Nanotechnology Perceptions
ISSN 1660-6795
www.nano-ntp.com

Adversarial Machine Learning Model For Medical Image Classification Using Nature-Inspired Grey Wolf Algorithm

Tasneem Jahan[1] , Dr. Divyarth Rai[2]

[1]Department of CSE, LNCT University, Bhopal,India Tasneemjahan.jahan@gmail.com
ORCID : 0000-0003-3172-3634
[2]Department of CSE LNCT University Bhopal, India divyarthrai@gmail.com

The medical data often undergoes issues of overfitting and convergence due to the presence of heterogeneous features. In addition the transmission of medical data over the web also suffers risk of theft and manipulation. In this paper, a novel approach of secured image transmission through multi classification in adversarial machine learning is proposed. The paper proposes development of an encryption algorithm which also performs compression and image optimization by implementing Grey Wolf Optimization. The grey wolf optimization employs multidimensional visual preprocessing to increase the efficiency of generalization and robustness. This research demonstrates the optimized classification accuracy as well as secured transmission. This algorithm will secure the medical image data and will also reduce the image dimensions by Hyper Spectral Imaging. The result analysis on the image dataset represents significant performance improvement than previous algorithms. The results demonstrate that the proposed medical image encryption model achieves high-security performance, making it an effective and reliable solution for the secure transmission of health data. Following results are achieved : For dataset images, the proposed model yields precision value by 9.084% as compared to the Alex-Net model. The model has achieved an average recall value improvement of 6.85 %. Average improvement was achieved by 8.16% as compared to other model, with accuracy of 97.43 over dataset images.

Keywords : Image Classification, Image Retrieval, secured classification. Adversarial machine learning, Grey Wolf Algorithm.

I.Introduction:

Image Security in the Intelligent Healthcare domain is increasingly popular for Electronic Health Records. The security to a certain extent has been achieved through Hyperspectral Image Classification [1] using CNN with Grey Wolf Optimization algorithm. Further improvement is made through Principal Component analysis [2]. This superpixel-based PCA uses feature extraction for production of Extended Morphological Profiles. The heterogeneous features coupled with varied distributions and characteristics. Hence the adversarial machine learning techniques could be beneficial for addressing stimulating aspects of EHR data [4]. It yields good performance in terms of sparsity and heterogeneous features. The adversarial machine learning and deep learning open avenues for medical image analysis with better accuracy and robustness [5]. The medical images travel across through number of networks. The secured image processing is required to ensure and analyze image encryption [6]. The chaotic map approach [7] has effective complexity and better image security for images with varied size.

The proposed work is an extension to the image security in medical domain using Advanced Encryption Standard [8] and integrating Grey Wolf Optimization. The approach is based on developing a Deep Learning Model to efficiently improve image retrieval. Feature extraction and dimensionality reduction is achieved using genetic algorithm. Image retrieval is accomplished by Cluster based sampling methods [9]. Under this method, image retrieval in healthcare and medical diagnosis on images with localised intervals of grey values is done.

The image encryption model is based on a CNN (Convolutional Neural Network), which modify the order of pixels position thus pixel value also changes. The chaotic system for image encryption [10] has cryptography systems with random sequences which generate chaotic mapping. This prevents the information contained in the content of image.

The approach could be utilized in intelligent healthcare [16]. This will help to upgrade conventional healthcare systems by enhancing their effectiveness through machine learning.

II.Related Work:

In [1], the hyperspectral image (HI) classification is achieved over pixel vectors. In HI classification, optimal parameters of CNN reduces the loss to provide the most accurate results possible.

Secured Image classification has been employed [17] using the multilevel discrete wavelet transform (DWT) for image decomposition. This yielded good results in preserving confidentially of image transmission and its privacy.

Greater security in network transmission of image a deep neural network model is developed [18]. It extracts features by sample training. This algorithm is designed to encrypt images while maintaining compatibility with the retrieval system, enabling the secure retrieval of ciphertext images. Experimental results conducted on multiple authoritative datasets demonstrate that the proposed approach not only guarantees the secure handling of encrypted images but also significantly enhances retrieval efficiency.

In[19], the authors developed a model for Multi-level security which ensures privacy by combining the Huffman code with certain cryptographic techniques, such as symmetric encryption algorithms.

III.Background :

The essence of proposed work lies in secured image retrieval of medical images. The encryption strategy is based on chaotic system [11]. It performs downsampling and image compression. The image reconstruction is performed by a CNN model. The network bandwidth is efficiently utilized by first performing encryption followed by compression.

The embeddings in image with unequal dimensions are based on asymmetric hashing [12]. It is also crucial to address challenges in the image data which involves its sparsity, heterogeneous nature [20], fluctuating sequence lengths of time dependent features. It is also important to protect these important features from adversarial attacks [13].

EHR-Safe is based on a two-stage model that consists of sequential encoder-decoder networks and generative adversarial networks [21]. Our innovations focus on the key challenging aspects of real-world EHR data: heterogeneity, sparsity, coexistence of numerical and categorical features with distinct characteristics, and time-varying features with highly-varying sequence lengths.

The optimization is achieved through Grey Wolf Optimization technique to refine the searching mechanism [14]. It also boosts the convergence momentum of chaotic algorithm.

Medical images are a crucial health record in decision making and data analytics modelling. They target predictions for diagnosis of ailment, fitness tracking, and drug response. [3]. The algorithm also targets privacy preservation for secured transmission.

IV.Proposed Method

The basis of the proposed work is based on developing a machine learning model using Convolutional Neural Networks (CNNs). The enhancement to the model is added by Grey Wolf Optimization Technique for hyperparameter optimization. enhanced by a hyperparameter optimization technique called Grey Wolf Optimizer (GWO) [1]. Under this proposed method, the hyperspectral medical images are characterized by the feature of high spectral resolution. This helps to provide more in-depth information about the image. The nature of this optimization algorithm is inspired by grey wolves' behaviour of hunting. Utilizing this approach, the proposed CNN will search for optimal values of hyperparameters, to further improve the classification accuracy and reducing bias-variance error.

The proposed method improves the security and robustness of the encryption and decryption processes by incorporating a key extension into the key schedule of the Advanced Encryption Standard (AES) algorithm.

1. **Visual Pre-Processing** : Read a image means making a matrix of the same dimension of the image then fill the matrix correspond to the pixel value of the image at the cell in the matrix.

In this step image is resize in fix dimension. As different image have different dimension. So conversion of each is done in this step. This can be understand as if one image have an dimension of the 30X30 and other image has the dimension of 29X28 then it need to resize it either in 30X30, so that it matrix operation can be easily perform on both matrix [22]. One more work is to convert all images in gray format. A different image has RGB, HSV, etc. format so working on single format is required [23].

2. Feature Extraction

Histogram Feature: In this step image vector obtained after pre-processing is used where histogram of the image is find at one bins. This can be understand as let scale of color in fig. 2 is 1 to 10, than count of each pixel value is done in the image. So as per above S vector H_i=[0, 0, 0, 4, 3, 5, 2, 1 2, 0] where H represent the color pixel value count and i represent the position in the H matrix with color value.

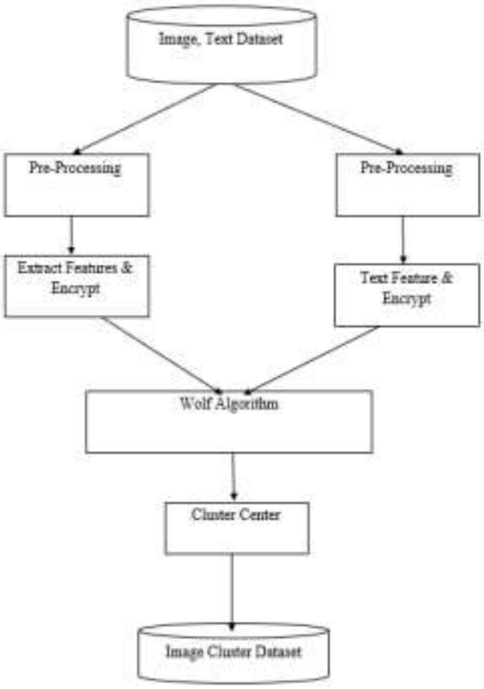


Fig 1. Block Diagram of Proposed Work

3. AES

Extracted feature visual and text terms will be encrypted using AES.. In this encryption algorithm four stages are perform in each round. These steps are common in both encryption as well as decryption algorithm where decryption algorithm is inverse of the encryption one. Now common step for all kind of data is that each data need to be convert into 16 element set of input. Here each input need to be in integer data type. So round consist of following four stages.

- Byte substitution (1 S-box used on every byte) Convert this to mathematical equation
- Shift rows (permute bytes between groups/columns)

- Mix columns (subs using matrix multiply of groups)
- Add round key (XOR state with key material)

A. Byte Substitution : Let the state matrix be -

S=[si,j]S = [s_{i,j}]S=[si,j], where i,j∈{0,1,2,3}i, j \in \{0, 1, 2, 3\}i,j∈{0,1,2,3}. Each byte si,js_{i,j}si,j is substituted as:

Si,j′=S-box(si,j)S'_{i,j} = {S-box}(s_{i,j})Si,j′=S-box(si,j)

where S-box(·)\{S-box}(\cdot)S-box(·) is the substitution function applied to each byte.

B. Shift Rows:

Row 0: Row 1: Row 2: Row 3: S0,j′′=S0,j′(noshift)S1,j′′=S1,(j+1)mod4′S2,j′′=S2,(j+2)mod4′ S3,j′′=S3,(j+3)mod4′

C. Mix Columns:

Each column of the state matrix is treated as a 4-element vector and multiplied by a fixed 4×44 \times 44×4 matrix over the finite field GF(28)GF(2^8)GF(28).

$$Cj = [S0, j'', S1, j'', S2, j'', S3, j'']T$$

M= $$\begin{bmatrix} 02\ 03\ 01\ 01 \\ 01\ 02\ 03\ 01 \\ 01\ 01\ 02\ 03 \\ 01\ 01\ 01\ 02 \end{bmatrix}$$

D. Add Round Key

Si,j(r)=Si,j′′′⊕ki,j

Where, ⊕ represents bitwise XOR.

For round r, the transformation of the state matrix SSS can be summarized as:

S(r)=AddRoundKey(MixColumns(ShiftRows(SubBytes(S(r−1)))),K(r))

4. Generate Wolfs

Wolfs are group of chromosome and a chromosome is possible solution cluster center. So a wolf is a vector of number of elements, where each element is number of image cluster center representative. So if w number of wolfs generate then WP is wolf population matrix having wxn dimension. Selection of n number of image in vector done by random value generator function Gaussian.

The Grey Wolf Algorithm functions in the following manner-

1. Initializes the image pixels to random positions in the search space
2. Iterate through all the positions through a maximum number of pixels.
3. Update the feature maps as per best positions.
4. Calculate new positions for each pixel relative to adaptive parameters
5. Apply chaotic map to all features maps and identify the global optimal with respect to a curve function
6. The best solution is updated in every iteration

WP←Generate_Wolf(w, n)

Representation of population matrix

WP_1	WP_7	WP_3	WP_9	WP_4
WP_{10}	WP_{12}	WP_4	WP_{19}	WP_2
WP_{16}	WP_7	WP_{19}	WP_1	WP_4
WP_9	WP_1	WP_7	WP_3	WP_{12}
WP_2	WP_4	WP_3	WP_{12}	WP_{16}

5. Fitness Function

Each wolf were rank as per hunting skill and assign in sub group. So evaluation of hunting skill done by fitness value. Wolf element vector pass in the fitness function for finding the

Euclidian distance function. This distance summation value is hunting parameter in the work to rank or assign a wolf in sub category of alpha, beta, delta and gamma.

1.Let Xi represent the position of the **i-th** pixel in the **d-dimensional** search space: $Xi=[xi^1,xi^2,\ldots\ldots\ldots\ldots,x_i^d]$,

$i=1,2,\ldots,N$

where N is the total number of pixels.

6. Fitness Evaluation

Evaluate the fitness of each pixel (solution) based on a specific **feature extraction criterion** (e.g., contrast, texture, etc.). The fitness function $f(X_i)$ quantifies how good a pixel's position is.

Identify Alpha (α), Beta (β), and Delta (δ) Wolves as:
Rank the pixels based on their fitness and identify the three best solutions:

$\alpha=\min(f(X_i))$,
$\beta=$2nd best,
$\delta=$3rd best

Distance Calculation:

The distance between the current pixel and each of the three leaders is:

$D_\alpha=|C_1\cdot X_\alpha-X_i|$
$D_\beta=|C_2\cdot X_\beta-X_i|$
$D_\delta=|C_3\cdot X_\delta-X_i|$

Position Update:

The new position of pixel XiX_iXi is the average influence of the three best solutions:

$Xi(t+1)= (X1+X2+X3)/3$

Global Best Update

After each iteration, update the global best position:

$X^*=\min(f(X_i))$for all i

Complete Equation for Position Update in GWO:

$X_i(t+1)=(X_\alpha-A_1\cdot|C_1\cdot X_\alpha-X_i|)+(X_\beta-A_2\cdot|C_2\cdot X_\beta-X_i|)+(X_\delta-A_3\cdot|C_3\cdot X_\delta-X_i|) / 3$

7 .Crossover

Genetic algorithm success depends on change of chromosomes, hence as per X values number of random position value of wolfs were modified. This operation was not done in alpha wolf. In this step each wolf X number of positions were modified randomly as per alpha wolf element set. These wolf were further test for hunting skill and compared its hunting skill with parent wolf if child wolf has better values then remove parent otherwise parent will continue. After this step if maximum iteration steps occur then jump to filter feature block otherwise evaluate fitness value of each wolf.

If new wolf fitness value is better than parent wolf then replace parent with new wolf in the population this is population updation in the work. After this population update perform same operation with other wolf in beta, delta and omega category. Once all wolf get update then check for iteration count if count is less than max iteration then jump to fitness value evaluation of updated population.

So let X is 1 and alpha wolf is m=2 then crossover operation occur as:

Other	WP$_1$	WP$_7$	WP$_3$	WP$_9$	WP$_4$
Alpha	WP$_{10}$	WP$_{12}$	WP$_4$	WP$_{19}$	WP$_2$
New	WP$_1$	WP$_7$	WP$_3$	WP$_{19}$	WP$_4$

New wolf fitness value is better than parent wolf then replace parent with new wolf in the population this is population updation in the work. After this population update perform same operation with other wolf in beta, delta and omega category. Once all wolf get update then check for iteration count if count is less than max iteration then jump to fitness value evaluation of updated population.

Update Population

After t number of iteration steps (fitness function, wolf position update, crossover) final wolf population pas through fitness function and best fitted wolf is consider as alpha wolf. This wolf cluster center are used to cluster image dataset.

V.Data Set

In order to conduct the experiment an real dataset obtain from http://wang.ist.psu.edu/docs/home.shtml which is a collection of images from different category are utilize. As images are of different format so first it is necessary to make it in readable format for experiment tool MATLAB.

VI. Experiment Setup:

Software and Hardware Requirement

This section presents the experimental evaluation of the proposed image retrieval technique. All algorithms and utility measures were implemented using the MATLAB tool. The tests were performed on 2.27 GHz Intel Core i3 machine, equipped with 4 GB of RAM, and running under Windows 7 Professional.

VII. Result

The histogram of the original image is demonstrated in Fig. 2. Further the average execution time of wolf algorithm is shown in Fig. 3.

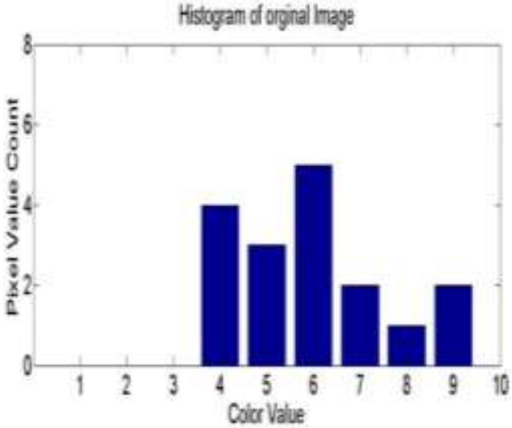


Fig. 2 Histogram of the original image.

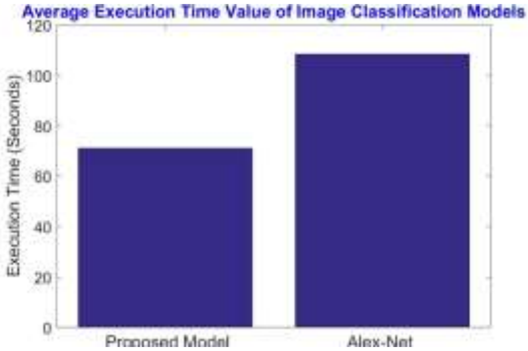
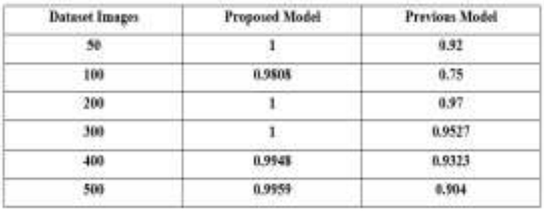


Fig. 3 Average Execution Time

VIII.Analysis

Precision values of image classification models in table 1 shows that proposed model has increases the correct detection of proposed model. It was found that use of wolf algorithm for image feature optimization has increases the learning of the model. Further Fig. 1 shows that with increase in testing data precision value of proposed model is always above 0.96. Table 1 shows that that proposed model has increases the precision value by 9.084% as compared Alex-Net model.

Table 1. Precision value based comparison of models.



Dataset Images	Proposed Model	Previous Model
50	1	0.92
100	0.9808	0.75
200	1	0.97
300	1	0.9527
400	0.9948	0.9323
500	0.9959	0.904

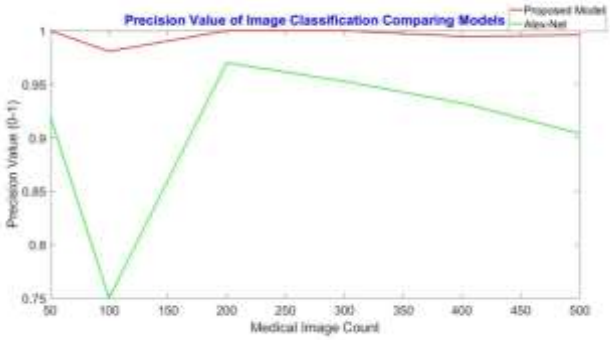
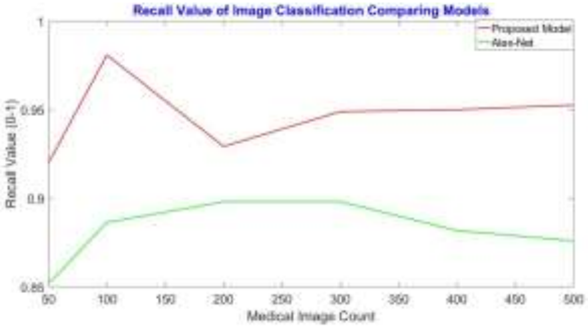


Table 2 shows recall values of image classification, it was found that encryption algorithm has not affect the classification accuracy. Further fig. 2 shows that with increase in testing images recall values improves where model has achieved an average recall value improvement of 6.85 % as compared to Alex-Net. Paper has found that genetic algorithm and histogram feature has work efficiently in classification of images.



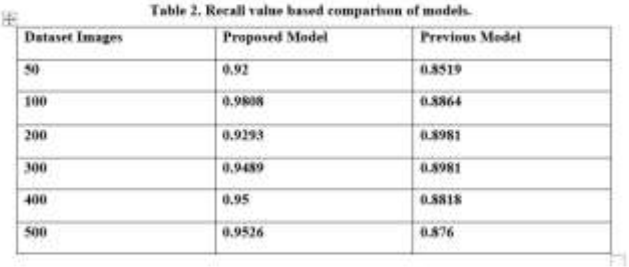


Table 2. Recall value based comparison of models.

Dataset Images	Proposed Model	Previous Model
50	0.92	0.8519
100	0.9808	0.8864
200	0.9293	0.8981
300	0.9489	0.8981
400	0.95	0.8818
500	0.9526	0.876

IX.Conclusion

In this paper, the proposed algorithm showed precision value by 9.084% as compared Alex-Net model. The detection accuracy of image class is high in proposed model. Use of wolf based selected image features has increases the learning of model and reduces the useless data. The proposed model has improved classification in all set of testing image dataset sizes. Average improvement was achieved by 8.16% as compared to other model. The Grey Wolf optimizer offered improved convergence speed by escaping local minima. The optimization process selects the chaotic map with most appropriate features and thus reduces the time for global convergence. Improving the ability to escape local optima, which is crucial for tackling complex optimization problems with multiple local minima or maxima is handled with robustness by this algorithm, and it also reduces the computational burden on the model. The other benefits are enhanced performance for high dimensional medical images.

X. Future Work

The proposed work can further be extended to identify the effect of multiple combinations of chaotic maps and dynamic selection of feature maps to optimize the model further. This could be a potential area for improving convergence and performance of the model. Also, the Grey wolf algorithm could be integrated with Local search algorithms employing meta heuristics search techniques to further enhance the applicability of the model.

References

1. Ladi, S.K., Panda, G.K., Dash, R. et al. A Novel Grey Wolf Optimisation based CNN Classifier for Hyperspectral Image classification. Multimed Tools Appl **81**, 28207–28230 (2022). https://doi.org/10.1007/s11042-022-12628-2

2. B. Asghari Beirami and M. Mokhtarzade, "Band Grouping SuperPCA for Feature Extraction and Extended Morphological Profile Production From Hyperspectral Images," in IEEE Geoscience and Remote Sensing Letters, vol. 17, no. 11, pp. 1953-1957, Nov. 2020, doi: 10.1109/LGRS.2019.2958833.
3. Yoon, J., Mizrahi, M., Ghalaty, N.F. et al. EHR-Safe: generating high-fidelity and privacy-preserving synthetic electronic health records. npj Digit. Med. 6, 141 (2023). https://doi.org/10.1038/s41746-023-00888-7, SPRINGER 2024

4.T. Dhar, N. Dey, S. Borra and R. S. Sherratt, "Challenges of Deep Learning in Medical Image Analysis—Improving Explainability and Trust," in IEEE Transactions on Technology and Society, vol. 4, no. 1, pp. 68-75, March 2023, doi: 10.1109/TTS.2023.3234203.

6. Q. Wang, "Application of computer image processing technology in clinical medicine," 2022 3rd International Conference on Education, Knowledge and Information Management (ICEKIM), Harbin, China, IEEE, 2022, pp. 1120-1123, doi: 10.1109/ICEKIM55072.2022.00243.

7. U. Hombal, D. R. B, A. Shinde and M. N. Chavan, "Modified Chaotic Map Approach for Medical Record Security," 2024 2nd International Conference on Networking, Embedded and Wireless Systems (ICNEWS), Bangalore, India, IEEE, 2024, pp. 1-6, doi: 10.1109/ICNEWS60873.2024.10730948.

8. A. C. H. Chen, "Evaluation of Advanced Encryption Standard Algorithms for Image Encryption," 2024 International Conference on Smart Systems for applications in Electrical Sciences (ICSSES), Tumakuru, India, 2024, pp. 1-6, doi: 10.1109/ICSSES62373.2024.10561385, IEEE, 2024

9. A. H. Ali, E. K. Gbashi, H. Alaskar and A. J. Hussain, "A Lightweight Image Encryption Algorithm Based on Secure Key Generation," in IEEE Access, vol. 12, pp. 95871-95883, 2024, doi: 10.1109/ACCESS.2024.3414334, IEEE 2024

10. Q. Zhang, Y. Yan, Y. Lin and Y. Li, "Image Security Retrieval Based on Chaotic Algorithm and Deep Learning," in IEEE Access, vol. 10, pp. 67210-67218, 2022, doi: 10.1109/ACCESS.2022.3185421.

9. Yixin Chen, J. Z. Wang and R. Krovetz, "CLUE: cluster-based retrieval of images by unsupervised learning," in IEEE Transactions on Image Processing, vol. 14, no. 8, pp. 1187-1201, Aug. 2005, doi: 10.1109/TIP.2005.849770.

10. Priyanka, Singh, A.K. A survey of image encryption for healthcare applications. Evol. Intel. 16, 801–818 (2023). https://doi.org/10.1007/s12065-021-00683, Springer

11. Priyanka, N. Baranwal, K.N. Singh, A.K. Singh, Using chaos to encrypt images with reconstruction through deep learning model for smart healthcare, Computers and Electrical Engineering, Volume 114, 2024, Elsevier

12. Zhan Yang, Osolo Ian Raymond, Wenti Huang, Zhifang Liao, Lei Zhu, Jun Long, Scalable deep asymmetric hashing via unequal-dimensional embeddings for image similarity search, Neurocomputing, Volume 412, 2020, Elsevier

13. Yoon, J., Mizrahi, M., Ghalaty, N.F. et al. EHR-Safe: generating high-fidelity and privacy-preserving synthetic electronic health records. npj Digit. Med. 6, 141 (2023). https://doi.org/10.1038/s41746-023-00888-7

14. Khan, H., Hazzazi, M.M., Jamal, S.S. et al. New color image encryption technique based on three-dimensional logistic map and Grey wolf optimization based generated substitution boxes. Multimed Tools Appl 82, 6943–6964 (2023), Springer

15. Mirjalili, S., Mirjalili, S. M., & Lewis, A. (2014). Grey Wolf Optimizer. Advances in Engineering Software, 69, 46-61. DOI: 10.1016/j.advengsoft.2013.12.007 :

16. Jahan, T. (2021). Machine Learning with IoT and Big Data in Healthcare. In: Bhatia, S., Dubey, A.K., Chhikara, R., Chaudhary, P., Kumar, A. (eds) Intelligent Healthcare. EAI/Springer Innovations in Communication and Computing. Springer, Cham. https://doi.org/10.1007/978-3-030-67051-1_5

17. S. Kaliswaran and M. Y. M. Parvees, "Modified Grey Wolf Optimization based Advanced Encryption Standard based Cryptographic Technique for Digital Images," 2021 6th International Conference on Inventive Computation Technologies (ICICT), Coimbatore, India, 2021, pp. 78-83, doi: 10.1109/ICICT50816.2021.9358786.

18. Q. Zhang, Y. Yan, Y. Lin and Y. Li, "Image Security Retrieval Based on Chaotic Algorithm and Deep Learning," in IEEE Access, vol. 10, pp. 67210-67218, 2022, doi: 10.1109/ACCESS.2022.3185421.

19. Ajagbe, S.A., Adeniji, O.D., Olayiwola, A.A. et al. Advanced Encryption Standard (AES)-Based Text Encryption for Near Field Communication (NFC) Using Huffman Compression. SN COMPUT. SCI. 5, 156 (2024). https://doi.org/10.1007/s42979-023-02486-6

20. M. Samiullah, W. Aslam, M. A. Khan, H. M. Alshahrani, H. Mahgoub, A. M. Abdullah, M. I. Ullah, and C.-M. Chen, Rating of modern color image cryptography: A next-generation computing perspective, Wireless Commun. Mobile Comput., vol. 2022, pp. 120, Mar. 2022.

21. Mohammed, Z.A., Gheni, H.Q., Hussein, Z.J. and Al-Qurabat, A.K.M. 2024. Advancing Cloud Image Security via AES Algorithm Enhancement Techniques. Engineering, Technology & Applied Science Research. 14, 1 (Feb. 2024), 12694–12701. DOI:https://doi.org/10.48084/etasr.6601.

22. Sun, F., Lv, Z. A secure image encryption based on spatial surface chaotic system and AES algorithm. Multimed Tools Appl 81, 3959–3979 (2022). https://doi.org/10.1007/s11042-021-11690-6

23. Hadj Brahim, A., Ali Pacha, A. & Hadj Said, N. An image encryption scheme based on a modified AES algorithm by using a variable S-box. J Opt 53, 1170–1185 (2024). https://doi.org/10.1007/s12596-023-01232-8

Declaration :

1.The Authors state that no external funding is involved in the manuscript.

2. Ethics, Consent to Participate, and Consent to Publish declarations: Not Applicable.