IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received January 31, 2021, accepted February 9, 2021, date of publication February 24, 2021, date of current version April 1, 2021.

*Digital Object Identifier 10.1109/ACCESS.2021.3061710*

# Lightweight Encryption Technique to Enhance Medical Image Security on Internet of Medical Things Applications

**MOHAMMAD KAMRUL HASAN[1], (Senior Member, IEEE), SHAYLA ISLAM[2], (Member, IEEE), ROSSILAWATI SULAIMAN[1], (Senior Member, IEEE), SHEROZ KHAN[3], (Senior Member, IEEE), AISHA-HASSAN ABDALLA HASHIM[4], (Senior Member, IEEE), SHABANA HABIB[5], (Member, IEEE), MOHAMMAD ISLAM[3], (Senior Member, IEEE), SALEH ALYAHYA[3], (Member, IEEE), MUSSE MOHAMED AHMED[6], (Senior Member, IEEE), SAMAR KAMIL[1,7], AND MD ARIF HASSAN[1], (Member, IEEE)**

[1]Center for Cyber Security, Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia (UKM), Bangi 43600, Malaysia
[2]Department of Computer Science, Institute of Computer Science and Digital Innovation, UCSI University, Kuala Lumpur 56000, Malaysia
[3]Department of Electrical and Renewable Engineering, Onaizah Colleges of Engineering, Al-Qassim 51452, Saudi Arabia
[4]Department of Electrical and Computer Engineering, International Islamic University Malaysia, Kuala Lumpur 53100, Malaysia
[5]Department of Information Technology, College of Computer, Qassim University, Buraydah 51452, Saudi Arabia
[6]Department of Electrical and Electronics Engineering, Universiti Malaysia Sarawak, Kota Samarahan 94300, Malaysia
[7]Department of Computer Science and Information Systems, Al-Mansour University College, Baghdad 10067, Iraq

Corresponding authors: Mohammad Kamrul Hasan (mkhasan@ukm.edu.my) and Sheroz Khan (sheroz@ieee.org)

This work was supported by the Universiti Kebangsaan Malaysia (UKM) under Fundamental Research Grant Scheme, FRGS/1/2020/ICT03/UKM/02/6.

**ABSTRACT** The importance of image security in the field of medical imaging is challenging. Several research works have been conducted to secure medical healthcare images. Encryption, not risking loss of data, is the right solution for image confidentiality. Due to data size limitations, redundancy, and capacity, traditional encryption techniques cannot be applied directly to e-health data, especially when patient data are transferred over the open channels. Therefore, patients may lose the privacy of data contents since images are different from the text because of their two particular factors of loss of data and confidentiality. Researchers have identified such security threats and have proposed several image encryption techniques to mitigate the security problem. However, the study has found that the existing proposed techniques still face application-specific several security problems. Therefore, this paper presents an efficient, lightweight encryption algorithm to develop a secure image encryption technique for the healthcare industry. The proposed lightweight encryption technique employs two permutation techniques to secure medical images. The proposed technique is analyzed, evaluated, and then compared to conventionally encrypted ones in security and execution time. Numerous test images have been used to determine the performance of the proposed algorithm. Several experiments show that the proposed algorithm for image cryptosystems provides better efficiency than conventional techniques.

**INDEX TERMS** Internet of Medical Things, medical image encryption, lightweight encryption.

## I. INTRODUCTION

The Internet of Things (IoT) defines the concept of connected devices and objects of all types over the internet, wireless, or wired. The concept's popularity has increased over the years since these technologies are used for various objectives such as transportation, communication, business development, and education. IoT created hyper-connectivity shows that individuals and organizations could communicate with each other effortlessly from their remote locations [1]. Approximately 26.66 billion IoT devices are present in the current world. This mass IoT utility exploration began in 2011

The associate editor coordinating the review of this manuscript and approving it for publication was Muhammad Tariq.

with home automation, smart energy meters, and wearable devices [2]. The investigation of IoT has helped organizations in various ways, such as improving business strategies, blockchain for transactions recording and tracking of assets, and market research. IoT has also enhanced the lifestyle of individuals through the introduction of automated services. Nonetheless, the uncontrolled exploration of these technologies has been posing security and privacy challenges.

The lack of device updates, unconscious use of the devices without realizing the associated consequences, and changing of passwords have increased the cybersecurity access and risks to malicious applications of sensitive data on IoT systems. The inappropriate security mechanisms increase the possibility of a data breach, among other threats. Further, most security experts consider that IoT devices provide vulnerable points for cyber-attacks because of weak security policies and protocols [2]. Despite the several security mechanisms that have been developed and put in place to protect IoT devices from cyber-attacks, guidelines on emerging security challenges are yet to be adequately documented. This means that the end-user cannot use protective measures to avert the attacks on data. Hackers have created various malware forms to infect IoT systems since 2008 [3]. They have developed different phishing mechanisms to provoke individuals or employees to share sensitive information and data. Hence, personal devices and corporate workstations face violations of privacy because of attacks on high-profile enterprise entities. If the security experts and device producers assess the cyber threats accurately, they could create efficient protective methods to counteract and prevent cyber threats. It is crucial to have experts to overcome various threat concerns and create comprehensive security policies and measures to protect business assets by enabling service stability and continuity.

Every day new technologies, energy, or modifications are added to the existing ones. For instance, the latest progressions from 1G to 5G networks play an important role in the IoT applications and systems [4], [5], [6]. This concept attracts researchers' curiosity and attention about the possible privacy and security risks, particularly with high bandwidth and frequency [7]. The short wavelength is likely to change the infrastructure, creating a need for more base stations serving the same region covered by the other wireless mechanism. The new structure could impose more threats, such as an increase in fake base stations.

Healthcare organizations and hospitals should balance the advantages of the Internet of Medical Things (IoMT) are providing while ensuring that they have the right protocols and policies for security challenges imposed. The different types of IoMT include consumer health monitory innovation such as Nike Fuel band, Fit Bit, or Withings that monitor the health of an individual or particular workout plan and connect to various mobile systems using Bluetooth innovation [3]. Another type is the internally-embed medical devices such as pacemakers or physically implanted procedures on a person but communicates wirelessly through Bluetooth or proprietary protocols. External medical devices or wearable are equipment such as mobile insulin pumps. Such devices utilize proprietary wireless protocols to send data and crucial information to doctors and patients. Stationary medical devices could include hospital-based chemotherapy systems or homecare cardio-monitoring stations. These systems use traditional wireless networks such as Wi-Fi networks to transfer data. Lastly, legacy medical equipment and medical procedures have been in use for more than 15 years [8]. Examples include X-ray systems, PACs, or CAT scan equipment currently utilized by health systems and hospitals. Although the devices cannot host modern Endpoint Detection and Response (EDR) systems, they still face similar security and privacy issues.

Managing IoMT-enabled security considers three considerations. First, recognize the devices as connected to a network. Second, determine and enforce what other systems, applications, and tools communicate. Lastly, ensure that these IoMT devices have interfered with other devices in the network or the organizations if something goes wrong. The accessibility of IoMT applications allows to make a diagnosis, make copies, data and retrieve a large number of digital images around the world. It often results in the production of illegitimate copies or unauthorized use in concern [9], [10], [11], [12], [13]. Therefore, to protect images, many researchers have focused on developing techniques for image security in the IoMT applications [6], [9]. Therefore, encryption is one of the effective ways to protect medical images.

The existing encryption techniques have been utilized the data encryption standard, advanced encryption standard, and Rivest–Shamir–Adleman algorithms for resolving the challenges for the circumstances of low-level efficiency though considering the low of size data as well as high redundancy [14], [15], [16], [16]. Therefore, these algorithms are hard enough to handle and ensure the appropriate encryption for medical images in the IoMT framework [9], [17], [18], [19]. Various image encryption algorithms or methods for converting, substituting, and inverting images different reversal methods have been reported. In a transposing mechanism, the plain image had been used applying the random rearrangement [18]. Permutation can be conducted for bits, pixel density, otherwise blocks [17]. Replacement, also attributed to as significance approaches have been explored, maps each element in the plain image to some other attribute in the cipher image [19]. Transcription methodologies are a hybrid of different basic particles which are position permutation and pixel value diffusion [15].

This paper's main contribution is a new lightweight encryption technique proposed to protect the privacy of the patients' medical image. We have considered the 256 bits for encryption for the image in the proposed lightweight encryption algorithm and then calculated the corresponding image's binary value by making 16 sub-blocks of 16 bits. The proposed technique guarantees the privacy and security of medical data being disseminated to healthcare centers. The

proposed technique is investigated. The safety is divided into three phases taking into account the 256-bit key value for logical operation.

The remaining part of this article is structured as follows: the related algorithms, techniques, and methods are discussed in section II. Security measurement and proposed lightweight encryption algorithm is presented in Section III. Section IV presents the experimental evaluation of the proposed technique. Finally, section V concluded the paper.

## II. RELATED WORK

The IoMT has benefited hospitals and healthcare organizations tremendously. However, advancement in technology imposes security and privacy challenges to organizations using this innovation—the concern on the security and privacy issues common in the IoMT. Medical systems pose a risk to each other regarding confidentiality, integrity, and data and information availability. Security problems could disrupt availability, compromise integrity, and affect confidentiality.

Further, medical data could be used for fraud or identity theft and discover medical prescriptions; hence, it enables hackers to order drugs online. Hackers might also engage in blackmail and extortion of people with specific illnesses they do not want to disclose. These aspects of confidentiality, integrity, and availability of IoMT-enabled wellbeing such as fitness trackers are also prominent. Another security issue is access control and authorization. In essence, exercising access control over the IoMT network is essential. It is crucial to establish if the user, once recognized and validated, has permission to access the demanded resources. Access control needs communication between software entities to request and gives access. Nonetheless, effective access control on the internet of medical things is challenging.

Identity management and authentication is another challenge to security and privacy in the IoMT. Identity management involves the unique objects' identification, and authentication then validates the identity relationship between parties. Authentication with IoT is crucial since confidentiality, integrity, and availability could be compromised without it. If an adversary could authenticate as a legitimate entity, they would have access to any data, hence compromising confidentiality, integrity, and availability [1]. Identification and authentication of users in the IoMT is a significant issue. Password and username pairs are the common forms of identification and authentication of parties in electronic systems. Other methods include biometric credentials, shared keys, and digital certificates. The high rate of heterogeneity and the large scale of IoMT systems would increase security threats to the current internet. Heterogeneity greatly influences network and protocol security services applied to IoMT [3]. Security solutions need to cope with various hardware specifications and need to offer authorization and authentication of IoT systems. Other security issues include physical restrictions of communications and devices. IoMT devices are embedded with low area and low power processors, and it is necessary to apply Internet Protocols even to the smallest devices. The limitations of IoMT devices restrict the ability to process information with more incredible speed [19]. This means there is a restricted memory, CPU, and energy budget. The challenging security forms are needed to satisfy the competing objectives of minimal resource consumption and robust performance. The restriction in power and size influences the efforts to maintain integrity and confidentiality in IoMT systems.

The use of security analytics could significantly decrease the vulnerability issues on the Internet of Medical Things applications. Security analytics involves gathering, correlating, and evaluating data from various sources that could help IoMT security providers to recognize potential threats and eliminate them. Apart from monitoring the IoMT gateway, multi-dimensional security analytics is necessary. Suspicious and malicious anomalies could be recognized by comparing data from multiple domains. This enables the security experts to gather anomalies and prevent them. Another solution is the use of critical public infrastructure [20]. Public key infrastructure refers to a set of hardware/software, policies, and procedures needed to develop, manage, and distribute digital resources. The security process has been proven as an efficient solution to IoT security challenges. Public Key infrastructure ensures data encryption through symmetric and asymmetric encryption procedures.

Therefore, the protection of electronic health-related images has attracted much attention recently, particularly when these pictures are sent through correspondence networks. An image encryption method tries to transform a picture into some other picture hard to realize. Security mechanisms deployed in present digital healthcare image methods are mainly based on traditional encryption methods like DES, AES, IDEA, and RSA [16]. It is appealing to create an effective healthcare image encryption scheme, particularly for real-time teleradiology or any other internet remote examinations, where big electronic medical pictures are transmitted more than public networks. Digital images have many uses in healthcare diagnostics such instance, computed tomography, and magnetic resonance imaging. Additionally, you can find many techniques, which are employed with electronic pictures including sound detection, watermarking, image segmentation, feature extraction, noise deletion, and picture compression [17]. For analysis and investigation needs, medical images, as probably the most essential component of health details. These images are often transmitted and exchanged using mobile communications and the internet between the research institutions and hospitals worldwide. Medical image storage and analysis are nowadays cloud-based, providing preconditions for effective coordination of full sharing and remote diagnosis of scientific investigation resources [18]. The patient information is private and should not be disclosed publicly. Doctors are transmitting the patient info via a public community in the form of a picture to consult professional doctors. Thus, security plays a crucial part in sending information through the Internet network system.

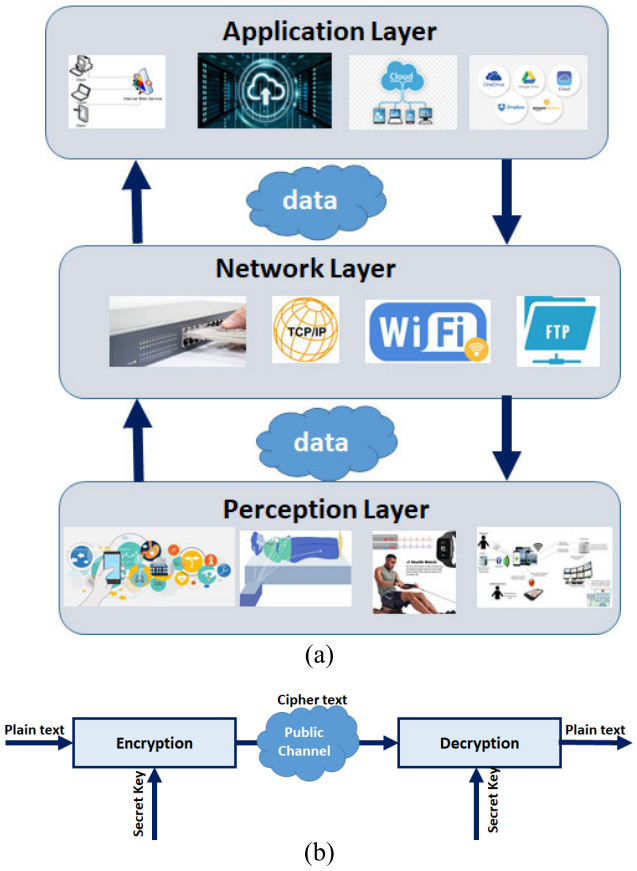



**FIGURE 1.** Representations of IoMT framework (a) And the Image security paradigm of IoM (b) [4].

Nowadays, the IoMT is advanced in evolving high-tech applications using medical data, and patient images are transferred globally through cloud servers. The patient data are primarily stored as a cloud server in the hospital and then used from various remote locations.

Therefore, the patient personal information, hospital data, and medical images need to be protected in such IoMT-enabled infrastructure [3], [4]. The conceptual framework for the medical images in IoMT infrastructure with the security paradigm is presented in Figure 1 [4]. Indeed, the structure it should have been made sure for the safe transmission and compelling stockpiling of clinical pictures interleaved with quiet data. An alternate disorganized framework in the phases of perplexity and dissemination has been dissected by choosing a complex disordered guide to additionally upgrade the intricacy of the calculation, thus improving the security [9], [13]–[15], and [19]–[23]. The representations of IoMT framework (a) and the Image security paradigm of IoM (b) are shown in Fig 1. The picture encryption calculation named Shuffle Encryption Algorithm (SEA) had exhibited a nonlinear byte-substitution arrange by utilizing an s-box with the assistance of a mixed activity [19]. The calculation in states by utilizing a query table (s-box) to play out the nonlinear byte substitution activity. Mostly, savage power assaults and factual assaults are discussed. In any case, different kinds of assaults irrelevant to the measurable or beast power assaults can likewise be conceivable to process with the technique. Another picture encryption calculation encodes just the touchy pieces of the pictures for the time-delicate applications. Similarly, the encryption of images dependent on the calculated guide utilizing bedlam based input cryptographic procedure had been executed with the thought of an outer mystery key of 256-piece long [20]. Besides, a half-breed advancement with cryptography encryption for clinical pictures in the IoMT system has been introduced [21]. The appropriate key will be chosen using hybrid swarm optimization, i.e., grasshopper optimization and particle swarm optimization in elliptic curve cryptography, to improve the security level of the encryption and decryption process. Because of this process, in the IoMT system, the medical images are protected. This section will summarize the existing research done by other researchers.

A hybrid model of the modified genetic algorithm (MGA) and the coupled map lattices medical image encryption method is proposed in [17]. The proposed method applies to the MGA to increase the cipher images' entropy and reduce the algorithm computational period. Experimental computer and results simulations all suggest which the proposed technique, which contains a hybrid algorithm, works with high-quality encryption and can also fight various typical attacks. Table 1 shows work related to IoMT.

Based on the encryption and decryption process, Hongjun *et. al.,* [22] have proposed an asymmetric encryption program for encryption of color pathological picture according to the Dadras complicated hyperactive chaotic system. The original problems for the chaotic device are produced by taking 512 bits of protected hash algorithm (SHA) worth of the basic image. The system seems to have a key size big enough to fight the brute force attack and also received great sensitivity to the key used. Do the similar work medical image encryption algorithm proposed by [23], the Proposed a healthcare image encryption algorithm dependent on confusion and also diffusion operation carried out by using Arnold's transformation and 2 chaotic methods, Logistic chart and also Henon map.

The Logistic chart is utilized to produce the original problems for the Henon chart and Arnold's transformation is being used for creating a scrambled healthcare picture. The Henon map is utilized to produce the XOR's chaotic sequence with the scrambled healthcare picture, producing the cipher image. Several medical image encryption techniques are proposed in [24]–[26] and [27]–[40]. M. Mukhedkar at el in [27] suggested that the image encryption was accomplished utilizing Blowfish Algorithm due to its excellent execution and delivery time. The method applied the Least Significant Bit (LSB) method for concealing the images. To provide substantial protection, a hybrid approach continues to be recommended that use a combination of image encryption plus image encryption plus image hiding. PSNR and MSE have been used for estimating the dynamics.

The 2D Zaslavsky chaotic map and the 2D Logistic map were used in reference [40] to encrypt real-time wireless capsule endoscopes (WCE). The Logisticsine chart was used in suggested [47] to encrypt medical images combined with mod service on a software platform and in combination with XOR. The MSB-based reversible data encryption approach was presented in reference [48], and the encrypt domain-based dual-image reversible hiding technology, which could also recover the database's lossless cover. The linear chaotic map and the logistic map were merged about [49] combined with DNA computation to encrypt medical images, incorporating patient information in the screening domain. In reference to [50], there is a method where the basic medical images are covered directly in the cover images. However, the patients images are not encrypted themselves. When a hacker learns, the knowledge is concealed in the cover image, and therefore it is possible to retrieve a medical image specifically. Since multi-scale transformations were compressed in medical pictures, various encryption technologies were employed, such as RSA [51], Blowfish, Concept, and RC5 [52]. There has been suggested a three-layer encryption system for medical files that can be used for encrypting watermarks, images, and file embedding [53].

## III. SECURITY MEASUREMENT AND PROPOSED LIGHTWEIGHT ENCRYPTION ALGORITHM

Security implementation is a significant issue in the advanced world, cryptography calculations are one of the approaches to guarantee security [41]–[43]. Focusing on the picture encryption issue in clinical pictures of IoMT application in IoMT based structure [44]. The entropy highlight is upgraded through a proficient encryption calculation and the relationship between two pixels can be diminished with the equivalent [45]. With the assistance of entropy and corresponded the worth. So the effectiveness can increment. Besides, we change the procedure that has been discovered complex in an investigation. The productivity of a calculation is registered based on entropy and connection. In strategy 1, we have presented a square-based change design to build the encoded pictures' security level. Then again, the unscrambled content must be equivalent to the first content. In any case, this prerequisite is not essential for picture information. Because of the Characteristic of human discernment, a decoded picture containing little expression is ordinarily satisfactory. Besides, picture-based information requires more exertion during encryption and decryption. A change procedure dependent on the mix of picture stage and a recently evolved encryption calculation called "Hyper Image Encryption Algorithm (HIEA)" presented [14], [19], [46]. From the chose picture, we will utilize the twofold worth squares, which will be reworked into a permuted picture using a change procedure, and afterward, the produced picture will be encoded utilizing the "Hyper Image Encryption Algorithm (HIEA)" calculation. All the current strategies utilizing the reasonable client characterized key is created with a similar goal. Likewise, separate between them with a proposed calculation utilized for encryption and decryption. For entropy esteem, connection worth, and execution time of the known cryptographic calculation with proposed cryptography calculations.

The proposed lightweight encryption algorithm focused on the efficiency and security of the medical images on IoMT application. The proposed algorithm considered the performance matric of entropy, as well as correlation. The detail is discussed below:

### A. ENTROPY

The entropy is a measure of the similarity between the original image and the encrypted-image. The results show that the cover image's entropy and the encrypted image are very closed or similar, which means that the proposed method has a very good visual quality. A plain image does have a value of 'zero' entropy. Consequently, by contraction, such a method of 'zero entropy' image can indeed be modified it into a smaller file size. On the other hand, a high entropy image (i.e., a moon image of intensely derived areas) with a large pixel density cannot be compacted into a smaller image as better as a close to zero image a dissimilar image. Therefore, the entropy can be represented in Eqn. (1) [6], [7].

$$E = -\sum_{N=0}^{S-1} P(n) \log P(n) \tag{1}$$

E denotes entropy, gray value of the input image present by S (0... 255), and P (n). The possibility of symbol S. parameter is also used to analyze the cover image and image encryption. This test measures proportions of the details, and it is usually presented as bits in units. A more significant entropy value indicates a higher level of security when applied to evaluate image encryption. Usually, an entropy value that is very close to an absolute value of 8 means it is safe from a brute force attack. Table 4 shows the information entropy of encrypted data. The results show that the proposed technique achieves entropy near to value 8. Thus, it provides a high level of security.

### B. CORRELATION

The University of South Carolina pioneered the development and growth of the digital image correlation (DIC) technique that has been updated and enhanced in recent decades. DIC is based on the extension of a correlation coefficient that can be defined by analyzing the pixel strength array sub-set on several image-related images and eliminating the deformation mapping function that equates to the images. A repeated strategy is applied to the use of nonlinear modeling strategies to decrease the 2D correlation coefficient. This feature confirms that the suggested encryption algorithm is effective against statistical attacks [6]. The cross-correlation coefficient ($\eta_{ij}$) can be defined as in Eqn. (2) [6], [7].

$$\eta = \frac{n\sum ab - \sum a \sum b}{\sqrt{\frac{n\sum (a^2) - \sum (a^2)}{n\sum (b^2) - \sum (b^2)}}} \tag{2}$$

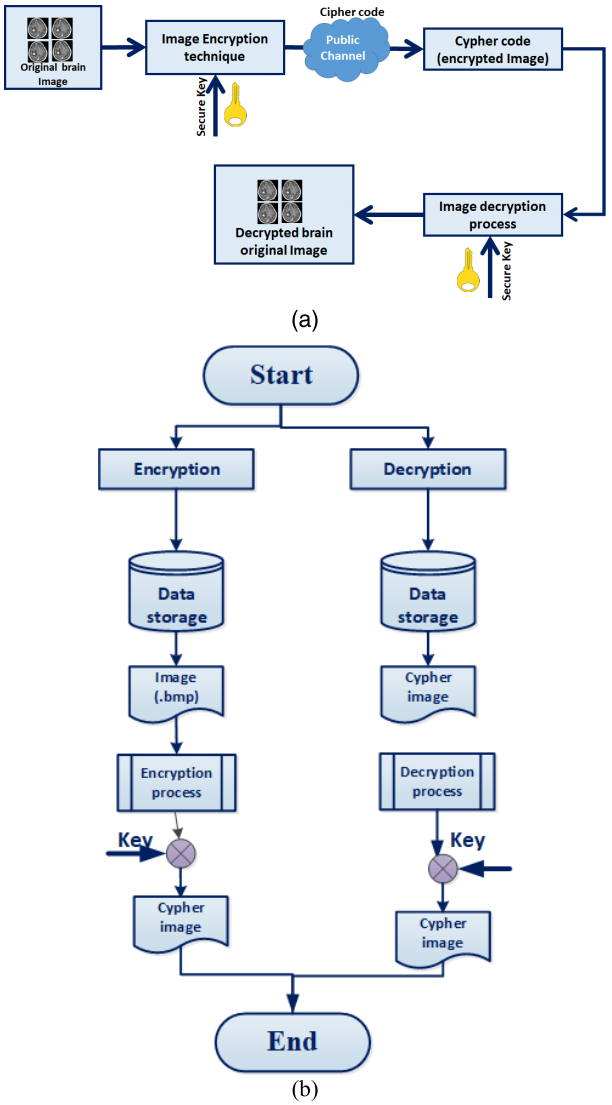



**FIGURE 2.** The working procedure of the proposed encryption and decryption system (a), and the flowchart for the encryption/decryption system (b).

where the correlation is denoted by $\eta$, number of pairs of data is denoted by n; $\Sigma ab$ the sum of the products of just the data series; $\Sigma a$ the sum of data, $\Sigma b$ the amount of squared data; and $\Sigma b^2$ the aggregate of the squared b data [5]. Some of the key performance depend on encryption quality, crypto-analysis, memory requirement, execution time [4], [8], [32], [33], [34]. In the underlying phase of the proposed picture encryption strategy and documents required to cover. It used the encoding module and extrication module, shown in Figure 2. It has been used the visual.net structure for image cryptosystem [3], [4]. Medical image security must follow the encryption method that should be secured that used encryption-decryption computationally and has no problem with the system performance. The proposed encryption techniques are classified into two techniques, which processes are illustrated in Figure 3. The existing technique is adopted and enhanced as follows.

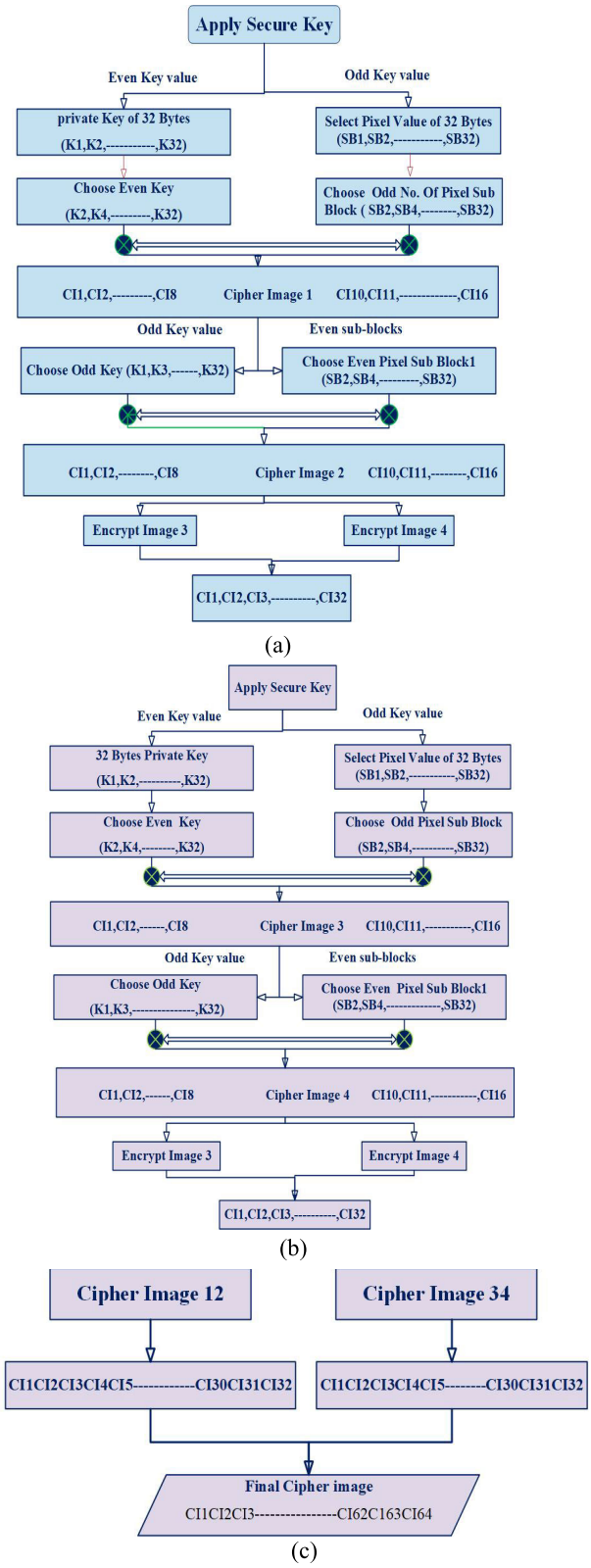



**FIGURE 3.** Proposed system architecture phase I (a), phase II (b), phase III (c).

- At first, an image will be selected,
- Pixel blocks are then created from the selected image by dividing.

- Estimating the pixel block = image width/10 at horizontal
- Estimate the pixel block = image height/10 at the vertical. Follows the estimation of the number of pixel blocks *(pixel blocks =horizontal pixel block * vertical pixel block)*. Then the number of pixel blocks will be checked by:
  *If pixel blocks / 2 ! = 0,* then *set number of pixel blocks = number of pixel blocks + extra pixel block.*

1. Split the pixel blocks into sub-blocks (SB1, SB2…)
2. Then select variables $I = 0$ and $R = 0$
   *(R => random variable).*
   While *(I < SB1. R = random number between (0, Sub-Block1-1))*
3. Set the new location of *block R <= pixel-block*
   $I = I + 1$
   *End While.*
4. Likewise for SB2. $I = 0$ *and* $R = 0$
   While *(I < SB2.R = random number between (0, SB2-1) R <= pixel-block).*
   $I = I + 1$
   End While.
5. Finally, we get the new location of pixels block in SB1 and SB2 [6].

The suggested encryption algorithm is designed with a three-phase process. In phase one, the transition mechanism's output passed as an input, and the output of step one passed as an input to phase two, eventually transferring the output of phase two as an input to phase three. Shuffled with 256-bit key value using logical operation in the whole process. The proposed system architecture is shown in Figure 3. The proposed techniques procedure is maintained as below:

1. At first, we configure the parameters
2. Then Appling Key for the brain images.
3. Start Key nomination and Image nomination process
4. The compute and apply:
   - Block-based Image encryption Transformation
   - The proposed lightweight Image encryption algorithm
5. Check for the computed best data

## IV. EXPERIMENTAL EVALUATION OF PROPOSED TECHNIQUE

The performance of the proposed encryption technique was evaluated using an experimental approach. The encryption technique uses three stages to encrypt the image considering 256 bits key value for logical operation. The experimental evaluation was made using the 8th Gen, Intel(R) Core(TM) i7-8550U CPU @ 1.80GHz 1.99 GHz, Microsoft Windows 10, 1TB HDD, Borland Delphi 7.0, Matlab 2016 and Windows10 64bit tools. For the experiment, 4 images such as image 1.jpeg, image 2.jpeg, image 3.jpeg, and image 4.jpeg have been considered where the image quality

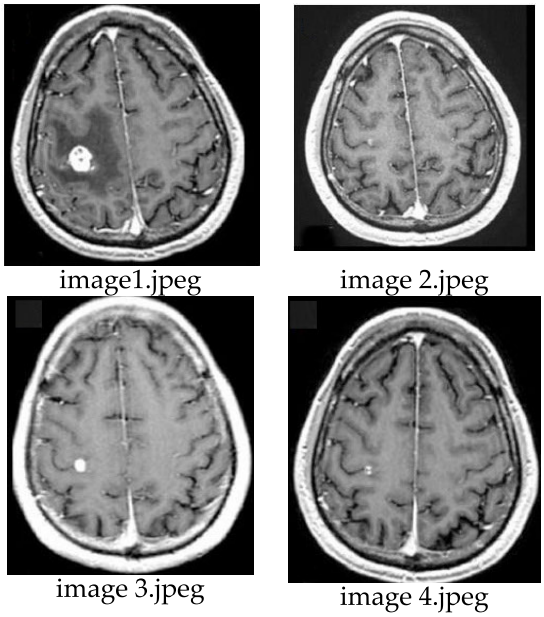



**FIGURE 4.** Sample images for the proposed technique.

was 512 x 512 pixels as well as 8 bits per pixel (bpp) in the grayscale image, which has 256 different colors in it or 256 shades. The entropy's value and the execution time of a known cryptography algorithm with the recommended cryptography algorithm selected 32-byte/256 bits key length. The image is decomposed into 10 pixels × 10 pixels blocks. Moreover, this key has been applied to various chosen images (shown in Figure 4).

The proposed new lightweight encryption technique mechanism considers the following steps:

- Select one image of 256 bits for encryption
- Calculate the binary value of the corresponding image to make 16 sub-blocks of 16 bits.
- Repeat the process until the end of the file
- Select the 256 bits key and creates the 16 sub-blocks of 16 bits
- From the transformation, the table choose 64 bits and build 4 blocks of 16 bits
- Use XOR operation concerning with initial 8 block of a particular image and 8 blocks of the selected key
- Again using the XOR operation between the last 4 blocks of the correspondence image and 4 blocks of the transformation table. Then the outcome will be stored in the image blocks
- Apply circular shift operation on the last 4 blocks of the applied key and the last 4 blocks of the particular image
- The XOR operation is applied between selected image with the key to achieve the output. Therefore the result is stored in the image.

The result comparison is presented in Table 2, Table 3, and Table 4 and graphical representation for technique one (1) and technique two (2). Table 2 describes the first technique in terms of execution time. Table 3 for the second

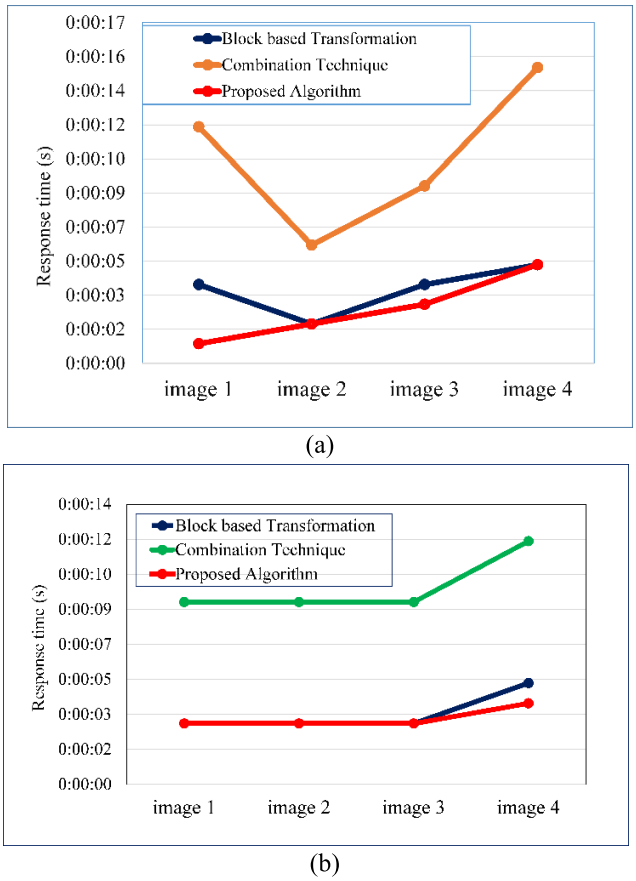



**FIGURE 5.** Encryption time comparison between the existing (a) And proposed algorithm (b).

technique compares existing algorithms with the proposed algorithm in terms of the original image's entropy. In contrast, Table 4 expresses the entropy of encrypted image and compares the traditional algorithm with the proposed algorithm. The entropy be determined by the algorithm's complexity, key, and images that have definite impacts on algorithm performance.

Figure 5 and Figure 6 demonstrate the computed data of the existing and the proposed technique.

A hybrid of block-based image transformation and proposed encryption is the proposed lightweight method for medical image protection. In this approach, the block density and correlation work oppositely, varying the entropy. The technique is then compared with commonly used existing algorithms. The proposed algorithm is secured and straightforward with higher efficiency that can produce the stronger cipher symmetric key.

The effectiveness of the proposed encryption method's time can determine the subsequent system to encode and unscramble the data execution quickly. The adaptability of the proposed encryption procedure is exceptionally high that can be presented in Figure 6. Using Table 3, Figure 6, displayed the Comparison of the execution time between the existing and proposed algorithm, (a) entropy of the original image (b) entropy of the encrypted image. Figure 7 presented the

**TABLE 1.** Related work.

| Author, year | Methods and Models | Evaluation Approach |
|---|---|---|
| Pareek et al. [16] 2016 | Genetic algorithms | Gray scale image security |
| Nematzadeh at el. [17] 2018 | hybrid model of the modified genetic algorithm (MGA) coupled map lattices | MATLAB 2013 on a laptop with an Intel Core i7, 2.3 GHz CPU, 8 GB memory and 500 GB hard disk with a Windows 8 operating system |
| Dai at el. [23] 2016 | chaos encryption | bit-plane decomposition |
| Avudaiappan et al. [24] 2018 | Dual Encryption | Oppositional Based Optimization Algorithm |
| Kanso at el. [25] 2015 | the chaos-based image encryption scheme | pseudorandom matrix |
| Lima at el. [26] 2015 | the cosine number transform | Matlab and images complying with the Digital Imaging and Communications in Medicine (DICOM) standard |
| Mukhedkar at el. [27] 2016 | cryptography & Steganography | Blowfish Algorithm (LSB technique) |
| Liu at el. [28] 2016 | Asymmetric color pathological image encryption | complex hyperchaotic system |
| Laiphrakpam et al. [29] 2017 | ElGamal encryption technique. | Koblitz encoding technique |
| Cao et al. [30] 2017 | edge maps | binary bit-plane decomposition |
| Gupta at al. [31] 2018 | chaotic map | The encryption is done by using 256bit long external secret key |
| Hamza at.al [47] 2020 | chaos-based encryption cryptosystem | Zaslavsky chaotic map and the 2D Logistic map |
| Hua Z, Yi S, Zhou Y [48] (2018) | scrambling and pixel adaptive diffusion | the pixel adaptive diffusion: bitwise XOR and modulo arithmetic |
| Ke G, Wang H, Zhou S, Zhang H 49[] (2019) | MSB-based reversible data encryption | dual-image reversible hiding technology |
| Khond S, Vijayakumar B [50] (2019) | Chaos and Dna encryption | reversible data hiding technology |
| Priya S, Santhi B[51] (2019) | visual medical image encryption | Visually biometric authentication |
| Raja SP [52] (2019) | Joint medical image compression–encryption | multiscale transform-based image compression encoding techniques |
| Raja SP [53] (2019) | Multiscale transform | symmetric key cryptography and ebcot encoding technique |
| Salama AS, Mokhtar MA, Tayel MB [54] (2019) | triple-layer encryption-watermarking technique | multi-level encryption-based technique |

Comparison between the current and proposed algorithm,(a) entropy of the original image (b) entropy of the encrypted image, respectively..

The proof of the improvement of effectiveness was accomplished between our ''proposed calculation'' and ''picture

**TABLE 2.** Encryption/decryption time (in second (S)) comparison of various image encryption algorithm with proposed algorithm.

| Image | Block-Based Transformation (S) | Combination of Technique (S) | Proposed Algorithm (S) |
|---|---|---|---|
| image1 | 0:00:04 | 0:00:12 | 0:00:01 |
| Image2 | 0:00:02 | 0:00:06 | 0:00:02 |
| Image3 | 0:00:04 | 0:00:09 | 0:00:03 |
| Image4 | 0:00:05 | 0:00:15 | 0:00:05 |

| Image | Block-Based Transformation (S) | Combination of Technique (S) | Proposed Algorithm (S) |
|---|---|---|---|
| image1 | 0:00:03 | 0:00:09 | 0:00:03 |
| Image2 | 0:00:03 | 0:00:09 | 0:00:03 |
| Image3 | 0:00:03 | 0:00:09 | 0:00:03 |
| Image4 | 0:00:04 | 0:00:12 | 0:00:04 |

**TABLE 3.** Comparison of the proposed and traditional algorithms in terms of the entropy of original image.

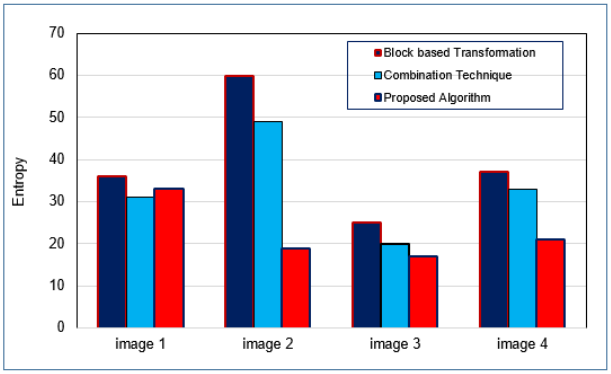
| Image | Block-Based Transformation (S) | Combination of Technique (S) | Proposed Algorithm (S) |
|---|---|---|---|
| image1 | 36 | 31 | 33 |
| Image2 | 60 | 49 | 19 |
| Image3 | 25 | 20 | 17 |
| Image4 | 37 | 33 | 21 |

| Image | Block-Based Transformation | Combination of Technique | Proposed Algorithm |
|---|---|---|---|
| image1 | 17 | 17.9 | 18 |
| image2 | 39 | 46 | 41 |
| image3 | 15 | 18 | 13 |
| image4 | 23 | 46 | 21 |

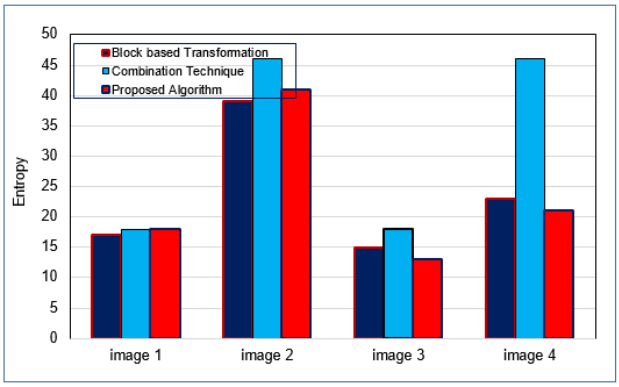
encryption utilizing square-based change calculation," "a picture encryption approach utilizing a mix of stage procedures followed by encryption." Besides, the encryption calculation offered here is a straightforward and direct mapping calculation that uses the festal structure and a couple of legitimate activities. This kind of measure conveys almost no entropy, and along these lines, it cannot be actualized during the time spent the encryption of the classified message. The proposed estimate would be helpful to solve the security and proficiency issues.

Finally, the discussions on the results obtained from the proposed algorithm recommend that it is significant to get a greater entropy of encrypted images than the conventional method. For this justification, it has integrated into any phase of encrypting any image. The computational complexity is not so much the main factor of entropy implications.

The key and the images just have that impact on it. Besides, based on the results shown in Table 5, the proposed method outperformed state-of-the-art encryption [41]. The proposed method achieved higher MSE than state-of-the-art encryption. The average MSE for the proposed method was 229.6, while for existing methods achieved about 224.4. The




(a)




(b)

**FIGURE 6.** Comparison between existing and proposed algorithm, (a) Entropy of the original image (b) Entropy of the encrypted image.

**TABLE 4.** Entropy of encrypted image comparison of various algorithm with proposed.

| Cover Images | Cover Image Entropy | Block-Based Transformation | Combination of Technique | Proposed Algorithm |
|---|---|---|---|---|
| Image 1 | 7.98 | 6.5069 | 7.1763 | 7.98 |
| Image 2 | 7.98 | 6.3389 | 6.9828 | 7.98 |
| Image 3 | 7.98 | 6.5953 | 6.2105 | 7.98 |
| Image 4 | 7.98 | 6.48037 | 6.78987 | 7.98 |

| Cover Image | Block-Based Transformation | Combination of Technique | Proposed Algorithm |
|---|---|---|---|
| image 1 | 3.21281.8 | 6.80750.9 | 7.8 |
| image 2 | 6.01113.4 | 5.90030.1 | 7.8 |
| image 3 | 5.61346.7 | 6.81041.8 | 7.8 |
| image 4 | 4.37681.9 | 4.80971.6 | 7.8 |

proposed method shows that the PSNR and MSE are most effective than the previous method

The Peak-Signal-to-Noise Ratio (PSNR) functions to assess the quality of an image [55]. A low value of PSNR reflects a promising image encryption method. Mathematically, this quality of the encrypted image can estimate based on PSNR as formulated in Eqn. (3).

$$PSNR = 10\frac{255^2}{MSE}, \tag{3}$$

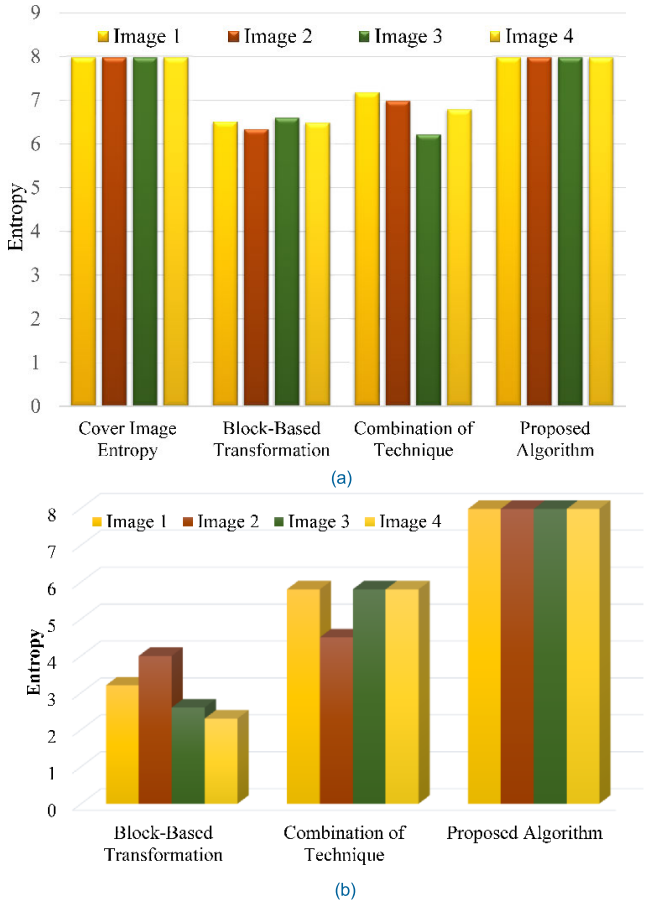



**FIGURE 7.** Comparison between existing and proposed algorithm, (a) Entropy of the original image (b) Entropy of the encrypted image.

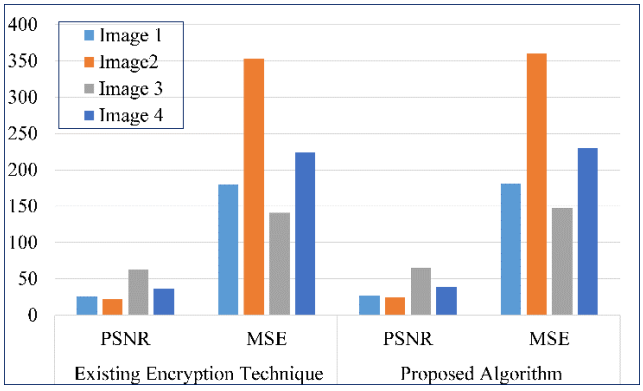



**FIGURE 8.** The MSE and PSNR, the performance of proposed and existing algorithm.

where MSE denotes the mean square error between the ground truth image and the encrypted image [56]. It calculated MSE using Eqn. (4)

$$\mathrm{MSE} = \sum_{i=1}^{N} \sum_{j=1}^{M} \frac{[P(i,j) - C(i,j)]^2}{NM}, \tag{4}$$

where P (i, j) is the pixel value of the original image, and C (i, j) The pixel value of the encrypted image, N and M, is row and column of the image, subsequently. ij are subscripted variables. Table 5 tabulates MSE and PSNR for different images consecutively. The results show that there is a minimum pixel bit match between original and encrypted of MSE generates. Thus, a high value of MSE generates. Further, MSE and PSNR are inversely proportional to each other. Therefore, a low value of PSNR achieves. The higher value of MSE and lower PSNR are the desired features of the appropriate encryption algorithm.

**TABLE 5.** MSE and PSNR for existing encryption and proposed algorithm.

| Image | Existing encryption [56] | | Proposed Algorithm | |
|---|---|---|---|---|
| | PSNR | MSE | PSNR | MSE |
| Image 1 | 25.58 | 179.65 | 27 | 181 |
| Image 2 | 22.56 | 352.72 | 25 | 360 |
| Image 3 | 62.64 | 140.96 | 65 | 148 |
| Average | 36.92 | 224.4 | 39 | 229.6 |

**TABLE 6.** Encryption speed for the proposed algorithm.

| Techniques | Encryption Speed MB/s | Experimental System Configuration |
|---|---|---|
| Proposed scheme | 0.1 | 8th Gen, Intel(R) Core (TM) i7-8550U CPU @ 1.80GHz 1.99 GHz, Microsoft Windows 10, MATLAB 16 |
| Block based transformation | 3 | Pentium IV 3.2GHz PC with 8GB RAM, Using Borland C++ builder software |

Complexity points are units of measure based on relative sizing. It is used to estimate development work in terms of complexity and size instead of traditional time-based methods that attempt to measure the duration of time required to complete some work unit. Therefore, searching complexity becomes reducing to ($n$), the proposed algorithm linearly searches the original data value in the image size lookup table, which generates complexity of $O(n)$, where $n$ denotes the size of the image (M X N), and I is the iteration. The time complexity of the proposed algorithm thus becomes O(MNI). The computational speed of the proposed algorithm is estimated by referring to Table 6. The encryption speed is measured in MB/s for various 512 × 512 images, and the mean speed is calculated, which is compared with other existing schemes in Table 6.

From the data presented above, it is clear that the existing algorithm still has limitations in terms of encryption/decryption time, entropy and complexity. However, the proposed algorithm has shown high performance in terms of encryption and lower decryption time, encrypted entropy, encryption speed, and low complexity.

## V. CONCLUSION

This paper has proposed a secure, lightweight algorithm encryption technology to protect patients' medical images' privacy. This paper also included different security measurements, encounter parts, and techniques for medical image encryption. This paper also discussed the various existing encryption techniques, using encryption quality, memory requirement, and execution time. The study has found that the current methods generated key based unsystematic sequence number that creates an enormous computation time. In comparison, it is evident from the result that the proposed algorithm has a small computation. Therefore, to secure the medical image, the proposed algorithm is designed carefully to get optimum security. The encryption technique uses three stages to encrypt the image considering 256 bits key value for logical operation. This study has used the 8th Gen, Intel(R) Core (TM) i7-8550U CPU 1.80GHz 1.99 GHz, MATLAB 16, 1TB HDD, Borland Delphi 7.0, MATLAB 2016, and Windows10 64bit tools are used to evaluate and analyze the performance. Each image quality has been 512 x 512 pixels and 8 bits per pixel, or 256 intensity levels. The experiment was conducted at the cybersecurity laboratory with the system, as mentioned earlier, to analyze the proposed and existing algorithms. From the experiment results and the comparison, the proposed technique achieves better efficiency than conventional methods in terms of execution time for the medical image encryption.

## ACKNOWLEDGMENT

The author would like to thank Onaizah Colleges, Qassim University, Saudi Arabia, International Islamic University Malaysia, and Universiti Malaysia Sarawak, Malaysia, for the collaborative work.

## CONFLICTS OF INTEREST

The authors declare no conflict of interest.

## REFERENCES

[1] J. Porras, J. Pänkäläinen, A. Knutas, and J. Khakurel, "January security in the Internet of Things—A systematic mapping study," in *Proc. 51st Hawaii Int. Conf. Syst. Sci.*, 2018, pp. 3750–3759.

[2] F. Alsubaei, A. Abuhussein, and S. Shiva, "Security and privacy in the Internet of medical things: Taxonomy and risk assessment," in *Proc. IEEE 42nd Conf. Local Comput. Netw. Workshops (LCN Workshops)*, Oct. 2017, pp. 112–120.

[3] M. Elhoseny, G. Ramirez-Gonzalez, O. M. Abu-Elnasr, S. A. Shawkat, N. Arunkumar, and A. Farouk, "Secure medical data transmission model for IoT-based healthcare systems," *IEEE Access*, vol. 6, pp. 20596–20608, 2018.

[4] M. K. Hasan, A. F. Ismail, S. Islam, W. Hashim, M. M. Ahmed, and I. Memon, "A novel HGBBDSA-CTI approach for subcarrier allocation in heterogeneous network," *Telecommun. Syst.*, vol. 70, no. 2, pp. 245–262, Feb. 2019.

[5] M. K. Hasan, A. F. Ismail, A. H. Abdalla, K. Abdullah, H. Ramli, S. Islam, and R. A. Saeed, "Inter-cell interference coordination in LTE–A HetNets: A survey on self organizing approaches," in *Proc. Int. Conf. Comput., Electr. Electron. Eng. (ICCEEE)*, Aug. 2013, pp. 196–201.

[6] M. Elhoseny, K. Shankar, S. K. Lakshmanaprabu, A. Maseleno, and N. Arunkumar, "Hybrid optimization with cryptography encryption for medical image security in Internet of Things," *Neural Comput. Appl.*, vol. 32, no. 15, pp. 10979–10993, Aug. 2020.

[7] F. A. Turjman and S. Alturjman, "Context-sensitive access in industrial Internet of Things (IIoT) healthcare applications," *IEEE Trans. Ind. Informat.*, vol. 14, no. 6, pp. 2736–2744, Jun. 2018.

[8] F. Restuccia, S. D'Oro, and T. Melodia, "Securing the Internet of Things in the age of machine learning and software-defined networking," *IEEE Internet Things J.*, vol. 5, no. 6, pp. 4829–4842, Dec. 2018.

[9] M. K. Hasan, R. A. Saeed, R. A. Alsaqour, A. F. Ismail, H. A. Aisha, and S. Islam, "Cluster-based time synchronisation scheme for femtocell network," *Int. J. Mobile Commun.*, vol. 13, no. 6, pp. 567–598, 2015.

[10] S. Islam, A. H. Abdalla, M. K. H. O. O. Khalifa, O. Mahmoud, and R. A. Saeed, "Macro mobility scheme in NEMO to support seamless handoff," in *Proc. Int. Conf. Comput. Commun. Eng. (ICCCE)*, Jul. 2012, pp. 234–238.

[11] M. K. Hasan, A. F. Ismail, S. Islam, W. Hashim, and B. Pandey, "Dynamic spectrum allocation scheme for heterogeneous network," *Wireless Pers. Commun.*, vol. 95, no. 2, pp. 299–315, Jul. 2017.

[12] M. K. Hasan, R. A. Saeed, A.-H. Abdalla, S. Islam, and O. Mahmoud, "An investigation of femtocell network synchronization," *Proc. IEEE Conf. Open Syst.*, Sep. 2011, pp. 202–207.

[13] K. Shankar, M. Elhoseny, E. Perumal, M. Ilayaraja, and K. Sathesh Kumar, "An efficient image encryption scheme based on signcryption technique with adaptive elephant herding optimization," in *Proc. Adv. Sci. Technol. Secur. Appl.*, 2019, pp. 31–42.

[14] T. K. Araghi and A. A. Manaf, "An enhanced hybrid image watermarking scheme for security of medical and non-medical images based on DWT and 2-D SVD," *Future Gener. Comput. Syst.*, vol. 101, pp. 1223–1246, Dec. 2019.

[15] H. M. Ghadirli, A. Nodehi, and R. Enayatifar, "An overview of encryption algorithms in color images," *Signal Process.*, vol. 164, pp. 163–185, Nov. 2019.

[16] Y. Wan, S. Gu, and B. Du, "A new image encryption algorithm based on composite chaos and hyperchaos combined with DNA coding," *Entropy*, vol. 22, no. 2, p. 171, Feb. 2020.

[17] Ü. Çavuşoğlu, S. Kaçar, I. Pehlivan, and A. Zengin, "Secure image encryption algorithm design using a novel chaos based S-box," *Chaos, Solitons Fractals*, vol. 95, pp. 92–101, Feb. 2017.

[18] A. Mitra, Y. V. S. Rao, and S. R. M. Prasanna, "A new image encryption approach using combinational permutation techniques," *Int. J. Electr. Comput. Eng.*, vol. 1, no. 2, pp. 127–131, 2006.

[19] S. J. Shackelford, M. Mattioli, S. Myers, A. Brady, Y. Wang, and S. Wong, "Securing the Internet of healthcare," *Minn. JL Sci. Tech.*, vol. 19, p. 405, Feb. 2018.

[20] D. Pishva, "Internet of Things: Security and privacy issues and possible solution," in *Proc. 19th Int. Conf. Adv. Commun. Technol. (ICACT)*, 2017, pp. 797–808.

[21] W. Sun, Z. Cai, Y. Li, F. Liu, S. Fang, and G. Wang, "Security and privacy in the medical Internet of Things: A review," *Secur. Commun. Netw.*, vol. 2018, Mar. 2018.

[22] V. A. R. Shaktawat, S. RS, N. Lakshmi, and A. Panwar, "A hybrid technique of combining AES algorithm with block permutation for image encryption," *Rel., Theory Appl.*, vol. 15, no. 1, p. 15, 2020.

[23] N. K. Pareek and V. Patidar, "Medical image protection using genetic algorithm operations," *Soft Comput.*, vol. 20, no. 2, pp. 763–772, Feb. 2016.

[24] H. Nematzadeh, R. Enayatifar, H. Motameni, F. G. Guimarães, and V. N. Coelho, "Medical image encryption using a hybrid model of modified genetic algorithm and coupled map lattices," *Opt. Lasers Eng.*, vol. 110, pp. 24–32, Nov. 2018.

[25] T. Y. Sun, G. X. B, X. Chen, and Y. Yang, "A survey on the new development of medical image security algorithms," in *Cloud Computing and Security* (Lecture Notes in Computer Science), vol. 11065, X. Sun, Z. Pan, and E. Bertino, Eds. Cham, Switzerland: Springer, doi: 10.1007/978-3-030-00012-7_42.

[26] B. Acharya, S. K. Panigrahy, S. K. Patra, and G. Panda, "Image encryption using advanced hill cipher algorithm," *ACEEE Int. J. Signal Image Process.*, vol. 1, no. 1, pp. 663–667. 2010.

[27] A. R. Aswatha, S. Sasi, B. Santhosh, D. Mehta, and S. Babuprasad, "Design and implementation of unreliable CFDP protocol over elliptic curve cryptography," *Smart Innov., Syst. Technol.*, vol. 160, pp. 627–638, Dec. 2020.

[28] A. Banik, Z. Shamsi, and D. S. Laiphrakpam, "An encryption scheme for securing multiple medical images," *J. Inf. Secur. Appl.*, vol. 49, Dec. 2019, Art. no. 102398.

[29] H. Liu, A. Kadir, and Y. Li, "Asymmetric color pathological image encryption scheme based on complex hyper chaotic system," *Optik*, vol. 127, no. 15, pp. 5812–5819, Aug. 2016.
[30] Y. Dai, H. Wang, and Y. Wang, "Chaotic medical image encryption algorithm based on bit-plane decomposition," *Int. J. Pattern Recognit. Artif. Intell.*, vol. 30, no. 4, pp. 1–15, 2016.
[31] T. Avudaiappan, R. Balasubramanian, S. S. Pandiyan, M. Saravanan, S. K. Lakshmanaprabu, and K. Shankar, "Medical image security using dual encryption with oppositional based optimization algorithm," *J. Med. Syst.*, vol. 42, no. 11, pp. 1–11, Nov. 2018.
[32] A. Kanso and M. Ghebleh, "An efficient and robust image encryption scheme for medical applications," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 24, nos. 1–3, pp. 98–116, Jul. 2015.
[33] J. B. Lima, F. Madeiro, and F. J. R. Sales, "Encryption of medical images based on the cosine number transform," *Signal Process., Image Commun.*, vol. 35, pp. 1–8, Jul. 2015.
[34] M. Mukhedkar, P. Powar, and P. Gaikwad, "Secure non real time image encryption algorithm development using cryptography & steganography," in *Proc. Annu. IEEE India Conf. (INDICON)*, Dec. 2015, pp. 1–6.
[35] M. Jia, Z. Yin, Q. Guo, G. Liu, and X. Gu, "Downlink design for spectrum efficient IoT network," *IEEE Internet Things J.*, vol. 5, no. 5, pp. 3397–3404, Oct. 2018.
[36] D. S. Laiphrakpam and M. S. Khumanthem, "Medical image encryption based on improved ElGamal encryption technique," *Optik*, vol. 147, pp. 88–102, Oct. 2017.
[37] W. Cao, Y. Zhou, C. L. P. Chen, and L. Xia, "Medical image encryption using edge maps," *Signal Process.*, vol. 132, pp. 96–109, Mar. 2017.
[38] S. K. Pal and S. Anand, "Cryptography based on RGB color channels using ANNs," *Int. J. Comput. Netw. Inf. Secur.*, vol. 10, no. 5, pp. 60–69, May 2018.
[39] K. Rarhi and S. Saha, "Image encryption in IoT devices using DNA and hyperchaotic neural network," *Lect. Notes Netw. Syst.*, vol. 82., pp. 347–375, 2020.
[40] R. Hamza, Z. Yan, K. Muhammad, P. Bellavista, and F. Titouna, "A privacy-preserving cryptosystem for IoT E-healthcare," *Inf. Sci.*, vol. 527, pp. 493–510, Jul. 2020, doi: 10.1016/j.ins.2019.01.070.
[41] T. M. Ghazal, M. K. Hasan, R. Hassan, S. Islam, S. N. H. S. Abdullah, M. A. Afifi, and D. Kalra, "Security vulnerabilities, attacks, threats and the proposed countermeasures for the Internet of Things applications," *Solid State Technol.*, vol. 63, no. 1s, pp. 2513–2521, 2020.
[42] R. Hassan, F. Qamar, M. K. Hasan, A. H. M. Aman, and A. S. Ahmed, "Internet of Things and its applications: A comprehensive survey," *Symmetry*, vol. 12, no. 10, p. 1674, Oct. 2020.
[43] N. Varish, A. K. Pal, R. Hassan, M. K. Hasan, A. Khan, N. Parveen, D. Banerjee, V. Pellakuri, A. U. Haqis, and I. Memon, "Image retrieval scheme using quantized bins of color image components and adaptive tetrolet transform," *IEEE Access*, vol. 8, pp. 117639–117665, 2020.
[44] O. S. Albahri, A. S. Albahri, A. A. Zaidan, B. B. Zaidan, M. A. Alsalem, A. H. Mohsin, K. I. Mohammed, A. H. Alamoodi, S. Nidhal, O. Enaizan, M. A. Chyad, K. H. Abdulkareem, E. M. Almahdi, G. A. Al. Shafeey, M. J. Baqer, A. N. Jasim, N. S. Jalood, and A. H. Shareef, "Fault-tolerant mHealth framework in the context of IoT-based real-time wearable health data sensors," *IEEE Access*, vol. 7, pp. 50052–50080, 2019, doi: 10.1109/ACCESS.2019.2910411.
[45] N. Misran, M. S. Islam, G. K. Beng, N. Amin, and M. T. Islam, "IoT based health monitoring system with LoRa communication technology," in *Proc. Int. Conf. Electr. Eng. Informat. (ICEEI)*, Jul. 2019, pp. 514–517.
[46] S. Safavi, A. M. Meer, E. Keneth Joel Melanie, and Z. Shukur, "Cyber vulnerabilities on smart healthcare, review and solutions," in *Proc. Cyber Resilience Conf. (CRC)*, Nov. 2018, pp. 1–5.
[47] Z. Hua, S. Yi, and Y. Zhou, "Medical image encryption using high-speed scrambling and pixel adaptive diffusion," *Signal Process.*, vol. 144, pp. 134–144, Mar. 2018, doi: 10.1016/j.sigpro.2017.10.004.
[48] G. Ke, H. Wang, S. Zhou, and H. Zhang, "Encryption of medical image with most significant bit and high capacity in piecewise linear chaos graphics," *Measurement* vol. 135, pp. 385–391, Mar. 2019, doi: 10.1016/j.measurement.2018.11.074.
[49] S. Khond and B. Vijayakumar, "Secure medical image processing using chaos and dna encryption enhanced using reversible data hiding," *Int. J. Eng. Adv. Technol.* vol. 8, pp. 1062–1067, Feb. 2019, doi: 10.35940/ijeat.F1202.0886S19.
[50] S. Priya and B. Santhi, "A novel visual medical image encryption for secure transmission of authenticated watermarked medical images," *Mobile Netw. Appl.*, Feb. 2019, doi: 10.1007/s11036-019-01213-x.
[51] S. P. Raja, "Joint medical image compression–encryption in the cloud using multiscale transform-based image compression encoding techniques," *Sādhanā*, vol. 44, no. 2, p. 28, Feb. 2019, doi: 10.1007/s12046-018-1013-9.
[52] S. P. Raja, "Multiscale transform-based secured joint efficient medical image compression-encryption using symmetric key cryptography and ebcot encoding technique," *Int. J. Wavelets, Multiresolution Inf. Process.*, vol. 17, no. 5, Sep. 2019, Art. no. 1950034, doi: 10.1142/S0219691319500346.
[53] A. Salama, A. Mokhtar, and M. Tayel, "A triple-layer encryption-based watermarking technique for improving security of medical images," *J. Med. Imag. Health Inf.*, vol. 9, no. 3, pp. 610–619, 2019, doi: 10.1166./jmihi.2019.2571.
[54] P. P. Dang and P. M. Chau, "Image encryption for secure Internet multimedia applications," *IEEE Trans. Consum. Electron.*, vol. 46, no. 3, pp. 395–403, Aug. 2000.
[55] S. Kamil, M. Ayob, Siti, and Z. Ahmad, "Lightweight and optimized multi-layer data hiding using video steganography paper," *Int. J. Adv. Comput. Sci. Appl.*, vol. 9, no. 12, pp. 256–262, 2018.
[56] S. Kamil, M. Ayob, S. N. H. Sheikh Abdullah, and Z. Ahmad, "Challenges in multi-layer data security for video steganography revisited," *Asia–Pacific J. Inf. Technol. Multimedia*, vol. 07, no. 2, pp. 53–62, Dec. 2018.