Journal of Electronics and Communication Engineering and Technology (JECET)
Volume 6, Issue 1, January-June 2025, pp. 1-23, Article ID: JECET_06_01_001
Available online at https://iaeme.com/Home/issue/JECET?Volume=6&Issue=1
ISSN Print: 2347-4181; ISSN Online: 2347-419X; Journal ID: 9981-3065
DOI: https://doi.org/10.34218/JECET_06_01_001

EFFICIENT HEALTH DATA TRANSMISSION SYSTEM BASED ON STEGANOGRAPHY USING HYBRID DOMAIN TECHNIQUE

Sangeetha N[1], Harshith K Raj[2], K B Raja[3]

[1]Department of ECE, Dr. Ambedkar Institute of Technology, Bengaluru, India,
[2]Department of CSE, JSS Academy of Technical Education, Bengaluru, India,
[3]University Visvesvaraya College of Engineering, Bangalore University, Bengaluru, India,

ABSTRACT

The data embedding technique maintains the integrity of the original image while reducing the possibility that unauthorized parties may find the secret image. This paper proposes an Efficient Health Data Transmission System based on Steganography using the Hybrid Domain Technique. The cover and secret images are transformed into low (LL band)- and high-frequency coefficients (LH, HL, and HH) using the Discrete Wavelet Transform (DWT) transform. This allows compression and noise reduction by considering LL coefficients for adequate data concealment. The encoded data is compressed and secured using the Singular Value Decomposition (SVD) on the LL bands of cover and secret images. The stego key: singular values of cover S_c, α, and attention_weight are embedded into the HL of the cover image using the Least Significant Bits (LSB) technique to obtain HL_new. The IDWT is used to derive spatial domain stegoimage. The secret image is extracted from the stegoimage using the reverse embedding process at the destination. The experimental result shows good imperceptibility of stegoimage with a PSNR of 71.48 dB and better robustness with an SSIM of 0.9990 for the proposed steganographic scheme with 33.2% capacity.

Keywords: DWT, Hybrid domain, LSB, Steganography, SVD.

Cite this Article: Sangeetha N, Harshith K Raj, K B Raja. Efficient Health Data Transmission System Based on Steganography Using Hybrid Domain Technique. *Journal of Electronics and Communication Engineering and Technology (JECET)*, 6(1), 2025, 1-23.

https://iaeme.com/MasterAdmin/Journal_uploads/JECET/VOLUME_6_ISSUE_1/JECET_06_01_001.pdf

1. INTRODUCTION

Data hiding is a crucial method for protecting data and resolving security issues. A significant area of data concealment is steganography, which is further subdivided by various carriers into image steganography [1], audio steganography [2] is the study of concealing data in sound, and video steganography [3] is embedding data in a video file. Image steganography aims to safely hide sensitive information in cover photos sent over public channels [4]. The benefits of modern digital media are exploited by image steganography; multimedia objects frequently have highly redundant representations that allow for a significantly large payload with only minor changes that maintain the perceptual content of the underlying cover image [5].

Medical data security in transit and storage should be integral to any innovative global health technology. Current technology improvements make it challenging to protect sensitive healthcare data. Protecting patient privacy and medical content is one of the most significant issues with medical information security. As the availability of medical information increases, algorithms need to incorporate security measures. Experts recently established image steganography as an extra data security safeguard for health records to Protect confidentiality and integrity. Electronic Medical Images (EMI) and patient records are electronic healthcare digital images that vary in dimensions. EMI can be of many types, such as X-ray [6], Magnetic Resonance Imaging **(**MRI) [7], and Computed Tomography (CT) Scan [8]. EMIs are valued and crucial for patients as they are used for future diagnoses. The recent year has witnessed a mass increase in attacks and threats to EMI; thus there is a rise in concern for the security of EMI.

The issues in steganographic systems are imperceptibility, robustness, capacity, and security [9]. (i) Imperceptibility: The carrier should display no properties that flag it as suspicious, whether to the human visual/auditory system or in increased file size for the carrier file. i.e., the cover data should not be significantly degraded by the embedded data. (ii)

Robustness: The embedded data should be immune to modifications from intelligent attacks. (iii) Capacity: Ideally, we want large capacity, but that would affect Imperceptibility and robustness. Hence, a compromise needs to be made between these three. (iv) Security: the inability of an adversary to detect hidden images accessible only to the authorized user.

Contribution: An efficient health data transmission system based on steganography using a hybrid domain technique is proposed. A DWT, SVD, and LSB-based image steganography system is developed to embed secret data into a cover to create a stegoimage that is invisible to the naked eye. The image is converted into low and high-frequency components using DWT, enabling selective editing. In order to make the image less susceptible to attacks and maintain the quality of the cover image, SVD converts LL band coefficients into a series of singular values, which aids in robustly embedding the data.

2. LITERATURE SURVEY

Subramanian et al., [10] examined and discussed the many deep-learning techniques utilized in image steganography. Three general categories can be used to classify deep learning approaches for image steganography: conventional methods, Convolutional techniques based on general adversarial networks and neural networks. The technique provides an in-depth synopsis of the datasets used, experimental setups considered, and assessment measures frequently employed. Abed et al. [11] suggested that the approach consists of three primary stages (preprocessing, embedding, and extracting), each with a distinct procedure. The Pixels Variance (PV) method, the eight neighbors method, and the Huffman coding algorithm are recommended as safe image steganography techniques to address the imperceptibility and capacity difficulties. It uses a new image partitioning with a Henon map to boost the security portion. This approach used various standard photos, including SIPI datasets and medical images.

Farhan Rafat and Muhammad Sajjad [12] designed a safe, reversible steganography algorithm based on the Least Significant Bit (LSB) technique, which is essential to achieving these high-security goals. Techniques to guarantee the confidentiality and integrity of transmitted data are required due to the growing demand for secure communication across public networks. Reversible steganographic techniques, distinguished by their capacity to preserve the original image and embedded data, are especially pertinent in fields where the inherent worth of the original image cannot be replaced, such as satellite and medical imaging.

To prevent unwanted access or manipulation, it is essential to maintain the security of the embedded data. Consequently, secure reversible image Steganography techniques in the spatial realm are crucial for strengthening sensitive data protection while maintaining the original image's purity and confidentiality. Accordingly, examining Kerckhoff's principle, which emphasizes that system security depends on the key's confidentiality rather than the algorithm, becomes important for guaranteeing strong security procedures. Ye et al., [13] presented a deep learning-based approach that automatically learns embedding probabilities by combining picture residuals, residual distances, and image local variance. Three essential guiding elements and an embedding probability generator are part of our framework: Residual guidance aims to simplify embedding in areas with complicated textures. Residual distance guidance aims to reduce the remaining variations between stego and cover images. Local variation guidance efficiently protects against changes in areas with simple or homogeneous textures. Together, the three elements direct the learning process and improve security performance. Ramadhan et al., [14] introduced a steganographic method for embedding bits of private information in photos by using tailored variations between nearby pixels. This method's outcomes are obtained by representing the secret data from a widely used dataset with general-purpose graphics and randomly generated bits.

Wahono et al., [15] presented a steganography-based data-hiding technique that uses neighboring pixel-based difference expansion within a digital image to increase the confidentiality of the hidden information. Al-Jarah and Ortega-Arjona [16] described how to use a hashing function on the secret data and insert a secret key steganography to conceal information inside an image. The SHA 256 function ensures that data arrives unaltered by detecting flaws. The suggested algorithm raises the security level by including a robustness parameter (secret key and hash function) and developing a novel insertion technique. Compared to LSB, it doubles the cover-image capacity to conceal a secret message inside a color image, which helps protect sensitive, pertinent, and significant data. Shmueli et al., [17] suggested a technique for spatial picture steganography. The technique embeds the secret data into RGB images without causing noticeable distortion and is based on LSB substitution. The technique defines the image's saliency map using an energy function. A cumulative maximum energy matrix is generated from the saliency image. The secret message is embedded along the maximum energy horizontal seams chosen from the cumulative matrix.

Naveen and Jayaraghavi [18] suggested concealing text, images, and other types of data using a combination of genetic algorithms (GA) and least significant bits (LSB) to communicate all hidden data. Furthermore, embedding many color images inside a single image demonstrates

the ability to store more hidden data. Additionally, the use of GA guarantees enhanced security. The quality of the stego picture and retrieved images is assessed using the Bit Error Rate (BER), Correlation coefficient, Structural Similarity Index Metric (SSIM), and Peak Signal to Noise Ratio (PSNR). Chiu and Lin [19] suggested a coverless image steganography based on the sequence mapping of Scale-Invariant Feature Transform (SIFT) and Discrete Wavelet Transform (DWT), which reduces the number of images needed by adopting a dual method for feature sequence generation, thereby increasing sequence diversity. Furthermore, providing the composite stego-image greatly improves security by avoiding the suspicion that comes with sending the encrypted auxiliary information. Partha Chowdhuri et al., [20] suggested two schemes, such as SVM, to distinguish between the Region of Interest (ROI) and Non-Region of Interest (NROI) in the medical image. IWT is then used to embed secret information within the medical image's NROI portion (Cover Image). A circular array and a shared secret key are applied to increase the suggested scheme's robustness.

Ramapriya and Kalpana [21] suggested image encryption techniques and medical picture steganography procedures that capitalize on the Dual Tree-Complex Wavelet Transform. An enhanced SSOA optimization technique is then used to identify smooth edge blocks. Consequently, choosing pixels for embedding is much easier. Following that, a double matrix XOR encoding embeds the Secret data into the cover image. Following the process of embedding, the stego image is created. To create the Stego Compressed image, the Stego output image is further compressed using Huffman Coding. Compressing the stego image quickly sends secret data over a wireless network. Ramyashree et al., [22] examined the difficulties of securely integrating messages into medical images utilizing the Least Significant Bit (LSB) and Discrete Cosine Transform (DCT) steganographic techniques. LSB-based steganography is becoming increasingly common in concealing sensitive information in the LSBs of pixel values without creating any noticeable distortion. By embedding the data and changing the image's structure, the Discrete Cosine Transform procedure increases the robustness of the data. Using performance metrics, the study contrasted the DCT and LSB steganography techniques.

3. BACKGROUND

The techniques used in our proposed method are discussed in detail

3.1 Discrete Wavelet Transform (DWT)

A potent method for transforming spatial domain photos into frequency domain [23, 24], it uses low and high pass filters with decimation by two to create low and high-frequency coefficients. Applying the DWT on an image yields the low- and high-frequency coefficient bands. Four equal-sized bands comprise the frequency domain, including one low-frequency band and three high-frequency bands. Its low-frequency band contains the important information of the original face image. The three high-frequency bands corresponding to the original face image's horizontal, vertical, and diagonal edges contain the unimportant edge data. Our approach considers low-frequency band coefficients by leaving out high-frequency band coefficients, leading to low-dimensional final features for fast calculation. The secret image and the cover image data are transformed using Haar filters based DWT, and then, the secret image DWT coefficients are embedded to the cover image DWT coefficients. The coefficients of the high-frequency bands, namely Low-High (LH), High-Low (HL), and High-High (HH), and the low-frequency band, Low-Low (LL), are obtained using equations 1–5 for the 2X2 image matrix.

$$X = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \text{----------(1)}$$

$$LL = \frac{a+b+c+d}{2} \text{----------=----------(2)}$$

$$LH = \frac{a+b-c-d}{2} \text{----------(3)}$$

$$HL = \frac{a-b+c-d}{2} \text{----------(4)}$$

$$HH = \frac{a-b-c+d}{2} \text{----------(5)}$$

Where a, b, c, and d are the coefficients of the 2X2 matrix.

The DWT is applied to the MRI cover image, yielding a low-frequency LL band and high-frequency LH, HL, and HH bands, as shown in Figure 1. The figure shows that significant information is available in the LL band, whereas insignificant information is present in the three high-frequency bands.

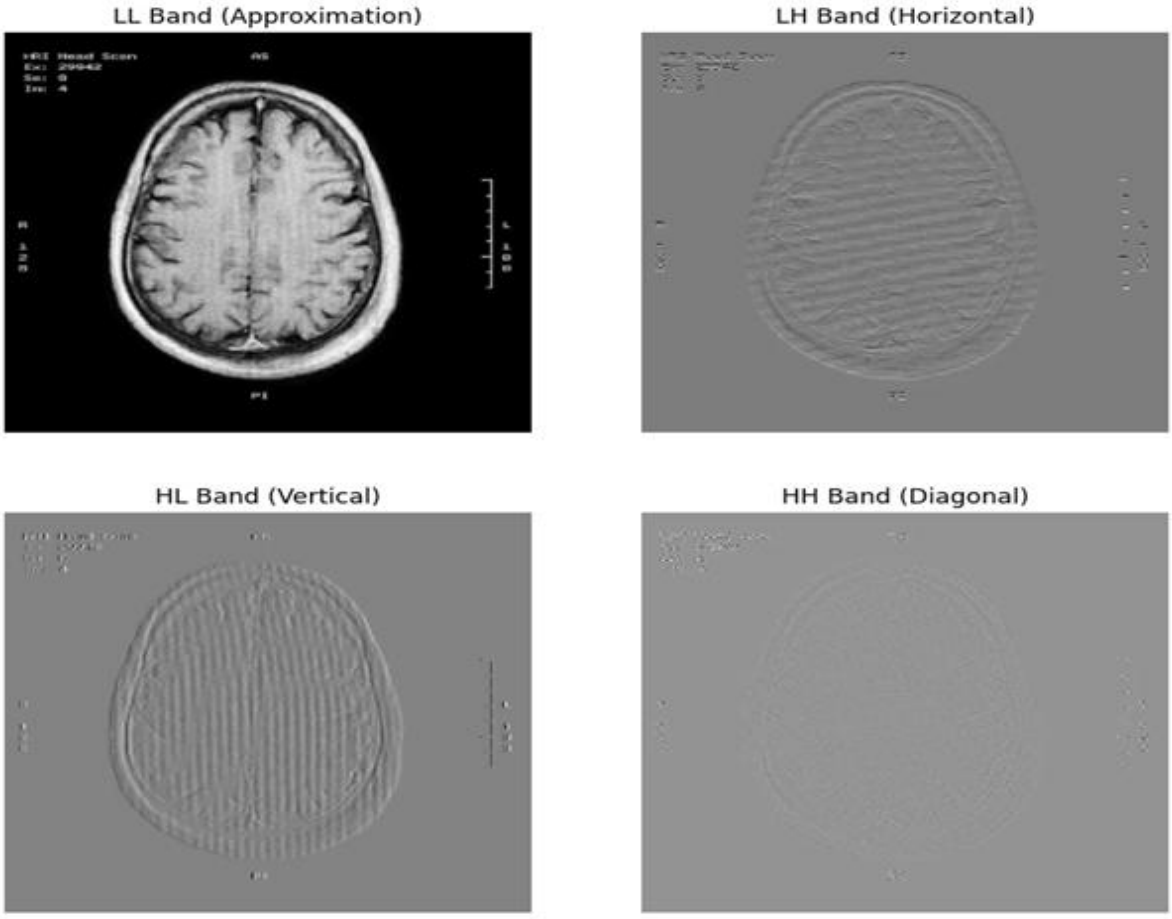

Fig 1. DWT on the cover image of MRI

3.2 Singular Value Decomposition (SVD)

It is a fundamental matrix factorization technique in linear algebra. It decomposes any matrix into three other matrices with specific properties. SVD is widely used in various applications, such as dimensionality reduction, image compression, machine learning, and signal processing. It is employed to determine the most crucial aspects of a matrix, ie., the original matrix size is reduced. The SVD reduces the dimensionality of image data by converting a large matrix of pixel values into a smaller matrix of principal components, which capture the essential features and shapes of the images [25-28].

Example: The SVD Computation of matrix *A* with 2x2 matrix

$$A=\begin{bmatrix}1 & 2\\ 3 & 4\end{bmatrix}$$

The matrix *A* is decomposed using SVD

$$A= USV^{T}$$

Where, *U* is a 2×2 orthogonal matrix containing the left singular vectors of *A*.

S is a 2×2 diagonal matrix containing the singular values of *A*.

V^T is a 2×2 orthogonal matrix containing the right singular vectors of *A*.

$A^TA = \begin{bmatrix}1 & 3\\ 2 & 4\end{bmatrix}\begin{bmatrix}1 & 2\\ 3 & 4\end{bmatrix} = \begin{bmatrix}10 & 14\\ 14 & 20\end{bmatrix}$

$AA^T = \begin{bmatrix}1 & 2\\ 3 & 4\end{bmatrix}\begin{bmatrix}1 & 3\\ 2 & 4\end{bmatrix} = \begin{bmatrix}5 & 11\\ 11 & 25\end{bmatrix}$

The eigenvalues of A^TA give the singular (S) values, and the eigenvectors of A^TA give the right singular vectors of A.

$\lambda I = \lambda\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix} = \begin{bmatrix}\lambda & 0\\ 0 & \lambda\end{bmatrix}$

λ = Eigenvalues

- *The Eigenvalues* of A^TA are computed using determinants as follows

$$\det(A^TA - \lambda I) = \begin{bmatrix}10 & 14\\ 14 & 20\end{bmatrix} - \begin{bmatrix}\lambda & 0\\ 0 & \lambda\end{bmatrix} = \begin{bmatrix}10-\lambda & 14\\ 14 & 20-\lambda\end{bmatrix} = 0$$

$$[(10-\lambda)(20-\lambda) - (14\text{x}14)] = 0$$

$$\lambda^2 - 30\lambda + 4 = 0$$

$$(\lambda - 29.86)(\lambda - 0.14) = 0$$

Two Eigenvalues are $\lambda 1 = 29.86,\ \lambda 2 = 0.14$

- *The Singular* Values are the square roots of the eigenvalues of A^TA:

$\sigma 1 = \sqrt{29.86} = 5.47 \qquad \sigma 1 = \sqrt{0.14} = 0.37$

$S = \begin{bmatrix}5.47 & 0\\ 0 & 0.37\end{bmatrix}$

- *To Compute the Right Singular Vectors (V)*

The eigenvectors of A^TA corresponding to the right singular vectors v_1 and v_2 in matrix V solve

Eigenvector for eigenvalue 29.86

$$\det(A^TA - 29.86\,I) = \begin{bmatrix}10 & 14\\ 14 & 20\end{bmatrix} - \begin{bmatrix}29.86 & 0\\ 0 & 29.86\end{bmatrix} = \begin{bmatrix}10-29.86 & 14\\ 14 & 20-29.86\end{bmatrix}$$

$$= \begin{bmatrix}-19.86 & 14\\ 14 & -9.86\end{bmatrix}$$

To find eigenvectors

$$\begin{bmatrix}-19.86 & 14\\ 14 & -9.86\end{bmatrix}\begin{bmatrix}v1\\ v2\end{bmatrix} = \begin{bmatrix}0\\ 0\end{bmatrix}$$

-19.86 v1 +14v2=0

14v1-9.86v2=0

The eigenvector corresponding to for eigenvalue 29.86 is $\begin{bmatrix}0.70\\1\end{bmatrix}$

Eigenvector for eigenvalue 0.14

$$\det(A^TA - 0.14\,I) = \begin{bmatrix}10 & 14\\14 & 20\end{bmatrix} - \begin{bmatrix}0.14 & 0\\0 & 0.14\end{bmatrix} = \begin{bmatrix}10-0.14 & 14\\14 & 20-0.14\end{bmatrix} = \begin{bmatrix}9.86 & 14\\14 & 19.86\end{bmatrix}$$

To find eigenvectors

$$\begin{bmatrix}9.86 & 14\\14 & 19.86\end{bmatrix}\begin{bmatrix}v1\\v2\end{bmatrix} = \begin{bmatrix}0\\0\end{bmatrix}$$

9.86v1+14v2=0, v1=-1.42v2, if v2=1, then v1=1.42

14v1+19.86v2=0

The eigenvector corresponding to for eigenvalue 0.14 is $\begin{bmatrix}1.42\\1\end{bmatrix}$

The eigenvectors is V= $\begin{bmatrix}0.70 & 1.42\\1 & 1\end{bmatrix}$

- *To Compute Left Singular Vectors (U)*

$A= USV^T$

$AVS^T = U$

- *Example: Dimensionality Reduction in SVD*

  Let's say we have a matrix A of size 5×4

  SVD of $A= USV^T$

  Where:

- U is 5×5,
- S is 5x4 % Diagonal singular values matrix
- V^T is 4x4

To reduce the dimensionality to 2 components, only the top 2 singular values from S and the corresponding vectors from U and V are kept. The reduced matrices will be:

- U_2: the first 2 columns of U (size 5×2),
- S_2: a 2×2 diagonal matrix with the two most significant singular values,
- V_2^T: the first two rows of V^T (size 2×4).

  The reduced matrix approximation $A_2 = U_2S_2V_2^T$

The matrix A_2, resulting from dimensionality reduction via SVD, represents a compressed version of the original matrix A. Although it retains the same dimensions 5×4, it captures the most significant features or patterns in the data, with less noise and redundant information. This reduction in complexity enables more efficient storage, processing, and data analysis.

4. PROPOSED MODEL

A patient's private health details, such as diagnosis or treatment information, are embedded into a medical image file, viz., a scanned MRI or X-ray image, without altering the visible content using steganography. Steganography offers an additional layer of security for sensitive health information, helping to address the growing concerns over privacy and data protection in the healthcare sector. It can enhance patient privacy, secure communications, and ensure data integrity while helping medical professionals maintain compliance with legal regulations. Our method introduces compression techniques, DWT and SVD, to reduce communication overhead for transmitting covert stego medical images.

4.1 IMAGE PRE-PROCESSING

Appropriate preprocessing techniques significantly enhance the steganographic process's effectiveness, security, and imperceptibility. The various pre-processing techniques employed on the cover and secrete images include image format conversion, image resizing, color space conversion, contrast enhancement, noise removal, normalization, etc. Our method resizes the cover and secret images, converting color images into greyscale images.

4.2 EMBEDDING ALGORITHM

Step 1: Input Cover image, Secret Image, and Preprocessing

- Read the cover image *C* and secret image *G*
- Convert color images to greyscale images and resize them to appropriative values.
- Convert both images to float 32 types and normalize to [0, 1] range

Step 2: Attention_Weight or Attention Map Generation [attention_map] = Attention Module (C)

- An attention map uses variations in brightness (shades of gray) to represent the intensity of attention the model gives to different parts of the image.
- Process cover image in 64×64 chunks
- Apply self-attention mechanism

- Normalize the attention map to the range [0.25, 0.75] to obtain attention weight.
- Brighter regions closer to white indicate areas the model is more attentive to. Darker regions closer to black indicate areas the model is paying less attention to. The grayscale attention map can reveal which parts of an image are considered more important for the model's predictions or decisions. Grayscale maps are particularly useful when focusing on simplicity and clarity or when dealing with models that process grayscale images.

Example:

Edge Density and Variance in block complexity give a sense of how information is distributed across a block. For example, blocks with high edge density and variance tend to have more complex, diverse information. Image processing or data embedding like steganography helps identify regions in an image with high information content. This can help decide where to place or hide data without significantly altering the image's visual quality or other properties.

In image steganography, secret data should ideally be embedded in regions where it won't be easily detected. High-complexity blocks are better suited for embedding data, as they have a wider range of pixel values and more subtle patterns, making alterations less noticeable.

(i) Block-wise Processing for each 8×8 block:

(a). Consider cover block *C* of sizes 8×8.

(b). Calculate block complexity using complexity = Edge_Density * Variance

(ii) Calculate Edge Density

Count how many non-zero pixel values exist in each of the blocks.

Suppose the *C* block has 50 non-zero values out of 64 pixels,

The edge density for the cover block *C* would =50/64≈0.78125

(iv) Variance

For example, the pixel values for the *C* block have a mean of 120 & variance of 2500, and the pixel values for the *G* block have a mean of 130 & variance of 1800.

(v) Compute Block Complexity

Block Complexity of Cover Block *C*= 0.78125 × 2500 =1953.125

By calculating block complexity, can identify suitable blocks for hiding information, thus improving the imperceptibility of the embedded data.

Step 3: Discrete Wavelet Transform

DWT (C_block, 'haar') = [LL_c, (LH_c, HL_c, HH_c)] % Cover image

DWT (G_block, 'haar') = [LL_s, (LH_s, HL_s, HH_s)] % Secret image

Step 4: SVD Decomposition

SVD (LL_s) = [U_s, S_s, V_s] % Secret image

SVD (LL_c) = [U_c, S_c, V_c] % Cover image

Step 5: Generate Singular Values of Stegoimage

Singular Values for stegoimage is S_stego = S_c + α * attention_weight * S_s

Where,

α is a scaling factor considered 0.100 in our proposed model for better results.

Attention_weight, depending on the image, is normalized in the range of 0.25-0.75.

Step 6: Stego Image Block Construction

- LL_stego = U_c * S_stego * V^T_c %Multiplication
- Key=S_c, α, and attention_weight; embed in HL_c band using LSB Technique.
- The cover image HL_c band will be new band HL_new

Stegoimage C'_block = IDWT (LL_stego, (LH_c, HL_new, HH_c), 'haar') %Spatial domain Stegoimage

4.3 EXTRACTION ALGORITHM

Step 1: Input Stegoimage

- Convert stegoimage C' to float 32 and normalize to [0,1]

Step 2: Block-wise Processing of stegoimage C' for each embedded block position and construct stego block C'

Step 3: Discrete Wavelet Transform

DWT (C'_block, 'haar') = [LL_stego, (LH_stego, HL_stego, HH_stego)] % Stegoimage

Step 4: SVD Decomposition

SVD (LL_stego) = [U_stego, S_stego, V_stego]

Step 5: Secret image Recovery

- Obtain S_c, α, and attention_weight from HL_stego using reverse process of LSB Technique
- Calculate: S_secret = (S_stego - S_c) / (α * attention_weight)

Step 6: Secret Block Reconstruction

LL_secret = U_stego * S_secret * V_{stego}^T % Multiplication

G'_block = IDWT (LL_secret, (LH_stego, HL_stego, HH_stego), 'haar')

Step 7: Final Secret Image Formation

- Combine all reconstructed secret G' blocks
- Validate and handle any numerical instabilities

- Form final extracted secret image G'

5 RESULT ANALYSIS

5.1 Definitions of Performance Parameters

The image quality is evaluated using non-linear measures such as the PSNR and SSIM.

5.1.1 Mean Square Error (MSE)

It is the difference between the original Cover image and the stegoimage divided by the total number of pixels [29] as given in Equation (6).

$$\text{MSE}= \frac{1}{M*N}\sum_{i=1}^{M}\sum_{j=1}^{N}[x(i,j)-y\,(i,j)]^2 \quad \text{----------(6)}$$

Where x and y are cover and stegoimages

5.1.2 PSNR

It measures the absolute difference between the CI and SI in decibels (dB) and quantifies the peak inaccuracy between two images. However, it is limited because it does not accurately reflect subjective visual quality, particularly in distorted images. It measures the quality of stego-image [30] as given in Equation 7.

$$PSNR = 10\,log_{10}\left[\frac{255^2}{MSE}\right] \quad \text{----------(7)}$$

5.1.3 Structural Similarity Index Measure (SSIM)

The SSIM compares the images' structure, contrast, and luminance to evaluate the visual quality. Since it is more in line with human visual perception, it is a superior statistic for evaluating image quality than PSNR, which is made to reflect perceived changes in images more correctly. The SSIM is frequently chosen over PSNR when human perception is crucial [31, 32]. An SSIM index is a decimal value that ranges from -1 to 1, where -1 denotes perfect anti-correlation, 0 denotes no similarity, and 1 denotes perfect similarity. The SSIM between two images, CI and SI, is given in Equation 8.

$$SSIM = \frac{(2\mu_x\,\mu_y+C_1)\,(2\sigma_{xy}+C_2)}{(\mu_x^2\,\mu_y^2+C_2)\,(\sigma_x^2+\sigma_y^2+C_2)} \quad \text{---------- (8)}$$

Where μ_x, μ_y are mean pixel values of CI and SI

σ_x^2 *and* σ_y^2 are the variance of pixel values

σ_{xy} are the covariance between CI and SI

c_1 and c_2 are constants

5.1.4 Capacity

It is a significant aspect of medical image steganography that should be considered when evaluating the overall effectiveness of the proposed approach [33]. It is the amount of information encoded in the host image, represented in bits per pixel (BPP) units as given in Equation 9.

$$\text{Capacity} = \frac{Total\ number\ of\ bits\ that\ can\ be\ embedded}{Total\ number\ of\ pixels\ in\ the\ image} \qquad \text{----------(9)}$$

5.2 Histogram visualization

This tool, which displays the number of pixels that correspond to each pixel intensity value, is a graphical depiction of the distribution of pixel values in a picture and is used to detect changes by steganography. In image steganography, histogram visualization helps evaluate how well data-hiding strategies work. The image's pixel value histogram can detect changes performed during steganography. Strategies like histogram shifting can enhance visual quality and expand the ability to conceal data. While evaluating possible distortions from the embedding process, this technique helps guarantee that the hidden message stays undetectable [34]. Figures 2 and 3 display the cover image and stegoimage histogram plots. Since the histograms are almost the same, it is concluded that the suggested steganographic technique has not significantly altered the stegoimage.

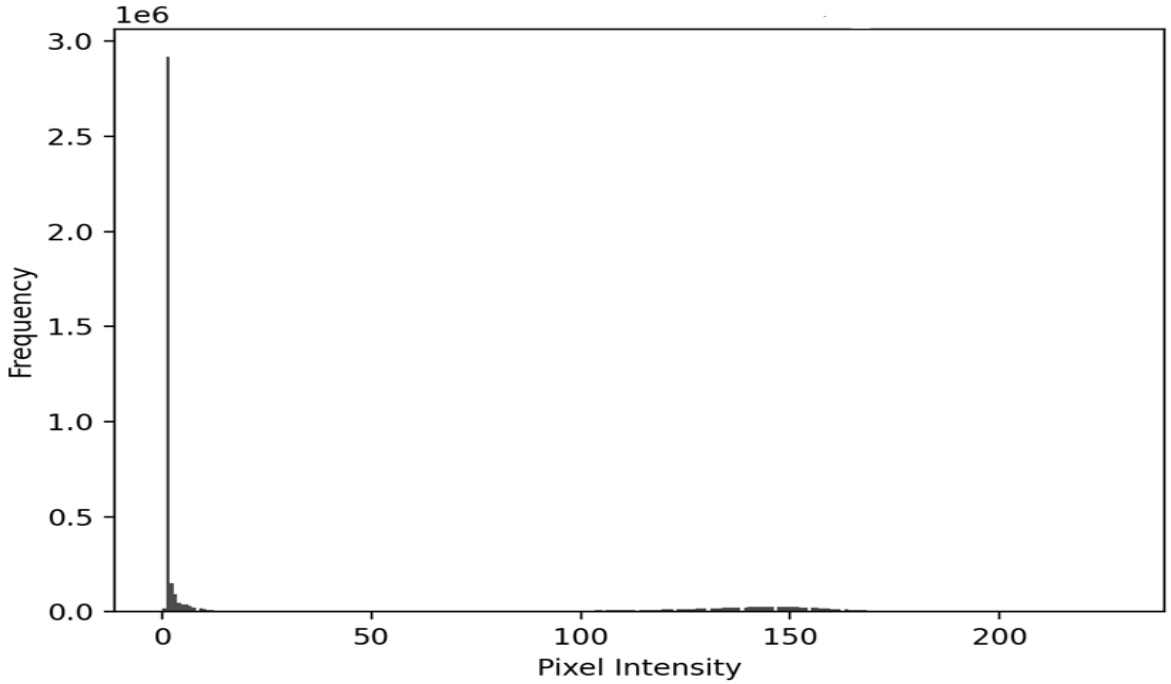

Fig 2. Histogram of MRI cover image

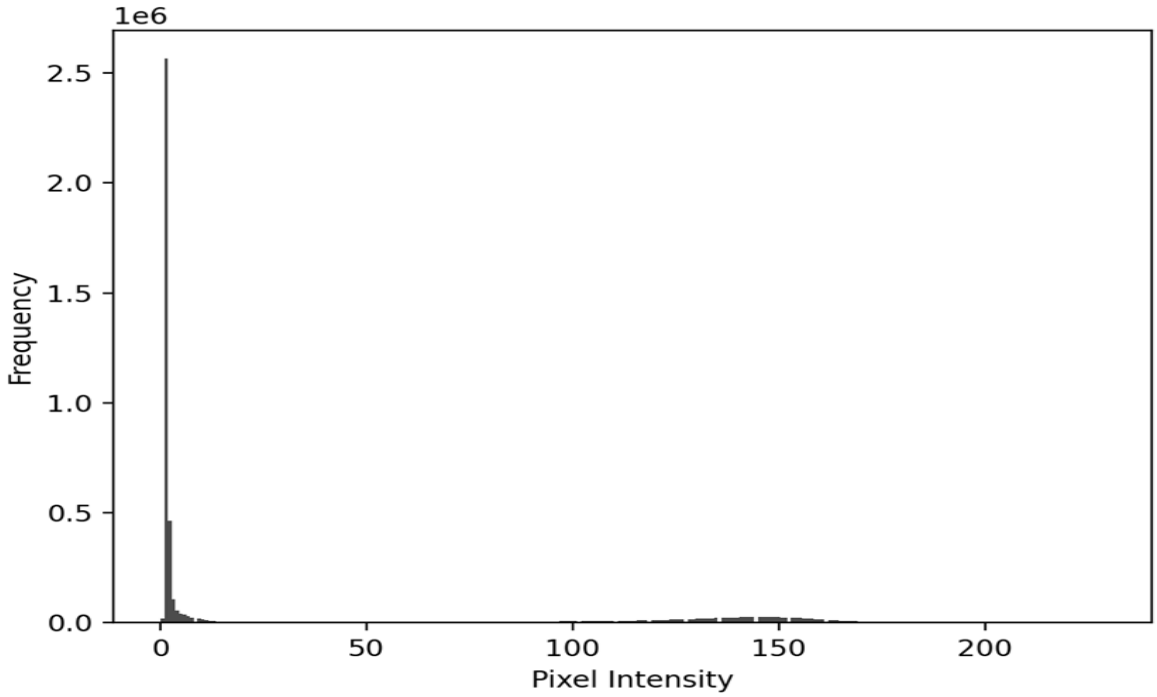

Fig 3. Histogram of MRI stegoimage

5.3 Performance Parameter Analysis

Figure 4 shows the medical cover images and people's secret images, which are considered to test the algorithm, with corresponding stego and extracted secret images.

(a) MRI Cover Image

(e) X-ray Cover Image

(b) Secret Image_ Boy

(f) Secret Image_ Girl

(c) Stegoimage

(g) Stegoimage

(d) Extracted Secret Image

(h) Extracted Secret Image

Fig. 4 Steganography images

The variations of MSE, PSNR, and SSIM with different capacities for MRI cover, stego, Boy secret, and extracted secret images are tabulated in Table 1. The values of PSNR and SSIM increase with a decrease in capacity. The maximum value of PSNR of 71.48 db and SSIM of 0.9990 are obtained with a capacity of 33.2% for cover and stegoimage. The quality of the stegoimage is very close to the original cover image. The quality of the extracted secret image is very close to the original secret image.

Table 1: Variations of performance parameters with capacity for MRI Cover image

Sl. No.	Secret image-Boy	% Capacity	Cover (MRI image) and Stegoimage			Secret and Extracted Secret image		
			MSE	PSNR	SSIM	MSE	PSNR	SSIM
1	444 x 444	100	0.00008	56.73	0.9980	0.01061	34.12	0.9697
2	362 x 362	66.5	0.00001	59.24	0.9982	0.0003	41.25	0.9708
3	256 x 256	33.2	0.000001	71.48	0.9990	0.0002	41.29	0.9717

The variations of MSE, PSNR, and SSIM with different capacities for X-ray cover, stego, Girl secret, and extracted secret images are tabulated in Table 2. The values of PSNR and SSIM increase with a decrease in capacity. The maximum value of PSNR of 56.49 db and SSIM of 0.9992 are obtained with a capacity of 33.2% for cover and stegoimage. The quality of the stegoimage is very close to the original cover image. The quality of the extracted secret image is very close to the original secret image. The PSNR values are dependent on the types of cover images.

Table 2: Variations of performance parameters with capacity for X-ray Cover image

Sl. No.	Secret image-Girl	% Capacity	Cover (X-Ray image) and Stegoimage			Secret and Extracted Secret image		
			MSE	PSNR (db)	SSIM	MSE	PSNR (db)	SSIM
1	444 x 444	100	0.00009	52.86	0.9990	0.00024	33.45	0.9471
2	362 x 362	66.5	0.00009	53.96	0.9990	0.00022	34.97	0.9607
3	256 x 256	33.2	0.00008	56.49	0.9992	0.00020	35.71	0.9681

5.4 Comparison of the proposed method with existing methods

Table 3 compares the suggested and current approaches for PSNR and SSIM parameters on the cover image and stegoimage. The cover photos, including MRI and X-ray, are regarded as medical photos. The details of people or person photos are the secret images. The PSNR and SSIM values are calculated between the cover and stegoimages. It is observed that the suggested approach outperforms the current approaches.

Table 3. The existing methods are compared with the proposed method by considering cover MRI image and stegoimage.

Sl No.	Authors	Publication Details	Techniques	PSNR (db)	SSIM
1	Shabir A. Parah et al., [35] X-Ray image	Springer Nature Link, Health Technol, 2020	Pixel to Block conversion technique	49.68	0.9912
2	Partha Chowdhuri et al., [36] MRI images	Springer Nature Link, Multimedia Tools and Applications, 2023	IWT and SVM	64	0.9998
3	Proposed Method		LSB, DWT and SVD	71.48	0.9990

6. CONCLUSION

Image steganography is an effective, secure communication method for protecting confidential data without raising suspicions of intruders. In this paper, an Efficient Health Data

Transmission System based on Steganography Using a Hybrid Domain Technique is proposed that focuses on embedding confidential patient details into medical data images while ensuring the information's confidentiality, integrity, and authenticity. The DWT is applied on the cover and secret images to obtain low-frequency LL and high-frequency bands LH, HL, and HH bands. The SVD is applied on LL bands of cover and secret images to get singular values. The singular values of cover and secret images are combined with α and attention_weight to obtain singular values of stegoimage. The stego key: singular values of cover S_c, α, and attention_weight are embedded into the HL of the cover image using the LSB technique to obtain HL_new. The IDWT is used to derive spatial domain stegoimage. The secret image is extracted from the stegoimage using the reverse embedding process at the destination. In the future, a combination of traditional and deep learning techniques can be further explored to obtain the benefits.

REFERENCES

[1] Chowdhuri P., Jana B., and Giri D., “Secured Steganographic Scheme for Highly Compressed Color Image using Weighted Matrix Through DCT,” *International Journal of Computers and Applications*, vol 43, no. 1, pp 38–49, 2021, doi.org/10.1080/1206212x.2018.1505024.

[2] J. Wu, B. Chen, W. Luo and Y. Fang, "Audio Steganography Based on Iterative Adversarial Attacks Against Convolutional Neural Networks," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 2282-2294, 2020, doi: 10.1109/TIFS.2019.2963764.

[3] Banerjee A. and Jana B., “A Secure High-Capacity Video Steganography Using Bit Plane Slicing Through (7, 4) Hamming Code,” *Advanced Computational and Communication Paradigms*. Springer, New York, NY, USA, vol 706, pp 85–98, 2018, doi.org/10.1007/978-981-10-8237-5_9.

[4] J. Tao, S. Li, X. Zhang and Z. Wang, "Towards Robust Image Steganography," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 29, no. 2, pp. 594-600, 2019, doi: 10.1109/TCSVT.2018.2881118.

[5] K B Raja, C R Chowdary, Venugopal K R, and L M Patnaik, “A Secure Steganography using LSB, DCT, and Compression Techniques on Raw Images,” *IEEE International Conference on Intelligence Sensing and Information processing*, pp.171 - 176, Bangalore, India, December 2005..

[6] Malhotra, S. Gupta, D. Koundal, A. Zaguia, M. Kaur, and H.-N. Lee, ‘‘Deep learning-based computer-aided pneumothorax detection using chest X-ray images,’’ *Sensors*, vol. 22, no. 6, 2278, Mar. 2022, doi: 10.3390/s22062278.

[7] http://openfmri.org/

[8] https://www.kaggle.com/datasets/kmader/siim-medical-images.

[9] K B Raja, C R Chowdary, Venugopal K R, L M Patnaik, “A Secure Image Steganography on Raw Images,” *International Journal of Computer Science and Network Security,* vol. 5, no. 11, pp. 123–129, 2005.

[10] N. Subramanian, O. Elharrouss, S. Al-Maadeed, and A. Bouridane, "Image Steganography: A Review of the Recent Advances," *IEEE Access*, vol. 9, pp. 23409-23423, 2021, doi: 10.1109/ACCESS.2021.3053998.

[11] M. K. Abed, M. M. Kareem, R. K. Ibrahim, M. M. Hashim, S. Kurnaz and A. H. Ali, "Secure Medical Image Steganography Method Based on Pixels Variance Value and Eight Neighbors," *IEEE International Conference on Advanced Computer Applications (ACA),* Maysan, Iraq, 2021, pp. 199-205, doi: 10.1109/ACA52198.2021.9626807.

[12] K. Farhan Rafat and S. Muhammad Sajjad, "Advancing Reversible LSB Steganography: Addressing Imperfections and Embracing Pioneering Techniques for Enhanced Security," *IEEE Access*, vol. 12, pp. 143434-143457, 2024, doi: 10.1109/ACCESS.2024.3468988.

[13] M. Ye, D. Huang, K. Wei, and W. Luo, "A Novel Residual-Guided Learning Method for Image Steganography," *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP),* Seoul, Korea, pp. 4565-4569, 2024, doi: 10.1109/ICASSP48485.2024.10446443.

[14] F. Ramadhan, R. D. A. Anandha, A. W. C. D’Layla, N. J. De La Croix and T. Ahmad, "Image Steganography using Customized Differences between the Neighboring Pixels," *IEEE 7th International Conference on Informatics and Computational Sciences (ICICoS),* Semarang, Indonesia, pp. 496-501, 2024, doi: 10.1109/ICICoS62600.2024.10636936.

[15] D. Wahono, H. Rahman, H. Syarif, N. J. De La Croix and T. Ahmad, "Enhancing Data Security Using Steganography in Spatial Domain Images," *IEEE Second International Conference on Emerging Trends in Information Technology and Engineering (ICETITE),* Vellore, India, 2024, pp. 1-6, doi: 10.1109/ic-ETITE58242.2024.10493831.

[16] A. I. H. Al-Jarah and J. L. Ortega-Arjona, "Enhancing the Capacity and Robustness of an LSB Algorithm Using a Novel Insertion Method, Hashing Function, and Secret Key," IEEE Access, vol. 12, pp. 159534-159544, 2024, doi: 10.1109/ACCESS.2024.3483832.

[17] Shmueli, R., Mishra, D., Shmueli T, and Ofer Hadar, "A Novel Technique for Image Steganography Based on Maximum Energy Seam," *Springer Nature Link Multimedia Tools Applications,* vol 83, pp 70907–70920, 2024, https://doi.org/10.1007/s11042-024-18476-6.

[18] Naveen P, and Jayaraghavi R, "Image Steganography Method for Securing Multiple Images Using LSB–GA," *Springer Nature Link Wireless Personal Communications* 135, 1–19, 2024. https://doi.org/10.1007/s11277-024-10945-3.

[19] S. H. Chiu and C. Y. Lin, "Robust Coverless Image Steganography Based on SIFT and DWT Sequence Mapping," *IEEE 4th Asia Conference on Information Engineering (ACIE),* Singapore, Singapore, 2024, pp. 41-45, doi: 10.1109/ACIE61839.2024.00014.

[20] Partha Chowdhuri, Pabitra Pal, and Tapas Si, "A Novel Steganographic Technique for Medical Image using SVM and IWT," *Springer Nature Link Multimedia Tools and Applications,* Vol 82, pp 20497–20516, 2023, doi.org/10.1007/s11042-022-14301-0.

[21] B. Ramapriya and Y. Kalpana, "A Competent Medical Image Steganography using Improved Optimization Algorithm with Huffman Encoding Techniques," *IEEE 7th International Conference on Computing Methodologies and Communication (ICCMC),* Erode, India, pp. 1065-1073, 2023, doi: 10.1109/ICCMC56507.2023.10083698.

[22] Ramyashree, P. S. Venugopala, S. Raghavendra and B. Ashwini, "Cryptic Care: A Strategic Approach to Telemedicine Security Using LSB and DCT Steganography for Enhancing the Patient Data Protection," *IEEE Access*, vol. 12, pp. 101166-101183, 2024, doi: 10.1109/ACCESS.2024.3430546.

[23] G. V. Sagar, S. Y. Barker, K. B. Raja, K. S. Babu, and Venugopal K R, "Convolution-based Face Recognition using DWT and Feature Vector Compression," *IEEE International Conference on Image Information Processing (ICIIP),* pp. 444-449, 2015, doi: 10.1109/ICIIP.2015.7414814.

[24] Po-Yueh Chen and Hung-Ju Lin, "A DWT Based Approach for Image Steganography," *International Journal of Applied Science and Engineering,* vol 4, no. 4, pp 275-290, 2006.

[25] Golub G H, and Reinsch C, “Singular Value Decomposition and Least Squares Solutions,” *Springer Nature Link Numerische Mathematik*, vol 14, no. 5, pp 403–420, 1970, doi.org/10.1007/BF02163027.

[26] Juhi Singh, and Mukesh Singla “Image Steganography Technique based on Singular Value Decomposition and Discrete Wavelet Transform,” *International Journal of Electrical and Electronics Research,* vol 10, issue 2, pp 122-125, 2022.

[27] Fadhil Kadhim Zaidan, “Digital Image Steganography Scheme Based on DWT and SVD,” *Diyala Journal of Engineering Sciences*, vol 13, No 4, pp10-17, 2020, doi: 10.24237/djes.2020.13402.

[28] A. Nevriyanto, S. Sutarno, S. D. Siswanti, and E. Erwin, *"Image Steganography Using Combine of Discrete Wavelet Transform and Singular Value Decomposition for More Robustness and Higher Peak Signal Noise Ratio," IEEE International Conference on Electrical Engineering and Computer Science (ICECOS),* Pangkal, Indonesia, 2018, pp. 147-152, doi: 10.1109/ICECOS.2018.8605205.

[29] Z. Wang and A. C. Bovik, "Mean Squared Error: Love it or leave it? A new look at Signal Fidelity Measures," *IEEE Signal Processing Magazine*, vol. 26, no. 1, pp. 98-117, Jan. 2009, doi: 10.1109/MSP.2008.930649.

[30] A. Horé and D. Ziou, "Image Quality Metrics: PSNR vs. SSIM," *IEEE 20th International Conference on Pattern Recognition*, Istanbul, Turkey, 2010, pp. 2366-2369, doi: 10.1109/ICPR.2010.579.

[31] Z. Wang, E. P. Simoncelli, and A. C. Bovik, "Multiscale Structural Similarity for Image Quality Assessment," *IEEE Thrity-Seventh Asilomar Conference on Signals, Systems & Computers,* Pacific Grove, CA, USA, 2003, pp. 1398-1402 Vol.2, doi: 10.1109/ACSSC.2003.1292216.

[32] Zhou Wang, A. C. Bovik, H. R. Sheikh and E. P. Simoncelli, "Image Quality Assessment: From Error Visibility to Structural Similarity," *IEEE Transactions on Image Processing*, vol. 13, no. 4, pp. 600-612, April 2004, doi: 10.1109/TIP.2003.819861.

[33] Partha Chowdhuri, Pabitra Pal, and Tapas Si, “A Novel Steganographic Technique for Medical Image using SVM and IWT,” *Springer Multimedia Tools and Applications*, vol 82, pp 20497-20516, 2023, doi.org/10.1007/s11042-022-14301-0.

[34] Geno Peter, Anli Sherine, Yuvaraja Teekaraman, Ramya Kuppusamy, and Arun Radhakrishnan, “Histogram Shifting-Based Quick Response Steganography Method for Secure

Communication," *Wiley Hindawi Wireless Communications and Mobile Computing*, pp 1-11, 2022. https://doi.org/10.1155/2022/1505133

[35] Shabir A. Parah, Farhana Ahad, Javaid A. Sheikh, and G.M. Bhat, "Hiding Clinical Information in Medical Images: A New High Capacity and Reversible Data Hiding Technique," *Elsevier Journal of Biomedical Informatics*, vol 66, pp 214-230, 2017, doi.org/10.1016/j.jbi.2017.01.006.

[36] Partha Chowdhuri, Pabitra Pal, and Tapas Si. "A Novel Steganographic Technique for Medical Image Using SVM and IWT," *In: Multimedia Tools and Applications* 82.13 pp. 20497–20516, 2023.

Citation: Sangeetha N, Harshith K Raj, K B Raja. Efficient Health Data Transmission System Based on Steganography Using Hybrid Domain Technique. Journal of Electronics and Communication Engineering and Technology (JECET), 6(1), 2025, 1-23.

Abstract Link: https://iaeme.com/Home/article_id/JECET_06_01_001

Article Link:
https://iaeme.com/MasterAdmin/Journal_uploads/JECET/VOLUME_6_ISSUE_1/JECET_06_01_001.pdf