Proceedings of the Fourth International Conference on Computing Methodologies and Communication (ICCMC 2020)
IEEE Xplore Part Number:CFP20K25-ART; ISBN:978-1-7281-4889-2

2020 Fourth International Conference on Computing Methodologies and Communication (ICCMC) 978-1-7281-4889-2/20/$31.00 ©2020 IEEE 10.1109/ICCMC48092.2020.ICCMC-00062

Hybrid Data Encryption Algorithm for Secure Medical Data Transmission in Cloud Environment

B. PUSHPA
Department of Computer and Information Science
Annamalai University
pushpasidhu@gmail.com

Abstract— **At present times, healthcare data stored in cloud is considered as a highly sensitive record, which should be hidden towards unauthorized accesses to protect the information about the patient. Hence, security related to cloud based medical data transmission receives significant attention among researchers and academicians. This study presents a new hybridization of data encryption model to shelter the diagnosis data in medical images. The proposed model is presented by the integration of 2D discrete wavelet transform technique with a proposed hybrid encryption scheme. The presented hybrid encryption scheme is derived by the integration of Blowfish and Two fish encryption algorithms. The presented model begins with the encryption of secrecy data and then concealed the outcome by the use of outcome in a cover image and 2D-DWT-1L or 2D-DWT-2L. The color images are utilized as cover images for concealing various text sizes. The outcome of the projected technique is tested against different benchmark images and the results are ensured by the use of different performance measures.**

Keywords— Cloud Computing, Medical data, Encryption, Blowfish

I. INTRODUCTION

Due to the recent advancements in the IoT and cloud healthcare based models, massive amount of healthcare data is being transmitted over the network. It is essential to design a proficient approach for ensuring the secrecy and reliability of the patient's diagnosis information communicated from IoT environment [1]. This intention has been takes place by steganographic approaches and data encryption models for hiding data to an image. Encryption cryptography is the procedure of encoding messages so that the attackers could not read it and can be decoded by a legal user. The advantages of steganography are that it could be employed for the transmission of secret images in a concealed manner. At the same time, discrete wavelet transform holds massive spatial localization, frequency spread, and multi resolution features that are equivalent with the concept of human visual system (HVS). This study designs 1 and 2 levels of DWT steganography approaches which work on frequency spectrum. It divides an image into the regions of high as well as low iterations. The former one holds edge details, and at the same time, the latter one is split into high and low iteration regions. The aim of steganography prevent the existence of secret data, however, it also removes the doubt of holding concealed data. The message is a top secret data to be communicated and masked in the carrier so that it is hard to identify. A set of two dimensions namely capacity and imperceptibility are present in any stenographic models. But, these two characteristics are not clear due to the fact that it is hard to raise the capacity by maintaining the steganography imperceptibility.

Initially, an extensive study has been done in Abdulaziz Shehab *et al.* [2] on the basis of security problems in IoT networks. Different types of security parameters like authentication, integrity, confidentiality has been explained. A relative study of diverse attacks, behavior, and risk factors which are classified as given in the following:

- Low-level attacks
- Medium-level attacks
- High-level attacks
- Extremely high-level attacks

Bairagi *et al.* [3] deployed a 3 color image steganography methodologies to protect the data present in IoT structure. The first as well as third model applies 3 (red, green, and blue) channels, whereas second technique employs 2 (green and blue) channels to hold the data. Subsequently, dynamic positioning models are employed to hide data in a deeper layer of image channels under the application of a shared secret key.

This study presents a new hybridization of data encryption model for securing the diagnosis information about the medical images. The proposed model is presented using the integration of 2D discrete wavelet transform model with hybrid encryption approach. The presented hybridization model is derived by the integration of Blowfish and Two fish encryption algorithms. The presented model begins with the encryption of secrecy data and then concealed the outcome by the use of outcome in a cover image by the use of 1L and 2L of 2D DWT. The color images are utilized as cover images for concealing various sizes of text. The performance of the proposed model has been tested against different benchmark images and the results are ensured by the use of different performance measures.

II. Related works

Anwar *et a*l. [4], implemented as model to protect any kind of images more specifically clinical images. It aims to balance the integrity of digitalized clinical data which ensures the accessibility of desired information, and integrity of information to assure the authority of people can use the data. Initially, AES encryption model is used on primary region. The ear print has been incorporated in this process, from where 7 values are filtered as feature vector from the ear image. The developed model enhanced the security for clinical images by forwarding images through online that has to be provided with more security to avoid the access of third party. Ahmed Abdelaziza *et al.* [5], studied a examination of the security liabilities and the threatening facts predicted in movable medical applications. Based on the risk factors, it has been split into remote observation, diagnosis maintain, management maintenance, medical data, education consciousness, interaction and training for healthcare employees. Also, it is added with 8 secured vulnerabilities as well as 10 risks factors forecasted by WHO (OWASP) mobile secured model in 2014 are examined.

Razzaq *et al*. [1] projected a fused security technique on the basis of encryption, steganography, as well as watermarking frameworks. It degraded as 3 levels; encryption of cover image by applying XOR operation, incorporating by least significant bit (LSB) to produce stego image, and watermark the stego image in spatial as well as frequency applications. The practical outcome ensures that the presented technique is more effective and protected. Jain *et al*.[6] implied a novel method to transmit patient medical details into medical cover image. It is performed to conceal information with the application of DT model. Here, a coding is processed as diverse blocks which are distributed in a similar manner. The secret code blocks have been declared for cover image to include data by matching technique like breadth-first search (BFS). In addition, RSA method has been employed to encipher the data in prior to embed the data. Yehia *et al.* [7] modeled diverse healthcare domains on the basis of wireless medical sensor network (WMSN).

In Zaw *et al*. [8], a framework on classifying the actual image into set of blocks has been presented, such that the blocks are organized as turns with the application of transformation methods. Then, a converted image is encrypted by employing Blowfish technology. It have been identified that association minimizes the entropy by improving the number of blocks with the application of minimum sized blocks. Sreekutty *et al.* [9] signified a medical integrity validation method to enhance the trust of clinical image. Hence, the projected technique is degraded as 2 steps: protection as well as verification. By using protection state, the binary format of secrecy information is incorporated in high frequency portion (HH) inside the cover image by utilizing 2-dimension Haar DWT frequency application method. While in case of verification, the derivation technique is employed to derive the actual cover image as well as hidden data.

Followed by, Bashir *et al.* [10] presented an image encryption model on the basis of combining transformed image blocks as well as the fundamental AES. Therefore, shifted method is utilized to segment the images as blocks. Every block is constrained with massive pixels, and it is shuffled under the application of shift model which modifies the place of rows and columns of actual image to generate shifted image. As a result, the shifted image is applied as input image for AES model for encrypting the pixels of shifted image.

III. Proposed Model

This study presents a healthcare security technique to secure the clinical data or details transmission in IoT platforms. The projected method is composed with 4 regular operations that are given as follows:

- The secret patient's information undergoes encryption with the help of developed hybrid encrypting model which has been deployed from Blowfish as well as Two-fish encrypting techniques.
- The already encoded information is concealed from cover image under the application of 1L and 2L of 2D DWT and generates a stego- image.
- The incorporated data has been obtained.
- The filtered data is again decoded to derive the actual data.

A. Data Encryption model

The developed method executes a cryptographic approach. Then, cryptographic model $\hat{C} = \{fnj, fi]^{-1}, C, S, T\}$ is comprised with encrypting and decrypting process. The whole encryption function has a plain text T which is classified to odd portion T_{odd} as well as even regions T_{even}. Here, Blowfish model is employed for encrypting T_{odd} with the help of secret public key s. While Two-fish method is employed to encrypt T_{even} under the application of secret public key m. The private key x has been applied in decrypting task at reception side undergoes encryption by applying Blowfish technology as well as forwarded to destination in encoded format to improve the level of security. The encryption technique could be numerically labelled as provided in the given notations.

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

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

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

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

1) Blowfish

It is a symmetrical cryptographic technique used in common applications. It is employed with massive number of cipher block as well as encryption product, along with SplashID. Its trust is sampled and proved. Since the public application of cipher, it is subjected to important cryptanalysis, as well as complete algorithm could not be broken. It is a rapid block cipher for general application, which makes an ideal product such as SplashID which performs on wider processors explored in smartphones and notebook.

It is used for replacing the classical DES and free from linked with alternate process. Blowfish is comprised with a block size 64-bits and key length of 32-448 bits. It is defined as16-round Feistel cipher and applies massive key-dependent S-boxes. It is same in arrangement to CAST-128 that applies S-boxes.

As Blowfish is considered to be Feistel network, it is inverted to XORing P17 and P18 for encrypting text blocks, then applying P-entry in backwards. Key allocates by initializing P-array as well as S-box with rates obtained from hexadecimal digits of pi that has no definite patterns. The secrecy key is again XOR with P-entries. The final outcome cipher text will replace P1 as well as P2. Furthermore, it is encrypted with the application of novel subkeys, and P3 and P4 are substituted by fresh ciphertext.

2) *Twofish*

It is defined as symmetric block cipher where an individual key is employed to encrypt and decrypt. It is composed with 128 bit blocks, and agrees a different key length of 256 bits. It is also a rapid model for 32-bit and 8-bit CPUs and hardware. It is more flexible and applied in network domains where it has the keys altered frequently and no RAM and ROM existence. It is assumed to be a Feistel network which refers that for all iterations, partial text block is forwarded by F function, and XOR with alternate halves of text blocks. DES is a Feistel network. 5 of AES submissions are named as Feistel networks. It has been surveyed from cryptography, and to understand the working process.

For all iterations of Twofish, a set of two 32-bit words are provided as input for F function. All words are split into 4 bytes, and 4 bytes are forwarded by four various key-dependent S-box. Hence, a set of outcome bytes as the S-box composed with 8-bit input as well as output are mixed with the application of Maximum Distance Separable (MDS) matrix and joined into a 32-bit word. Furthermore, two 32-bit words are integrated by employing Pseudo-Hadamard Transform (PHT), included to 2 round sub-keys, then XORed again with right halves of a text. In addition, 2 1-bit rotations are carried out, 1 previous to and another one after XOR. Twofish includes "pre-whitening" and "post-whitening;" extra subkeys that have been XORed as text block of before the initial iteration as well as after the final process. Twofish screams on maximum end CPUs, and reliable for minimum smart-card CPUs.

Most of the encryption techniques are composed with key-setup routines, a path of consuming the key and form a round sub keys which is applied by a model. It requires a key and forms key-dependent S-box as well as round sub keys. It also needs a similar function, which is very slow in fixing the key that takes 521 encryptions. It is fast in setting up the keys as 1.5 encryptions.

Twofish is composed with different options. Either it may consume longer time of key setup and encryption runs in rapid manner; which forms a sense to encrypt more number of plaintext using same key. The key might be fixed rapidly while encryption is minimum which sense an encryption of small blocks with faster alteration keys.

B. Embedding Procedure

Here, Haar-DWT has been executed. The entire Haar-DWT, 2L 2D DWT could be formed as subsequent conversion with the help of low-pass as well as high pass filters for rows of images; subsequently the final outcome is degraded into columns of the image. The unit degradation of $C_j(n, m)$ image size $N \times M$ in 4 reduced sub band images that have been named as high high (HH), high low (HL), low high (LH), and a low low (LL) frequency bands.

The projected model executes the steganographic approach. It is $\hat{S} = \{f\eta, f\eta^{-1}, C, S, T\}$ filled with embedding as well as extraction function. As the embedding task consumes a cover image C and undisclosed text message T as input and produce a stego image S. Since the extraction task is helpful in extracting the integrated message. It is modeled in a mathematical function as provided in the following equations.

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

The overall embed task has the secrecy text as converted to ASCII form and separated as even as well as odd values. Here, odd ones undergo concealment in vertical coefficients defined by $LH2$. Besides, the even ones are hidden from diagonal coefficients processed by HH2.

C. Extraction Process

Once text is incorporated to the cover image, the 2L 2D DWT model is processed to obtain secret text as well as to derive cover image. After extracting the secret message, the cover image has been designed from reformed estimate by inducing inverse DWT for alternate levels.

D. Decryption

After the extraction process gets completed, the decryption process will begin. It is defined as transforming encrypted data to user readable form; that is the upside down process of encryption technique. The proposed method follows symmetrical encryption where the encryption and decryption process are identical to one another, but follows in a reverse direction. In the decryption process, the similar key is applied by sender which should be employed to cipher text to the entire encryption task. It indicates that the key used for encryption and decryption is similar. The decryption could be defined in mathematical format in the form of given functions.

IV. Performance Evaluation

For experimentation, a set of two benchmark dataset, namely DR dataset [13] and Kvasir dataset [13] is used. Fig. 1 shows the sample medical images, comprising the images from DR [12] and WCE images [13].

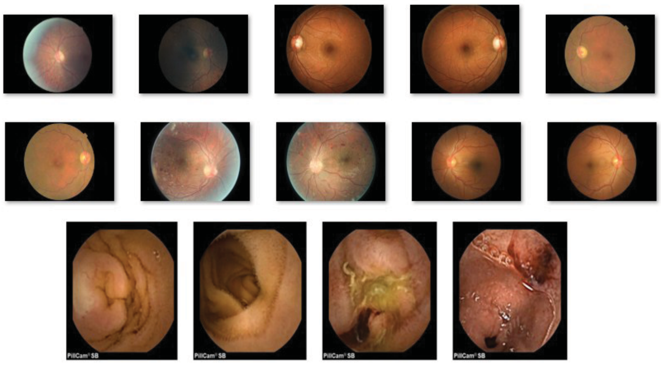
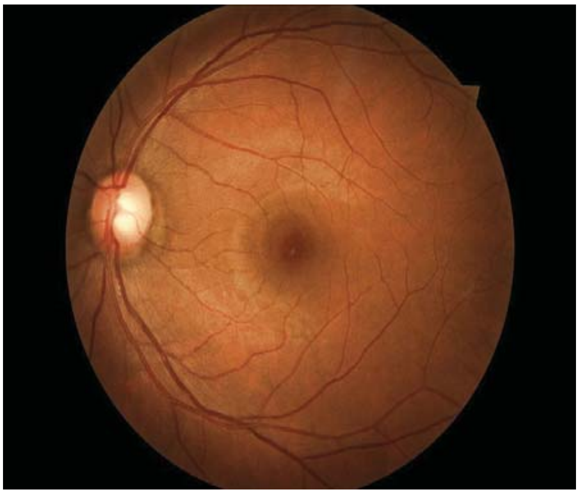
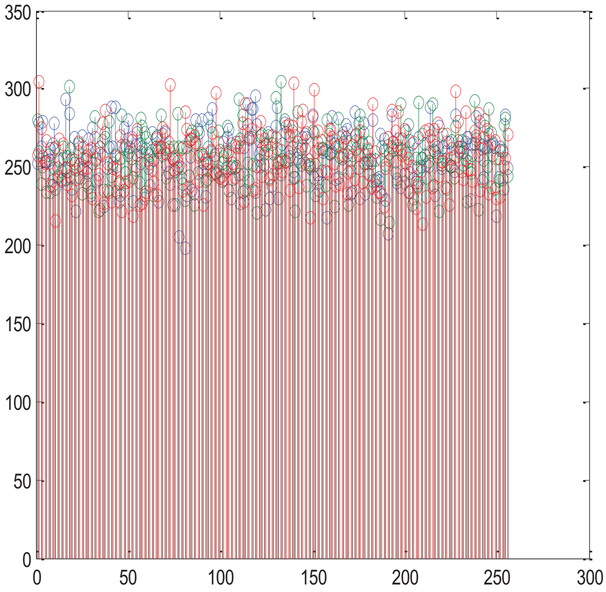


Fig. 1. Sample test images

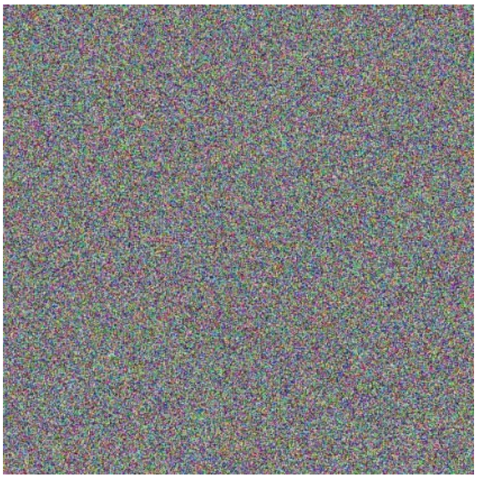
Fig. 2 shows the original image along with its original image along with its histogram. Fig. 2a shows the original DR image along with its corresponding histogram of the applied image. Fig. 2c shows the encrypted form of the DR input image.



(a)Input image



(b) Histogram of Input image



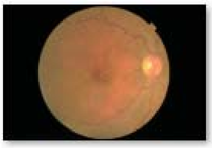
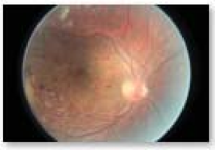
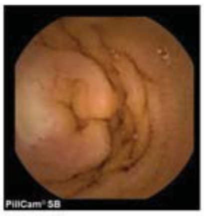
(c)Histogram of Encrypted Image

Fig. 2. Results offered by proposed model

Table 1 and Fig. 3 shows the visualization of the results attained by different models under the applied set of images. The table values indicated that the employed image “Image 001” is encrypted by the use of 256 bytes and offered a minimum MSE of 0.10 and PSNR of 58.13. The applied image “Image 002” exhibits that the encrypted image is provided with the MSE of 0.08 and 59.09. Similarly, the image “Image 003” exhibits that the encrypted image is provided with the MSE of 0.07 and 59.67.

TABLE I

MSE AND PSNR VALUES OF PROPOSED METHOD FOR COLOR IMAGES

Images	Image Code	Text size (Bytes)	MSE	PSNR
	001	256	0.10	58.13
	002	256	0.08	59.09
	003	256	0.07	59.67

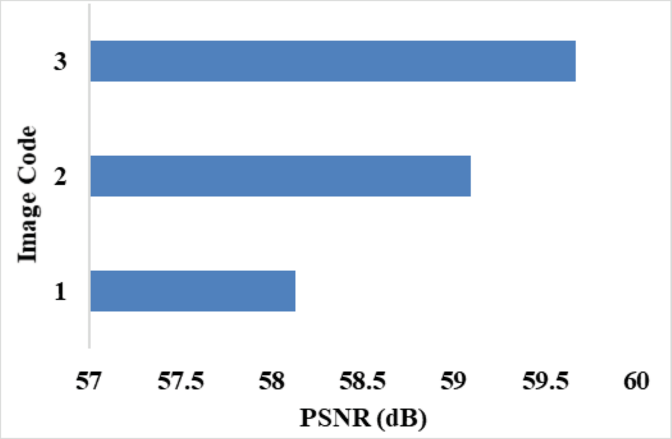


Fig. 3. PSNR analysis of proposed method

Fig. 4 shows the results offered by the proposed model under different set of test images. Table 2 provides a comparison of the results attained by diverse models on the applied set of images interms of MSE and PSNR. The table values portrayed that the existing that Anwar et al. showed the ineffective performance on the applied set of images by offering a maximum MSE of 0.13 and minimum PSNR of 56.76dB respectively. At the same time, the Elhoseny et al. model has offered slightly better results by attaining a lower MSE and higher PSNR of 0.12 and 57.02dB respectively. However, it is interesting that the proposed model has attained supreme results by offering a minimal MSE of 0.08 and maximum PSNR of 58.96dB respectively.

TABLE II

RESULTS OF PROPOSED WITH EXISTING METHODS

Methods	MSE	PSNR
Proposed	0.08	58.96
Elhoseny et al. [11]	0.12	57.02
Anwar et al.	0.13	56.76

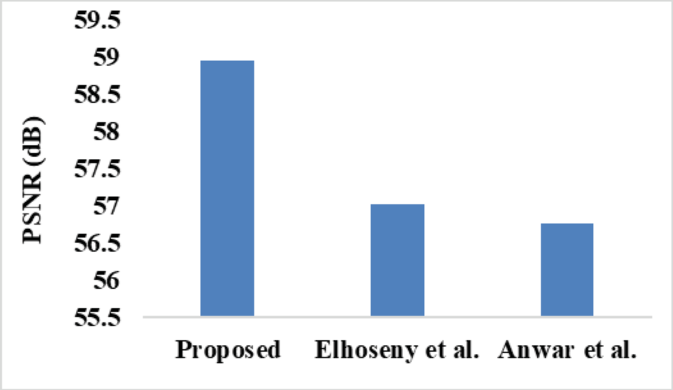


Fig. 4. PSNR analysis of diverse models

V. CONCLUSION

This study has presented a new hybridization of data encryption model for safeguarding the diagnosis data in medical images. The proposed model is presented by the integration of 2D DWT process with a hybridization of Blowfish and Two fish encryption algorithms. The presented model begins with the encryption of secrecy data and then concealed the outcome by the use of outcome in a cover image by the use of 1L and 2L 2D DWT. The color images are utilized as cover images for concealing various text sizes. The performance of the proposed model has been tested against different benchmark images and the results are ensured by the use of different performance measures. It is interesting that the proposed model has attained supreme results with a minimal MSE of 0.08 and maximum PSNR of 58.96dB.

REFERENCES

[1] Razzaq, M. A., Sheikh, R. A., Baig, A., & Ahmad, A. “Digital image security: Fusion of encryption, steganography and watermarking”. International Journal of Advanced Computer Science and Applications (IJACSA), 8(5), 2017.

[2] Abdulaziz Shehab, Mohamed Elhoseny, Khan Muhammad, Arun Kumar Sangaiah, Po Yang, Haojun Huang, Guolin Hou; Secure and Robust Fragile Watermarking Scheme for Medical Images, IEEE Access, 2018, Volume: PP, Issue: 99

[3] Bairagi, A. K., Khondoker, R., & Islam, R.. “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, 2016.

[4] Anwar, A. S., Ghany, K. K. A., & Mahdy, H. E.. "Improving the security of images transmission". International Journal, 3(4), 2015.

[5] 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.

[6] Jain, M., Choudhary, R. C., & Kumar, A., "Secure medical image steganography with RSA cryptography using decision tree", In Contemporary Computing and Informatics (IC3I), 2016 2nd International Conference on (pp. 291-295). IEEE.

[7] Yehia, L., Khedr, A., & Darwish, A., "Hybrid security techniques for Internet of Things healthcare applications", Advances in Internet of Things, 2015, 5(03).

[8] Zaw, Z. M., & Phyo, S. W., "Security Enhancement System Based on the Integration of Cryptography and Steganography", International Journal of Computer (IJC), 2015, 19(1), 26-39.

[9] Sreekutty, M. S., & Baiju, P. S., "Security enhancement in image steganography for medical integrity verification system", In Circuit, Power and Computing Technologies (ICCPCT), 2017 International Conference on (pp. 1-5). IEEE.

[10] Bashir, A., Hasan, A. S. B., & Almangush, H., "A new image encryption approach using the integration of a shifting technique and the AES algorithm", International Journal of Computers and Applications, 42(9), 2012.

[11] Elhoseny, M., Ramírez-González, G., Abu-Elnasr, O.M., Shawkat, S.A., Arunkumar, N. and Farouk, A., "Secure medical data transmission model for IoT-based healthcare systems", *Ieee Access*, *6*, pp.20596-20608, 2018.

[12] https://www.kaggle.com/c/diabetic-retinopathy-detection/data

[13] https://datasets.simula.no/kvasir/#data-collection