MILESTONE TRANSACTIONS ON
MEDICAL TECHNOMETRICS
VOL. 1, ISSUE. 1, 2023



RESEARCH ARTICLE

# A Modified Framework for Image Encryption and Decryption Using Modified Chaotic Algorithms Towards Medical Image Security

**Nagashree N[1]. Shantakumar Patil[1]. Narayan K[2] . Chethana N[1]. Chandana N[1]. Rakshitha Mansi HT[1]. Sparshithraj[1]**

[1]Department of Computer Science and Engineering
Sai Vidya Institute of Technology, VTU, Bangalore, Karnataka, India.
[2]NITTE Meenakshi Institute of Technology
VTU, Bangalore, Karnataka, India.

Received: 25 April 2023 / Revised: 22 May 2023 / Accepted: 09 June 2023

DOI: 10.5281/zenodo.8069902

**Abstract –** The brain child of the paper is to design a framework for performing secure medical image transmission via networks. There are several image cryptographic techniques available for better encryption and decryption of images. This paper proposes a modified chaotic algorithm based on Arnold cat map and Hanon map using Harris corner detector to secure the images at extra level. The proposed framework has given around 98% of accuracy in contrast to the earlier existing methods. The performance evaluators are executed to measure the accuracy of proposed system.

**Index Terms –** Arnold, mapping, Henon, Harris, Image encryption, decryption, modified chaotic algorithm, ORB , feature matching

## I. INTRODUCTION

As we live in digitized world, we use lots of electronics gadgets and those are the mediators for the transfer of data from one device to the other. One can keep sending medical data such as x ray, MRI, CT images of patients to other devices [1]. Though technology has new-fangled now a days, there is always a prone to threat regarding data being corrupted, loss or trespassing by third party. Thus, there is a better scope for cryptographic techniques to securely transfer the data to other end. Several image cryptographic methods are in practice out of which mathematical and statistical based methods are in modus operandi now [2]. Image cryptography is the process of transforming an image into another form so that except authorised receiver, others will not be able to see the original image thus preserving security [3]. The process involves 2 steps image encryption and decryption. The first one being transformation of

original image to transformed image obtained by randomly changing coordinate points of original image to get encrypted image [4]. Image decryption on the other hand is converting back of encrypted image to original image.

These processes happen one at sender's end and other one at receiver's end [5]. Much of the research has happened in the field of image encryption and decryption where public key and private key generation methods are adopted to perform cryptography. Recently few of Machine learning and deep learning techniques have been adopted which makes use of CNN techniques for image encryption [6]. Though there are several recent DL approaches, those methods give better accuracy and robustness in case only there are many images. It will not work well for small dataset. The main challenge in medical image encryption is the security of the data transmission. If an MRI data of a patient must be sent to other person through e mail, it is practically not a feasible idea to use machine learning or deep learning techniques which always uses large set of data.

As the images must be secured, a simple mathematical transformation such as Henon map and Arnold cat map is read. Much of the result is done by authors and researchers in the field of image cryptography. Mahoumad Ahmad et al suggested a method for image encryption though XOR transformation [1]. G chaitanya et al showed some linear regression models and interpolation techniques to add random pixels over original image to get encrypted image [2]. In another research work, optimization and fusion strategy is used to image cryptography [3]. Saeed et al presented that, using high level synthesis would result into good results. [4]. Much of the researchers claim that we do not have anything to study further using genetic algorithm [5]. Wan et al in this research work [6] has been suggested image cryptography methods which has given accurately done [6].

In [7] author has proposed that inverse of cosine of an example is used for image encryption. In another work image segmentation and object detection is done which is helpful for image transformation and security at the later stages [8]. Al- Abaidy in his research work presented ANN approach for detection of image encryption and decryption [9] which goes well for large set of data. Some researchers have worked on signalling-based image encryption which gives better results [10]. Recently many authors have suggested and working well on chaos theory of image encryption and decryption which is a mathematical modelling theory based on image transformations of applied mathematical models [11,12].

## II. METHODOLOGY

The proposed methodology has the following phase which is depicted in the architectural diagram as shown below in fig 1. The proposed method involves an efficient way to develop digital image cryptographic technique to ensure better image security in medical and remote sensing images. The image encryption block diagram is shown in the below fig 2. The original image is reshaped into a square and then the Arnold's cat map is applied to shear the image and change the pixel positions of the image, later Henon map is applied to change the grey values of the pixels in the image to enhance security. The image decryption block diagram is shown in fig 3, here the confused image is passed through reverse Henon algorithm, the process also called diffusion, and later reverse of Arnold's cat map algorithm is applied,

then the borders of the image is cropped off to get the actual image shape and we obtain the decrypted image.

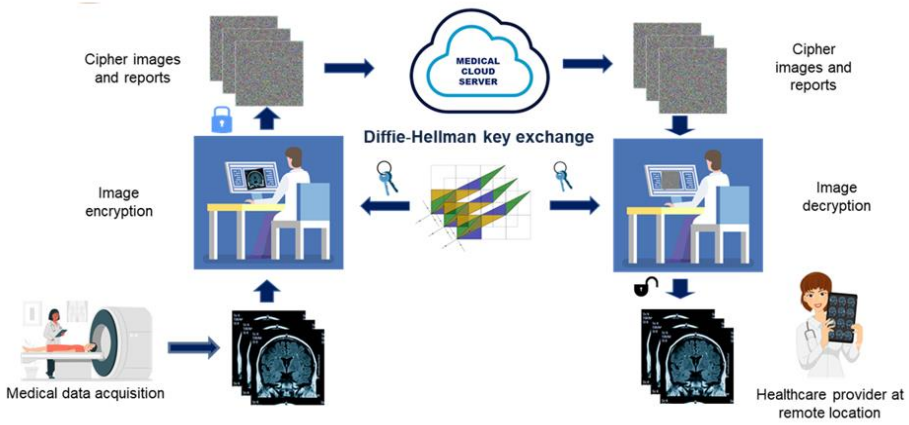


**Fig: 1 System Architecture**

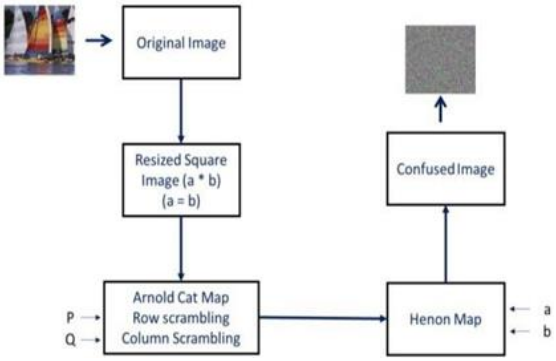


**Fig: 2 Image Encryption block diagram**

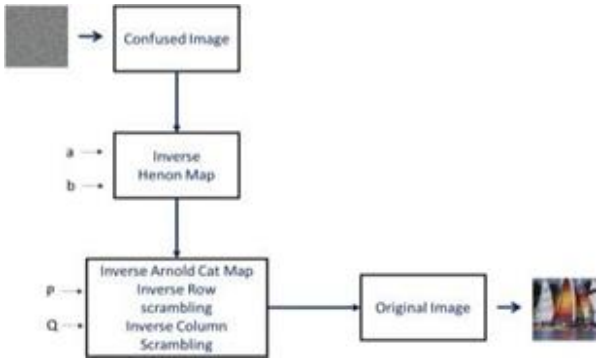


**Fig: 3 Image decryption block diagram**

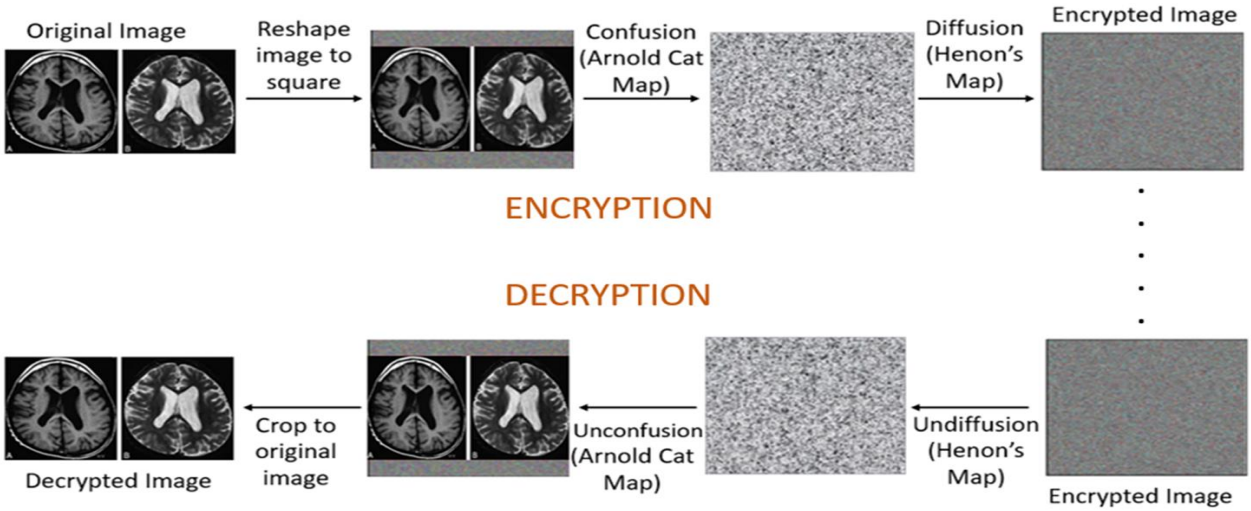


**Fig: 4 Flow diagram of the system**

## III. RESULTS AND DISCUSSIONS

- Initially there is key generation using Diffie-Hellman key exchange algorithm to login into this application. To login we need to input the private key value whose length is 30 digits.
- After Logging in to the application, a screen shown below opens, where we need to input the image to be encrypted and the source folder path where the image exists and the receivers public key and then click on the encrypt button.
- Here we have used a brain MRI image as our image to be encrypted. This is shown in fig 7.
- The encrypted image is stored in the encrypted image folder created by the user. This is depicted in fig 8
- Now to decrypt the image we give the parameters accordingly, which includes the encrypted image path, the destination folder where the decrypted image must be stored and the receivers public key. The below image 9 shows the same
- Now we can find the decrypted image which will be stored in the destination folder given by the user. The below figure 10 shows the decrypted image

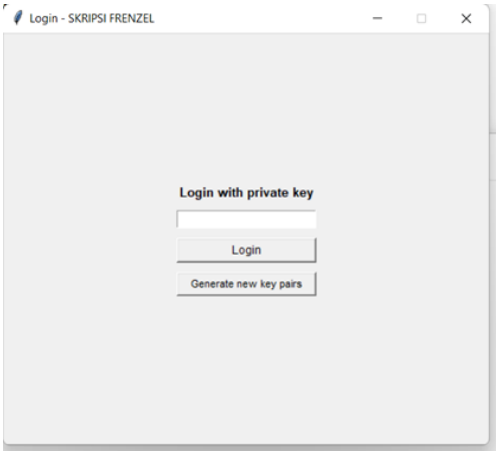


**Fig: 5 Login Window.**


**Fig: 6 Image Encryption Window**

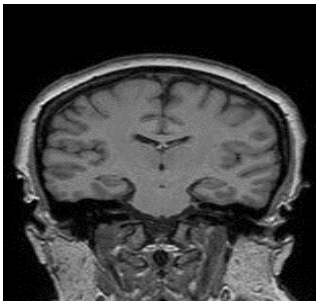

**Fig: 7 Brain MRI image to encrypt**

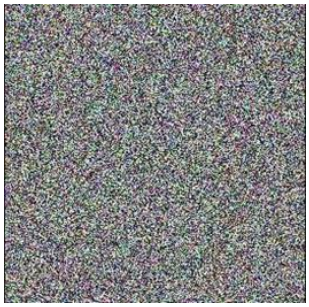

**Fig: 8 Encrypted Image**

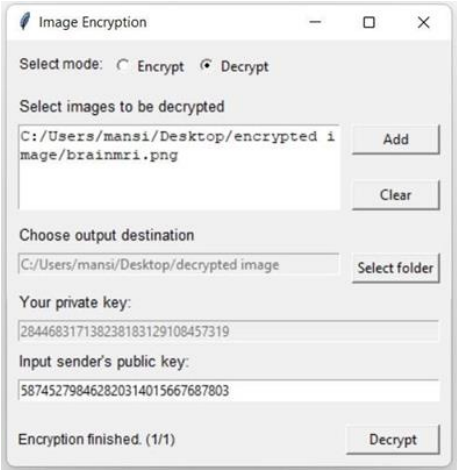


**Fig: 9 Image Decryption Window**

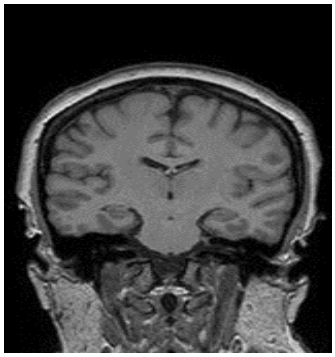

**Fig: 10 Decrypted Image**

## Performance Evaluation

Performance evaluation is done on identifying three coordinate points on encrypted and original image. Calculate the distance between each coordinate point from one image to that of other, if the difference in distance is nearer to 0 it means the accuracy of our algorithm is 100%. Let {Ex1,Ey1}, {Ex2,Ey2} and {Ex3 Ey3} be the coordinate points of encrypted image and {Ox1,Oy1}, {Ox2,Oy2} and {Ox3,Oy3} are the points of original image. Applying Euclidean distance for the above results we got the values as 0.01 which is approximately 0. And thus we can prove that the algorithm is 100% efficient. The points selected to check for exact matching between both the images are generated as form of coordinates, called descriptors.

## Oriented Fast and Rotated Brief (ORB Algorithm)

The ORB Algorithm is used to detect features in an image. Points, structures, objects in an image is are called 'Features'. Its focused at trying to gauge similarities in the properties of an image. A string of numerals which describe some salient features in an image are called as Feature Descriptors.

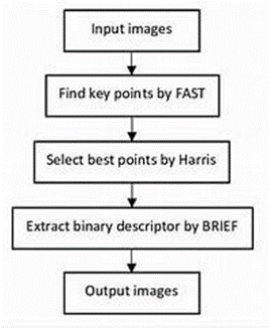


**Fig : 11 ORB Algorithm steps**

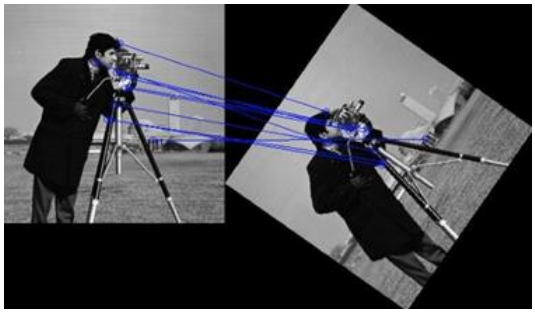

**Fig: 12 Depicts keypoints being matched in rotated image**

Initially, the image for which features have to be detected is input. Now, the first step involves finding keypoints by FAST (Features from Accelerated Segments Test). Keypoints are the interest points which are the features that stand out distinctly in an image. The reason why keypoints are special is because no matter how the image changes : whether the image rotates, shrinks/expands, is also translated (all of these would be an affine transformation by the way) or is subject to distortion (i.e. a projective transformation or homography), you should be able to find the same keypoints in this modified image when comparing with the original image.

In case of FAST, the keypoints are detected by the following way : It takes a central pixel, say p and demarcate by a circle.. Now let this have intensity ip. Let's define a treshold value as th. So, upper threshold of intensity is ip+th and lower threshold is ip-th. Now, demarcated by a circle, say the pixel p is surrounded by 16 pixels. If 8 out of these 16 surrounding pixels have intensity higher than the central pixel p, i.e, greater than ip+th, then the pixel p is regarded as a keypoint. In this way, we first gather all the keypoints and move to the next step of corner detection.

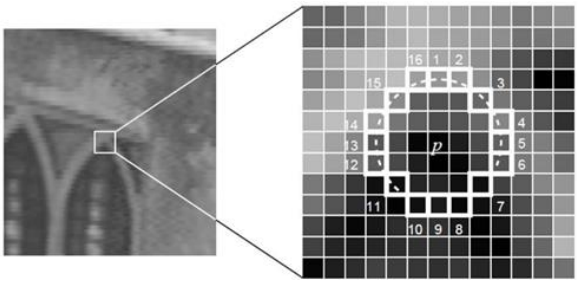


**Fig 13 : Keypoints detection and demarcation**

**Fig 14 : Keypoints with size**

**Fig 15 : Keypoints without size**

Next step is selection of best points by Harris. When a point is characterized by large intensity variation in all directions, its called a corner. In previous step, we get all keypoints. But now, we filter out to get only corners from that. Corners are stable over change of viewpoint and illumination and so, are important in computer vision and detection. By finding image derivatives in x and y directions and putting them in matrix format, we can derive a matrix called as the structure Tensor ( denoted by M) :

$$M = \sum_{(x,y) \in W} g(x,y) \begin{bmatrix} I_x I_x & I_x I_y \\ I_x I_y & I_y I_y \end{bmatrix} \quad \text{(Eq. 1)}$$

Using the Structure Tensor, we derive the Response function (R) that detects a corner presence : $R = \det(M) - k\,\mathrm{tr}(M)^2$.

k is a constant in range [0.04, 0.06] det(M) = $\lambda 1\ \lambda 2$ , tr(M) = $\lambda 1 + \lambda 2$ , $\lambda 1$ and $\lambda 2$ are called Eigen values.

So the eigenvalues determine whether a region is an edge, a corner or flat

1. if λ1 and λ2 are small, then |R| is small and the region is flat;

2. if λ1 >> λ2or vice versa, then R<0 and the region is an edge;

3. if λ1 ≈ λ2 and both eigenvalues are large, then R is large and the region is a corner.

From this, we only choose corners and move to the next step. What makes key points different between frameworks is the way you describe these keypoints. These are what are known as descriptors. Each keypoint that you detect has an associated descriptor that accompanies it, usually a string of numerals. These descriptors are found for the corners we detected from Harris Corner Detection algorithm, using the BRIEF Algorithm.

**BRIEF stands for Binary Robust Independent Elementary Features**

This is a feature point descriptor which is also general- purpose and can be combined with other arbitrary descriptors. These descriptors are nothing but feature vectors which are strings of 128-512 bits consisting only of 0s and 1s.

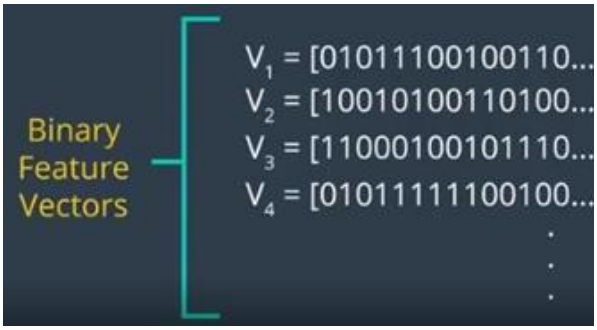


**Fig 16 : BRIEF Vector Generation**

In order to avoid sensitivity to high frequency noise, Brief smoothens the image using Gaussian Kernal. Now a neighborhood (termed as patch) is defined around that keypoint and within that patch 2 more random pixels are chosen. The first pixel is chosen from Gaussian Distribution centered around that keypoint with standard deviation of Sigma. The second pixel is chosen from Gaussian Distribution centered around the first pixel chosen, with standard deviation of sigma/2. If first pixel is brighter than the second pixel, the corresponding bit value is 1 else it is 0.

Again , brief selects a random pair and assign the value to them. For a 128-bit vector, brief repeat this process for 128 times for a keypoint. Brief create a vector like this for each keypoint in an image. However, BRIEF also isn't invariant to rotation so orb uses rBRIEF(Rotation-aware BRIEF). ORB tries to add this functionality, without losing out on the speed aspect of BRIEF.

**Brute Force Feature Matcher**

So far, we only spoke of a single image and how we detect features, keypoints generation, filtering out the corners and then generating their descriptors. However, in order to talk about accuracy, the same ORB algorithm is applied separately to the Original Image and then to the image obtained even after Decryption. Later, each of these features are matched from the Original Image to the Decrypted Image. And if all the features are perfectly matched, we can say that our algorithm is 100% accurate. It takes the descriptor of one feature in first set and is matched with all other features in second set using some distance calculation. And the closest one is returned.

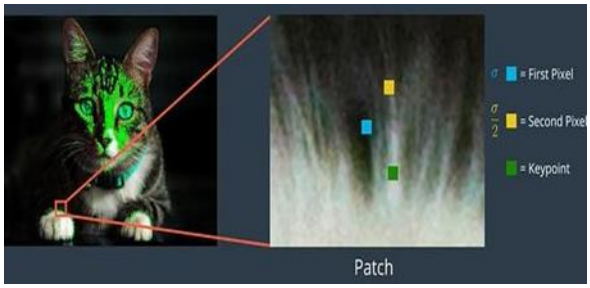


**Fig 17 : Choosing points within the patch**

Similarly, it takes the descriptor of the second feature, matches it with all other features in the second image and the closest one is returned as a successful matcher. Similarly, it is repeated for each feature.

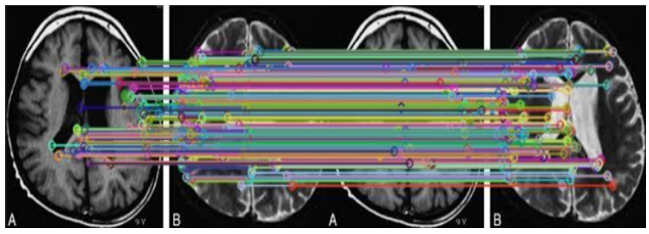

**Fig 17 : Brute force feature matcher applied on Original image (left) and Image obtained after Decryption(Right)**

On comparing ORB with other algorithms such as SIFT and SURF, we notice that ORB is the fastest among the 3 and each of them have their own added value in different scenarios. But for our application, ORB is best-suited and has provided us with 100% accuracy in the tests performed so far

**Table.1: Matching Rate versus Rotation Angle**

| Angle → | 0 | 45 | 90 | 135 | 180 | 225 | 270 |
|---|---|---|---|---|---|---|---|
| SIFT | 100 | 65 | 93 | 67 | 92 | 65 | 93 |
| SURF | 99 | 51 | 99 | 52 | 96 | 51 | 95 |
| ORB | 100 | 46 | 97 | 46 | 100 | 46 | 97 |

**Table. 2: Results of Comparing Image with Scaled Image**

| | Time (sec) | Kpnts1 | Kpnts2 | Matches | Match rate (%) |
|---|---|---|---|---|---|
| SIFT | 0.25 | 248 | 1210 | 232 | 31.8 |
| SURF | 0.08 | 162 | 581 | 136 | 36.6 |
| ORB | 0.02 | 261 | 471 | 181 | 49.5 |

## REFERENCES

1. Kumar, U., Shukla, S., Malik, I., Singh, S., Bhardwaj, H., Sakalle, A., & Bhardwaj, A. (2021, December). Image encryption using chaotic neural network. In 2021 3rd International Conference on Advances in Computing, Communication Control and Networking (ICAC3N) (pp. 1424-1427). IEEE.
2. Jiang, A., Yu, J., & Cang, X. (2010, September). Image encryption algorithm based on chaos and contourlet transform. In 2010 First International Conference on Pervasive Computing, Signal Processing and Applications (pp. 707-710). IEEE.
3. Agbedemnab, P. A. N., Baagyere, E. Y., & Daabo, M. I. (2019, September). A new image encryption and decryption technique using genetic algorithm and residual numbers. In 2019 IEEE AFRICON (pp. 1-9). IEEE.
4. Bo, L., Na, L., Jianxia, L., & Wei, L. (2011, August). Research of image encryption algorithm base on chaos theory. In Proceedings of 2011 6th International Forum on Strategic Technology (Vol. 2, pp. 1096-1098). IEEE.
5. Nagashree, N., Patil, P., Patil, S., & Kokatanur, M. (2021, June). Alpha beta pruned UNet-a modified unet framework to segment MRI brain image to analyse the effects of CNTNAP2 gene towards autism detection. In 2021 3rd International Conference on Computer Communication and the Internet (ICCCI) (pp. 23-26). IEEE.
6. Al-Shammari, N. K., Syed, T. H., & Syed, M. B. (2021). An Edge–IoT framework and prototype based on blockchain for smart healthcare applications. *Engineering, Technology & Applied Science Research*, *11*(4), 7326-7331.
7. Wan, N., & Zhang, Y. (2020, December). Digital image encryption and decryption algorithm based on optimization and fusion strategy. In 2020 13th International Symposium on Computational Intelligence and Design (ISCID) (pp. 244-248). IEEE.
8. Nagashree, N., Patil, P., Patil, S., & Kokatanur, M. (2022). InvCos curvature patch image registration technique for accurate segmentation of autistic brain images. In Soft Computing and Signal Processing: Proceedings of 3rd ICSCSP 2020, Volume 2 (pp. 659-666). Springer Singapore.
9. Nagesh, N., Patil, P., Patil, S., & Kokatanur, M. (2022). An architectural framework for automatic detection of autism using deep convolution networks and genetic algorithm. International Journal of Electrical and Computer Engineering (IJECE), 12(2), 1768-1775.
10. Al-Abaidy, S. A. F. (2020). Artificial neural network based image encryption technique. International Journal of Services Operations and Informatics, 10(3), 181-189.
11. Sathiyamoorthi, V., Ilavarasi, A. K., Murugeswari, K., Ahmed, S. T., Devi, B. A., & Kalipindi, M. (2021). A deep convolutional neural network based computer aided diagnosis system for the prediction of Alzheimer's disease in MRI images. *Measurement*, *171*, 108838.
12. AlMutairi, F., & Bonny, T. (2020, November). Image encryption based on chua chaotic oscillator. In 2020 3rd International Conference on Signal Processing and Information Security (ICSPIS) (pp. 1-4). IEEE
13. Vijayakumari, G., & Holi, G. Assessment of Joint Space in Knee Osteoarthritis using Particle Swarm Optimization Technique.
14. Ahmed, S. T., Kumar, V., & Kim, J. (2023). AITel: eHealth Augmented Intelligence based Telemedicine Resource Recommendation Framework for IoT devices in Smart cities. *IEEE Internet of Things Journal*.
15. Bo, L., Na, L., Jianxia, L., & Wei, L. (2011, August). Research of image encryption algorithm base on chaos theory. In Proceedings of 2011 6th International Forum on Strategic Technology (Vol. 2, pp. 1096-1098). IEEE.