A Lossless Data Embedding Technique For Medical Image Based On Different Expansion

Banti Chie
Software Engineering
University Of Lay Adventists Of Kigali
Nyanza, Rwanda.
bantichie2007@gmail.com

Galal Abaker Adam
Software Engineering
University *Of Lay Adventists Of Kigali*
Nyanza,Rwanda
jalaltwix504@gmail.com

CorneliusD.Chon
SoftwareEngineering
University Of Lay Adventists Of Kigali
Nyanza Rwanda
choncornelius7@gmail.com

***Abstract*—this study proposes a novel lossless data embedding technique for medical images using a difference expansion using a difference expansion approach to enhance secure data transmission. The method focuses on embedding confidential information within radiological images while maintaining high image quality and ensuring full reversibility. Unlike existing techniques that struggle to balance payload capacity and imperceptibility, the proposed algorithm optimizes pixel value differences, particularly along image rows, to increase embedding efficiency with minimal distortion. The approach selectively modifies pixels under controlled conditions and records embedding locations using a key, enabling accurate data extraction and complete recovery of the original image. Experimental results on various medical images demonstrate that the method achieves high peak signal-to-noise ratio (PSNR) values even with increased pay loads, confirming its effectiveness in preserving image quality. This technique offers a reliable solution for secure medical data handline and can be applied in sensitive fields requiring both data confidentiality and image integrity.**

Keywords— Medical Images, Difference Expansion, Steganography, Data Hiding, Secure Data Transmission, Pixel Value Differences, Image Quality, Reversibility.

I. INTRODUCTION

This image steganography has recently received growing attention as a technique for hiding data, and it stands out as a reliable solution for strengthening the security of transmitting sensitive information [1]. Steganography is a data-hiding technique that involves embedding secret information within digital media, such as audio and video [2], [3] and images [4]. Data hiding can be mathematically represented in (1), where S denotes the steganographic scheme, the medium carrying the secret information is referred to as the cover, and the final output is known as the stego medium.

F(cover, secret _data) = stego

The primary goal of any steganographic method is to maintain high visual quality of the stego image, even when a large amount of data is embedded [5], [6], while also minimizing the risk of the stego image being detected or exposed by steganalysis techniques [7], [8], [9]. Although many steganographic methods have been introduced to enhance the quality of stego images, balancing image quality with payload capacity remains a persistent challenge in digital image steganography.

In recent studies, efforts have been directed toward reducing noticeable distortion in stego images that contain large amounts of hidden data, often through the application of different mathematical techniques such as pixel sorting. [10], modification of image feature styles, [11] and other related techniques [12], [13]. However, existing approaches have not fully resolved the problem but rather provide only promising improvements. In this study, we build upon these prior works to propose a new steganographic algorithm aimed at enhancing the security of stego images while maintaining high imperceptibility.

The proposed method addresses the issue of reduced imperceptibility caused by embedding large amounts of data by focusing on medical images. These images offer an advantage due to the presence of many less significant pixels, which makes them suitable for hiding information. As a result, radiological medical images can serve as effective carriers for sensitive data. Therefore, our approach introduces an algorithm that can be effectively applied in medical data security by embedding patients' confidential information within their corresponding radiological images. [14]-[16] aiming to enhance the data hiding process by improving the expansion of differences between neighboring pixels. We further validate the effectiveness of our proposed algorithm through experiments conducted on sample medical images.

To accomplish this, we designed a steganographic algorithm that optimizes pixel value differences along image rows. Our approach is inspired by existing studies. The remaining sections of this paper are organized as follows: Section II reviews related works that share similar objectives; Section III explains the proposed steganographic method, including both data embedding and extraction processes; Section IV presents and analyzes the experimental results; and Section V concludes the study [17].

II. LITERATURE REVIEW

In this part, we review previously proposed methods aimed at improving steganographic algorithms. The selected references are primarily from the last five years to ensure the use of up-to-date research. A prior study [10] presented a data-hiding technique that preserved the visual quality of images very effectively. However, the method was limited to embedding data in only about half of the image pixels, making it unsuitable for large payloads. The

approach relied on a different expansion algorithm to utilize gaps between adjacent pixels and included a pixel-sorting process. This sorting step may pose risks in sensitive fields such as medical or military applications, as it can lead to data loss and affect the recovery of the original cover image. Despite its strong performance, the method is not ideal where data integrity is critical.

In another study [4] a new steganographic scheme was proposed that combines fuzzy logic with difference expansion to embed secret bitstreams into images. This approach demonstrated good performance by reducing the tradeoff between payload capacity and image imperceptibility. However, the method showed limitations, as it did not perform optimally for certain types of images, making it less suitable for specific real-world applications such as medical or space-related systems. Furthermore, due to the use of fuzzy logic, the original image could not be perfectly recovered, which is a significant drawback for sensitive applications like military or medical use. A study in [14]-[16] introduced a data-hiding method for encrypting images to enhance embedding capacity. The authors applied vector quantization prediction to identify suitable locations within image pixels for embedding data. This technique estimates available space within the cover image and uses it for encryption and data insertion. The method produced promising results by leveraging minimal differences between vector quantization outputs and predicted pixel values. However, the study did not clearly demonstrate how the method could be applied in real-world scenarios. Therefore, there is a need for a more adaptable algorithm that can be applied to domains such as medical imaging.

In [5], [6], another reversible steganographic technique was proposed for embedding secret data into encrypted images using a hierarchical approach. A label map hierarchy is created through prediction, then compressed and embedded into the encrypted image. This method is designed to maximize data embedding capacity by categorizing prediction errors into three levels—small, medium, and large—with each assigned to a specific label. Unlike traditional methods, this approach allows both small and large prediction errors to be used for data hiding, significantly increasing embedding capacity. Although experimental results showed good performance on digital images, the issue of balancing payload size and stego image quality remains unresolved.

```
// Algorithm I: Embedding the secret data (s)

static void EmbedSecretData(int[,] image, int[,] stegoImage, int[,] d, int[,] key, int s)
{
rows = 512;
int cols = 512;
for (int row = 1; row <= rows; row++)
        {
        for (int col = 1; col <= cols; col++)
                {
                        // row-1 and col-1 because C# arrays start from 0
                        if ((row % 2 == 0) &&
                                (0 <= d[row - 1, col - 1] && d[row - 1, col - 1] <= 2) &&
                                (image[row - 1, col - 1] <= 252))
                        {
                                stegoImage[row - 1, col - 1] =
                                image[row - 1, col - 1] + d[row - 1, col - 1] + s;
                                key[row - 1, col - 1] = 1;
                        }
                }
        }
}
```

```
1.    // Algorithm I: Embedding the secret data (s)
class SteganographyAlgorithm
{
   static void Main()
   {
      int rows = 512;
      int cols = 512;

      int[,] image = new int[rows, cols];
      int[,] stegoImage = new int[rows, cols];
      int[,] coverImage = new int[rows, cols];
      int[,] d = new int[rows, cols];
      int[,] key = new int[rows, cols];

      int s = 1; // secret data bit example
   }
}
```

The study in [16] introduces a new method for embedding data within encrypted images. This approach utilizes a double linear regression prediction model, which improves the accuracy of estimating pixel values based on their neighboring pixels. As a result, more space is created for embedding secret information. Additionally, an error map is generated to identify regions where prediction inaccuracies occur, and this map can be compressed efficiently without any loss of information, thereby minimizing the storage overhead of auxiliary data. The method also guarantees complete and reversible recovery of the original image.

Similarly, in [14]-[16] the authors proposed a novel data-hiding technique in encrypted images referred to as the Vacant Room after Encryption (VRAE) method. This approach addresses the limitations of earlier methods that suffered from prediction inaccuracies, which affected full reversibility. By incorporating a linear regression-based predictor, the method improves prediction precision, while an error-detection map is used to correct inaccuracies. These improvements significantly enhance the embedding capacity and ensure that the original image can be perfectly restored without any loss.

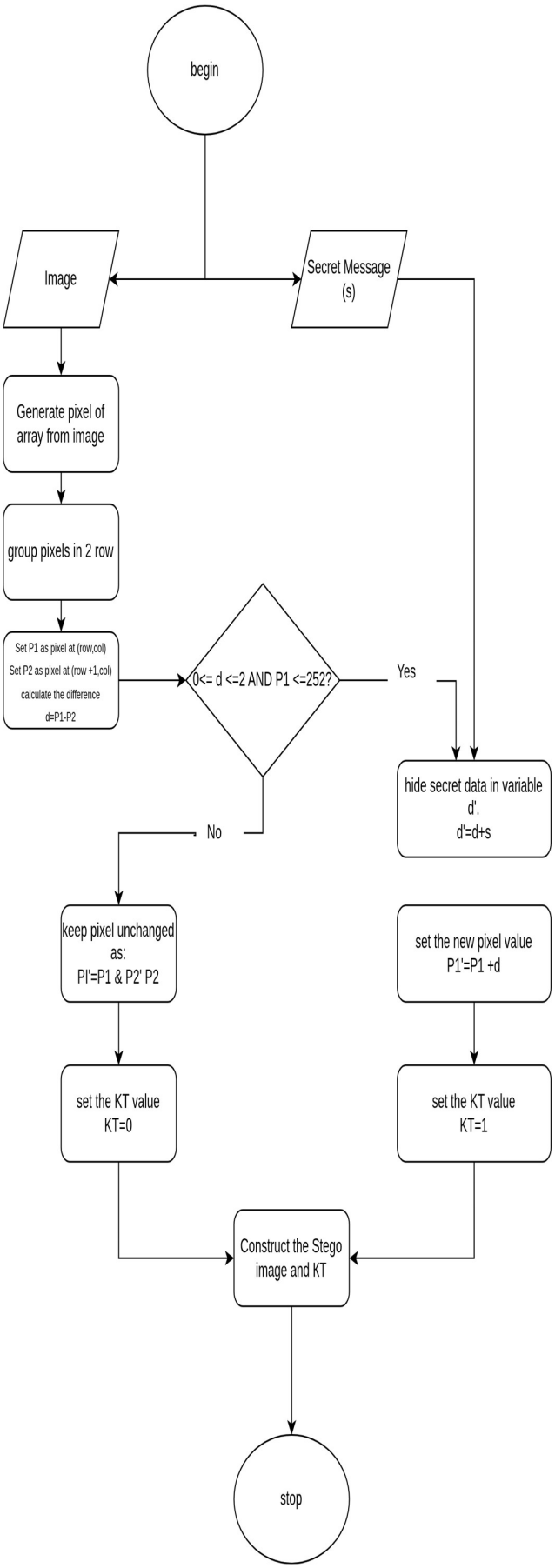
III METHODOLOGY

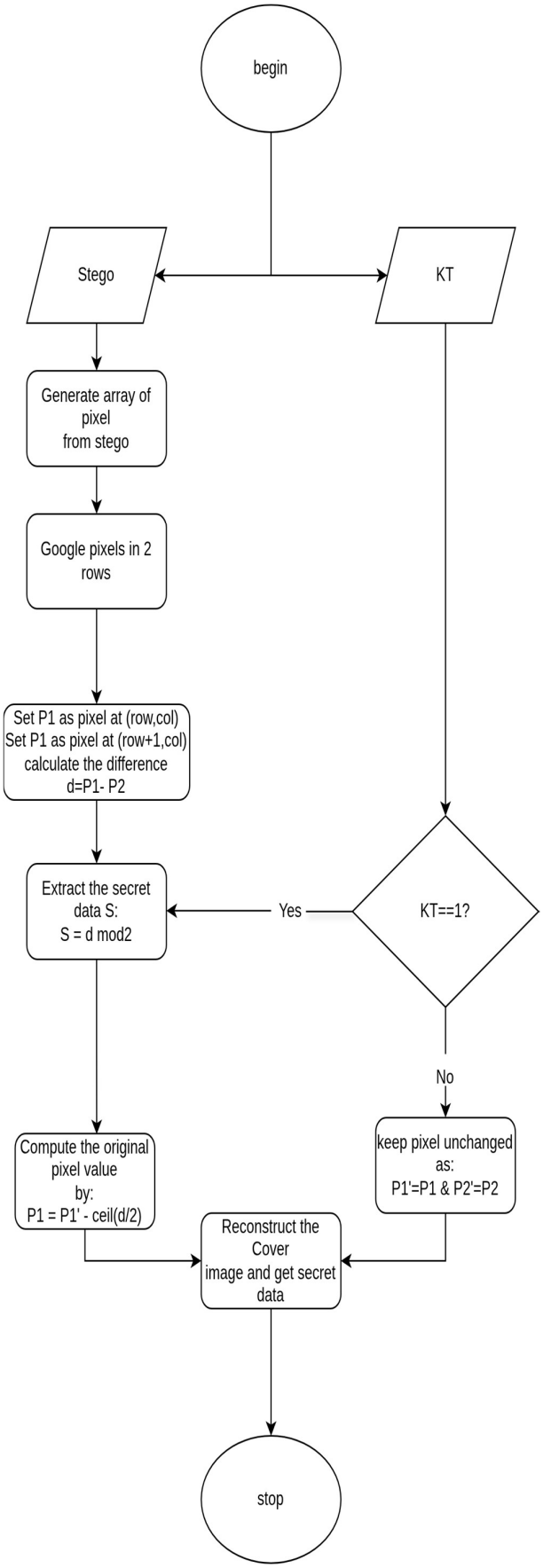
In this work, we aim to develop a new algorithm for embedding secret data into medical images. Given that medical applications require exact reconstruction of the original image, our approach focuses on optimizing the extraction process to ensure complete recovery without any data loss.

Payload (kb)	**Obtained Results**	
	Cover image	**PSNR (in Decibels)**
1	Hand	69.3981
	Leg	69.6328
	Chest	71.8513
	Head	73.1517
	Abdominal	73.1517
10	Hand	60.7945
	Leg	61.3610
	Chest	61.5132
	Head	61.5823
	Abdominal	60.8293
20	Hand	58.7451
	Leg	58.9904
	Chest	58.3000
	Head	58.2003
	Abdominal	58.0174
30	Hand	57.4282
	Leg	57.6109
	Chest	56.5644
	Head	56.5298
	Abdominal	56.6310
40	Hand	56.2908
	Leg	56.5900
	Chest	55.1288
	Head	55.4308
	Abdominal	55.2777
50	Hand	55.2406
	Leg	55.8959
	Chest	54.1360
	Head	54.5721
	Abdominal	54.1795
60	Hand	54.3256
	Leg	55.2687
	Chest	53.3273
	Head	53.8700
	Abdominal	53.3717
70	Hand	53.5839
	Leg	54.5757
	Chest	52.8421
	Head	53.2809
	Abdominal	52.7028
80	Hand	52.9735
	Leg	53.7156
	Chest	52.4754
	Head	52.8479
	Abdominal	52.0815
90	Hand	52.4816
	Leg	52.6478

	Chest	52.0340
	Head	52.8223
	Abdominal	51.9304
100	Hand	52.1200
	Leg	51.9729
	Chest	51.7514
	Head	52.8202
	Abdominal	51.9271

Algorithm II describes a systematic procedure for retrieving both the hidden data (s') and the original cover image from the stego image. The process scans every pixel in a 512×512 image. For each pixel, it checks the corresponding key value (key[row−1] [col]) to determine whether that pixel was altered during embedding, specifically when the key equals 1. If this condition is satisfied, the algorithm proceeds to recover the secret data and the original pixel value. The hidden data ('s') is obtained by computing the remainder of the modified difference value (d′[row−1] [col]) when divided by 2. In addition, a value 'X' is calculated as half of the difference value, rounded up to the nearest integer using the ceiling function. The original cover image pixel is then reconstructed by subtracting 'X' from the corresponding pixel in the stego image (Stego_image[row−1] [col]). Through this process, the algorithm successfully retrieves both the embedded secret data and the original image while identifying which pixels were modified during embedding achieves the highest embedding capacity of 102,063 pixels. comparison, the "Head" image has a lower payload capacity (0.3056), suggesting more limited capacity for data concealment. Overall, these findings contribute valuable insights into the application of steganography in medical imaging.





IV. RESULTS

This section presents the experimental outcomes achieved using the proposed method. The performance of the algorithm is assessed using the peak signal-to-noise ratio (PSNR), expressed in decibels (dB), along with payload capacity measured in bits per pixel (bpp). Table I reports the PSNR values obtained for various images under different payload sizes.

The results in Table I provide a comprehensive analysis of how payload size (in kb) affects PSNR across several medical images, namely “Hand,” “Leg,” “Chest,” “Head,” and “Abdominal.” PSNR serves as an important measure of image quality, where higher values indicate better quality. As the payload increases from 1 kb to 100 kb, a general decline in PSNR is observed for all images, demonstrating the tradeoff between embedding more data and maintaining image quality. Among the tested images, the “Chest” and “Head” consistently achieve higher PSNR values, suggesting greater robustness to data embedding while preserving visual quality.

Table II highlights key findings related to embedding capacity. It presents both the payload capacity—defined as the ratio of hidden data to total pixel count—and the actual embedding capacity in terms of the number of pixels available for data hiding. The “Chest” image shows the highest payload capacity (0.3893), indicating its ability to store a relatively large amount of hidden data per pixel, and correspondingly

V. CONCLUSION

This study focuses on addressing a key issue in medical image steganography—the imbalance between the capacity to embed secret data and the resulting image quality after embedding. Earlier approaches have attempted to solve this problem but often resulted in a noticeable trade-off between PSNR and payload size. To overcome this limitation, we proposed a new method based on difference expansion in medical images improve the performance of existing techniques. The experimental results confirm that our approach significantly outperforms previous methods, allowing larger amounts of data to be hidden while preserving the quality of the stego image.

Looking ahead, future work will aim to broaden the application of this method and strengthen the security of stego images across different fields. Further improvements will also focus on reducing the tradeoff between payload capacity and image quality, leading to more effective and reliable steganographic solutions.

REFERENCES

[1] Z. Yin, Y. Xiang, and X. Zhang, "Reversible Data Hiding in Encrypted Images Based on Multi-MSB Prediction and Huffman Coding," *IEEE Trans. Multimedia*, vol. 22, no. 4, pp. 874–884, Apr. 2020, doi: 10.1109/TMM.2019.2936314.

[2] I. B. Prayogi, T. Ahmad, N. J. de La Croix, and P. Maniriho, "Hiding Messages in Audio using Modulus Operation and Simple Partition," in *2021 13th International Conference on Information & Communication Technology and System (ICTS)*, IEEE, Oct. 2021, pp. 51–55. doi: 10.1109/ICTS52701.2021.9609028.

[3] T. Ahmad and A. N. Fatman, "Improving the performance of histogram-based data hiding method in the video environment," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 4, pp. 1362–1372, Apr. 2022, doi: 10.1016/j.jksuci.2020.04.013.

[4] N. J. De La Croix, C. C. Islamy, and T. Ahmad, "Secret Message Protection using Fuzzy Logic and Difference Expansion in Digital Images," in *2022 IEEE Nigeria 4th International Conference on Disruptive Technologies for Sustainable Development (NIGERCON)*, IEEE, Apr. 2022, pp. 1–5. doi: 10.1109/NIGERCON54645.2022.9803151.

[5] I. Théophile, N. J. De La Croix, and T. Ahmad, "Fuzzy Logic-based Steganographic Scheme for high Payload Capacity with high Imperceptibility," in *2023 11th International Symposium on Digital Forensics and Security (ISDFS)*, IEEE, May 2023, pp. 1–6. doi: 10.1109/ISDFS58141.2023.10131727.

[6] C. Yu, X. Zhang, X. Zhang, G. Li, and Z. Tang, "Reversible Data Hiding With Hierarchical Embedding for Encrypted Images," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 32, no. 2, pp. 451–466, Feb. 2022, doi: 10.1109/TCSVT.2021.3062947.

[7] J. D. L. C. Ntivuguruzwa and T. Ahmad, "A convolutional neural network to detect possible hidden data in spatial domain images," *Cybersecurity*, vol. 6, no. 1, p. 23, Sep. 2023, doi: 10.1186/s42400-023-00156-x.

[8] N. J. De La Croix and T. Ahmad, "Toward secret data location via fuzzy logic and convolutional neural network," *Egyptian Informatics Journal*, vol. 24, no. 3, p. 100385, Sep. 2023, doi: 10.1016/j.eij.2023.05.010.

[9] N. J. de La Croix and T. Ahmad, "Toward Hidden Data Detection via Local Features Optimization in Spatial Domain Images," in *2023 Conference on Information Communications Technology and Society (ICTAS)*, IEEE, Mar. 2023, pp. 1–6. doi: 10.1109/ICTAS56421.2023.10082736.

[10] N. J. de La Croix, C. C. Islamy, and T. Ahmad, "Reversible Data Hiding using Pixel-Value-Ordering and Difference Expansion in Digital Images," in *2022 IEEE International Conference on Communication, Networks and Satellite (COMNETSAT)*, IEEE, Nov. 2022, pp. 33–38. doi: 10.1109/COMNETSAT56033.2022.9994516.

[11] Y. Sun, J. Liu, and R. Zhang, "Large capacity generative image steganography via image style transfer and feature-wise deep fusion," *Applied Intelligence*, vol. 53, no. 23, pp. 28675–28693, Dec. 2023, doi: 10.1007/s10489-023-04993-8.

[12] A. J. Ilham, T. Ahmad, N. J. D. La Croix, P. Maniriho, and M. Ntahobari, "Data Hiding Scheme Based on Quad General Difference Expansion Cluster," *Int. J. Adv. Sci. Eng. Inf. Technol.*, vol. 12, no. 6, pp. 2288–2296, Nov. 2022, doi: 10.18517/ijaseit.12.6.16002.

[13] A. N. Fatman, T. Ahmad, N. Jean De La Croix, and Md. S. Hossen, "Enhancing Data Hiding Methods for Improved Cyber Security Through Histogram Shifting Direction Optimization," *Mathematical Modelling of Engineering Problems*, vol. 10, no. 5, pp. 1508–1514, Oct. 2023, doi: 10.18280/mmep.100502.

[14] K. Chen and C.-C. Chang, "Error-free separable reversible data hiding in encrypted images using linear regression and prediction error map," *Multimed. Tools Appl.*, vol. 78, no. 22, pp. 31441–31465, Nov. 2019, doi: 10.1007/s11042-019-07946-x.

[15] S. Xu, C.-C. Chang, and Y. Liu, "A high-capacity reversible data hiding scheme for encrypted images employing vector quantization prediction," *Multimed. Tools Appl.*, vol. 80, no. 13, pp. 20307–20325, May 2021, doi: 10.1007/s11042-021-10698-2.

[16] F. Li, H. Zhu, J. Yu, and C. Qin, "Double linear regression prediction based reversible data hiding in encrypted images," *Multimed. Tools Appl.*, vol. 80, no. 2, pp. 2141–2159, Jan. 2021, doi: 10.1007/s11042-020-09805-6.

[17] D. Gut, Z. Tabor, M. Szymkowski, M. Rozynek, I. Kucybala, and W. Wojciechowski, "Benchmarking of Deep Architectures for Segmentation of Medical Images," *IEEE Trans. Med. Imaging*, vol. 41, no. 11, pp. 3231–3241, Nov. 2022, doi: 10.1109/TMI.2022.3180435.