IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Mathematical Modelling of Engineering Problems
Vol. 12, No. 3, March, 2025, pp. 807-814
Journal homepage: http://iieta.org/journals/mmep

A Symmetric-Key Block Cipher Method for Medical Image Encryption to Promote Internet of Medical Things Applications

Asraa Y. Youssef[1], Sawsan D. Mahmood[2], Mohanad Sameer Jabbar[3*], Azmi Shawkat Abdulbaqi[4], Jamal Fadhil Tawfeq[5], Ravi Sekhar[6], Pritesh Shah[6], Shilpa Malge[6]

[1] College of Agriculture, Department of Soil Sciences and Water Resources, University of Diyala, Baqubah 32001, Iraq
[2] College of Education for Pure Science, University of Diyala, Baqubah 32001, Iraq
[3] Medical Instruments Techniques Engineering Department, Technical College of Engineering, Al-Bayan University, Baghdad 10001, Iraq
[4] Renewable Energy Research Center, University of Anbar, Anbar 31001, Iraq
[5] Department of Medical Instrumentation Technical Engineering, Medical Technical College, Al-Farahidi University, Baghdad 10001, Iraq
[6] Symbiosis Institute of Technology (SIT), Symbiosis International (Deemed University) (SIU), Pune 412115, India

Corresponding Author Email: mohanad.s@albayan.edu.iq

https://doi.org/10.18280/mmep.120307

Received: 30 April 2024
Revised: 9 July 2024
Accepted: 15 July 2024
Available online: 31 March 2025

Keywords:
IoT in the medical field (IoMT), symmetric-key block cipher, modified RC5 (Mod-RC5)

ABSTRACT

The security of medical healthcare images has been the subject of several research projects; therefore, security is a challenge in medical imaging. A solution to image confidentiality is encryption, which does not risk data loss. E-health data cannot be directly encrypted due to limitations in data size, redundancy, and capacity, especially when transmitted over open channels. As images contain more information than text, patients may lose privacy in the content of their medical records because they are not as confidential as text. These threats have been identified by researchers, who have proposed several ways to mitigate the security risks associated with them. The study found that several application-specific security issues remain with the existing proposed techniques. Using an efficient, encryption algorithm, this paper presents an image encryption technique for healthcare. A robust encryption technique is used to encrypt medical images using the Least Significant Bit (LSB) technique. Our novel contribution here is that watermarks are embedded in encrypted domains and their extraction is performed in encrypted and decrypted domains. The proposed algorithm was evaluated using numerous test images. According to the experiment, the proposed algorithm performs better than conventional methods when it comes to image cryptosystems.

1. INTRODUCTION

Organizations that implement applications must pay attention to security when it comes to images. The military, government, civilian, hospital, and industrial sectors are sending, receiving, and storing large amounts of data for decision-making, security, and other purposes such as healthcare, video surveillance, and IoMT. Especially when it comes to medical images, image security is important because its medical data must be protected: first, against accidental loss and corruption, and second, from deliberate attempts to gain access to or alter the data before it can be accessed by a specialist in real-time. To prevent passive and active fraud involving medical images, cryptography is generally considered the best method [1, 2].

An encrypted format for storing or sending medical image data is called cipher-text, which is created using a cryptographic system (cipher or cryptosystem). Using a "cipher key" or keys, the encryption process transforms plaintext into ciphertext by ciphering, manipulating, or transforming it. When a cipher-text is manipulated or transformed, that is, transformed from cipher-text to plaintext, a decipher key is used. The encryption algorithm and key are known only to the sender and receiver in such encrypted transmissions [3]. Traditional symmetrical cryptosystems such as YC5, DES, IDEA, and AES use decrypting data to evaluate encrypted data. A secure channel (e.g., secure courier, secured telephone line, or the like) must be used to send the encryption key to the device (Specialists/Doctors) to provide protection.

Encryption methods that use public keys (e.g., RSA and El Gamal) can avoid the difficulties of exchanging protected keys. In order to simplify the computation of the enciphering function, an encrypting function must be selected so that once the enciphering key is known, the function can be easily computed. Nevertheless, computing the inverse of the encrypting transformation function is computationally impossible. Functions like this are called "trap door functions" or "one-way functions" [4, 5].

PRNGs (additional stream ciphers) and public key algorithms (block-encryption algorithms) are the most

commonly used asymmetric algorithms (block encryption algorithms). Using the secret key, an existing string can be transformed into one that is of similar length (typically 64, 168, or 256 bits) [6]. The traditional ciphering algorithms, though efficient for text and binary data, cannot handle massive image, video, or audio data, which requires a high bit rate (near-real-time communication). Rivest developed the RC5 algorithm for encrypting data. This algorithm is iterative, uses variable block sizes, rounds, and secret keys, and can handle words of varying lengths using parameters. Three operations are needed to encrypt a file: addition, exclusive-OR, and rotation [7]. Thus, performance characteristics and security levels can be greatly altered. The RC5 algorithm offers many advantages, including its easy implementation on both hardware and software, as well as its easier analysis than other block ciphers. One of Rivest's objectives was to simplify design and analysis [8].

A correlation attack based on full rounds and tests can, however, breach RC5. In addition to time attacks, plain-text correlation attacks can be used to break RC5, as naive implementations may result in rotations taking a long time, for example, as a function of the data [9].

In RC5-32 with r rounds and 26.14r+2.27 plain texts, weak security can be revealed through differential attacks of up to 512. This has a 90% success rate. RC5 has a long encryption time, making it ineffective for real-time applications. There are several differences between imagery and text. Since image sizes are almost always larger than text sizes, the decrypted text must be the same size as the original text. Data in images do not need to meet this requirement. Real-time applications benefit from the modifications to RC5 (Mod-RC5) that improve their efficiency and security. A pseudorandom round key sequence can be improved using this algorithm by combining chaos and cryptographic primitives. An expanded key table and the adapted secret key are mixed using a chaotic skew tent map. Data-dependent rotations are also heavily used by our encryption process to increase diffusion per round [10, 11]. Table 1 describes the comparison between the proposed technique and the traditional techniques described in the literature.

Table 1. Comparison between proposed and traditional techniques in the literature

A Technique Characteristic	The Proposed Technique	The Traditional Techniques
The keys to encrypt and decrypt	Using the same key results in the same result	Encryption and decryption use different keys
The speed at which encryption/decryption is performed.	Very fast and efficient	Less expensive and slower techniques
The size of the encrypted text that is generated as a result.	Usually, the plaintext size remains the same or is somewhat smaller than the original plaintext size.	Larger than plaintext
Keys for encryption and decryption are known and can be used.	In symmetric key encryption, the key should be known by both parties.	Public key encryption involves two parties knowing one key
Several aspects of use must be considered.	Confidentiality, integrity, and availability	Signatures, confidentiality

In this work, the following steps were taken: Literature-related works were described in Section 2. The methodology system was introduced in Section 3. In Section 4, the LSB technique (The watermarking) was presented, and the embedding process with a modified block cipher was used. In Section 5, security analysis was described. The conclusion is given in Section 6.

2. RELATED WORKS

Healthcare organizations and hospitals have greatly benefited from the IoMT. In addition to the security and privacy challenges posed by technological advancements, the IoTs also pose privacy concerns. Data and information security, confidentiality, integrity, and data availability are all threats to medical systems. Integrity, confidentiality, and availability could be affected by security problems. In addition, hackers can order drugs online using medical data for fraud and identity theft [12]. Those who don't want to disclose their illnesses can also be blackmailed and extorted by hackers. A fitness tracker is a well-known example of IoMT-enabled well-being which incorporates these aspects of confidentiality, integrity, and availability. It is necessary to control access to the IoMT network. Once the user has been identified and validated, authorization should be established to access the requested resources. Communication between software entities is necessary for obtaining and granting access [13]. Despite this, the IoMT can be challenging to control effectively [14]. Authentication and identity management are major challenges in IoMT security and privacy. An object's unique identification is used to validate the relationship between two parties. An authentication process is required to make the Internet of Things secure, reliable, and available. Adversaries who possess credentials to verify their legitimacy can acquire confidential, integrity, or availability-compromising data [15]. Identification and authentication of users are major challenges in IoMT. The use of passwords and usernames is commonly used in E-Systems to authenticate and identify parties. Biometric credentials, digital certificates, and shared keys are other methods. With the heterogeneous and larger nature of IoMT systems, security threats will increase as well. Heterogeneity greatly impacts security services for IoMT. The authentication and authorization of IoT systems is one of the most essential features of security solutions for IoT systems. Security-related restrictions also apply to devices and communications [16].

Even the smallest IoMT devices need Internet Protocols because they contain low-power processors and a small area. Information processing with incredible speed is limited by the limitations of IoMT devices [17]. In other words, there is a limited amount of memory, CPU, and energy. To achieve minimal resource consumption while maintaining robust performance, challenging security forms are necessary. It is difficult to maintain confidentiality and integrity in IoMT systems due to power and size constraints [18, 19]. In applications based on the IoMTs, security analytics could significantly reduce vulnerabilities. Using security analytics, IoMT security providers can detect and eliminate potential threats through the correlation and evaluation of data collected

from different sources. It is important to perform multidimensional security analytics in addition to monitoring the IoMT gateway. Data from multiple domains can be compared to identify suspicious or malicious anomalies. Anomalies can then be gathered and prevented by security experts. Using critical public infrastructure is another solution [19]. Digital resources can be developed, managed, and distributed using public key infrastructure, which includes hardware, software, policies, and procedures. In the case of IoT security challenges, the security process has proven effective. Asymmetric and symmetric encryption procedures ensure data encryption in public key infrastructure. As a result, it has drawn much attention recently to protect electronic health-related images, especially when they are sent via correspondence networks [20]. Image encryption is a method of transforming an image into something impossible to recognize. Digital healthcare image methods utilize the security mechanisms DES, AES, IDEA, and RSA. Cryptography would be helpful in real-time teleradiology and other remote examinations that utilize large digital medical images that take more than a few seconds to transmit. Healthcare diagnostics use digital images such as CT scans and MRIs [21]. In addition to sound detection, watermarking, segmenting images, extracting features, and reducing noise, many other techniques are used with electronic images. Analyzing and investigating health information involves the use of images. International research institutions and hospitals often exchange images via the Internet and mobile communications. Scientific investigation resources are shared and diagnosed remotely with the help of cloud storage and analysis of medical images today [22]. Disclosing patient information to the public is not appropriate. Patients' images are transmitted to professional doctors via a public community, enabling them to consult with them. The secure transfer of information is made possible by the Internet.

3. THE SYSTEM METHODOLOGY

As shown in Figure 1 and Figure 2, the proposed technique is organized as a block diagram. Input medical images are decomposed into wavelet sub-bands using 1-level DWT decompositions. In the LH sub-band, we embed a binary watermark by using the LSB method after encrypting the LL sub-band with Mod-RC5 [23]. A medical image that needs to be encrypted watermarked and sent to the sender is generated using the inverse DWT algorithm. Recovering watermarks and decrypting them are performed by the receiver in LL and LH sub-bands [24].

3.1 Encryption based on Mod-RC5

RC5 is vulnerable to attacks because of its weak keys. Diffusion and confusion play a role in the weakness of the structure. Our key schedule generates round keys using a chaotic skew tent map. This equation describes a piece-wise linear map of a chaotic skew tent in 1-D [25].

$$x(t) = \begin{cases} \dfrac{x}{q} & \text{when } x \text{ belongs to the vector[zero to } q] \\ \dfrac{One - x}{One - q} & \text{when } x \text{ belongs to the vector } [q \text{ to one}) \end{cases} \quad (1)$$

There is a constant q in the vector [zero to one], where q is the value of a constant within the vector. As a result, skew tent maps have uniform invariant densities and produce better pseudorandom sequences. To increase diffusion per round, rotations are heavily used in the encryption operation. We refer to this modified version as Mod-RC5-w/r/b [26].

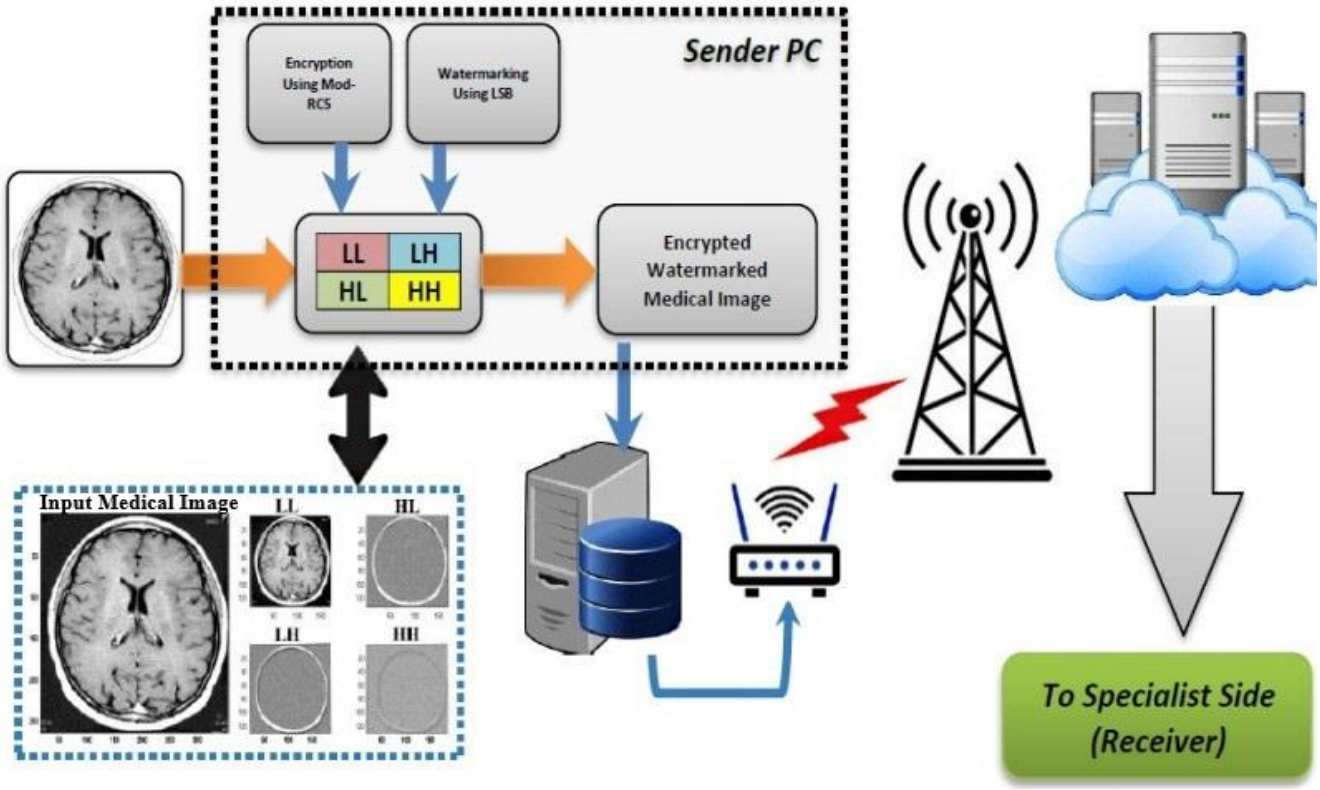


Figure 1. A block diagram showing the encryption and watermarking process on the sender and receiver sides

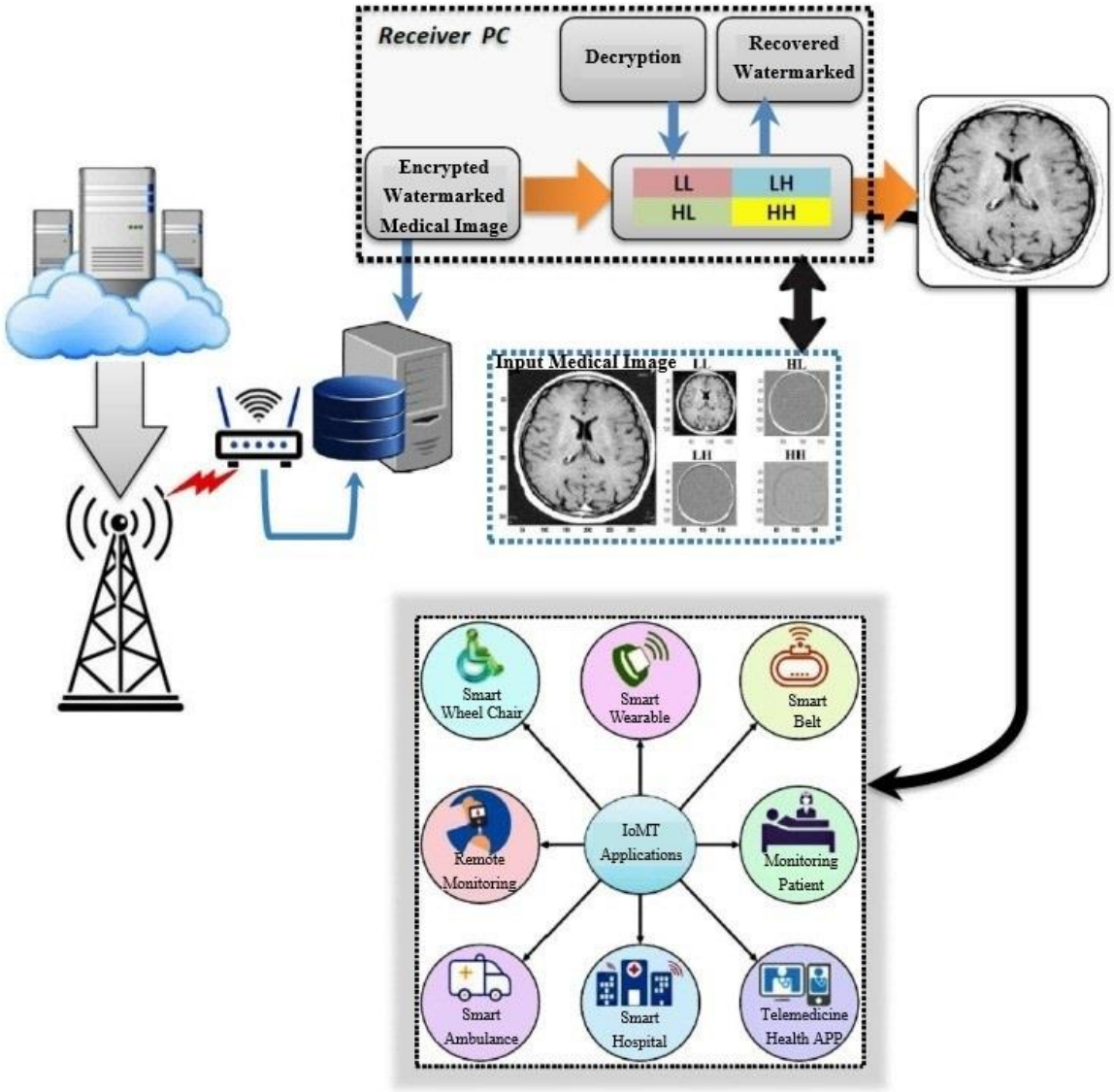


Figure 2. A block diagram showing the decryption and watermarking process on the receiver side

3.1.1 Algorithm expands keys on a schedule

By using the user's secret key K, key expansion generates random binary words of $t = 2 * r + 2$. There are three components to the algorithm [27]. There are two magic constants that are used: a magic number and a magic constant. A conversion can be categorized as converting, initializing, or mixing. Pseudocode algorithms can be found here [17].

(1) Conversion

There is an array L $[0 \ldots f-1]$ containing a secret key for the user K $[0 \ldots h-1]$, where $c = [h/y]$, where u equal to w/8 is the number of bytes in a word. K is composed of consecutive key bytes that are added to each subsequent word in L from low-order to high-order. These paddings are applied to unfilled byte positions in L [28]:

$$F = [max(h, One)/y];$$
$$\text{For } i = from\ b\ to\ Zero, Continue$$
$$\text{Let } L[i/y] = (L[i/y] \longleftarrow Eight) + K[i]$$

(2) Initialization

By assigning the array X to the magic constants Q_w and P_w, a pseudorandom bit pattern is generated.

$$X[Zero] = Pw$$
$$\text{For } i = One\ to\ t - One; Continue$$
$$X[i] = X[i - One] + Qw$$

(3) Mixing

Use the X and L arrays to combine a user's secret key. Arrays with a larger dimension will be processed in one step, whereas arrays with a smaller dimension may take three steps [29].

```
Start
M = N = i = j = Zero
V = 3 * max(f, Two * r + Two);
For X = One to v; Continue
Begin
M = X[i] = (X[i] + N + N ⟵ lgw;
M = L[j] = L[j] + M + N ⟵ M + N;
I = (i + One)mod(Two * r + Two);
J = (j + One)modf;
End of Begin
End of Start
```

K cannot be determined from S using the key-scheduler function because there are too many "one-ways".

3.2 Encryption algorithm

A permutation process and a diffusion process are used in the encryption process of images. Using chaotic logistic maps, we generate random sequences to scramble and diffuse the images. Pixels of the original image will be scrambled in the spatial domain in the permutation process. Random binary sequences generated in the diffusion process are masked with pixels in the original picture. Two w-bit registers M and N are used to store the input block, and M and N are used to store the output block.

Here is a detailed explanation of the encryption process:

Process of permutation: Random sequences will be generated from a logistic map to scramble pixels of the original image.

Process of diffusion: The scrambled image pixel bits are shifted either rightward (if odd) or leftward (if even) in response to a random integer sequence generated by (9).

Sine and cubic maps generate a random binary sequence, which changes the scrambled image pixel bits. Lastly, the cipher image is created by converting the random binary sequence into intersequence, and then repeating this process twice.

In terms of encryption algorithm, pseudo code can be described as follows which shows how the encryption process works:

$Start$
$M = (M \longleftarrow X[Zero]) + X[Zero];$
$N = (N \longleftarrow X[One]) + X[One];$
$For\ i = from\ 1\ to\ r; Continue$
$Begin$
$M = (M \longleftarrow X[i] + X[i+1]);$
$N = (N \longleftarrow X[i + One] + X[i + Two]);$
$M = ((M + N) \longleftarrow N) + X[Two * i];$
$N = ((N + M) \longleftarrow M) + X[Two * i + One];$
$Endo\ f\ Begin;$
$End\ of\ Start$

3.3 Decryption algorithm

Defining the decryption process is an easy routine. Decryption processes are considered the inverse methods of encryption processes. First, logistic maps are used to generate a random sequence with the same initial value as used in encryption. Once the original image has been retrieved, the permutation and diffusion methods will be used to figure out how it was obtained. According to this algorithm, decryption can be achieved:

$Start$
$For\ i = from\ r\ to 1; Continue$
$Begin$
$M = (M \longrightarrow X[i + One] - X[i]);$
$N = N \longrightarrow X[i + Two] - X[i + One];$
$N = (N - X[Two * (i + One)]) \longrightarrow M + M;$
$M = (M - X[Two * i]) \longrightarrow N + N;$
$End\ of\ Begin;$
$N = N \longrightarrow X[One] - X[One]$
$A = (M \longrightarrow X[Zero]) - X[Zero]$
$End\ of\ Start$

3.4 LSB technique (The watermarking)

Watermark embedders and detectors are fundamental components of digital watermarking systems. Using the embedded watermark, the watermark detector detects the presence of the watermark on the cover image.

4. EMBEDDING PROCESS

4.1 Embedding the watermark

There is a lot of energy concentrated in the lower-frequency sub-bands of the image. Watermarks embedded in these sub-bands could corrupt images. When high frequencies are involved, humans cannot detect HH sub-band changes. The middle-frequency sub-bands HL and HL are especially suitable for watermarks because they are highly imperceptible and robust [11]. To embed LSB watermarks in this scheme, the lower harmonic band (LH) is chosen as the sub-band for high-frequency sub-bands that are most sensitive to human vision. Data is encrypted with digital watermarks or LSB substitutions. During digital watermarking, the watermark bits are distributed throughout the image so that they cannot be detected or removed. The cover image of a digital image can be enhanced with information by inserting it directly into each bit or into a busy area. Information is encoded in every pixel of the cover image [25, 28].

4.2 Extracting the watermark

Extracting the watermark is the reverse process of embedding. A watermarked image's LSB can be extracted to retrieve the watermark bit. The LSB algorithm (n bits) is as follows:

1: One pixel for each image.
2: Analyzing the image pixels.
3: Substituting the secret image binary sequence for the final n bits of the binary code.
4: End [13, 22].

4.3 Security analysis

The proposed cipher is subjected to a strict security analysis against a number of attacks. This approach significantly outperforms conventional security mechanisms when applied to critical medical images that are critical to human health. In different security analysis tests, the effectiveness of the proposed algorithm is proven against RC5 algorithm.

5. RESULTS AND DISCUSSION

On the transmitter side (Patient), the results after encryption and watermark embedding were presented, while on the receiver side (Specialist), the results after extraction and decryption of the watermark were presented.

5.1 Medical image entropy

The entropy of random variables measures their uncertainty. It is important for a secure cryptosystem to ensure that the ciphered image does not reveal any information about the plain image. Using Eq. (2), we can calculate information entropy:

$$He = -\sum_{K=Zero}^{G=One} P(K) log_{Two}(P(K)) \quad (2)$$

A gray value of 0 to 255 refers to the input medical image's entropy, where *He* refers to the entropy. Furthermore, $P(K)$ refers to the probability of the symbol K occurrence.

5.2 Noise-resistance of encrypted images

An image cryptosystem's robustness against a noisy cipher image is assessed using the MSE. The pixel (i_n, j_n) MSE is calculated mathematically using $p_1(i_1, j_1)$ and $p_2(i_2, j_2)$.

Table 2 shows the entropy findings after the Mod-RC5 algorithm was applied over various original medical images, with medical images time-consuming. Table 3 shows the histogram and MSE for each decrypted medical image. Figure 3 shows the statistical parameters of the proposed method.

Table 2. Entropy analysis of medical images using Mod-RC5 algorithm with time consumption

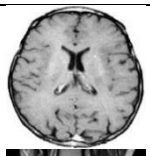
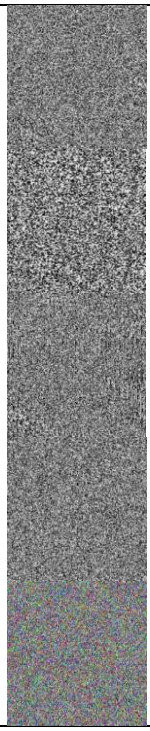
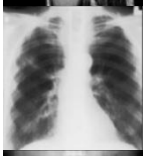
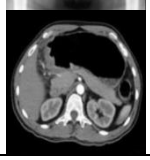
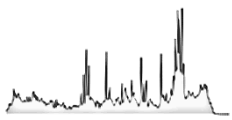
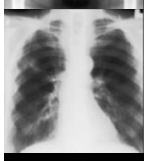
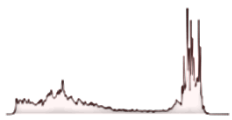
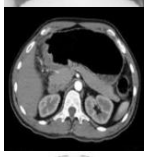
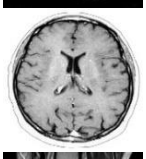
Medical Image No.	Original Medical Image	Entropy of Plain Text Medical Image	Encrypted Medical Image	Entropy AFTER RC5 Algorithm Applying	Medical Image Size	Time Consuming in (Seconds)
1		1.6511		7.3746	300×300	0.016
2		3.5685		7.8657	600×600	0.048
3		1.2331		7.8657	520×520	0.032
4		7.7441		7.8657	900×900	0.141
5		7.7543		7.9926	1200×600	0.111

Table 3. Analysis of histogram and MSE for decrypted medical images

Medical Image No.	Medical Decrypted Images	Medical Image Histogram	MSE	Values of PSNR
1			0.37	43.22
2			0.41	43.33
3			0.36	42.84
4			0.31	42.92
5			0.45	46.08

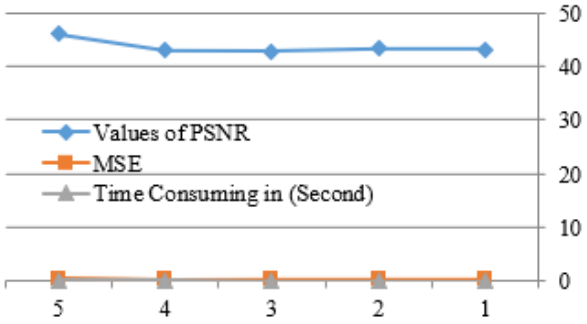


Figure 3. Statistical parameters of the proposed method

6. CONCLUSION

The Mod-RC5 algorithm is used in this paper to encrypt and decrypt images. Using symmetric key and quadrate structures, the proposed system is fast and secure. By taking advantage of today's computers' powerful operations, it offers much-improved security and performance over existing ciphers. Based on the correlation, entropy, and histogram measurements, the modified Mod-RC5 algorithm demonstrated that security can be measured using correlation, entropy, and histogram measurements.

As a result of this technique, the encrypted images have a higher security level via a decreased correlation between their elements, which increases their entropy value by decreasing the mutual information among them. Hence, we propose an ideal method of encrypting images for storage and transmission.

Asymmetric and symmetric encryption are the most common types of encryptions in the IoT. Encrypting and decrypting data using symmetric encryption requires one cryptographic key. Symmetric encryption is easy to use because of this advantage. This encryption algorithm does not affect the functionality of IoMT applications since it is extremely fast, requires few resources, and doesn't impede network speeds.

Encrypting medical images has both positive and negative ethical consequences. Furthermore, medical image encryption is effective in preserving the privacy of sensitive personal information. In addition to concealing illicit content or supporting unauthorized surveillance, medical image encryption may be used illegally for a range of purposes. In addition to ethical concerns about freedom of expression, medical image encryption schemes that censor information may also raise ethical concerns. Due to the possibility of misuse and infringement of rights, medical image encryption should take ethical considerations into account as well as privacy and security requirements.

REFERENCE

[1] Azeez, R.A., Abdul-Hussein, M.K., Mahdi, M.S., ALRikabi, H.T.S. (2021). Design a system for an approved video copyright over cloud based on biometric iris and random walk generator using watermark technique. Periodicals of Engineering and Natural Sciences, 10(1): 178-187. https://doi.org/10.21533/pen.v10i1.2577

[2] Aljazaery, I., Alrikabi, H., Aziz, M. (2020). Combination of hiding and encryption for data security. International Journal of Interactive Mobile Technologies, 14(9): 34-47. https://doi.org/10.3991/ijim.v14i09.14173

[3] Mahdi, M.S., Azeez, R.A., Hassan, N.F. (2020). A proposed lightweight image encryption using ChaCha with hyperchaotic maps. Periodicals of Engineering and Natural Sciences, 8(4): 2138-2145. http://doi.org/10.21533/pen.v8i4.1708

[4] ALRikabi, H.T., Hazim, H.T. (2021). Enhanced data security of communication system using combined encryption and steganography. International Journal of Interactive Mobile Technologies, 15(16): 145. https://doi.org/10.3991/ijim.v15i16.24557

[5] Alseelawi, N., Hazim, H.T., Salim ALRikabi, H.T. (2022). A novel method of multimodal medical image fusion based on hybrid approach of NSCT and DTCWT. International Journal of Online & Biomedical Engineering, 18(3): 114-133. https://doi.org/10.3991/ijoe.v18i03.28011

[6] Jamil, A.S., Azeez, R.A., Al-Adhami, A., Hassan, N.F. (2023). Multibiometric system with runs bits permutation for creating cryptographic key generation technique. Iraqi Journal of Science, 64(1): 452-468. https://doi.org/10.24996/ijs.2023.64.1.40

[7] Earle, A.E. (2005). Wireless Security Handbook. Auerbach Publications.

[8] Mushtaq, M.F., Jamel, S., Disina, A. H., Pindar, Z.A., Shakir, N.S.A., Deris, M.M. (2017). A survey on the cryptographic encryption algorithms. International Journal of Advanced Computer Science and Applications, 8(11): 333-344. https://doi.org/10.14569/IJACSA. 2017.081141

[9] Obaida, T.H., Jamil, A.S., Hassan, N.F. (2022). A review: Video encryption techniques, advantages and disadvantages. Webology, 19(1): 7209-7222.

[10] Mezaal, Y.S., Hammood, D.A., Ali, M.H. (2016). OTP encryption enhancement based on logical operations. In 2016 Sixth International Conference on Digital Information Processing and Communications, Beirut, Lebanon, pp. 109-112. https://doi.org/10.1109/ICDIPC.2016.7470801

[11] Singh, D.A.A.G., Priyadharshini, R. (2016). Performance analysis of data encryption algorithms for secure data transmission. International Journal for Science and Advance Research in Technology, 2(12): 388-390.

[12] Obaida, T.H., Jamil, A.S., Hassan, N.F. (2022). Real-time face detection in digital video-based on Viola-Jones supported by convolutional neural networks. International Journal of Electrical and Computer Engineering, 12(3): 3083. https://doi.org/10.11591/ijece.v12i3. pp3083-3091

[13] Mezaal, Y.S., Hussein, H.A., Alfatlawy, F.A., Abdulkareem, Z.J., Yousif, L.N. (2019). Investigation of PAPR reduction technique using TRC-SLM integration. International Journal of Simulation-Systems, Science & Technology, 19(6): 34. https://doi.org/10.5013/IJSSST.a.19.06.34

[14] Cruz, B.F., Domingo, K.N., De Guzman, F.E., Cotiangco, J.B., Hilario, C.B. (2017). Expanded 128-bit data encryption standard. International Journal of Computer Science and Mobile Computing, 68(8): 133-142.

[15] Aljazaery, I.A., Salim ALRikabi, H.T., Alaidi, A.H.M. (2022). Encryption of color image based on DNA strand

and exponential factor. International Journal of Online & Biomedical Engineering, 18(3): 101-113. https://doi.org/10.3991/ijoe.v18i03.28021

[16] Shareef, M.S., Abd, T., Mezaal, Y.S. (2020). Gender voice classification with huge accuracy rate. TELKOMNIKA (Telecommunication Computing Electronics and Control), 18(5): 2612-2617. https://doi.org/10.12928/telkomnika.v18i5.13717

[17] Qian, G.B., Jiang, Q.F., Qiu, S.S. (2009). A new image encryption scheme based on DES algorithm and Chua's circuit. In 2009 IEEE International Workshop on Imaging Systems and Techniques, Shenzhen, China, pp. 168-172. https://doi.org/10.1109/IST.2009.5071626

[18] Kandar, S., Chaudhuri, D., Bhattacharjee, A., Dhara, B. C. (2019). Image encryption using sequence generated by cyclic group. Journal of Information Security and Applications, 44: 117-129. https://doi.org/10.1016/j.jisa.2018.12.003

[19] Liu, H., Wang, X. (2010). Color image encryption based on one-time keys and robust chaotic maps. Computers & Mathematics with Applications, 59(10): 3320-3327. https://doi.org/10.1016/j.camwa.2010.03.017

[20] Faragallah, O.S. (2011). Digital image encryption based on the RC5 block cipher algorithm. Sensing and Imaging: An International Journal, 12(3): 73-94. https://doi.org/10.1007/s11220-011-0062-5

[21] Zhao, T., Ran, Q., Yuan, L., Chi, Y., Ma, J. (2015). Image encryption using fingerprint as key based on phase retrieval algorithm and public key cryptography. Optics and Lasers in Engineering, 72: 12-17. https://doi.org/10.1016/j.optlaseng.2015.03.024

[22] Li, L., Abd El-Latif, A.A., Niu, X. (2012). Elliptic curve ElGamal based homomorphic image encryption scheme for sharing secret images. Signal Processing, 92(4): 1069-1078. https://doi.org/10.1016/j.sigpro.2011.10.020

[23] Alam, S., Jamil, A., Saldhi, A., Ahmad, M. (2015). Digital image authentication and encryption using digital signature. In 2015 International Conference on Advances in Computer Engineering and Applications, Ghaziabad, India, pp. 332-336. https://doi.org/10.1109/ICACEA.2015.7164725

[24] Özkaynak, F. (2018). Brief review on application of nonlinear dynamics in image encryption. Nonlinear Dynamics, 92(2): 305-313. https://doi.org/10.1007/s11071-018-4056-x

[25] Hua, Z., Zhou, Y., Huang, H. (2019). Cosine-transform-based chaotic system for image encryption. Information Sciences, 480: 403-419. https://doi.org/10.1016/j.ins.2018.12.048

[26] Sun, Y.J., Zhang, H., Wang, X.Y., Wang, X.Q., Yan, P.F. (2020). 2D non-adjacent coupled map lattice with q and its applications in image encryption. Applied Mathematics and Computation, 373: 125039. https://doi.org/10.1016/j.amc.2020.125039

[27] El Hanouti, I., El Fadili, H., Zenkouar, K. (2021). Breaking an image encryption scheme based on Arnold map and Lucas series. Multimedia Tools and Applications, 80(4): 4975-4997. https://doi.org/10.1007/s11042-020-09815-4

[28] Díaz-Muñoz, J.D., Cruz-Vega, I., Tlelo-Cuautle, E., Ramirez Cortes, J.M., de Jesús Rangel-Magdaleno, J. (2021). Kalman observers in estimating the states of chaotic neurons for image encryption under MQTT for IoT protocol. The European Physical Journal Special Topics, 231: 945-962. https://doi.org/10.1140/epjs/s11734-021-00319-2

[29] Batool, S.I., Waseem, H.M. (2019). A novel image encryption scheme based on Arnold scrambling and Lucas series. Multimedia Tools and Applications, 78: 27611-27637. https://doi.org/10.1007/s11042-019-07881-x