyses. The authors were able to achieve very low MSE values (and consequently high PSNR values) as well as really high cover object capacity (53,000 characters). The authors of [3] propose a double layer reversible security scheme. The data is first encrypted using the Blowfish algorithm and then concealed within an image using LSB embedding. The specific color channels in which the embedding occurs are chosen in accordance with a Gray code sequence. The performance was measured using the PSNR, MSE and SSIM values. The authors of [13] propose a triple layer message security scheme. The message is first encrypted using AES–128 then a chaotic logistic map is applied on the output of the encryption process. The message is then embedded in a 2D image using LSB embedding following a zigzag pattern. Since the embedding is done in an unusual pattern, it is harder to detect by any unwanted parties. The proposed scheme's performance was measured using many different metrics such as the PSNR, MSE, SSIM, normalized cross correlation (NCC) and image fidelity (IF) values, as well as a visual histogram analysis. The authors were able to achieve low MSE values and consequently high PSNR values. In another paper [14], the authors proposed a double–layer security scheme in which the data is first encrypted using one of either AES–128, AES–192, AES–256, Blowfish or a Logistic Map. The second layer is of a steganographic nature where a number of complex mathematical sequences such as an arithmetic sequence, a triangle sequence and a square sequence are used to determine the color channel in which the encrypted bits would be embedded in. The performance of this scheme was evaluated in terms of the MSE, the PSNR, the SSIM, image fidelity (IF), embedding capacity, entropy values of the cover and stego images and the R measurement. The authors of [15] attempted to conceal a secret message within a colored image. They proposed encrypting the message using AES–256. As for the steganographic layer, two different techniques are proposed. Both of these techniques use LSB embedding, with the difference being the manner in which the pixels that are to be embedded within the message are chosen. An arithmetic sequence is employed for the first scheme to determine the location of embedding, whereas a geometric sequence is used for the second. In both these cases the specific color plane where the embedding occurs in each RGB pixel is based on the Rudin–Shapiro sequence. The authors measured the performance of their proposed schemes using the MSE, PSNR and entropy values, as well as a histogram analysis. The authors were able to achieve high PSNR values compared to its counterparts from the literature. In [16], two different schemes are proposed. Both of these schemes also use AES–256 to encrypt the hidden message. The steganography technique proposed by the authors is classic LSB embedding by means of color–plane cycling. The cycling follows a prime number sequence in the first scheme and the Fibonacci sequence in the second one. The MSE, PSNR and entropy values of the images, as well as a histogram analysis are used to evaluate the proposed schemes' performance. Using these metrics, the authors were able to show that the Fibonacci sequence was superior to the prime number sequence. The authors of [17] propose a novel technique for steganography based on a *matrix pattern*. In this technique, the message is embedded in only the blue layer of certain blocks. The blocks in which the embedding occurs are chosen randomly using a random number generator. Each block then forms a matrix of pixels referred to as a matrix pattern for each keyboard character, using the bit difference of neighbouring pixels. The secret message is then embedded in the remaining part of the block that has no role in the forming of the matrix pattern. The proposed scheme was shown to achieve better transparency in the stego–image than other works in the literature. The authors also tested their scheme against many frequency and spatial domain attacks such as: RS, Sample pair, X2 and DCT based attacks, and were able to prove its resiliency against malicious efforts. The authors of [18] also propose a steganography technique based on matrix patterns. The RGB image is first divided into square sized blocks then 95 matrix patterns are automatically formed using the 4th and 5th bit layers of the green layer of each block. These matrices are then assigned to 95 English keyboard characters. The embedding of the message is done in the blue layer of each block by adding the matrix patterns which are assigned to the characters of the secret message. The scheme was shown to have high resistance against steganalysis attacks including Regular Singular, Sample Pair, and PVD based attacks and has higher capacity than [17]. In [19], a combination of two steganography techniques is proposed, matrix pattern steganography such as in [17] and [18], and standard LSB substitution. The matrix pattern technique first divides the RGB cover–image into a number of non–overlapping blocks. The data is then hidden in the 4th through 7th bit layers of the blue layer of the image, by generating unique matrix patterns for each character in each block. In the proposed scheme, the first three bit layers of the blue layer of the image are used for LSB substitution whilst the 4th to 7th bit layers are used for the matrix pattern technique. The data can be embedded using either method; LSB is used for binary messages (which can be any digital media) while the matrix pattern method is only used when the data solely consists of text. The authors were able to achieve a high capacity and high PSNR values. Some papers embed the data in 3D images in an attempt to increase the capacity. In [20], the authors attempt to hide a secret message within a 3D image. To avoid distortion, the embedding is done in only one of the 3 dimensions ($x-$ direction). To evaluate the performance of their proposed scheme, the authors measured the PSNR, SSIM and the normalized absolute error (NAE) of the stego image in comparison with the cover image. The readings were recorded for the front view, side view, and top view of each image and were then averaged. The PSNR values that were achieved using this scheme were relatively low considering the size of the embedded message (4,473 characters). In another paper [21], the authors propose a high capacity steganographic scheme using 3D models. The algorithm re–triangulates a part of a triangle mesh and embeds the secret information into newly added positions of triangle meshes. The scheme's performance was measured using MSE and PSNR values, bit error rates (BER) and the normalized Hausdorff distances (HD). The authors were able to achieve very high PSNR values in comparison to other works in the literature. In [22], four layers of security are implemented in this paper as opposed to just two. The secret data is first encrypted using AES–128. The second layer involves encoding the encrypted data using a repetition code with a repetition index n that is suitable to overcome any added noise. The message is then embedded in the 3D image using regular LSB embedding. Finally, the encapsulated data is jammed, applied in the form of random noise addition. The authors measured the performance of this scheme using MSE and PSNR values. In [23], an adaptive 3D steganographic algorithm that considers surface complexity is proposed. The algorithm uses a vertex decimation process to determine its referencing neighbours in order to increase the accuracy of the complexity estimation for each embedding vertex. Afterwards, different amounts of data are embedded in each vertex according to its calculated surface properties. The proposed algorithm preserves the model's shape and minimizes distortion. The authors were able to achieve high data capacity and very good MSE and PSNR values. The authors of [24] propose a reversible data hiding technique in 3D models. The algorithm shifts the difference between the vertices to embed the secret data within them. Furthermore, the coordinates in which the data is embedded are chosen using a chaotic logistic map. The system was shown to withstand rotation, scaling and translation attacks. The algorithm also gives a unique mesh traversal system for every 3D model. This approach provides better embedding capacity than most previous approaches in the field of reversible data hiding in 3D cover models. In [25], another 3D object steganography scheme is presented. The authors hide a message in the indexed representation of a mesh by permuting the order in which faces and vertices are stored. This permutation is relative to a reference ordering that an encoder and decoder derive from the mesh connectivity. Since the proposed algorithm does not modify the geometry of the mesh, it is distortion free. The authors were able to achieve a data capacity that is almost an order of magnitude higher than previous steganographic methods involving polygonal meshes. The authors of [26] proposed to first encrypt the data using the Blowfish algorithm. The triangular meshes of various 3D models are then very slightly modified so that they include the secret data within them. The authors found their scheme to be resilient against many common attacks on 3D models such as scaling, translation and rotation. The performance of the proposed scheme was measured using the achieved capacity of the cover object, the embedding time, the extraction time, and the MSE. This approach resulted in one of the highest cover object capacities in the literature and was found to be very time efficient.

In this work, a double–layer message security system based on cryptography and steganography is proposed for secure information transmission between the sender and the receiver sides. The first layer is the cryptography layer where AES–128 is used for encryption. The second layer is of a steganographic nature where the encrypted message bits are hidden in a 3D image using LSB substitution. The image is first divided into slices, then the slices in which the embedding takes place are chosen using different mathematical sequences. The mathematical sequences used for the steganography layer are an arithmetic sequence, a geometric sequence, the Fibonacci sequence and an N–bit Gray code sequence. Beyond carrying out a comparative study among the various security schemes that adopt different mathematical sequences, the main contribution of this paper is the secure embedding of a very high capacity of bits through the use of a 3D image. The rest of the paper is organized as follows. Section 2 outlines the mathematical sequences employed in the proposed scheme. Section 3 describes the proposed message security scheme. Section 4 presents the results of the numerical analysis and finally Section 5 draws the conclusions.

2. MATHEMATICAL SEQUENCES

A. Arithmetic Sequences

An arithmetic sequence is a sequence in which the difference d between two consecutive terms is constant. The n^{th} term is defined as

$$a_n = a_0 + (n-1)d, \tag{1}$$

where $a_0$is the first term in the sequence. For example, the sequence 1, 6, 11, 16, ... is an arithmetic sequence with $a_0 = 1$ and $d = 5$ [27].

B. Geometric Sequence

A geometric sequence is a sequence where each term after the initial term, a_0, is obtained by multiplying the previous one by a fixed, non-zero number called the common ratio r [28]. The n^{th} term is given by

$$a_n = ar^{n-1}. \tag{2}$$

For example, the sequence 1, 2, 4, 16, 32, ... is a geometric one, with a_0= 1 and $r =$ 2.

C. Fibonacci Sequence

In mathematics, the Fibonacci numbers, commonly denoted by F_n form a sequence, called the Fibonacci sequence, such that each number is the sum of the two preceding ones, starting from 0 and 1 as in [29],

$$F_0 = 0,\ F_1 = 1, \tag{3}$$

and

$$F_n = F_{n-1} + F_{n-2}, \tag{4}$$

for $n > 1$.

In some references, F_0, the 0 is omitted, and the Fibonacci sequence starts with $F_1 = F_2 = 1$ [30]. The beginning of the sequence is thus 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144 ...

D. N-Bit Gray Code Sequence

Binary reflected Gray code sequence is a binary sequence in which two successive values differ only in one bit position [31]. So, if the bits in a number are summed, the sum of the next number should only change by one, with the sum alternating even and odd. For example, with $N = 3$, the Gray codes are 000, 001, 011, 010, 110, 111, 101, and 100, converting these numbers to decimal, the outcome sequence is 1, 3, 2, 6, 7, 5, 4, respectively.

3. PROPOSED MESSAGE SECURITY SCHEME

In this section, we outline the proposed 3D image steganography technique. The scheme consists of two main security layers. In the first layer, the secret message is encrypted using AES–128 with key length of 128 bits. In the second layer, 3D image steganography is performed to mask the secret data. In this step, a 3D cover image is sliced into 110 2D image layers and the encrypted bits are LSB embedded in these slices. Moreover, this algorithm is performed four times using four different sequences for the selection and the ordering of the slices, as the terms in each sequence correspond to the indices of image slices. The first sequence is the arithmetic sequence with a common difference of 2. The second sequence is the geometric sequence with a common ratio of 2. Then the third sequence is the Fibonacci sequence but since the first and second terms are both ‘1’s, the first term is omitted leaving the sequence with non–repeated numbers. Finally, the fourth sequence is the reflected binary code (RBC) which is also known as Gray code with $N = 6$. Upon the completion of the encryption process and the embedding of the secret data, the stego object is ready to be transmitted through a communication channel to the receiver. At the receiver side, the extraction process is done by extracting the LSB following the same sequences in a way similar to that used for embedding. Finally, the extracted bits are decrypted to form the secret message originally sent. Fig. 1 provides a graphical representation of the operation of the proposed scheme.

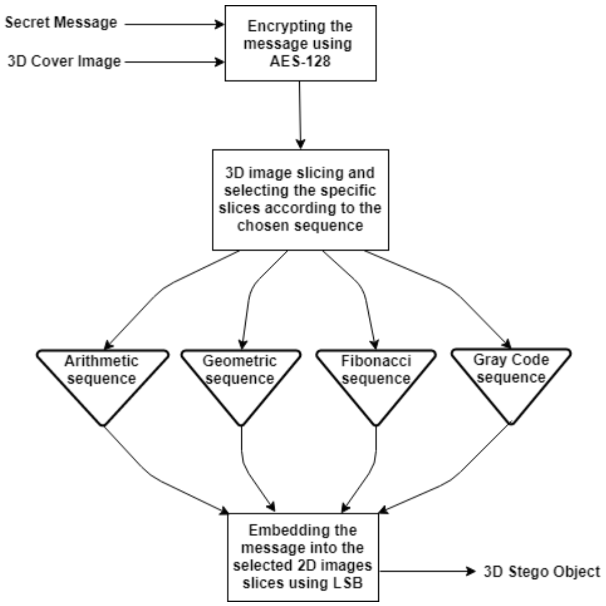
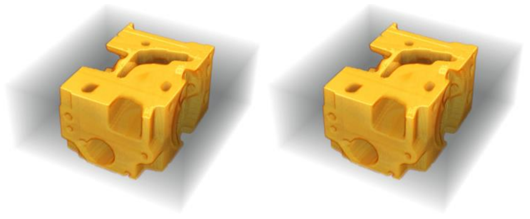

Secret Message
3D Cover Image
Encrypting the message using AES-128
3D image slicing and selecting the specific slices according to the chosen sequence
Arithmetic sequence
Geometric sequence
Fibonacci sequence
Gray Code sequence
Embedding the message into the selected 2D images slices using LSB
3D Stego Object

FIGURE 1. A BLOCK DIAGRAM ILLUSTRATING THE PROPOSED SECURITY SCHEME.



(a) Cover image. (b) Stego image.

Figure 2. CTEngine cover image (a) and stego image (b).

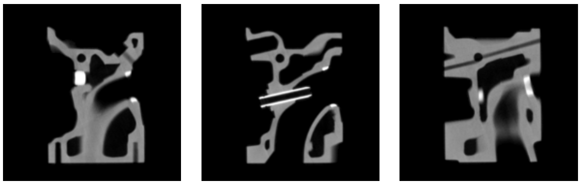
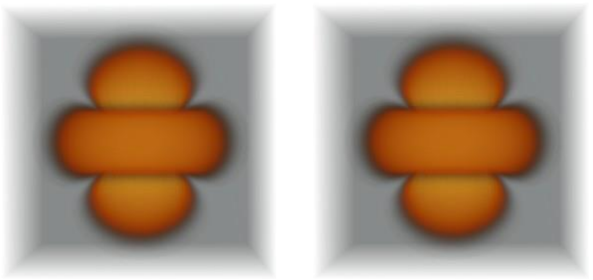


Figure 3. Three slices in 2D of the 3D image of CTEngine.



(a) Cover image. (b) Stego image.

Figure 4. Orbit cover image (a) and stego image (b).

TABLE I. PERFORMANCE EVALUATION OF THE PROPOSED SECURITY SCHEME USING CTENGINE IMAGE.

Performance metrics	**Mathematical Sequences**			
	Arithmetic	Geometric	Fibonacci	Gray-Code
MSE	0.04093	0.32213	0.22625	0.03519
PSNR	62.01	53.05	54.58	62.66
Hc	1.77153	1.77153	1.77153	1.77153
Hs	1.86015	1.83969	1.84056	1.86017
MSSIM	0.99738	0.98139	0.98691	0.99788
R	0.999993	0.999971	0.999965	0.999994
NCC	1	0.999976	0.999987	1
IF	0.999987	0.999907	0.999933	0.99998
Image Distance	0.203109	0.569792	0.477526	0.188332
Time [s]	3.47944	1.470148	1.739967	3.72005

4. NUMERICAL RESULTS

In this section, the performance of the proposed multiple layer message security scheme is evaluated and compared to its counterparts from the literature. The proposed security scheme is implemented using Wolfram Mathematica® 11.3 on a machine running a Windows 10 (64–bit) operating system with 16 GB of RAM and an Intel® Core™ i7–7700HQ CPU with a maximum clock rate of 3.8 GHz.

Our analysis starts with examining the behavior of the implemented scheme for each sequence with regards to various image performance metrics with a payload size (i.e. the length of the secret message) of 36,930 characters which are represented by 295,680 bits. Two different 3D cover images are considered. These are "CTEngine" and "Orbits" and are shown in Fig. 2 and Fig. 4 respectively. Fig. 3 shows three 2D slices of "CTEngine" as a sample of the overall number of slices which are 110 slices. Table I provides the performance results related to the "CTEngine" image for the four proposed sequences (e.g. arithmetic, geometric, Fibonacci, Gray–code) in terms of the extraction and decryption time, MSE, PSNR, the entropy, SSIM, R measurement, NCC, IF and the Euclidean distance. As expected, the Gray–code sequence with $N = 6$ provides the best performance. This is because this sequence has 64 elements which correspond to the number of slices ready for the message to be embedded in. As the number of bits to be embedded is 295,680 bits in the whole 3D image, then each slice has a capacity of 4,620 bits. Since the capacity in each slice is rather low, the change in each slice is considered too small and hence the Gray–code sequence achieves a very low MSE value as well as a relatively high PSNR value. However, it does so at a slightly higher extraction and decryption time over the other tested sequences. Furthermore, the arithmetic sequence resulted is a slightly worse performance since

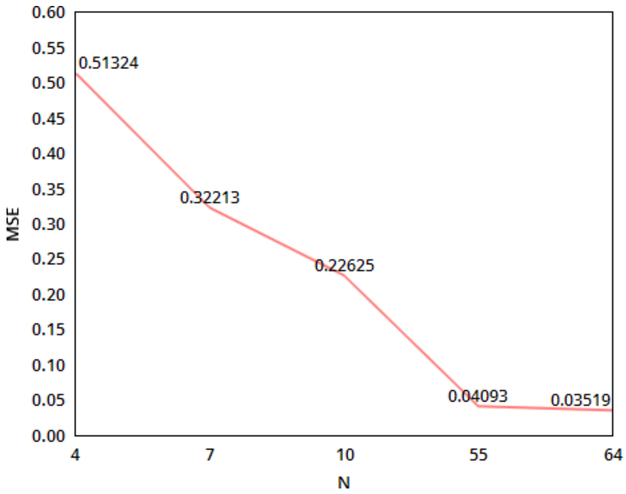


Figure 5. MSE behavior versus number of slices *N* used for hiding the message of length *l* = 36,930 using CTEngine image.

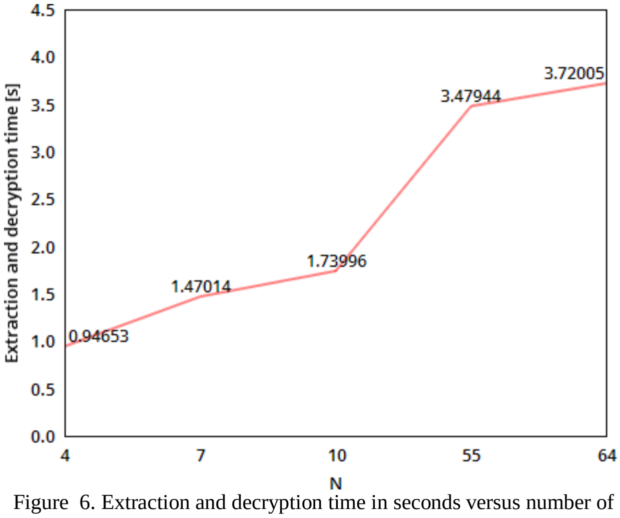


Figure 6. Extraction and decryption time in seconds versus number of slices N *used* for hiding the message of length l_m = 36,930 using CTEngine image.

the number of the slices used for embedding is lower than that of the Gray–code sequence with only 55 slices, so the capacity in each slice will be higher with 5,376 bits. In contrary to both arithmetic and Gray–code sequences, the geometric and Fibonacci sequences resulted in low performance metrics values due to the relatively much lower number of slices used for embedding with only 7 slices for the geometric sequence which is capable of hiding 42,240 bits per slice and 10 slices for the Fibonacci sequence with a capacity of 29,568 bits per slice. These results are illustrated graphically in Fig. 5 and Fig. 6, and they show that by increasing the number of slices used to hide the message in (where the message is of length l_m = 36,930 characters), the MSE increases proportionally, but the drawback is that the extraction and decryption time also increase.

The proposed algorithm using the Gray–code sequence is compared with a number of other 3D image steganography schemes from the literature and the results are tabulated in Table II. Regarding the security of the message, all schemes except [20] used a type of encryption standard, the scheme in [21] adds a layer of security on top of steganography, by using a simple key. On the contrary to our scheme and the scheme in [22] which employs AES–128, thus providing a higher security level. Moreover, the scheme in [32] used Blowfish encryption standard with a key length of 256 bits. While Blowfish is considered faster than AES, AES tends to be more secure and reliable. As for the relation between the number of bits embedded in a 3D image and the performance metrics results. Firstly, the algorithm proposed in [21] is a spatial domain scheme that used the method of triangular meshes formed by a stego–key, then the secret message is embedded into the vertices of theses triangles. Secondly, the scheme in [22] also proposed a spatial domain steganographic technique, where a 3D image is generated by using random numbers for each pixel and is then divided into 2D image slices. The message is then only embedded in the blue channels using LSB. Thirdly, the scheme in [20] takes the only one coordinate (e.g. *x*) from the 3D image and the embedding is carried out by converting the secret message into its ASCII format, then LSB is employed to replace 3 digits after the decimal point of each *x*–coordinate by the secret message. Moreover, the scheme in [32] presented a similar scheme to our proposed one by also using arithmetic and Fibonacci sequences for choosing the slices where the message is going to be embedded in, but as the results show, our scheme proved to be superior over the other schemes in terms of the relation between the number of embedded message bits and the performance metrics results. This is clearly seen in Table II, with the proposed scheme achieving the highest capacity, with an embedding of 295,680 bits within the 3D image. This is achieved at a relatively high PSNR value of 62.66 dB.

5. Conclusions

In this paper, we proposed a high capacity and high security spatial domain based 3D image steganography for embedding secret information in the 2D image slices of the 3D image model. The proposed scheme consists of two layers of security, where the first layer is of a cryptographic nature that uses AES–128 for encryption and decryption, while the second layer is of a steganographic nature that uses LSB technique for the embedding and extraction processes. A comparison in

TABLE II. PERFORMANCE EVALUATION OF THE PROPOSED SECURITY SCHEME USING CTENGINE IMAGE.

Author	***Image Model***	***Achieved Capacity [bits]***	***PSNR [dB]***	***MSE***
Thiyagarajan et al. [21]	Bunny	64496	55.3442	0.18930
	Cylinder	70352	58.703	0.064404
	Dinosaurs	75464	68.9317	0.007752
Salma et al. [22]	Patient's head	1792	53.1714	0.313284
Anish et al. [32]	Sports car	35784	41.25	N/A
	Flower pot	35784	42.6	N/A
Amr et al. [32]	CTEngine	75520	65.2548	0.01939
Proposed Scheme	CTEngine	295680	62.66	0.03519

terms of some image performance evaluation metrics is carried out between four mathematical sequences (e.g. arithmetic, geometric, Fibonacci and Gray–code), that are employed to choose the number and the order of slices in which the secret message will be hidden. The use of 3D images and these sequences makes it hard for third parties to intercept and reveal the data. The numerical results showed that the Gray–code sequence had the best capacity–performance relation, since it generates a larger number of slices than the other sequences, thus, embeds a smaller number of bits in each slice. Moreover, the results were compared with counterparts' schemes from the literature. The results indicate a high capacity, time efficient and a robust 3D image steganography scheme.

REFERENCES

[1] M. Bellare and P. Rogaway, "Introduction to modern cryptography," Ucsd Cse, vol. 207, p. 207, 2005. J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[2] F. Piper, "Cryptography," Encyclopedia of Software Engineering, 2002.

[3] G. Mostafa and W. Alexan, "A high capacity double–layer gray code based security scheme for secure data embedding," in 2019 International Symposium on Networks, Computers and Communications (ISNCC), Turkey, Jun. 2019

[4] C. Paar and J. Pelzl, Understanding cryptography: a textbook for students and practitioners. Springer Science & Business Media, 2009.

[5] J. Daemen, "" aes proposal: Rijndael," aes algorithm submission," http://csrc. nist. gov/encryption/aes/Rijndael. pdf, 1999.

[6] A. Biryukov, O. Dunkelman, N. Keller, D. Khovratovich, and A. Shamir, "Key recovery attacks of practical complexity on aes-256 variants with up to 10 rounds," in Annual International Conference on the Theory and Applications of Cryptographic Techniques, Springer, 2010, pp. 299–319.

[7] N. F. Johnson and S. Jajodia, "Exploring steganography: Seeing the unseen," Computer, vol. 31, no. 2, pp. 26–34, 1998.

[8] D. Neeta, K. Snehal, and D. Jacobs, "Implementation of lsb steganography and its evaluation for various bits," in 2006 1st International Conference on Digital Information Management, IEEE, 2006, pp. 173– 178.

[9] Y.-K. Lee, G. Bell, S.-Y. Huang, R.-Z. Wang, and S.-J. Shyu, "An advanced least-significant-bit embedding scheme for steganographic encoding," in Pacific-Rim Symposium on Image and Video Technology, Springer, 2009, pp. 349–360.

[10] S. Narayana and G. Prasad, "Two new approaches for secured image steganography using cryptographic techniques and type conversions," Signal & Image Processing: An International Journal (SIPIJ), vol. 1, no. 2, pp. 60–73, 2010.

[11] S. Farrag and W. Alexan, "Secure 2D Image Steganography Using Recamàn's Sequence," in 2019 International Conference on Advanced Communication Technologies and Networking (CommNet'19), Morocco, Apr. 2019.

[12] Z. Wang, A. C. Bovik, H. R. Sheikh, E. P. Simoncelli, et al., "Image quality assessment: From error visibility to structural similarity," IEEE transactions on image processing, vol. 13, no. 4, pp. 600–612, 2004.

[13] S. Farrag, W. Alexan, and H. H. Hussein, "Tripleâa¸slayer image ˘ security using a zigzag embedding pattern," in 2019 International Conference on Advanced Communication Technologies and Networking (CommNet'19), Morocco, Apr. 2019.

[14] M. Tarek, W. Alexan, and H. Hussein, "Double–Layer Image Security Scheme With Aggregated Mathematical Sequences," in 2019 International Conference on Advanced Communication Technologies and Networking (CommNet'19), Morocco, Apr. 2019.

[15] W. Alexan, H. Medhat, A. Hamza, and H. Hussein, "Sequence-based bit-cycling in double layer message security," in 2018 Advances in Wireless and Optical Communications (RTUWO), IEEE, 2018, pp. 23– 28.

[16] W. Alexan, A. Hamza, and H. Medhat, "An aes double–layer based message security scheme," in 2019 International Conference on Innovative Trends in Computer Engineering (ITCE), IEEE, 2019, pp. 86– 91.

[17] A. F. Nilizadeh and A. R. N. Nilchi, "Steganography on rgb images based on a" matrix pattern" using random blocks.," International Journal of Modern Education & Computer Science, vol. 5, no. 4, 2013.

[18] A. Nilizadeh, W. Mazurczyk, C. Zou, and G. T. Leavens, "Information hiding in rgb images using an improved matrix pattern approach," in 2017 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), IEEE, 2017, pp. 1407–1415.

[19] A. Nilizadeh and A. R. N. Nilchi, "A novel steganography method based on matrix pattern and lsb algorithms in rgb images," in 2016 1st Conference on Swarm Intelligence and Evolutionary Computation (CSIEC), IEEE, 2016, pp. 154–159.

[20] K Anish, N Arpita, H Nikhil, K Sumant, S Bhagya, and S. Desai, "Intelligence system security based on 3-d image," in Proceedings of the 5th International Conference on Frontiers in Intelligent Computing: Theory and Applications, Springer, 2017, pp. 159–167.

[21] P Thiyagarajan, V Natarajan, G Aghila, V. P. Venkatesan, and R Anitha, "Pattern based 3d image steganography," 3D Research, vol. 4, no. 1, p. 1, 2013.

[22] S. Elsherif, G. Mostafa, S. Farrag, and W. Alexan, "Secure message embedding in 3d images," in 2019 International Conference on Innovative Trends in Computer Engineering (ITCE), IEEE, 2019, pp. 117–123.

[23] Y.-Y. Tsai, "An adaptive steganographic algorithm for 3d polygonal models using vertex decimation," Multimedia Tools and Applications, vol. 69, no. 3, pp. 859–876, 2014.

[24] A. Girdhar and V. Kumar, "A reversible and affine invariant 3d data hiding technique based on difference shifting and logistic map," Journal of Ambient Intelligence and Humanized Computing, pp. 1–15, 2019.

[25] A. Bogomjakov, C. Gotsman, and M. Isenburg, "Distortion-free steganography for polygonal meshes," in Computer graphics forum, Wiley Online Library, vol. 27, 2008, pp. 637–642.

[26] S. Farrag and W. Alexan, "A High Capacity Geometrical Domain Based 3D Image Steganography Scheme," in 2019 International Conference on Advanced Communication Technologies and Networking (CommNet'19), Morocco, Apr. 2019.

[27] W. Alexan, H. Medhat, A. Hamza, and H. Hussein, "Sequence–Based Bit–Cycling in Double Layer Message Security," in 2018 Advances in Wireless and Optical Communications (RTUWO), IEEE, 2018, pp. 23– 28.

[28] S. A. Parah, J. A. Sheikh, U. I. Assad, and G. M. Bhat, "Hiding in encrypted images: A three tier security data hiding technique," Multidimensional Systems and Signal Processing, vol. 28, no. 2, pp. 549–572, 2017.

[29] É. Lucas, Le calcul des nombres entiers. Le calcul des nombres rationnels. La divisibilité arithmétique. Gauthier-Villars, 1891, vol. 1.

[30] M. Beck and R. Geoghegan, The Art of Proof: basic training for deeper mathematics. Springer Science & Business Media, 2010.

[31] M. Ali, M. N. Islam, and A. Foysal, "Algorithms for generating binary reflected gray code sequence: Time efficient approaches," in 2009 International Conference on Future Computer and Communication, IEEE, 2009, pp. 79–83.

[32] A. S. Amin, "Stegocrypt3d: 3d image slicing and blowfish," B.S. Comms, IET Faculty, GUC, Cairo, Egypt, 2019.

Wassim Alexan was born in Alexandria, Egypt, in 1987. He received the BSc, MSc and PhD in Communications Engineering and an MBA from the German University in Cairo (GUC), respectively in 2010, 2012, 2017 and 2019. From 2010 till 2017 he was with the Mathematics department and is now an assistant professor at the faculty of Information Engineering and Technology at the GUC. His research interests lie in the fields of wireless communications, security, image and signal processing.

Mazen El Beheiry was born in Cairo, Egypt, in 1998. He received the BSc in Communications Engineering from the German University in Cairo in 2019. He is currently enrolled in a pre-master program at the same university. His research interests lie in the fields of wireless communication, security and steganography.

Omar Islam Gamal-Eldin was born in Cairo, Egypt, in 1995. He received the BSc in Communications Engineering from the German University in Cairo in 2019. He is currently enrolled in a pre-master program at the same university. His research interests lie in the fields of steganography, cryptography and wireless communications.