ISSN 2063-5346

DEEP LEARNING BASED IMAGE ENCRYPTION AND DECRYPTION

Mr.M.Prakash[1], Saravanan S[2], Suthi G[3], Sasikumar R[4]

Article History: Received: 01.02.2023 Revised: 07.03.2023 Accepted: 10.04.2023

Abstract

The suggested approach generates a sample medical picture. A new hybrid security algorithm for the RSA cryptosystem is described. For decryption and encryption, the system employs two distinct keys: a private key and a public key. As a result, it provides a more secure channel for the encryption and decryption processes. The phi generates the value of n public keys and n private keys, as well as completing the decryption and encryption operations. A reconstruction network is used to restore the encrypted image to the original (plaintext) image. To ease data mining straight from the privacy-protected environment, an area of interest (ROI)-mining-network is developed to extract the interesting item from the encrypted picture. The suggested method is evaluated using a medical X-ray dataset. Comprehensive experimental results and security evaluations show that the proposed approach may give a significant level of safety while remaining efficient. This project's front end is written in MATLAB JAVA. The identification of medical photographs is widespread. To encrypt and decrypt the binary data, we employ the RSA model for safe encryption and the stegno image model. The most famous and commonly used cryptosystem is RSA, whose security is determined by the difficulty of obtaining the private key in an acceptable amount of time rather than the algorithm's specifics. RSA requires the highest type of representation in the picture encryption field to achieve maximum security.

Keywords: Deep learning, Image.

[1]Assistant Professor, Department of Computer Science and Engineering, K.S.Rangasamy College of Technology, Tiruchengode-637 215.

[2,3,4]Students, Department of Computer Science and Engineering, K.S.Rangasamy College of Technology, Tiruchengode-637215.

prakashm@ksrct.ac.in[1],saravanan472002@gmail.com [2], suthiganesan77@gmail.com[3], sasikumarcse28@gmail.com[4]

DOI:10.31838/ecb/2023.12.s1-B.393

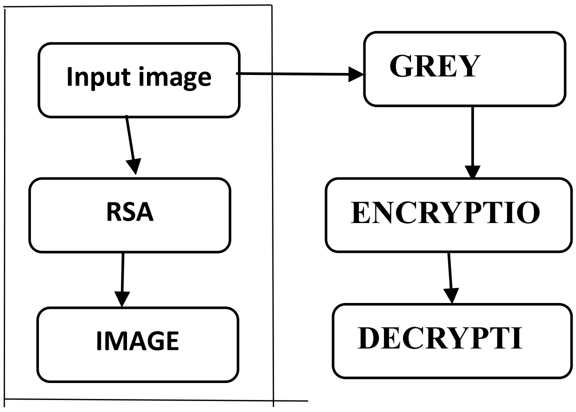
1.INTRODUCTION

1.1 ABOUT THE PROJECT

The Internet of Medical Things (IoMT), often referred to as the Internet of Medicine (IoM), is a multidisciplinary area that utilises Internet of Things (IoT) technologies to medical applications. With the advancement of IoMT, numerous medical imaging devices, such as brain magnetic resonance imaging (MRI) for brain tumor diagnosis and computerized tomography (CT) of the lung for lung nodule identification, have become widely attached and used to aid physicians in the diagnosis and treatment process. Medical pictures are typically kept in IoMT using a system known as Picture Archival and Telecommunication Networks (PACS) When a patient is scanned with medical imaging equipment, the images are saved in the PACS at first. As the doctor starts assessing the patient, the PACS retrieves the images from the database and transports them to the doctor's workstation, which is connected to the hospital's information system (HIS). With the rapid advancement of clinical gadget innovation, it became simple to assess various illnesses employing clinical images. Clinical images are supplied through many organizations; so, obtaining these images has recently become a critical issue. Confidentiality, honesty, and verification are required for the secure sharing of clinical pictures. Illegal use of such photos may jeopardize patient information security. Additionally, when these photos are pressed for any slight alteration, it may result in an inaccurate analysis, putting patients' lives in jeopardy. Image steganography, picture watermarking, and image encryption are common methods for obtaining digital images. Encryption is the simplest and most efficient approach for assuring clinical picture security, transforming a basic image into an incomprehensible one with the use of a secret key. Nobody will be able to restore the basic image unless they have access to that weird key. Picture encryption is based on two key activities: confusion and dispersion. Traditional encryption algorithms are inadequate for complicated photographs, particularly clinical shots, because to the close relationship between image pixels, large-scale images, and information repetition. To decrease connection and excess, some clinical picture encryption calculations have been provided.

IMAGE ENCRYPTION

Encryption refers to the method of entering data in cryptography. The initial data representation, also known as plaintext, is altered during the process into an alternate form called as cypher text. Only authorized individuals should be able to decipher cypher text and retrieve the original data. Encryption does not, in and of itself, preclude interference, but it does limit an interceptor access to comprehensible content. A pseudo-random encryption technique created by an algorithm is widely used in an encryption approach for technical reasons. Although the message may be decrypted without the secret, a well-encrypted solution requires substantial computational resources and experience. The originator's key, which is only disclosed to approved receivers, allows an authorized receiver to readily decode the signal. Many encryption methods have historically been employed to help with cryptography. In the early days, military communications were routinely encrypted. Since that time, new approaches have arisen and spread throughout all aspects of contemporary computing. Public-key and symmetric-key ideas are used in modern encryption systems. Because modern computers are ineffective at cracking encryption, modern encryption techniques give security.



3.EXISTING SYSTEM

Medical JPEG photographs include personal information about the patients, and the protection of that information is becoming increasingly critical as computer and biological technologies develop. Steganography is used to disguise sensitive information in order to safeguard the privacy of medical pictures. The most well-known JPEG steganography techniques integrate information by changing discrete cosine transform (DCT) values, causing the DCT coefficient relationships to be disrupted. In this paper, we present a breakthrough medical JPEG picture steganography approach that utilizes inter-block coefficient relationships. The basic objective is to retain as many disparities between DCT coefficients as feasible in close DCT blocks. The cost amounts are dynamically assigned all through the embedding process based on changes in inter-block neighbors. Experiment findings reveal that the proposed method cluster inter-block embedding changes and beats the current steganography approach.

4.PROPOSED SYSTEM

The input image is chosen, the binary message is inserted, and the grey scale image processing is completed. The message is then buried within the Stego picture. The RSA encryption is completed, and the encrypted picture is displayed as a consequence. The decoded picture is then retrieved. The image is imported with a path name and a file name, and it has a size of 200x200 pixels. Image processing in greyscale occurs. Stego encoding of patient confidential information is performed with the message as input. The cypher procedure is done out by picture encryption using the rsa approach. The decryption model is executed.dec1= decrypting (cipher, enc, d,n);

4.1 LSB

The least significant bit, or LSB, is the bottom bit in a binary numeral sequence. It is the leftmost or rightmost bit in a binary number, depending on the architecture of the system. The arrangement is known to as "little-endian" if the LSB is on the right. The design is known as "big-endian" whenever the LSB is on the left. With a little-endian system, the LSB of binary number 00000001, for example, is 1.

4.2 STEGNO IMAGE

Image Steganography is the process of hiding data within an image file. The image used for this purpose is known as the cover image, and the image obtained after steganography is known as the Stego image. Image steganography is explored, and one method is utilized to demonstrate it since it may be done in a variety of ways. The practice of hiding information in photos is known as image steganography. Here The binary separated value maintains the length of the ascii value, and the counting for the row and column is stated with the LSB for the picture and the binary message is input.

4.3 DECODING

The functionality of the row and size will be identified during the recording process, and the messages in the form of BITS will be carried out to the total number of least significant bit format, followed by the message in the bits being appointed to the total number of binary recording process, where the image will be added to the original string format.

4.4 DECRYPTION

Just compute the plaintext M as: M = Cd mod N to decrypt a cypher text C using an RSA public key. Because both RSA decryption and encryption need modular exponentiation, the Repeated Squares Algorithm should be used to make both approaches relatively efficient.

5. RESULT ANALYSIS

The pixel difference among plain and encrypted photos is used to assess encryption quality. If the difference is considerable, the encryption algorithm is called efficient. Where is the histogram difference between the RSA and the encrypted image Our suggested algorithm's maximum deviation values are presented. The RSA encryption range and the AES encryption range indicate the respective range of values. These figures are entered as approximations.

6. CONCLUSION

Based on picture blocks and chaos, this research developed a novel technique for encrypting medical images. The suggested algorithm's RSA encryption performance, correlation coefficient, differential attack, key space, and key sensitivity have all been satisfactorily evaluated. The suggested approach is effective for encrypting grey scaled medical pictures, according to the results. Our method was put to the test against other modern encryption methods, and the results reveal that the proposed technique is successful for encrypting greyscale medical pictures.

7. REFERENCES

[1] A. Gatouillat, Y. Badr, B. Massot, and E. Sejdic', "Internet of Medical Things: A Review of Recent Contributions Dealing With Cyber-Physical Systems in Medicine," IEEE Internet of Things Journal, vol. 5, no. 5, October 2018, pp. 3810-3822.

[2] N Zhang, P Yang, J Ren, et al., "Big data and 5G wireless network synergy: potential, techniques, and problems," IEEE Wireless Communications, vol. 25, no. 1, pp. 12-18, 2018.

[3] D. Chen, N. Zhang, Z. Qin, X. Mao, Z. Qin, X. Shen, and X. Y. Li, "S2M: A Lightweight Acoustic Fingerprints-Based Wireless Device Authentication Protocol," IEEE Internet of Things Journal, vol. 4, no. 1, Feb. 2017, pp. 88-100.

[4] B. Liu and H. Huang, "Picture archiving and communication systems for the healthcare sector," Biomedical Information Technology, Academic Press, 2020, pp. 105-164.

[5] K. Zhang, J. Ni, K. Yang, X. Liang, J. Ren, and X. S. Shen, "Security and privacy in smart city applications: Challenges and solutions," IEEE Communications Magazine, vol. 55, no. 1, Jan. 2017, pp. 122-129.

D. Chen, N. Zhang, N. Cheng, K. Zhang, Z. Qin, X. Shen, Physical Layer based Message Authentication with Secure Channel Codes, IEEE Transactions on Dependable and Secure Computing, DOI: 10.1109/TDSC.2018.2846258

S. Jaeger, S. Candemir, S. Antani, et.al., “Two public chest X-ray datasets for computer-aided screening of pulmonary diseases,” Quantitative imaging in medicine and surgery, vol. 4, pp. 475-7, Dec. 2014

K. He, X. Zhang, S. Ren and J. Sun, “Deep residual learning for image recognition,” in Proc. IEEE CVPR2016, USA, pp. 770-778, Sept. 2016

A. Ferdowsi and W. Saad, “Deep Learning for signal authentication and security in massive Internet of Things Systems,” IEEE Transactions on

Communications, vol. 67, no. 2, pp. 1371-1387, Feb. 2019.

D. Chen, N. Zhang, et. al., “An LDPC code based physical layer message authentication scheme with prefect security”, IEEE Journal on Selected Areas in Communications, vol. 36, no. 4, pp. 748-761, 2018.