

STEGANOGRAPHY METHOD BASED ON MESH REPRESENTATION AND CONTEXT OF TEXTURE

Mohammed Majid Jabbar¹, Tawfiq A. Abbas²

¹ Software Department, College of Information Technology, University of Babylon, Hilla,
Iraq

² Software Department, College of Information Technology, University of Babylon, Hilla,
Iraq

¹ mohammedmajidj.sw@student.uobabylon.edu.iq

² Tawfiqasadi@itnet.uobabylon.edu.iq

Abstract

This paper presents image steganography technique that utilizes depth-based geometric analysis to enhance the accuracy and security of data embedding. The proposed system used a pre-trained MiDaS convolutional neural network to generate a depth map from the cover image, then Shi-Tomasi corner detection to detecting the key points. Delaunay triangulation is then applied to generate a mesh of triangles. In order to compute the correlation degree for each triangle, Spearman's correlation coefficient is used. After computing the correlation degree, the number of secret messages is embedded. One bit to three bits of secret message is embedded. According to experimental results, the proposed method achieved high PSNR, which mean that the proposed method has ability to preserve visual quality and extract the embedded message accurately.

Keywords: Image Steganography; Mesh Geometry; MiDaS Model; Shi-Tomasi Algorithm

1. Introduction

Due to the widespread use of multimedia data and technological improvements in the areas of image, audio, and video transmission, secret communication between a sender and a receiver has taken place on a significant amount of significance in order that the third parties (attackers) cannot access critical or confidential information [1]. So, in the modern world, security issues related to information transit have grown to be a major concern. As long as this information is kept safe, individuals will be satisfied [2]. To prevent unanticipated outcomes, information security is essential for any firm [3]. Therefore, it is suggested that information hiding be used that hide the information in a cover file [2] [3]. Steganography and watermarking are two widely used techniques for information hiding [4]. They both directly alter the media file's content (such as images, videos, and music), providing copyright protection and covert communication or sender identification [5]. Steganography is a process for hiding secret information by enclosing it in a regular, non-secret file or communication; the information is subsequently extracted at the designated place [6]. Many works have been done in image steganography because images are one of the crucial carriers utilized in multimedia

communication [7]. Image Steganography is the technique of hiding the existence of the communicated information within images [6].

2. Related Work

Zhang et al. (2019) proposed SteganoGAN model for image steganography. The model achieved high imperceptibility (PSNR ~42 dB) and a payload capacity (up to 4.4 bpp). Also, the model generates stego images resistant to detection even by modern steganalysis methods. With more than tested architectures, the Dense variant outperformed others, offering good trade-off between embedding capacity and imperceptibility. In general, this model is highly relevant as it demonstrates how deep learning has more performance than traditional steganography methods in achieving secure and high-capacity image embedding for covert communication. [8].

Duan et al. (2020) a SteganoCNN model for image steganography based on CNN. This model embeds two secret images into one cover image. Experimental results show that the model achieves 47.92 bit per pixel. Also, the model has the ability to produce stego-images with high quality. In addition, the method addresses the challenge of balancing high payload capacity with maintaining stego-image quality and security [9].

Tang et al. (2021) proposes MDC-GCNs framework for 3D mesh segmentation and classification. MDC-GCNs represent each face as a graph node and extract rich geometric features from a 1-ring face neighbourhood. This framework improves both local and non-local feature learning. The MDC-GCNs achieve high performance with fewer parameters and without relying on data augmentation. Experimental results show that MDC-GCNs supports deep architectures while maintaining high accuracy and efficiency. [10]

Dong et al. (2023) proposed convolutional neural network (CNN) model leveraging the Laplacian-Beltrami spectral domain to show the challenges in understanding irregular triangle meshes for tasks such as shape classification and semantic segmentation. The proposed method converts polygonal surfaces into a spectral domain. Also, it enables traditional CNNs to process irregular meshes by decoupling geometry from connectivity. Key features include a channel-wise self-attention mechanism, Laplacian pooling/unpooling for multi-resolution feature fusion, and integration of intrinsic and extrinsic geometric features. There are several advantages of the proposed such as its robustness against noise, tolerance to mesh defects. However, there are several limitations such as reducing performance in datasets emphasizing high-frequency details and computational demands due to eigen decomposition [11]

Liu et al. (2024) proposed framework augmented with Transformer blocks, designed to embed multiple images based on StegFormer model. This model achieves high payload capacity of up to 96 bpp. The model illustrates important several advantages, such as high embedding capacity and high imperceptibility. Also, the model improves the PSNR with 3–5 dB compared to previous methods such as HiNet and DeepMIH. However, the approach has some limitations such as the requirement for extensive training and computational resources, and a potential reduction in interpretability relative to conventional steganography techniques. [12]

Huo et al. (2024) proposed CHASE, a deep learning-based image steganography method that combines chaotic mapping and invertible neural networks (INNs) to achieve high capacity and strong security. The study categorizes existing methods into traditional approaches (e.g., LSB, DCT) and deep learning-based ones. Modern techniques focus on enhanced cover image generation, steganographic distortion optimization, and encoder-decoder-based hiding. GAN-based models like HayesGAN and SteganoGAN improve imperceptibility but suffer from irreversibility and color distortion. INNs such as NICE, RealNVP, and Glow offer reversible encoding, with applications extended to steganography through models like ISN, HiNet, and DeepMIH. CHASE builds upon these by integrating chaotic scrambling and GAN training to improve both secrecy and image fidelity [13].

3. Preliminaries

3.1. Delaunay Triangulation

This algorithm is utilized for partitioning a plane set of points into triangles such that no point is contained in the circumcircle of a triangle. It is utilized extensively in a variety of applications including computer graphics and mesh generation [14]. Let us explain the steps of algorithm.

1. Select set of points
2. Select triangle that encompasses all the points
3. Draw circle around the selected triangle
4. If there no fourth point, then selected triangle is correct
5. Else select another point to be triangle.

3.2. Shi-Tomasi algorithm

Shi-Tomasi algorithm [15] used for corner detection. It is using in computer vision for identifying corners or interest points in an image. The mathematical operations of the algorithm can be listed as follows:

For a given point in the image, the algorithm computes the covariance matrix of image gradients in a small window:

$$M = \begin{bmatrix} I_x^2 & I_x I_y \\ I_x I_y & I_y^2 \end{bmatrix} \quad (1)$$

Where I_x and I_y are gradients in the x and y directions, respectively. The eigenvalues (λ_1, λ_2) of M represent the changes in color intensity in two orthogonal directions.

The corner selection criterion can be as follows:

A point will be "corner" if both eigenvalues are large. Shi-Tomasi modifies this by selecting points.

where:

$$R = \min(\lambda_1, \lambda_2) > \text{threshold} \quad (2)$$

This ensures corners are identified based on the smaller eigenvalue, avoiding issues where one eigenvalue might dominate.

3.3. Spearman's Correlation Coefficient(ρ)

Spearman's correlation coefficient (ρ) is a non-parametric measure of rank correlation. In the other word, it explains how well the relationship between two variables can be described by a monotonic function [16]. The form of Spearman's correlation coefficient equation is written as follows:

$$\rho = 1 - \frac{6 \sum d_i^2}{n(n^2-1)} \quad (3)$$

Where:

d_i = Difference between ranks of corresponding X and Y values.

n = Number of observations.

3.4. MiDaS model

MiDaS is a pre-trained CNN model for monocular depth estimation, which predicts depth information from a single RGB image. It is trained on a mixture of datasets to ensure robust generalization and outputs a relative depth map useful in 3D scene understanding, augmented reality, and robotics. This model is used in the proposed method. For more details read the reference [17].

4. Proposed System

Figure 1 illustrates the general block diagram of the proposed system. The proposed system consists of several parts as follows:

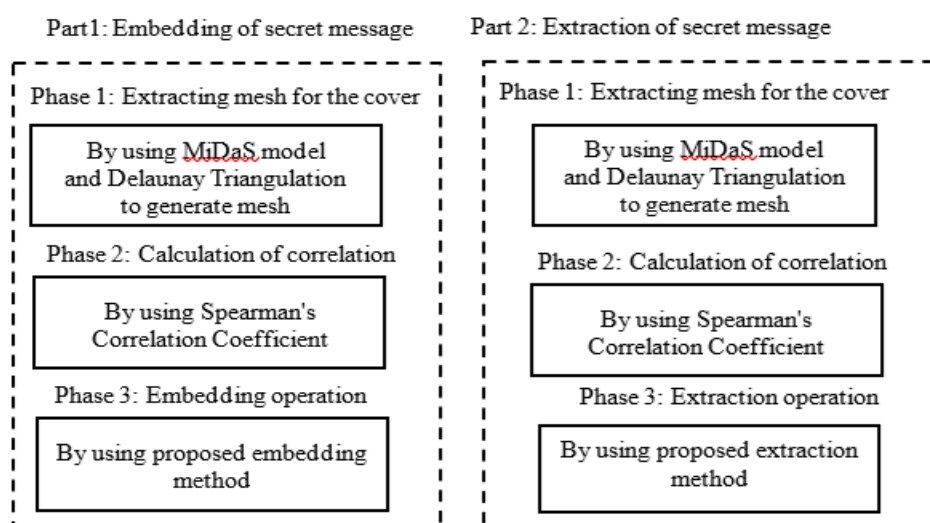


Figure 1. General block diagram of the proposed system

Part 1: Embedding the secret message: This part related to sender side. In which the secret message is embedded into selected cover. Figure 2 illustrates the embedding operation. Also, this part consist of several phases as follows:

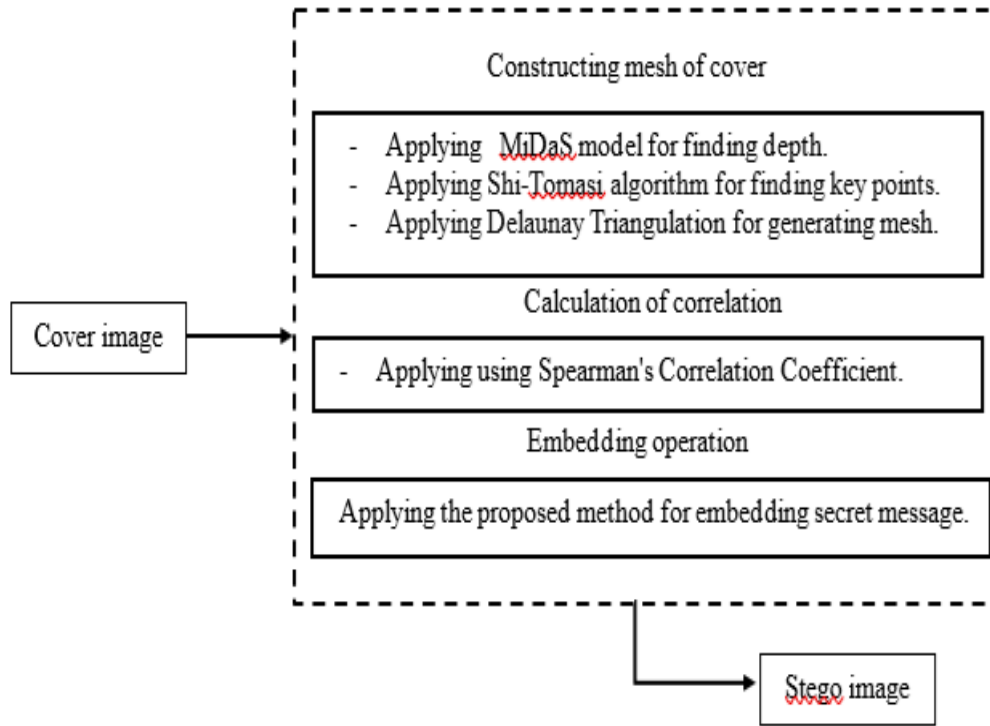


Figure 2. Embedding operation

Phase 1: Extracting mesh for the cover image: In this phase, the mesh is extracted for the cover image. The mesh is used later as position for embedding the secret message. This phase consists of several steps which can be listed as follows:

1. Extraction of cover image depth: In this step, the MiDaS model is used extracting the depth of cover image. The depth map is used to understand the spatial relationships and relative dimensions of objects in the image.
2. Generation of key points: Based on the extracted image depth, the key points are generated based on the structure of image using Shi-Tomasi algorithm.
3. Generating of triangle mesh: Based on Depth which generated in step 1, the generated point is merged based on the proposed Merging Points (MP) algorithm. The MP is used decrease the number of points in image. In the other word, the points are filtered.
 - Reducing the outlier points.
 - Increase the accuracy of drawing the mesh of triangles when using Delaunay Triangulation Algorithm.
 - Representing the resulting image structure in more accurate.
 - Reducing the consuming time to perform computation.

Algorithm 1 explains Merging points method:

Algorithm 1: Merging Points Based on Depth Values
Input:

points: A set of 2D points (e.g., [(x1, y1), (x2, y2), ...])

depth_values: A set of depth values (e.g., [d1, d2, ...])

threshold: A allowable depth difference

Output:

filtered_points: A list of 2D points that meet the merging criteria

begin
Step 1: Check Input Validity:

- Ensure that the number of points matches the number of depth values.
- If they are unequal, report an error and stop the algorithm.

Step 2: Initialize the filtered points list:

- Set *filtered_points* = [*points* [0]] (Start with the first point).

Step 3: Iterate through the remaining points:

- For each index *i* from 1 to len(*points*) - 1:
 - **Step 3.1: Calculate the depth difference:**
 $depth_difference = depth_values[i] - depth_values[i-1]$
 - **Step 3.2: Compare the depth difference with the threshold:**
 - If $depth_difference \leq threshold$:
 Add *points*[*i*] to *filtered_points*.
 - Else:
 Exclude *points*[*i*] from *filtered_points*.

Step 4: Return the final filtered_points list.
End

4. Mesh creation: In this step the mesh is created using Delaunay Triangulation based on steps 3 and 4. The result of this step is irregular mesh of triangles covering the regions represented by the points.

5. Localize each triangle: In this step each triangle is localized.

6. Collect pixels: In this step, all pixels inside the position triangle are collected except for the pixels that represent the vertices of the triangle and that are located on the edges of the triangle.

Phase 2: Calculation of correlation: In this phase, the correlation between pixels is calculated. The correlation is calculated using Spearman's correlation coefficient according equation 1.

Phase 3: Embedding operation: In this phase, the secret message is embedded in the cover image. The priority of selecting triangle for embedding operation depends on the number of pixels inside the triangle and the value of calculated correlation between pixels. The embedding operation can be listed in the several steps:

1. Choosing the suitable cover by compare the capacity of cover and size of the secret message. In the other word the size of secret message must be less than or equal the size of cover.

2. Depending on the correlation value, the embedding operation can be done as follows:

- If the correlation value between pixels within triangle is high, one bit from secret message will be embedded in the cover image.
- If the correlation value between pixels within triangle is medium, two bits from secret message will be embedded in the cover image.
- If the correlation value between pixels within triangle is low, three bits from secret message will be embedded in the cover image.

3. Embedding the coordinate of the vertex of triangle in the border of cover image.

4. Getting the stego image.

Part 2: Extraction the secret message: This part related to receiver side. In which the secret message is extracted from cover. Figure 3 illustrates the extracting operation. Also, this part consist of several phases as follows:

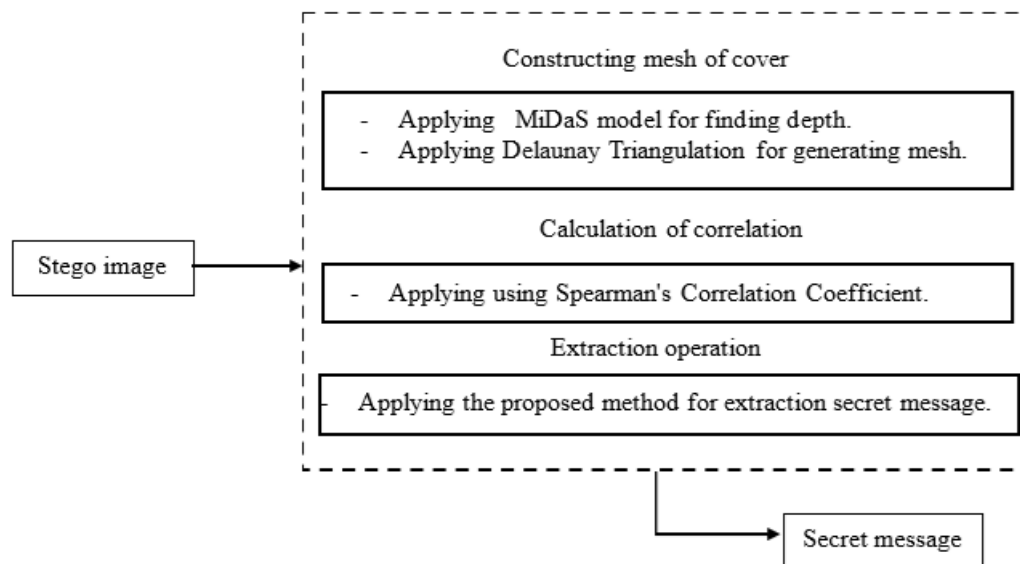


Figure 3. Extraction operation

Phase 1: Extracting mesh for the stego image: In this phase, the mesh is extracted for the stego image. The mesh is used later as position for extracting the secret message. This phase consists of several steps which can be listed as follows:

1. Extraction of stego image depth: In this step, the MiDaS model is used extracting the depth of stego image. The depth map is used to understand the spatial relationships and relative dimensions of objects in the stego image.
2. Extracting the coordinate vertex: In this step, the coordinate vertex is extracted from the border of stego image. The extracted coordinate vertex will used later for extracted the secret message.
3. Generating of triangle mesh: the triangle is generated depending on coordinate vertex and extracted depth (in step 1).
4. Mesh creation: In this step the mesh is created using Delaunay Triangulation based on steps 2 and 3. The result of this step is irregular mesh of triangles covering the regions represented by the points.
5. Localize each triangle: In this step each triangle is localized.
6. Collect pixels: In this step, all pixels inside the position triangle are collected except for the pixels that represent the vertices of the triangle and that are located on the edges of the triangle.

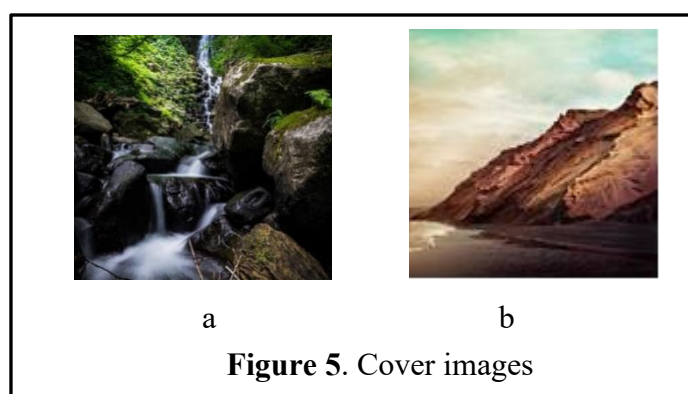
Phase 2: Calculation of correlation: In this phase, the correlation between pixels is calculated. The correlation is calculated using Spearman's correlation coefficient according equation 3.

Phase 3: Extracting operation: In this phase, the secret message is extracted from the stego image. The priority of selecting triangle for extracting operation depends on the number of pixels inside the triangle and the value of calculated correlation between pixels. The extracting operation can be listed in two steps:

1. Depending on the correlation value, the extracting operation can be done as follows:
 - If the correlation value between pixels within triangle is high, one bit from secret message will be extracted from the stego image.
 - If the correlation value between pixels within triangle is medium, two bits from secret message will be extracted from the stego image.
 - If the correlation value between pixels within triangle is low, three bits from secret message will be extracted from the stego image.
2. Getting the secret message.

5. Experimental Result

This section explains the experimental result after implementing the proposed system. Figure 4 shows sample of secret message. The secret message is gray image of 75*75 pixels. Figure 5 shows sample of cover image in which the secret message will be embedded. The cover image is RGB image of 300*300 pixels.



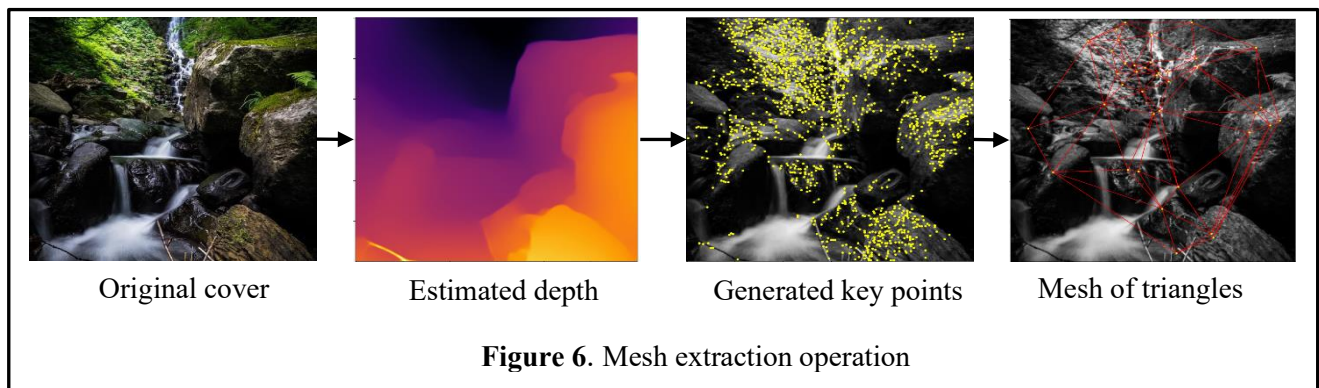
Let us explain the proposed method with an example and several stages:

Part one: This part is done in the sender side. In which the secret message is embedded in the cover. Also, part one can be listed into several steps:

1. Preparing the optimal mesh of triangle in which the secret message is embedded. This activity can be done as follows:

- a. Get the original cover as shown in Figure 5(a).
- b. Get the secret message as shown in Figure 4.
- c. Extract the estimated depth from the original cover.
- d. Generate key points.
- e. Generate mesh of triangles.

Figure 6 shows mesh extraction operation.



- f. Collect the number of pixels inside each triangle.
- g. Calculate the correlation between pixels within triangles.

According to Figure 4, the size of secret message is 45000 ($75 \times 75 \times 8$). The capacity of triangle cover in Figure 5. (a) is 106791. So, the cover in Figure 5. (a) suitable for embedding the secret message.

Table 1. Triangles with its vertices, pixels, correlation degree, and max. capacity of triangles

Triangle Number	Point 1 (x, y)	Point 2 (x, y)	Point 3 (x, y)	Number of pixels	Correlation degree	No. of embedded bit(s)	The max. capacity of triangle
1	(176, 207)	(159, 234)	(134, 188)	492	Low	3	1476
2	(44, 189)	(159, 234)	(174, 289)	2182	Low	3	6546
3	(159, 234)	(159, 186)	(134, 188)	50	Medium	2	100
.	.	.	.	.		.	.
.	.	.	.	.		.	.
66	(150, 186)	(159, 113)	(176, 207)	49	High	1	49

67	(123, 186)	(150, 117)	(134, 188)	152	Low	3	456
The total capacity of cover							106791

Embedding the secret message, the optimal mesh of triangle in which the secret message is embedded. This activity can be done as follows:

- Storing the coordinates of vertex of all triangle in the border of cover using LSB method.
- Embedding the bit(s) of secret message in the triangles using LSB method depending on the correlation degree of each triangle. According of correlation degree for each triangle the number of bit(s) is embedded. For example, in each pixel of triangle number **1**, **3** bits of secret message can be embedded. Also, in each pixel of triangle number **3**, **2** bits of secret message can be embedded. Also, in each pixel of triangle number **66**, **1** bit of secret message can be embedded. The PSNR value is 58.3 db.

Part two: This part is done in the receiver side. In which the secret message is extracted from stego image. Also, part two can be listed into several steps:

1. Extracting the depth of stego image.
2. Extracting the coordinates of vertex of all triangles from the border of stego image.
3. Generate mesh of triangles depending of the extracted vertices.
4. Calculate the correlation between pixels within triangles.
5. Extracting the bit(s) of secret message from the triangles using LSB method depending on the correlation degree of each triangle. According of correlation degree for each triangle the number of bit(s) is extracted. For example, in each pixel of triangle number **1**, **3** bits of secret message can be extracted. Also, in each pixel of triangle number **3**, **2** bits of secret message can be extracted. Also, in each pixel of triangle number **66**, **1** bit of secret message can be extracted.

6. Conclusions and Future Works

This research proposed a steganographic method embeds the secret message in the mesh of triangle of image. The mesh of triangle is generated by several steps. The first step is estimation the depth of image using the MiDaS CNN model. In the second step, keypoint is detected using the Shi-Tomasi algorithm. The third step the mesh of triangles is generated using Delaunay triangulation. The embedding of secret message depending on the correlation degree of each triangle. Experimental results show that the proposed method offers a high PSNR (58.3 dB), flexible embedding capacity based on regional correlation, and a well-structured extraction mechanism.

Several future works can be listed as follows:

1. Studying the ability of building and train a new model for estimating the depth of image rather than pre-trained model in order to estimate more accurate depth. This operation may enhance the proposed method.

2. Studying the ability of extending the proposed method be work with another media rather than RGB image such audio, video, and text.
3. Studying the ability of the proposed method to work in real-time or near real-time optimization for live applications.
4. Studying the ability of proposed method to extract the secret message without needing to store coordinates on the image border. This development can improve security and make the method more practical in constrained environments.

References

- [1] D. Ashenden, "Information Security management: A human challenge?," Information Security Technical Report, vol. 13, no. 4, pp. 195–201, 2008, doi: 10.1016/j.istr.2008.10.006.
- [2] A. Shaik, V. Thanikaiselvan, and R. Amitharajan, "Data security through data hiding in images: a review," Journal of Artificial Intelligence, vol. 10, no. 1, pp. 1–21, 2017, doi: 10.3923/jai.2017.1.21.
- [3] B. Madhu, G. Holi, and S. Murthy, "An overview of image security techniques," International Journal of Computer Applications, vol. 154, no. 7, pp. 37–46, 2016, doi: 10.5120/ijca2016911834.
- [4] K. Hu, M. Wang, X. Ma, J. Chen, X. Wang, and X. Wang, "Learning-based image steganography and watermarking: A survey," Expert Systems with Applications, vol. 249, part C, p. 123715, 2024, doi: 10.1016/j.eswa.2024.123715.
- [5] Z. Wang, O. Byrnes, H. Wang, R. Sun, C. Ma, H. Chen, Q. Wu, and M. Xue, "Data hiding with deep learning: A survey – Unifying digital watermarking and steganography," arXiv preprint arXiv:2107.09287, 2023.
- [6] Z. I. Nezami, H. Ali, M. Asif, H. Aljuaid, I. Hamid, and Z. Ali, "An efficient and secure technique for image steganography using a hash function," PeerJ Computer Science, vol. 8, e1157, 2022, doi: 10.7717/peerj-cs.1157.
- [7] "A review on image steganography techniques," International Research Journal on Advanced Engineering Hub (IRJAEH), vol. 2, no. 7, pp. 1986–1996, 2024, doi: 10.47392/IRJAEH.2024.0271.
- [8] K. A. Zhang, A. Cuesta-Infante, L. Xu, and K. Veeramachaneni, "SteganoGAN: High capacity image steganography with GANs," arXiv preprint arXiv:1901.03892, 2019.
- [9] X. Duan, N. Liu, M. Gou, W. Wang, and C. Qin, "SteganoCNN: Image steganography with generalization ability based on convolutional neural network," Entropy, vol. 22, no. 10, p. 1140, 2020, doi: 10.3390/e22101140.
- [10] W. Tang and G. Qiu, "Dense graph convolutional neural networks on 3D meshes for 3D object segmentation and classification," Image and Vision Computing, vol. 114, p. 104265, 2021, doi: 10.1016/j.imavis.2021.104265.

- [11] Q. Dong *et al.*, "Laplacian2Mesh: Laplacian-Based Mesh Understanding," in *IEEE Transactions on Visualization and Computer Graphics*, vol. 30, no. 7, pp. 4349-4361, July 2024, doi: 10.1109/TVCG.2023.3259044.
- [12] K. X. Ke, H. Wu, and W. Guo, "StegFormer: Rebuilding the Glory of Autoencoder-Based Steganography," in **Proceedings of the AAAI Conference on Artificial Intelligence**, vol. 38, no. 3, pp. 2723-2731, 2024, doi: 10.1609/aaai.v38i3.28051.
- [13] L. Huo, R. Chen, J. Wei, and L. Huang, "A High-Capacity and High-Security Image Steganography Network Based on Chaotic Mapping and Generative Adversarial Networks," *Applied Sciences*, vol. 14, no. 3, p. 1225, Feb. 2024, doi: 10.3390/app14031225.
- [14] Lee, D. T., & Schachter, B. J. (1980). Two algorithms for constructing a Delaunay triangulation. *International Journal of Computer & Information Sciences*, 9(3), 219-242, doi: 10.1007/BF00977785
- [15] J. Shi and C. Tomasi, "Good features to track," *Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit.*, no. March 2000, pp. 593–600, 1994, doi: 10.1109/cvpr.1994.323794.
- [16] C. Spearman, "The Proof and Measurement of Association between Two Things," *The American Journal of Psychology*, vol. 15, no. 1, pp. 72-101, Jan. 1904. [Online]. Available: <https://www.jstor.org/stable/1412159>.
- [17] Ranftl, R., Lasinger, K., Hafner, D., Schindler, K., & Koltun, V. (2020). Towards Robust Monocular Depth Estimation: Mixing Datasets for Zero-shot Cross-dataset Transfer. *IEEE Transactions on Pattern Analysis and Machine Intelligence (TPAMI)*.