IOT devices based improved cryptosystem for secure image sharing

Budida Harikranth, Venkatakrishna Adla, Lingamaiah Malle

Department of Electrical and Electronics Engineering

Sree Dattha Group of Institutions, Hyderabad, Telangana, India.

Abstract

The security and integrity of medical data have become major problems for healthcare services applications due to the considerable growth of the internet of things (IoT) in the healthcare industry. For protecting diagnostic text data in medical pictures, this study offers a hybrid security architecture. The suggested model is created by combining a proposed hybrid encryption method with either 2D-Discrete Wavelet Transform 1 Level (2D-DWT-1L) or 2D-DWT-2L steganography. The Advanced Encryption Standard (AES) and Rivest, Shamir, and Adleman (RSA) algorithms are combined in the proposed hybrid encryption scheme. The Advanced Encryption Standard (AES) and Rivest, Shamir, and Adleman (RSA) algorithms are combined in the proposed hybrid encryption scheme. The suggested methodology encrypts the secret data first, then uses 2D-DWT-1L or 2D-DWT-2L to conceal the result in a cover picture. To hide varying text sizes, cover pictures in both colour and grayscale are utilized. The results of the experiments demonstrate that the suggested picture steganography approach achieves a reasonable balance of resilience and invisibility, even for messages of various sizes.

Keywords: Rivest, Shamir, and Adleman, Advanced Encryption Standard, Redundant Discrete Wavelet Transform.

1. Introduction

Growing use of the Internet and exchange of information electronically has resulted into ever increasing need for security services specific to the type of data or information being protected. Authentication and non-repudiation are two major services of information security and digital steganogrphy is a commonly used method. Data in the form of multimedia content is exploding and hence digital image steganogrphy is an active research area. Transform domain methods for image steganogrphy are popular for robustness and imperceptibility. A lot of applications like digital copyrights management and protection make digital image steganogrphy a very active research field. The Internet has made it easy for people to share, promote and sell their intellectual property such as images, videos, documents, etc. The high pace emergence in technologies and associated computing approaches have given rise to a broad horizon serving an array of applications among which medical image communication is a dominating one. In present day health care system, biomedical image transmission has become one of the inevitable needs to ensure efficient seamless and secure data transmission over uncertain channels. Presently, the telemedicine field has gained impressive momentum which has enabled efficient and timely diagnosis remotely. However, the probable adversaries, caused due to (image) information deviation, could not be ignored.

Thus, exposing significant information. This key information could be accessed by any party without having access rights and this as a result could cause misuse. Interestingly, in telemedicine applications ensuring intact image attribute and key information is inevitable. In such applications retaining image information intact during transmission throughout the channel is a must. With this motivation, several

efforts have been made to enable data security during transmission. However, with specific medical image information security data hiding or data embedding approaches have gained widespread attention.

2. Literature survey

This section presents some of the key works discussing medical data security using steganography (say, medical image steganography (MIS) and various associated technologies. In recent years, the significance of telemedicine has been realized globally and hence it has emerged as one of the dominating research domains across academia-industries. However, to ensure seamless and flawless processes, maintaining optimal medical data security is a must. Steganography, being one of the most efficient approaches for medical data security applied image transformation schemes to embed critical data embedding within cover image (i.e., medical image). In fact, the efficiency of reversible steganography techniques significantly relies on the efficacy of image transformation, data embedding and pixel adjustment to enable maximum imperceptibility.

In most of the existing approaches integer wavelet transform techniques (IWT) or wavelet transformation approaches have been applied [8][9][10][11] for steganography. In [8], authors developed a real-time data embedding model using IWT technique where it was applied in the transform domain. Being an image compression-based approach authors have applied IWT as it outputs in the integer form and hence consumes low memory space.

In [12], authors applied IWT based steganography for medical image security. Authors focussed on converting multiple medical images into single one where the cover image was processed with left-flipping and a dummy cover image was generated. Authors considered the patient's medical diagnosis image as the secret image and to retrieve the scrambled image they applied Arnold transform. In process, the scrambled medical diagnostic image (i.e., secret image) was embedded into the dummy cover image and IWT was applied to obtain the dummy secret image. In the next phase, authors fused the cover image with the dummy secret image to obtain stego-image. However, the computational overheads of such techniques can’t be ignored.

Authors in [10], derived a reversible data hiding or critical data embedding approach using compressive-steganography technique. Authors applied wavelet transform technique to exhibit data embedding; however, could not address the distortion caused due to compression and its effect on the hiding capacity. To further enhance compression based reversible steganography for medical data security over uncertain transmission channel, a low distortion reversible data hiding scheme was developed in [13], where authors compressed a fixed section of the signal, which is prone to get distorted. Tian [11] applied pixel value difference expansion approach to enable a high-capacity reversible data embedding for image steganography. However, authors could not address the aftermath consequences leading to vulnerability towards attacks.

Similarly, in [14] [15] a Difference Expansion (DE) embedding model was applied where authors exploited HAAR wavelet transform by using horizontal as well as vertical difference images to perform secret data hiding. Authors [15] found that DE along with sophisticated location map with enhanced expandability could achieve higher embedding capacity.

With goal to exploit histogram-based approaches for steganography, authors [16] applied a histogram shifting approach that shifts (by one pixel) a fraction of the histogram parts in between the peak and the zero level to the right direction. This as a result created an empty bin in conjunction with the peak point

where they hide data. Similarly, in [17], a histogram modification model was incorporated where authors modified histogram on pixel differences that similar to [16] forms sufficient place to hide data. However, these approaches could not address the attack conditions, especially statistical attacks in channel.

Authors [18] focused on medical data confidentiality issue through steganography where the cover images were at first transformed into onedimensional sequence by means of Hilbert filling curve, which was then processed for splitting into non-overlapping clusters of three pixels in each. To enrich imperceptibility, authors applied adaptive pixel pair match (APPM) based data embedding, where pixel value differences (PVD) of the three pixels individually is retrieved and data is embedded in those pixel ternaries. This as a result causes low distortion and hence high imperceptibility. Considering efficacy of LSB embedding, authors [19] developed a LSB matching model where data hiding was performed in the edges and the pixel bits of the secret message were matched with the LSB plane.

In [20] a fuzzy logic-based steganography model was proposed for medical diagnostic image security. Authors applied random LSB selection-based approach to hide the secret data. Authors applied personal data and the diagnostic suggestions as secret information that was compressed and encrypted to enable attack resiliency. However, this approach might be complicated. In [21] authors derived a data hiding model for 3D MRI images, where at first, they applied segmentation to perform region localization followed by LSB embedding.

3. Proposed Method

In this work, we present a healthcare security model for protecting medical data transmission in Internet of Things (IoT) contexts. The suggested model is made up of four separate processes:

- The sensitive patient's data is encrypted using a suggested hybrid encryption method that combines AES and RSA encryption algorithms.
- The encrypted data is hidden in a cover picture using either 2D-DWT-1L or 2D-DWT-2L, resulting in a stego-image.

To recover the original data, the extracted data is decrypted. The overall structure of our suggested methodology for safeguarding medical data transmission at both the source and destination sides is shown in Figure 1.

A. Data Encryption Scheme

The cryptographic scheme is implemented in the suggested model. Encryption and decoding operations make up the cryptographic system. The plain text T is split into odd and even pieces throughout the encryption process. The AES algorithm encrypts data using a secret public key. The RSA algorithm encrypts data with a secret public key m. To improve the security level, the private key x utilized in the decryption process at the receiver side is encrypted using the AES method and delivered to the receiver in an encrypted form. The following equations can be used to mathematically model the encryption process.

$$C = \{'E_{AES}, 'E_{RSA}, T_{odd}, T_{even}, \dot{T}_{odd}, \dot{T}_{even}, s, m, x\} \quad (1)$$

$$\dot{T}_{odd} = \{'E_{AES}(T_{odd}, s)\} \quad (2)$$

$$\dot{T}_{even} = \{'E_{RSA}(T_{even}, m)\} \quad (3)$$

$$\dot{X} = \{'E_{AES}(x, s)\} \quad (4)$$

The encryption algorithm is detailed in the next section.

Algorithm (1): Hybrid (AES & RSA) Algorithm.
Inputs: secret plain Stext message.
Output: main_cipher message , key s
Begin
1. Divide plain msg into two parts (Odd_Msg, Even_Msg)
2. Generate new AES key s
3. EncOdd = AES-128 (Odd_Msg, s)
4. Generate new RSA key (public = m) and (private = x)
5. EncEven = RSA (Even_Msg, m)
6. Build FullEncTxt by inserting both EncOdd and EncEven in their indices
7. EncKey = AES-128 (x, s)
8. Compress FullEncMsg by convert to hashs
9. Compress EncKey by convert to hashs
10. Define message empty main_cipher = ""
11. main_cipher = Concatenate (FullEncMsg, EncKey)
12. Return main_cipher and s

End

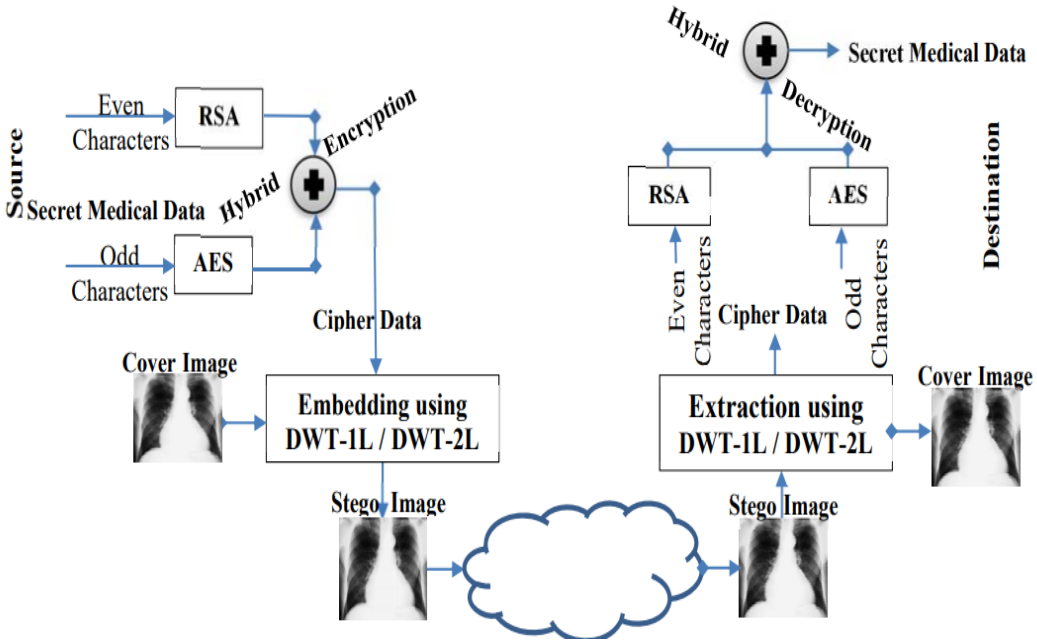


Figure 1: The suggested architecture for protecting the transfer of medical data.

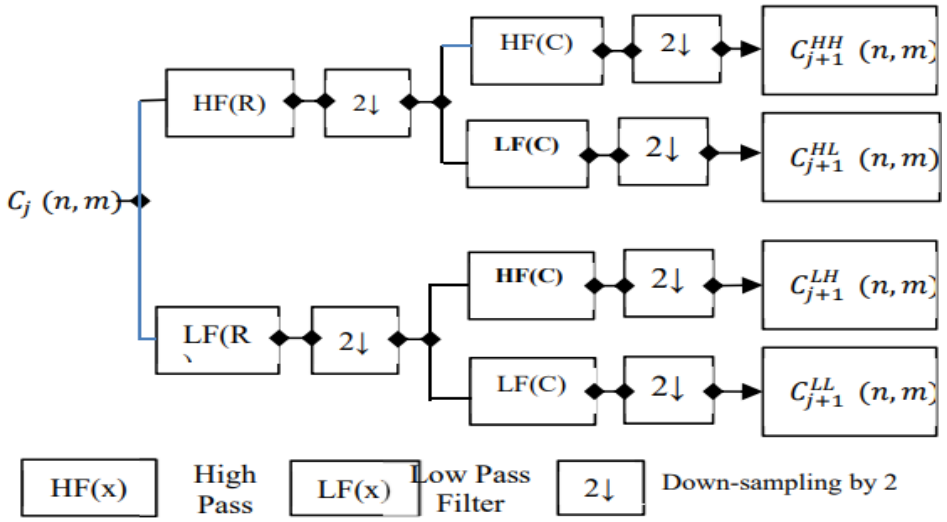


Figure 2: The DWT-2L decomposition method.

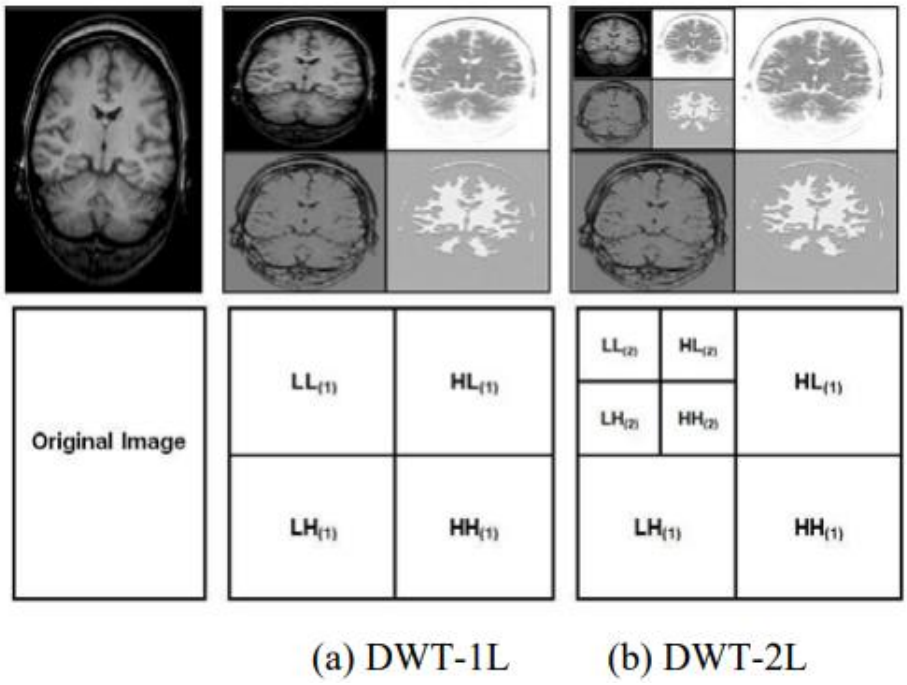


Figure 3: The DWT-2L technique of decomposition.

B. Embedding Procedure

The 2D-DWT-2L, like Haar-DWT, may be defined as a sequential transformation employing low-pass and high-pass filters along the image's rows, with the output dissected along the image's columns [21]. This procedure is seen in Figure 2. The elemental breakdown process for Cimage of size N x M is shown in Fig. 2 as four decomposed subband pictures referred to as high-high (HH), high-low (HL), low-high (LH), and low-low (LL). The effect of the decomposition procedure on the image is seen in Figure 3.

The steganographic approach is implemented in the suggested paradigm. The embedding and extraction operations make up the steganographic. The embedding method creates a stego-picture S from a cover image C and a hidden text message T. The embedded message is extracted in reverse during the extraction procedure. It may be mathematically described using the equations shown below.

$$\hat{S} = \{= \{f\eta, f\eta^{-1}, C, S, T\} \quad (5)$$
$$S = \{f\eta(C, T)\} \quad (6)$$
$$T = \{f\eta^{-1}(S)\} \quad (7)$$

Algorithm (2): Embedding 2D-DWT-2L Algorithm.
Inputs: cover image, a secret message (main_cipher and s).
Output: stego image.
Begin
1. Convert the secret message in ASCII Code as asciiMsg
2. Divide asciiMsg to odd and even
3. Scan the image row by row as img
4. Compute the 2D wavelet for the first level by harr filter that generates (LL1), (HL1), (LH1), and (HH1)
5. Compute the 2D wavelet for the second level by harr filter that generates (LL2), (HL2), (LH2), and (HH2)
6. Loop
   6.1 Hide odd values in vertical coefficient, set LH2(x,y) = odd values
   6.2 Hide even values in vertical coefficient, set HH2(x,y) = even values
7. End Loop
8. Return Stego image
End.

The secret text is converted to ASCII format and then split into even and odd values during the embedding procedure. LH2 mentions vertical coefficients, which hide the odd values. The HH2 specifies diagonal coefficients that hide the even values. The algorithm utilized by evolved 2D-DWT-2L in the embedding operation is given below in algorithm 2.

C. Extraction Procedure

The 2DDWT-2L method is used to extract the secret message and recover the cover picture after the text has been incorporated into the cover image. Below is a description of the extraction algorithm.

Algorithm (3): Extraction algorithm.
Inputs: stego image
Output: Retrieved secret message and original cover image
Begin
1. Scan the stego image row by row
2. Compute the 2D wavelet for the first level by harr filter
3. Compute the 2D wavelet for the second level by harr filter
4. Prepare msg = ""
5. Loop
   5.1 Extract the text embedded in vertical coefficient, set odd values =LH2(x,y)
   5.2 Extract the text embedded in vertical coefficient, set even values = HH2(x,y)
6. End Loop
7. msg = Append (odd values, even values)
8. Compute idwt2 for the constructed approximation that generates the original image
9. Return msg as a retrieved secret message and original cover image

The cover image is generated from the reconstructed approximation by invoking the iDWT2 for the second level and then for the first level [21] after the secret text message has been retrieved. The fundamental DWT synthesis method is depicted in Figure 4.

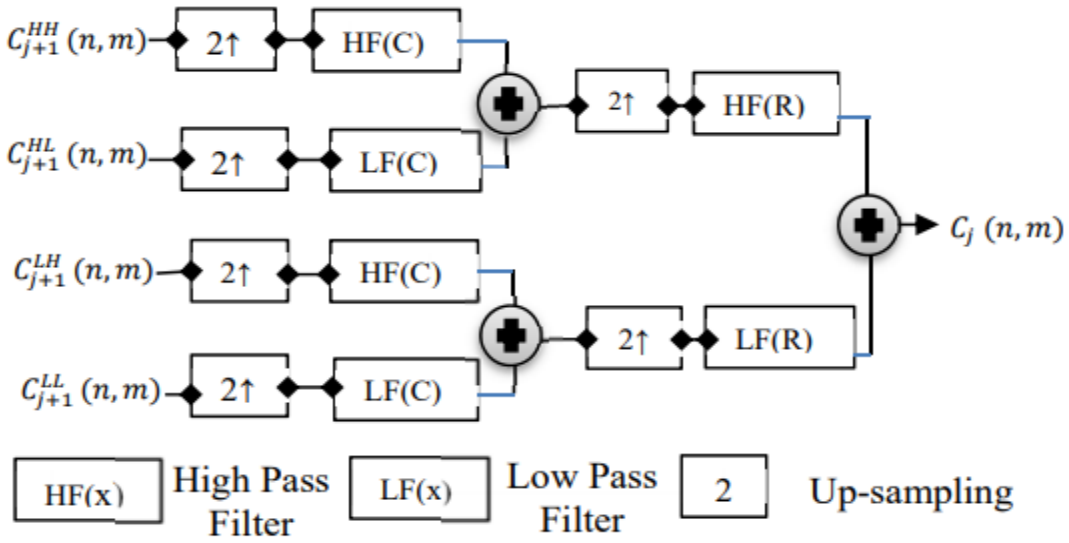


Fig. 4. The synthesis process of 2D-DWT-2L.

D. Data Encryption Scheme

Decryption refers to the process of converting the encrypted data back to the user in a well-known format, which is the reverse of the encryption process. The same key used by the sender has to be used over the cipher-text throughout the encryption process. The decryption process can be mathematically expressed as given in the following equations below.

$$\hat{C} = \{ \acute{E}_{AES}^{-1}, \acute{E}_{RSA}^{-1}, T_{odd}, T_{even}, \dot{T}_{odd}, \dot{T}_{even}, s, x \quad (8)$$

$$x = \{\acute{E}_{AES}(\dot{X}, s)\} \quad (9)$$

$$T_{even} = \{\acute{E}_{RSA}^{-1}(\dot{T}_{even}, x)\} \quad (10)$$

$$T_{odd} = \{\acute{E}_{AES}^{-1}(\dot{T}_{odd}, s)\} \quad (11)$$

Algorithm (4): Hybrid Decryption (AES & RSA) Algorithm.
Inputs: main_cipher (secret) message , key
Output: secret (plain, text) message.
Begin
1. Divide main_cipher into two parts; HashedTxt and HashedKey
2. FullEncMsg = Decompress (HashedTxt)
3. EncKey = Decompress (HashedKey)
4. x = Decrypt_AES-128 (EncKey, s)
5. EncOdd = Split (FullEncMsg, odd)
6. EncEven = Split (FullEncMsg, even)
7. Odd_Msg = Decrypt_ AES-128 (EncOdd, s)
8. Even_Msg = Decrypt_ RSA (EncEven, x)
9. Define main_plain message
10. Loop on All Char
    10.1 If odd
        Insert odd characters into odd indices within main_plain message
    10.2 Else
        Insert even characters into even indices within main_plain message
11. End of Loop
12. Return main_plain (text) message

End

4. Results

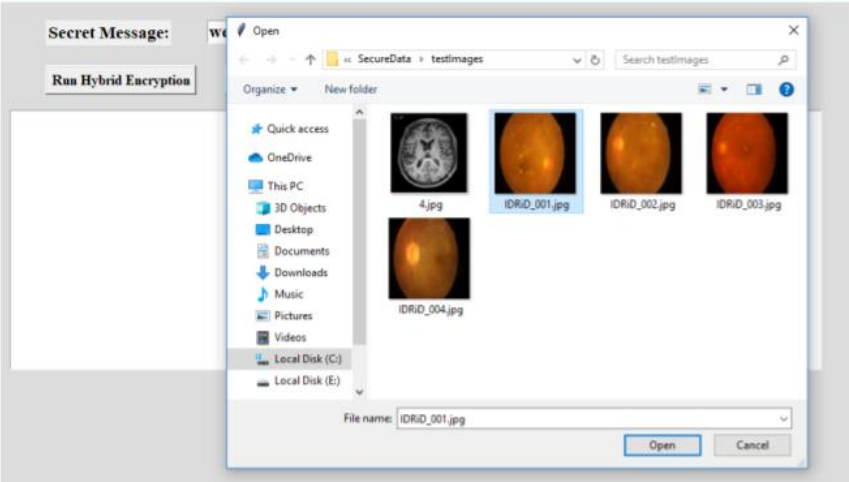
The invisibility and robustness of the suggested technique are examined in this section. To begin, the best adaptive scaling factor for watermarks with different sizes is determined by analyzing the scaling factor across NC, PSNR, and SSIM. In the trials, the adaptive optimum scaling factors of watermarks with different sizes are employed. Subjective eye observation and objective quantitative analysis are used to detect the suggested method's invisibility and resilience. Furthermore, a variety of assaults with varying characteristics are employed to test the resilience. Finally, the suggested method's invisibility and robustness are compared to previous studies.

Step 1: To run project double click on ‘run.bat’ file to get below screen. In screen enter some message in ‘Secret Message’ field.

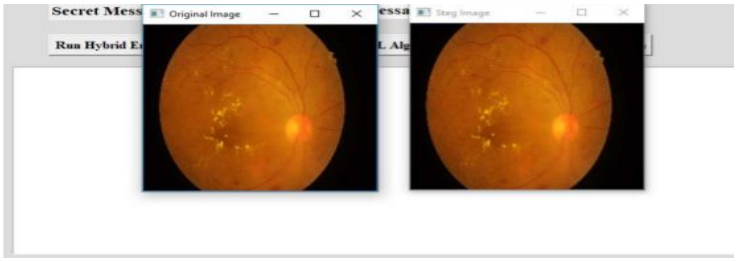
Step 2: In below screen enter some message and then click on 'Run Hybrid Encryption' button to encrypt message using RSA and AES.

Step 3: In below screen displaying complete message with ODD And EVEN parts and then encrypting both parts with AES and RSA and now message is ready and now click on 'Embedding 2d-DT-2L Algorithm' button to upload image and then hide that encrypted message.

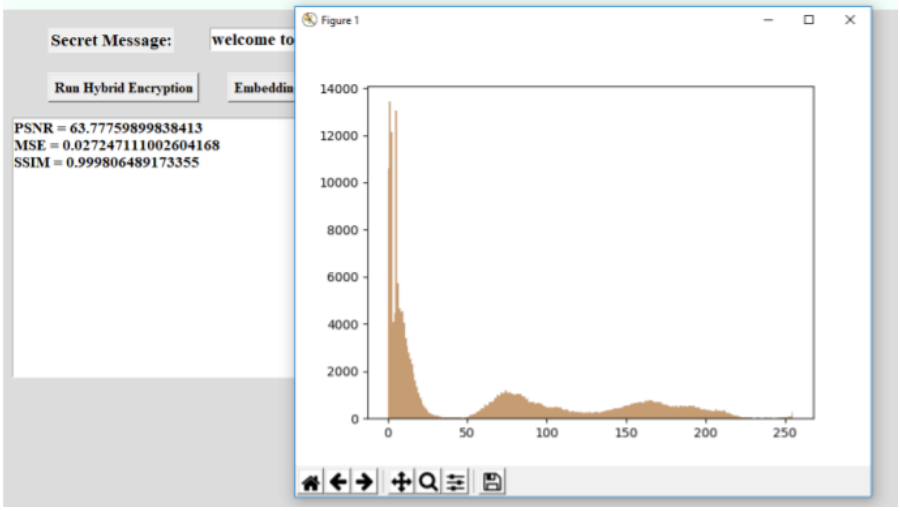
Step 4: In below screen I am selecting one image and it has both colour and grey images and now click on 'Open' button to get below output



Step 5: In below screen first image is the original image and second image contains steganography hidden message and both messages look similar and now close both images to get below histogram graph of both images



Step 6: In above histogram we can see both images are showing equal size bars show after hiding message not much change we can see in Steg image and in above screen in text area we got PSNR as 63% which is more than paper and MSE 0.027 which is less than paper and we got SSIM as 0.99 which is slight lower than paper output as in paper author getting 1 as SSIM. So from above output we are getting close output compare to paper. Similarly, you can upload other images and test. Now click on 'Extraction Algorithm' button to extract and decrypt message from image.



Step 7: In below screen in text area, we extracted encrypted message and then decrypt that message to get original content.

Table 1. Performance comparison

Method	PSNR	SSIM	MSE
DWT [11]	42.48	0.9746	0.085
DWT-DCT [13]	52.497	0.9846	0.0636
Proposed	63.77	1	0.027

From Table 1, it is observed that the proposed method resulted in superior performance as compared to the DWT [11], DWT-DCT [13] methods.

5. Conclusion

For a healthcare-based IoT context, a secure patient diagnostic data transfer model employing both color and gray-scale pictures as a cover carrier has been proposed. The suggested model used 2D-DWT-1L or 2D-DWT-2L steganography, as well as a mix of AES and RSA cryptography. A unique picture steganography approach based on DWT-HD-SVD transformations is proposed in this paper. The FOA is specifically used to determine the best scaling factor. Numerical simulation tests are used to examine the method's invisibility and resilience, and the findings demonstrate that the stego host pictures have high visual quality, PSNRs, and SSIMs. Furthermore, with reasonably high NCs, the messages may be clearly retrieved from the stego host picture against various assaults. Furthermore, the suggested image steganography approach may achieve high invisibility and resilience even for messages of various sizes. In addition, a comparison with comparable studies is provided, and the metric values demonstrate that the suggested technique performs better in terms of robustness for the majority of assaults. It's worth mentioning that the suggested technique is extremely resilient to attacks on the filter, noise, JPEG compression, JPEG2000 compression, and sharpening. In future research, the suggested steganography approach may need to pay more attention to repelling additional attacks, such as rotation and cropping attacks. Furthermore, if the enhanced FOA method is used, the steganography performance may be increased even further.

References

[1] T. Moerland. Steganography and Steganalysis. [Online]. Available: www.liacs.nl/home/ tmoerl/privtech.pdf.
[2] M. Mohan and P. R. Anurenjan, “A Novel Data Hiding Method in Image using Contourlet Transform,” Recent Advances in Intelligent Computational Systems (RAICS), 2011.
[3] A. Cheddad, J. Condell, K. Curran, and P. Kevitt, “Digital image steganography – survey and analysis of current methods”, J. Signal Processing, Vol. 90, No. 3, 2010, pp.752–825.
[4] R. Gonzalez, and R. Woods, “Digital Image Processing,” 2nd ed., Prentice Hall, PHI. 2001.
[5] W. Chen, “A comparative study of information hiding schemes using amplitude, frequency and phase embedding,” PhD thesis, National Cheng Kung University, Taiwan, May 2003.

[6] C. K. Chan and L. M. Chang, "Hiding data in images by simple LSB substitution," Pattern Recognition, Mar. 2004, pp. 469-474.

[7] J. Xu, L. Yang, and D. Wu, "Ripplet: a new transform for image processing," J. Vis. Commun. Image R, Vol. 21, No. 1, 2010, pp.627–639.

[8] S. Lavania, P. S. Matey and V. Thanikaiselvan, "Real-time implementation of steganography in medical images using integer wavelet transform," IEEE International Conference on Computational Intelligence and Computing Research, Coimbatore, 2014, pp. 1-5.

[9] G, P., R, D. B., & S, R. P. "Multi Secure and Robustness for Medical Image based Steganography scheme," International Conference on Circuits, Power and Computing Technologies, 2013, pp. 1188-1193.

[10] J. M. Barton, "Method and Apparatus for Embedding Authentication Information within Digital Data," U.S. Patent 5646997, 1997

[11] J. Tian, "Reversible data embedding using a difference expansion," IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890-896, Aug. 2003.

[12] G. Prabakaran, R. Bhavani and P. S. Rajeswari, "Multi secure and robustness for medical image-based steganography scheme," International Conference on Circuits, Power and Computing Technologies (ICCPCT), Nagercoil, 2013, pp. 1188- 1193.

[13] M.U. Celik, G. Sharma, A.M. Tekalp, and E. Saber, "Reversible data hiding," in Proc. Int. Conf. Image Processing, vol. II, Sept. 2002, pp 157-160.

[14] Y. Hu, "Difference Expansion based Reversible data hiding using two embedding directions," IEEE Trans.On Multimedia, vol.10, no. 8, Dec. 2008.

[15] H. J. Kim, V. Sachnev, Y.Q. Shi, "A novel difference expansion transform for reversible data embedding." IEEE Trans. Inf. Forensic Secur., vol. 3, no. 3, pp. 456-465, Sep 2008

[16] Z. Ni, Y. Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," IEEE Trans. Circuits Syst. Video Technol., vol. 16, no.3. pp. 354-362, Mar, 2006.

[17] W. Tai, C. Yeh, C. Chang, "Reversible data hiding based on histogram modification of pixel differences," IEEE Trans. On Circuits and Systems for Video Technol., vol. 19, no.6, June 2009

[18] J. Liu, G. Tang, and Y. Sun, "A secure steganography for privacy protection in healthcare system". Journal of Medical Systems, Vol. 37, No. 2, 2013.

[19] W. Luo, F. Huang, and J. Huang, 'Edge adaptive image steganography based on LSB matching revisited', IEEE Transactions on Information Forensics and Security, Vol. 5 No. 2, pp.201–214, 2010.

[20] R. Karakış, İ. Güler, İ. Çapraz and E. Bilir, "A new method of fuzzy logic-based steganography for the security of medical images," 23nd Signal Processing and Communications Applications Conference (SIU), Malatya, 2015, pp. 272-275.