Received 19 October 2023, accepted 19 November 2023, date of publication 24 November 2023,
date of current version 29 December 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3336682

APPLIED RESEARCH

Secured Gray-Code-Based Steganographic Technique in Geometrical-Based Domain

AYA Y. ALKHAMESE[1], HEWAYDA A. ELGAWALBY[1], IBRAHIM M. HANAFY[2], WAEL A. AWAD[3], AHMED ISMAIL EBADA[3,4], S. S. ASKAR[5], AND MOHAMED ABOUHAWWASH[6,7]

[1]Department of Physics and Engineering Mathematics, Faculty of Engineering, Port Said University, Port Said 42526, Egypt
[2]Department of Mathematics and Computer Science, Faculty of Science, Port Said University, Port Said 42526, Egypt
[3]Department of Computer Science, Faculty of Computers and Artificial Intelligence, Damietta University, Damietta 34519, Egypt
[4]Department of Information Systems, Faculty of Computers and Artificial Intelligence, Damietta University, Damietta 34519, Egypt
[5]Department of Statistics and Operations Research, College of Science, King Saud University, Riyadh 11451, Saudi Arabia
[6]Department of Mathematics, Faculty of Science, Mansoura University, Mansoura 35516, Egypt
[7]Department of Computational Mathematics, Science, and Engineering (CMSE), Michigan State University, East Lansing, MI 48824, USA

Corresponding author: Mohamed Abouhawwash (abouhaww@msu.edu)

This project is funded by King Saud University, Riyadh, Saudi Arabia. Researchers Supporting Project number (RSP2024R167).

ABSTRACT The past decades witness a tremendous exchange in data and information in almost all domains. This leads to the need for applying data security to ensure information safety during communication. One of the main used technique is the steganography. Steganography is a technique that involves hiding information within objects, such as images, audio, video, or 3D objects, without leaving any noticeable alterations. We propose a 3D steganographic technique that increases security using Gray-code sequence and a Least Significant Bit technique. We construct the 64-binary representation for the 3D cover-object. A Gray-code sequence defined the 3D object vertices that will be utilized for concealing the information. The binary representation of the information is to be concealed in the least significant bits of either the x- or the y-components of the defined vertices. The least significant bits, are the last two bits in the binary representation of the vertex components. Exploitation the binary representation, gives us the capability of increasing the data security, and the data capacity. The proposed steganographic technique has been evaluated through multiple evaluation metrics to assess its performance; including Mean Square Error Ratio, Peak Signal-to-Noise Ratio, Histogram, and Normalized Correlation Experimental results, indicate that the security level of the proposed technique is superior comparing to several existed techniques. Moreover, when testing against some common attacks such as the noise, the median, the Gaussian and the Laplacian filters; the results show the efficiency and the robustness of the proposed technique.

INDEX TERMS 3D steganographic technique, gray-code, information hiding, peak signal-to-noise ratio.

I. INTRODUCTION

As information technology has advanced, the issue of information security has emerged as a significant concern within the interactive environment. Several techniques were provided to secure the data from the sender to the receiver as shown in Figure 1. Information hiding and cryptography play a remarkable role in protecting sensitive information. Cryptography protects sensitive information by converting them from a readable format into an unreadable one. Several techniques can be found in literature such as the work introduced in [1] and [2]. The two primary categories of techniques for concealing information are steganography and watermarking. Watermarking provides protection against illegal data transmission by embedding the watermark into digital signals. Numerous methods are available in the literature, including those introduced in references [3], [4]. Steganography conceals information within data without producing any noticeable effect on the object [5]. Steganography differs from cryptography in that cryptography scrambles the information to make it incomprehensible by unauthorized parties but it may arouse suspicion. Whilst steganography conceals the information within a cover-object to obscure its existence and no one can doubt the existence of hidden

The associate editor coordinating the review of this manuscript and approving it for publication was Songwen Pei.

information [6]. In watermarking, the embedded data contains supplementary information related to the cover-object, with the primary focus is the cover-object itself. In steganography, the a cover-object is utilized as a carrier to conceal information within it, making the hidden message the primary object of the communication channel.

The remaining sections of our paper are constructed as: in Section II, we present an overview of steganography, as well as 3D object steganography with its domains. The Least Significant Bit (LSB) technique and the Gray-code sequence are also discussed. In Section III, we show some of the existing works in the geometrical-based domain. Section IV explains the embedding algorithm and the extraction algorithm of our technique with illustrating example, and charts. In Section V, we involve an assessment of our technique and a comparison of the numerical results with those of similar techniques found in the literature. Finally, Section VI draws a conclusion and offers recommendations for future research directions.

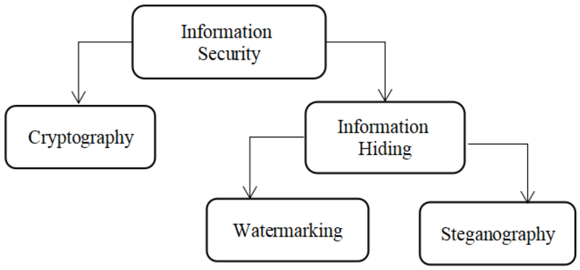


FIGURE 1. Information security system.

II. STEGANOGRAPHY

Steganography is the art and the science of hiding information and keeping the security of this information. The term "Steganography" finds its origins in the Greek words "stegano," denoting "covered," and "graphein," denoting "writing," which directly translates to "covered or hidden writing.". An well-known illustration of real-life steganography involves the utilization of invisible ink for writing on paper. The message embeds upon the paper drying and appears when the paper is exposed to heat. While modern steganography commonly employs digital media to conceal confidential messages and transmit them through the Internet. The steganographic system consists of the cover-object, the stego-object, the secret message, the embedding algorithm, and the extraction algorithm. The original object is to be called a cover-object, while the object generated after hiding the message is to be called a stego-object. On the one hand, the transmitter utilizes an embedding algorithm to create the stego-object; on the other hand, the receiver uses an extracting algorithm to obtain the embedded message [5], [6].

Security, robustness, and capacity are the significant attributes of any steganographic system. In any steganographic system, the primary concern is security, which involves preventing any unauthorized individuals from accessing a concealed message. Capacity refers to the maximum size of the concealed information in an object without introducing any noticeable distortion to it. Robustness measures the ability to endure various digital attacks, such as affine transformation, vertex reordering, noise addition, and smoothing. The interrelation between these attributes can be illustrated using the steganography triangle, as depicted in Figure 2. To improve one attribute, two other attributes must be sacrificed. For instance, if security is increased, capacity may be at risk of being compromised. Similarly, if there is a high level of robustness, both capacity and security decreases [7].

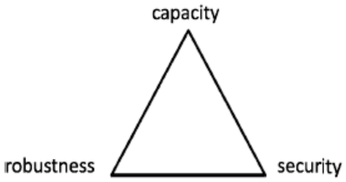


FIGURE 2. Steganography triangle.

Steganography is widely used in several fields as medical, military, multimedia, and industry. In the medical field, steganography is utilized for conserving the private information of privacy of patients' data. A connection is preserved by the patient within the image without effecting on its quality. Steganographic systems is used in the military field by transmitting information in a secure manner that the enemies cannot observe the presence of the hidden information. Steganographic techniques are used in the multimedia applications for marking the copyright of a specific media. Despite of watermarking, steganography has more significance for the cover media than the secret data [8]. Here are a few examples of applications [8]: Smartsteg on mobile devices [9], safeguarding multimodal biometric data [10], ensuring Intellectual Property (IP) protection, and even embedding personal information within smart identity cards [11].

A. STEGANOGRAPHY CATEGORIES

Steganographic techniques are categorized according to the category of the cover-object; the need to retrieve the original cover-object, and the type of extraction algorithm.

1) CATEGORIES ACCORDING TO THE TYPE OF COVER-OBJECT

Digital steganography can be distinguished into several categories based on the type of digital cover-object chosen. The steganographic category is named according to the digital object used as shown in Figure 3.

1) Image steganography: It is the most commonly used type of steganography. The information is embedded in the pixels of the 2D image in a way that is impossible to be detected by human eyes.

2) Text steganography: It is one of the oldest types of steganography. As it is a way of hiding texts inside another.
3) Audio steganography: It conceals the information into a frequency that is out of human hearing range.
4) Video steganography: It is the technique for embedding the information in a video file. The advantage of this type is that a video file contains a series collection of sounds and images. A large amount of data can be embedded without distortion.
5) Protocol steganography: The message can be concealed in the TCP/IP packet in unused or optional fields.

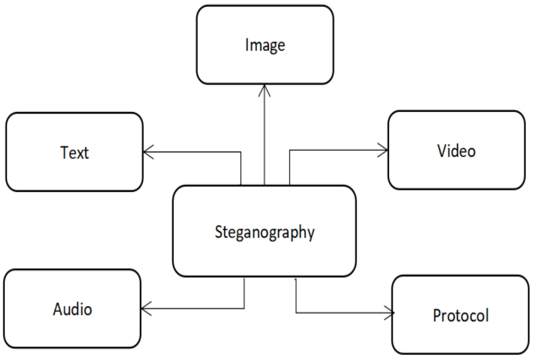


FIGURE 3. Steganography categories according to type of cover-object.

2) CATEGORIES ACCORDING TO THE THE SECRET KEY

There are three types of the steganographic techniques according to the secret key (pure steganographic technique, secret key steganographic technique and public key steganographic technique).

1) Pure Steganographic Technique: It is a steganographic technique that doesn't need the exchange of a stego key between the communication partners before sending secret message. If any attacker knows the encoding algorithm, this technique does not become secure.

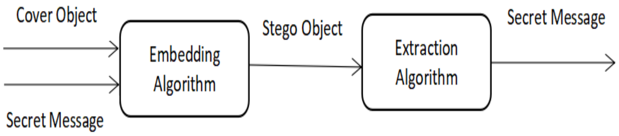


FIGURE 4. Pure steganographic technique.

2) Secret Key Steganographic Technique: This steganographic technique operates with a shared secret key accessible to both the sender and receiver.
3) Public Key Steganographic Technique: This steganographic technique contains a public key and a private key. The public key is utilized through the embedding algorithm. The secret key is utilized through the extraction algorithm to obtain the secret message.

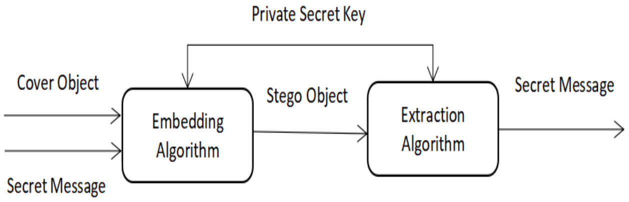


FIGURE 5. Secret steganographic technique.

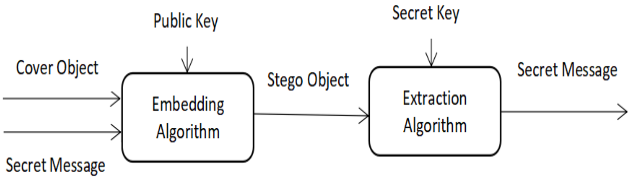


FIGURE 6. Public steganographic technique.

3) CATEGORIES ACCORDING TO THE NEED TO RETRIEVE THE COVER-OBJECT

The steganographic techniques can be designed with two types: reversible or irreversible.

1) Irreversible Steganographic Technique: The significance is placed on the message, while the cover-object is just utilized for concealing the message. The original object cannot be restored from the stego-object in the extraction process [8].
2) Reversible Steganographic Technique: It is one of the most important fields in steganography, both cover-object and secret message is important. A reversible steganographic techniques can perfectly restorative the original object from the stego-object after the hidden message has been extracted. This technique has particularly valuable in advanced communication scenarios contexts such as military and medical applications, unlike common communications [8].

4) CATEGORIES ACCORDING TO THE TYPE OF EXTRACTION ALGORITHM

The steganographic techniques can be classified into two categories according to the type extraction algorithm:

1) A Blind Steganographic Technique: It doesn't requires the cover-object for the extraction phase.
2) A Non-blind Steganographic Technique: It requires the cover-object for the extraction phase.

B. 3D-OBJECT STEGANOGRAPHY

Images are a perfect camouflage medium for digital steganography. The large size of the images makes the process of hiding information not detected by unaware users. In the image steganography process, the message is embedded without detection and the cover-object preserves its original appearance [6]. Multimedia files in 3D are increasingly important in many standard applications, including education, entertainment, games, business, video conferencing, marketing, advertising, and more. Consequently, numerous 3D-data hiding techniques have been developed by researchers and academics [12]. The primary benefit of utilizing a 3D object over a 2D image in steganographic techniques is its capability to hide more bits of the secret information due to the larger number of vertices in a 3D object. 3D-object steganography is the process of concealing secret message 3D object by means of remaining imperceptible to Human Vision System (HVS).

A 3D object is composed of a collection of points, each point is known as a vertex. Each vertex is defined by the x, y, and z- component. An edge is created as resulting of the connection between two vertices. A mesh is created by combining a set of vertices with a set of edges. When a closed set of edges forms a shape, it is referred to as a face. A mesh that consists of triangular faces is called a triangle mesh, while one with quadrilateral faces is termed a quad mesh. In Figure 7, you can observe a 3D representation of a horse object, showcasing both a triangle mesh and a quad mesh variant. There are multiple file formats available for storing a 3D object, including: .obj,.m,.ply, and others.

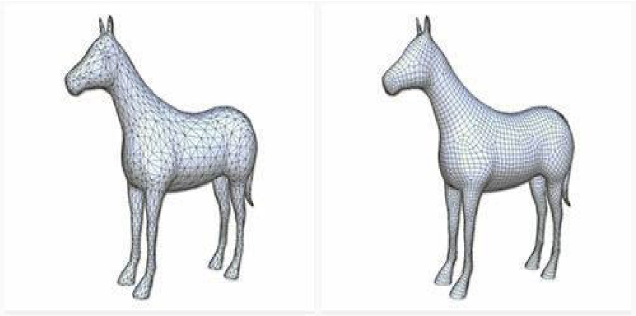


FIGURE 7. **Triangle mesh and quad mesh [13].**

3D-object steganography can be utilized within one of three different domains, namely geometry-based steganography domain, topology-based steganography domain, and representation-based steganography domain.

1) Geometry-based Steganography Domain: The 3D objects geometrical components are employed for concealing messages. However, concealing in these components is susceptible to affine transformations including rotation, that can impact the concealed information [14]. The primary benefit of using the geometrical-based techniques is the achieved high capacity compared to other techniques in the other two domains [15].
2) Topology-based Steganography Domain: Topology-based steganographic techniques involves altering the connectivity of a 3D object's vertices or topology to conceal the message. 3D objects contain more connectivity information than the geometrical components that are used in geometry-based steganography techniques. The techniques in the topology-based domain preserve the geometry of the mesh surface [5], [15].
3) Representation-based Steganography Domain: Secret messages are embedded in this domain by utilizing the redundancy in mesh representation. The redundant information in the mesh is added and manipulated to conceal the message. The embedding capacity in this domain is comparatively lower than that offered by the other two domains. As a result, there are limited contributions made in this domain [15].

C. GEOMETRY-BASED STEGANOGRAPHY DOMAIN

The integration of steganography into 3D objects involves varied topological and geometrical operations with several embedding algorithms [14]. The techniques within the geometrical domain can be categorized into two primary categories: concealing information within the spatial domain and concealing it within the transform domain. In spatial domain, techniques involve the direct concealment of messages within the cover-object. In the frequency domain, the cover-object is initially converted into frequency coefficients which are obtained as a result of applying a transform as Wavelet transform (WT). Then, messages are concealed with the coefficients of these transformations. The spatial domain techniques have been the primary focus of research due to two important reasons. Firstly, techniques of the spatial domain offer a higher embedding capacity. Furthermore, the conversion between the spatial and the frequency domains introduces further complexity for the hiding and retrieving techniques.

One of the most utilized image steganographic techniques in the the spatial domain is the LSB technique. In this technique, we re-define The least significant bit (or bits) of the pixel in a cover-image, according to the message. For an illustration, if we intend to embed the character 'A' within an 8-bit image. The binary representation for eight consecutive pixels, beginning from the top left corner of the image, is as follows:

11001001 00100111 11101011 10101100
00011011 11001100 01110100 01110100

The binary representation of the letter 'A' is (01100101). It is concealed in a sequential manner to the least significant bits (the least valued bits) of the corresponding binary representation of image pixels.

Ultimately, the bit pattern's output will be as depicted below:

1100100**0** 00100111 11101011 10101100
0001101**0** 1100110**1** 01110100 0111010**1**

So in this technique, only four bits of the 8 pixels are changed to embed this character into this part image. These four changed bits are shown bold.

To apply the LSB technique, one might conceal the information keeping the same order of the pixels of the cover-object; which is known as a successive substitution. However, for more security, one might construct a pseudo-random number generator to embed in the cover-object pixels at a specific order [16]. This results from a minor modification to the pixel, that is imperceptible to the human eye.

A binary numbering system, namely, the Gray-code; was introduced by Frank Gray in 1953. This system, follows a methodology to arrange the binary numbers in a way such that any two successive numbers defer only in one digit. That means one bit 0 can be altered to 1, or a bit 1 can be altered to 0 [17]. In this work, the Gray-code was utilized due to its simplicity, efficient hardware implementation, and its excellent power to enable error–correction in digital communications [14]. The Gray-code sequence has a high embedding capacity in steganographic system comparing to many other sequences, as it generates more numbers rather than many other sequence. Equation 2 is employed for converting the numbers $B_0, B_1, B_2 \ldots . B_n$ to the numbers of Gray-code sequence donated as G_0, G_1, G_2, ... G_n can be defined as follows:

$$G_k = \begin{cases} B_k & \text{if } k = n \\ B_{k+1} \oplus B_k & \text{if } 1 \preccurlyeq k \preccurlyeq n-1 \end{cases} \quad (1)$$

Equation (2) is utilized to covert the numbers of the Gray-code sequence.

$$B_k = \begin{cases} G_k & \text{if } k = n \\ B_{k+1} \oplus G_k & \text{if } 1 \preccurlyeq k \preccurlyeq n-1 \end{cases} \quad (2)$$

In these equations, the operation ⊕ is a bit-wise XOR operation [17]. Thus using the Gray-code, the leftmost or the most significant bit of Gray-coded binary is same to that of the binary bit. Furthermore, the 2^{nd} significant bit of the Gray-coded binary is determined using the operation of XOR between the 1^{st} and the 2^{nd} bits. In the same way, the 3^{rd} Gray-coded binary is calculated by reiterating the same XOR operation for the 2^{nd} and 3^{rd} bits and so on. For example, a binary number of 10111001 has a corresponding Gray-coded binary of 11100101.

Furthermore, Table 1, provides decimal numbers, natural binary, Gray-code binary, and decimal of Gray. In the Gray-code sequence, only a single bit changes between each pair of adjacent Gray-code numbers. This property enables a system designer to perform error checking, as any occurrence of more than one bit changing state between adjacent numbers indicates that the data is incorrect [18]. The number of integers in the Gray-code sequence presents as {1, 2, 4, ..., 2^n} in which n is the number of bits. For instance, if n equals 3, the Gray-code sequence consists of the binary numbers 000, 001, 011, 010, 110, 111, 101, and 100. If we convert these binary converting these binary representations to decimal, we obtain the resulting sequence of 0, 1, 3, 2, 6, 7, 5, and 4, respectively [19].

TABLE 1. The decimal, binary, and gray-coded binary representations for numbers 0 to 7, as well as the decimal equivalent of the Gray-coded representation.

Decima l	Binary	Gray-coded binary	Decimal of Gray
0	0000	0000	0
1	0001	0001	1
2	0010	0011	3
3	0011	0010	2
4	0100	0110	6
5	0101	0111	7
6	0110	0101	5
7	0111	0100	4

III. RELATED WORK

In literature, several techniques were produced, based on embedding the message in the 3D-cover object in some geometric domain. For instance, the authors in [20] introduced a steganographic technique with a high embedding rate using the triangulated mesh of the 3D objects. In this technique, a part of the triangle mesh is re-triangulated to conceal the messages in newly added positions. The 3D mesh was also used in [21], where the authors perform perform the embedding process in vertices of a 3D mesh utilizing a Hamiltonian path. Along this path, alterations are applied to the vertices by adjusting the components within the Spherical Coordinate System (SCS). Also, in [22], a 3D-object steganography technique was proposed. This technique conceals the encrypted message in the polygons of the object. The vertices of polygons are utilized for hiding the message. If the value of the embedded bit is 1, a random odd number between 1 and 9 is selected for the 4th or 5th decimal place of the vertices of polygons. Conversely, if the embedded bit value is 0, a random even number between 1 and 9 is chosen for the 4th or 5th decimal place. In [23], the authors used a simple algorithm in which the decimal representation of the secret data is concealed in the value of the x-component. Using four layers of security, the authors in [24], propose to conceal the information in a geometrical domain-based technique. The first layer involves the encryption of the message using AES–128. The next layer contains encoding the encrypted message using a repetition code with a repetition index n that is used to overcome any added noise. In the third layer, the message is hidden using the LSB technique. Finally, the encapsulated message is jammed and applied in the form of random noise addition. In [25], the authors rely on employing the vertex normal to determine the embedding process. The authors in [26], propose a 3D geometrical technique using difference shifting. To conceal the message, this technique shifts the difference between the vertices. The message is concealed in the components chosen utilizing a chaotic logistic map. Consequently, a value of the vertex pair in a chosen component axis is selected. Next, the difference in this value is calculated and then altered to conceal the message. Next, the new component values are calculated using the modified distance. Two-message security steps technique was introduced in [19]. The first step requires encrypting the message with AES-128. The second step requires utilizing the least significant bit (LSB) technique to hide encrypted message. Several mathematical sequences such as arithmetic, geometric, Fibonacci, and Gray-code are utilized. A comparison is made to evaluate the effectiveness of each sequence. The outcomes indicate the Gray-code sequence offers the most favorable capacity and performance relationship. In [14], A twofold layer algorithm was used for insecure messages concealed in 3D objects. Blowfish or AES–128 algorithms are carried out in a cryptography layer and a Gray-code sequence in a steganography layer. The Gray-code provides the order of the vertices over which the secret messages are hidden.

IV. THE PROPOSED HIGH SECURED GRAY-CODE BASED STEGANOGRAPHIC TECHNIQUE FOR 3D OBJECT IN A GEOMETRIC DOMAIN

In this section, we propose a steganography technique that takes advantage of the geometry of 3D objects. The new technique uses the Gray-code sequence to determine the vertices for hiding the message based on. The Gray-code sequence is utilized to enhance capacity and security. The LSB technique is also used to increase the security of our technique. Our technique was tested against common attacks such as noise, and filters to assess its efficiency and robustness. The proposed technique is composed of two phases: an embedding and an extraction.

A. THE PROPOSED EMBEDDING PHASE

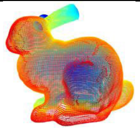
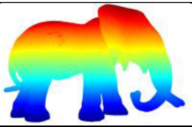
To commence, the message intended for hiding is first transformed into ASCII code and subsequently converted into an its 8-bit binary representation resulting in a binary bit stream. We calculate the length of the message and the size of 3D-cover objects to select an appropriate object with sufficient size to contain this binary representation of the message. The geometric data of 3D object is utilized to extract the vertices and convert them into its 64-bit binary representation. The Gray-code sequence is created using 24 bits. Then, it is converted to decimal numbers. Based on the Gray-code number, the message is concealed in the least valued bits of the vertices using the LSB technique.

1) THE PROPOSED EMBEDDING ALGORITHM

To get the stego-object, the following steps are to be included:

a) Obtain the 3D cover-object vertices.
b) Convert these vertices to binary representation.
c) Change the secret message into its binary representation.
d) Generate the Gray-code sequence using 24 bits.
e) If the Gray-code number is equal to 0, one bit of the message is concealed in the least valued bit of the x-component.
f) If the Gray-code number is equal to 1, one bit of the message is concealed in the least valued bit of the x-component.
g) If the Gray-code number is more than 1, it is a prim even number: two bit of secret message is concealed in the least valued bit and the bit immediately preceding of x-component.
h) If the Gray-code number is a non-prim even number: one bit of secret message is concealed only in the least valued bit of the x-component.
i) If the Gray-code number is a prim odd number: two bit of secret message is concealed in the least valued bit and the bit immediately preceding of y-component.
j) If the Gray-code number is a non-prim odd number: one bit of secret message is concealed only in the least valued bit of the y-component.
k) Construct the stego-object.

TABLE 2. **Some of used experimental 3D objects and their number of vertices.**

3D Object		Number of Vertices
Horse		15,336
Bunny		35,947
Elephant		162,487
Armadillo		172,974

The embedding algorithm's procedural steps are depicted in the chart displayed in Figure 8.

2) EMBEDDING PHASE ILLUSTRATIVE EXAMPLE

This subsection demonstrates the implementation of the embedding algorithm. Suppose the secret message has the binary representation begins with '0101011'. The last two bits of the first five vertices in the x-component are {'11', '00', '10', '01', '00'}. The last two bits of the first five vertices in the y-component are {'00', '00', '11', '11', '00'}. Assuming that we are using the first five numbers of the Gray-code sequence, which are{0, 1, 3, 2, 6}. For the first number in the Gray-code sequence which is 0, the least valued bit of the x-component in the first vertex is altered from '1' to '0'. The second number in this sequence is 1, the least valued bit of the x-component in the second vertex in is altered from '0' to '1'. The third number in this sequence is 3 (a prim odd number), the least valued bit and the bit immediately preceding of the y-component in third vertex are altered from '11' to '10'. The fourth number in this sequence is 2 (a prim even number), the least valued bit, and the bit immediately

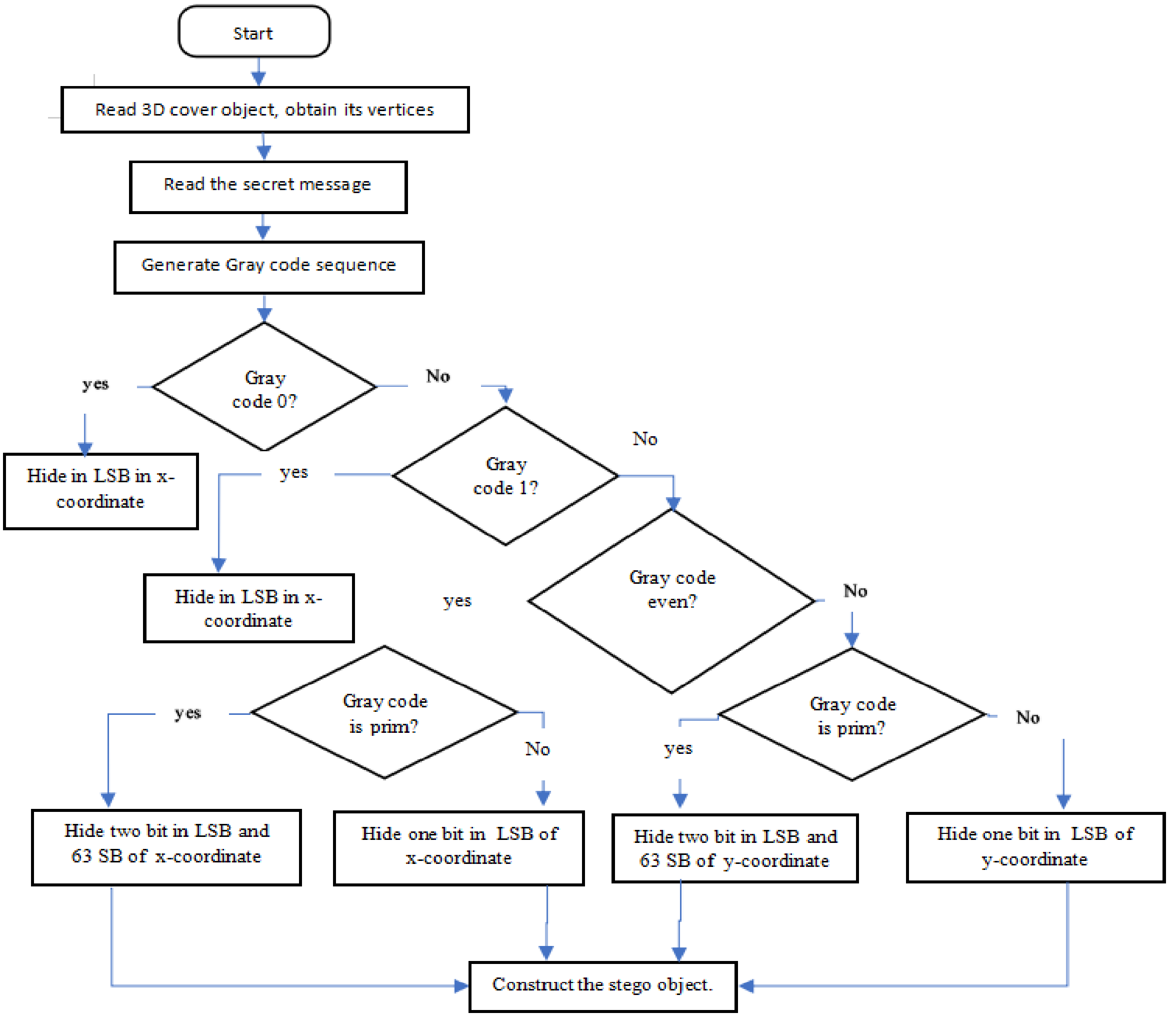

Start
Read 3D cover object, obtain its vertices
Read the secret message
Generate Gray code sequence
Gray code 0?
yes
No
Hide in LSB in x-coordinate
Gray code 1?
yes
No
Hide in LSB in x-coordinate
Gray code even?
yes
No
Gray code is prim?
yes
No
Gray code is prim?
yes
No
Hide two bit in LSB and 63 SB of x-coordinate
Hide one bit in LSB of x-coordinate
Hide two bit in LSB and 63 SB of y-coordinate
Hide one bit in LSB of y-coordinate
Construct the stego object.

FIGURE 8. Embedding algorithm chart.

preceding of the x-component in the fourth vertex are altered from ’01’ to ’10’. The fifth number in this sequence is 6 (a non-prim even number), the least valued bit of the fifth vertices in the x-component is altered from ’0’ to ’1’. Thus, the vertices of the x-component are then modified to be {’10’, ’01’, ’10’, ’10’, ’01’}.

The vertices of the y-component are then modified to be {‘00’, ‘00’, ‘10’, ‘11’}.

B. THE PROPOSED EXTRACTION PHASE

To obtain the embedded message, the vertices of the 3D stego-object are retrieved. They are converted to binary representation. The Gray-code sequence is generated using 24 bits, which are transformed into decimal numbers. If the Gray-code number is a prim even number, the least valued bit and the bit immediately preceding of x-component are extracted. If the Gray-code number is a non-prim even number, the least valued bit of the x-component is retrieved. If the Gray-code number is a prim odd number, the least valued bit and the bit immediately preceding of x-component are to be retrieved. If the Gray-code number is a non-prim odd number, the least valued bit of the y-component is retrieved. Transform the obtained stream into an 8-bit binary representation and subsequently reverse it to its original textual format.

TABLE 3. The results of embedding capacity [Bits], MSE, and PSNR for “Bunny” object.

Embedding Capacity [bits]	MSE	PSNR
10,000	1.20 x 10^{-17}	154.635
20,000	1.87 x 10^{-17}	152.717
30,000	2.50 x 10^{-17}	151.462
39,750	3.18 $\times 10^{-17}$	150.427

1) THE PROPOSED EXTRACTION ALGORITHM

To reveal the secret message, several steps are to be followed:

a) Obtain the vertices of the 3D-stego object.
b) Convert these vertices to binary representation.
c) Construct Gray-code sequence using 24 bits.
d) If the Gray-code number equals 0, retrieve the least valued bit of the x-component located at index 0.

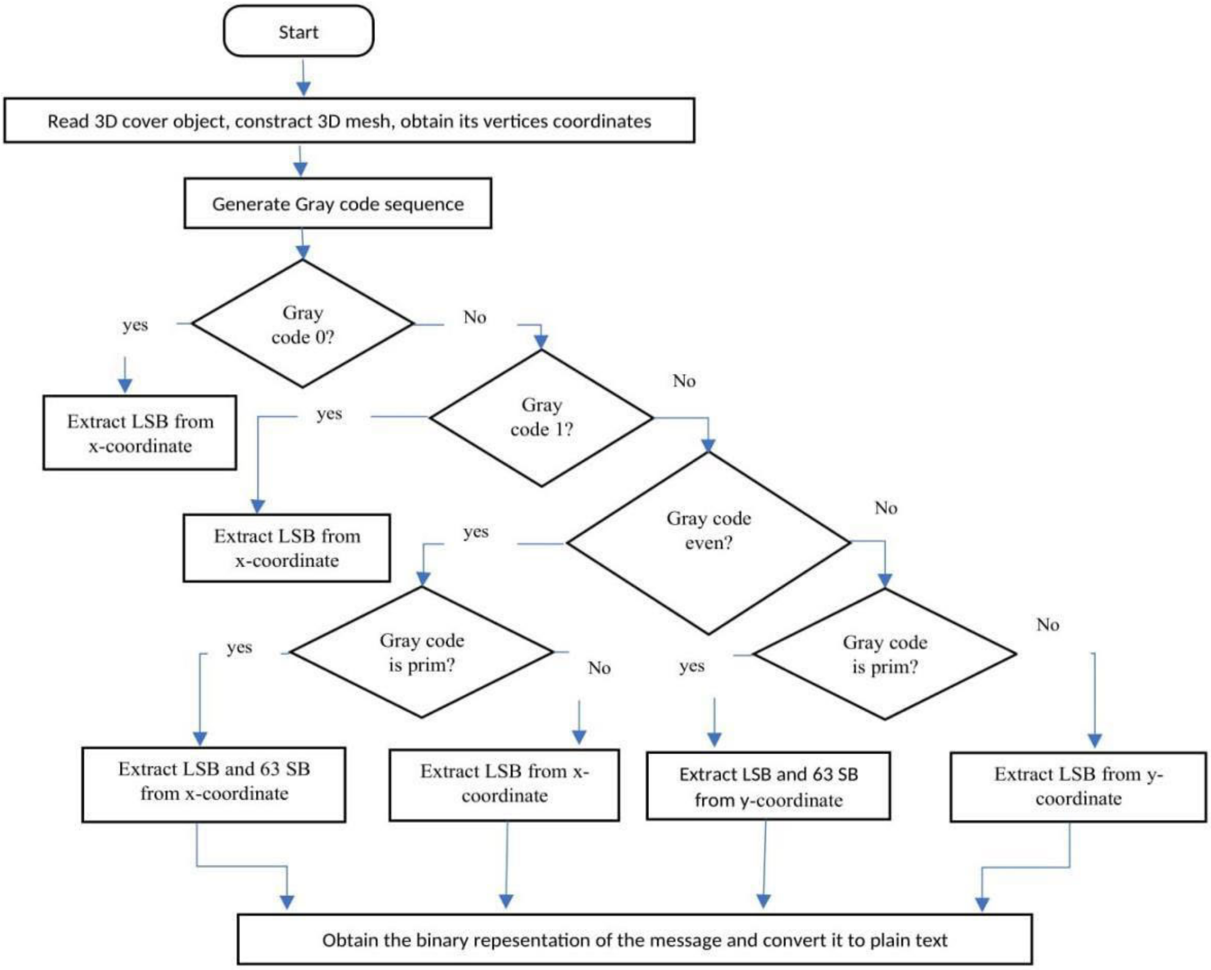

Start
Read 3D cover object, constract 3D mesh, obtain its vertices coordinates
Generate Gray code sequence
Gray code 0?
yes
No
Extract LSB from x-coordinate
Gray code 1?
yes
No
Extract LSB from x-coordinate
Gray code even?
yes
No
Gray code is prim?
yes
No
Gray code is prim?
yes
No
Extract LSB and 63 SB from x-coordinate
Extract LSB from x-coordinate
Extract LSB and 63 SB from y-coordinate
Extract LSB from y-coordinate
Obtain the binary repesentation of the message and convert it to plain text

FIGURE 9. Extraction algorithm chart.

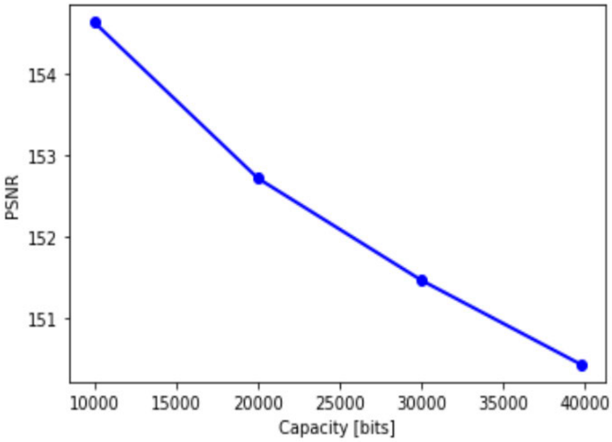


FIGURE 10. PSNR as opposed to capacity, evaluated for the Bunny object.

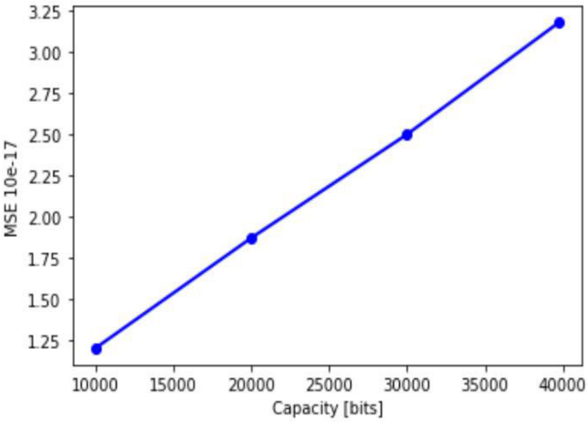


FIGURE 11. MSE as opposed to capacity, evaluated for the Bunny object.

e) If the Gray-code number equals 1, retrieve the least valued bit of the x-component located at index 1.

f) If Gray-code number equals more than 1; if it is a prim even number: retrieve the least valued bit and the bit immediately preceding of x-component.

g) If the Gray-code number is a non-prim even number: retrieve the least valued bit of the x-component.

h) If the Gray-code number is a prim odd number: retrieve the least valued bit and the bit immediately preceding of y-component.

TABLE 4. Cover-objects, stego-object and their histogram.

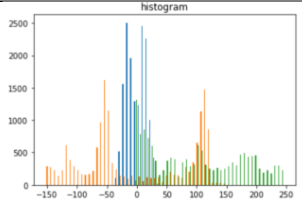
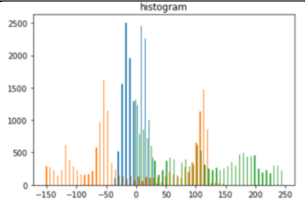
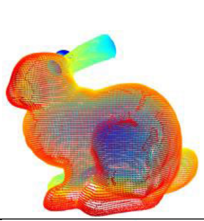
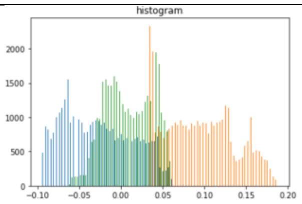
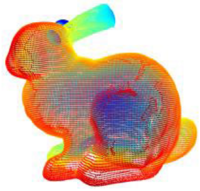
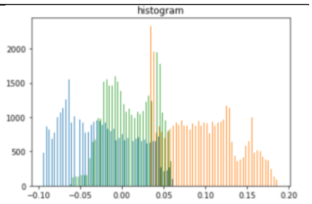
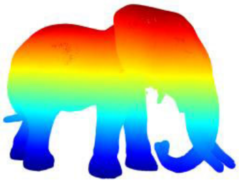
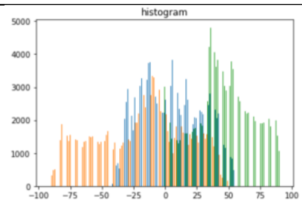
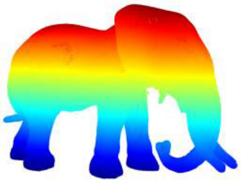
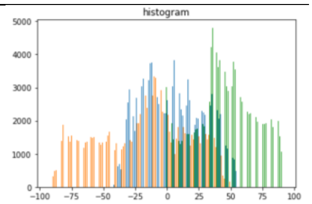
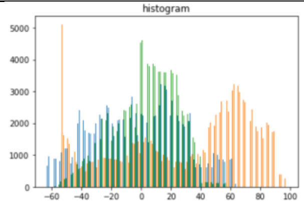
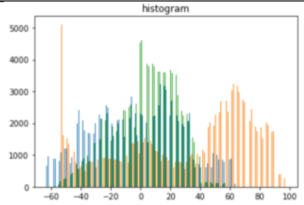
Object Name	Cover-Object	Histogram of Cover-Object	Stego-Object	Histogram of Stego-Object
Horse				
Bunny				
Elephant				
Armadillo				

TABLE 5. Evaluation of the optimum capacity, MSE, PSNR, and NC across several objects.

Object	Maximum capacity [bits]	MSE	PSNR	NC
Horse	17,118	4.405×10^{-30}	341.367	1.0
Bunny	39,750	3.18×10^{-17}	150.4274	0.9999999999999969
Elephant	184,184	1.934×10^{-30}	336.387	0.9999999999999931
Armadillo	188,639	2.956×10^{-30}	335.035	1.0

i) If the Gray-code number is a non-prim odd number: retrieve the least valued bit of the y-component.

j) Transform the retrieved stream into an 8-bit binary representation and then to its original textual format.

The extraction algorithm's procedural steps are depicted in the chart displayed in Figure 9.

TABLE 6. Normalized correlation values against various attacks.

Attacks		Horse	Bunny
Median filtering		0.86039	0.50200
Gaussian filtering		0.78575	0.66657
Laplacian filtering		-0.85098	-0.92424
Noise	Gaussian	0.99979	0.99980
	Speckle	0.68064	0.67976

2) EXTRACTION PHASE ILLUSTRATIVE EXAMPLE

This subsection demonstrates the same hidden message shown in the embedding phase illustrative example. At the receiver side, the Gray-code sequence numbers are generated. The first five numbers of this sequence are {0, 1, 3, 2, 6}. Looking at the first two number in this sequence which are 0 and 1, the least valued bit of the x-component in the first and the second vertex are extracted {'0', '1'}. The third number of this sequence is 3 (a prim odd number), the least valued bit and the bit immediately preceding of the y-component in third vertex are extracted {'0', '1'}. The fourth number in this sequence is 2 (a prim even number), the least valued bit and the bit immediately preceding of the x-component in the fourth vertex are retrieved {'0', '1'}. The fifth number in this sequence is 6 (a non-prim even number), the least valued

TABLE 7. A comparison between various techniques within domain of 3D geometrical steganography.

Year	Authors	Algorithm
2013	P. Thiyagarajan [20]	Hiding after mesh re-triangulation
2017	K. Anish [23]	Hiding within the x-coordinate of vertices
2017	Z. Li [21]	Hiding in vertices of a 3D mesh utilizing a Hamiltonian path
2019	S. Farrag [15]	Hiding in polygons
2019	A. Girdhar [26]	Hiding utilizing difference shifting
2019	S. Elsherif [24]	Embedding in 4th and 5th decimal places after the decimal point of the vertices of polygons
2022	G. Mostafa [14]	Hiding in the coordinates utilizing Gray-code sequence
2023	The Proposed Technique	Concealing in a binary representation of the x-, and y-components using Gray-code sequence

TABLE 8. A comparison between the existing techniques in the geometrical domain.

Authors	Encryption	Embedding location	Blind
P. Thiyagarajan [20]	No	Vertices	Yes
K. Anish [23]	No	Vertices	Yes
A. Girdhar [26]	No	Vertices	Yes
S. Farrag [22]	Yes	Polygon	Yes
S. Farrag [15]	No	Vertices	Yes
G. Mostafa [14]	Yes	Vertices	Yes
Proposed Technique	No	Vertices	Yes

TABLE 9. Assessment of performance for certain technique.

Authors	Object	Maximum Capacity [bits]	PSNR	MSE
P. Thiyagarajan [20]	Bunny	64,496	55.3442	0.18930
S. Elsherif [24]	Patient's head	1,792	53.1714	0.31329
W. Alexan [19]	CTEngine	295,680	62.66	0.03519
S. Farrag [22]	Bunny	1,249,800	—	0.355×10^{-6}
G. Mostafa [14]	Armadillo	4,151,37	239.34	6.0968×10^{-8}
Proposed Technique	Armadillo	188,639	335.035	2.956×10^{-30}

bit of the x-component in the fifth vertices is extracted {1}. Consequently, the revealed message is '0101011'.

V. PERFORMANCE EVALUATION METRICS AND COMPARATIVE NUMERICAL ANALYSIS

To assess the feasibility of our technique, several 3D objects with various sizes have been selected in the experiments. Table 2, indicates four of the famous experimental 3D objects and their number of vertices. Our technique is implemented utilizing Python on a machine running a 64–bit operating system that has Intel® Core(TM) i5-1135G7 2.40GHz CPU and 8.00 GB of RAM.

To assess the performance of our steganographic technique; Mean Square Error (MSE), Peak Signal-to-Noise Ratio (PSNR), Histogram, and Normalized Correlation (NC). PSNR is defined as $20 \log_{10}(\frac{D_{max}}{MSE})$ (where D_{max} is the diagonal distance of the smallest oriented cuboid bounding box of the 3D object).

Now, to gauge the security level of our technique, we computed the MSE, and the PSNR with different embedding capacities [bits] for the 3D object "bunny". The obtained results are shown in Table 3 and explained in Figure 10 and Figure 11. The results indicate that our technique achieved high PSNR and low MSE, despite the higher capacity.

Figure 10 depicts the relation between PSNR and the capacity (in bits). Figure 11 depicts the relation between MSE and the capacity (in bits). More difference in values of vertex components and a higher value of MSE is a result of greater embedding capacity. The PSNR and the MSE inversely proportional, signifying that as the MSE enhances, the PSNR reduces. Consequently, when the embedding capacity rises and MSE increases, PSNR decrease.

Experimenting, the proposed technique with several 3D objects, Table 4, shows the cover-object, the stego-object, and the histogram of both the cover- and stego-objects, for the 3D objects (horse, bunny, elephant, and Armadillo). The HVS is unable to observe any substantial differences between the cover- and the stego-objects, as well as between their respective histogram plots.

Table 5 displays the numerical data for the optimum capacity, MSE, PSNR, and NC across several objects which indicates a higher security level. From the numerical results, our technique has a minimum MSE which is 1.934×10^{-30}. That implies that there is limited dissimilarity between the cover and the stego objects. Our technique achieves the highest PSNR of 336.387. The value of NC for all 3D objects is also near to 1.0 that indicates the higher quality of the proposed technique.

Tables 6 shows the results of NC values against various attacks, including median filtering, Gaussian filtering, Laplacian filtering, Gaussian noise, and Spackle noise. It also shows the results of NC values against various filters attacks (such as the median, and the Gaussian) and noise attacks (such as Gaussian, and Spackle) is almost equal 1. These results indicate the efficiency and the robustness of the proposed technique.

Comparing the proposed technique to several geometrical domain techniques; Table 7 shows the different algorithms used in [21, 24, 22, 15, 27, 25, and 14]. While in Table 8, we demonstrate the difference between those techniques in terms of embedding location, encryption, and the type of extraction process (blind). To increase the security level, techniques [14] and [22] employ a encryption and steganography. As for the blind extraction, In all the techniques, the extraction process is carried out without access to the cover-object.

Table 9 provides a comparison of the proposed technique utilizing many 3D-cover objects. the comparison showed significant difference between the proposed technique and the other techniques; That is, the proposed technique has a higher PSNR and a lower MSE. PSNR for the 3D object (Armadillo) is 335.035 dB that indicates a significant similarity between both the cover- and the stego-object. MSE of the proposed technique using the same 3D object is found 2.956 $\times 10^{-30}$ introduces negligible distortion that is imperceptible to the HVS.

VI. CONCLUSION AND FUTURE WORK

The proposed steganographic technique utilizes a Gray-code sequence to scramble the arrangement of the vertices of the 3D object used for concealing the information. The embedding and the extraction algorithms are determined based on if the Gray-code number. This technique is implemented while preserving a high level of security, without causing any effects on the 3D object quality. Various performance metrics were utilized for evaluating the technique, such as: MSE, PSNR, and NC. According to the PSNR results, we can claim the superior of the proposed technique in data security, comparing to several existing techniques, which had been reviewed in this paper; that the results shown in Table 9 indicated a significant similarity between the cover and the stego-object. Further more, when testing against the noise, the median, and the Gaussian, the obtained NC values, showed the efficiency and robustness of the proposed technique. For future work, our plan is to process the embedding step in some topological and representation domains to enhance the embedding capacity. Moreover, we will test using other sequences rather than the Gray-code sequence; for the purpose of reducing the embedding and extraction time. Then, to test the proposed technique against more different types of attacks and noise.

REFERENCES

[1] Z. Li, X. Kong, J. Zhang, L. Shao, D. Zhang, J. Liu, X. Wang, W. Zhu, and C. Qiu, "Cryptography metasurface for one-time-pad encryption and massive data storage," *Laser Photon. Rev.*, vol. 16, no. 8, Aug. 2022, Art. no. 2200113, doi: 10.1002/lpor.202200113.

[2] F. Zhang, Y. Guo, M. Pu, L. Chen, M. Xu, M. Liao, L. Li, X. Li, X. Ma, and X. Luo, "Meta-optics empowered vector visual cryptography for high security and rapid decryption," *Nature Commun.*, vol. 14, no. 1, pp. 1–9, Apr. 2023, doi: 10.1038/s41467-023-37510-z.

[3] D. Li, J. Li, U. A. Bhatti, S. A. Nawaz, J. Liu, Y.-W. Chen, and L. Cao, "Hybrid encrypted watermarking algorithm for medical images based on DCT and improved DarkNet53," *Electronics*, vol. 12, no. 7, p. 1554, Mar. 2023, doi: 10.3390/electronics12071554.

[4] T. Harte and A. G. Bors, "Watermarking 3D models," in *Proc. Int. Conf. Image Process.*, Rochester, NY, USA, vol. 3, 2002, pp. 661–664, doi: 10.1109/icip.2002.1039057.

[5] Z. Li, "Steganalytic methods for 3D objects," Ph.D. thesis, Dept. Comput. Sci., Univ. York, Heslington, U.K., 2018.

[6] A. Y. AlKhamese, W. R. Shabana, and I. M. Hanafy, "Data security in cloud computing using steganography: A review," in *Proc. Int. Conf. Innov. Trends Comput. Eng. (ITCE)*, Feb. 2019, pp. 549–558, doi: 10.1109/ITCE.2019.8646434.

[7] H. Ge, M. Huang, and Q. Wang, "Steganography and steganalysis based on digital image," in *Proc. 4th Int. Congr. Image Signal Process.*, vol. 1, Oct. 2011, pp. 252–255, doi: 10.1109/CISP.2011.6099953.

[8] I. J. Kadhim, P. Premaratne, P. J. Vial, and B. Halloran, "Comprehensive survey of image steganography: Techniques, evaluations, and trends in future research," *Neurocomputing*, vol. 335, pp. 299–326, Mar. 2019.

[9] D. Bucerzan and C. Rațiu, "Testing methods for the efficiency of modern steganography solutions for mobile platforms," in *Proc. 6th Int. Conf. Comput. Commun. Control*, 2016, pp. 30–36.

[10] C. Whitelam, N. Osia, and T. Bourlai, "Securing multimodal biometric data through watermarking and steganography," in *Proc. IEEE Int. Conf. Technol. Homeland Secur.*, Nov. 2013, pp. 61–66.

[11] N. Lofgren, S. K. Decker, H. L. Brunk, and J. S. Carr, "Digitally watermarking holograms for use with smart cards," U.S. Patent 6 608 911, Aug. 19, 2003.

[12] R. Tanwar, U. Pilania, M. Zamani, and A. A. Manaf, "An analysis of 3D steganography techniques," *Electronics*, vol. 10, no. 19, p. 2357, Sep. 2021.

[13] S. Farrag, W. Alexan, and M. Mashaly, "High capacity 2D and 3D reliable image steganography schemes," M.S. thesis, Dept. Commun., Faculty Inf. Eng. Technol., German Univ., Cairo, Egypt, 2019.

[14] G. Mostafa and W. Alexan, "A robust high capacity gray code-based double layer security scheme for secure data embedding in 3D objects," *ITU J. Future Evolving Technol.*, vol. 3, no. 2, pp. 310–325, 2022, doi: 10.52953/ufka9833.

[15] S. Farrag and W. Alexan, "Secure 3D data hiding technique based on a mesh traversal algorithm," *Multimedia Tools Appl.*, vol. 79, nos. 39–40, pp. 29289–29303, Oct. 2020.

[16] D. Giarimpampa, "Blind image steganalytic optimization by using machine learning," M.S. thesis, Dept. Intell. Syst. Digit. Des., School Inf. Technol., Halmstad Univ., Halmstad, Sweden, 2018.

[17] C.-C. Chen and C.-C. Chang, "LSB-based steganography using reflected gray code," *IEICE Trans. Inf. Syst.*, vol. E91-D, no. 4, pp. 1110–1116, Apr. 2008, doi: 10.1093/ietisy/e91-d.4.1110.

[18] S. Dagar, V. Kumar, and Y. Bagoriya, "Image steganography using secret key & gray codes," *Int. J. Innov. Technol. Exploring Eng.*, vol. 2, no. 5, pp. 241–245, 2013.

[19] W. Alexan, M. El Beheiry, and O. Gamal-Eldin, "A comparative study among different mathematical sequences in 3D image steganography," *Int. J. Comput. Digit. Syst.*, vol. 9, no. 4, pp. 545–552, Jul. 2020.

[20] P. Thiyagarajan, V. Natarajan, G. Aghila, V. P. Venkatesan, and R. Anitha, "Pattern based 3D image steganography," *3D Res.*, vol. 4, no. 1, pp. 1–8, Mar. 2013.

[21] Z. Li, S. Beugnon, W. Puech, and A. G. Bors, "Rethinking the high capacity 3D steganography: Increasing its resistance to steganalysis," in *Proc. IEEE Int. Conf. Image Process. (ICIP)*, Sep. 2017, pp. 510–414.

[22] S. Farrag and W. Alexan, "A high capacity geometrical domain based 3D image steganography scheme," in *Proc. Int. Conf. Adv. Commun. Technol. Netw. (CommNet)*, Apr. 2019, pp. 1–7.

[23] K. Anish, N. Arpita, H. Nikhil, K. Sumant, S. Bhagya, and S. D. Desai, "Intelligence system security based on 3-D image," in *Proc. 5th Int. Conf. Frontiers Intell. Comput., Theory Appl.* Singapore: Springer, 2017, pp. 159–167.

[24] S. Elsherif, G. Mostafa, S. Farrag, and W. Alexan, "Secure message embedding in 3D images," in *Proc. Int. Conf. Innov. Trends Comput. Eng. (ITCE)*, Feb. 2019, pp. 117–123, doi: 10.1109/ITCE.2019.8646685.

[25] H. Zhou, K. Chen, W. Zhang, Y. Yao, and N. Yu, "Distortion design for secure adaptive 3-D mesh steganography," *IEEE Trans. Multimedia*, vol. 21, no. 6, pp. 1384–1398, Jun. 2019, doi: 10.1109/TMM.2018.2882088.

[26] A. Girdhar and V. Kumar, "A reversible and affine invariant 3D data hiding technique based on difference shifting and logistic map," *J. Ambient Intell. Humanized Comput.*, vol. 10, no. 12, pp. 4947–4961, Dec. 2019.

AYA Y. ALKHAMESE received the bachelor's and master's degrees in computer science from Port Said University, Port Said, Egypt, in 2013 and 2019, respectively. She is currently an Assistant Lecturer with the Faculty of Engineering, Port Said University. Her research interests include information security, cryptography and steganography, and image procession.

HEWAYDA A. ELGAWALBY received the Ph.D. degree in computer science from York University, in 2011. She is currently a Lecturer with the Faculty of Engineering, Port Said University, Port Said, Egypt. Her research interests include image processing, topology, and information security.

IBRAHIM M. HANAFY is currently a Professor with the Department of Mathematics, Faculty of Science, Port Said University, Port Said, Egypt.

WAEL A. AWAD is currently with the Department of Computer Science, Faculty of Computers and Artificial Intelligence, Damietta University, Damietta, Egypt.

AHMED ISMAIL EBADA is currently a Researcher, the Technical Project Manager, and the CTO/Co-Founder in Munich, Germany. He has been working in the industrial research area. His research interests include the IoT, edge, wearables, biosensors, AI, speech recognition, cloud computing, big data analysis, robotics, and entrepreneurship. He has served as an Associate Editor and a Peer-Reviewer for IEEE, Elsevier, and *Nature* (Springer). His motto is, science is a way to improve people's lives, neither a tool for philosophy nor fame.

S. S. ASKAR received the B.Sc. degree in mathematics and the M.Sc. degree in applied mathematics from Mansoura University, Egypt, in 1998 and 2004, respectively, and the Ph.D. degree in operation research from Cranfield University, U.K., in 2011. He has been an Associate Professor with Mansoura University, since 2016. He has joined King Saud University, in 2012, where he is currently with the Department of Statistics and Operation Research as a Professor. His research interests include game theory and its applications that include mathematical economy, dynamical systems, and network analysis.

MOHAMED ABOUHAWWASH received the B.Sc. and M.Sc. degrees in statistics and computer science from Mansoura University, Mansoura, Egypt, in 2005 and 2011, respectively, and the joint Ph.D. degree in statistics and computer science from Michigan State University, East Lansing, MI, USA, and Mansoura University, Egypt, in 2015.

Currently, he holds significant academic positions at Distinguished Institutions, including Computational Mathematics, Science, and Engineering (CMSE), Biomedical Engineering (BME), and Radiology, Institute for Quantitative Health Science and Engineering (IQ) at Michigan State University, East Lansing, MI, USA. Additionally, he serves as an Associate Professor at the Department of Mathematics, Faculty of Science, Mansoura University, Egypt. He dedicated to advancing knowledge transcends geographical boundaries, as evidenced by his role as a Visiting Scholar at the Department of Mathematics and Statistics, Faculty of Science, Thompson Rivers University, Kamloops, BC, Canada, during 2018. He is a Distinguished Researcher and Academician, widely recognized for his outstanding contributions to the fields of computational intelligence, machine learning, and image reconstruction. With an illustrious career, he has published over 160 papers in esteemed journals, including notable publications like IEEE Transactions on Evolutionary Computation, IEEE Transactions on Medical Imaging, IEEE Transactions on Emerging Topics in Computational Intelligence, Artificial Intelligence Review, Expert Systems with Applications, Swarm and Evolutionary Computation, Knowledge-Based Systems, and Applied Soft Computing. In addition to his prolific research output, he has showcased his expertise by authoring several edited books published by reputable academic publishers such as Springer, Wiley, Taylor, and Francis. His impact on the academic community is further amplified through his editorial board service in numerous prestigious journals and conferences. Throughout his illustrious career, he has received recognition for his academic excellence, notably being honored with the best master's and Ph.D. Thesis Awards from Mansoura University in 2012 and 2018, respectively.