JES
Journal of Engineering Sciences

Vol 13, Issue 06, JUNE / 2022

ISSN NO:0377-9254

A NOVEL SYSTEM TO ENCRYPT BIO MEDICAL DATA

[1]Prathyusha Muthukur,[2]Shaik Misbah Nurein

[3]Leena Goyal Dudekula,[4]Y. Prashanthi

[5]Kadire Meghana

[6]M Janardhan

[1,2,3,4,5,]STUDENT [6] ASSISTANT PROFESSOR

G PULLAIAH COLLEGE OF ENGINEERIONG AND TECHNOLOGY - KURNOOOL

ABSTRACT:

I. Because of the critical headway of the web of things (IoT) in the medical services area, the security and the trustworthiness of the clinical information turned out to be huge difficulties for medical services administrations applications. This paper proposes a half breed security model for getting the demonstrative text information in clinical pictures. The proposed model is created through incorporating either 2D Discrete Wavelet Transform 1 Level (2D-DWT-1L) or 2D Discrete Wavelet Transform 2 Level (2D-DWT-2L) steganography strategy with a proposed half and half encryption plot. The proposed cross breed encryption composition is fabricated utilizing a mix of Advanced Encryption Standard (AES), and Rivest, Shamir, and Adleman (RSA) calculations. The proposed model beginnings by encoding the restricted information; then, at that point, it conceals the outcome in a cover picture utilizing 2D-DWT-1L or 2D-DWT-2L. Both variety and dark scale pictures are utilized as cover pictures to hide different text sizes. The exhibition of the proposed framework was assessed in view of six factual boundaries; the Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE), Bit Error Rate (BER), Structural Similarity (SSIM), Structural Content (SC), and Correlation. The PSNR values were generally shifted from 50.59 to 57.44 in the event of variety pictures and from 50.52 to 56.09 with the dim scale pictures. MSE values changed from 0.12 to 0.57for the variety pictures and from 0.14 to 0.57 for the dim scale pictures. BER values were zero for the two pictures, while SSIM, SC and Correlation values were ones for the two pictures. Contrasted with the cutting edge strategies, the proposed model demonstrated its capacity to conceal the private patient's information into a communicated cover picture with high subtlety, limit, and negligible weakening in the got stego-picture.

I. INTRODUCTION

IoT creates an integrated communication environment of interconnected devices and platforms by engaging both virtual and physical world together [1]. 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 [2-8]. This goal is carried out using steganography techniques and system encryption algorithms together to hide digital information in an image [9- 16]. Cryptography is another term for data encryption [17]. 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 [18].

AES is a symmetric cipher where the same key is used on both sides [19]. 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 [20]. It has the advantage of having a variable key size ranging from (2-2048) bits. The primary research in hiding data started with steganography, which refers to the science and art of hiding information within an image. The benefit of steganography is that it can be utilized to transmit classified messages without the fact of the transmission being detected.

The DWT has a tremendous spatial localization, frequency spread, and multiresolution characteristics, which are matching with the theory of forms in the human visual system. 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 [21]. The purpose of the steganography is not only preventing others from knowing the hidden information, but also removing the suspicion in having hidden information.

The message is a confidential document to be transmitted and camouflaged in the carrier so that it becomes difficult toI. INTRODUCTION IoT creates an integrated communication environment of interconnected devices and platforms by engaging both virtual and physical world together [1]. 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 [2-8]. This goal is carried out using steganography techniques and system encryption algorithms together to hide digital information in an image [9-16]. Cryptography is another term for data encryption [17].

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 [18]. AES is a symmetric cipher where the same key is used on both sides [19]. 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 [20]. It has the advantage of having a variable key size ranging from (2-2048) bits. The primary research in hiding data started with steganography, which refers to the science and art of hiding information within an image. The benefit of steganography is that it can be utilized to transmit classified messages without the fact of the transmission being detected. The DWT has a tremendous spatial localization, frequency spread, and multiresolution characteristics, which are matching with the theory of forms in the human visual system. 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 [21]. The purpose of the steganography is not only preventing others from knowing the hidden information, but also removing the

suspicion in having hidden information. The message is a confidential document to be transmitted and camouflaged in the carrier so that it becomes difficult toII.

II. MAIN OBJECTIVE

(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 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.

III. LITERATURE REVIEW

Security enhancement in image steganography for medical integrity verification system. In Circuit, Power and Computing Technologies

Nowadays image steganography has major role in confidential medical image communication. When the medical image is transmitted through insecure public network, there is a chance for tampering medical images. Therefore, it is crucial to check the integrity of medical images to prevent any unauthorized modification. To check the integrity we calculate cryptographic hash function of ROI (Region Of Interest) by using SHA algorithm. The hash value (H1) will be embedded in the RONI using discrete wavelet transform. By comparing the hash value at receiver side, we can check the integrity of medical image. If any tampering occurs, the hash function does not match. This paper proposes a new method to improve the security. The modified medical image is embedded in an ordinary looking image by spatial reversible steganography method. It helps to conceal the existence of secret medical data. It ensures that the eavesdroppers will not have any suspicion that medical image is hidden in that image. This combined approach will give enhanced security.

Internet of Things: Securing Data Using Image Steganography

Internet of Things (IoT) is a common thing (object) in today's world, which serves as part of our routine life activities. Although it benefits the residential district in several ways, various challenges such as data confidentiality and privacy are created. As a matter of fact, the community is concerned what information may leak out via IoT. Therefore, the needs of a secure

environment is vital in order to secure the transmitting data from it devices over the network. As a result, in this paper, a secure scheme is suggested on using image steganography as an alternative security mechanism in conjunction with a home server to secure the transmitted data from IP camera as the IoT device to the other devices, either in LAN or WAN networks.

The Application of Hybrid Encryption Algorithm in Software Security

Because of the defect of only the single data encryption and the use of famous encryption algorithm, which was not improved in traditional methods of the registration process, a combined encryption algorithm is proposed in this thesis. That is, the algorithm security is greatly improved, through researching several famous data encryption algorithms, and improving some data encryption algorithms, and arranging encryption algorithms in some order. Finally, the combined encryption algorithm is successfully made by using the initial encryption algorithm, Micro Genard encryption algorithm and the famous Base64 encryption algorithm. That is, in accordance with the order of the initial encryption algorithm, the improved Micro Genard encryption algorithm and the famous Base64 encryption algorithm, the user's information is gradually encrypted, and the algorithm security is greatly enhanced. Besides, to video surveillance software system for instance, which is widely used in the field of the traffic security management, the combined encryption algorithm is completely validated, and its security is very high.

Image quality assessment: from error visibility to structural similarity

Objective methods for assessing perceptual image quality traditionally attempted to quantify the visibility of errors (differences) between a distorted image and a reference image using a variety of known properties of the human visual system. Under the assumption that human visual perception is highly adapted for extracting structural information from a scene, we introduce an alternative complementary framework for quality assessment based on the degradation of structural information. As a specific example of this concept, we develop a structural similarity index and demonstrate its promise through a set of intuitive examples, as well as comparison to both subjective ratings and state-of-the-art objective methods on a database of images compressed with JPEG and JPEG2000.

Security enhancement in image steganography for medical integrity verification system

Nowadays image steganography has major role in confidential medical image communication. When the medical image is transmitted through insecure public network, there is a chance for tampering medical images. Therefore, it is crucial to check the integrity of medical images to prevent any unauthorized modification. To check the integrity we calculate cryptographic hash function of ROI (Region Of Interest) by using SHA algorithm. The hash value (H1) will be embedded in the RONI using discrete wavelet transform. By comparing the hash value at receiver side, we can check the integrity of medical image. If any tampering occurs, the hash function does not match. This paper proposes a new method to improve the security. The modified medical image is embedded in an ordinary looking image by spatial reversible steganography method. It helps to conceal the existence of secret medical data. It ensures that the eavesdroppers will not have any suspicion that medical image is hidden in that image. This combined approach will give enhanced security.

IV. EXISTING SYSTEM

Here 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.

5. METHODOLOGY

Razzaq, M. A, et al. [2], surveyed a comprehensive study on security issues in IoT networks. Various security requirements such as authentication, integrity, confidentiality were discussed. A comparative study of different types of attacks, their behavior, and their threat level that categorized into lowlevel, medium-level, high-level, and extremely high-level attacks and suggested possible solutions to encounter these attacks were provided. Bairagi, A. K., et al. [3], 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. [4], 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. Cifuentes, Y., et al. [5], surveyed the analysis of the security vulnerabilities and the risk factors detected in mobile medical apps. According to risk factor standards, these apps can be categorized into remote monitoring, diagnostic support, treatment support, medical information, education and awareness, and communication and training for healthcare workers. Eight security vulnerabilities and ten risks factors detected by the World Health Organization (OWASP) mobile security project in 2014 have been analyzed.

III. THE PROPOSED MODEL

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 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.

V. ADVANTAGES AND APPLICATIONS

- The proposed model starts by encrypting the secret data.
- 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.
- It has the advantage of having a variable key size.
- Healthcare enables interoperability, machine-to-machine communication.
- The systems can collect data about patient health status through multiple sensors.
- For securing the diagnostic text data in medical images.
- Steganography technique with a proposed hybrid encryption scheme
- Combination of Advanced Encryption Standard (AES), and Rivest, Shamir, and Adleman (RSA) algorithms
- For encrypting the secret data.

VI. 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 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 transmitted cover image with high imperceptibility, capacity, and minimal deterioration in the received stego-image.

VII. REFERENCES

[1] Ashraf Darwish, Aboul Ella Hassanien, Mohamed 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)

[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, Volume: PP, Issue: 99, (DOI: 10.1109/ACCESS.2018.2799240).

[3] 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.

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

[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, 2018 (https://doi.org/10.1016/j.measurement.2018.01.022)

[6] 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.

[7] Muhammad Sajjad, Mansoor Nasir, Khan Muhammad, Siraj Khan, Zahoor Jan, Arun Kumar Sangaiah, Mohamed Elhoseny, Sung Wook Baik, "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)

[8] Kumar, P., & Lee, H. J. (2011). Security issues in healthcare applications using wireless medical sensor networks: A survey. Sensors, 12(1), 55-91.

[9] 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).

[10] Dey, N., & Santhi, V. (Eds.). (2017). Intelligent Techniques in Signal Processing for Multimedia Security. Springer International Publishing.

[11] Jain, M., Choudhary, R. C., & Kumar, A. (2016). 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.

[12] Yehia, L., Khedr, A., & Darwish, A. (2015). Hybrid security techniques for Internet of Things healthcare applications. Advances in Internet of Things, 5(03), 21.

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

[14] Gupta, R. K., & Singh, P. (2013). A new way to design and implementation of hybrid crypto system for security of the information in public network. International Journal of Emerging Technology and Advanced Engineering, 3(8), 108- 115.

[15] Laskar, S. A., & Hemachandran, K. (2012). High Capacity data hiding using LSB Steganography and Encryption. International Journal of Database Management Systems, 4(6), 57.

[16] Yu, L., Wang, Z., & Wang, W. (2012). The application of hybrid encryption algorithm in software security. In Computational Intelligence and Communication Networks (CICN), 2012 Fourth International Conference on (pp. 762- 765). IEEE.

[17] Mare, S. F., Vladutiu, M., & Prodan, L. (2011). Secret data communication system using Steganography, AES and RSA. In Design and Technology in Electronic Packaging(SIITME), 2011 IEEE 17th International Symposium for (pp. 339-344). IEEE.

[18] Mandal, A. K., Parakash, C., & Tiwari, A. (2012). Performance evaluation of cryptographic algorithms: DES and AES. In Electrical, Electronics and Computer Science (SCEECS), 2012 IEEE Students' Conference on (pp. 1-5). IEEE.

[19] Mjolsnes, Stig F. (Eds.). (2011). A Multidisciplinary Introduction to Information Security. CRC Press.

[20] Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 21(2), 120-126.

[21] Sreekutty, M. S., & Baiju, P. S. (2017). 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.

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

[23] Muhammad, K., Ahmad, J., Farman, H., Jan, Z., Sajjad, M., & Baik, S. W.

(2015). A Secure Method for Color Image Steganography using Gray-Level Modification and Multi-level Encryption. TIIS, 9(5), 1938-1962.

[24] Yin, J. H. J., Fen, G. M., Mughal, F., & Iranmanesh, V. (2015). Internet of Things: Securing Data using Image Steganography. In Artificial Intelligence, Modelling and Simulation (AIMS), 2015 3rd International Conference on (pp. 310-314). IEEE.

[25] Seyyedi, S. A., Sadau, V., & Ivanov, N. (2016). A Secure Steganography Method Based on Integer Lifting Wavelet Transform. IJ Network Security, 18(1), 124-132.

[26] Khalil, M. I. (2017). Medical Image Steganography: Study of Medical Image Quality Degradation when Embedding Data in the Frequency Domain. International Journal of Computer Network and Information Security, 9(2), 22.

[27] Abdel-Nabi, H., & Al-Haj, A. (2017). Efficient joint encryption and data hiding algorithm for medical images security. In Information and Communication Systems (ICICS), 2017 8th International Conference on (pp. 147-152). IEEE.

[28] Li, L., Hossain, M. S., El-Latif, A. A. A., & Alhamid, M. F. (2017). Distortion less secret image sharing scheme for Internet of Things system. Cluster Computing, 1-15.

[29] Sajjad, M., Muhammad, K., Baik, S. W., Rho, S., Jan, Z., Yeo, S. S., & Mehmood, I. (2017). Mobile-cloud assisted framework for selective encryption of medical images with steganography for resource-constrained devices. Multimedia Tools and Applications, 76(3), 3519-3536.

[30] Parah, S. A., Sheikh, J. A., Ahad, F., & Bhat, G. M. (2018). High Capacity and Secure Electronic Patient Record (EPR) Embedding in Color Images for IoT Driven Healthcare Systems. In Internet of Things and Big Data Analytics Toward Next-Generation Intelligence (pp. 409-437). Springer, Cham.

[31] Johnson, N. F., & Jajodia, S. (1998). Exploring steganography: Seeing the unseen. Computer, 31(2).

[32] Jassim, F. A. (2013). A novel steganography algorithm for hiding text in image using five modulus method. arXiv preprint arXiv:1307.0642.

[33] Wikipedia contributors. Mean absolute error. https://en.wikipedia.org/wiki/Mean_absolute_error

[34] Wang, Z., Bovik, A. C., Sheikh, H. R., & Simoncelli, E. P. (2004). Image quality assessment: from error visibility to

structural similarity. IEEE transactions on image processing, 13(4), 600-612.

[35] ECE, C., & Mullana, M. M. U. (2011). Image quality assessment techniques in spatial domain. Int. J. Comput. Sci. Technol, 2(3).

[36] Silva, E. A., Panetta, K., & Agaian, S. S. (2007). Quantifying image similarity using a measure of enhancement by entropy. Mobile Multimedia/Image Processing for Military and Security Applications, 6579, 65790U.

[37] Rabbani, H., Allingham, M. J., Mettu, P. S., Cousins, S. W., & Farsiu, S. (2015). Fully Automatic Segmentation of Fluorescein Leakage in Subjects With Diabetic Macular EdemaAutomatic Leakage Segmentation in DME. Investigative ophthalmology & visual science, 56(3), 1482-1492.

[38] McEvoy, F. J., & Svalastoga, E. (2009). Security of patient and study data associated with DICOM images when transferred using compact disc media. Journal of digital imaging, 22(1), 65-70.