SECURED MEDICAL DATA TRANSMISSION MODEL FOR IoT (INTERNET of THINGS) - BASED HEALTH CARE SYSTEMS

CH. Hema Sree[1], K. Anji Babu[2]

[1]Student, Dept. of ECE, A.K.R.G College of Engineering and Technology, JNTU Kakinada, AP, India
[2]Assistant Professor, Dept. of ECE, A.K.R.G College of Engineering and Technology, JNTU Kakinada, AP, India

Abstract - *This project investigates an advancement of the Internet of Things (IoT) in the healthcare sector, the security, and the integrity of the medical data became big challenges for healthcare services applications. This paper proposes a hybrid security model for securing the diagnostic text data in medical images. The proposed model is developed through integrating either 2-D discrete wavelet transform 1 level (2D-DWT-1L) or 2-D discrete wavelet transform 2 level (2D-DWT-2L) steganography technique with a proposed hybrid encryption scheme. Then it hides the result in a cover image using 2D-DWT-1L or 2D-DWT-2L. Both color and gray-scale images are used as cover images to conceal different text sizes. The performance of the system was evaluated based on certain parameters.*

Key Words: **DWT-1level, DWT-2level, Healthcare services, Cryptography, Steganography, Encryption, Medical images.**

1. INTRODUCTION

An efficient model to ensure the security and integrity of the patient's diagnostic data transmitted and received from IoT environment becomes a major problem. So, this is carried out using steganography techniques and system encryption algorithms together to hide digital information in an image. The data is a confidential which is to be transmitted and changes in the carrier. So it is very difficult to detect. There are two main aspects in any stenography system which are steganography capacity and imperceptibility. These all are analyzed with different type of attacks and their behaviors respectively.

1.1 Data Encryption

The confidential patient's data is encrypted using a proposed hybrid encryption scheme that is developed from both AES and RSA encryption algorithms. The encrypted data is being concealed in a cover image using either 2D-DWT-1L or 2D-DWT-2L and produces a stego-image.

The plain text T is divided into odd part Todd and even parts Teven. The AES is used to encrypt Todd using a secret public key s. The RSA is used to encrypt Teven using a secret public key m. The private key x that used in the decryption process at the receiver side is encrypted using AES algorithm and sent to the receiver

1.2 Cryptography

It refers to secure information and communication techniques derived from mathematical concepts and a set of rule-based calculations called algorithms

Algorithms are used for cryptographic key generation, digital signing, verification to protect data privacy, web browsing on the internet, and confidential communications such as credit card transactions and email.

2. PROPOSED SYSTEM

The confidential patient's data is encrypted using a proposed hybrid encryption scheme that is developed from both AES and RSA encryption algorithms. The encrypted data is being concealed in a cover image using either 2D-DWT-1L or 2D-DWT-2L and produces a stego-image.

The embedded data is extracted and it is decrypted to retrieve the original data. The general framework of our proposed model for securing the medical data transmission at both the source's and the destination's sides shown in figure 1.

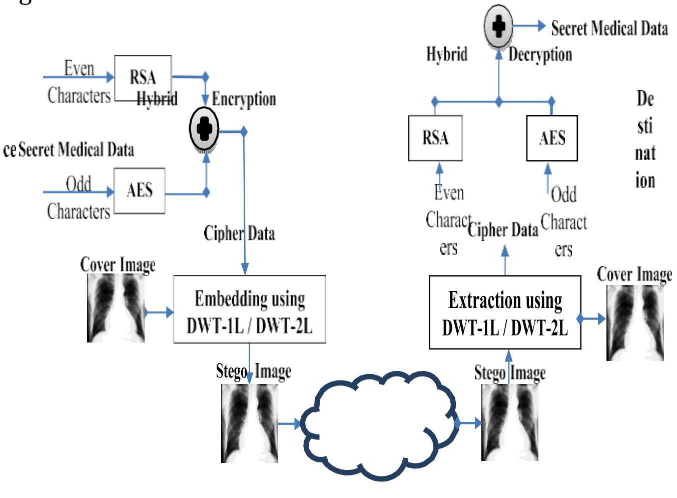

Fig- 1 Proposed frame work for securing the medical data transmission

A Haar-DWT was implemented. Throughout Haar-DWT, 2D-DWT-2L can be formulated as a consecutive transformation using low-pass and high-pass filters along the rows of the image and then result decomposed along the rows of the image

3. IMPLEMENTATION

The process is described below with important algorithms to understand the process.

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
```

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 as shown in figure 2. This shifted image is then used as an input image to the AES algorithm to encrypt the pixels of the shifted image.

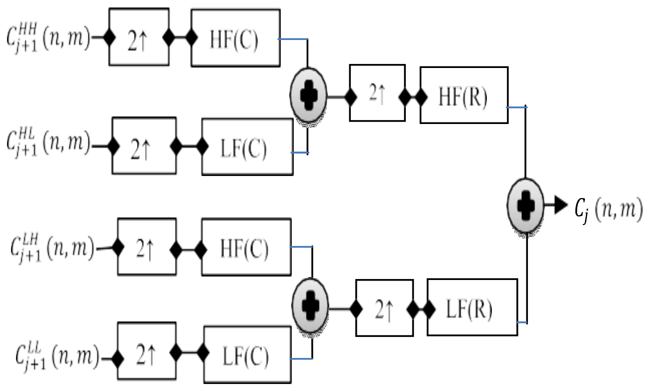

Fig-2 Synthesis process of 2D-DWT-2L.

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

BER calculates the probability that a bit will be incorrectly received due to noise. It is the number of bits received in error divided by the total number of bits transferred. The BER is calculated using the following form.

BER = Errors/Total Number of Bits

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 elemental decomposition process for $C_j(n, m)$ image of a size N M in four decomposed sub- band images which are referred to a high-high (HH), a high- low (HL), a low-high (LH), and a low-low (LL) frequency bands.

It can be mathematically given as below in equation form.

$$\hat{S} = \{f\eta, f\eta^{-1}, C, S, T\}$$

$$S = \{f\eta\,(C,\underset{\Sigma}{T})\}$$

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

Throughout the embedding process, the secret text is transformed into an ASCII format and then divided into even and odd values. The odd values are concealed in vertical coefficients mentioned by LH2. The even values are concealed in diagonal coefficients specified by HH2. Once the secret text message has been extracted, the cover image is synthesized from the reconstructed approximation by calling the idwt2 for the second level and then for the first level.

The text is encrypted by using the evolved hybrid encryption scheme that was previously explained. Then it is being embedded using either 2D-DWT-1L or 2D-DWT-2L stenography techniques. It was found that DWT-2L gives better PSNR and MSE results compared with DWT-1L.

The PSNR values were relatively reached to 57.44 and 56.39 in case of DWT-2L for color images and gray-scale images respectively. While the PSNR values were relatively reached to 56.13 and 55.42 in case of DWT-1L for color images and gray-scale images, respectively. The MSE values using DWT-2L varied from 0.12 to 0.56 for the color images and from 0.14 to 0.56 for the gray images. While the MSE values by using DWT-1L were ranged from 0.16 to 3.44 for the color images; and from 0.18 to 3.48 for the gray scale images.

4. SECURITY ANALYSIS

The model was tested using different messages with different lengths and hiding them in both color and gry scale images. The hidden message was analyzed before being transmitted and after being received by the expected recipient. That it will occur less distortion within to the original message after concealing the secret one.

5. RESULTS

Table-1: Comparing the performance of proposed model with Anwar approach

MODEL	PSNR	MSE
Anwar	56.76	0.1338
Proposed	57.02	0.1288

The performance of our model was compared with another technique developed by Anwar on 256 256 pixel medical color image using 18-byte text size. Table 1 shows the obtained PSNR and MSE values from applying our model as compared. The results obtained after applying the models on 256 256 color medical images with text size 18 bytes. It was found that our proposed model had a higher PSNR value and a smaller MSE value that reveals the higher performance of our proposed model.

6. CONCLUSION

This project engaged with either 2D-DWT-1L or 2D-DWT-2L steganography,hybrid blending AES and RSA cryptographic techniques. The experimental results were evaluated on both color and gray-scale images with different text sizes. The performance was assessed based on the six statistical parameters (PSNR, MSE, BER, SSIM, SC, and correlation). Compared to the state-of-the-art methods, the proposed model proved its ability to hide the confidential patient's data into a trans- mitted cover image with high imperceptibility, capacity, and minimal deterioration in the received stego image.

REFERENCES

[1] A. Darwish, A. E. Hassanien, M. Elhoseny, A. K. Sangaiah, and K. Muhammad, "The impact of the hybrid platform of Internet of Things and cloud computing on healthcare systems: Opportunities, challenges, and open problems," J. Ambient Intell. Humanized Comput., to be pub- lished, doi: https://doi.org/10.1007/s12652-017-0659-1

[2] A. Shehab et al., "Secure and robust fragile watermarking scheme for medical images," IEEE Access, vol. 6, pp. 10269–10278, 2018, doi: 10.1109/ACCESS.2018.2799240.

[3] A. K. Bairagi, R. Khondoker, and R. Islam, "An efficient stegano- graphic approach for protecting communication in the Internet of Things (IoT) critical infrastructures," Inf. Secur. J., Global Perspect., vol. 25, nos. 4–6, pp. 197–212, 2016.

[4] A. S. Anwar, K. K. A. Ghany, and H. El Mahdy, "Improving the security of images transmission," Int. J. Bio-Med. Inform. e-Health, vol. 3, no. 4, pp. 7–13, 2015.

[5] A. Abdelaziz, M. Elhoseny, A. S. Salama, and A. M. Riad, "A machine learning model for improving healthcare services on cloud computing environment," Measurement, vol. 119, pp. 117–128, Apr. 2018. [Online].

Available: https://doi.org/10.1016/j.measurement.2018.01.022

[6] M. Paschou, E. Sakkopoulos, E. Sourla, and A. Tsakalidis, "Health Inter- net of Things: Metrics and methods for efficient data transfer," Simul. Model. Pract. Theory, vol. 34, pp. 186–199, May 2013.

[7] M. Sajjad et al., "Raspberry Pi assisted face recognition framework for enhanced law-enforcement services in smart cities," Future Gen- erat. Comput. Syst., to be published, doi: https://doi.org/10.1016/j.future.2017.11.013

[8] P. Kumar and H.-J. Lee, "Security issues in healthcare applications using wireless medical sensor networks: A survey," Sensors, vol. 12, no. 1, pp. 55–91, 2012

[9] P. Kumar and H.-J. Lee, ''Security issues in healthcare applications using wireless medical sensor networks: A survey,'' Sensors, vol. 12, no. 1, pp. 55–91, 2012.

[10] M. A. Razzaq, R. A. Shaikh, M. A. Baig, and A. A. Memon, ''Digital image security: Fusion of encryption, steganography and watermarking,'' Int. J. Adv. Comput. Sci. Appl., vol. 8, no. 5, pp. 224–228, 2017.

[11] N. Dey and V. Santhi, Intelligent Techniques in Signal Processing for Mul- timedia Security. New York, NY, USA: Springer, 2017, doi: 10.1007/978- 3-319-44790-2.

[12] M. Jain, R. C. Choudhary, and A. Kumar, ''Secure medical image steganog- raphy with RSA cryptography using decision tree,'' in Proc. 2nd Int. Conf. Contemp. Comput. Inform. (IC3I), Dec. 2016, pp. 291–295.