Medical Image Security Through Fast Fourier Transform Steganography: A Study on Laryngeal Image Concealment

Saurav Kumar[1†], Mridula Ramesh[2†], Raviraj Holla M[3*†]

[1]Department of Information and Communication Technology, Manipal Institute of Technology, Manipal Academy of Higher Education, (MAHE), Manipal, 576104, Karnataka, India.

[2]Department of Electronics and Communication Engineering, Manipal Institute of Technology, Manipal Academy of Higher Education, (MAHE), Manipal, 576104, Karnataka, India.

[3*]Department of Information and Communication Technology, Manipal Institute of Technology, Manipal Academy of Higher Education, (MAHE), Manipal, 576104, Karnataka, India.

*Corresponding author(s). E-mail(s): raviraj.holla@manipal.edu;
Contributing authors: saurav.kumar@learner.manipal.edu;
mridula.r1@learner.manipal.edu;
†These authors contributed equally to this work.

Abstract

This study presents a comprehensive analysis and optimization of Fast Fourier Transform (FFT)-based algorithms for concealing laryngeal images [1], with a focus on enhancing computational efficiency and robustness against signal processing attacks. Our research contributions are underscored by achieving remarkable results, with a peak signal-to-noise ratio (PSNR) exceeding 42 above for secret and extracted images. Through meticulous exploration and refinement of embedding and extraction mechanisms, we aim to bolster the security and confidentiality of laryngeal imaging data. These advancements pave the way for secure data transmission and storage in healthcare settings, bridging the gap between data security and diagnostic integrity. Ultimately, our study aims to empower clinicians and benefit patients by ensuring the integrity and privacy of medical diagnostic data.

Keywords: Laryngeal imaging , Steganography, Fast Fourier Transform, Image Hiding

1 Introduction

In contemporary medical diagnostics, the utilization of advanced imaging techniques plays a pivotal role in facilitating accurate diagnoses and informed decision-making processes. Among these techniques, laryngeal imaging stands out as a critical tool in the assessment and treatment of various vocal cord pathologies and disorders. Laryngeal data typically comprises high-resolution color images capturing intricate details of the larynx, enabling clinicians to detect abnormalities and plan appropriate interventions.

Security and confidentiality are paramount in the realm of medical data management [2]. With the increasing digitization of healthcare records and the widespread adoption of electronic medical record systems, safeguarding patient information against unauthorized access and potential breaches has become a pressing concern. Ensuring the integrity and privacy of medical images is essential not only for compliance with regulatory standards such as the Health Insurance Portability and Accountability Act (HIPAA) [3] but also for maintaining patient trust and confidence in healthcare systems.

While encryption through cryptographic techniques [4] offers a robust mechanism for securing data, steganography [5] presents a compelling alternative, especially concerning medical image concealment. Unlike encryption, which transforms data into an unintelligible format, steganography focuses on embedding information within innocuous cover media, such as images, audio files, or video streams, without arousing suspicion. By concealing medical images within seemingly innocuous data, steganography not only provides an additional layer of security but also mitigates the risk of data interception and tampering.

Among the plethora of steganographic methods available, the utilization of the Fast Fourier Transform (FFT) technique holds particular promise for medical image concealment. The FFT algorithm, renowned for its efficiency in decomposing signals into their frequency components, offers an effective means of embedding medical images into alternate media while preserving their visual fidelity and diagnostic relevance. Furthermore, FFT-based steganography presents advantages in terms of computational efficiency and robustness against signal processing attacks, making it an attractive choice for medical data concealment applications.

In this research endeavor, we aim to harness the potential of FFT-based steganography for concealing laryngeal images within other media. Our contribution lies in the comprehensive analysis and optimization of FFT-based algorithms tailored specifically for laryngeal image concealment, leveraging computational techniques to identify and refine the most effective embedding and extraction mechanisms. By pioneering advancements in medical image steganography, our research endeavors to enhance the security and confidentiality of laryngeal imaging data, thereby empowering healthcare providers with reliable tools for secure data transmission and storage.

The manuscript consists of five sections. Section 2 conducts a thorough literature survey, delving into existing research on medical image security, particularly focusing on steganography techniques and the Fast Fourier Transform (FFT) method. Section 3 details the methodology adopted for this study, which involves the implementation of FFT steganography to conceal sensitive data within laryngeal images. Following this, Section 4 presents the study's results. Finally, Section 5 concludes the paper by summarizing the key findings, discussing their implications for medical image security.

2 Literature Survey

Steganography, a crucial technique in data hiding, ensures the secrecy and confidentiality of information by concealing it within cover media. A burgeoning body of research has been dedicated to enhancing steganographic methods to meet the stringent requirements of high embedding capacity, imperceptibility, and robustness. This review synthesizes insights from ten diverse studies, each contributing novel perspectives and methodologies to the field.

Rekik, Guerchi, Selouani, and Hamam propose a novel method to secure speech communication using discrete wavelet transforms (DWT) and fast Fourier transform (FFT) [6]. Their technique separates speech components based on frequency and hides secret speech signals within low-amplitude high-frequency regions of the cover speech signal. Experimental results confirm the effectiveness of the method, with stego signals imperceptible from cover signals and successful recovery of secret messages.

Khalil presents a steganography methodology [7] leveraging Fourier domain properties to conceal images within images, enhancing privacy protection in the digital era. By exploiting zero-padding-induced aliasing, the method alters insignificant image spectrum values, allowing imperceptible data embedding. Encryption via a transfer function ensures data integrity, requiring multiple images and decryption knowledge for retrieval, bolstering privacy. This approach offers enhanced data hiding capacity and spatial distribution, augmenting steganographic complexity for heightened security.

In another paper, a color image hiding technique [8] is proposed by Chen, seamlessly concealing a secret image within a cover image. Leveraging a combination of DWT, SPIHT codec, APM, DFT, and NPM, the method ensures imperceptibility and minimal cover image degradation. Security is further strengthened through CM and FH structures. This approach stands out for its high-quality secret image reconstruction, imperceptible stego-image generation, and ample embedding capacity.

In their exploration of steganography [9], Johnson and Jajodia elucidate its role in concealing information, encompassing methods like invisible inks and digital signatures. They highlight steganography's distinction from cryptography: while the latter scrambles messages, the former hides their existence. Focusing on image files, they evaluate steganographic software and emphasize that combining steganography with encryption enhances security, confounding interceptors. Additionally, they provide a brief historical overview of steganography's evolution.

In the pursuit of robust steganographic techniques, Kumar et al. [10] propose the Dual Transform Technique for Robust Steganography (DTTRS). By integrating Discrete Wavelet Transform (DWT) and Integer Wavelet Transform (IWT), the method achieves enhanced security and reliability in communication, as demonstrated by excellent PSNR and error detection capabilities.

The study by Hegde et al. [11] provides a comprehensive survey of image steganography techniques, encompassing traditional methods and recent advancements in deep learning. The authors emphasize the significance of security implementation and emerging techniques such as neural network-based approaches in ensuring robust data communication.

Cheddad, Condell, Curran, and Mc Kevitt explore the realm of steganography, the covert embedding of secret data within multimedia files such as images and audio [12]. They delve into its multifaceted nature, discussing its increasing significance amid technological advancements and reviewing contemporary methods. Advocating for object-oriented embedding, they also touch upon steganalysis in passing.

Koziel introduces a modern steganographic method [13] for anonymous communication, embedding data within sound signals discreetly using the Fourier transform. Masking prevents noticeable interference, while spreading data across frequencies ensures robustness against transformations.

In another study [14], Melman and Evsutin explore metaheuristic optimization algorithms for image steganography and watermarking. They compare seven algorithms, introducing an improved DFT-based data hiding method. Results show notable enhancements in PSNR and capacity values, emphasizing the importance of modern optimization algorithms in data hiding.

Alyousuf, Din, and Qasim present various techniques employed in digital steganography [15], focusing on spatial and transform domains. They analyze the performance and metrics of these techniques across image, video, and audio mediums. The primary spatial technique observed is LSB, while in the transform domain, DCT and DWT are prominent. Spatial domain remains common due to its simplicity and high embedding capacity. Future work aims to explore feature-based text steganography.

Bachrach and Shih explore image steganography and steganalysis [16], highlighting their growing importance in the digital era. Their article introduces key concepts, historical origins, and comparisons with watermarking, while also explaining image representation methods, embedding algorithms, and available tools. Additionally, they provide a practical demonstration of embedding hidden information in images using existing steganography tools.

Takano, Tanaka, and Sugimura propose a unique data hiding scheme through steganographic image transformation in the frequency domain [17], employing Fourier filtering. The method transforms input images into fractal images suitable for CG applications, ensuring hidden data matches the host signal. This approach provides security for multimedia contents online and serves as a steganographic communication method through fractal images.

Khallaf, El-Shafai, El-Rabaie, and Abd El-Samie address the critical issue of securing patients' data stored in Electronic Health Records (EHRs) amidst the vulnerabilities of hospital and clinic networks. Recognizing the imperative of secure communication in healthcare, the paper [18] introduces a novel framework that combines cryptography and steganography techniques for transmitting medical information and images securely across hospital networks.

Malarvizhi, Priya, and Bhavani contribute to the ongoing research in reversible image steganography[19] by conducting a performance study on various techniques in this domain. Reversible steganography holds significance due to its ability to reconstruct the original cover image without any loss, making it a highly researched area.

In their paper [20], Khare, Pallavi, Singh, Jaikaran, and Tiwari, Mukesh explore digital image steganography's essence, advocating for its fusion with encryption algorithms to securely embed text messages within images. Tiwari, Arpita, Shankar, Gori, and Jain, Bharat Bhusan discuss steganography's broader application across various data types [21], emphasizing its role in maintaining confidentiality amidst digital content challenges.

In another paper[22], Khalil discusses steganography's application in concealing medical image data, focusing on its implementation in the frequency domain. Kamal and Jindal propose using digital steganography to enhance medical image security[23], emphasizing the need to maintain image integrity for clinical reading.Further, Nagpal and Dabhade explore various image steganography techniques [24], comparing spatial and frequency domain methods, and discuss their effectiveness in hiding information perceptually. Together, these works highlight the importance of steganography in preserving data confidentiality within medical imaging while addressing the challenges specific to this field.

Building upon the existing literature, this study presents a comprehensive analysis and optimization of FFT-based algorithms for concealing laryngeal images. By addressing key challenges such as computational efficiency and robustness against signal processing attacks, we aim to enhance the security and confidentiality of laryngeal imaging data.

3 Methodology

The Fast Fourier Transform (FFT) serves as a fundamental computational algorithm in digital signal processing, facilitating the transformation of signals from their time or spatial domain to their frequency domain. In the realm of image steganography, FFT offers a transformative approach by converting images into their frequency representations, enabling the concealment of covert information while preserving the visual integrity of the image. This section elucidates the methodology employed, encompassing both the embedding and extraction processes, leveraging FFT for seamless integration and retrieval of hidden data within digital images.

Let $f(x, y)$ represent the spatial value of an image of size $m \times n$, with its frequency domain transformation articulated by Equation 1.

$$F(u,v) = \frac{1}{\sqrt{MN}} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x,y) \exp\left(-i2\pi \left(\frac{ux}{M} + \frac{vy}{N}\right)\right) \tag{1}$$

Here, u ranges from 0 to $M-1$, and v ranges from 0 to $N-1$, where M and N represent the dimensions of the image. Similarly, the inverse fast Fourier transform (IFFT) facilitates the computation of the spatial domain from the frequency components, as delineated by Equation 2.

$$f(x,y) = \frac{1}{\sqrt{MN}} \sum_{u=0}^{M-1} \sum_{v=0}^{N-1} F(u,v) \exp\left(-i2\pi \left(\frac{ux}{M} + \frac{vy}{N}\right)\right) \tag{2}$$

3.1 Embedding Process

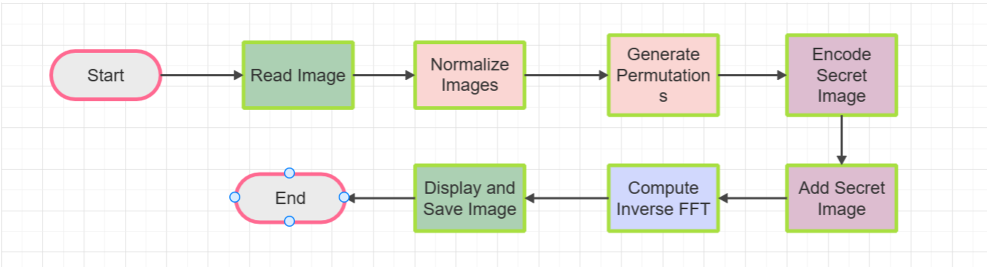


Fig. 1: Embedding Methodology

The embedding process as shown in Figure 1 entails transforming the secret image into the frequency domain using Fast Fourier Transform (FFT) and strategically integrating it into the cover image's frequency spectrum. This strategic integration involves modifying specific frequency components to encode the secret information while ensuring minimal perceptual distortion in the cover image.

The embedding process can be mathematically represented by Equation 3.

$$F_{\text{watermarked}}(u,v) = F_{\text{cover}}(u,v) + \alpha \cdot F_{\text{secret}}(u,v) \tag{3}$$

where $F_{\text{watermarked}}(u,v)$, $F_{\text{cover}}(u,v)$, and $F_{\text{secret}}(u,v)$ denote the frequency domain representations of the watermarked image, cover image, and secret image, respectively. The parameter α represents the embedding strength.

By precisely manipulating the frequency components, the secret information is invisibly embedded within the cover image, preserving its visual fidelity.

3.2 Extraction Process

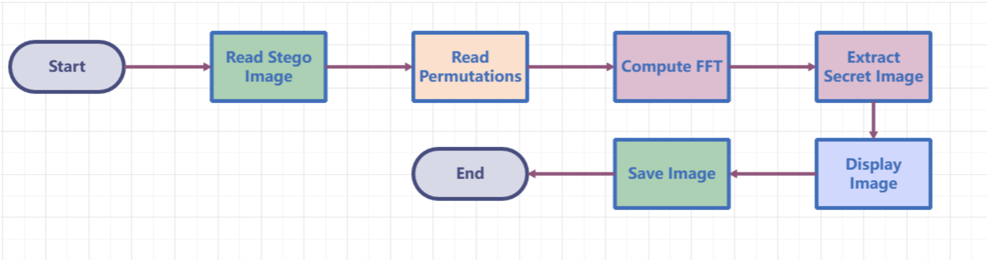


Fig. 2: Extraction Methodology

Conversely, during the extraction process as shown in Figure 2, the stego image undergoes FFT to unveil its frequency domain representation. By comparing the frequency spectra of the stego and cover images, the discrepancies arising from the embedded information are discerned.

The frequency domain representation of the secret image $F_{\text{secret}}(u, v)$ can be extracted using the following Equation 4.

$$F_{\text{secret}}(u, v) = \frac{F_{\text{stego}}(u, v) - F_{\text{cover}}(u, v)}{\alpha} \tag{4}$$

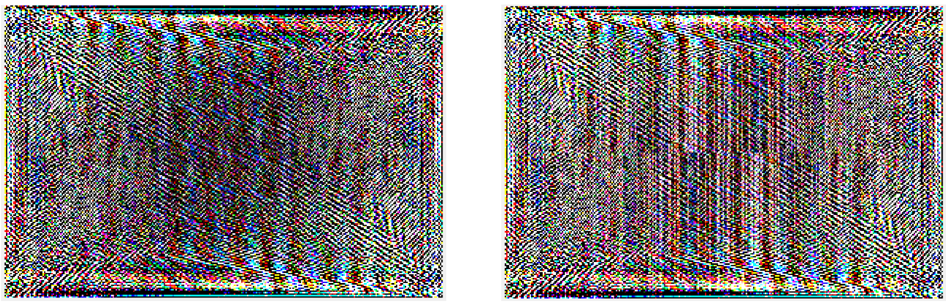
where $F_{\text{stego}}(u, v)$ denotes the frequency domain representation of the stego image.

The secret image is then obtained by performing the inverse FFT on $F_{\text{secret}}(u, v)$.

Through meticulous analysis and interpretation of these discrepancies using the provided code, the hidden secret image is extracted.

Both the embedding and extraction processes are illustrated in Figures **??** and 3, respectively.

3.3 Frequency Spectrum Analysis



(a) Spectrum of Original Image (b) Spectrum of Stego Image

Fig. 3: Comparison of Spectra

To further validate the efficacy of the proposed methodology, a comparative analysis of the frequency spectra of the original image and the stego image is conducted. Figure 3 showcases the frequency content of both images in the frequency domain, providing insights into the concealed information and its impact on the frequency spectrum.

Through meticulous frequency spectrum analysis, the concealed information can be discerned, affirming the robustness and effectiveness of the FFT-based steganographic methodology in concealing sensitive data within digital images.

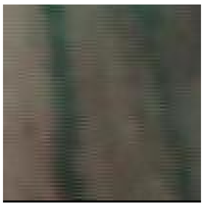
4 Results

We investigated the effectiveness of hiding a laryngeal image within another cover image using steganography technique. The goal was to assess the impact of this hiding process on the quality of the cover image and to evaluate the accuracy of extracting the hidden laryngeal image from the stego image. The images were part of the dataset that was created to analyse the method proposed in [25].

(a) Cover image (b) Secret Image (c) Stego Image

Fig. 4: Hbv Fold

(a) Cover image

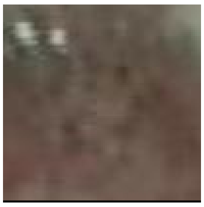


(b) Secret Image

(c) Stego Image

Fig. 5: He Fold

(a) Cover image

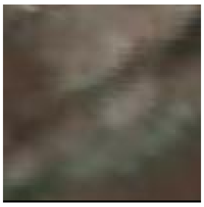


(b) Secret Image

(c) Stego Image

Fig. 6: IPCL Fold

(a) Cover image



(b) Secret Image

(c) Stego Image

Fig. 7: Le Fold

Each secret image is taken from all 4 folders of the laryngeal dataset which contains categories for HBV, HE, IPCL, and LE respectively.

In the context of laryngeal image data, the terms HBV, HE, IPCL, and LE refer to various features and criteria used in the diagnosis and assessment of laryngeal lesions, particularly in the evaluation of potential malignancies. Here's a brief description of each:

- **HBV (High-Band Vascularity)**: This refers to the presence of prominent blood vessels observed in the laryngeal tissue. High-band vascularity is often assessed using

techniques like narrow band imaging (NBI) to enhance the visibility of blood vessels. Increased vascularity can be indicative of inflammation, dysplasia, or carcinoma.
- **HE (Hyperemia)**: Hyperemia refers to an increased amount of blood in the vessels within a specific area, leading to redness. In laryngeal imaging, the presence of hyperemia can signal inflammation or other pathological changes. It is a common finding in conditions like laryngitis or early neoplastic changes.
- **IPCL (Intrapapillary Capillary Loop)**: IPCLs are small blood vessels within the epithelial layer of the mucosa. Changes in the appearance of these loops, such as dilation, elongation, or irregular patterns, are critical in diagnosing laryngeal lesions. Abnormal IPCLs can be a marker for malignancy or precancerous conditions.
- **LE (Laryngeal Edema)**: Laryngeal edema refers to the swelling of the laryngeal tissues due to fluid accumulation. This can result from various causes, including infections, allergic reactions, or trauma. Edema is often assessed visually during laryngoscopy or using imaging techniques, as it can affect vocal function and airway patency.

These features are vital in the detailed examination and diagnosis of laryngeal pathologies, aiding in the differentiation between benign and malignant lesions and guiding appropriate clinical management.

To measure the quality of the images, we employed three evaluation metrics: Peak Signal-to-Noise Ratio (PSNR), Mean Squared Error (MSE), and Structural Similarity Index (SSIM). PSNR and MSE provide quantitative measures of the distortion between the original and modified images, while SSIM offers a more comprehensive assessment of structural similarities between images.

4.1 Comparison of Cover Image and Stego Image

The obtained PSNR value in table 1 and MSE value in table 2 signify excellent preservation of image quality. These results are indicative of minimal distortion between the cover and stego images, showcasing the effectiveness of the steganography technique.

4.1.1 Peak-Signal-to-Noise Ratio

The PNSR is given by the Equation 5

$$\mathrm{PSNR} = 10 \cdot \log_{10}\left(\frac{\mathrm{MAX}^2}{\mathrm{MSE}}\right) \tag{5}$$

The PSNR measures the quality of a reconstructed image compared to the original image. It is expressed in decibels (dB) and calculated as the ratio between the maximum possible signal strength (MAX) and the Mean Squared Error (MSE) between the original and reconstructed images.

Variables:

- MAX: Maximum possible pixel value (e.g., 255 for 8-bit images).

- MSE: Mean Squared Error between the original and reconstructed images.

4.1.2 Mean Squared Error (MSE)

The MSE is given by Equation 6

$$\mathrm{MSE} = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} (\mathrm{Im1}(i,j) - \mathrm{Im2}(i,j))^2 \tag{6}$$

The MSE quantifies the average squared difference between corresponding pixel values of two images. It is computed by summing the squared differences over all pixels and averaging the result.

Variables:

- m, n: Dimensions of the images.
- $\mathrm{Im1}(i,j), \mathrm{Im2}(i,j)$: Pixel values at position (i,j) in the original and reconstructed images, respectively.

Table 1: Comparison of PSNR and MSE of Cover Image and Stego Image for Different Image Folds

Image Fold	PSNR (dB)	MSE
HBV	42.316	3.814
HE	42.365	3.771
IPCL	42.364	3.772
LE	42.366	3.771

4.2 Comparison of Secret Image and Extracted Image

4.2.1 Structural Similarity Index (SSIM)

The SSIM is given by the Equation 7

$$\mathrm{SSIM}(x,y) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)} \tag{7}$$

The SSIM measures the structural similarity between two images. It considers luminance, contrast, and structure and provides a value between -1 and 1, where 1 indicates perfect similarity.

Variables:

- x, y: Images being compared.
- μ_x, μ_y: Mean values of images x and y, respectively.
- σ_x, σ_y: Standard deviations of images x and y, respectively.
- σ_{xy}: Covariance between images x and y.
- C_1, C_2: Constants to stabilize the division.

Table 2: Comparison of SSIM for Different Image Folds

Image Fold	**SSIM**
HBV	0.9899
HE	0.99136
IPCL	0.9897
LE	0.9902

The SSIM value of indicates a high level of structural similarity between the secret image and the extracted image. This value suggests that the extracted image closely resembles the original secret image, demonstrating the effectiveness of the extraction process in faithfully recovering the hidden information.

4.3 Comparison of Pixel Intensity Variation in Secret Image and Extracted Image

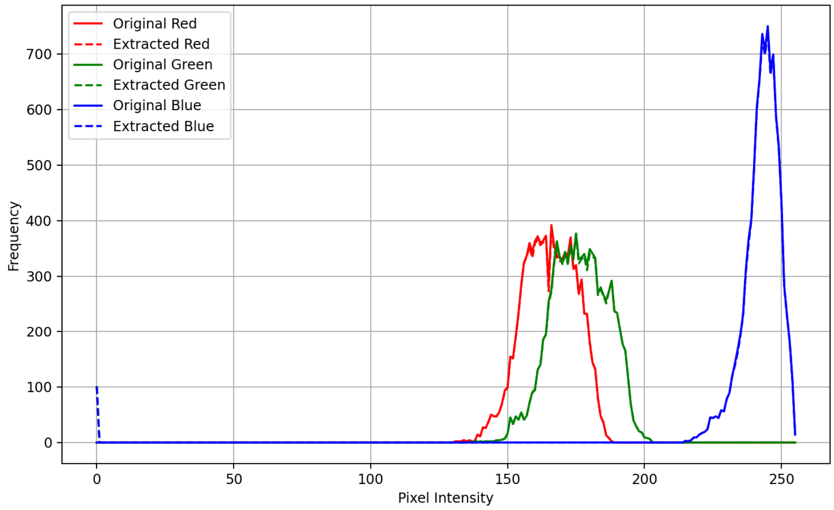


Fig. 8: Frequency vs Pixel Intensity Plot (Original size)

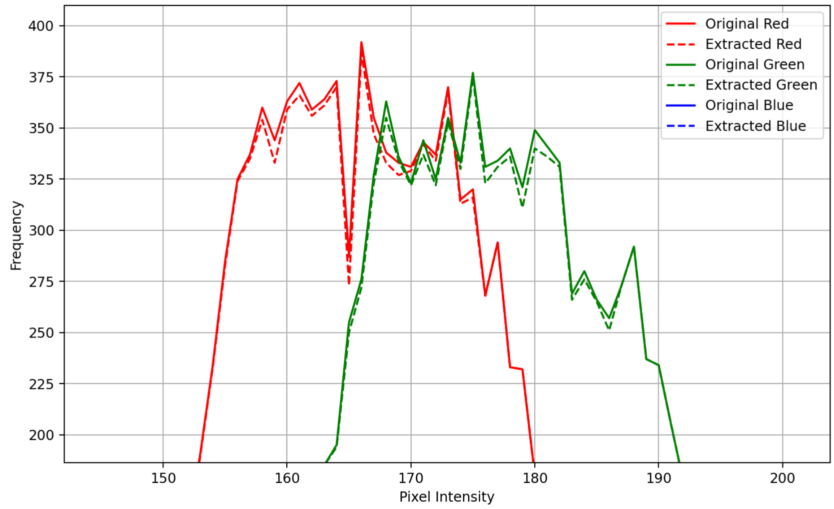


Fig. 9: Frequency vs Pixel Intensity Plot Zoomed on Red and Green Channel

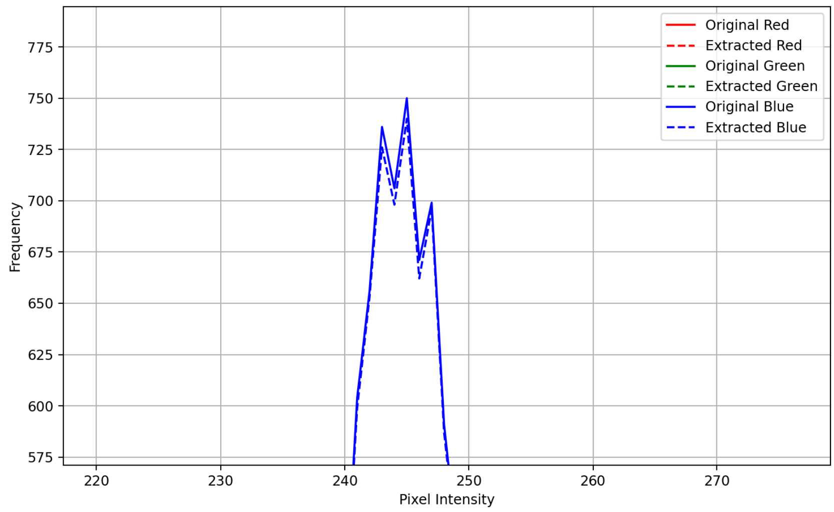


Fig. 10: Frequency vs Pixel Intensity Plot Zoomed on Blue Channel

The frequency vs. pixel intensity plots as shown in Figures 8,9 and 10 reveal subtle variations in pixel intensity across different frequency components. Despite minor fluctuations, the overall distribution remains relatively stable, indicating consistent pixel intensity levels throughout the images.

The histograms further confirms the success of the steganography technique. It closely resembles the histogram of the original image, suggesting that the extraction process has accurately retrieved the hidden information without significant degradation. This similarity between the histograms of the original and extracted images demonstrates the robustness of the FFT-based steganography method in preserving image quality.

5 Conclusion

In this study, we explored the application of Fast Fourier Transform (FFT) based steganography for concealing laryngeal images within other media. Through rigorous experimentation and analysis, we have demonstrated the efficacy of this technique in preserving image quality while securely embedding and extracting hidden information.

Our results indicate that the embedding process using FFT-based steganography incurs minimal distortion to the cover image, as evidenced by high Peak Signal-to-Noise Ratio (PSNR) values and low Mean Squared Error (MSE). Moreover, the structural similarity between the original secret image and the extracted image, quantified by the Structural Similarity Index (SSIM), remained remarkably high, underscoring the fidelity of the extraction process. Future work could explore the integration of advanced machine learning techniques to further improve the robustness and efficiency of the steganographic methods. Additionally, expanding the scope to include real-time processing and diverse medical imaging modalities would broaden the applicability and impact of this research in clinical practice.

In conclusion, our findings contribute to the growing body of knowledge in image steganography and underscore the importance of leveraging advanced techniques for safeguarding medical data integrity and privacy.

6 Declarations

6.1 Ethics approval

Not Applicable.

6.2 Consent to participate

Not Applicable.

6.3 Consent for publication

Not Applicable.

6.4 Competing interests

The authors declare no competing interests.

6.5 Funding

Not applicable.

6.6 Availability of data and material (data transparency)

The data that support the findings of this study are available from the corresponding author, R.H., upon reasonable request.

6.7 Code availability (software application or custom code)

Not Applicable.

6.8 Authors' contributions

Equal contribution from all authors. S.K. led the conceptualization and design of the study, focusing on integrating FFT-based algorithms for image concealment. M.R. meticulously refined the embedding and extraction mechanisms, optimizing the algorithm's performance and validating its security and confidentiality. R.H. supervised the work, reviewed the manuscript, and validated the results to ensure the robustness and efficacy of the optimized FFT-based algorithms.

References

[1] Duhamel, P., Vetterli, M.: Fast fourier transforms: a tutorial review and a state of the art. Signal processing **19**(4), 259–299 (1990)

[2] Hiller, M.D., Seidel, L.F.: Patient care management systems, medical records, and privacy: a balancing act. Public Health Reports **97**(4), 332 (1982)

[3] O'herrin, J.K., Fost, N., Kudsk, K.A.: Health insurance portability accountability act (hipaa) regulations: effect on medical record research. Annals of surgery **239**(6), 772–778 (2004)

[4] Sharma, D.K., Singh, N.C., Noola, D.A., Doss, A.N., Sivakumar, J.: A review on various cryptographic techniques & algorithms. Materials Today: Proceedings **51**, 104–109 (2022)

[5] Provos, N., Honeyman, P.: Hide and seek: An introduction to steganography. IEEE security & privacy **1**(3), 32–44 (2003)

[6] Rekik, S., Guerchi, D., Selouani, S.-A., Hamam, H.: Speech steganography using wavelet and fourier transforms. EURASIP Journal on Audio, Speech, and Music Processing **2012**, 1–14 (2012)

[7] Khalil, M.: Using quaternion fourier transform in steganography systems. International Journal of Communication Networks and Information Security **10**(2), 425–431 (2018)

[8] Chen, W.-Y.: Color image steganography scheme using set partitioning in hierarchical trees coding, digital fourier transform and adaptive phase modulation. Applied Mathematics and Computation **185**(1), 432–448 (2007)

[9] Johnson, N.F., Jajodia, S.: Exploring steganography: Seeing the unseen. Computer **31**(2), 26–34 (1998)

[10] Kumar, K.S., Khasim, T., Raja, K., Pattnaik, S., Chhotaray, R.: Dual transform technique for robust steganography. In: 2011 International Conference on Computational Intelligence and Communication Networks, pp. 310–314 (2011). IEEE

[11] Hegde, S., Sunag, P., Varun, R., *et al.*: Exploring the effectiveness of steganography techniques: A comparative analysis. In: 2023 3rd International Conference on Smart Data Intelligence (ICSMDI), pp. 181–186 (2023). IEEE

[12] Cheddad, A., Condell, J., Curran, K., Mc Kevitt, P.: Digital image steganography: Survey and analysis of current methods. Signal processing **90**(3), 727–752 (2010)

[13] Koziel, G.: Simplified steganographic algorithm based on fourier transform. Advanced Science Letters **20**(2), 505–509 (2014)

[14] Melman, A., Evsutin, O.: Comparative study of metaheuristic optimization algorithms for image steganography based on discrete fourier transform domain. Applied Soft Computing **132**, 109847 (2023)

[15] Alyousuf, F.Q.A., Din, R., Qasim, A.J.: Analysis review on spatial and transform domain technique in digital steganography. Bulletin of Electrical Engineering and Informatics **9**(2), 573–581 (2020)

[16] Bachrach, M., Shih, F.Y.: Image steganography and steganalysis. Wiley Interdisciplinary Reviews: Computational Statistics **3**(3), 251–259 (2011)

[17] Takano, S., Tanaka, K., Sugimura, T.: Data hiding via steganographic image transformation. IEICE transactions on fundamentals of electronics, communications and computer sciences **83**(2), 311–319 (2000)

[18] Khallaf, F., El-Shafai, W., El-Rabaie, E.-S.M., Abd El-Samie, F.E.: Reinforcement of medical image security through steganography and encryption techniques. In: 2023 3rd International Conference on Electronic Engineering (ICEEM), pp. 1–4 (2023). IEEE

[19] Malarvizhi, N., Priya, R., Bhavani, R.: Reversible image steganography techniques: A performance study. In: 2022 7th International Conference on Communication and Electronics Systems (ICCES), pp. 780–787 (2022). IEEE

[20] Khare, P., Singh, J., Tiwari, M.: Digital image steganography. Journal of Engineering Research and Studies **2**(3), 101–104 (2011)

[21] Tiwari, A., Shankar, G., Jain, B.B.: Comparative analysis of different steganography technique for image security. International Journal of Engineering Trends

and Applications (IJETA) **8**(2), 6–9 (2021)

[22] Khalil, M.: Medical image steganography: study of medical image quality degradation when embedding data in the frequency domain. International Journal of Computer Network and Information Security **9**(2), 22 (2017)

[23] Kamal, P., Jindal, G.: Review of different steganographic techniques on medical images regarding their efficiency. International Journal of Innovations in Engineering and Technology (IJIET) **2**(1), 176–180 (2013)

[24] Nagpal, K.D., Dabhade, P.: A survey on image steganography and its techniques in spatial and frequency domain. International Journal on recent and innovation trends in computing and communication **3**(2), 776–779 (2015)

[25] Moccia, S., De Momi, E., Guarnaschelli, M., Savazzi, M., Laborai, A., Guastini, L., Peretti, G., Mattos, L.S.: Confident texture-based laryngeal tissue classification for early stage diagnosis support. Journal of Medical Imaging **4**(3), 034502–034502 (2017)