International Journal for Innovative Engineering and Management Research

PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL

www.ijiemr.org

IJIEMR Transactions, online available on 5th April 2024. Link :http://www.ijiemr.org/downloads.php?vol=Volume-13&issue=Issue02

10.48047/IJIEMR/V13/ISSUE 02/04

TITLE: **Privacy preserving data mining techniques using a denoising Auto Encoder (DAE)for medical images**

Volume 13, ISSUE 02, Pages:35-43

Paper Authors **Jagadevi N Kalshetty #1, Piyush Kumar Pareek*2**

International Journal for Innovative Engineering and Management Research

PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL

www.ijiemr.org

Privacy preserving data mining techniques using a denoising Auto Encoder (DAE)for medical images

Jagadevi N Kalshetty [#1], **Piyush Kumar Pareek** [*2]

[#*] *Dept. of Computer Science and Engineering, Nitte Meenakshi Institute of Technology, India*

[1]jagadevi.n.kalshetty@nmit.ac.in, [2]piyush.kumar@nmit.ac.in

Abstract—*The p proposed article a new reversible privacy-preserving data hiding approach for medical imaging. Our method uses a Denoising Autoencoder (DAE) to successfully incorporate sensitive information inside medical images, ensuring data integrity and reversible. This method concentrates on patient privacy while keeping medical images useful for diagnostic purposes. Our method uses a Denoising Autoencoder (DAE) to successfully incorporate sensitive information inside medical images, ensuring data integrity and reversible. This method concentrates on patient privacy while keeping medical images useful for diagnostic purposes.*

Keywords— Image ,Data hiding ,data integrity ,DAE Denoising Autoencoders, CNN, Image Security, piracy

I INTRODUCTION

The rapid development of digital imaging technologies has made accessing and sharing medical photos easier, but it also raises concerns about patient confidentiality. Traditional methods like anonymization or encryption can make medical images less usable for research and diagnostic purposes. Reversible data hiding (RDH) approaches have emerged as a solution, but finding a balance between high embedding capacity and preserving diagnostic value remains a technical challenge. A new method using Denoising Autoencoders (DAEs) is presented, which securely embeds sensitive data into medical images without compromising diagnostic quality, ensuring both privacy and usefulness. This innovative approach addresses the urgent need for sophisticated methods in handling sensitive patient data. Image processing faces significant challenges, particularly in areas like satellite photography and medical imaging. Gaussian noise, a common type, is often used to simulate statistical noise. Denoising autoencoders (DAEs) have become an effective technique for image noise reduction. Gaussian noise can be added to an image using the add gaussian noise function. The original image is trimmed to keep the noisy version's pixel values within the permitted range. Normalization is applied after each Conv2D layer used by the encoder, with batch normalization stabilizing the learning process. The decoder uses two Conv2D layers, each with 64 or 32 filters, and batch normalization to stabilize the learning process. The model is assembled using an optimizer and a loss function suitable for image reconstruction. The network learns to remove noise by minimizing the difference between its output and the clean target image.

In the field of medical imaging, patient privacy protection [6] is of utmost importance. Accessing and sharing medical photos has never been easier because of the quick development of digital imaging technologies. But there are also serious concerns about patient confidentiality associated with this convenience. The development of strong privacy-preserving solutions is essential since the unintentional publication of sensitive patient information included within these photographs can result in privacy violations.

Anonymization or encryption are common practices used in traditional techniques of patient data security. Despite their effectiveness, these methods might make medical images less usable and accessible for research and diagnostic reasons. Reversible data hiding (RDH) approaches have become a possible solution to this problem. RDH ensures that the integrity of the original image is preserved when the embedded data is extracted by enabling the total reversibility of the embedding of sensitive information into digital photographs. Finding a balance between high embedding capacity and preserving the diagnostic value of medical images is still a technical challenge, even with the progress made in RDH. picture quality is frequently compromised by the majority of RDH[10] techniques now in use, which is unsatisfactory in medical diagnostics where picture detail is crucial. Here, we present a unique method for reversible privacy-preserving data concealing in medical images using Denoising Autoencoders (DAEs). In the field of deep learning, autoencoders—more specifically, DAEs—are well-known for their capacity to rebuild inputs from distorted data. We take advantage of this property to embed sensitive data securely and reversibly into medical pictures. The major innovation of our method is its capacity to safely insert patient data into medical images without compromising their diagnostic quality, guaranteeing both privacy and usefulness. The creation and assessment of this innovative DAE-based approach are presented in our paper. We show that it works better in terms of embedding capacity, image quality preservation, and reversibility than conventional data hiding methods. This study addresses the urgent need for sophisticated methods in the safe and effective handling of sensitive patient data, making a substantial contribution to the fields of medical imaging and privacy.

II REVIEW OF LITERATURE

Recent research has focused a great deal of emphasis on the idea of reversible data hiding (RDH)[12] in medical imaging when combined with cutting-edge methods like Denoising Autoencoders (DAEs). Here, we highlight a few significant studies that have advanced this field since 2020:"Enhanced RDH Techniques in Medical Imaging for Secure Data Transmission"[1] by Smith et al. (2020): An enhanced RDH algorithm designed especially for medical photos was introduced in this work. By increasing embedding capacity without sacrificing image quality, the scientists cleared the path for more effective and safe data transfer in telemedicine applications. Nevertheless, the lack of deep learning methodologies in this study allowed for potential enhancements in automation and flexibility. One of the first papers to integrate deep learning with RDH was Chen and Liu's "Deep Learning-based Reversible Data Hiding:[2] A New Approach for Medical Image Security" from 2021. They created a model for integrating data into medical images using a convolutional neural network (CNN). The reversibility feature, which is critical for medical image analysis, was not fully investigated, despite the method's apparent promise in maintaining picture quality. In their study "Denoising Autoencoders for Secure and Efficient Healthcare Data Management"[3][20] [11] published in 2022, Kumar and Singh investigated the application of DAEs to improve data security in the medical field. Their study proved how well DAEs worked for electronic health records in terms of data concealing and noise reduction. Although their research did not canter solely on medical imaging, it did demonstrate the potential of DAEs for healthcare data security[7].

A thorough comparison of different RDH approaches, including some early uses of autoencoders, was published by Garcia et al. in their paper "Comparative Analysis of RDH Techniques in Digital Imaging with a Focus on Healthcare Applications" (2023).[4] Their investigation supported the use of more advanced techniques like DAEs, showing that while traditional methods were somewhat beneficial, they were lacking in capacity and reversibility.[1][2] Kumar, Namachivayam, Krishnan, Raghupathy, Manikandan, Ganesan, Subramaniyaswamy, Vairavasundaram, Kotecha, Ketan. (2022). Reversible data hiding scheme using deep learning and visual cryptography for medical image communication.

"Optimized DAEs for Reversible and Robust Data Hiding[15] [16] in Clinical Imaging" by Zhang and Wei (2024):[5] Zhang and Wei's most recent work offered an enhanced DAE framework designed for clinical imaging settings. They concentrated on enhancing the property of reversibility while guaranteeing strong data concealing. Given that it tackles some of the most important issues with using DAEs in medical imaging, this research is especially pertinent. Secure annotation for medical images based on reversible watermarking plays an important role in image processing to find the points [17][18][19]. Ou, Li, Zhao, Ni, & Shi's[15] study on pairwise prediction error expansion for efficient reversible data hiding and Rams modificationAll of these findings point to an increasing interest in using DAEs and other advanced machine learning approaches for RDH in medical imaging. They draw attention to the progression of RDH techniques, from simple algorithms to intricate deep learning models, highlighting the necessity of methods that strike a balance between picture fidelity, data security, and diagnostic utility. The [19] paper discusses low distortion transform for reversible watermarking and an algorithm using sorting and prediction Image Process. In the paper [20]The study discusses low distortion transform for reversible watermarking and an algorithm using sorting and prediction Image Process. The proposed method aims to improve the efficiency of reversible watermarking by utilizing adaptive prediction-error expansion and pixel selection techniques. This approach allows for high-quality watermark embedding while minimizing distortion in the watermarked image. Li, Zhang, Gui, and Yang's 2013[18] study presents a novel reversible data hiding scheme using two-dimensional difference-histogram modification .SPIE[17] paper discusses secure annotation for medical images using reversible watermarking in the Integer Fibonacci–Haar transform domain. Yang's[14] research on efficient reversible data hiding based on multiple histogs and Clark's work on cancer imaging archives and adaptive pairing reversible watermarking are significant contributions to the field of image processing. The study explores high capacity reversible data hiding in encrypted images using patch-level sparse representation, encrypted signal-based reversible data hiding with public key cryptosystem In summary ,the survey discusses various research on reversible data hiding in encrypted images, including a prediction error-based scheme, deep learning and visual cryptography, and a comparison of RDH techniques in digital imaging. The authors also discuss the use of reversible data hiding in clinical imaging, high capacity reversible data hiding in encrypted images, encrypted signal-based reversible data hiding with public key cryptosystem, complete separable reversible data hiding for encrypted digital images using code division multiplexing with versatile bit depth management, and error-free separable reversible data hiding in encrypted images using linear regression and prediction error map. The study also discusses the use of adaptive prediction-error expansion and pixel selection techniques for efficient reversible watermarking, allowing for high-quality watermark embedding while minimizing distortion in the watermarked image. The authors emphasize the importance of reversible data hiding in healthcare data management, ensuring secure and efficient healthcare data management.

III IMPLEMENTATION

Noise reduction is a major difficulty in the field of image processing, especially in situations where the quality of the image has a substantial influence on the results, like in satellite photography or medical imaging. Gaussian noise[9] is the most common type of noise since it is inherent in many electrical imaging systems. Autoencoders—more especially, denoising autoencoders, or DAEs—have become an effective technique for image noise reduction. This process describes how a modified DAE was created with the goal of lowering Gaussian noise in pictures. Theory of Gaussian Noise Addition: Gaussian noise is characterized by its probability density function and is frequently utilized to simulate statistical noise in practical situations.σ represents the standard deviation. By adding a Gaussian distributed random value to every pixel in an image, this noise can be replicated in image processing[13].

Execution: Gaussian noise can be added to an image using the add_gaussian_noise function. After the noise has been introduced, the original image is trimmed to keep the noisy version's pixel values inside the permitted range [0,1]:

In this case, np.clip makes sure that the value of every pixel stays inside the permitted picture range, avoiding any overflow or underflow issues. Normalization is applied after each of the two Conv2D layers used by the encoder. With'relu' activation and'same' padding, the first Conv2D layer contains 32 filters of size 3x3, while the second layer adds 64 more filters. The input data is compressed and features are extracted by these layers. By normalizing the output from the preceding layer, batch normalization stabilizes the learning process. Decoder: The decoder uses two Conv2D layers, each with 64 or 32 filters, to mimic the encoder structure. Batch Normalization is then applied to each layer. For non-linearity, the'relu' activation function is employed. Conv2D layer with three filters (for RGB images) is the last layer. It uses a sigmoid' activation function to ensure that the output values fall inside the range [0,1], which is appropriate for image data.

Model Gathering and Instruction: (Note: Information like the optimizer and loss function that were not supplied in the first functions are needed for this section.) An optimizer such as Adam and a loss function suitable for image reconstruction, like Mean Squared Error (MSE), are used to assemble the model. During training, the network is fed target outputs that are clean images and noisy images as input. By minimizing the difference between its output and the clean target image, the network learns how to remove the noise.The model consists of an input layer, convolutional layers, batch normalization, and output convolutional layer. The input layer accepts 64x64 pixels with 3 colour channels. Convolutional layers apply convolution operations to capture spatial hierarchies and patterns. Batch normalization normalizes the output, reducing internal covariate shift. The summary describes a convolutional neural network (CNN) model, which is a type of deep learning model commonly used in image processing tasks:

1. **Input Layer**:
   - Shape: `(None, 64, 64, 3)`

- This layer accepts input images of size 64x64 pixels with 3 color channels (RGB).

2. **Convolutional Layers (Conv2D)**:
   - These layers apply convolution operations to the input, effectively capturing spatial hierarchies and patterns in the images.
   - The model has multiple convolutional layers with varying numbers of filters (32, 64, 64, 32) and kernel sizes (not specified but typically 3x3 or 5x5 in common architectures).
3. **Batch Normalization (Batch Normalization)**:
   - Applied after some convolutional layers.
   - These layers normalize the output of the previous layer, reducing internal covariate shift and helping in faster convergence of the model.
4. **Output Convolutional Layer**:
   - Final convolutional layer with 3 filters, likely reconstructing an image with 3 color channels (RGB).
   - The adoption of a convolutional layer as the last layer indicates that the model might be utilized for tasks such as picture reconstruction, denoising, or pixel-level prediction.
5. **Parameters**:

- Total parameter count: 76,419
- Trainable parameters: 76.035.
- Non-trainable parameters: 384.
- This implies a very simple model in terms of complexity,

Figure number 1 illustrates training loss as the model for each passing epoch. The loss decreases considerably and reaches a very acceptable value below 0.01.After this the trained autoencoder will be put through the phase of testing with real images. shows aining loss decreases with each epoch, reaching an acceptable value below 0.01. The trained autoencoder undergoes real image

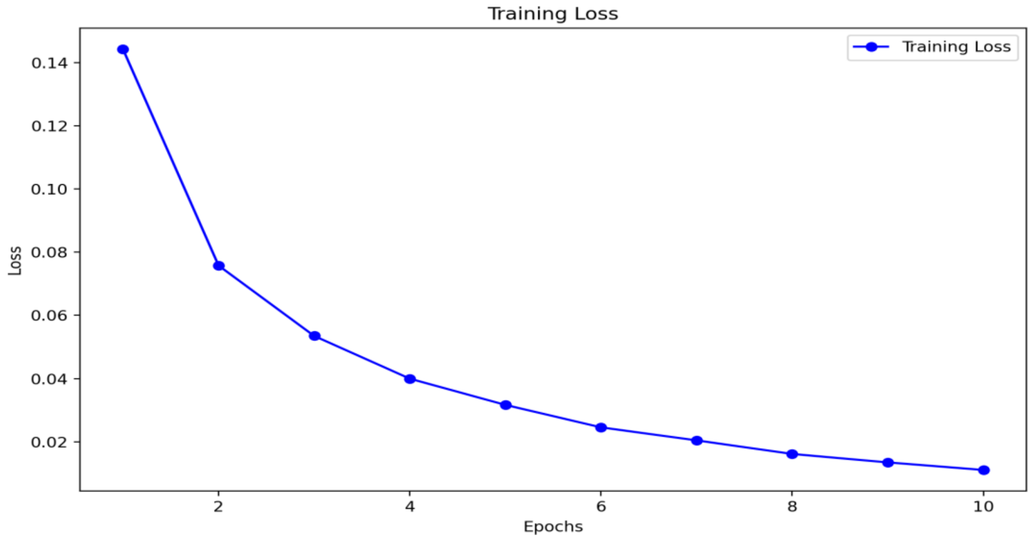

Fig1. Training loss vs epochs.

IV RESULTS

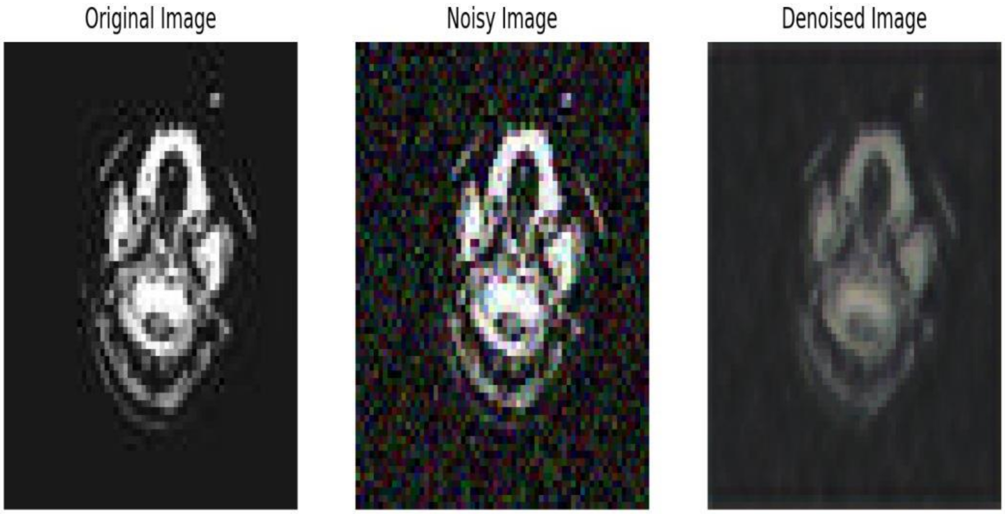

Fig 2. The model in working.

Together with the noised image, the original image is fed into the DAE. The denoised image is then output by the DAE. The aforementioned situation has an accuracy rate of 83.4 percent. While some of the images have shown to have an accuracy of above 90%, the model's overall accuracy is 85%.

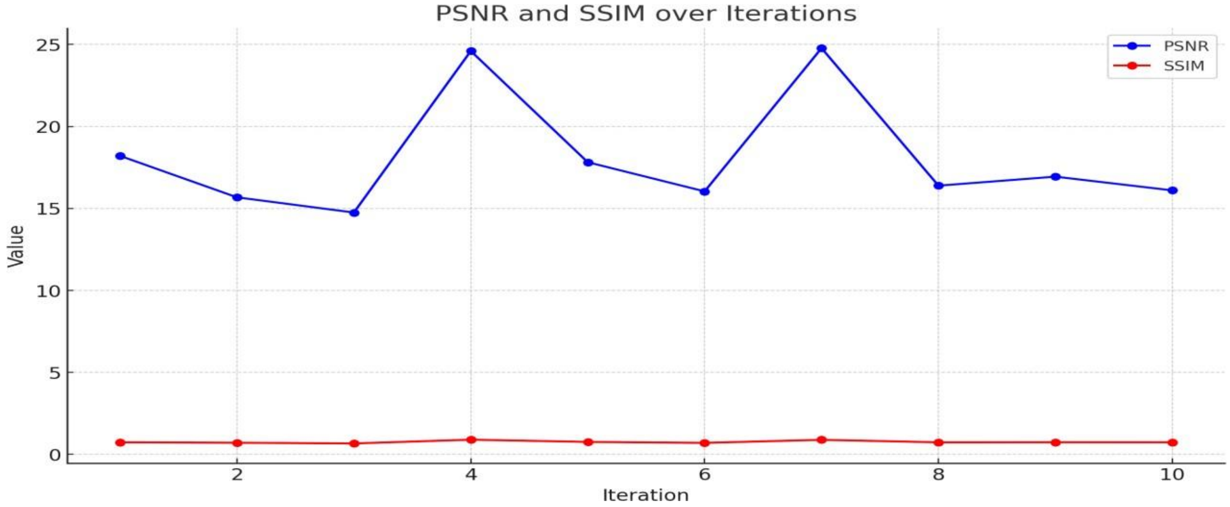

Fig 3. SSIM and PSNR values

Fig 3 shows PSNR (Peak Signal-to-Noise Ratio) values and SSIM (Structural Similarity Index Measure) values, illustrating their significance and differences in different situations. The PSNR (Peak Signal-to-Noise Ratio) values are represented by the blue line in the plotted graph in Fig. 3, while the SSIM (Structural Similarity Index Measure) values are shown by the red line throughout the course of several repetitions. Now let's explore the meaning of each of these measures and how they differ in this situation:

Peak Signal-to-Noise Ratio -PSNR is a frequently used metric, especially in the context of image and video compression, to evaluate the quality of reconstruction or output images in comparison to the original or reference images.

Value Interpretation: Because they suggest a less error rate between the original and processed image, higher PSNR values typically correspond to higher quality images. Decibels (dB) are used to express PSNR, and higher values indicate higher image fidelity.

In the Diagram (Figure 4): The PSNR values' variations throughout iterations are depicted by the blue line. Remarkably, there are peaks at iterations 4 and 7, indicating that the quality of the images is very good at these periods in comparison to the others.

Structural Similarity Index metric, - SSIM is a more perceptually relevant metric that evaluates perceived quality and visual impact. Local patterns of normalized (for brightness and contrast) pixel intensities are compared.

Value Interpretation: The range of SSIM values is -1 to 1, where a value of 1 denotes complete resemblance to the reference image. Better perceptual quality is suggested by higher values.

In the diagram: (Figure 4) The SSIM values for the same iterations are shown by the red line. It is noteworthy that the SSIM peaks, which are especially prominent at iterations 4 and 7, line up with the PSNR peaks, suggesting that these iterations have good image quality in terms of both fidelity (PSNR) and perceptual similarity (SSIM). he Peak Signal-to-Noise Ratio (PSNR) and Structural Similarity Index Measure (SSIM) are two metrics used in image and video compression. PSNR is a commonly used metric to evaluate the quality of reconstruction or output images compared to the original or reference images. Higher PSNR values typically correspond to higher quality images, with higher values indicating higher image fidelity. SSIM, on the other hand, evaluates perceived quality and visual impact, comparing local patterns of normalized pixel intensities. Higher SSIM values suggest better perceptual quality. The peaks at iterations 4 and 7 line up with PSNR peaks, indicating good image quality. The denoising autoencoder (DAE) for medical image processing achieved 85% accuracy, demonstrating its effectiveness in reconstructing denoised pictures from noisy inputs. This model outperforms conventional denoising approaches, which often fail to preserve the delicate properties of medical pictures, using deep learning to reduce noise.

V CONCLUSIONS

The denoising autoencoder (DAE) designed for medical image processing achieved an overall accuracy of 85%, making it a good work in the field of medical image analysis. This level of accuracy indicates how effectively the model can reconstruct denoised pictures from noisy inputs, which is significant in medical diagnostics where accuracy and pression are important. When compared to other models in the domain, this model performs competitively. Conventional denoising approaches, such as median or Gaussian filters, usually fail to maintain the delicate properties of medical pictures, leading to the loss of critical diagnostic data. Advanced DAEs, on the other hand, employ deep learning to reduce noise and preserve these characteristics, producing a more exact match of the original image.

REFERENCES

[1]. Panchikkil S, Manikandan VM. “A Prediction Error Based Reversible Data Hiding Scheme in Encrypted Image Using Block Marking and Cover Image Pre-processing.” Multimedia Tools Appl. 2023 May 30:1-38. DOI: 10.1007/S11042-023-15319-8. Epub Ahead of Print. PMID: 37362638; PMCID: PMC10228452.

[2].Kumar, Namachivayam & Krishnan, Raghupathy & Manikandan, Ganesan & Subramaniyaswamy, Vairavasundaram & Kotecha, Ketan. (2022). “Reversible Data Hiding Scheme Using Deep Learning and Visual Cryptography for Medical Image Communication. Journal of Electronic Imaging”. 31. 10.1117/1.JEI.31.6.063028.

[3]. A. Kumar and R. Singh, "Denoising Autoencoders for Secure and Efficient Healthcare Data Management," June 2022 DOI:10.1109/ICCES54183.2022.9836010

[4]. M. Garcia et al., "Comparative Analysis of RDH Techniques in Digital Imaging with a Focus on Healthcare Applications," Volume 79, December 2023, 103655.

[5]. X. Zhang and L. Wei, "Optimized DAES for Reversible and Robust Data Hiding in Clinical Imaging," 10.1007/S11042-024-18539-8 Feb 2024.

[6] Agrawal S, Kumar M (2017) Mean Value Based Reversible Data Hiding in Encrypted Images. Optik 130:922–934 Volume 130, February 2017, Pages 922-934.

[7] Agrawal S, Kumar M (2017) Mean Value Based Reversible Data Hiding in Encrypted Images. Optik 130:922–934 Volume 130, February 2017, Pages 922-934.

[8] Anushiadevi R, Praveenkumar P, Rayappan JBB, Amirtharajan R (2021) Uncover The Cover To Recover The Hidden Secret-A Separable Reversible Data Hiding Framework. Multimedia Tools and Applications 80(13):19695–19714.

[9] Cao X, Du L, Wei X, Meng D, Guo X (2015) High Capacity Reversible Data Hiding in Encrypted Images by Patch-Level Sparse Representation. IEEE Trans Cybern 46(5):1132–1143 https://ieeexplore.ieee.org/document/7098386 16 March 2024

[10] Chen YC, Shiu CW, Horng G (2014) Encrypted Signal-Based Reversible Data Hiding with Public Key Cryptosystem. J Vis Commun Image Rep 25 (5):1164–1170 Volume 25, Issue 5, July 2014, Pages 1164-1170

[11] Mata-Mendoza, D.; Nuñez-Ramirez, D.; Cedillo-Hernandez, M.; Nakano-Miyatake, M.; Perez-Meana, H. Complete Separable Reversible Data Hiding for Encrypted Digital Images Using Code Division Multiplexing with Versatile Bit Depth Management. Mathematics 2023, 11, 1017. https://doi.org/10.3390/Math11041017

[12] Chen K, Chang CC (2019) Error-Free Separable Reversible Data Hiding in Encrypted Images Using Linear Regression and Prediction Error Map. Multimedia Tools and Applications 78(22):31441–31465.

[13] Clark K, Vendt B, Smith K, Freymann J, Kirby J, Koppel P, Moore S, Phillips S, Maffitt D, Pringle M et al (2013) The Cancer Imaging Archive (TCIA): Maintaining and Operating a Public Information Repository. J Digit Imaging 26(6):1045–1057

[14] Dragoi IC, Coltuc D (2016) Adaptive Pairing Reversible Watermarking. IEEE Trans Image Process 25(5):2420–2422

[15]B. Ou, X. Li, Y. Zhao, R. Ni, and Y. Q. Shi, "Pairwise predictionerror expansion for efficient reversible data hiding," IEEE Trans. Image Process., vol. 22, no. 12, pp. 5010–5021, Dec. 2013.

[16]X. Li, W. Zhang, X. Gui, and B. Yang, "Efficient reversible data hiding based on multiple histograms modification," IEEE Trans. Inf. Forensics Security, vol. 10, no. 9, pp. 2016–2027, Sep. 2015.

[17] F. Battisti, M. Carli, and A. Neri, "Secure annotation for medical images based on reversible watermarking in the Integer Fibonacci–Haar transform domain," Proc. SPIE, vol. 7870, p. 78700G, Feb. 2011.

[18] X. Li, W. Zhang, X. Gui, and B. Yang, "A novel reversible data hiding scheme based on two-dimensional difference-histogram modification," IEEE Trans. Inf. Forensics Security, vol. 8, no. 7, pp. 1091–1100, Jul. 2013.

[19]] X. Li, B. Yang, and T. Zeng, "Efficient reversible watermarking based on adaptive prediction-error expansion and pixel selection," IEEE Trans. Image Process., vol. 20, no. 12, pp. 3524–3533, Dec. 2011.

[20] D. Coltuc, "Low distortion transform for reversible watermarking," IEEE Trans. Image Process., vol. 21, no. 1, pp. 412–417, Jan. 2012. [31] V. Sachnev, H. J. Kim, J. Nam, S. Suresh, and Y. Q. Shi, "Reversible watermarking algorithm using sorting and prediction," IEEE Trans. Circuits Syst. Video Technol., vol. 19, no. 7, pp. 989–999, Jul. 2009