History of Medicine, 2020, 6(1): 12-25

DOI:10.48047.v6.2.2020.2

ENHANCING MEDICAL DATA SECURITY IN IOT HEALTHCARE: A HYBRID AES-RSA ENCRYPTION APPROACH WITH 2D-DWT STEGANOGRAPHY

Senthil Kumar Murugesan[1], Akula Rajini[1], Kunsoth Umarani[1]

[1]Department of Electronics and Communication Engineering

[1]Sree Dattha Group of Institutions, Sheriguda, Hyderabad, Telangana.

Abstract

There have been substantial issues brought about in terms of the security and integrity of medical data as a result of the ever-increasing use of the Internet of Things (IoT) in the healthcare industry. In this research, a unique way to addressing these problems is presented. The technique involves the proposal of a hybrid security architecture for the purpose of protecting diagnostic text data contained within medical images. The suggested model incorporates a one-of-a-kind hybrid encryption strategy in addition to steganography approaches that utilize the 2D Discrete Wavelet Transform (2D-DWT), more especially the 2D-DWT-1 Level and the 2D-DWT-2 Level technologies. The Advanced Encryption Standard (AES) and the Rivest-Shamir-Adleman (RSA) algorithms, which are frequently utilized, are combined in this encryption scheme. The workflow of the suggested model begins with the encryption of sensitive data, which is then followed by the concealment of the encrypted result within a cover image by employing either the 2D-DWT-1 Level or the 2D-DWT-2 Level steganography techniques. When it comes to cover images, both color and grayscale images are utilized. This allows for a wider range of text sizes to be accommodated, which in turn ensures increased data safety and security.

Keywords: Advanced Encryption Standard (AES), Rivest-Shamir-Adleman (RSA), Internet of Things, Discrete Wavelet Transform, Healthcare Security, Data Encryption, Steganography

1. Introduction

In recent years, the healthcare industry has shown rapid growth and has been a major contributor to revenue and employment. A few years ago, the diagnosis of diseases and abnormality in the human body was only possible after having a physical analysis [1] in the hospital. Most of the patients had to stay in the hospital throughout their treatment period. This resulted in an increased healthcare cost and strained the healthcare facility at rural and remote locations. The technological advancement that has been achieved through these years has now allowed the diagnosis of various diseases and health monitoring using miniaturized devices [2] like smartwatches. Moreover, technology has transformed a hospital-centric healthcare system into a patient-centric system. For example, several clinical analyses (such as measuring blood pressure, blood glucose level, pO2, level, and so on) can be performed at home without the help of a healthcare professional [3]. Further, clinical data can be communicated to healthcare centers from remote areas with the help of advanced telecommunication services. The use of such communication services in conjunction with the rapidly growing technologies (e.g., machine learning, big data analysis, Internet of things (IoT), wireless sensing, mobile computing, and cloud computing) has improved [4] the accessibility of the healthcare facilities. IoT creates an integrated communication environment of interconnected devices and platforms by engaging both virtual and physical world together [5]. With the advent of remote digital healthcare based IoT systems, the transmission of medical data has become a daily routine. Therefore, it is necessary to develop an efficient model to ensure the security and integrity of the patient's diagnostic data transmitted and received from IoT environment. This goal is carried out using steganography techniques and system encryption algorithms together to hide digital information in an image.

IoT has not only enhanced independence but also diversified the ability of humans to interact with the external environment [6]. IoT, with help of futuristic protocol and algorithms, became a major contributor to global communication. It connects many devices, wireless sensors, home appliances, and electronic devices to the Internet. The application of IoT can be found in the field of agriculture, automobiles, home, and healthcare [7]. The growing popularity of the IoT is due to its advantage of show agriculture, automobiles ser cost, and its ability to predict future events in a better way. Further, increased knowledge of software and applications, with the upgradation of mobile and computer technologies, easy availability of wireless technology, and the increased [8] digital economy have added to the rapid IoT revolution. The IoT devices (sensors, actuators, and so on) have been integrated with other physical devices to monitor and exchange information using different communication protocols such as Bluetooth, Zigbee, IEEE 802.11 (Wi-Fi), and so on [9]. In healthcare applications, the sensors, either embedded or wearable on the human body, are used to collect physiological information such as temperature, pressure rate, electrocardiograph (ECG), electroencephalograph (EEG), and so on from the patient's body. Additionally, environmental information such as temperature, humidity, date, and time can also be recorded [10]. These data help in making meaningful and precise inferences on the health conditions of the patients. Data storage and accessibility also play an important role in the IoT system as a large amount of data is acquired/recorded from a variety of sources (sensors, mobile phones, e-mail, software, and applications).

Rest of the paper is organized as follows: Section 2 details about literature survey, section 3 details about the proposed methodology, section 4 details about the results with discussion, and section 5 concludes article with references.

2. Literature Survey

In [11] surveyed various healthcare applications based on wireless medical sensor network (WMSN) that can be implemented in IoT environment. Also, discussed the security techniques that are used for handling the security issues of healthcare systems, especially hybrid security techniques. In [12] Proposed system first compresses data with run-length encoding technique then encrypt it using the AES method but with a rotated key then the source transfers the encoded and encrypted data to the destination where the data is decrypted then decoded to restore the original data then the original data is upload to the destination's website. In [13] presented an algorithm based on dividing the original image to the group of blocks, where these blocks are arranged in the form of turns using a transformation algorithm. After that, the transformed image is encrypted using the Blowfish algorithm. It was found that the correlation decreases, and the entropy increases by increasing the number of blocks through using smaller block sizes. In [14] Internet of things (IoT) is a new paradigm that combines several technologies such as computers, Internet, sensor networks, radio frequency identification (RFID), communication technology and embedded systems to form a system that links the real world with digital world. Currently, many smart objects and different type of devices are interconnected and more and more they are being used in Ambient Assisted Living (AAL) scenarios for improving the daily tasks of elderly and disabled people. Presented an IoT architecture and protocol for Ambient Assisted Living and e-health. It is designed for heterogeneous AAL and e-health scenarios where an IoT network is the most suitable option to interconnect all elements. In [15] proposed a medical integrity verification system to improve the security of medical image. The proposed system mainly decomposed into two stages: 1) the protection and 2) the verification. Through the protection stage, the binary form of the secret data is embedded in the high-frequency part (HH) within the cover image using 2D Haar DWT frequency domain technique. Through the verification stage, the extraction algorithm is applied to retrieve the original cover image and secret data.

In [16] Presented a combined image of the most significant function as well as services obtainable by Health Monitoring System method (HMS) for the detecting and monitoring human behavior. It is counting its processing techniques, approaches, and concepts etc. Furthermore, it is provided a general, in detail study and assessment of the obtainable research conclusion in the field of e- health systems through IoT. In [17] proposed an image encryption technique based on the integration of shifted image blocks and the basic AES. The shifted algorithm technique is used to divide the image into blocks. Each block consists of many pixels, and these blocks are shuffled by utilizing a shift technique that moves the rows and columns of the original image in such a way to produce a shifted image. This shifted image is then used as an input image to the AES algorithm to encrypt the pixels of the shifted image. In [18] proposed an efficient, secure method for RGB images based on gray level modification (GLM) and multi-level encryption (MLE). The secret key and the secret data are encrypted using MLE algorithm before mapping it to the gray-levels of the cover image. Then, a transposition function is applied to the cover image before data hiding. The usage of transpose, secret key, MLE, and GLM adds four different levels of security to the proposed algorithm, making it very difficult for a malicious user to extract the original secret information. In [19] Data Networking (NDN) represents a promising future networking paradigm fitting perfectly with the requirements of IoT applications and especially those related to security and privacy. In this paper, we leverage the basic feats of NDN vision for designing a robust privacy preserving NDN-based e-health IoT system (PP-NDNoT). It ensures security and fulfills content and contextual privacy requirements. In [20] proposed an image steganography approach based on Inverted LSB (ILSB) technique for securing the transmitted face images from the IP camera as the IoT device to the home server in the LAN network. The local home server serves as a processing power node for the encryption of the stego images before transmitting them to the cloud and other devices for further processing.

3. Proposed Methodology

3.1 Proposed Model

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.

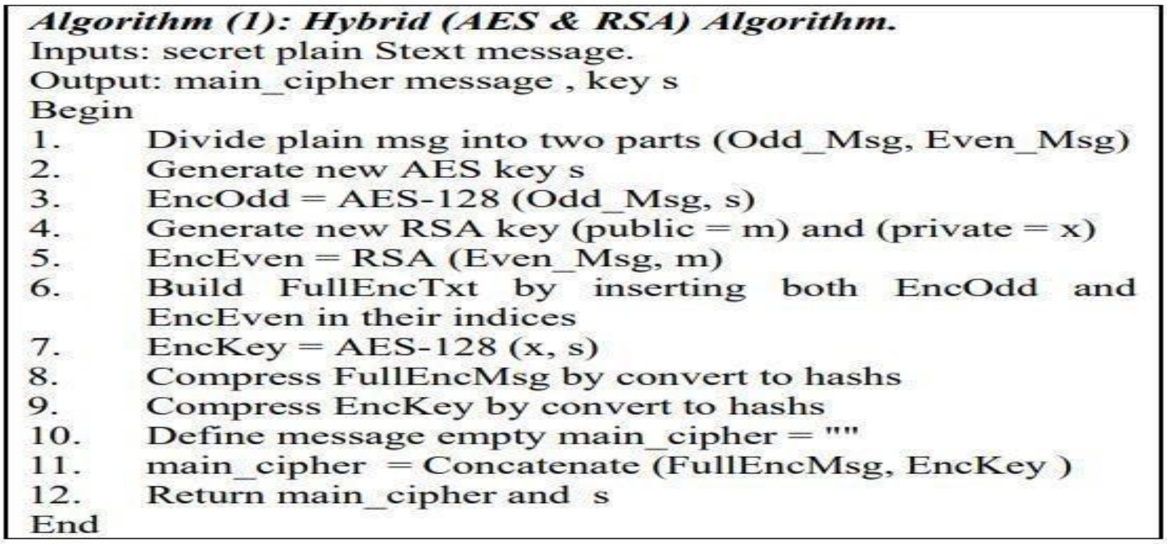
$$C = \{{}'E_{AES}, {}'E_{RSA}, T_{odd}, T_{even}, \dot{T}_{odd}, \dot{T}_{even}, s, m, x\} \qquad (1)$$

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

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

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

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
```

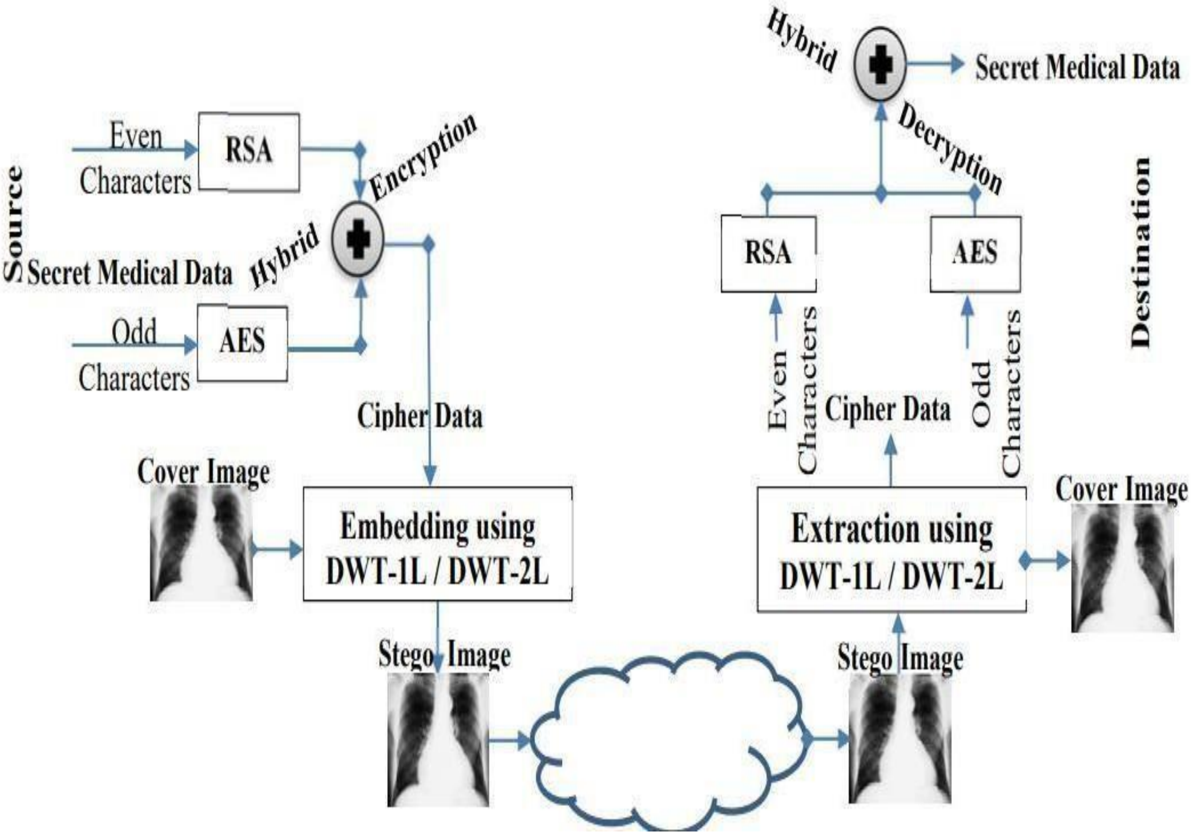


Figure 1: The suggested architecture for protecting the transfer of medical data

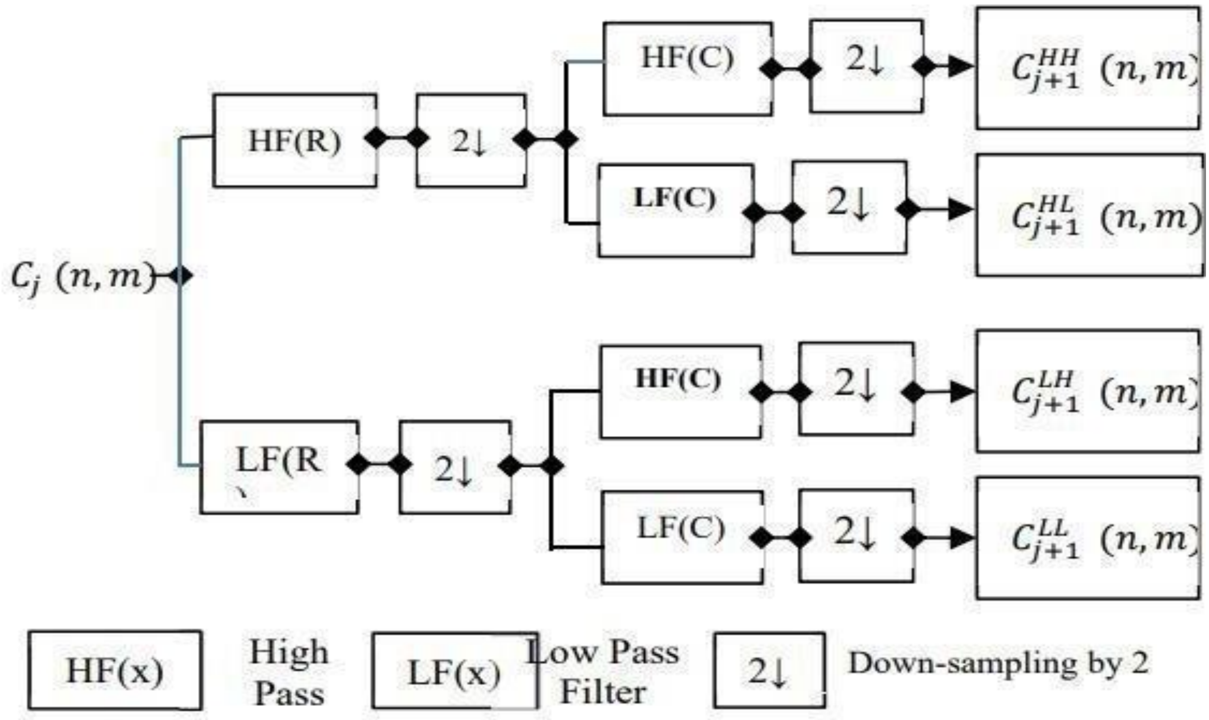
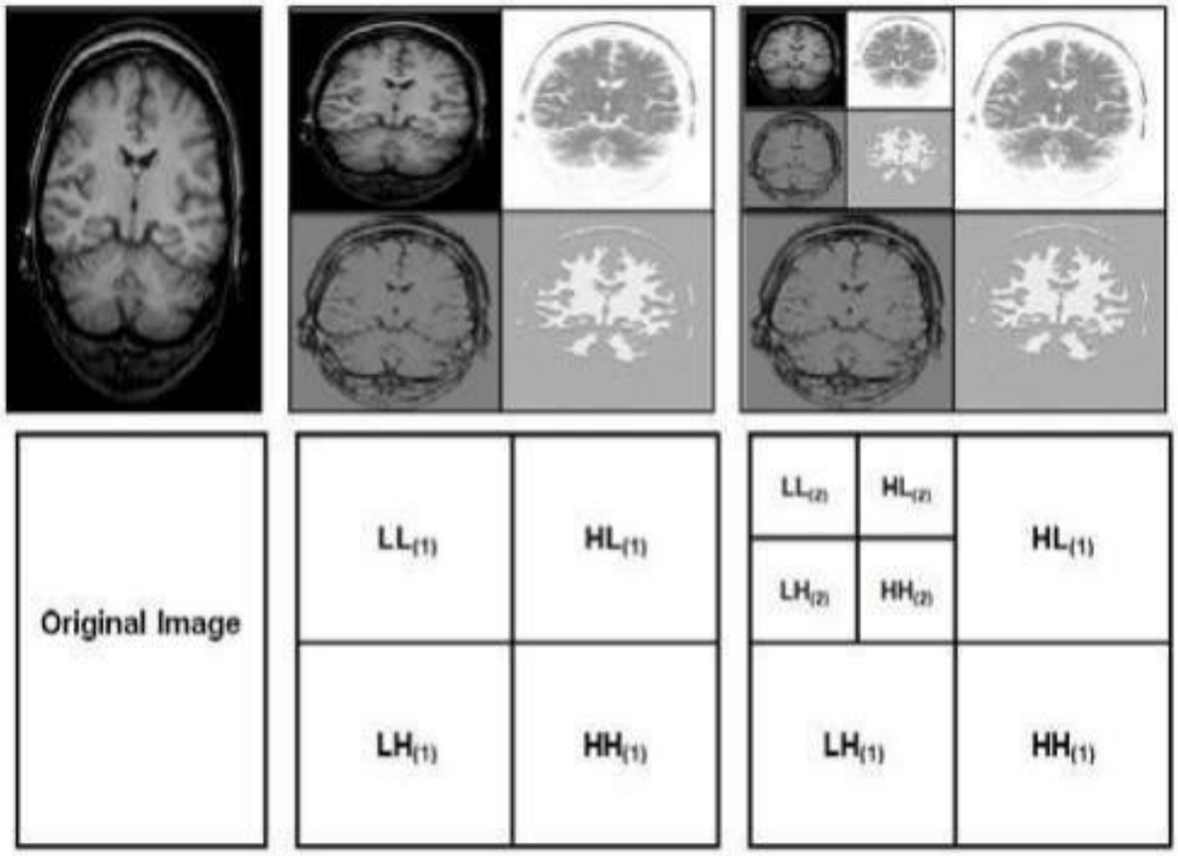


Figure 2: The DWT-2L decomposition method



(a) DWT-1L (b) DWT-2L

Figure 3: The DWT-2L technique of decomposition

B. Embedding Procedure

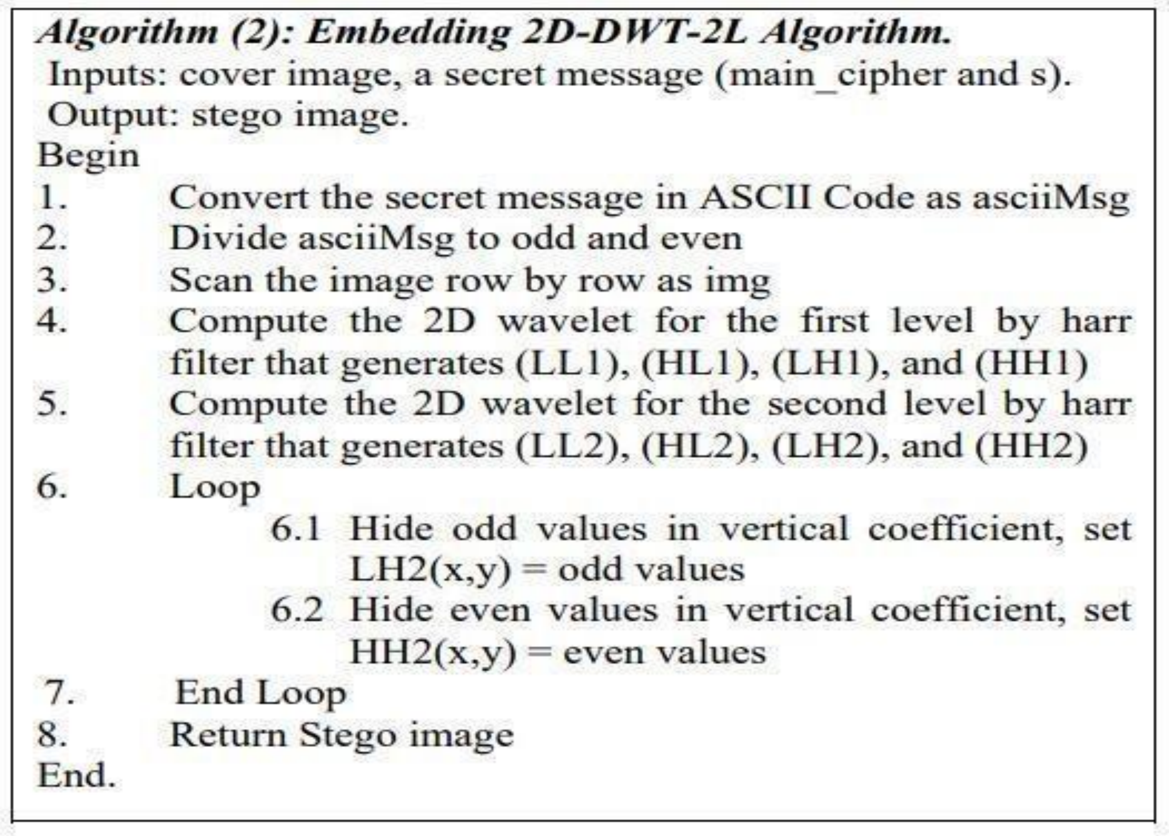
A Haar-DWT was used in this procedure. 2D-DWT-2L, like Haar-DWT, may be defined as a sequential transformation employing low-pass and high-pass filters along the image's rows, with the output dissected along the image's columns [21]. This procedure is seen in Figure 2. The elemental breakdown process 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.

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

$$S = \{f\eta(C, T)\} \qquad (6)$$

$$T = \{f\eta^{-1}(S)\} \qquad (7)$$



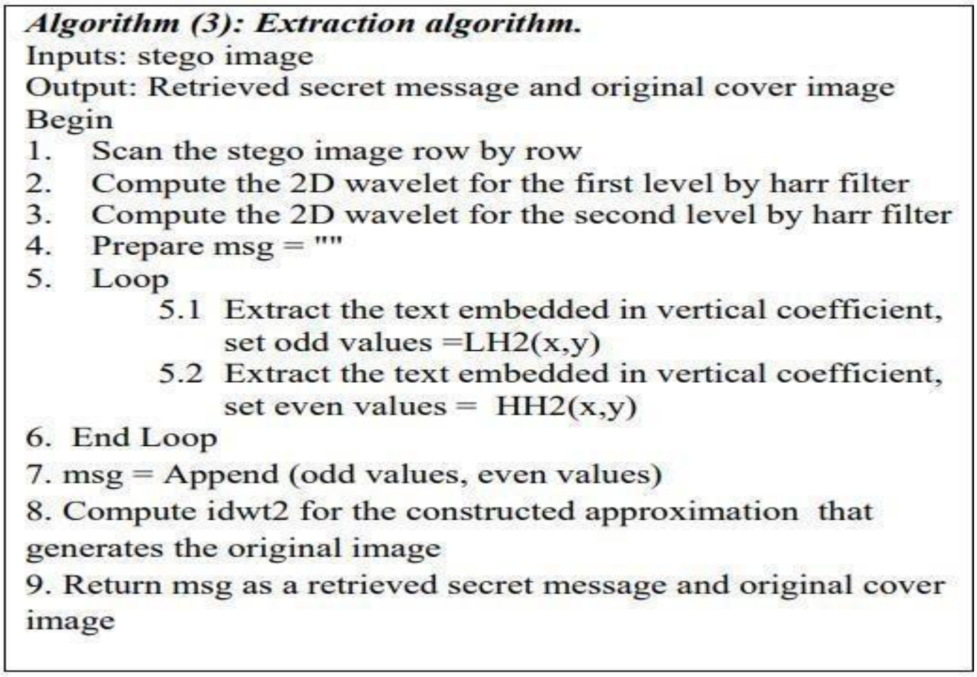
Algorithm (2): Embedding 2D-DWT-2L Algorithm.

```
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. 3



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.

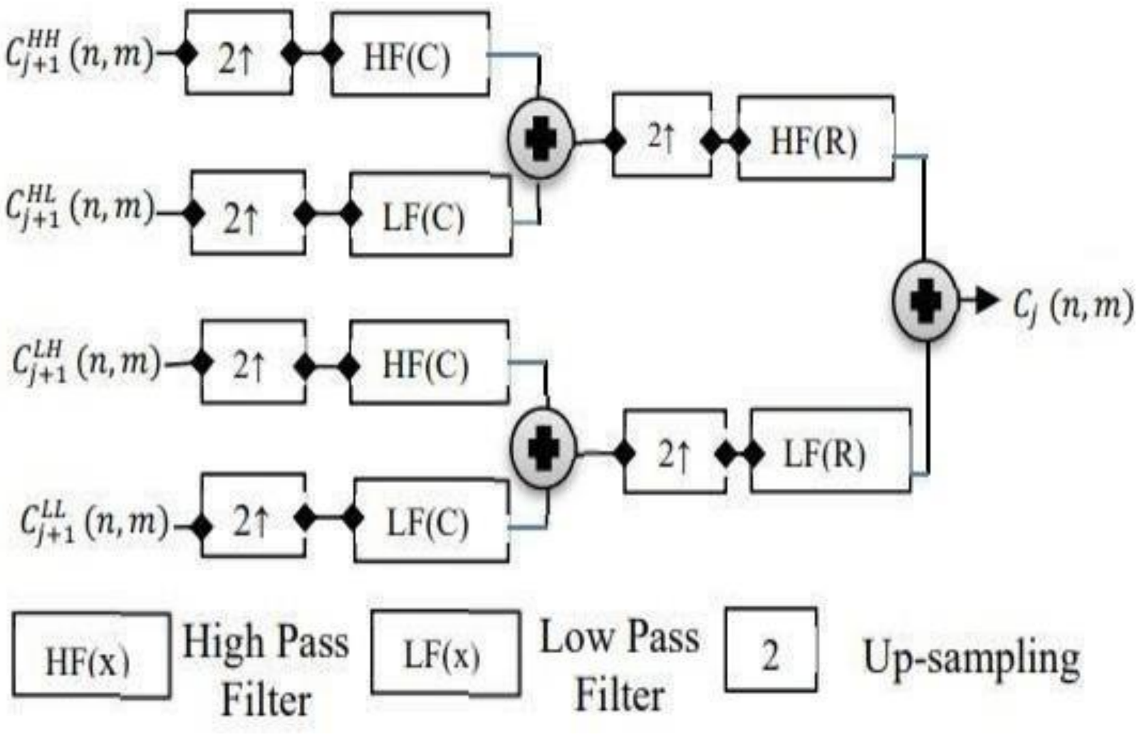


Figure 4. The synthesis process of 2D-DWT-2L

D. Data Encryption Scheme

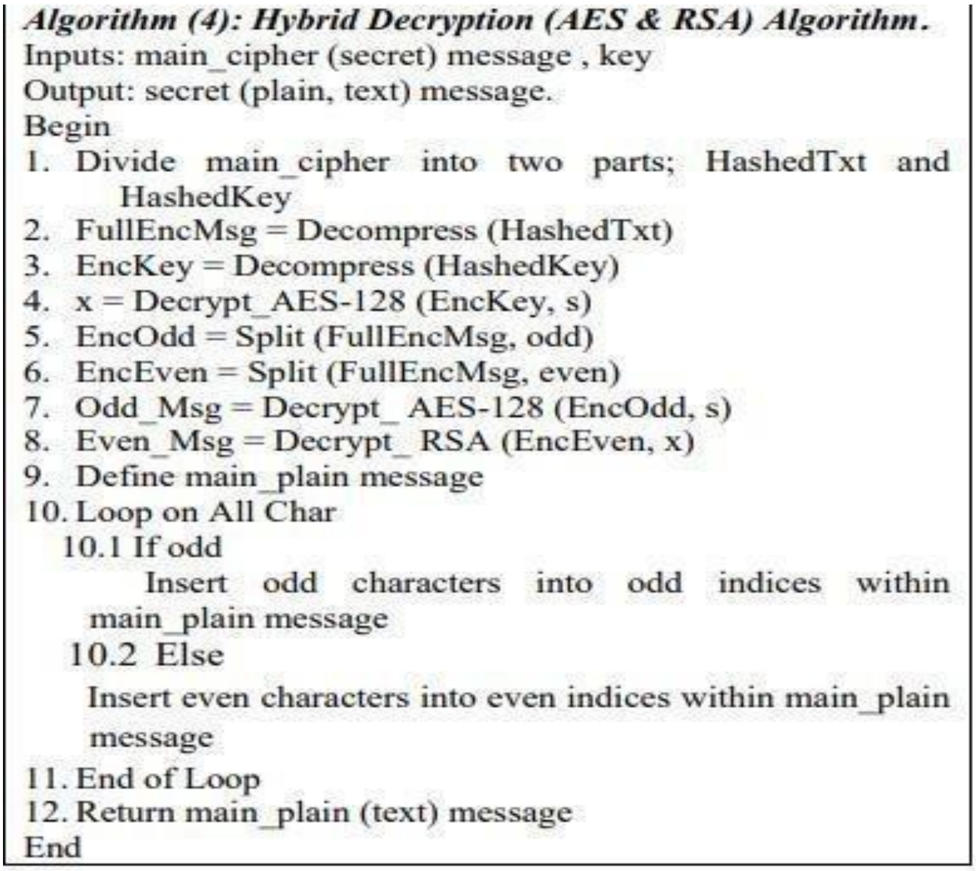
Decryption refers to the process of converting the encrypted data back to the user in a well-known format, which is the reverse of the encryption process. The same key used by the sender has to be used over the cipher-text throughout the encryption process. The decryption process can be mathematically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

$$\hat{C} = \{ 'E_{AES}^{-1}, 'E_{RSA}^{-1}, T_{odd}, T_{even}, \dot{T}_{odd}, \dot{T}_{even}, s, x \quad (8)$$

$$x = \{'E_{AES}(\dot{X}, s)\} \quad (9)$$

$$T_{even} = \{'E_{RSA}^{-1}((\dot{T}_{even}, x)\} \quad (10)$$

$$T_{odd} = \{'E_{AES}^{-1}(\dot{T}_{odd}, s)\} \quad (11)$$



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
```

Discrete Wavelet Transform (DWT):

A primary level DWT segments the entire image into four frequency sub bands termed LL, HL, LH, and HH. Here, LL marks lower resolution approximation factor, and HL, LH, and HH mark horizontal, vertical, and diagonal detail components respectively. LL band may be further decomposed into four frequency sub-bands [5]. Procedure may be implemented frequently (say, n) to gain nLevel DWT. Generally, LL sub-bands acquired after n-degree DWT are used to embed messages because this area marks high energy region to which human eye is less touchy.

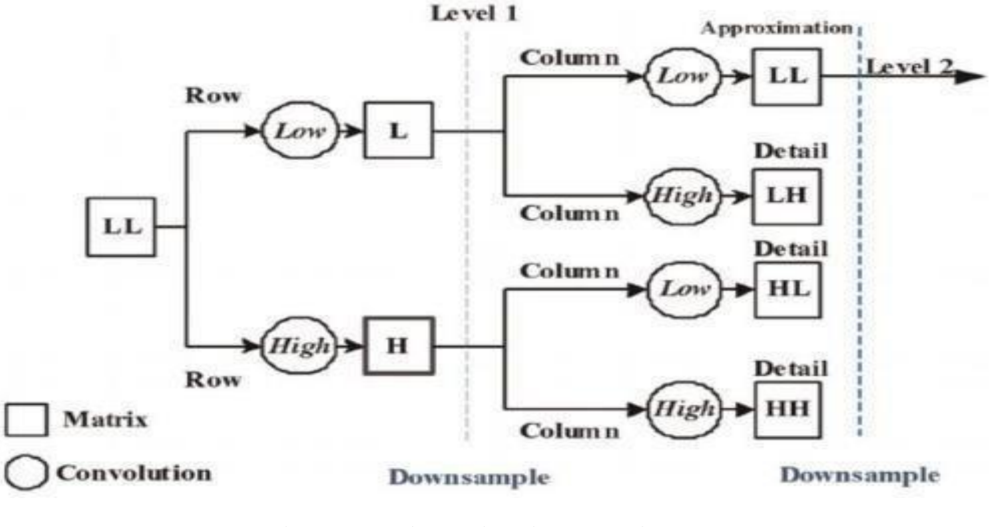
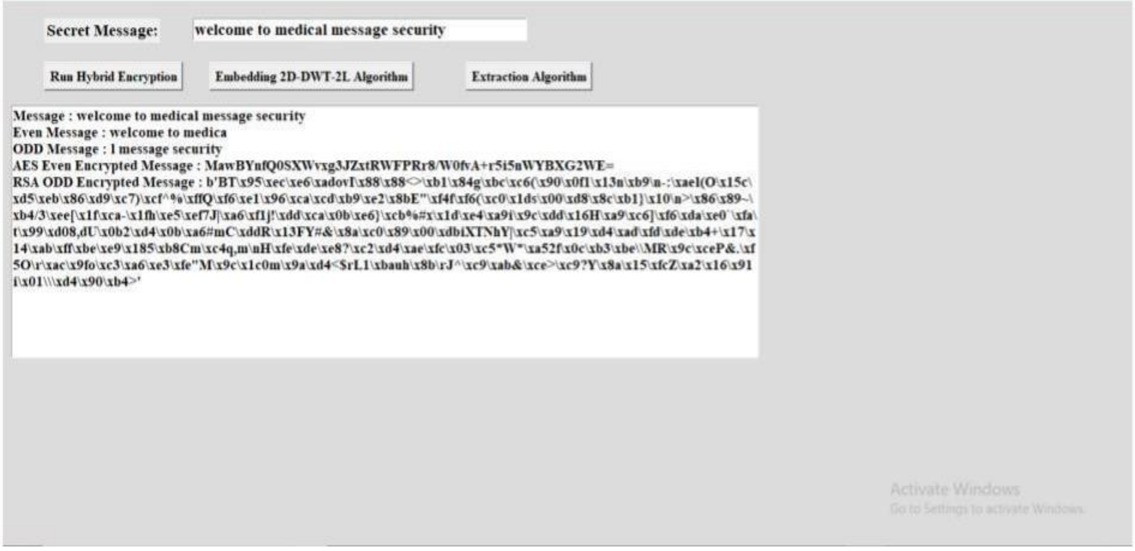


Figure 5. Schematic Diagram of DWT

4. Results and Discussion

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 resilience. Finally, the suggested method's invisibility and robustness are compared to previous studies.

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.



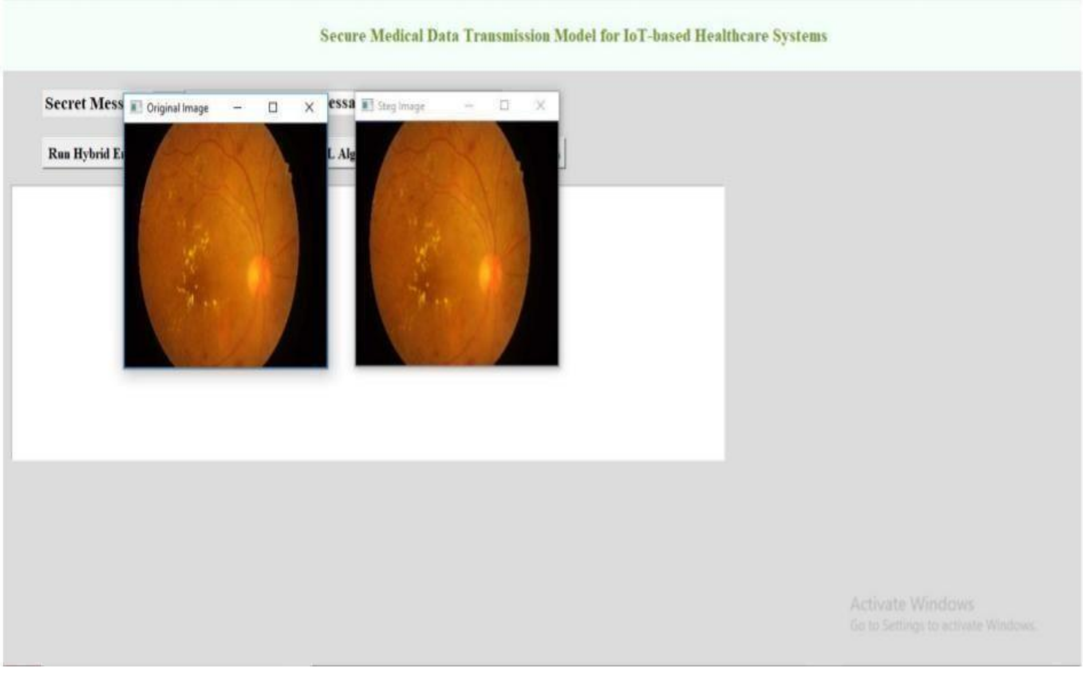
Secret Message: welcome to medical message security

Run Hybrid Encryption
Embedding 2D-DWT-2L Algorithm
Extraction Algorithm
Activate Windows
Go to Settings to activate Windows.

```
Message : welcome to medical message security
Even Message : welcome to medica
ODD Message : l message security
AES Even Encrypted Message : MawBYnfQ0SXWvxg3JZxtRWFPRr8/W0fvA+r5i5nWYBXG2WE=
RSA ODD Encrypted Message : b'BT\x95\xec\xe6\xadovI\x88\x88<>\xb1\x84g\xbc\xc6(\x90\x0f1\x13n\xb9\n-:\xael(O\x15c\
xd5\xeb\x86\xd9\xc7)\xcf^%\xffQ\xf6\xe1\x96\xca\xcd\xb9\xe2\x8bE"\xf4f\xf6(\xc0\x1ds\x00\xd8\x8c\xb1}\x10\n>\x86\x89~\
xb4/3\xee[\x1f\xca-\x1fh\xe5\xef7J|\xa6\xf1j!\xdd\xca\x0b\xe6}\xcb%#x\x1d\xe4\xa9i\x9c\xdd\x16H\xa9\xc6]\xf6\xda\xe0`\xfa\
t\x99\xd08,dU\x0b2\xd4\x0b\xa6#mC\xddR\x13FY#&\x8a\xc0\x89\x00\xdbiXTNhY|\xc5\xa9\x19\xd4\xad\xfd\xde\xb4+\x17\x
14\xab\xff\xbe\xe9\x185\xb8Cm\xc4q,m\nH\xfe\xde\xe8?\xc2\xd4\xae\xfc\x03\xc5*W*\xa52f\x0c\xb3\xbe\\MR\x9c\xceP&.\xf
5O\r\xac\x9fo\xc3\xa6\xe3\xfe"M\x9c\x1c0m\x9a\xd4<$rL1\xbauh\x8b\rJ^\xc9\xab&\xce>\xc9?Y\x8a\x15\xfcZ\xa2\x16\x91
i\x01\\\xd4\x90\xb4>'
```

Figure 6.

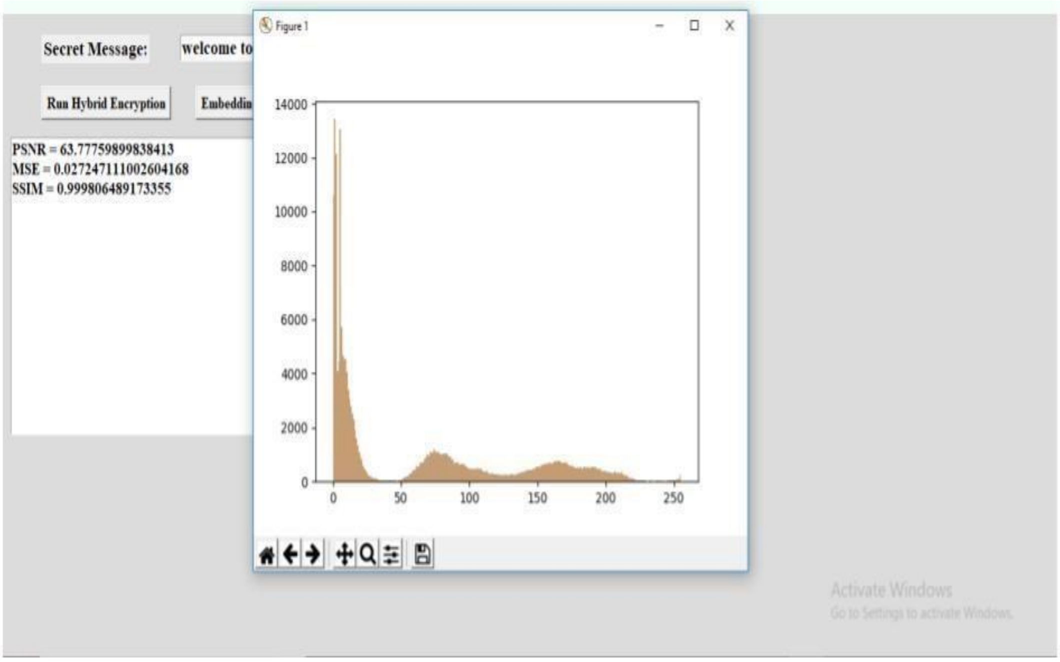
In below screen first image is the original image and second image contains steganography hidden message and both messages look similar and now close both images to get below histogram graph of both images



Secure Medical Data Transmission Model for IoT-based Healthcare Systems
Secret Mess
essa
Run Hybrid E
L Alg
Original Image
Steg Image
Activate Windows
Go to Settings to activate Windows.

Figure 7. Secure medical data Transmission Model for IoT-based health care

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 the above output we are getting a closer output compared to paper. Similarly, you can upload other images and test. Now click on 'Extraction Algorithm' button to extract and decrypt message from image.



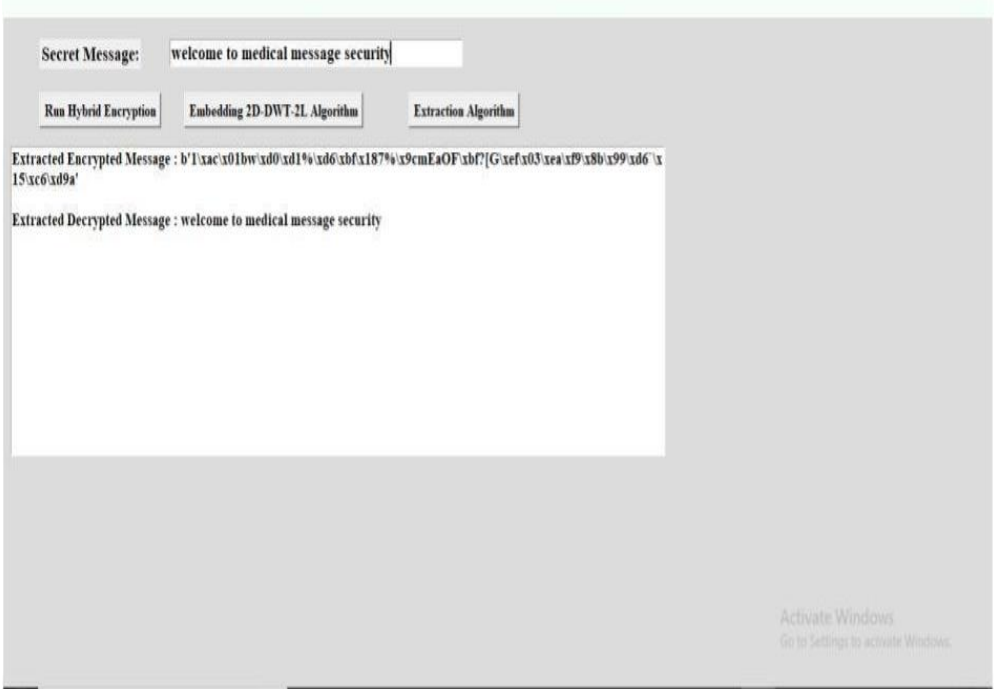
Secret Message: welcome to

```
PSNR = 63.77759899838413
MSE = 0.027247111002604168
SSIM = 0.999806489173355
```

Figure 8.

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

Figure 9.



Secret Message: welcome to medical message security

```
Extracted Encrypted Message : b'1\xac\x01bw\xd0\xd1%\xd6\xbf\x187%\x9cmEaOF\xbf?[G\xef\x03\xea\xf9\x8b\x99\xd6`\x
15\xc6\xd9a'

Extracted Decrypted Message : welcome to medical message security
```

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 superiorperformance 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.

References

[1]. Humayun, M., Jhanjhi, N. &amp; Alamri, M. (2020). IoT-based Secure and Energy Efficient scheme for E-health applications. Indian J Sci Technol, 13(28), 2833-2848.

[2]. Almulhim, M., &amp; Zaman, N. (2020, February). Proposing secure and lightweight authentication scheme for IoT based E-health applications. In 2018 20th International Conference on advanced communication technology (ICACT) (pp. 481-487).

[3]. Mallikarjuna, B., Kiranmayee, D., Saritha, V., &amp; Krishna, P. V. (2021, June). Development of efficient e-health records using iot and blockchain technology. In ICC 2021- IEEE International Conference on Communications (pp. 1-7). IEEE.

[4]. Amare &amp; Vuda (2021) .Edge Devices for Internet of Medical Thing Technologies, Techniques, and Implementation, eddah 22246-48.

[5]. Sarath Sabu, Swaraj Hegde et.al Global Transitions Proceedings 2 (2), 429-433, 2021.

[6]. Bairagi et al. (2019), IoT-Based Healthcare-Monitoring System towards Improving Quality of Life. hulna 9208, Bangladesh.

[7]. Shahzadi, R., Niaz, A., Ali, M., Naeem, M., Rodrigues, J. J., Qamar, F., & Anwar, S. M. (2019). Three tier fog networks: Enabling IoT/5G for latency sensitive applications. China Communications, 16(3), 1-11.

[8]. Hussain, A., Ali, T., Adeelaziz, F., Draz, U., Irfan, M., Yasin, S., ... & Alqhtani, S. (2021). Security framework for IoT based real-time health applications. Electronics, 10(6), 719.

[9]. Karolak, M., Razzaque, A., & Al-Sartawi, A. (2021). E-services and M-services using IoT: an assessment of the Kingdom of Bahrain. In Artificial Intelligence Systems and the Internet of Things in the Digital Era: Proceedings of EAMMIS 2021 (pp. 523-533). Cham: Springer International Publishing.

[10]. Dhatterwal, Jagjit Singh, Kuldeep Singh Kaswan, Anupam Baliyan, and Vishal Jain. "Integration of Cloud and IoT for Smart e-Healthcare." In Connected e-Health: Integrated IoT and Cloud Computing, pp. 1-31. Cham: Springer International Publishing, 2022.

[11]. Ould-Yahia, Youcef, Soumya Banerjee, Samia Bouzefrane, and Hanifa Boucheneb. "Exploring formal strategy framework for the security in iot towards e-health context using computational intelligence." Internet of things and Big data technologies for next generation healthcare (2017): 63-90.

[12]. Farahat, AS Tolba, Mohamed Elhoseny, Waleed Eladrosy Security in smart cities: models, applications, and challenges, 117-142, 2019.

[13]. Momin, Md Sarfaraz, Abu Sufian, Debaditya Barman, Paramartha Dutta, Mianxiong Dong, and Marco Leo and Zaw and Phyo. "In-home older adults' activity pattern monitoring using depth sensors: A review." Sensors 22, no. 23 (2022): 9067.

[14]. Amine Rghioui, Sandra Sendra, Jaime Lloret, Abedlmajid Oumnad Network Protocols and Algorithms 8 (3), 15-28, 2016.

[15]. Denis, R., & Madhubala, P. (2021). Hybrid data encryption model integrating multi- objective adaptive genetic algorithm for secure medical data communication over cloud-based healthcare systems. Multimedia Tools and Applications, 80, 21165-21202.

[16]. V Kanchana, Surendra Nath, Mahesh K SinghMaterials Today: Proceedings 51, 961- 964, 2022.

[17]. Chen, Shengbo, Jingtian Wang, Lanxue Zhang, Keping Yu, Ali Kashif Bashir, Rupak Kharel, and Celimuge Wu. "When internet of things meets e-health: an indoor temperature monitoring and control approach." IEEE Internet of Things Magazine 4, no. 3 (2021): 12-16.

[18]. Kaw, Javaid A., Nazir A. Loan, Shabir A. Parah, Khan Muhammad, Javaid A. Sheikh, and Ghulam Mohiuddin Bhat. "A reversible and secure patient information hiding system for IoT driven e-health." International Journal of Information Management 45 (2019): 262-275.

[19]. Rihab Boussada, Balkis Hamdane, Mohamed Elhoucine Elhdhili, Leila Azouz Saidane 2019 IEEE Wireless Communications and Networking Conference (WCNC), 1-6, 2019.

[20]. Rahmani, A. M., Gia, T. N., Negash, B., Anzanpour, A., Azimi, I., Jiang, M., & Liljeberg, P. (2018). Exploiting smart e-Health gateways at the edge of healthcare Internet-of-Things: A fog computing approach. Future Generation Computer Systems, 78, 641-658.