**SECURE MEDICAL DATA TRANSMISSION MODEL FOR**

**IOT- BASED HEALTHCARE SYSTEMS**

**ABSTRACT**

The transmission of data through any channel of communication needs strong encryption techniques for the purpose of data security. Internet of things (IoT) creates an integrated communication environment of interconnected devices and platforms by engaging both virtual and physical world together. Due to the significant advancement of the 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 2D Discrete Wavelet Transform 2 Level (2D-DWT-2L) steganography technique with a proposed hybrid encryption scheme. The proposed hybrid encryption schema is built using a combination of Advanced Encryption Standard (AES), and Rivest, Shamir, and Adleman (RSA) algorithms. The proposed model starts by encrypting the secret data; then it hides the result in a cover image using 2D-DWT-2L. Both color and gray-scale images are used as cover images to conceal different text sizes. The performance of the proposed system was evaluated based on six statistical parameters; the Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE), Bit Error Rate (BER), Structural Similarity (SSIM), Structural Content (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 transmitted cover image with high imperceptibility, capacity, and minimal deterioration in the received stego-image.

**OBJECTIVES**

This paper aims to improve the security of medical data transmission based on the integration between a steganography technique and a hybrid encryption scheme to get a highly secured healthcare system.

**EXISTING SYSTEM**

With the advent of remote digital healthcare based IoT systems, the transmission of medical data becomes a daily routine.

* Bairagi, A. K., et al, proposed three color image steganography approaches for protecting information in an IoT infrastructure. The first and third approaches use three (red, green, and blue) channels, while the second approach uses two (green and blue) channels for carrying information. Dynamic positioning techniques have been used for hiding information in the deeper layer of the image channels with the help a shared secret key.
* Anwar, A. S., et al, developed a technique to secure any type of images especially medical images. They aimed to maintain the integrity of electronic medical information, ensuring availability of that information, and authentication of that information to ensure that authorized people only can access the information. First, the AES encryption technique was applied on the first part. The ear print also embedded in this work, where seven values were extracted as feature vector from the ear image. The proposed technique improved the security of medical images through sending them via the internet and secured these images from being accessed via any unauthorized person.
* Abdel-Nabi, H., et al, proposed a crypto-watermarking approach based on AES standard encryption algorithm and reversible watermarking data hiding technique to secure medical images. The results proved that the proposed approach achieves both the authenticity and integrity of the images either in the spatial domain or the encrypted domain or both domains.

**EXISTING SYSTEM DRAWBACKS**

* Theconventional encryption methods failed to give the desired result of protecting the data.
* DES is breakable, as the key is 56-bit length.
* The existing Encryption Standard comparatively slower.

**PROBLEM STATEMENT**

With the advent of remote digital healthcare based IoT systems, the transmission of medical data becomes 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.

**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 and RSA encryption algorithms.
2. The encrypted data is being concealed in a cover image using 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.

Encryption cryptography is the process of encoding messages in a way that hackers cannot read it, but that can be authorized personnel. The two main algorithms used for data encryption in this work are the Advanced Encryption Standard (AES) and the Rivest-Shamir-Adleman (RSA) algorithm. AES is a symmetric cipher where the same key is used on both sides. It has a fixed message block size of 128 bits of text (plain or cipher), and keys of length 128,192, or 256 bits. When longer messages are sent, they are divided into 128-bit blocks. Apparently, longer keys make the cipher more difficult to break, but also enforce a longer encrypt and decrypt process. On the contrary, the RSA is a public key algorithm, which widely used in business and personal communication sectors. It has the advantage of having a variable key size ranging from (2-2048) bits.

This paper implements both 1-level and 2-level of DWT steganography techniques that operate on the frequency domain. It split up the image into high and low iteration parts. The high iteration part contains edge information, whereas the low iteration part is frequently divided into high and low iteration parts.

**PROPOSED SYSTEM BLOCK DIAGRAM**

**DIAGNOSTIC TEXT**

**STEGO**

**IMAGE**

**ODD PART**

**EVEN PART**

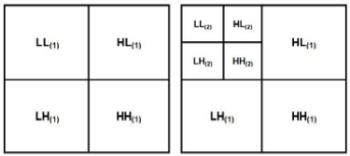
**AES**

**RSA**

**DISCRETE WAVELET TRANSFORM (DWT)**

**DECOMPOSED IMAGE**

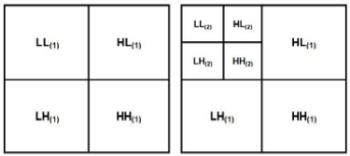
**COVER IMAGE (COLOR & Gray )**



**CLOUD (IOT)**

**STEGO**

**IMAGE**



**COMPOSED IMAGE**

**INVERSE DISCRETE WAVELET TRANSFORM (DWT)**

CIPHER DATA

**COVER IMAGE (COLOR & Gray )**

**+++**

**+++**

**ODD PART**

**EVEN PART**

**AES**

**RSA**

**DIAGNOSTIC TEXT**

CIPHER DATA

**STEGO**

**IMAGE**

**FIGURE 1: THE PROPOSED FRAMEWORK FOR SECURING THE MADICAL DATA TRANSMISSION.**

**FLOW CHART:**

TEXT

IMAGE

KEY

WAVELET TRANSFORM

ENCRYPTION

ENCRYPT Text

SEND IMAGE

INVERSE WAVELET TRANSFORM

HH-3 sub-band

WAVELET TRANSFORM

HH-3 sub-band

DECRYPTED DATA

EXTRACTED DATA

**PROPOSED METHODOLOGIES**

**Algorithm (1): Hybrid (AES & RSA) Algorithm.**

Inputs: secret plain Stext message.

Output: main\_cipher message , key s

**Algorithm-:**

Throughout the encryption process, the plain text T is divided into odd part T-ODD and even parts T-EVEN.

The AES is used to encrypt T-ODD using a secret public key s. The RSA is used to encrypt T-EVEN using a secret public key m.

<https://www.geeksforgeeks.org/rsa-algorithm-cryptography/>

<https://www.youtube.com/watch?v=ayiOhApI6SM>

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

**Algorithm-:** **Haar-DWT**

2D-DWT-2L can be formulated as a consecutive transformation using low-pass and high-pass filters.

**Algorithm-2: Least Significant Method**

Step-1: Read the value of the pixel.

Step-2: Convert it to its equivalent binary form.

Step-3: Modify the least significant bit accordingly.

**PROPOSED SYSTEM ADVANTAGES**

* The benefit of steganography is that it can be utilized to transmit classified messages without the fact of the transmission being detected.
* It is safe, secure and protected transmission of data .
* AES is faster.
* In AES we can use 128,192 or 259 bits long key ,so AES key is harder to break than DES,
* The encrypted text is embedded in the LL-sub-band of the wavelet transformed image.
* Compared to the state-of-the-art methods, the proposed model proved its ability to hide the confidential patient's data into a transmitted cover image with high imperceptibility, capacity, and minimal deterioration in the received stego-image.]\

**SOFTWARE REQUIREMENTS**

* MATLAB 7.14 Version R2012

**MATLAB**

The MATLAB high-performance language for technical computing integrates computation, visualization, and programming in an easy-to-use environment where problems and solutions are expressed in familiar mathematical notation.

* Data Exploration ,Acquisition ,Analyzing &Visualization
* Engg drawing and Scientific graphics
* Analyzing of algorithmic designing and development
* Mathematical functions and Computational functions
* Simulating problems prototyping and modeling
* Application development programming using GUI building environment.

Using MATLAB, you can solve technical computing problems faster than with traditional programming languages, such as C, C++, and Fortran.