ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 7, July 2019

IOT Security in Healthcare Using Steganography

Jayashree Walimbe, Prof. Name Prof. S. B Mule

Professor, Department of Electronics and Telecommunication Engineering, Sinhgad College of Engineering, Pune, India

ABSTRACT: In this implementation, problem of security and integrity of medical data transmission in medical applications is addressed. This project proposes steganography technique to secure medical data through 2-D discrete wavelet transform 1 level (2D-DWT-1L) or 2-D discrete wavelet transform 2 level (2D-DWT-2L). Proposed model is a combination of cryptography, steganography and OFDM for secure and robust data transmission and reception of medical images in healthcare systems.

KEYWORDS: Cryptography, DWT-1level, DWT-2level, Encryption, Healthcare Services, Internet of Things, Medical Images, OFDM.

I. INTRODUCTION

IoT makes a coordinated correspondence condition of interconnected gadgets and stages by connecting with both virtual and physical world together. With the approach of remote computerized human services based IoT frameworks, the transmission of therapeutic information turns into an every day schedule. Subsequently, it is important to build up an effective model to guarantee the security and uprightness of the patient's demonstrative information transmitted and got from IoT condition. This objective is done utilizing steganography strategies and framework encryption calculations together to cover up computerized data in a picture.

Cryptography is another term for information encryption. Encryption cryptography is the way toward encoding messages such that programmers can't peruse it, yet that can be approved faculty. The two principle calculations utilized for information encryption in this work are the Advanced Encryption Standard (AES) calculation. AES is a symmetric figure where a similar key is utilized on the two sides. It has a fixed message square size of 128 bits of content (plain or figure), and keys of length 128,192, or 256 bits. At the point when longer messages are sent, they are partitioned into 128-piece squares. Obviously, longer keys make the figure increasingly hard to break, yet in addition uphold a more drawn out encode and unscramble process.

AES encryption encrypts secret plain text data which is then embedded in a cover image using Discrete Wavelet Transform. Resulting stego-image is then transmitted to other end using OFDM.

On the receiver end, encrypted data is extracted from the stego-image and then it is decrypted. This mgives us the original plain text data.

The scheme can be typically used in medical data transmission in healthcare industry.

II. PROPOSED SYSTEM

This paper proposes a healthcare security model for securing a medical data transmission in IoT environments. The proposed model composes of four continuous processes: (1) The confidential patient's data is encrypted using a proposed hybrid encryption scheme that is developed from both AES encryption algorithms. (2) The encrypted data is being concealed in a cover image using either 2D-DWT-1L or 2D-DWT-2L and produces a stego-image. (3) The embedded data is extracted. (4) The extracted data is decrypted to retrieve the original data. Fig. 1 shows the general framework of our proposed model for securing the medical data transmission at both the source's and the destination's sides.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 7, July 2019

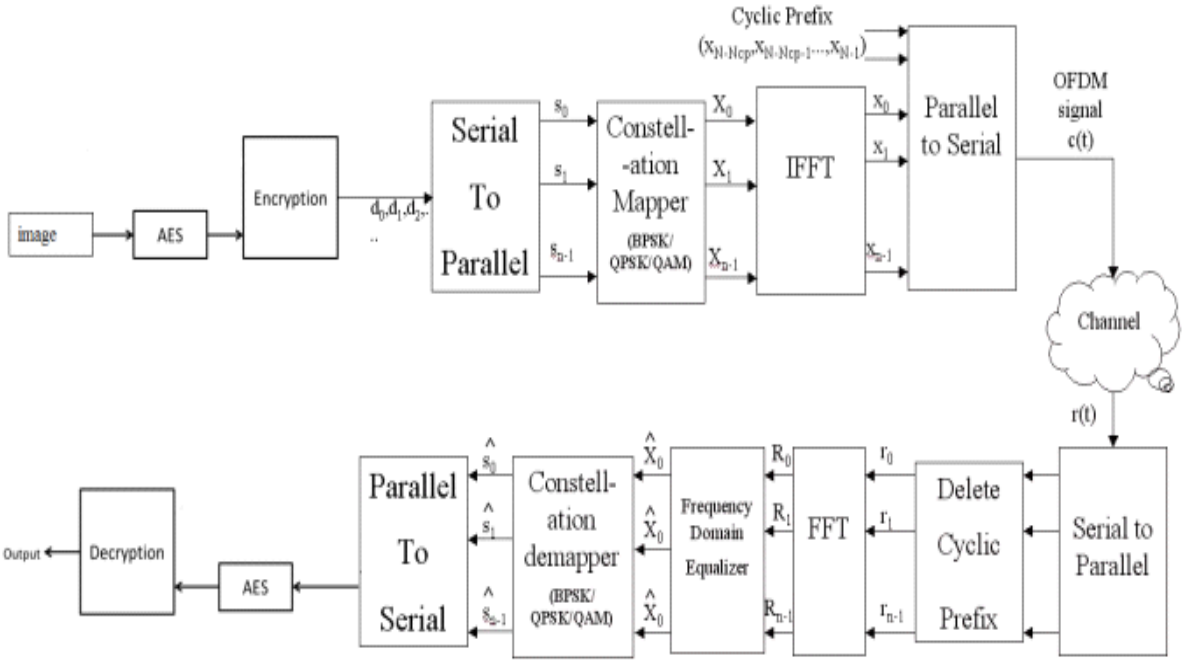

Fig 1 block diagram of proposed system

DATA ENCRYPTION SCHEME

Assume that somebody needs to make an impression on a collector, and needs to make certain that nobody else can peruse the message. Nonetheless, there is the likelihood that another person opens the letter or hears the electronic correspondence. In cryptographic wording, the message is called plaintext or clear content. Encoding the substance of the message so that conceals its substance from untouchables is called encryption. The scrambled message is known as the figure content.

The way toward recovering the plaintext from the figure content is called decoding. Encryption and unscrambling as a rule utilize a key, and the coding strategy is with the end goal that decoding can be performed just by knowing the best possible key. Cryptography is the craftsmanship or art of keeping messages mystery. Cryptanalysis is the specialty of breaking figures, for example recovering the plaintext without knowing the correct key. Individuals who do cryptography are Cryptographers, and professionals of cryptanalysis are Cryptanalysts. Cryptography manages all parts of secure informing, confirmation, advanced marks, electronic cash, and different applications. Cryptology is the part of science that reviews the numerical establishments of cryptographic techniques.

Basic Cryptographic Algorithms

A technique for encryption and decoding is known as a figure. Some cryptographic strategies depend on the mystery of the calculations; such calculations are just of chronicled intrigue and are not satisfactory for certifiable necessities. Every single present day calculation utilize a key to control encryption and unscrambling; a message can be decoded just if the key matches the encryption key. The key utilized for unscrambling can be not the same as the encryption key, yet for most calculations they are the equivalent. There are two classes of key-based calculations, symmetric (or mystery key) and uneven (or open key) calculations. The thing that matters is that symmetric calculations utilize a

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 7, July 2019

similar key for encryption and unscrambling (or the decoding key is effectively gotten from the encryption key), though topsy-turvy calculations utilize an alternate key for encryption and unscrambling, and the decoding key can't be gotten from the encryption key.

EMBEDDING PROCEDURE

Haar-DWT

The most straightforward of all discrete wavelet changes is the Discrete Haar Wavelet Tranformation (HWT). How about we propel it's development with the accompanying precedent:

Assume you had the eight numbers 100, 200, 44, 50, 20, 20, 4, 2 (these could be grayscale forces) and you needed to send a guess of the rundown to a companion. Because of transmission capacity limitations (this is an extremely old framework!), you are just permitted to send your companion four qualities. What four qualities would you send your companion that may speak to a guess of the eight given qualities?

There are clearly numerous conceivable responses to this inquiry, yet a standout amongst the most well-known arrangements is to take the eight numbers, two at any given moment, and normal them. This calculation would create the four qualities 150, 47, 20, and 3. This rundown would speak to a guess to the first eight qualities. Sadly, if your companion gets the four qualities 150, 47, 20, and 3, she gets no opportunity of delivering the first eight qualities from them - more data is required. Assume you are permitted to send an extra four qualities to your companion. With these qualities and the initial four qualities, she ought to have the capacity to reproduce your unique rundown of eight qualities. What esteems would you send her?

Assume we sent our companion the qualities 50, 3, 0, and - 1. How could we touch base at these qualities? They are basically the guided separations from the pairwise normal to the second number in each pair: 150 + 50 = 200, 47 + 3 = 50, 20 + 0 = 20, and 3 + (- 1) = 2. Note that in the event that we subtract the qualities in this rundown from the pairwise midpoints, we land at the primary number in each pair: 150 - 50 = 100, 47 - 3 = 44, 20 - 0 = 20, and 3 - (- 1) = 4. So with the rundowns (150,47,20,3) and (50,3,0,- 1), we can totally recreate the first rundown (100,200,44,50,20,20,4,2).

EXTRACTION PROCEDURE

In the wake of fusing the content into the spread picture, the 2DDWT-2L method is conveyed to remove the mystery message and recover the spread picture

When the mystery instant message has been separated, the spread picture is orchestrated from the reproduced estimate by calling the idwt2 for the second dimension and afterward for the principal level.

DATA DECRYPTION SCHEME

Decoding alludes to the way toward changing over the scrambled information back to the client in a notable arrangement; which is the turn around of the encryption procedure. A similar key utilized by the sender must be utilized over the figure message all through the encryption procedure.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 7, July 2019

III. RESULT

Fig. 2. Cover Image

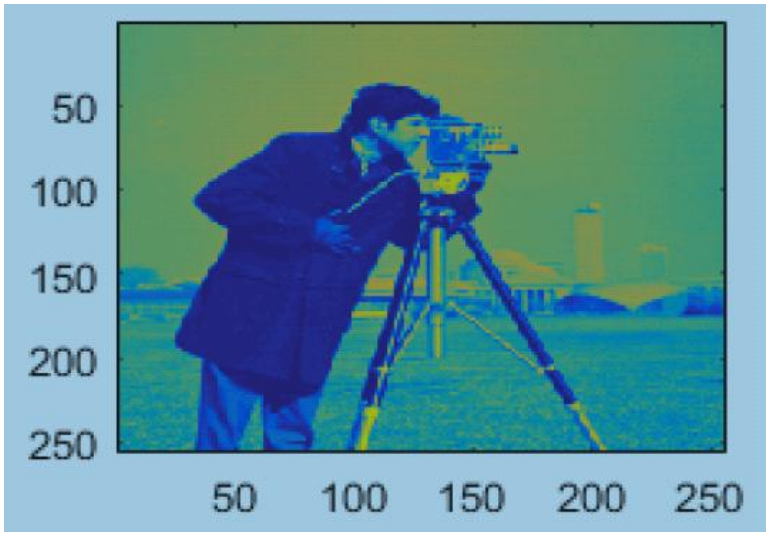

Fig. 3.ApproxCoeff

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 7, July 2019

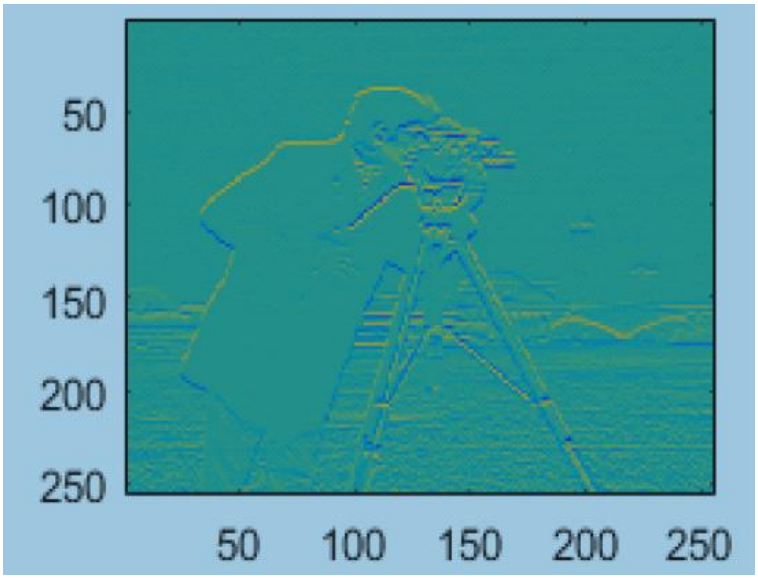

Fig. 4. Detail Coeff : Horizontal

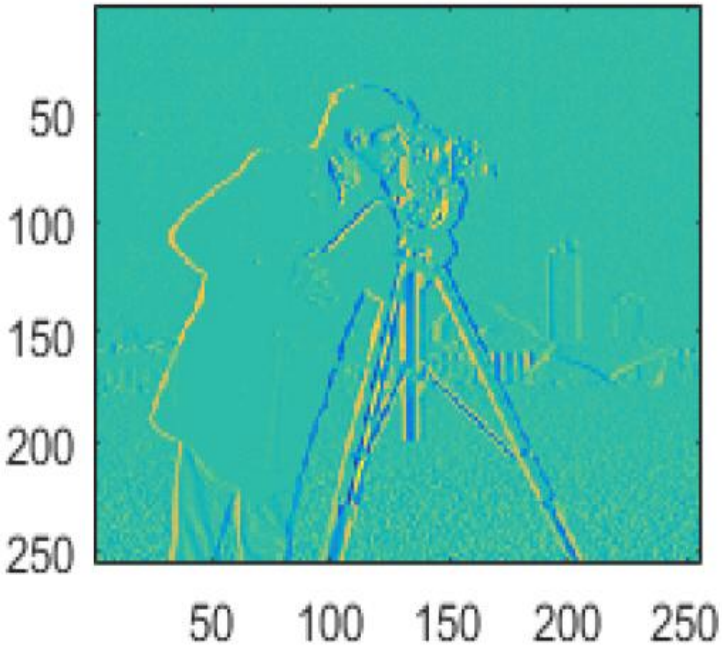

Fig. 5. Detail Coeff : Vertical

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 7, July 2019

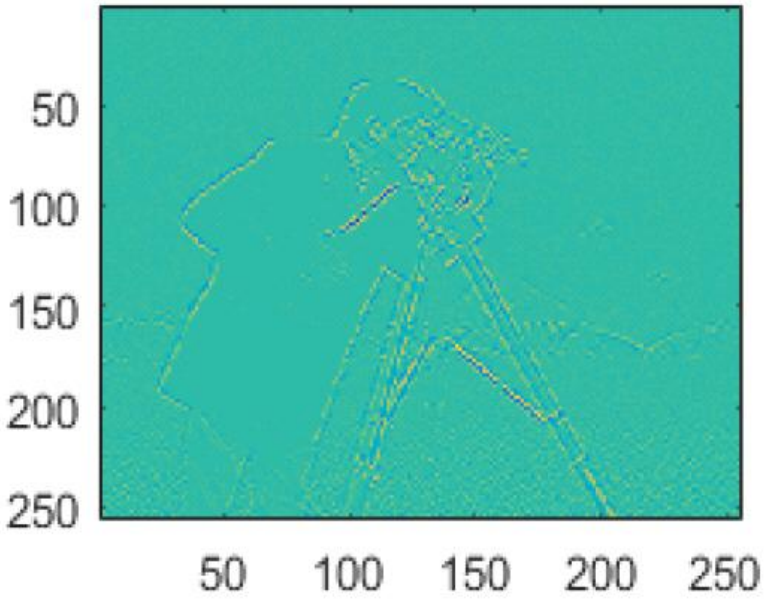

Fig. 6. Detail Coeff : Diagonal

Fig. 7.Reconstructed Image

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 7, July 2019

IV. CONCLUSION

A secure patient's diagnostic data transmission model using both color and gray-scale images as a cover carrier for healthcare based IoT environment has been proposed. The proposed model engaged either 2D-DWT-1L or 2D-DWT-2L steganography and hybrid blending AES cryptographic techniques. The experimental results were evaluated gray-scale images with different text sizes. The performance was assessed based on statistical parameters (BER and SNR). Proposed system was successful in hiding a secret text message inside a picture image without any distortion in cover image and data loss in text message.

REFERENCES

1. Mohamed Elhoseny, Gustavo Ramírez-González, Osama M. Abu-Elnasr, Shihab A. Shawkat, Arunkumar N, Ahmed farouk, "Secure Medical Data Transmission Model for IoT-based Healthcare Systems", 2169-3536 (c) 2018 IEEE
2. Elhoseny, Arun Kumar Sangaiah, Khan Muhammad, The Impact of the Hybrid Platform of Internet of Things and Cloud Computing on Healthcare Systems: Opportunities, Challenges, and Open Problems, Journal of Ambient Intelligence and Humanized Computing, 2017 (https://doi.org/10.1007/s12652- 017-0659-1)
3. AbdulazizShehab, Mohamed Elhoseny, Khan Muhammad, Arun Kumar Sangaiah, Po Yang, Haojun Huang, GuolinHou; Secure and Robust Fragile Watermarking Scheme for Medical Images, IEEE Access, Volume: PP, Issue: 99, (DOI: 10.1109/ACCESS.2018.2799240).
4. Bairagi, A. K., Khondoker, R., & Islam, R. (2016). An efficient steganographic approach for protecting communication in the Internet of Things (IoT) critical infrastructures. Information Security Journal: A Global Perspective, 25(4-6), 197-212.
5. Anwar, A. S., Ghany, K. K. A., &Mahdy, H. E. (2015). Improving the security of images transmission. International Journal, 3(4).
6. Ahmed Abdelaziza, Mohamed Elhoseny, Ahmed S. Salama, A.M. Riad,"A Machine Learning Model for Improving Healthcare services on Cloud Computing Environment", Measurement, Volume 119, April 2018, Pages 117-128, 2018
7. Paschou, M., Sakkopoulos, E., Sourla, E., &Tsakalidis, A. (2013). Health Internet of Things: Metrics and methods for efficient data transfer. Simulation Modelling Practice and Theory, 34, 186-199.
8. Muhammad Sajjad, MansoorNasir, Khan Muhammad, Siraj Khan, Zahoor Jan, Arun Kumar Sangaiah, Mohamed Elhoseny, Sung WookBaik, "Raspberry Pi assisted face recognition framework for enhanced law-enforcement services in smart cities", Future Generation Computer Systems, Elsevier, 2018 (DOI: https://doi.org/10.1016/j.future.2017.11.013).
9. Kumar, P., & Lee, H. J. (2011), Security issues in healthcare applications using wireless medical sensor networks: A survey. Sensors, 12(1), 55-91.
10. Razzaq, M. A., Sheikh, R. A., Baig, A., & Ahmad, A. (2017) Digital image security: Fusion of encryption, steganography and watermarking. International Journal of Advanced Computer Science and Applications (IJACSA), 8(5).