Computers, Materials & Continua
DOI: 10.32604/cmc.2023.034435
Article

Severity Based Light-Weight Encryption Model for Secure Medical Information System

Firas Abedi[1], Subhi R.M. Zeebaree[2], Zainab Salih Ageed[3], Hayder M.A. Ghanimi[4], Ahmed Alkhayyat[5,*], Mohammed A.M. Sadeeq[6], Sarmad Nozad Mahmood[7], Ali S. Abosinnee[8], Zahraa H. Kareem[9], Ali Hashim Abbas[10], Waleed Khaild Al-Azzawi[11], Mustafa Musa Jaber[12,13] and Mohammed Dauwed[14]

[1]Department of Mathematics, College of Education, Al-Zahraa University for Women, Karbala, Iraq
[2]Energy Eng. Department, Technical College of Engineering, Duhok Polytechnic University, Duhok, Iraq
[3]Computer Science Department, College of Science, Nawroz University, Duhok, Iraq
[4]Biomedical Engineering Department, College of Engineering, University of Warith Al-Anbiyaa, Karbala, Iraq
[5]College of Technical Engineering, The Islamic University, Najaf, Iraq
[6]ITM Department, Technical College of Administration, Duhok Polytechnic University, Duhok, Iraq
[7]Computer Technology Engineering, College of Engineering Technology, Al-Kitab University, Iraq
[8]Altoosi University College, Najaf, Iraq
[9]Department of Medical Instrumentation Techniques Engineering, Al-Mustaqbal University College, Hillah, 51001, Iraq
[10]College of Information Technology, Imam Ja'afar Al-Sadiq University, Al-Muthanna, 66002, Iraq
[11]Department of Medical Instruments Engineering Techniques, Al-Farahidi University, Bagdad, Iraq
[12]Department of Medical Instruments Engineering Techniques, Al-Turath University College, Baghdad, 10021, Iraq
[13]Department of Medical Instruments Engineering Techniques, Al-Farahidi University, Baghdad, 10021, Iraq
[14]Department of Medical Instrumentations Techniques Engineering, Dijlah University College, Baghdad, Iraq
*Corresponding Author: Ahmed Alkhayyat. Email: ahmedalkhayyat85@iunajaf.edu.iq
Received: 16 July 2022; Accepted: 22 September 2022

Abstract: As the amount of medical images transmitted over networks and kept on online servers continues to rise, the need to protect those images digitally is becoming increasingly important. However, due to the massive amounts of multimedia and medical pictures being exchanged, low computational complexity techniques have been developed. Most commonly used algorithms offer very little security and require a great deal of communication, all of which add to the high processing costs associated with using them. First, a deep learning classifier is used to classify records according to the degree of concealment they require. Medical images that aren't needed can be saved by using this method, which cuts down on security costs. Encryption is one of the most effective methods for protecting medical images after this step. Confusion and dispersion are two fundamental encryption processes. A new encryption algorithm for very sensitive data is developed in this study. Picture splitting with image blocks is now developed by using Zigzag patterns, rotation of the image blocks, and random permutation for scrambling the blocks. After that, this research suggests a Region of Interest (ROI) technique based on selective picture encryption. For the first step, we use an active contour picture segmentation to separate the ROI from the Region of Background (ROB).

Permutation and diffusion are then carried out using a Hilbert curve and a Skew Tent map. Once all of the blocks have been encrypted, they are combined to create encrypted images. The investigational analysis is carried out to test the competence of the projected ideal with existing techniques.

Keywords: Deep learning; encryption; medical images; scrambling; security; skew tent map; rotation; zigzag pattern

1 Introduction

Embedded electronic devices, Radio Frequency Identification (RFID), tags, sensors, software, and actuators are all used in the Internet of Things (IoT), which connects physical goods (things) to the Internet and exchanges large volumes of data with other devices. The implementation of this technology results in better, more reliable, and safer physical infrastructures [1,2]. Examples of physical infrastructure include buildings (such as residences, schools, and workplaces), utility networks (such as power lines, gas pipelines, and waterways), transportation networks (such as roads and rail lines), vehicles (such as cars and trains), waste management systems (such as trucks and garbage trucks), industrial control systems (such as air traffic controllers), and healthcare systems (such as hospitals and clinics) [3,4], sensor-based devices and IoT and mobile technologies are combined to gather data and integrate it communication and optimal resource utilization in healthcare systems [5].

Over the last two decades, research into electronic health record (EHR) information security has grown significantly. To safeguard the security of video and audio, an unencrypted channel must be used [6,7]. Redundancy is greater in images than in text, therefore traditional cryptosystems like advanced encryption standard (AES) and data encryption standard (DES) are ineffective because of their high correlation with visuals [8,9]. Although these algorithms are extremely secure, their computing requirements are prohibitive rounds. In today's world, preserving the quality, authenticity, availability, and confidentiality of medical photographs is critical. For this reason, several researchers are working to create an image encryption method that incorporates a wide range of nonlinear systems and transforms, such as Fourier transform [10,11], discrete wavelet transform [12], compressive sensing [13], and chaos [14,15].

New algorithms for protecting medical photos may be explained in this research work. It is necessary to use a more secure permutation (scrambling) strategy to remove the strong association between adjacent pixels in medical imaging. Image splitting, image scrambling, key creation, and diffusion are all part of a new method shown here. To begin, a new picture splitting approach is used to separate the original image into blocks and sub-blocks, respectively. After that comes the skew tent map, which is constructed by using an image as a starting point. Finally, the secret key is used to alter the image's pixel values. Section 2 describes the related works, whereas the projected methodology is mentioned in Section 3. The validation of the projected model with existing techniques is presented in Section 4. Lastly, the conclusion of the research work is provided in Section 5.

2 Related Works

An image encryption cryptosystem based on binary bit plane extraction and multiple chaotic maps (IEC-BPMC) bit-level encryption system proposed by Shafique and colleagues [16] that uses the variation function exclusively on the most noteworthy bitplanes to minimize computation. This is because the most significant bit (MSB) planes contain the vast majority of the data. Gradually reducing the amount of information as we move from the MSB to the least significant bit (LSB)

bit-planes. It was a security breach, even though the author(s) had developed encryption techniques for real-time applications. The IEC-BPMC was breached through the use of a plaintext attack tactic selected by the author. By uniting only four MSB bit-planes, a plain image can be retrieved using bit-plane encryption algorithms with minimal information loss. High levels of security can be achieved using this approach, but the encryption strategy would be lossy, making it unsuitable for applications requiring precise data retrieval. Recently, researchers bring forth a great number of outstanding methods for image encryption [17].

A noise-resistant picture encryption technique was proposed by Shafique et al. [18]. Bit-plane extraction was used to encrypt the image rather than pixel-by-pixel decryption using discrete wavelet transform (DWT) and a cubic logistic map. The proposed work's initial and last sections encrypt the image using its location. DWT is used to encrypt the frequency domain in the middle of the proposed process. Because the frequency domain is sandwiched between the spatial and frequency domains, we dubbed it "sandwich encryption". Using the proposed method, all of an image's pixel values may be recovered, making it lossless. Statistical analyses such as correlation and contrast have been utilized to examine the suggested scheme's performance.

Khashan et al. [19] provides a lightweight approach for the encryption of medical pictures' edge maps. Using an edge detection method, the map's edges are first gathered. To generate a vast key space is then employed as a generator. In this paper, we present a one-time pad approach for encrypting the relevant picture blocks discovered. An appropriate percentage of encrypted image data has been found in the suggested encryption system, as demonstrated by the results of the experiments. Image can be done in a lightweight manner, making the technique suitable for real-time use cases. Our system is also resistant to a wide range of security assaults, as shown by the security study.

Using sparse awareness with a convolutional neural network (CNN), a novel and improvised denoising technique is created to investigate several medical modalities [20]. CNN uses patch construction and dictionary methods to gather data for evaluation and validation purposes. An image assessment quantitative measure such as peak signal to noise ratio (PSNR), structural similarity (SSIM), or mean squared error is used in the suggested framework, which is superior to current approaches in terms of picture quality evaluation (MSE). It also aims to progress the visual quality of the image by speeding up the computation time.

With Hasan et al. [21] efficient and lightweight encryption algorithm the healthcare industry may provide secure image encryption. Two permutation approaches are used in the proposed lightweight encryption method to safeguard medical photos. An evaluation and comparison of the suggested method's security and execution time are made to conventionally encrypted ones. Images from a variety of sources have been utilized to evaluate the suggested algorithm's performance. According to the results of several trials, the optional algorithm for picture cryptosystems is more efficient than the currently used techniques.

3 The Proposed Method

In the first step of the research work, the EHR is identified into sensitive and non-sensitive data using deep learning techniques. Three key metrics are included in the system such as "Identification (IDN)," "Classification (CLF)," and "Securing (SC)". Fig. 1 demonstrates the working flow of the projected model.

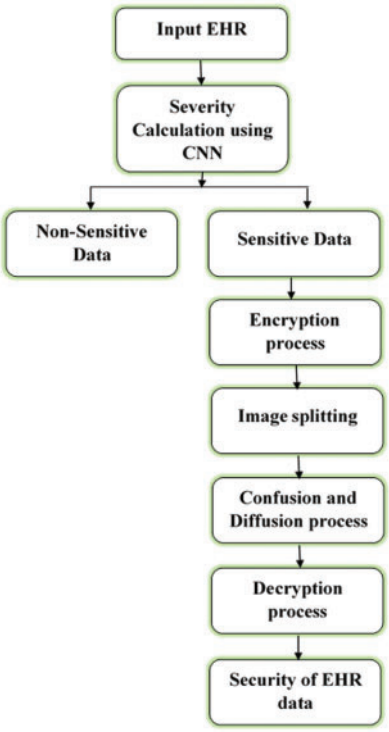

Figure 1: Working flow diagram of the proposed method

3.1 Classification of Data

EHR must be protected under the IDN and CLF definitions. As part of this process, EHR would be identified (so that researchers can distinguish between its criticality and sensitivity). The person who accesses the patient data can emphasize prerequisites to determine the IDN of Health data. There are typically two main classifications, each with its own set of sub-categories. High-level security for confidential information, as well as open/public information.

Classification in EHR determines the level of secrecy for a record according to its nature. It aids in the selection of the EHR that should be protected, which in turn reduces the cost of security. Five separate sub-classifications can be found within these two categories (based on the degree of severity, which is identified by using CNN and is described below). References to each of the five distinct subcategories are provided in the list below. There are five different sorts of keys for each of the following five sub-categories:

i) Sensitive Less Data
   - Doctor's/availability specialist hours and clinic locations are public data.
   - In addition, the patient's name and gender come under the non-sensitive data.

ii) Sensitive Data
   - Medical centers to whom the patient is being referred; dates and times of patient-doctor appointments, etc., are examples of moderately sensitive data.
   - Patients' diagnostic reports come under the example of highly sensitive data.
   - Highly Sensitive Data, such as Genetics, etc.

3.1.1 Classification using CNN

Fig. 2 shows the working flow of EHR classification that depicts the CNN's conv, pooling, and Fully Connected (FC) layers. Using these layers, CNN models with different block sizes may be constructed, as well as the adding or removal of blocks.

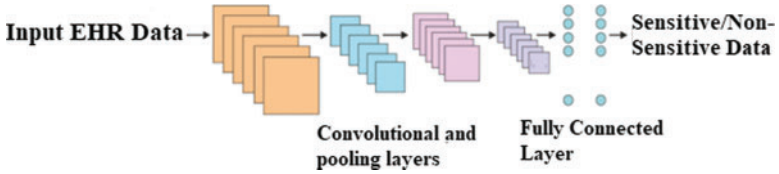

Figure 2: Construction of CNN for severity classification

i) Convolutional Layer

From one neural network to the next, not all pixels are connected to the next layer with weights and biases in the same way. Because of these weights/biases, the image/EHR is partitioned into smaller pieces. Filters or kernels are used to combine smaller regions of an image as input and produce feature maps as output. Feature searches in the input and the convolution layer find the filters as 'features' that are easier to understand. There are fewer parameters needed for convolution because each image feature is traversed by a comparable filter. The convolution layer's hyperparameters are filter count and padding. These hyper settings are fine-tuned for optimal performance according to the input image's size and genre.

ii) Pooling Layer

The pooling layer is used to save processing costs by plummeting the image's spatial dimension and parameter count. Because it performs a predetermined task over input, no parameters are necessary. There are several types of pooling layers, including average, stochastic, and maximum. When the nxn window is moved over the input with a stride value s, the maximum pooling can be applied. The input size is reduced since the maximum value in the n $\times$ n region is taken into consideration for each place. A tiny difference in position can still be discerned thanks to its translational invariance.

iii) FC Layer

Each neuron is related to the current layer, making it a classical neural network (NN). Because of this, the layer has a higher number of parameters. Connected to the output layer, this module is also known as the classifier.

iv) Activation Function

Different CNN architectural models employ various activation functions. Swish are examples of nonlinear activation functions. By using a nonlinear activation function, you can expedite your training. In this study, the ReLUs function was found to be more effective than other functions. By the classification of EHR, the severity of sensitive or non-sensitive data can be identified. After that, encryption can be applied to only sensitive data, which is described below.

3.2 Encryption

Four phases make up our technique for encrypting medical photos. The first thing we do is separate the images. The second step is to create confusion (scrambling). The final stage is a skew tent map-based key creation. The diffusion process is depicted in the final stage.

3.2.1 Plain Image Setting

Blocks of the same size are used to divide the original image into non-overlapping sections. Depending on the block size selected by the user, our algorithm can work with blocks of 16, 32, or 64 bits. After that, each block is either separated into equal-sized sub-blocks or left alone.

3.2.2 Confusion

The process of pixel rearrangement in image results in confusion. In our algorithm, blocks and sub-blocks are confused in the following manner:

- The zigzag pattern can be used on both whole blocks and sub-blocks.
- All blocks and sub-blocks are rotated by 90 degrees.
- An arbitrary random vector r is generated with a length equal to the sum of blocks in the original image.
- The image is scrambled using a random block permutation algorithm based on the vector r.

3.3 Key Generation using ROI-Based Encryption Model

Before studying the region of interest (ROI) process, some preliminaries must be studied, which include the active contour model, Hilbert scan pattern, and skew tent map.

3.3.1 Active Contour Method

The active contour has become the most widely used method for motion tracking and picture segmentation in the previous decade. It is possible to adapt the deformable outlines to the motions and diverse forms of the objects in the scene. Edge-based and region-based active image segmentation contour models are based on force-evolving contours. Using Edge-based active contours are used to find and draw the boundaries of sub-regions. In terms of segmentation, it is extremely. The statistical data about picture intensity within each subset is employed in the region-based active contours tactic. Because it is nearly identical to a regional method [22,23].

3.3.2 Hilbert Scan Pattern

The Hilbert curve is used to scan a $2^m \times 2^m$ an array of points in its entirety. Starting the scan route from the bottom left (LB), top left (LT), and right bottom (RB), of a square grid is an option [24]. A Hilbert curve unique image to produce the scrambled image. The Hilbert Curve's order 0 is empty. The first-order Hilbert curve can be constructed using three straight-line connections and four zero-order curves. It is the same for all higher-order curves.

3.3.3 Skew Tent Map

If you're looking for a simple and dynamic equation that has a complex chaotic behavior then you'll want to check out the skew tent map [25]:

$$X_{n+1} = \begin{cases} \dfrac{X_n}{b}, \; for \; 0 < X_n \leq b \\ \dfrac{1 - X_n}{1 - b}, \; for \; b < X_n < 1 \end{cases} \tag{1}$$

3.3.4 Proposed ROI Technique

The suggested ROI-based enhanced encryption scheme's architecture. The size of a medical image is represented in this study by the ratio of P to Q. The i-th row and j-th column's plain text image pixel value is denoted by $P(i, j)$. The proposed strategy entails three key steps.

First, an active contour method is used to extract the ROI portion of the original image, while in the second step, a Hilbert scan pattern is used to modify the location of every pixel in the ROI portion. To generate a random matrix R, we use a skew tent map as our last tool. Below, more information on each of these processes is identified:

i) Step 1

This ROI component is obtained by multiplying the original medical image by the ROI binary image, which has a size of M by N and then applying active contour-based images.

$$ROI\_Part = Original\ Medical\ image.\ *\ ROI\ binary\ image \tag{2}$$

ii) Step 2

We must design an Nth-order Hilbert curve starting from the right bottom (RB) location. For instance, the third-order Hilbert curve in an 88-square grid, starts from the RB cell.

iii) Step 3

For Sine to work, the following conditions must be met: b = 0.2838 and X0 = 0.73846.

To generate a random vector, iterate Eq. (1) M times over N times.

X's random vector has been updated by a multiple of 1014.

The Modulo 256 procedure is used to generate a new random sum that falls within the range (0–255).

$$\alpha = Modulo(X, 256) \tag{3}$$

A matrix R with XORed bitwise is designed by the pixels in the ROI block.

$$Diff_{Block} = bitxor\,(ROI, R) \tag{4}$$

Finally combining the diffused ROI and ROB blocks to produce an encrypted image in the Diffusion Block.

3.4 Decryption

The plain picture can be recovered using the original key and an inversion of the encryption phases. The following is a breakdown of the decryption procedure:

Scrambled images are generated by performing an exclusive bitwise OR on a secret vector and the key K.

It is possible to rotate both entire blocks and their sub-blocks both in the inverse direction and in the form of zigzags.

4 Result and Discussion

Here, the proposed analysis is presented from a variety of angles in the medical context. In this section, we current the findings of our study on the projected project's performance analysis. Our

research focused entirely on performance analysis criteria and compared them against those of other widely used block ciphers. A performance evaluation of a proposed strategy is shown in Table 1 is the environmental setup. Medical photos can be encrypted using our approach, where the input images are taken from [26] and Levoy [26] provided the grey photos, while [26] provided the colour photographs for this part, as seen in Fig. 3. There are two sets of images and all images are set to the 512 × 512.

Table 1: Setup for experiments

Setup	Description
System	64-bit OS, X-64 Processor
Platform	Visual C++ (Visual Studio Community 2017)
OS	Windows 10
Processor	Intel (R) Core (TM) i7

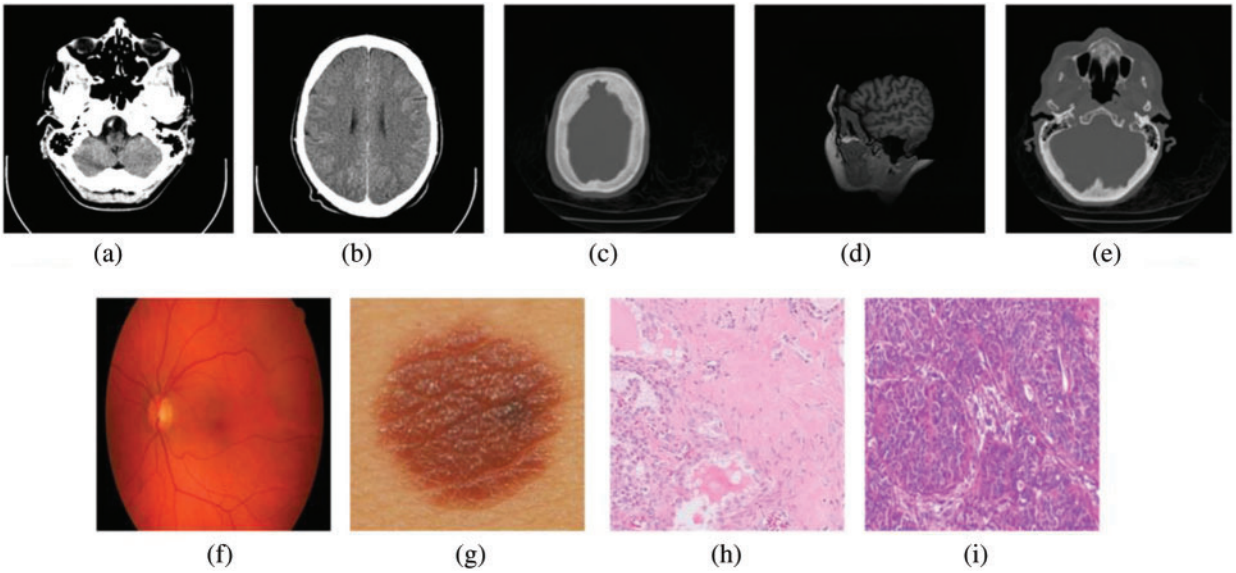

Figure 3: Sample images

The analysis of information entropy, analysis of encryption efficiency (PSNR), analysis of encryption quality (maximum deviation), image histogram, and analysis of differential attack are considered in this work [26]. Table 2 provides the experimental analysis of entropy, a number pixel change rate (NPCR), and the number average changing intensity (UACI) for different testing images. Figs. 4–6 shows the graphical representation of entropy, NPCR, and UACI.

Table 2: Experimental analysis for different testing images

Test image	Entropy	NPCR	UACI
Img1	7.9993	99.6223	33.4406

(Continued)

Table 2: Continued

Test image	Entropy	NPCR	UACI
Img2	7.9994	99.6216	33.4813
Img3	7.9974	99.6002	33.4535
Img4	7.9972	99.6231	33.4903
Img5	7.9977	99.6043	33.4246
Img6	7.9976	99.6135	33.4241
Img7	7.9932	99.6246	33.4920
Img8	7.9968	99.6082	33.4733
Img9	7.9943	99.6273	33.4456

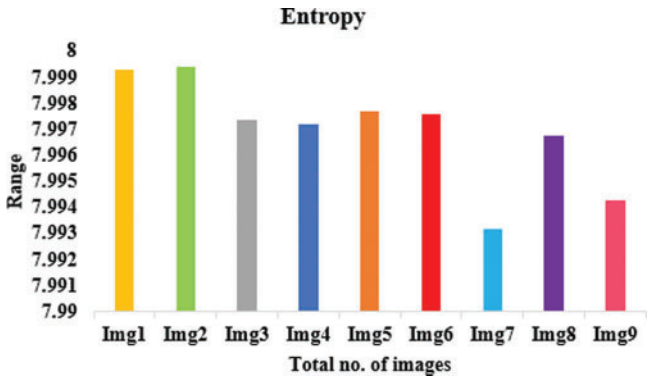

Figure 4: Proposed model in terms of entropy

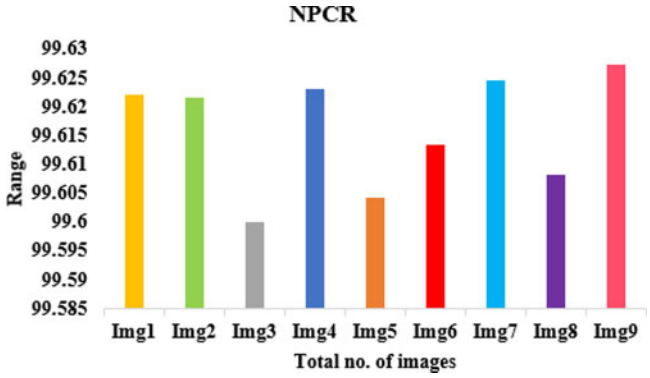

Figure 5: Proposed model in terms of NPCR

Table 2 lists the entropy values of the encrypted images that were used in this experiment and the results of the encryption using the suggested approach. The results show that all of the entropy values are close to 7.99, indicating that the encrypted images are truly random. Table 4 associates the entropy values of our proposed procedure with those of the other algorithms, and as can be observed, ours has a greater entropy value. The results of this experiment demonstrate that the algorithm under consideration ensures the generation of encrypted images with a large degree of randomness. To perform a differential attack, a little alteration is made to the plain image and then both images are

encrypted with the same algorithm. To see if there's a connection between the plain image and the encrypted one, we compare the two. As long as the technique is practical, any little change in the plain image should result in a different encrypted image. These two metrics were used to gauge how well an algorithm performed. Table 2 records the NPCR and UACI values among the two encrypted images to test the proposed algorithm's resistance to differential assaults. All testing photographs met or exceeded NPCR 98% of the time and UACI 33% of the time. Table 3 shows the results of PSNR, histogram deviation, and maximum deviations.

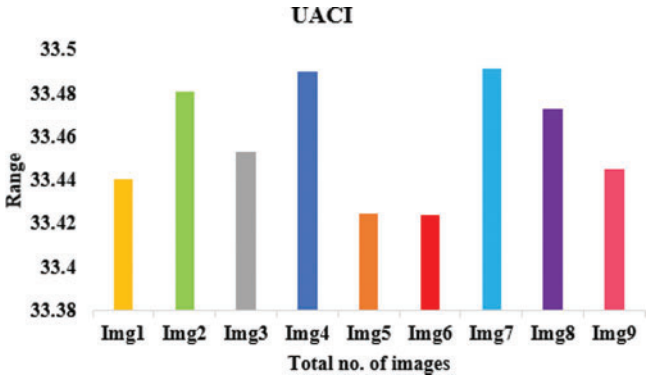

Figure 6: Proposed model in terms of UACI

Table 3: Comparison of various metrics on different images

Test image	PSNR	Maximum deviation	Histogram deviation
Img1	5.1192	33219	0.0254
Img2	5.8811	37093	0.0225
Img3	5.6825	96016	0.0510
Img4	5.2935	95631	0.0476
Img5	6.0865	89861	0.0523
Img6	5.6398	67291	0.0284
Img7	5.4792	83711	0.0735
Img8	5.9836	86721	0.0456
Img9	5.5392	45653	0.0339

The lower PSNR values imply that the original and encrypted images differ significantly. The image's pixel distribution is shown in the histogram. Encrypted images have a flat histogram to prevent any information from being guessed by the attackers. It's also important that the histograms of both encrypted and unencrypted images are not the same. A visual depiction of the suggested model is depicted in Figs. 7–9 using various three metrics. The histograms of the encrypted images generated by our approach are unchanging and distinct from the histograms of the original photos. To ensure that the encrypted image's histogram is uniform, an additional experiment has been conducted. The alteration in pixel values among the plain and encrypted images is used to measure the quality of encryption in the study of maximum deviations (MAXD). If this difference is significant, the encryption procedure is deemed to be efficient. According to our proposed technique, the maximum

deviation values are shown in the Table 3. Encrypted using provided algorithms are completely diverse from the original image, which shows our algorithm's great security presentation.

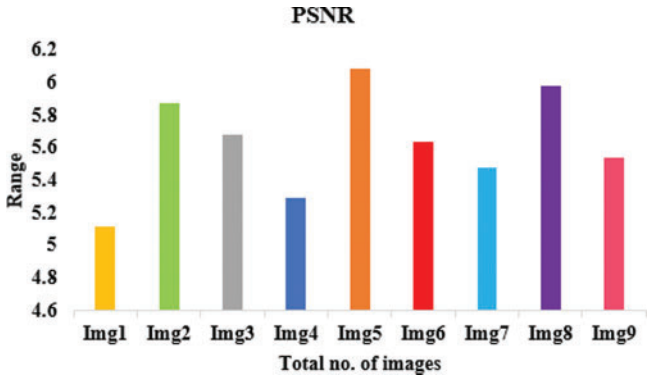

Figure 7: Proposed model in terms of PSNR

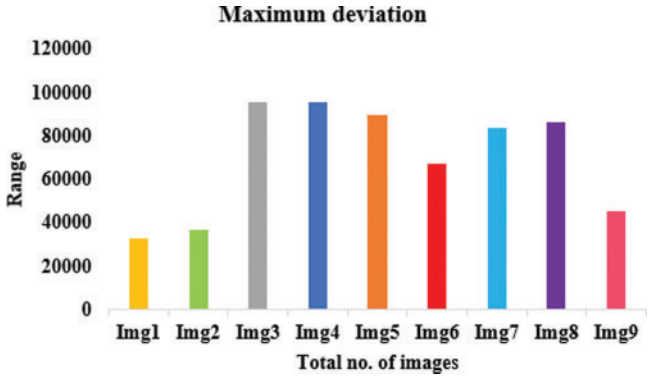

Figure 8: Proposed model in terms of maximum deviation

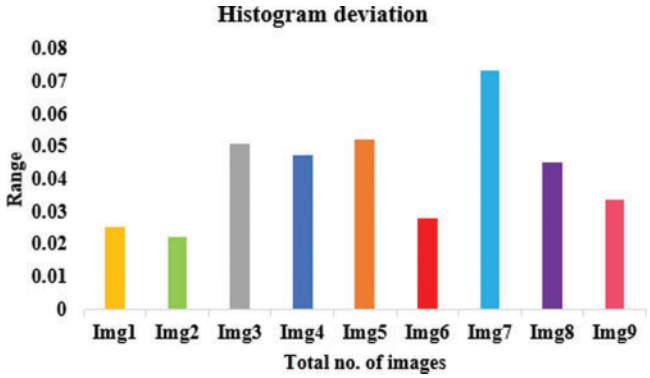

Figure 9: Proposed model in terms of histogram deviation

Table 4 offerings the analysis of the projected model with existing techniques in terms of various parameters.

Table 4: Experimental analysis of the proposed model with existing systems

Test image	PSNR	Maximum deviation	Histogram deviation	Entropy	NPCR	UACI
RC5	7.3413	1,79,372	0.06783	5.5383	98.3242	32.4923
RC6	6.6822	2,45,281	0.07892	5.8932	97.3724	31.6372
Blowfish	8.3422	2,25,272	0.06782	6.6534	98.5382	31.9076
AES	6.6539	1,97,538	0.06371	6.9053	97.2466	32.5729
DES	6.5822	1,80,439	0.06423	7.1102	98.5821	31.5374
3DES	7.7313	2,18,392	0.06381	6.9047	98.3567	31.6482
Proposed	5.6338	1,40,890	0.04224	7.7769	99.6161	33.4583

We also ran our system through its paces on Levoy pictures [26]. Table 4 lists the averages of entropy, NPCR, UACI, PSNR, maximum deviation, and histogram error [26]. All images are 256 256 pixels in size and stored as 8-bit TIF files. The robustness of our approach is demonstrated by the fact that all of the outcomes generated by our suggested algorithm are perfect. The widespread use of colour medical imaging in detecting diseases was made possible by advancements in the modern technology of medical instruments. Encryption of medical images in colour is also possible using the suggested approach. Because each pixel in a colour image contains three values, they typically hold more information than greyscale photos (Red, Green, and Blue). To encrypt colour photos, the image can be alienated into three channels (R, G, and B) and then encrypted individually using the technique. There is a dataset [26] that includes 70 cancer and 100 nevus images to test the suggested technique. JPG photos are used, and the average of all images in each channel is used to resize all images to 512 by 512. As a result, the encryption of colour medical images using our approach is highly effective.

Memory utilization is an important metric for performance analysis. The memory usage of AES, Blowfish, Rivest Cipher (RC)-5, RC6 DES, 3DES, and the suggested is shown in Fig. 10. The "Visual studio analysis tab" was used to aid with this investigation. 11.043 s were spent in kilobytes of memory during the suggested model diagnostic session. The memory consumption for AES was 16.265, Blowfish 12.457, RC5 15.342, and RC6 14.587 while for consumption of kilobytes for Blowfish and RC5.

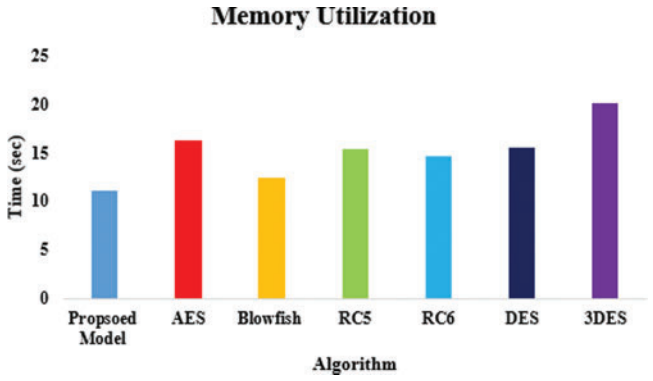

Figure 10: Memory utilization of the proposed model

5 Conclusion

Despite the medical system's possible solutions for health record monitoring, several obstacles limit the system's most important potential. Security and privacy are the most significant roadblocks to the widespread implementation of patient monitoring in healthcare. A significant research hole exists here. An image block and chaos-based encryption technique are designed to encrypt medical images using a CNN model to determine the sensitivity of the data. Using the Hilbert scan and Skew Tent map principles, a selective image cryptography system that encrypts only the ROI portion of a medical image is provided in the confusion process, where a zigzag pattern is utilized. The proposed method may encrypt any medical image securely and efficiently, using little resources and a higher level of protection. A portion of the ROI is retrieved using an active contour approach. This is followed by a Hilbert scan pattern and a skew tent map with predetermined threshold values being used to diffuse the ROI portion of the image. Entropy, histogram, correlation coefficient, memory consumption, and key sensitivity were used to evaluate the projected procedure's image encryption performance. Both grey and colour medical images can be encrypted using the suggested algorithm, according to the results. Comparisons with other recently developed encryption techniques show that the proposed procedure is effective at encrypting medical images in both grey and colour.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] J. Liu, Y. Ma, S. Li, J. Lian and X. Zhang, "A new simple chaotic system and its application in medical image encryption," *Multimedia Tools and Applications*, vol. 77, no. 17, pp. 22787–22808, 2018.

[2] X. Ma, Y. Niu, L. Gu, Y. Wang, Y. Zhao *et al.,* "Understanding adversarial attacks on deep learning based medical image analysis systems," *Pattern Recognition*, vol. 110, no. 2, pp. 1–15, 2021.

[3] D. L. G. Hill, P. G. Batchelor, M. Holden and D. J. Hawkes, "Medical image registration," *Physics in Medicine & Biology*, vol. 46, no. 3, pp. R1–R45, 2001.

[4] D. Jha, P. H. Smedsrud, M. A. Riegler, D. Johansen, T. D. Lange *et al.,* "Resunet++: An advanced architecture for medical image segmentation," in *2019 IEEE Int. Symp. on Multimedia (ISM)*, San Diego, CA, USA, pp. 225–2255, 2019.

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

[6] A. Roy, A. P. Misra and S. Banerjee, "Chaos-based image encryption using vertical-cavity surface-emitting lasers," *Optik*, vol. 176, pp. 119–131, 2019.

[7] J. S. Khan and J. Ahmad, "Chaos based efficient selective image encryption," *Multidimensional Systems and Signal Processing*, vol. 30, no. 2, pp. 943–961, 2019.

[8] R. Riyaldhi, Rojali and A. Kurniawan, "Kurniawan Improvement of advanced encryption standard algorithm with shift row and S. box modification mapping in mix column," *Procedia Computer Science*, vol. 116, no. 2, pp. 401–407, 2017.

[9] B. M. Hennelly and J. T. Sheridan, "Image encryption and the fractional fourier transform," *Optik*, vol. 114, no. 6, pp. 251–265, 2003.

[10] J. B. Lima and L. F. G. Novaes, "Image encryption based on the fractional fourier transform over finite fields," *Signal Processing*, vol. 94, no. February (2), pp. 521–530, 2014.

[11] G. Bhatnagar, Q. M. J. Wu and B. Raman, "Discrete fractional wavelet transform and its application to multiple encryption," *Information Sciences*, vol. 223, no. 6, pp. 297–316, 2013.

[12] S. S. Maniccam and N. G. Bourbakis, "Image and video encryption using SCAN patterns," *Pattern Recognition*, vol. 37, no. 4, pp. 725–737, 2004.
[13] Y. Zhang, L. Y. Zhang, J. Zhou, L. Liu, F. Chen *et al.,* "A review of compressive sensing in information security field," *IEEE Access*, vol. 4, pp. 2507–2519, 2016.
[14] I. Hussain, A. Anees, A. H. AlKhaldi, A. Algarni and M. Aslam, "Construction of chaotic quantum magnets and matrix Lorenz systems S-boxes and their applications," *Chinese Journal of Physics*, vol. 56, no. 4, pp. 1609–1621, 2018.
[15] R. Ge, G. Yang, J. Wu, Y. Chen, G. Coatrieux *et al.,* "A novel chaos based symmetric image encryption using bit-pair level process," *IEEE Access*, vol. 7, pp. 99470–99480, 2019.
[16] A. Shafique and J. Shahid, "Novel image encryption cryptosystem based on binary bit planes extraction and multiple chaotic maps," *The European Physical Journal Plus*, vol. 133, no. 8, pp. 331, 2018.
[17] K. Shankar, D. Taniar, E. Yang and O. Yi, "Secure and optimal secret sharing scheme for color images," *Mathematics*, vol. 9, no. 19, pp. 1–20, 2021.
[18] A. Shafique, J. Ahmed, M. U. Rehman and M. M. Hazzazi, "Noise-resistant image encryption scheme for medical images in the chaos and wavelet domain," *IEEE Access*, vol. 9, pp. 59108–59130, 2021.
[19] Q. Khashan and M. AlShaikh, "Edge-based lightweight selective encryption scheme for digital medical images," *Multimedia Tools and Applications*, vol. 79, no. 35, pp. 26369–26388, 2020.
[20] S. More, J. Singla, S. Verma, Kavita, U. Ghosh *et al.,* "Security assured cnn-based model for reconstruction of medical images on the internet of healthcare things," *IEEE Access*, vol. 8, pp. 126333–126346, 2020.
[21] M. K. Hasan, S. Islam, R. Sulaiman, S. Khan, A. H. A. Hashim *et al.,* "Lightweight encryption technique to enhance medical image security on internet of medical things applications," *IEEE Access*, vol. 9, pp. 47731–47742, 2021.
[22] T. Chan and L. A. Vese, "Active contours without edges," *IEEE Transactions on Image Processing*, vol. 10, no. 2, pp. 266–277, 2001.
[23] K. Ma, J. He and X. Yang, "Learning geodesic active contours for embedding object global information in segmentation CNNs," *IEEE Transactions on Medical Imaging*, vol. 40, no. 1, pp. 93–104, 2021.
[24] T. Sivakumar and R. Venkatesan, "Image encryption based on pixel shuffling and random key stream," *International Journal of Computer and Information Technology*, vol. 3, no. 7, pp. 321–341, 2014.
[25] A. Kadir, A. Hamdulla and W. Q. Guo, "Color image encryption using skew tent map and hyper chaotic system of 6th-order CNN," *Optik*, vol. 125, no. 5, pp. 1671–1675, 2014.
[26] S. T. Kamal, K. M. Hosny, T. M. Elgindy, M. M. Darwish, M. M. Fouda *et al.,* "A new image encryption algorithm for grey and color medical images," *IEEE Access*, vol. 9, no. 5, pp. 37855–37865, 2021.