International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 4
DOI: https://doi.org/10.17762/ijritcc.v11i4.6398
***Article Received**: 09 February 2023 **Revised**: 05 March 2023 **Accepted**: 12 March 2023*

Iot Based Alzheimer's Disease Diagnosis Model for Providing Security Using Light Weight Hybrid Cryptography

[*1]Anjani Yalamanchili, [2]Dr. D. Venkatasekhar, [3]Dr. G. Vijay Kumar
[*1]Research Scholar, Department of Information Technology,
Annamalai University, Annamalai Nagar, Tamil Nadu, 608002, India.
Email: anjaniyalamanchili@gmail.com
[2]Professor, Department of Information Technology,
Annamalai University, Annamalai Nagar, Tamil Nadu, 608002, India.
Email: ramavenkatasekar@yahoo.co.in
[3]Professor, Department of Computer Science & Engineering,
SSCET, Challapalli, Andhra Pradesh 521131, India.
[*]Email: vijayg.teja@gmail.com

Abstract- Security in the Internet of things (IoT) is a broad yet active research area that focuses on securing the sensitive data being circulated in the network. The data involved in the IoT network comes from various organizations, hospitals, etc., that require a higher range of security from attacks and breaches. The common solution for security attacks is using traditional cryptographic algorithms that can protect the content through encryption and decryption operations. The existing solutions are suffering from major drawbacks, including computational complexities, time and space complexities, slower encryption, etc. Therefore, to overcome such drawbacks, this paper introduces an efficient light weight cryptographic mechanism to secure the images of Alzheimer's disease (AD) being transmitted in the network. The mechanism involves major stages such as edge detection, key generation, encryption, and decryption. In the case of edge detection, the edge maps are detected using the Prewitt edge detection technique. Then the hybrid elliptic curve cryptography (HECC) algorithm is proposed to encrypt and secure the images being transmitted in the network. For encryption, the HECC algorithm combines blowfish with the elliptic curve algorithm to attain a higher range of security. Another significant advantage of the proposed method is selecting the ideal private key, which is achieved using the enhanced seagull optimization (ESO) algorithm. The proposed work has been tested in the Python tool, and the performance is evaluated with the Alzheimer's dataset, and the outcomes proved its efficacy over the compared methods.

Keywords- Light weight cryptography, Elliptic curve cryptography, blowfish algorithm, enhanced seagull optimization, optimal key selection, denial of services.

I. INTRODUCTION

IoT devices utilize embedding sensors for collecting, exchanging and sharing data with other devices and applications in real time. In the IoT, smart devices, actuators and sensors work together for screening and dealing with physical conditions. Remote patient management (RPM) is employed in more healthcare services, such as in the prominent observation of signals using arrhythmia diagnosis, implantable sensors, glucose level regularization and chemotherapy treatment [1]. However, this technology is not widely adopted due to security, fault-tolerance and lack of stability. The Internet of medical things (IoMT) is the most versatile using IoT technology in the medical field [2]. Due to the advancement of the IoMT, various medical imaging devices are mainly utilized for facilitating the diagnose process [3, 4].

In e-medical applications, the physiological information of patients is collected by healthcare IoT devices and then transmitted to cloud and edge devices. Hackers and attackers easily access it; hence security problems occur. The cyber-attacks such as ransomware and denial of services (DoS) can minimize the robustness of existing e-health care models and highly break off medical services. Hence, there is a need to develop a security solution for securing medical images and protecting patient privacy [5].

In the IoMT, healthcare images are generally provided by the image Archiving and Communication Systems (PACS). When the screening equipment monitors the patient, the obtained medical images are initially stored in the PACS [6]. When the physicians try to examine the patient, the PACS retrieves the images from the databases and transforms the images into the physician's workplace [7]. However, PACS has some security challenges in storing, transferring and retrieving medical images. When internal or external attackers have the

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 4
DOI: https://doi.org/10.17762/ijritcc.v11i4.6398
***Article Received**: 09 February 2023 **Revised**: 05 March 2023 **Accepted**: 12 March 2023*

potential to attack the PACS, it is easy to hack the medical images, which results in severe information leakage [8].

To provide security to IoMT, encryption and decryption models are applied to medical images. In medical technology, digital images play a major role in diagnosing diseases. Healthcare has attained many achievements with the integration of image as digital and the Internet [9]. Digital imaging has certain intrinsic characteristics like high data capacity and high correlation. Block cipher and streams are the most commonly used classical cypher models used to encrypt medical images [10]. When compared to block cipher models like advanced encryption standard (AES), data encryption standard (DES), hash function, Rivest Shamir Adleman (RSA) and International data encryption algorithm (IDEA), the stream model has better security and has better speed in encryption and decryption [11-16]. These algorithms use one secret key for encrypting and decrypting the data. The key is shared between the sender and receiver and is the major issue because the attacker can identify the key exchanging medium for decrypting the data. Asymmetric encryption utilizes two keys, one for private and another for public [17]. The data with the public key is used for sending the data, and the private key is used for decrypting the data.

A. Motivation

The emergence of the IoT is considered to make changes in healthcare industries and lead to the emergence of the Internet of Medical Things (IoMT). Security in the IoT is one of the most challenging objectives to be achieved in the real world due to the nature of the IoT environment. However, it is crucial to promote the security of the data circulated in the network as the data are highly sensitive and vulnerable to several intrusion categories. Apart from these, if intruders break the security systems, the sensitive contents might be misused, directly affecting the overall reputation of the IoT. To avoid this, several cryptographic systems are introduced into existing literary works, which can protect the environment from intrusions to some extent. Traditional security solutions are failing due to the recent development of sophisticated intrusion software. A hybrid framework is introduced to deal with the issues and maintain higher network performance, which can guarantee a higher range of security to the patient's data in IoT. The proposed hybrid framework integrates two efficient algorithms that achieve the desired performance.

B. Contribution

The main contributions of the proposed work are as follows:

- An efficient, lightweight cryptographic framework is designed and developed to secure the transfer of medical images in the IoT network with the combination of effective techniques.
- To propose a hybrid elliptic curve cryptography (HECC) algorithm with blowfish and elliptic curve cryptography to promote high level security for the images circulated in the hazardous IoT environment.
- Using an optimal key in the encryption phase provides numerous advantages and resolves the problems of slow encryption and storage issues. The proposed framework introduces the enhanced seagull optimization (ESO) algorithm to choose the ideal private key for effective encryption.
- The performance efficacy of the proposed framework is proved through extensive simulations, and the quality assessments are carried out with different existing state-of-the-art methods.

C. Organization

The structure of the paper is as follows: section 2 covers the literature survey of the existing papers related to security, section 3 explains the proposed methodology with mathematical descriptions and algorithms, section 4 includes the results and evaluations part, and section 5 concludes the paper.

II. RELATED WORKS

Some of the related works based on medical image encryption and decryption using various techniques are listed in this section.

Ding et al. [18] introduced deep learning based key generation for generating the private key utilized to encrypt and decrypt medical images. The DL model GAN (generative adversarial network) was utilized as the learning model for generating the private key. The encryption and decryption model combined the stream-cipher created by a deep key generation with the XOR. This model was evaluated on three benchmark datasets and achieved a better entropy value of 7.9870 and also the key generation time was very less (2.0714 s) compared to other models. Further, this model was resistant to different kinds of attacks.

Chirakkarottu and Mathew [19] presented a new encryption model for medical images using two dimensional Zaslavski mapping (2D-ZM) and DNA cryptography. The encryption process in this model has the stages like pixel position permutation and diffusion of the permuted images. The pseudorandom generator shuffled the image's pixels on the basis of 2D-ZM. Then, the permuted images were encrypted using DNA encryption. This model achieved high NPCR, UACI and entropy values of 99.9, 33.45 and 7.9, respectively. These results proved that this model was more robust over the differential attack and yielded highly correlated images compared to the plain images.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 4
DOI: https://doi.org/10.17762/ijritcc.v11i4.6398
***Article Received**: 09 February 2023 **Revised**: 05 March 2023 **Accepted**: 12 March 2023*

Chen et al. [20] presented a medical image encryption model using high speed scramble and pixel adaptive diffusion. The external random pixels were provided to the plain image. Then, high speed scramble and pixel adaptive diffusion were used for shuffling adjacent pixels and provided to the cipher image. To overcome the bad randomness, cipher image was recovered using the plain image attack. Then, the enhanced encryption model was proposed for performing non-linear operations on the permuted images. This model achieved better NPCR and UACI values of 99.616% and 33.459% respectively on the MRI brain images.

Ding et al. [21] presented a deep learning based encryption decryption (DLED) model for the privacy of medical images. The model cycle-GAN was considered the major network for transferring the medical images from the original to the target term. The target term was considered as the hidden factor for guiding the learning model for realizing the encryption process. The encrypted image was restored to plaintext via a reconstruction process for decrypting the images. The SSIM and PSNR values achieved by this model were 37.74 and 0.90 on the chest x-ray dataset.

El-Shafai et al. [22] introduced a robust cryptography model for DNA-based chaos for securing healthcare and tele-medical applications. Initially, a piecewise linear chaotic map (PWLCM) was used to generate the private key image. After that, the DNA rules were exploited to encode the secret key image and input image using the logistic chaos map. Then, the logistic map was used to obtain the intermediate image as another secret key image for setting DNA functions. Finally, the best cipher image was obtained using image columns.

Lakshmi et al. [23] developed a Hopfield neural network (HNN) model for image-based encryption. In this work, back propagation network (BPN) was used for generating image-specific keys and was resistant to hackers. The confusion and diffusion were evaluated on HNN, which enhanced the prediction process's complexity. For every image, the weighted matrix of the HNN was updated, producing pseudo sequence generation. This model provided connectivity between the authorized user and the cloud environment.

TABLE 1. COMPARATIVE ANALYSIS OF THE EXISTING WORKS

Authors and citation	**Methods**	**Advantages**	**Limitations**
Ding et al. [18]	GAN	The private key generated by this model provided better security and randomness	The process involved in using GAN was complex
Chirakkarottu and Mathew [19]	2D-ZM-DNA	This model was efficient, robust and secure.	The time taken to complete the process was high
Chen et al. [20]	high speed scramble and pixel adaptive diffusion	This model achieved better efficiency and robustness	Time consumption was high, and slow convergence occurred.
Ding et al. [21]	DLED	Ensured high security level and images were encrypted and decrypted in an efficient manner	This work associated every input image with one output image
El-Shafai et al. [22]	PWLCM-DNA	This model provided better security with less processing time	Need improvement in security performance
Lakshmi et al. [23]	HNN	Enhanced the key complexity and prediction was better	Restricted to local optimization on the training process for achieving network stability
Ahmed et al. [24]	DL-GSM	Classified abnormal and normal data with better accuracy	Less dataset consideration, and only minimal aspects were analyzed.

Ahmed et al. [24] proposed an automatic IoT system for the detection and classification of brain MRI on the basis of DL and Arduino global system of mobile communication (GSM). The regression principle was applied to the MRI data through the adoption of a genetic algorithm. The noise present in the data was minimized through bilateral filtering. The genetic algorithm was effectively used to generate the best fusion data from the source and reference data. CNN technique was applied for brain tumour classification, and the appropriate messages were sent to the patients through GSM. The proposed model was tested to classify abnormal and normal data, whereas an accuracy of 98.8% was obtained. A comparative analysis of the existing works is presented in Table 1.

A. Problem statement

After reviewing the literature methodologies, it has been identified that several encryption techniques can offer better security to medical data. Most of these techniques suffer from security or storage issues that result in performance degradation. Medical images are highly sensitive and require sophisticated security systems that can completely hide and protect the data from intruders while transmitting them through hazardous environments, i.e. IoT networks. The existing solutions cannot completely resolve the issues in encrypting these images. Moreover, some algorithms are computationally expensive, and the encryption process is slow in most cases as several steps must be followed. To resolve all the above-said

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 4
DOI: https://doi.org/10.17762/ijritcc.v11i4.6398
***Article Received**: 09 February 2023 **Revised**: 05 March 2023 **Accepted**: 12 March 2023*

issues, the proposed work combines two efficient and secure algorithms that can offer a higher range of security to the images along with being time-efficient.

III. PROPOSED METHODOLOGY

To attain the modernization of IoT, it is more significant to create client awareness and confidence about its protection and security as well as express strongly that there can't be any genuine threat to their data secrecy, and integrity in the medical system. The instantaneous growth of protection and security on an extensive scale is considered the influencing IoT variables to anchor the transmission of medical AD images. This section proposes the IoT-based hybrid cryptography model (IoT-HCM) for AD medical images. The proposed IoT-HCM comprises three significant stages: edge detection, key generation, encryption and decryption. At first, the medical images are decomposed into non-overlapping pixel blocks of definite size. Next, the Prewitt edge detection process is adapted to detect edge maps. The plain image is encrypted using hybrid symmetric and asymmetric encryption processes, which means a hybrid Elliptic curve cryptography (HECC) model is employed for encrypting the AD medical images. The HECC is the integration of Elliptic curve cryptography and blowfish. Further, the optimal key is generated using enhanced seagull optimization (ESO). The ESO is exploited for upgrading both private and public keys. The optimal key is generated to enhance encryption and decryption's security phase. The optimal key is introduced to decrease the execution time and increase the image quality of cipher image. The obtained cipher image is decrypted using the reverse process of encryption. This model ensures better security and confidentiality to the sensitive data of patients. The block diagram of the proposed model is presented in Figure 1.

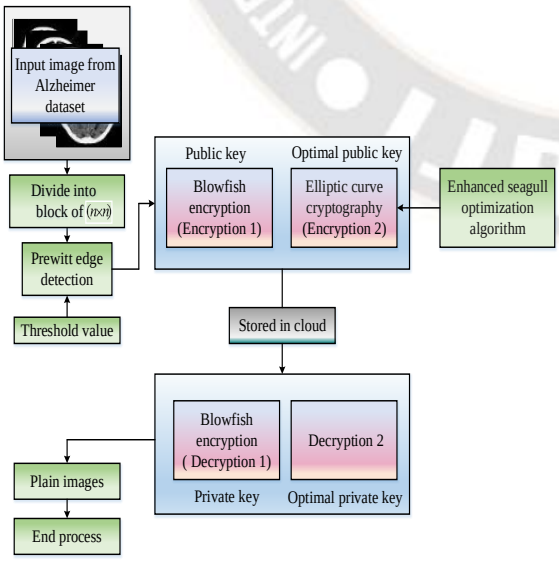


Figure 1. Block diagram of the proposed model

A. Prewitt edge detection

In the proposed IoT-HCM, the Prewitt edge detection scheme is employed to detect the substantial edge maps in AD images by applying a definite threshold value. The Prewitt detector partakes inexpensive computational cost, simple implementation, as well as accuracy for determining the position of the edges in AD images. The Prewitt operator is considered a discrete differentiation operator and builds on the gradient or decisive initial-direction derivative of ordinary image pixels. The repetition of Prewitt expands the magnitude and orientation of the edge in the image. The significant phases of the Prewitt edge detection model are stated below as follows:

The two 3×3 convolutional kernels R_X and R_Y are convoluted with the input image by using the equation (1). At each point, vertically and horizontally decomposed images are stated as R_Y and R_X. The following machinist is used to computed R_X and R_Y.

$$R_X = \begin{bmatrix} -1 & 0 & 1 \\ -1 & 0 & 1 \\ -1 & 0 & 1 \end{bmatrix} * j \quad Q_Y = \begin{bmatrix} -1 & -1 & -1 \\ 0 & 0 & 0 \\ 1 & 1 & 1 \end{bmatrix} * j \tag{1}$$

$$j(g_X^{'}(X,Y) = g(X+1,Y-1) - g(X-1,Y-1) + g(X+1,Y) - g(X-1,Y) + g(X+1,Y+1) - g(X-1,Y+1) \tag{2}$$

$$j(g_Y^{'}(X,Y) = g(X-1,Y+1) - g(X-1,Y-1) + g(X,Y+1) - g(X,Y-1) + g(X+1,Y+1) - g(X+1,Y-1) \tag{3}$$

$$R[g(X,Y)] = \sqrt{g_X^{'2}(X,Y) + g_Y^{'2}(X,Y)} \tag{4}$$

An approximate magnitude is typically expressed using the below equation,

$$|R| = |R_X| + |R_Y| \tag{5}$$

Besides, the angle orientation of the edge can be provided as follows:

$$\phi = \tan^{-1}\left(R_X / R_Y\right) \tag{6}$$

The output of (R) as well as the input AD image (j) has been gained through the Prewitt edge detection scheme. In the proposed IoT-HCM, the following are the phases being carried out for the edge detection mechanism.

- Initially, the input AD image is categorized into non-overlapping blocks with size $n\times n$, where N represents the total number of blocks in the AD image (j).
- In each detected block $(C_{j,k})$, count the total number of pixels (Q) and then compute its relating significant degree (T) by utilizing $T_{j,k} = Q_{j,k} / N$, where $C_{j,k}$ indicates the coordinate block position in the detected image.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 4
DOI: https://doi.org/10.17762/ijritcc.v11i4.6398
Article Received: 09 February 2023 Revised: 05 March 2023 Accepted: 12 March 2023

- Next, set the value of the threshold (u), $(0 \le u \le 1)$. In each block $C_{j,k}$, if $T_{j,k} \ge u$, it represents that the resultant block is significant and if $T_{j,k} < u$, it is considered insignificant.
- In an AD image, the binary index array of size $1 \times N$ has employed to represent the index of blocks. The element 0 states that the resulting block is the non-significant block, whereas it specifies the significant ones.
- Finally, each significant block is encrypted in sequence and then employed to exchange the original block in identical corresponding locations, consequently attaining the encrypted AD image.

B. Hybrid Elliptic curve cryptography (HECC)

The encryption stage is the most important stage of the proposed work, where the input images are encrypted for secure transmission. A hybrid encryption algorithm is introduced to encrypt the input AD images into cipher images. The proposed hybrid encryption algorithm combines the blowfish with the ECC algorithm to attain a higher range of security. The blowfish algorithm is executed at the initial phase of encryption to encrypt the images, followed by the ECC algorithm to further strengthen the security in the second phase. The sequential steps followed in the encryption phase are as follows:

***First phase*:** In the initial phase of encryption, the blowfish algorithm is implemented for key generation and encryption. This algorithm is mainly chosen due to its advantages of efficiency and security. Another advantage is that it is simple to implement. Since the proposed work involves the combination of two encryption algorithms, the time complexity and efficiency of the algorithms are required to be considered. To avoid such issues, the blowfish algorithm is combined with ECC. This algorithm is a 64-bit symmetric block cipher that uses key sizes varying between 32 and 448 bits. The main intention of the algorithm is to generate a 64-bit cipher image from the 64-bit input plaintext in a secure manner.

Subkeys in blowfish: A huge number of sub-keys are involved in the blowfish algorithm, and these subkeys must be preconfigured before the encryption and decryption procedures. The initial contents correspond to one array called the P-array to possess 18, 32-bit subkeys with 432-bit S-boxes of 256 parts each. The representation is as follows:

$$\begin{aligned} &S_{1,0}, S_{1,1}, \ldots . S_{1,255} \\ &S_{2,0}, S_{2,1}, \ldots . S_{2,255} \\ &S_{3,0}, S_{3,1}, \ldots . S_{3,255} \\ &S_{4,0}, S_{4,1}, \ldots . S_{4,255} \end{aligned} \quad (7)$$

The key is initially parted into 32-bit sections, and the XOR operation is performed on the parted key and then compared with the P-array. Each component in the P-array is XORed with the key bits, and if the key is shorter than 576-bits, the comparison is spun from the beginning of the key.

Encryption: The Image of AD is passed as the input to the encryption process. The encryption process can partition the input image data bit stream based on the block length permitted through the algorithm. The array's components are arranged in a row from left to right; every line corresponds to one line of output, and the image is encrypted line by line. Every input block provided as input can be 64-bits, whereas the key used is 448-bits in length. The data obtained in the last step is provided as input to the F-function for permutation, where the XOR operation is performed on the input block. After completing the XOR operation, the 32-bit blocks of the first and second parts are exchanged, and the steps are iterated. The F-function can be mathematically given as follows:

$$F() = \left(\left(S_{1,d} + S_{2,d} \bmod 2^{32} \right) XOR\, S_{3,c} \right) + S_{4,q} \bmod 2^{32} \quad (8)$$

where, d *and* c are the two parts of the input block and q specifies the P-array value. The steps are repeated until all the lines of the image are encrypted to generate the cipher image. After encrypting the input image, the cipher image is then provided to the second phase, where another encryption is carried out to promote extra security. The exact reverse process of this encryption is the decryption procedure, where the P-array is utilized in reverse order.

Second phase: The second phase involves the encryption process of the ECC algorithm, where the output obtained from the first phase is encrypted again. The ECC is a public curve cryptography that functions based on elliptic curves over finite fields. The purpose of additionally using this algorithm in the encryption process is to strengthen the overall security provided by the proposed framework. ECC is popular for its security feature and is faster and more efficient in creating a cryptographic key. Also, the key size used by this algorithm is smaller, thereby being memory efficient. The key generation process in the elliptic curve algorithm depends on the property of the elliptic curve equation given as follows:

$$y^2 = x^3 + ax + b \quad (9)$$

where, a *and* b specify the elliptic curve coefficients.

Let $\mathrm{E}_{C(a,b)}$ indicates an elliptic curve and consider the following equation:

$$B = KA \quad (10)$$

where, A *and* B are the two points belonging to the curve $A \in E_{C(a,b)}$. The value of B can be easily calculated from the above equation given the values of A *and* K. But the problem arises with the calculation of K as it is a trapdoor function which can be called a discrete logarithm.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 4
DOI: https://doi.org/10.17762/ijritcc.v11i4.6398
***Article Received**: 09 February 2023 **Revised**: 05 March 2023 **Accepted**: 12 March 2023*

For encrypting the input image, the communicating parties agree upon the elliptic curve equation and a generator function. For instance, if Alice wants to encrypt the message and send to Bob, the cipher image generated by Alice can be given as $C_I = [\kappa G, I_C + \kappa p_b]$ where, κ indicates a random integer chosen for encryption, G indicates the generator function, I_C indicates the input image and p_b indicates Bob's public key computed from the private key. The cipher image obtained from Alice can be decrypted by Bob, which can be given as $D_I = [I_C + \kappa p_b - p_r \kappa G]$ where, p_r is the private key of Bob. To further improve the security offered by the proposed framework, an ideal private key selected by an effective meta-heuristic optimization algorithm is desirable. The proposed work uses the ESO algorithm with the combination of logistic chaotic maps to effectively searching an ideal key suitable for encryption. The decryption process of HECC is the exact reverse operation of the entire algorithm. This operation is performed on the hospital side after receiving the requested image.

C. Enhanced seagull optimization algorithm for key optimization

In order to provide better security of AD images, a key optimization of ECC strategy for hash function discovery is important. Here an ESO (Enhanced Seagull Optimization) algorithm is used to update the private and public keys. Typically, ESO is thought of as a bio-inspired algorithm that mimics the seagull's move and attack characteristics. These features are mathematically modeled to highlight exploration and exploitation in the provided search area. The ESO is started by initializing the key for the key optimization process. During initialization, the logistic chaotic map is adjusted to improve key optimization performance.

$$K = key_1, key_2, \ldots key_n \tag{11}$$

Fitness evaluation: The fitness selection is considered a crucial viewpoint in the ESO algorithm. The AB image security process has considered PSNR as the fitness of each image with the optimal solution. The fitness can be given as:

$$Fitness\_F_j = Maxi(PSNR) \tag{12}$$

Exploration stage (migration): In the exploration stage, the ESO evaluated how the seagulls transfer towards another location. Here, three conditions are necessary to satisfy the seagull, and it is given as follows:

Collision avoidance: Here, an additional variable B has been used to compute the location of search agents for avoiding the collision between adjacent seagulls.

$$\vec{D}_t = B \times \vec{Q}_s(y) \tag{13}$$

where, $\vec{D}_t$ represents the location of the seagull, which can't collide with one another, $\vec{Q}_s$ indicates the search agent's current position, y resembles the current iteration, and B specify the search agent's movement characteristics in a specified search area.

$$B = g_d - (y \times (g_d / Maxi_{ite})), \quad y = 0,1,2,3,\ldots Maxi_{ite} \tag{14}$$

where, g_d is applied to manage the frequency of using the variable B, which linearly minimized from g_d to 0.

Here , g_d is considered as 2.

Movement close to the direction of best neighbour: Here, the search agents can be moved in the direction of the best neighbour after executing the collision avoidance.

$$\vec{N}_t = C \times (\vec{Q}_{bs}(y) - \vec{Q}_t(y)) \tag{15}$$

where, $\vec{Q}_t$ indicates the best fittest seagull (search agent), $\vec{N}_t$ indicates the location of $\vec{Q}_t$ towards $\vec{Q}_t$. This randomized characteristic can provide a better balance between exploration and exploitation. C can be computed as follows:

$$C = 2 \times B^2 \times dr \tag{16}$$

where, dr indicate the random number between 0 and 1.

Remaining close to the fittest search agent: At last, the location of the search agents can be updated corresponding to the best search agent.

$$\vec{E}_t = \left| \vec{D}_t + \vec{N}_t \right| \tag{17}$$

where, $\vec{E}_t$ indicates the distance between the fitted search agent and the search agent.

Exploitation stage (Attacking): This stage concentrates on exploiting the experience and history of the search process. During migration, the seagull can vary the speed and angle of attack. They preserve their amplitude by utilizing their weights and wings. Besides, when attacking the prey, the spiral movement characteristic has happened in the air. The characteristics in $X, Y,$ and Z planes have presented below as follows:

$$X' = s \times \cos(l) \tag{18}$$

$$Y' = s \times \sin(l) \tag{19}$$

$$Z' = s \times l \tag{20}$$

$$s = v \times e^{lw} \tag{21}$$

where, s resembles the radius of each spiral turn, l specifies the random number of range $[0 \le l \le 2\pi]$, and e specifies the base of the natural algorithm. v and w imply the constant for defining the spiral shape. Then, the updated location of the search agent can be computed as:

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 4
DOI: https://doi.org/10.17762/ijritcc.v11i4.6398
***Article Received**: 09 February 2023 **Revised**: 05 March 2023 **Accepted**: 12 March 2023*

$$\vec{Q}_t(y) = (\vec{E}_t \times X^{'} \times Y^{'} \times Z^{'}) + \vec{Q}_{bs}(y) \quad (22)$$

where, $\vec{Q}_{bs}(y)$ can update the location of other search agents and saves the best solution.

The pseudocode of ESO is provided in Algorithm 1. Here, the ESO initiates with a randomly generated population. During the iteration process, the search agents updated their location according to the best. ESO is being considered for key optimization due to better exploration and exploitation capabilities.

Algorithm 1: Enhanced seagull optimization for key optimization
Start
Initialize the parameters
Set $g_d \leftarrow 2$
Set $v \leftarrow 1$
Set $w \leftarrow 1$
While $(y < Maxi_{ite})$ do
$\vec{Q}_{bs} \leftarrow Compute\ fitness(\vec{Q}_t)$
/*Exploration characteristics*/
$dr \leftarrow rand(0,1)$
$l \leftarrow rand(0,2\pi)$
/*Exploitation characteristics*/
$s \leftarrow v \times e^{lw}$
Compute the distance $\vec{E}_t$
$Q = X^{'} \times Y^{'} \times Z^{'}$
$\vec{Q}_t(y) = (\vec{E}_t \times Q) + \vec{Q}_{bs}$
$y \leftarrow y + 1$
End while
Return $\vec{Q}_{bs}$
End

IV. RESULTS AND DISCUSSION

The experimental outcomes of the proposed IoT-HCM for AD medical images are defined in this section. The performances of the proposed model are assessed using PYTHON. Several existing methodologies are compared with the proposed model to evaluate the overall model performance to analyze superiority. After decomposing the AD medical images into non-overlapping pixel blocks, the edge maps are detected using Prewitt edge detection. Encryption is carried out using the HECC approach through ECC and Blowfish integration. Optimal keys are produced using ESO, whereas decryption of data can be performed with greater security. The dataset description, details of diverse performance metrics with its mathematical formulation, performance analysis and comparison are provided in the following sub-sections. Table 2 indicates the system configuration details of the proposed model.

TABLE 2. SYSTEM CONFIGURATION DETAILS

Sl. No	Parameters	Configuration
1	Pen and touch	No pen or touch input is available for the display
2	System type	64-bit operating system, x64-based processor
3	Installed RAM	8.00 GB
4	Processor	Intel(R) Core(TM) i7-8700 CPU @ 3.20 GHz
5	Device name	Ssm113.smg.local

A. Details of the dataset

The MRI image data utilized for assessing the security performance through encryption and decryption are gathered from Alzheimer's dataset. The dataset was accomplished from the open Access series of imaging studies (OASIS) created by Washington university knight Alzheimer's disease research Centre. The specific website contains a collection of brain MRI images comprising four diverse classes: mild demented, moderate demented, non-demented and very mild demented. The data is gathered from public sources and contains training and testing data. It grasps two data files for training and testing with a total of around 5000 images that are separated on the basis of AD class severity. The download link for Alzheimer's dataset is provided as https://www.kaggle.com/datasets/tourist55/alzheimers-dataset-4-class-of-images.

B. Metrics considered for performance analysis

The proposed IoT-HCM performance of data encryption and decryption can be assessed through the consideration of diverse metrics, including Entropy, Correlation coefficient, unified change intensity as average (UACI), pixel number change rate (NPCR), peak signal-to-noise ratio (PSNR) and Multiple Scale-Structural Similarity Index measures (MS-SSIM). These metrics' explanations and mathematical descriptions are provided for analyzing the proposed performance.

➔ ***Analysis of Entropy:*** Entropy is an outstanding feature that represents the uncertainty image degree, which can be analyzed using the below expression.

$$P(s) = \sum_{u=0}^{2A-1} H(s_u) \log_2 \frac{1}{H(s_u)} \quad (23)$$

From the above expression, $H(s_u)$ represents the variable occurrence probability s_u .

➔ ***Analysis of Histogram:*** The gray level frequency of every pixel can be defined through histogram analysis. An analytical image behaviour and a better encrypted proposed model make the encryption image distribution uniform. Through this, the demonstration of the flexibility of the

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 4
DOI: https://doi.org/10.17762/ijritcc.v11i4.6398
***Article Received**: 09 February 2023 **Revised**: 05 March 2023 **Accepted**: 12 March 2023*

proposed strategy in consideration of various attacks can be analyzed.

➔ ***Analysis of the Correlation coefficient:*** Correlation analysis acts as a special feature to analyze the resistance against security attacks of image encryption. The correlation can be reduced over the image through the adjustment of pixels in the case of encrypted images. The correlation coefficient can be evaluated in the middle of two pixels. It can be mathematically formulated as,

$$C_{uv} = \frac{|Cov(u,v)|}{\sqrt{D(u)} \times \sqrt{D(v)}} \tag{24}$$

From the above given expression, the two adjacent gray level pixels are denoted as u and v.

➔ ***Analysis of UACI and NPCRs:*** The proposed model performs the encryption process over the original image and contributes fewer variations over the original image. Two preceding and succeeding images are compared to attain significant association among the original encrypted images. The two criteria, UACI and NPCR, determine the attack resistance. The mathematical formulation of UACI and NPCR are given as follows.

$$UACI = \sum_{u=1}^{A}\sum_{v=1}^{B} \frac{|K_1(p,q) - K_2(p,q)|}{255 \times A \times B} \times 100\% \tag{25}$$

$$NPCR = \frac{\sum_{u=1}^{A}\sum_{v=1}^{B} D(p,q)}{A \times B} \times 100\% \tag{26}$$

$$\text{Here, } D(p,q) = \begin{cases} 0 & if \quad K_1(p,q) = K_2(p,q) \\ 1 & if \quad K_1(p,q) \neq K_2(p,q) \end{cases} \tag{27}$$

From the above expressions, A represents the height and width are denoted as B. The two digit image and unique pixel variance are denoted as K_1 and K_2, respectively. The size of the encryption image is represented as $A \times B$, the normal encryption image is denoted as K_1 and decrypting image is denoted as K_2.

➔ ***Analysis of PSNR:*** PSNR assesses the ratio between two images in decibels. The specified ratio is used as a quality estimator between the original and encrypted images, whereas the PSNR value describes the assessment of peak error. The lower value of MSE indicates a lower error of PSNR, and it can be mathematically expressed as,

$$PSNR = 10\log_{10}\left(\frac{F^2}{MSE}\right) \tag{28}$$

From the above equation, MSE denotes the mean square error, F signifies the maximum fluctuation of the input image.

➔ ***Analysis of MS-SSIM:*** The similarity of Color secret images is evaluated as MS-SSIM. The SSIM look like a full reference metric that assesses or predicts an image's quality based on the original image as reference. The SSIM index can be deliberated as.

$$SSIM(a,b) = \frac{(2\eta_a\eta_b + c_1)(2\sigma_{ab} + c_2)}{(\eta_a^2 + \eta_b^2 + c_1)(\sigma_a^2 + \sigma_b^2 + c_2)} \tag{29}$$

From the above expression, η_a denotes the average of a, η_b represents the average of b, σ_a^2 represents the variance of a and σ_b^2 denotes the variance of b. The covariance of a and b indicates σ_{ab}, c_1 and c_2 are the two variables utilized for stability improvement. The MS-SSIM can be calculated as follows.

$$MS - SSIM = \frac{1}{N}\sum_{t=1}^{N} SSIM(a_t - b_t) \tag{30}$$

C. Performance assessment and comparison

The comparison results of the existing algorithms are taken from PWLCM [22]. The proposed IoT-HCM model is compared with several existing methods like Chaos and interweaving of ranks (CIR), Multiple mixed hash functions and cyclic shift (MMHF-CS), Fractional order Hyper chaotic chen system and DNA operations (FOHCCDNA), hybrid reversible encryption approach for the authentication and security (HRSA), as well as block-shuffling-based Image ciphering scheme (BSICS). In addition, Image encryption algorithm based on DNA sequence operations and chaotic systems (IEA-DNASO), CNN-based Color image encryption algorithm (CNN-IEA), chaos and DNA encoding (C-DNAE) and DNA-chaos cryptosystem for secure telemedicine and healthcare applications (PWLCM-DNA) are also employed to evaluate the security performance. The performance outcomes of the proposed model are assessed to entropy, correlation coefficient, MS-SSIM, PSNR, UACI and NPCR by comparing them with the existing models.

The PSNR comparison is done using the proposed model and existing techniques such as ROI Medical Image Watermarking Technique (ROI-MIW), Fractional Order Hyper Chaotic Chen System and DNA Operations (FOHCCDNA), Secure Medical Image Encryption based on Intensity Level Using Chaos Theory and DNA Cryptography (CT-DNAC), Choas and DNA Coding (C-DNAE) and DNAchaos Cryptosystem for Secure Telemedicine and Healthcare Applications (PWLCM-DNA). On the other hand, the proposed MS-SSIM performance is compared to certain existing models such as the SVD-based robust image steganography model using RIWT and DCT for secure transmission of medical images (SVM-RIWT-DCT), the theory of compression detection and coefficients of Fast Discrete Curve Transformation (CS-FDCuT), Robust Symmetric Image Coding (RSIES), and Multiscale Transform-based Image

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 4
DOI: https://doi.org/10.17762/ijritcc.v11i4.6398
***Article Received**: 09 February 2023 **Revised**: 05 March 2023 **Accepted**: 12 March 2023*

Compression Coding Scheme (MTICES). Implemented with PYTHON, the proposed model has achieved better performance results in terms of security. Through this research, the error can be greatly minimized by providing optimally selected keys. Figure 2 shows the entropy performance of the proposed and existing models.

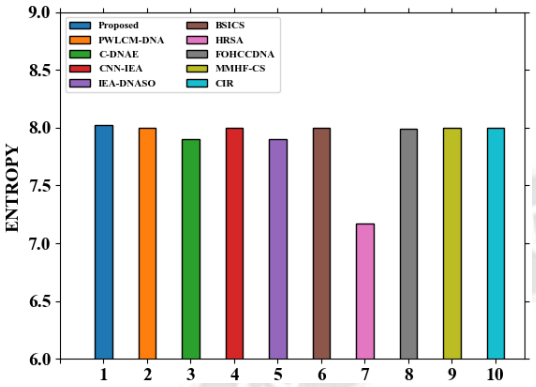


Figure 2. Entropy performance assessment

The entropy values of ciphered medical images are measured to be 7.996 for CIR, 7.995 in the case of MMHF-CS, 7.98 in the case of FOHCCDNA, 7.17 by HRSA and 7.99 in the case of BSICS. Accordingly, 7.90 through IEA-DNASO, 7.99 in case of CNN-IEA, 7.90 by C-DNAEiphere and 7.99 obtained by PWLCM-DNA. The estimated entropy value of the proposed model is found to be 8.01. The entropy values of tested encrypted medical AD images are represented graphically. It is observed that the entropy values of ciphered medical AD images are near the value 8. But the value of the proposed model is greater than 8, and hence it ensures the immunity of the proposed model is higher than the existing models. Figure 3 indicates the PSNR performance of the proposed and existing models.

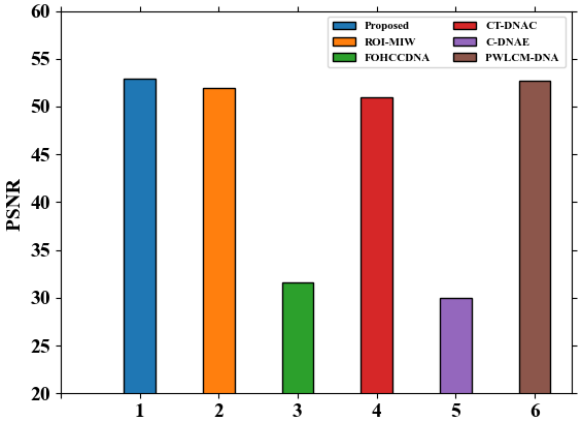


Figure 3. PSNR performance assessment

The PSNR performance of the proposed model is compared with the existing models like ROI-MIW, FOHCCDNA, CT-DNAC, C-DNAE and FWLCM-DNA models. The PSNR values of the proposed model are evaluated in terms of dB. The ROI-MIW has attained 51.95 dB of PSNR value, FOHCCDNA as 31.58 dB, CT-DNAC ass 51.01 dB, C-DNAE as 30.02 dB and FWLCM-DNA as 52.73 dB. The proposed model has attained 52.9 dB of PSNR value, which shows that the proposed model has attained better performance than the existing approaches in terms of security enhancement. Figure 4 (a)-(b) shows the NPCR and UACI performance of the proposed and existing models.

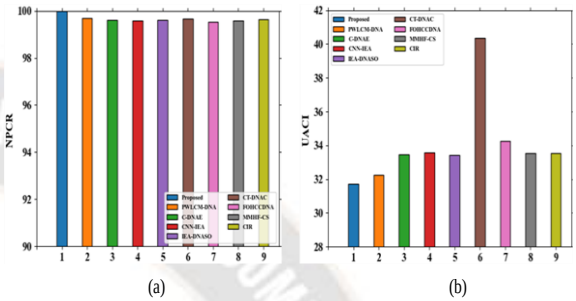


Figure 4. Performance of proposed and existing models (a) NPCR (b) UACI

The NPCR and UACI performance of the proposed model are compared with the existing approaches, and it is observed from the figure that an effective performance is obtained in terms of NPCR and UACI. The NPCR values of ciphered medical images are measured to be 99.63 for CIR, 99.59 in the case of MMHF-CS, 99.52 for FOHCCDNA, 99.67 for BSICS, 99.60 by IEA-DNASO, 99.59 in case of CNN-IEA, 99.61 obtained by C-DNAEiphere and 99.69 by PWLCM-DNA. The UACI values of ciphered medical images are evaluated to be 33.52 for CIR, 33.52 for MMHF-CS, 34.26 for FOHCCDNA, 40.37 in the case of BSICS, 33.42 by IEA-DNASO, 33.58 for CNN-IEA, 33.47 by C-DNAEiphere and 32.24 attained by PWLCM-DNA. The proposed NPCR value evaluated over the encrypted images is obtained to be 99.98, and the UACI value of the proposed model is attained to be 31.73. The proposed model obtained superior performance in providing data security compared with the existing models. Figure 5 indicates the MS-SSIM performance of the proposed and existing models.

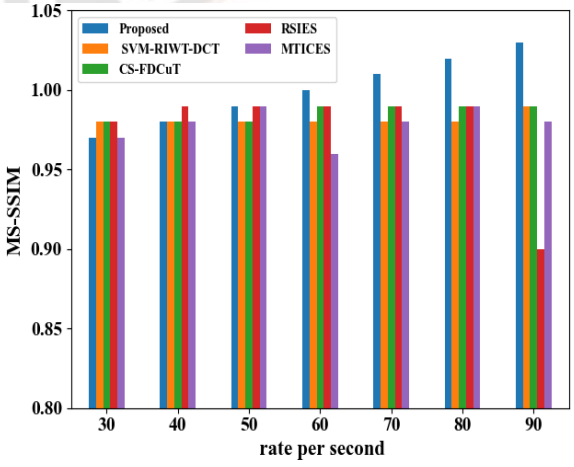


Figure 5. MS-SSIM performance comparison

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 4
DOI: https://doi.org/10.17762/ijritcc.v11i4.6398
***Article Received**: 09 February 2023 **Revised**: 05 March 2023 **Accepted**: 12 March 2023*

The performance of MS-SSIM is analyzed by varying the rates per second. The proposed MS-SSIM performance is compared with certain existing models like SVM-RIWT-DCT [25], CS-FDCuT [26], RSIES [27] and MTICES [28]. The results demonstrate that the proposed model has obtained 97% of the MS-SSIM value. The existing models like SVM-RIWT-DCT attained 65%, CS-FDCuT at 72%, RSIES at 48% and MTICES at 55%. The proposed model obtained a better MS-SSIM value in comparing the proposed and existing models. The correlation coefficient performance of the proposed model is portrayed in Figure 6.

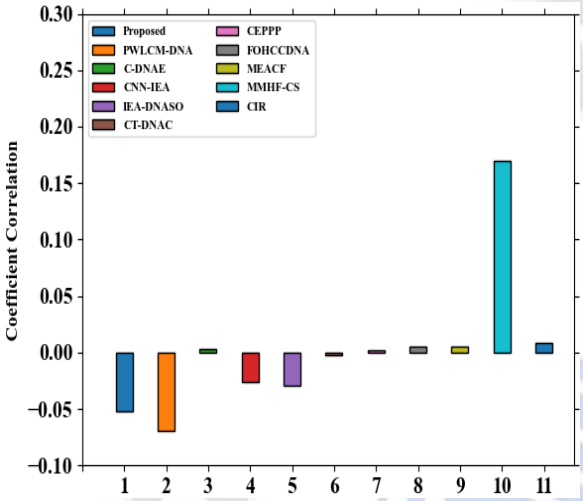


Figure 6. Performance comparison of correlation coefficient

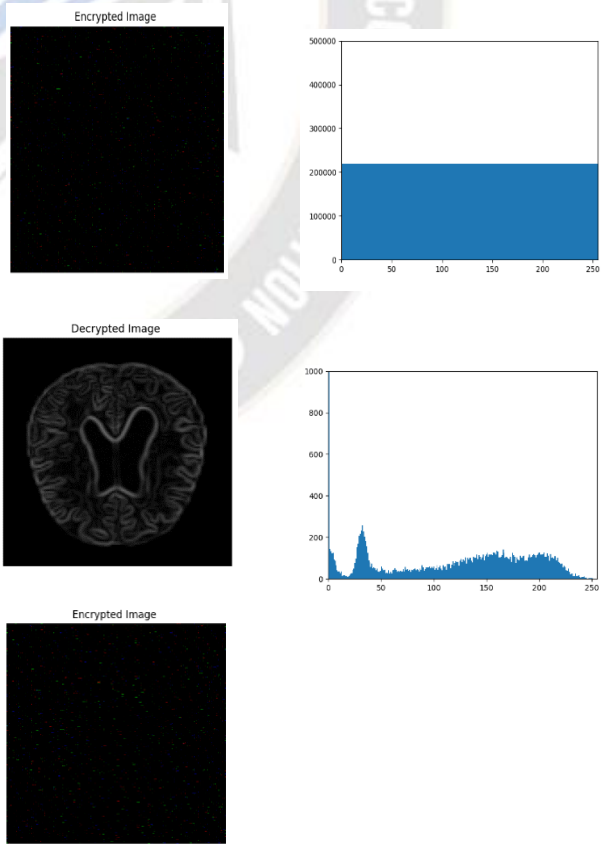
The performance of the correlation coefficient is utilized to estimate the ciphering efficiency and quality and medical image cryptosystem quality. The relationship amongst neighbouring pixels can be evaluated through this performance. The performance of the proposed model is compared with the existing techniques CIR, Modified encryption algorithm based on chaotic function (MEACF), MMHF-CS, FOHCCDNA, pixel position permutation based on Chaotic encryption (CEPPP), Chao's theory and DNA cryptography (CT-DNAC), IEA-DNASO, CNN-IEA, C-DNAE and PWLCM-DNA. The correlation coefficient of 0.008 in terms of CIR, 0.170 for MEACF, and 0.004 for MMHF-CS are attained during evaluation. Besides, the existing models have also gained 0.005 for FOHCCDNA, CEPPP as 0.0002, CT-DNAC as -0.002, IEA-DNASO as -0.02, CNN-IEA as -0.02, C-DNAE as 0.002 and PWLCM-DNA -0.047. Table 3 indicates the computational time comparison of the proposed and existing models.

TABLE 3. PERFORMANCE COMPARISON OF COMPUTATIONAL TIME

Techniques	Computational time (Seconds)
SVM-RIWT-DCT [25]	384.26
CS-FDCuT [26]	312.54
RSIES [27]	258.48
MTICES [28]	123.3
Proposed	**11.978**

When comparing the computational time of the proposed IoT-HCM model with existing approaches, the proposed run time is highly lesser than the existing methods. The proposed IoT-HCM model has attained only 11.978 seconds during implementation for the AD dataset. In contrast, existing SVM-RIWT-DCT obtained 384.26 seconds, CS-FDCuT 312.54 seconds, RSIES 258.48 seconds, and MTICES consumed 123.3 seconds. Because of huge data processing and more complexity in encrypting data, existing approaches obtained increased run time. From this, a clear analysis can be made that the proposed algorithm is proven to offer better performance. Figure 7 indicates the histogram analysis for the encrypted and decrypted image.

The figure shows the histogram outcomes of encrypted and decrypted images. The amount of confusion produced by the encryption scheme is evaluated through histogram analysis. The pixel distribution of the image over a particular intensity level can be shown. The histogram of encrypted images should be equalized and distributed uniformly for the overall intensity range in the case of a highly secure encryption approach. Better performance can be obtained if the decrypted image turns out to be the same as the input image. The histogram outcomes proved that the performance efficiency of the proposed IoT-HCM is better. Figure 8 depicts an instance of edge detection analysis.



International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 4
DOI: https://doi.org/10.17762/ijritcc.v11i4.6398
***Article Received**: 09 February 2023 **Revised**: 05 March 2023 **Accepted**: 12 March 2023*

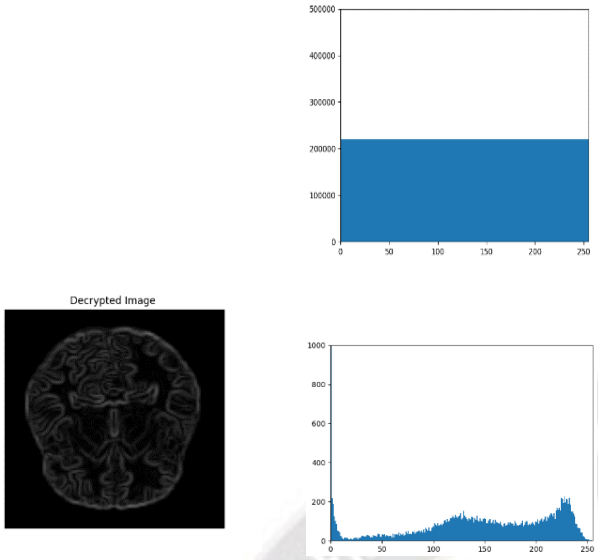
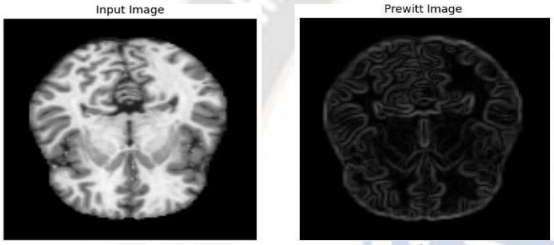


Figure 7. Histogram analysis of medical AD images



(a) (b)

Figure 8. Edge detection analysis (a) Input Image (b) Prewitt Image

The edge information of medical AD images has to be preserved from attackers. The visual distortion of ciphered edge images can be analyzed as the distortion present in medical images. The edges are detected using the Prewitt detection method in the proposed IoT-HCM model for a given sample input image. Also, it can be observed that the detected edges in decrypted images are the same as that of the original images. Hence, these edge detection outcomes prove that the efficiency of the proposed IoT-HCM model performs better.

V. CONCLUSION

Providing security to medical images is crucial in IoT networks as the images are highly sensitive and are the main target of intruders. Intruders are breaking traditional cryptographic systems by developing sophisticated software and tools. To avoid such tragic issues, a new lightweight cryptography is proposed in this work, which includes different phases to secure the data. In the proposed work, the AD images are considered input images to be saved before transmission on the network. Initially, the images are provided as input to the edge detection module, where the edge maps are detected using the Prewitt edge detection technique. Then, the encryption process is carried out using the proposed HECC algorithm, which integrates blowfish and ECC. The encryption process involves two phases; the blowfish algorithm is executed for encryption in the first phase. Then, the output obtained is provided to the second phase, where the ECC is utilized to encrypt the images. To further enhance the security and efficiency of the framework, the ideal private key is selected using the ESO algorithm, which is then utilized in the encryption process. The exact reverse process of the HECC algorithm results in the decrypted image. The proposed framework has been evaluated using the AD dataset, and the results proved that the proposed model is more efficient and secure than the compared techniques. The proposed framework can also be easily adapted to secure other medical images before transmitting through the IoT network. Also, with minor modifications, it can be followed to secure other medical data formats of varied sizes. In future, it is desired to conduct real-time experiments by directly collecting different modalities of medical data and assessing the performance of the proposed approach. Also, other effective metaheuristics will be used in place of ESO, and the performance will be evaluated.

ACKNOWLEDGEMENTS

None

REFERENCES

[1] C.R. Su, J. Hajiyev, C.J. Fu, K.C. Kao, C.H. Chang and C.T. Chang, “A novel framework for a remote patient monitoring (RPM) system with abnormality detection”. Health Policy and Technology, vol. 8, no. 2, pp.157-170, 2019.

[2] M.M. Salim, I. Kim, U. Doniyor, C. Lee and J.H. Park, “Homomorphic Encryption Based Privacy-Preservation for IoMT”. Applied Sciences, vol. 11, no. 18, pp.8757, 2021.

[3] R.O. Ogundokun, J.B. Awotunde, E.A. Adeniyi and F.E. Ayo, “Crypto-Stegno based model for securing medical information on IOMT platform”. Multimedia tools and applications, vol. 80, no. 21, pp.31705-31727, 2021.

[4] M.K. Hasan, T.M. Ghazal, R.A. Saeed, B. Pandey, H. Gohel, A.A. Eshmawi, S. Abdel-Khalek and H.M. Alkhassawneh, “A review on security threats, vulnerabilities, and counter measures of 5G enabled Internet-of-Medical-Things”. IET Communications, vol. 16, no. 5, pp.421-432, 2022.

[5] M.A. Mohammed, D.A. Ibrahim and K.H. Abdulkareem, “Bio-inspired robotics enabled schemes in blockchain-fog-cloud assisted IoMT environment”. Journal of King Saud University-Computer and Information Sciences 2021.

[6] K.V. Greeshma and J.V. Gripsy, “A Review on Classification and Retrieval of Biomedical Images Using Artificial Intelligence”. The Fusion of Internet of Things, Artificial Intelligence, and Cloud Computing in Health Care, pp.47-66, 2021.

[7] K. Fuchs, W.C. Harding, F. Hudson and M. Parker, “TIPPSS for Facilitating Connected Healthcare Interoperability”. In Mobile Medicine. Productivity Press pp. 269-279, 2021.

[8] K.Y. Tehseen, N. Imran, A.S. Qazi, W. Ahmad, F. Arslan, A. Ijaz and M. Ali, “Transformative Effects of COVID-19 on

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 4
DOI: https://doi.org/10.17762/ijritcc.v11i4.6398
***Article Received**: 09 February 2023 **Revised**: 05 March 2023 **Accepted**: 12 March 2023*

Global Economy and Internet of Medical Things (IoMT): Current Vision, Role and Applications". International J. on Emerging Technologies, vol. 12, no. 2, pp.66-76, 2021.

[9] N. Jain and S.S. Chauhan, "Novel Approach Transforming Stream Cipher to Block Cipher". In 2021 International Conference on Technological Advancements and Innovations (ICTAI) IEEE pp. 182-187, 2021.

[10] A. Sevin and A.A.O. Mohammed, "A survey on software implementation of lightweight block ciphers for IoT devices". Journal of Ambient Intelligence and Humanized Computing, pp. 1-15, 2021.

[11] M.K. Hasan, M. Shafiq, S. Islam, B. Pandey, Y.A.B. El-Ebiary, N.S. Nafi, R.C. Rodriguez and D.E. Vargas, "Lightweight cryptographic algorithms for guessing attack protection in complex Internet of things applications". Complexity, vol. 2021, 2021.

[12] H. Xu, K. Thakur, A.S. Kamruzzaman and M.L. Ali, "Applications of Cryptography in Database: A Review". In 2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS) pp. 1-6, 2021.

[13] A.K. Bermani, T.A. Murshedi and Z.A. Abod, "A hybrid cryptography technique for data storage on cloud computing". Journal of Discrete Mathematical Sciences and Cryptography, vol. 24, no. 6, pp.1613-1624, 2021.

[14] S. Kumar, G. Karnani, M.S. Gaur and A. Mishra, "Cloud security using hybrid cryptography algorithms". In 2021 2nd International conference on intelligent engineering and management (ICIEM) IEEE pp. 599-604, 2021.

[15] P. William, A. Choubey, G.S. Chhabra, R. Bhattacharya, K. Vengatesan and S. Choubey, "Assessment of Hybrid Cryptographic Algorithm for Secure Sharing of Textual and Pictorial Content". In 2022 International Conference on Electronics and Renewable Systems (ICEARS) IEEE, pp. 918-922, 2022.

[16] M.U. Bokhari, Q.M. Shallal and Y.K. Tamandani, "Reducing the required time and power for data encryption and decryption using K-NN machine learning". IETE Journal of Research, vol. 65, no. 2, pp. 227-235, 2019.

[17] R. Abid, C. Iwendi, A.R. Javed, M. Rizwan, Z. Jalil, J.H. Anajemba and C. Biamba, "An optimized homomorphic CRT-RSA algorithm for secure and efficient communication". Personal and Ubiquitous Computing, pp.1-14, 2021.

[18] Y. Ding, F. Tan, Z. Qin, M. Cao, K.K.R. Choo and Z. Qin, "DeepKeyGen: a deep learning-based stream cipher generator for medical image encryption and decryption". IEEE Transactions on Neural Networks and Learning Systems vol. 2021, 2020.

[19] S. Chirakkarottu and S. Mathew, "A novel encryption method for medical images using 2D Zaslavski map and DNA cryptography". SN Applied Sciences, vol. 2, no. 1, pp.1-10, 2019.

[20] Y. Chen, C. Tang and R. Ye, "Cryptanalysis and improvement of medical image encryption using high-speed scrambling and pixel adaptive diffusion". Signal Processing, vol. 167, pp.107286, 2020.

[21] Y. Ding, G. Wu, D. Chen, N. Zhang, L. Gong, M. Cao and Z. Qin, DeepEDN: a deep-learning-based image encryption and decryption network for Internet of medical things. IEEE Internet of Things Journal, vol. 8, no. 3, pp.1504-1518, 2020.

[22] W. El-Shafai, F. Khallaf, E.S.M. El-Rabaie and F.E.A. El-Samie, "Robust medical image encryption based on DNA-chaos cryptosystem for secure telemedicine and healthcare applications". Journal of Ambient Intelligence and Humanized Computing, vol. 12, no. 10, pp.9007-9035, 2021.

[23] C. Lakshmi, K. Thenmozhi, J.B.B. Rayappan, S. Rajagopalan, R. Amirtharajan and N. Chidambaram, "Neural-assisted image-dependent encryption scheme for medical image cloud storage". Neural Computing and Applications, vol. 33, no. 12, pp.6671-6684, 2021.

[24] A.S. Ahmed and H.A. Salah, "The IoT and registration of MRI brain diagnosis based on genetic algorithm and convolutional neural network." Indonesian Journal of Electrical Engineering and Computer Science vol. 25, no. 1, pp. 273, 2022.

[25] S. Arunkumar, V. Subramaniyaswamy, V. Vijayakumar, Naveen Chilamkurti, and R. Logesh. "SVD-based robust image steganographic scheme using RIWT and DCT for secure transmission of medical images." Measurement vol. 139, pp. 426-437, 2019.

[26] S. Borra, R. Thanki, N. Dey and K. Borisagar, "Secure transmission and integrity verification of color radiological images using fast discrete curvelet transform and compressive sensing". Smart Health vol. 12, pp. 35-48, 2019.

[27] W.I. Khedr, "A new efficient and configurable image encryption structure for secure transmission." Multimedia Tools and Applications vol. 79, no. 23, pp. 16797-16821, 2020.

[28] S.P. Raja, "Joint medical image compression–encryption in the cloud using multiscale transform-based image compression encoding techniques." Sādhanā vol. 44, no. 2, pp. 1-10, 2019.