International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

Applications of Difital Image Stegnographic Techniques in Medical Image Analysis

[1]Nalini Bodasingi, [2]T S N Murthy
[1]Dept of ECE, JNTUGV
Vizianagram, India
e-mail: nalinib.ece@jntugvcev.edu.in
[2]Dept of ECE, JNTUGV
Vizianagram, India
e-mail: tsnmurthyece.jntuk@ieee.org

Abstract— In this digitized world maintaining the security of the secret information is a challenging task. While, sending secret information through the internet draws the attention of hackers. The highly authenticated information can be hidden by using Steganography. Image processing plays a very important role in such stenographic techniques. The advantage of stenography can be enhanced to medical images and creation of database for a particular patient under one authentication with security. Steganography techniques used in bio-medical field to hide the person medical data like prescription, X-ray, Iris, MRI, CT scan images behind a single cover media. In this paper the embedding Schemes to store complete medical data under one authentication is done by using Spatial and transform domains. The performance of the techniques is compared and the best method to hide medical information by using steganographic techniques with high PSNR, less MSE and high SSIM is identified for different modalities. Implementation of steganography in bio-medical field yields high imperceptibility and embedding capacity

Keywords- *Cover-image, stegofile, LSB, PVD, DCT, DWT,PSNR, MSE, SSIM*

I. INTRODUCTION

In modern era, image processing plays vital role in bio-medical field (1). Image processing is used to extract the features of an image or information from an image. Steganography which is mainly used in image processing, emerges to implement a high secure communication in medical field. Digital medical images are most fundamental for diagnosis of diseases, and communication of patient data between the doctors. Steganography is presently used in the bio-medical field used to transmit the data with high security over the unsecure medium.

Internet plays a major role in the development of the communities. Enormous amount of information being transmitted which is vital, to secure this information is critically needed. There are many techniques used to hide information like Cryptography, Watermarking (2). But Steganography unlike other techniques hide the information behind any digital media and can be applied to any form of digital media (3). Thus, steganography for digital images is a technique of covert communication aims to transmit a large amount of data relative to the size of the cover image.

The word Steganography derived from the Greek word which means “secret writing”. It is the practical process that hide data within a cover image sometimes it is also called as carrier in such a way that the hidden information which is embedded behind the cover is undetectable (4).

The cover Image can be audio, video, text file or image. Secret information can also be audio, video, text file or image (5). Image steganography is the process of embedding information behind the cover image without modifying the characteristics of the cover image. The produced file is called as STEGO File. The stego file contains the data of cover image along with hidden data. In future the extraction of the data is done using decoding.

Types of steganography:

Steganography can be classified in various ways, depending on the cover medium.

1.Text
2.Audio
3.Video
4.Image

1. Text Steganography

The text Steganography is the older method historically to hide information by changing the format of the text or the words within the text. It is not much used because the text files have a very small amount of redundant data (6).

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

2. Audio Steganography

It is about to hiding information into the audio. An audible sound becomes hidden in the presence of louder sound. It secures the information by exploiting the properties of human ear to hide information unpredictable (7). It is less popular than image steganography.

3. Video Steganography

Video Steganography used video as a cover media. The capacity of video steganography is high. Large amount of information can be stored in a video. It has more security against third party. In this technique combination of pictures is used as a carrier any type of digital data can be embedded into it (8). Generally, DCT technique is used to hide the information, which unnoticeable by human eye.

4. Image Steganography

Most popular technique in steganography is the image steganography. In digital world images are widely used because of their availability. In this technique images used as cover media and hiding data can be any form (9). The hiding capacity related to the size of the cover image. By using embedding algorithm is used to hide the information and produces a Stego file and transmitted. The Stego image same as cover image the existence of the hidden data only known to the recipient (10).

Considering the advantage of all the stenographic techniques in general the medical data is now a days available in text, audio, video or image format. maintain of the records of all the patients occupies a very high space. The maintenance of the medical record plays a crucial role in further examination of the patient or it is easy to carry when it is digitalised. Now a day's maintenance of a health card also plays a very crucial role in development of the country. In the proposed work as a module of health card development an attempt is made to study the techniques which help to create a medical data storage under one authentication.

In this paper an attempt is made to store the medical data of a patient under a cover media by using different steganographic techniques such as spatial and transform domain, and evaluated their performance by using metrics such as PSNR, MSE, and SSIM.

The organization of paper is as follows: Section-ii describes the methodology under these 3 subsections are present. Which describes what is data hidden secret data under., cover media embedding and extraction process. Section-iii describes the techniques used for this application. Section-iv performance evaluation of methods. Section-v results and discussion Section vi describes the conclusion.

II. METHODOLOGY

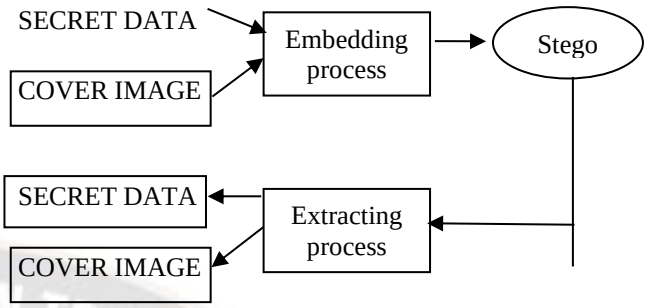


Figure 1. Stegonography Process

The working model of steganography system is shown above. The model consists of three subparts i. secret data ii. cover media iii. Embedding and Extracting process. Cover image used to hide the secret image (11). Stego image produced after the embedding of secret image into cover image. The extraction process recovers the secret data from the Stego image.

a. Secret Data:

Secret data represents hidden data. Secret data can be of any form like image, audio, video, text files, documents or any other types (12). In this paper the secret data set are images and text files. The images are bio-medical images collected from the standard rsna web. The images are X-ray, CT-scan, MRI, IRIS scan images, each of 15 samples are taken, image format such as jpeg, jpg, png, tif, tiffor any other. The text files are prescription files these are.txt files.

b. Cover media:

Cover media basically, represents the container of the secret data. The characteristics of cover files are modified in order to add these secret data (13). However, these changes are highly, imperceptible to the human eye. Therefore, the format of cover file should remain same after the embedding of the secret data (14). The cover files can be an executable file like .exe files. The cover can be an image, audio file, video or text. In this paper the cover media is an Aadhaar card the format of cover image can be jpeg, jpg, png, or any other type.

c. Embedding and Extracting process

The Stegofile is resultant of merging the secret data and cover image (15). At the recipient side the decoding the confidential data can be done with an efficient extracting algorithm and this process of extracting the secret data from the cover data is known as steganalysis (16). The whole process can be done using image steganography techniques. In those techniques the methods are described about the embedding and extracting process comprehensively.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

III. TECHNIQUES

Image Steganography generally classified into two domains Spatial domain and Transform domain.

A. Spatial Domain

In this domain for hiding data directly image pixel values are changed for hiding data. This domain method is frequently used because of its fine concealment, great capability of hidden information. Mostly used methods in this domain are *Least Significant Bit method and Pixel value differencing method*.

a. Least Significant Bit Method(LSB):

This method is a simple approach that hide information just by replacing the least significant bit(LSB). The LSB is the right most bit in the data for example 11001101 in this the right most one is the LSB bit. The cover image LSB is replaced by the secret data bits and the embedding process has done (17). In this embedding process least significant bits of cover image pixels are replaced with the bits of the secret data. The obtained Stego file is similar to the cover image because change in the pixel value of the cover image does not bring much difference. But if the information exceeds then the relevant size of the cover image then the change in the cover image can be noticeable. Because the adjacent bit to the LSB is also changed due to excess information. At the recipient side decoding algorithm is used and the secret data has been extracted (18). This can be implemented for colour and grey scale images. This paper proposes the medical data hidden under the Aadhaar card as a cover image by using above-described algorithm and the extraction has been done with the algorithm. The LSB method embedded and extracted of data such as X-ray, CT scan, Iris, MRI images under a Aadhaar card as shown below:

Fig1,2.3.4 shows the carrier image i.e., cover image, secreat image and stegmentented image which is created by embedding phase, recovered image which is an extraction output using LSB technique for MRI image, CTscan, Iris and X-ray images respectively.

b. *Pixel Value Differencing Method (PVD):*

PVD method is based on the adjacent pixel value differencing. It gives good robustness and more embedding capacity. First the cover data broken into block of pixels, each block contains 2 pixels these pixels are selected for embedding the data. The difference value of the pixels is replaced by the secret data value. The number of bits which can be embedded in a pixel pair depends on the difference value. The quantization table is used to determine the pay load between the consecutive pixels (19). Two neighbouring pixels differencing is given by $d=g_{i+1}-g_i$

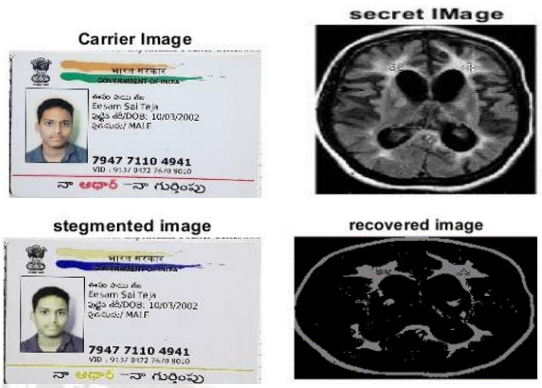


Figure 2. LSB method for embeding MRI image

Figure 3. LSB method for embeding CT scan image

High imperceptibility can be achieved through this method. PVD method is basically used to hide the text files. The concealed data can be extracted by performing the extracting process from the hidden pixels. Due to the modification in the values of the pixels the hidden data is not noticeable behind the cover image. More information can be hidden in this method. Many new implementations have discovered based on modulus function (20). In this proposed paper only text file hiding has done under the cover image.

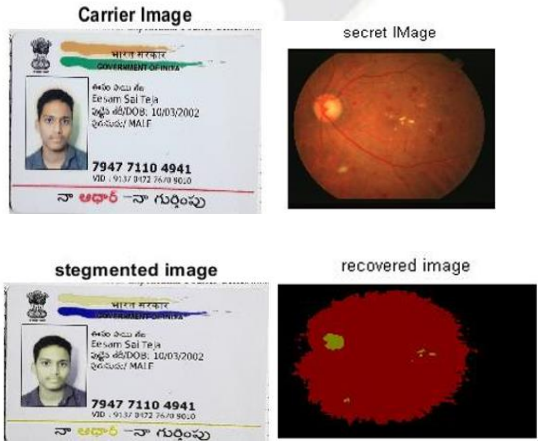


Figure 4. LSB method for embeding IRIS image

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

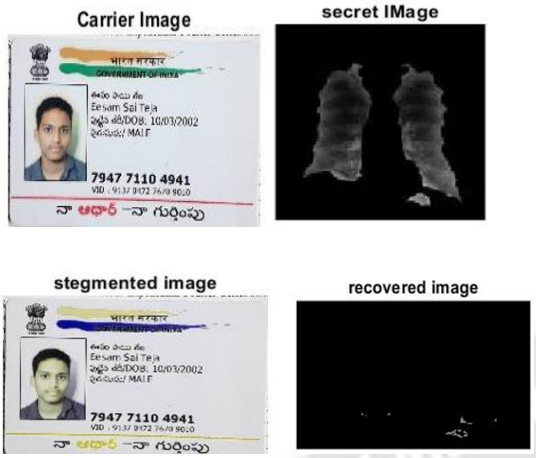


Figure 5. LSB method for embeding X-ray image

Figure 6. PVD method for file hiding

Fig 5 shown are carrier and Stego images under this Stego file the secret .txt file is concealed .

B. Transform Domain

The Transform domain also called as frequency domain in this domain secret data is concealed in the transform domain coefficients. The methods involved are Discrete Cosine Transformation and Discrete Wavelet Transformation.

a. Discrete Cosine Transformation (DCT):

This method is complicated to implement because the data is saved in frequency domain instead of spatial domain. It generally transforms the images from the spatial domain to frequency domain. First the cover image is broken into 8*8 pixels blocks (21) then DCT is applied from top to bottom and right to left to each pixel block. Each block is compressed to quantization table and scaled to DCT coefficients. The message is embedded in the DCT coefficients.

For calculating the DCT coefficients for a 2-d image is:

$$V_{xy}=u_x u_y \sum_{i=0}^{M-1} \left(u_{ij} \cos\frac{\pi(2i+1)x}{2M} \cos\frac{\pi(2j+1)y}{2N} \right)$$

Where i and j are rows and columns of image and V is the output image

The hiding capacity is not much because the block size is fixed like 8*8 and 16*16 (22). The Stego file is created by applying the inverse discrete cosine transform. The Stego file is same as cover image, hidden data behind this file is unpredictable by the human eye. At the recipient side inverse quantization has been done and extracted the hidden data. This technique is widely used by combining with the LSB and Huffman coding (23).

Figure 7. DCT method for MRI image

Figure 8. DCT method for CT-scan image

Figure 9. DCT method for X-ray

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

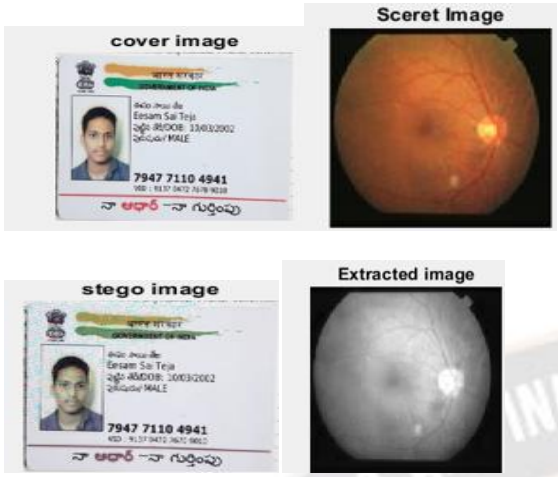


Figure 10. DCT method for IRIS image

This paper proposes the medical data hidden under the Aadhaar card as a cover image by using above-described algorithm and the extraction has been done with the algorithm. The DCT method embedded and extracted data such as X-ray, CT scan, Iris, MRI images under a Aadhaar card as presented in Fig 6 to Fig. 9.

b. Discrete Wavelet Transformation (DWT):

DWT is the most widely used method compared to other methods. This method gives the highest robustness. Different wavelets can be applied to perform the DWT, but most commonly used is the Haar-wavelet knowns Haar-DWT. Haar is a sequence of rescaled square shaped functions which together form a wavelet basis. Haar DWT is a 2-Dimensional operation: one is the horizontal operation and other is a vertical operation (24). It scans the pixels in both horizontal and vertical directions and store the corresponding pixels sum and differencing values in the sub-bands. The wavelet coefficients of cover image are obtained by filtering and the data is hide inside these coefficients (25), the Stego file is created. The Stego file is exactly same as cover image, but for colour the slight variation in the cover image can be appear. The more amount of data can be embedded in this method because the bands can store more information. The inverse transformation applied at the recipient side and extracted the secret data from the Stego file. Due to is more embedding capacity and robustness this technique is mostly used.

4.Extracted Image

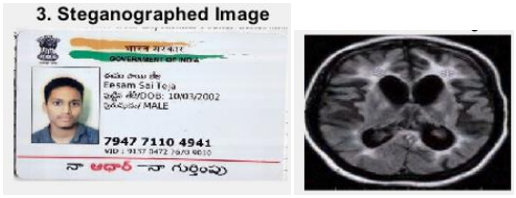


Figure 11. DWT method for MRI

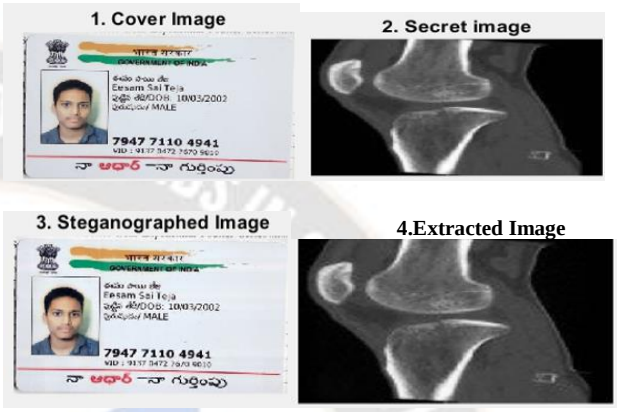


Figure 12. DWT method for CT-scan image

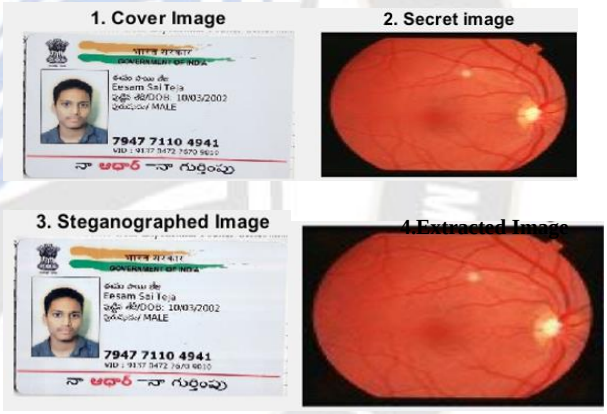
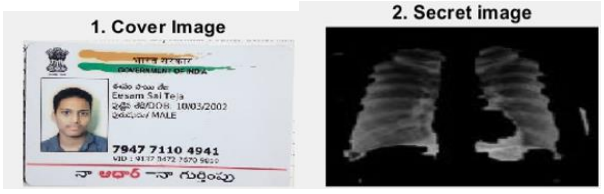


Figure 13. DWT method for IRIS image

This paper proposes the medical data hidden under the Aadhaar card as a cover image by using above-described algorithm and the extraction has been done with that algorithm. The DWT method embedded and extracted data such as MRI, CT scan, Iris, and X-ray images under a Aadhaar card are shown in Fig. 10, Fig. 11, Fig. 12 and Fig. 13.



4.Extracted Image

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

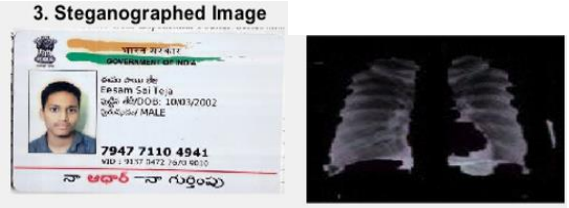


Figure 14. DWT method for X-ray

IV. Prepare Your Paper Before Styling

The performance of the 4 methods viz LSB, PVD, DCT, DWT, can be evaluated by using the performance metrics. There are various performance metrics in order to examine the performance of steganographic methods. The objective quality assessment of the image predicts the perceived image quality (26). The mostly used common distortion measures used to evaluate the quality of the image are peak signal to noise ratio (PSNR), mean square error (MSE) and structural similarity index measure (SSIM).

PSNR and MSE are most commonly used full reference metrics which uses a reference image for the evaluating. The PSNR measures the how close two images are related i.e., similarity between two images. The PSNR measured in decibels. The PSNR value should be high for a good method and it is low for the less efficient method (27). The PSNR can be defined as follows:

$$PSNR = 10 \log_{10} (R^2/MSE)$$

Where R is maximum range

MSE represents the cumulative error between two images. It is measured in percentage. The MSE is the statistical difference between the secret image and the extracted image. The MSE between two images can be defined as:

$$MSE=\frac{1}{MN}\sum_{n=0}^{M}\sum_{m=1}^{N}[g\hat{}(n,m)-g(n,m)]2$$

SSIM measures the perceptual difference between two images. It looks for the similarity within the pixels, it is defined as follows:

$$SSIM\ (x, y) =[L\ (x,y)]\alpha\ *[c\ (x,y)]\beta\ *[s\ (x,y)]\gamma$$

L is the luminance, c is the contrast, s is the structure

α, β, γ are the positive constants.

V. Results and Discussion

In this paper, the above-mentioned metrics are evaluated for the medical Images viz X-ray images, CT-scan images, Iris images and MRI images. These images are embedded under a cover image the Adhaar card takes as a cover image. 15 samples of each image are taken and embedded using different embedding algorithms namely LSB, DCT, DWT

The performance metrics calculated for each method and average values are compared and shown in table1,2, and 3. The PSNR, SSIM and MSE are calculated for those samples, from the obtained values the average values are calculated for each metric in the corresponding method. The comparison of the metrics with different modalities like CT, MRI, IRIS, X ray, CT Scan are shown.

TABLE 1: Average values of PSNR for medical images

Method	CT scan	Iris	MRI	X-ray
LSB	2.64	4.456	2.54	4.24
DCT	7.349	6.579	6.75	6.45
DWT	27.481	9.416	7.825	37.004

TABLE 2: Average values of MSE for medical images

Method	CT scan	Iris	MRI	X-ray
LSB	177.63	120.04	179.21	136.72
DCT	1.18	1.489	1.51	1.44
DWT	16.1	6.25	6.522	9.673

TABLE 3: Average values of SSIM for medical images

Method	CT scan	Iris	MRI	X-ray
LSB	0.089	0.18	0,13	0.259
DCT	0.27	0.077	0.54	0.29
DWT	0.55	0.71	0.86	0.75

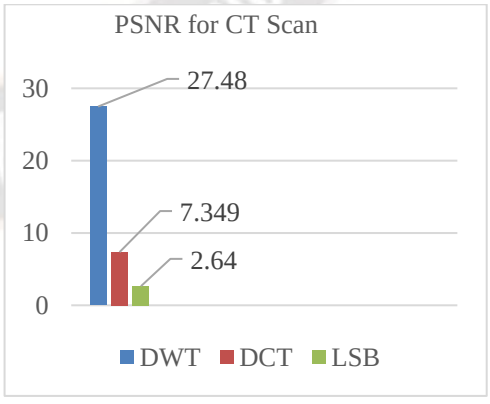


Figure 15. PSNR Values for CT Scan

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

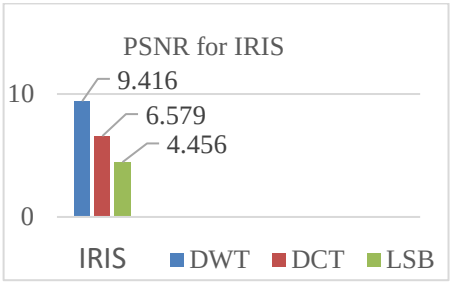


Figure 16. PSNR Values for IRIS

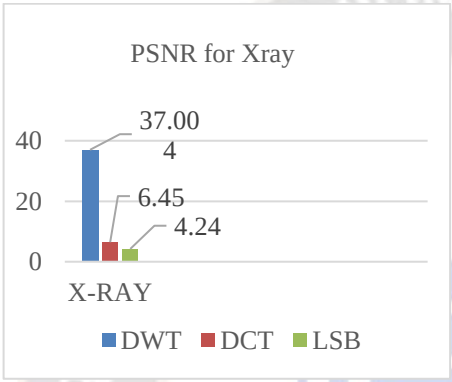


Figure 17. PSNRValues for CT Scan

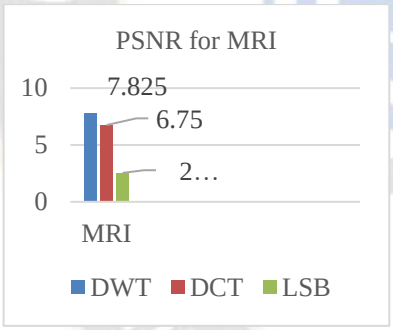


Figure 18. PSNR Values for MRI

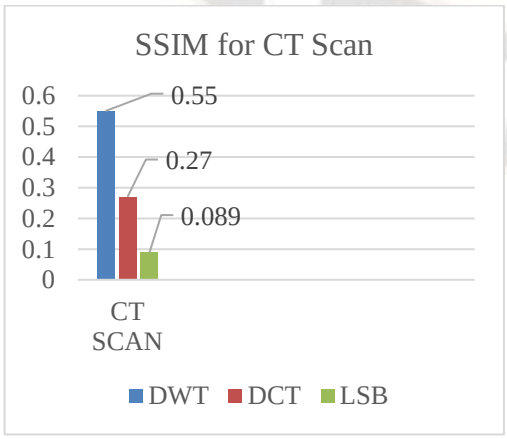


Figure 19. SSIM Values for MRI

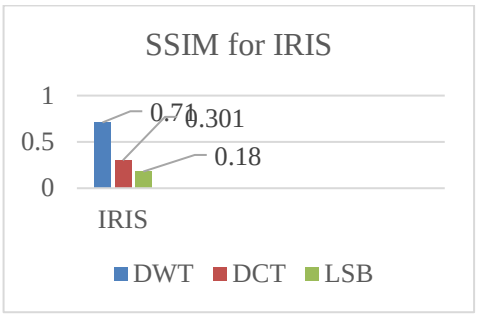


Figure 20. SSIM Values for IRIS

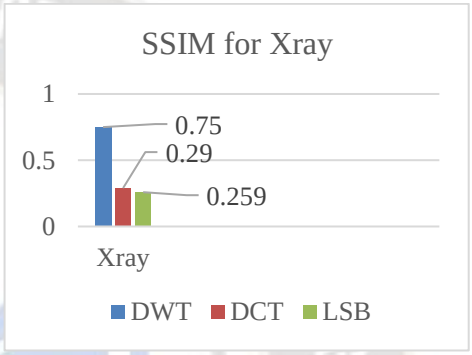


Figure 21. SSIM Values for X-Ray

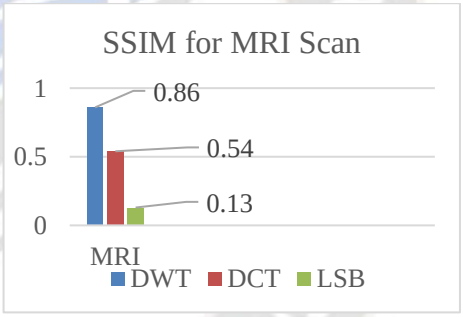
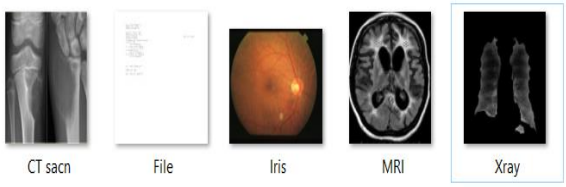


Figure 22. SSIM Values for MRI Scan

From the comparision method it is identified that DWT based is more accurate in all parameters. Hence, In this paper an attempt is made to store medical prescription (text file) ,CTScan, Iris,Mri,Xray is created as folder .The folder is hidden using the DWT method.The complete medical information of a patient is covered under a carrier image.T he secreat images which are strored and the extracted data are shown the Fig 14 as stegnographed data.

SECRET IMAGES:



International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

EXTRACTED IMAGES:

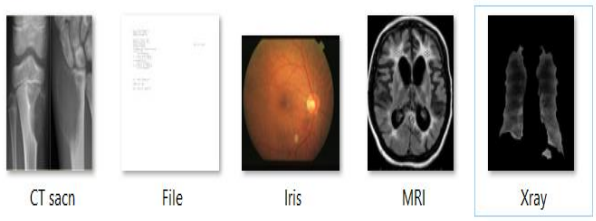


Fig. 22. DWT Based stegngrafed data

VI. Conclusion

Now a day's storage of medical data or carrying the medical file by a patient is one of the aspect in which the digital transformation is required. It is challenging task to have storage of medical data like, prescriptions, scans of different modalities are to be stored under one account authentication card. The digital image processing technique like steganography has performance of hiding the data under the cover image. Considering the advantage of stenographic techniques an attempt is made to find the best transformation technique that can be adopted for storage of medical data under one authentication. The three different techniques like LSB, PVD, DCT, DWT. It is observed that the LSB method is deviating with more loss of data though it is Robust. PVD method is though it is creating noise it is highly imperceptible to the human eye.

The DCT method algorithm allows to hide the individual image to conceal behind the cover image. The text file hiding is more complex. The performance measures are in the range of expected values, so this method provides the good robustness and imperceptibility to the human eye.

In DWT method allows to hide individual data and folder behind the cover image. This method performance measures are very close to the expected values, so it provides more robustness compared to the other methods. This method provides more embedding capacity and high imperceptibility to the human eye and also more secured.

It is realized that DWT is the more efficient method in the image steganography than the other methods. The performance measure's such as PSNR is high compared to other methods average values, SSIM is high for this method. DWT is more efficient method nearly 85% than the other methods.

Acknowledgment

The authors would like to thank Dept. of ECE, JNTUGV, Vizianagram, India for providing labs and software's.

References

[1] Al-Dmour Hayat, Ahmed Al-Ani. 2016. Quality optimized medical image information hiding algorithm that employs edge detection and data coding. Computer methods and programs in biomedicine.

[2] Cheng Yu-Ming, Chung-Ming Wang. 2009. A Novel Approach to Steganography in High-Dynamic-Range Images. IEEE Multi Media.

[3] Shie Shih-Chieh, Shinfeng D. 2009. Lin. Data hiding based on compressed VQ indices of images. Computer Standards & Interfaces.

[4] Jain Rupali, Jayshree Boaddh. 2016. Advances in digital image steganography. Innovation and Challenges in Cyber Security (ICICCS-INBUSH), 2016 International Conference.

[5] Lee Chin-Feng, Chin-Chen Chang et al. 2008. An improvement of EMD embedding method for large payloads by pixel segmentation strategy. Image and Vision Computing.

[6] Abuadbba, A., & Khalil, I. (2017). Walsh-Hadamard-based 3-D steganography for protecting sensitive information in point-of-care. IEEE Transactions on Biomedical Engineering, 64(9), 2186–2195.

[7] Altaay, A. A. J., Bin, S. S., & Zamani, M. (2012). An introduction to image steganography techniques. Proceedings - 2012 International Conference on Advanced Computer Science Applications And Technologies, ACSAT 2012, 122–126. Kuala Lumpur, Malaysia.

[8] Ansari, A. S., Mohammadi, M. S., & Parvez, M. T. (2020). A multiple-format steganography algorithm for color images.

[9] Baawi, S. S., Mokhtar, M. R., & Sulaiman, R. (2018). A comparative study on the advancement of text steganography techniques in digital media. ARPN Journal of Engineering and Applied Sciences.

[10] Gulia, S., Mukherjee, S., & Choudhury, T. (2016). An extensive literature survey on medical image steganography. CSI Transactions on ICT, 4(2–4), 293–298.

[11] Hu, D., Xu, H., Ma, Z., Zheng, S., & Li, B. (2018). A spatial image steganography method based on nonnegative matrix factorization.

[12] Muñoz, A., Carracedo, J., & Álvarez, I. A. (2010). Hiding short secret messages based on linguistic steganography and manual annotation. Proceedings - 10th IEEE international conference on computer and information technology, CIT2010, 7th IEEE International conference on embedded software and systems, ICESS-2010, ScalCom-2010, (Cit), 960–964. Bradford, West Yorkshire, UK

[13] Johnson Neil F, Sushil Jajodia. 1998. Exploring steganography: Seeing the unseen

[14] Datta Biswajita, Upasana Mukherjee et al. 2016. LSB Layer Independent Robust Steganography using Binary Addition. Procedia Computer Science.

[15] Fridrich Jessica, Miroslav Goljan et al. 2001. Reliable detection of LSB steganography in color and grayscale images. Proceedings of the 2001 workshop on Multimedia and security: new challenges.

[16] Chakraborty, S., Jalal, A. S., & Bhatnagar, C. (2017). LSB based non blind predictive edge adaptive image steganography. Multimedia Tools and Applications.

[17] Chandramouli, R., & Memon, N. (2001). Analysis of LSB based image steganography techniques. IEEE International Conference on Image Processing.

[18] Nilizadeh Amirfarhad, Ahmad Reza Naghsh Nilchi. 2016. A novel steganography method based on matrix pattern and LSB algorithms in RGB images. 1st Conference on Swarm Intelligence and Evolutionary Computation (CSIEC) .

[19] Kalita, M., & Tuithung, T. (2016). A novel steganographic method using 8-neighboring PVD (8nPVD) and LSB substitution. International

conference on systems, signals, and image processing, 2016-June, 6–10. Slovak University of Technology, Bratislava.

[20] Pan, F., Li, J., & Yang, X. (2011). Image steganography method based on PVD and modulus function. 2011 International Conference on Electronics, Communications and Control, ICECC 2011.

[21] Walia, E., & Jain, P. (2010). An Analysis of LSB & DCT based Steganography. Global Journal of Computer Science and Technology GJCST Computing Classification

[22] Behbahani Yasser M, Parham Ghayour et al. 2011. Eigenvalue Steganography based on eigen characteristics of quantized DCT matrices. Information Technology and Multimedia (ICIM).

[23] MAO Jiafa, HUANG Yanhong, NIU Xinxin et al. 2016. A method to estimate the steganographic capacity in DCT domain based on MCUU model. Wuhan University Journal of Natural Sciences.

[24] Mstafa, R. J., Elleithy, K. M., & Abdelfattah, E. (2017). A robust and secure video steganography method in DWT-DCT domains based on multiple object tracking and ECC. IEEE Access, 5(c), 5354–5365.

[25] Bhatnagar Gaurav, QM Jonathan Wu et al. 2013. Discrete fractional wavelet transform and its application to multiple encryptions. Information Sciences.

[26] Islam, S., & Gupta, P. (2014). Robust edge based image steganography through pixel intensity adjustment. Proceedings - 16th IEEE International Conference on High Performance Computing and Communications, HPCC 2014, 11th IEEE International Conference on Embedded Software and Systems, ICESS 2014 and 6th International Symposium on Cyberspace Safety and Security.

[27] Zhou, W., Zhang, W., & Yu, N. (2017). A new rule for cost reassignment in adaptive steganography. IEEE Transactions on Information Forensics and Security