Blockchain-based Model for Image Encryption in IoT Communication Environment

Esmeralda Kazia[1]

[1] Department of Applied and Computer Sciences, Barleti University, Albania

Email: ict.co@umb.edu.al

Abstract

Nowadays, the internet of things (IoT) has become increasingly common and finds application in various fields, particularly in the health care industry. However, the development and design of IoT data analysis methods face some problems such as lack of adequate training data, resource constraints, centralized framework, security, and privacy. In contrast, the increase in blockchain techniques provides a decentralized framework. It is promoted to remove centralized control and resolve the problem of AI as well as allow secured distribution of data and resources to the diverse nodes of IoT system. This paper devises a new IoT with Blockchain based Secure Image Encryption with Disease Classification model.

Keywords: Internet of Things; Blockchain; Image encryption; Security; Data classification

1. Introduction

Due to increase in the massive number of laptop and personal computer users, and its occurrence in the field of multimedia technology, several sensitive image files are generated. An ever increasing number of possible dangers to abuse the protection of these put away items, a portion of these dangers are unexpected, for example, actual unapproved access, gadget lost or taken [1]. To limit these unlawful activities, security of different levels is required, and to satisfy such security needs, encryption of computerized images is a successful method for forestalling data spillage and disappointing malignant assaults from unapproved parties [2]. Though, advanced images will live on plate in an encoded structure and get too simple for the lawful client. Then again, involving known encryption calculations for scrambling a computerized image that has various nature from text and has qualities like mass information limit, high overt repetitiveness, and high relationship between's pixels [3]. A few stockpiling encryption techniques are accessible for dynamic encryption and decoding. The encryption instrument can be performed on the entire single or different plate parts, or by scrambling individual documents or catalogs. Choosing the fitting stockpiling encryption choice relies upon certain elements, for example, how much data is inside the plate, the required security level, and the sort of encircled dangers. Straightforwardness is one more significant variable to work with a simple to utilize and viable capacity cryptographic arrangement [4]. The greater part of the applied encryption programs that dwell on the application space is completely founded on client by consistently requesting to choose the mystery documents at whatever point the records are utilized [5]. Nonetheless, this additional above caused by the client presents a perilous encryption plot, since the daily schedule of purpose makes it the client is not difficult to neglect to encode the documents and simply fail to remember the various encryption keys.

Security for the most part alludes to insurance from ill-disposed powers [6]. This work centers around safeguarding visual data that permits us to recognize an individual, the time, and the area of the taken photo. Untrusted stages and unapproved clients are thought to be foes. Different perceptual image encryption strategies are projected for safeguarding the visual data of images. Contrasted and full encryption with provable security like homomorphic encryption (HE) [7], they for the most part have a low computational expense and can offer encoded information powerful against different sorts of

Doi: https://doi.org/10.54216/IJWAC.050105
Received: April 19, 2022 Accepted: October 28, 2022

commotion and blunders. Likewise, some of them expect to consider both security and effective pressure so they can be adjusted to distributed storage and organization sharing. Be that as it may, except for a couple of past bits of work, most customary perceptual encryption strategies have never been considered for application to AI calculations [8].

To get the information protection issue of individual information suppliers, the greater part of the current arrangements zeroed in on cryptography and differential security. Those arrangements expected that the information expected for preparing could be acquired safely from different information suppliers to characterize and examine. Issues of proprietorship and information trustworthiness were centered around inconsequentially [9]. Nonetheless, arrangements are invalid because of expected assaults, for most cases, as a general rule. This paper utilizes the BC innovation to construct a solid information sharing patio, which can cover the hole between practical control and run of the mill forecast. As a rule, a common documenting plan expected to allow the circulation of carefully designed records among different people is known as a BC [10]. Examining is empowered on BC for changeless records, which affirms the responsibility for information.

This manuscript devises a new IoT with Blockchain based Secure Image Encryption with Disease Classification model. The proposed model devises optimal double chaotic logistic map with convolutional autoencoder (ODLCM-CAE) model for medical image security with BC technology. The BC is applied to securely transmit the images. Primarily, the DLCM model is used to encrypt the input images and the particle swarm optimization (PSO) algorithm optimally picks up the keys. Next, the convolutional neural network (CNN) model is applied to produce a collection of feature vectors. Finally, CAE approach was applied to allot proper class labels to the input images. The experimental result analysis of the ODLCM-CAE model is tested using a series of test images.

2. Related works

Neelakandan et al. [11] present a new BC with DL assisted secure medical data transmission and diagnosis (BDL-SMDTD) method. The BDL-SMDTD algorithm aimed for securely transfer the medical images and prognose the disease with maximal detection rates. The BDL-SMDTD method inculcates distinct levels of functions like BC, image acquisition, diagnostic procedure, and encryption. Mainly, moth flame optimization (MFO) together with ECC is termed MFO-ECC approach can be utilized to image encryption processes in which the optimum keys of ECC were generated utilizing MFO method. Also, BC technology was used for storing encrypted images. After, the diagnostic processes inculcate SVM-related classification, histogram-related segmentation, and Inception with ResNet-v2-related feature extracting. In [12], the cryptographic pixel value of an image was saved over the BC, assuring the security and privacy of image data. On the basis of the information entropy analysis, the unified averaged changed intensity (UACI), and number of pixels change rate (NPCR), evaluation of the robustness of presented image encrypted method ciphers regarding variance assaults.

Li et al. [13] modelled a secure and verifiable multikey image search (SVMIS) technique in cloud-enabled edge computing. Firstly, the pre-trained CNN method can be used for extracting image feature vectors for enhancing search accurateness. Next, a key distributing protocol was devised for converting the encoded indexes of various owners, and a transformation key list can be built for supporting the multi-key background in edge computing. And then, the learning along with errors related secure KNN technique was employed for encoding feature vectors to enhance security. Khayyat et al. [14] modelled a novel BC-assisted Shark Smell Optimizing together with Hopfield Chaotic NNs (SSO-HCNNs) for secure encrypting in IoT networks. The suggested SSO-HCNN method will make exploitation of a composite Chaotic Map (CM) that can be complied into staged logistic and tent maps to originally processes images and advance the parameters required for Arnold mapping. Moreover, the SSO technique was advanced with maximal PSNR and co-efficient FF for selecting the optimal public and secret keys of mechanism among random numerals. A BC related Chaotic Deep Generative Adversarial Network (GAN) Encrypted method was introduced in [15]. The BCDGE leverages BC technology for protecting personal data and verifies the data authenticity. Then, the Chaotic Deep GAN Encrypted technique employs diffusion, confusion, and substitution principles for encoding the healthcare image.

3. The Proposed Model

In this study, a new IoT with Blockchain based Secure Image Encryption with Disease Classification model has been presented, named ODLCM-CAE model for medical image security with BC technology. The BC is applied to securely transmit the images

Doi: https://doi.org/10.54216/IJWAC.050105
Received: April 19, 2022 Accepted: October 28, 2022

3.1 BC Assisted Data Transmission

The BC is applied to securely transmit the images. In general, a blockchain (BC) is referred to as a collection of blocks [16]. An individual block is made up of four parts: timestamp, information regarding the transaction (Bitcoin, Ethereum), hash value of the preceding, and present blocks. As well, a BC is a typical and shared digital ledger that is employed to record transaction information at different points. As a result, it is no longer possible for the attackers to reclaim the information, meanwhile, every block holds a cryptographic measure of the present block. Here, each transaction is retrieved via a cryptographic hash value that is authenticated by every miner. Decentralized storage is the source in BC, and an enormous amount of information is connected and saved from the preceding to the present blocks via a smart contract code.

3.2 Optimal Image Encryption Approach

Primarily, the DLCM model is used to encrypt the input images. The image encryption of DLCM is comprised of 2 components such as scrambling and confusion process [17]. The abovementioned procedures are shown below:

1) Progress the primary a and b measures for pseudo-random series of approximation technique, and fix approximation attributes $\mu_1 = 3$ of L1 for calculating pseudo-random sequence value X.

2) Decide the unit of pseudo-random sequence value in $(x_i \times 256)$ mod 256, and convert the estimated outcome as binary, and $M \times N$ protracted series value

3) If primary component g_i in G, XOR is implemented according to $X' \oplus g_i$. It is assessed by the following:

$$I'(k) = X'(k) \oplus \{[X'(k) + g_k] mod N\} \oplus I'(k+1) \quad (1)$$

In Eq. (1), k indicates k pixel in the image.

4) Return the pixel sequence obtained from preceding phase, change the real $M \times N$ units to preliminary position, and adjusts the real $M \times (N-1)$ units in the subsequent location. In addition, using Eq. (1), the last obfuscation task is implemented.

The image scrambling method is shown as follows:

1) The I is homogenization and empty vector Y of $M \times N$ size was allotted, and X component was extended for integer space of $(0,\ M \times N)$ according to homogenized of X component, and results are formulated by vector Y.

2) The Y vector is accomplished in preceding stage and encrypted images I'afterward, the conclusion of confusion process and pixel undergo scrambling for I'. Therefore, gray value of $i\text{-}th$ pixel and gray value of $y\text{-}th$ pixel $I'$are switched.

3) The concluding result of scrambling is constraint to a positive and negative order confusion according to 4th and 5th stages; henceforth, encrypted image I'' was accomplished.

As per the preceding scrambling and confusion process, binary chaotic digital encrypted image technique employs confusing process when scrambling for encrypted images. Consequently, the confusing inverse process is calculated by.

$$g_k = \{X'(k) \oplus I'(k) \oplus I'(k-1) - X'(k)\} \quad (2)$$

In this study, the PSO algorithm optimally picks up the keys. A population-based heuristic optimization technique termed PSO is introduced by Kennedy and Eberhart [18]. In searching space, the potential solution for candidate is termed particle P_i with a finite-length string. From the swarm, all the particles make use of their corresponding memory and knowledge in searching for an optimum solution. Fig. 1 demonstrates the flowchart of PSO technique.

Doi: https://doi.org/10.54216/IJWAC.050105
Received: April 19, 2022 Accepted: October 28, 2022

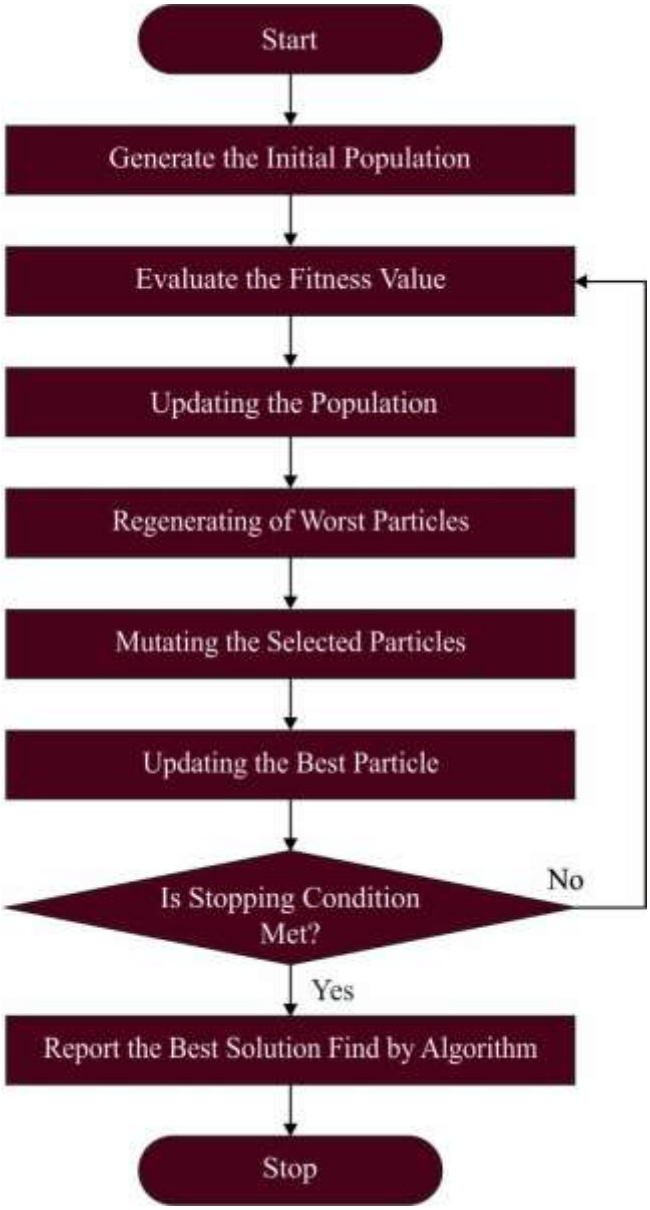

Figure 1: Flowchart of PSO technique

Every particle adapt the direction of searching to determine potential solution according to better experience of flying companions (g_{best}) and optimum prior experience(p_{best}). All the particles move through an n-dimension searching region *S* with a major function

$$f: S \subseteq \Re^n \to \Re \quad (3)$$

All the particles have a location $x_{i,t}$ with a velocity $v_{i,t}$ and fitness function $f(x_{i,t})$. In comparison with $z_2 \in S$ if $f(z_1) < f(z_2)$, a novel location is well-known as $z_1 \in S$. According to the knowledge shared with close particles, particle improves subsequently to discover an optimum solution; it employs knowledge and memory extracted through the swarming procedure. Using the *t* iteration and previous experiencep_{best}, the finest searching location particle *i* have visited. Set of particles is assigned to the close particle to all the particles. The preceding experience of neighbor is named as g_{best}. All the particles encompass a proportion of older velocity. The particle changes the position and velocity with the resulting PSO approach as follows.

$$v_{pd}^{new} = \omega^* v_{pd}^{old} + C_1 * rand_1() * \left(pbest_{pd} - x_{pd}^{old}\right) + C_2 * rand_1() * (gbest_{d_d} - x_{pd}^{old}) \quad (4)$$

$$x_{pd}^{new} = x_{pd}^{old} + v_{pd}^{new} \quad (5)$$

The particle's previous flying velocity is given in most important part of Eq. (4).

Doi: https://doi.org/10.54216/IJWAC.050105
Received: April 19, 2022 Accepted: October 28, 2022

3.3 Data Classification Module

Here, the CNN model is applied to produce a collection of feature vectors. The CNN layers contain: (i) a convolutional input with a group of learnable filters for extracting local features; (ii) a point-wise non-linearity, i.e., the logistic function, for allowing deep structures for learning nonlinear representation of input data; and (iii) the pooling operator that aggregating the statistics of features at neighbouring places [19], for reducing the computational cost (with decreasing the spatial size of images), but offering a local translational invariance from the earlier extracting feature. The final convolution layer is then a fully connected (FC) resultant layer.

The operation executed from a single convolution layer is written as:

$$O^l = poo1_P\big(\sigma(O^{l-1} \star W^l + b)\big) \tag{6}$$

In which O^{l-1} refers to the input feature map to l^{th} layer; $\theta^l = \{W^l, b^l\}$ signifies the group of learnable parameters (weight as well as bias) of layers, σ stands for the point-wise nonlinearity, pool is a sub-sampling function, P denotes the size of pooling region3, and the symbol $\star$ signifies the linear convolutional. Noticeable in the context of CNN, the convolutional is multi-dimensional with all the filters. An input of 1st layer is input data, during this case a multi/hyperspectral images, viz.$O^0 = I$, whereas I $\in \Re^{R^0 \times C^0 \times N_h^0}$ implies the input image, R^0 and C^0 are their width as well as height and N_h^0 signifies the amount of spectral channels (bands). More commonly, the input to succeeding layer l refers to the feature map $0^{l-1} \in \Re^{R^{l-1} \times C^{l-1} \times N_h^{l-1}}$, whereas R^{l-1} and C^{l-1} represents the width as well as height of l^{th} layer's input feature map and N_h^{l-1} stands for the amount of outputs of $(l-1)^{th}$ layer. The CNN structures have an important amount of meta-parameters. The most important ones are probably: (i) the amount of layers; (ii) the count of outputs per layer; (iii) the size of filters, also named receptive field; and (iv) the size and type of spatial pooling.

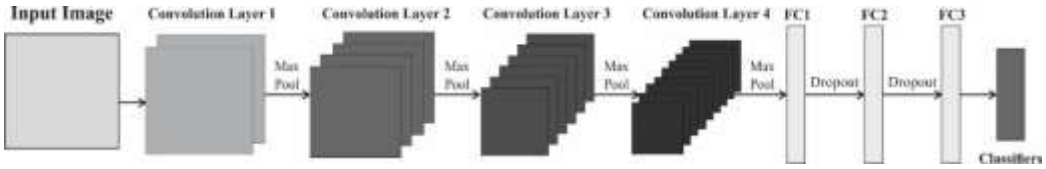

Figure 2: Structure of CNN

Another essential feature is for training such structures. The deep convolutional network is trained in supervised fashion, i.e., using standard backpropagation, or in unsupervised fashion, through greedy layer-wise pre-trained. Fig. 2 depicts the infrastructure of CNN technique. Unsupervised greedy layer-wise pre-trained is for training deep CNN. Supervised processes commonly need a huge count of reliable labeled data that is complex for obtaining from remote sensing classifier issues. Thus, in the case of multi- and hyper-spectral images, it can be desired to utilize an unsupervised learning approach provided the classically some accessible labeled pixels per class.

Finally, CAE model is applied to allot proper class labels to the input images. The AE structure, a variant of encoder-decoder structure which reduces the reconstructed error, was reliably applied for manifold modelling and feature extraction [20]. This network combines an encoder $f(x)$ and a decoder $g(x)$ networks from which the last one is generally an inverse of the preceding one, interconnected through the Z-layer, a bottleneck FC layer using Z neurons. Assume a sample subset of $X = \{x_i \in \mathbb{R}^D\}$ of D dimensional vector, the AE learns lower dimension presentation of the data in Z-layer $z_i \in \mathbb{R}^Z$, viewed as the description of a novel Z-manifold-and minimalizes the reconstructed error among the input of encoder x and the output of decoder $\hat{x} = g(f(x))$. In the study, Mean Squared Error (MSE) is used as reconstructed error among the input images I as well as the reconstruction images at the output $\hat{I}_i = g(\mathrm{f}(I_i))$:

$$\mathcal{L} = \frac{1}{N}\sum_i (I_i - g\big(f(I_i)\big))^2 \tag{7}$$

Now, the output of every neuron at Z-layer, or Z-feature is calculated for the $i\text{-}th$ subjects in the following:

$$z_i = f(I_i) \rightarrow z_i \in \mathbb{R}^z \tag{8}$$

Doi: https://doi.org/10.54216/IJWAC.050105
Received: April 19, 2022 Accepted: October 28, 2022

And is viewed as a coordinate of every subject in the Z-manifold. In the study, they are employed as features in classification and for modelling the topology of the data.

Here, we utilized a convolutionAE, the CAE, specific kind which employs each convolution layer except for the Z-layer. This is a realistic method because convolution layer has several benefits over standard densely interconnected network that encompasses location -invariance because of the integration of filter in the pooling and convolution steps, or small memory requirement owing to shared variable. Also, it enables user to apply the volumetric image sets as input$I = \{I_i \in \mathbb{R}^{64\times64\times64}\}$. Many pooling layers, though, are substituted with novel techniques in CNN including the usage of convolution with stride that offers same outcomes without losing any data.

Standard CAE applies dense layer eventually in the encoder and initially in the decoder for interfacing with the Z-layer.

4. Experimental Validation

In this section, the experimental validation of the ODLCM-CAE model is tested under distinct aspects.

Table 1: PSNR analysis of ODLCM-CAE approach with existing approaches under distinct images

Images	ODLCM-CAE	OPSO	PSO	GWO
Image 1	58.77	51.55	45.21	44.49
Image 2	60.15	53.21	46.85	44.62
Image 3	65.37	58.14	47.2	49.56
Image 4	61.54	55.86	48.17	46.2
Image 5	62.07	55.12	48.82	49.12

Table 1 and Fig. 3 report a comparative peak signal to noise ratio (PSNR) inspection of the ODLCM-CAE model with recent models. The experimental values indicated that the ODLCM-CAE model has achieved increasing PSNR values. In image 1, the ODLCM-CAE technique has provided improved PSNR of 58.77dB but the OPSO, PSO, and GWO models have attained lower PSNR of 51.55dB, 45.21dB, and 44.49dB respectively. Simultaneously, in image 2, the ODLCM-CAE model has offered increased PSNR of 60.15dB while the OPSO, PSO, and GWO models have obtained decreased PSNR of 53.21dB, 46.85dB, and 44.62dB respectively. Eventually, in image 5, the ODLCM-CAE model has provided higher PSNR of 62.07dB where the OPSO, PSO, and GWO models have attained minimal PSNR of 55.12dB, 48.82dB, and 49.12dB respectively.

Doi: https://doi.org/10.54216/IJWAC.050105
Received: April 19, 2022 Accepted: October 28, 2022

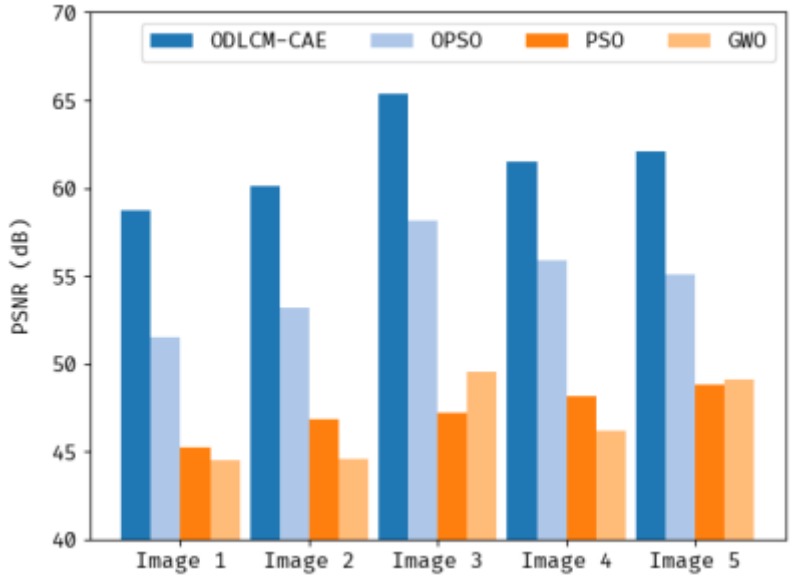

Figure 3: PSNR analysis of ODLCM-CAE approach under distinct images

A comparative study of the ODLCM-CAE model with other models in terms of compressed size (CS) is demonstrated in Table 2 and Fig. 4. The outcomes implied that the ODLCM-CAE technique has shown enhanced results with higher CS values. For instance, with 500 transactions and original size of 620 bytes, the ODLCM-CAE model has gained reduced CR of 258 bytes whereas the HVE-NIS, LZW, and LZMA approaches have attained increased CR of 290, 571, and 539 bytes respectively. In the meantime, with 1000 transactions and original size of 1180 bytes, the ODLCM-CAE model has resulted in decreased CR of 607 bytes whereas the HVE-NIS, LZW, and LZMA methodologies have demonstrated enhanced CR of 646, 1000, and 852 bytes respectively.

Table 2: Compressed size analysis of ODLCM-CAE approach with distinct transactions

Compressed Size (in bytes)					
No. of transactions	**Original**	**ODLCM-CAE**	**HVE-NIS**	**LZW**	**LZMA**
500	620	258	290	571	539
1000	1180	607	646	1000	852
1500	1793	1181	1214	1519	1384
2000	2354	1618	1655	1917	1743
2500	2985	2015	2046	2245	2200

Table 3 and Fig. 5 report a comparative peak signal to noise ratio (CR) analysis of the ODLCM-CAE technique with recent approaches. The experimental values implicit the ODLCM-CAE model has achieved increasing CR values. On image 500, the ODLCM-CAE model has offered higher CR of 2.403 whereas the HAVE-NIS, LZW, and LZMA models have reached lower CR of 2.138, 1.086, and 1.15 correspondingly. At the same time, on image 1000, the ODLCM-CAE model has presented increased CR of 1.944 while the HVE-NIS, LZW, and LZMA systems have obtained decreased CR of 1.827, 1.18, and 1.385 correspondingly. Ultimately, on image 2500, the ODLCM-CAE approach has rendered superior CR of 1.481 whereas the HVE-NIS, LZW, and LZMA models have attained lesser CR of 1.459, 1.33, and 1.357 correspondingly.

Doi: https://doi.org/10.54216/IJWAC.050105
Received: April 19, 2022 Accepted: October 28, 2022

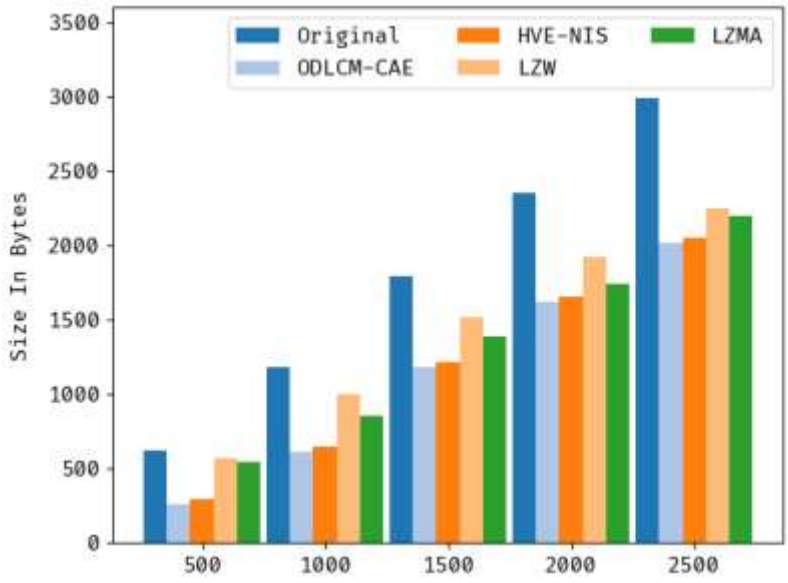

Figure 4: CS analysis of ODLCM-CAE approach with distinct transactions

Table 3: Compressed ratio analysis of ODLCM-CAE approach with distinct transactions

Compression Ratio (CR)				
No. of transactions	**ODLCM-CAE**	**HVE-NIS**	**LZW**	**LZMA**
500	2.403	2.138	1.086	1.15
1000	1.944	1.827	1.18	1.385
1500	1.518	1.477	1.18	1.296
2000	1.455	1.422	1.228	1.351
2500	1.481	1.459	1.33	1.357

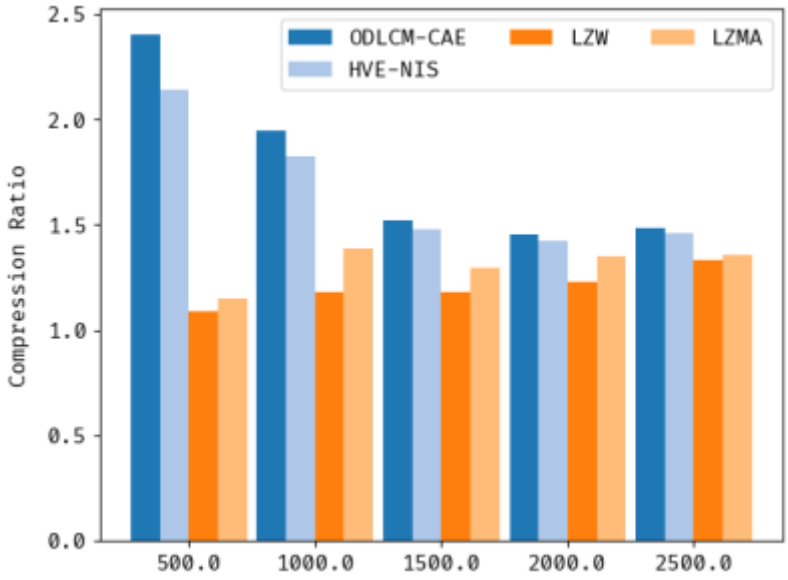

Figure 5: CR analysis of ODLCM-CAE approach with distinct transactions

Table 4 demonstrates the comparison examination of the ODLCM-CAE model with other recent models.

Doi: https://doi.org/10.54216/IJWAC.050105
Received: April 19, 2022 Accepted: October 28, 2022

Table 4: Comparative analysis of ODLCM-CAE approach with recent algorithms

Method	Accuracy	Sensitivity	Specificity
ODLCM-CAE	99.41	97.48	95.37
OPSO-DNN	96.38	95.4	92.92
MLP	83.77	78.4	74.95
RBF	86.46	88.66	55.38
Linear	78.52	90.43	37.48
ANN	88.57	88.94	81.48
KNN	93.41	91.54	85.46
DNN	89.45	83.98	91.53

Fig. 6 depicts a brief $accu_y$ assessment of the ODLCM-CAE technique with existing models. The figure reported that the ODLCM-CAE approach has exhibited effectual performance with the maximum $accu_y$ values. Particularly, it is noticed that the ODLCM-CAE methodology has shown enhanced outcomes with higher $accu_y$ of 99.41% whereas the OPSO-DNN, MLP, RBF, linear, ANN, KNN, and DNN models have reported lower $accu_y$ values of 96.38%, 83.77%, 86.46%, 78.52%, 88.57%, 93.41%, and 89.45% respectively. These results shown the enhanced results of the ODLCM-CAE model.

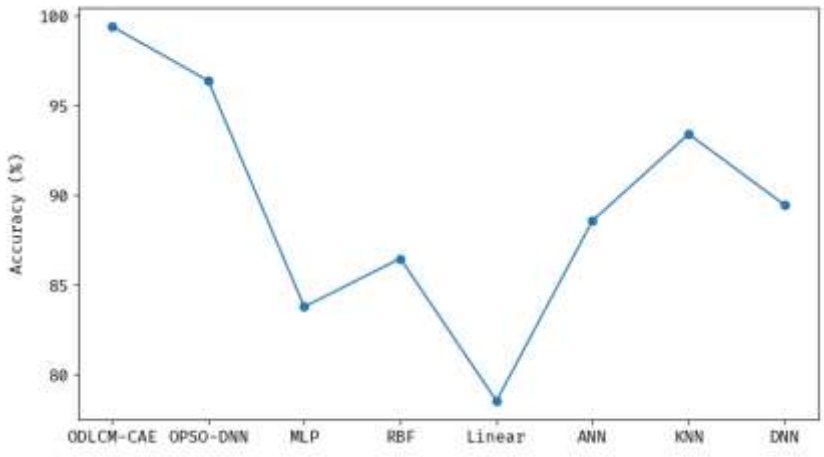

Figure 6: $Accu_y$ Analysis of ODLCM-CAE approach with existing methodologies

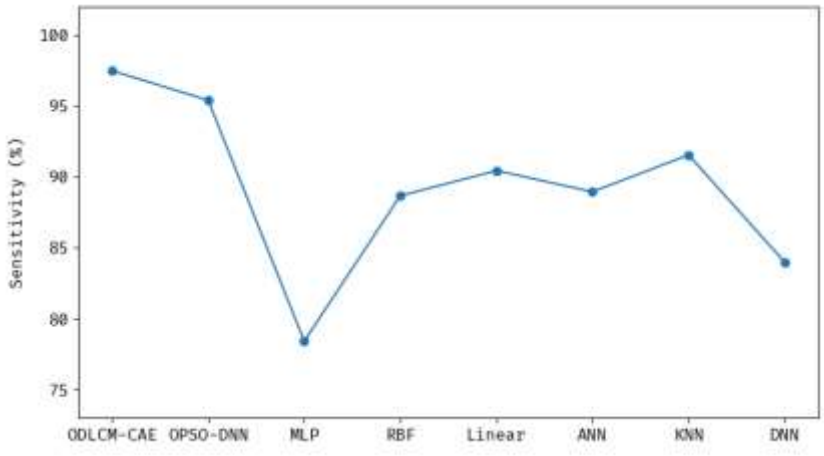

Figure 7: $Sens_y$ Analysis of ODLCM-CAE approach with existing methodologies

Doi: https://doi.org/10.54216/IJWAC.050105
Received: April 19, 2022 Accepted: October 28, 2022

Fig. 7 portrays a brief $sens_y$ assessment of the ODLCM-CAE approach with existing models. The figure reported that the ODLCM-CAE algorithm has shown effectual performance with the maximum $sens_y$ values. In Particular, it is noted that the ODLCM-CAE system has shown improved outcomes with higher $sens_y$of 97.48% whereas the OPSO-DNN, MLP, RBF, linear, ANN, KNN, and DNN models have reported lower $sens_y$ values of 95.4%, 78.4%, 88.66%, 90.43%, 88.94%, 91.54%, and 83.98% correspondingly. These results exhibited the enhanced results of the ODLCM-CAE model.

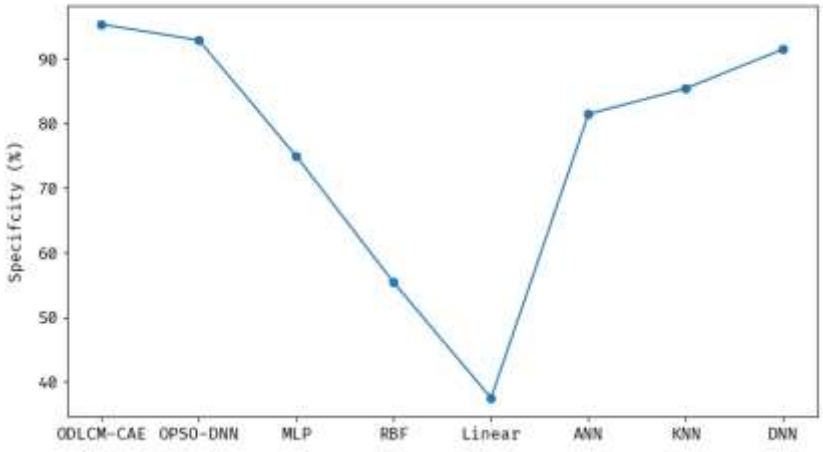

Figure 8: $Spec_y$ Analysis of ODLCM-CAE approach with existing methodologies

Fig. 8 demonstrates a brief $spec_y$ assessment of the ODLCM-CAE approach with existing models. The figure represented the ODLCM-CAE model has displayed effectual performance with the maximum $spec_y$ values. Specifically, it is noted that the ODLCM-CAE system has shown higher outcomes with higher$spec_y$of 95.37% whereas the OPSO-DNN, MLP, RBF, linear, ANN, KNN, and DNN models have reported lower $spec_y$ values of 92.92%, 74.95%, 55.38%, 37.98%, 81.48%, 85.46%, and 91.53% correspondingly. These results revealed the enhanced results of the ODLCM-CAE model.

5. Conclusion

In this study, a new IoT with Blockchain based Secure Image Encryption with Disease Classification model has been presented, named ODLCM-CAE model for medical image security with BC technology. The BC is applied to securely transmit the images. Primarily, the DLCM model is used to encrypt the input images and the PSO algorithm optimally picks up the keys. Next, the CNN model is applied to produce a collection of feature vectors. Finally, CAE approach was applied to allot proper class labels to the input images. The experimental outcome analysis of the ODLCM-CAE model is tested utilizing a series of test images. The experimental outcomes portrayed that the ODLCM-CAE model has showcased enhanced results over other models.

References

[1] Alqaralleh, B.A., Vaiyapuri, T., Parvathy, V.S., Gupta, D., Khanna, A. and Shankar, K., 2021. Blockchain-assisted secure image transmission and diagnosis model on Internet of Medical Things Environment. Personal and ubiquitous computing, pp.1-11.

[2] Mitra, A., Bera, B. and Das, A.K., 2021, May. Design and testbed experiments of public blockchain-based security framework for IoT-enabled drone-assisted wildlife monitoring. In IEEE INFOCOM 2021-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS) (pp. 1-6). IEEE.

[3] Ferrag, M.A. and Shu, L., 2021. The performance evaluation of blockchain-based security and privacy systems for the Internet of Things: A tutorial. IEEE Internet of Things Journal, 8(24), pp.17236-17260.

[4] Rahman, M.S., Khalil, I., Moustafa, N., Kalapaaking, A.P. and Bouras, A., 2021. A blockchain-enabled privacy-preserving verifiable query framework for securing cloud-assisted industrial internet of things systems. IEEE Transactions on Industrial Informatics, 18(7), pp.5007-5017.

[5] Meng, Y. and Li, J., 2021. Data sharing mechanism of sensors and actuators of industrial IoT based on blockchain-assisted identity-based cryptography. Sensors, 21(18), p.6084.

Doi: https://doi.org/10.54216/IJWAC.050105
Received: April 19, 2022 Accepted: October 28, 2022

[6] Unal, D., Hammoudeh, M., Khan, M.A., Abuarqoub, A., Epiphaniou, G. and Hamila, R., 2021. Integration of federated machine learning and blockchain for the provision of secure big data analytics for Internet of Things. Computers & Security, 109, p.102393.
[7] Ferrag, M.A. and Shu, L., 2021. The performance evaluation of blockchain-based security and privacy systems for the Internet of Things: A tutorial. IEEE Internet of Things Journal, 8(24), pp.17236-17260.
[8] Khan, J., Li, J.P., Ahamad, B., Parveen, S., Haq, A.U., Khan, G.A. and Sangaiah, A.K., 2020. SMSH: Secure surveillance mechanism on smart healthcare IoT system with probabilistic image encryption. IEEE Access, 8, pp.15747-15767.
[9] Islam, A. and Shin, S.Y., 2020. A blockchain-based secure healthcare scheme with the assistance of unmanned aerial vehicle in Internet of Things. Computers & Electrical Engineering, 84, p.106627.
[10] Cao, S., Zhang, G., Liu, P., Zhang, X. and Neri, F., 2019. Cloud-assisted secure eHealth systems for tamper-proofing EHR via blockchain. Information Sciences, 485, pp.427-440.
[11] Neelakandan, S., Rene Beulah, J., Prathiba, L., Murthy, G.L.N., Irudaya Raj, E.F. and Arulkumar, N., 2022. Blockchain with deep learning-enabled secure healthcare data transmission and diagnostic model. International Journal of Modeling, Simulation, and Scientific Computing, p.2241006.
[12] Khan, P.W. and Byun, Y., 2020. A blockchain-based secure image encryption scheme for the industrial Internet of Things. Entropy, 22(2), p.175
[13] Li, Y., Ma, J., Miao, Y., Liu, L., Liu, X. and Choo, K.K.R., 2020. Secure and verifiable multikey image search in cloud-assisted edge computing. IEEE Transactions on Industrial Informatics, 17(8), pp.5348-5359
[14] Khayyat, M.M., Khayyat, M.M., Abdel-Khalek, S. and Mansour, R.F., 2022. Blockchain enabled optimal Hopfield Chaotic Neural network based secure encryption technique for industrial internet of things environment. Alexandria Engineering Journal, 61(12), pp.11377-11389
[15] Neela, K.L. and Kavitha, V., 2022. Blockchain based Chaotic Deep GAN Encryption scheme for securing medical images in a cloud environment. Applied Intelligence, pp.1-15
[16] Dinh, T.T.A., Wang, J., Chen, G., Liu, R., Ooi, B.C. and Tan, K.L., 2017, May. Blockbench: A framework for analyzing private blockchains. In Proceedings of the 2017 ACM international conference on management of data (pp. 1085-1100).
[17] Safi, H.W. and Maghari, A.Y., 2017, October. Image encryption using double chaotic logistic map. In 2017 International Conference on Promising Electronic Technologies (ICPET) (pp. 66-70). IEEE.
[18] Sengupta, S., Basak, S. and Peters, R.A., 2018. Particle Swarm Optimization: A survey of historical and recent developments with hybridization perspectives. Machine Learning and Knowledge Extraction, 1(1), pp.157-191.
[19] Romero, A., Gatta, C. and Camps-Valls, G., 2015. Unsupervised deep feature extraction for remote sensing image classification. IEEE Transactions on Geoscience and Remote Sensing, 54(3), pp.1349-1362.
[20] Zhang, C., Yu, J. and Ye, L., 2021. Sparsity and manifold regularized convolutional auto-encoders-based feature learning for fault detection of multivariate processes. Control Engineering Practice, 111, p.104811.

Doi: https://doi.org/10.54216/IJWAC.050105
Received: April 19, 2022 Accepted: October 28, 2022