Journal of Information Systems Engineering and Management
2025, 10(45s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Multibiometric Secured E-Voting Based on Hyper Elliptic Curve Cryptography

R. Lavanya[1], R. Sarasu[2], C. Murukesh[3], K. Pandikumar[4]
[1]Department of Information Technology, Aalim Muhammed Salegh College of Engineering, Chennai, India.*
[2]Institute of CSE, Saveetha School of Engineering, SIMATS, Chennai, India.
[3]Department of ECE, Velammal Engineering College, Chennai, India.
[4]Department of CSE, Dhanalakshmi College of Engineering, Chennai, India.
[*]Corresponding author : m.lavanya.ams@gmail.com

ARTICLE INFO

Received: 29 Dec 2024

Revised: 12 Feb 2025

Accepted: 27 Feb 2025

ABSTRACT

In popular democratic countries, the voting system plays an important part during choosing the right government. Electronic voting machines are less secure with regard to data, time consuming and need further workforce to avoid illegal casting of votes. The proposed system have a secured authentication method with a multibiometric system integrating both fingerprint and iris recognition system. The stored iris data is encrypted using hyper elliptic curve cryptography (HECC) algorithm. The Daugman's algorithm smoothen the noise posterior to the iris localization and feature extraction is carried out to non-varying and unique parameters of an iris image. Further biometric data used is fingerprint recognition, which is a complex recognition parameter. It includes algorithms and procedures for image improvement and linearization, rooting for miniaturized features and matching for authenticating the candidates. To ensure security, iris images converted to cipher templates using HECC, thereby data can be saved from duplication without the chance of intrusion. The proposed system witnessed a true acceptance rate of 98% with 2.5% of equal error rate and accuracy of 95%. The minimum recognition time achieved is 4 seconds and has been identified as an outperforming model than existing solutions in voting applications.

Keywords: Hyper Elliptic Curve Cryptography, Multibiometric system, Daugman's algorithm, Cipher templates and FLANN algorithm.

INTRODUCTION

The voting system in India is vital for establishing a democratic government, ensuring justice, rights, education, a healthy environment, and financial stability for all. Key challenges in the e-voting system include voter duplication, multiple vote casting, and the unlawful exclusion of voter names, which undermine democratic participation. Additionally, manual voter verification compromises security and legality. These issues can be addressed through real-time biometric authentication, such as iris and fingerprint recognition, which enhance data security and voting integrity. Iris biometrics offer unique identification features, while fingerprints provide reliable performance for secure systems. The proposed system integrates fingerprint and iris subsystems to create a robust, independent, and automated voting infrastructure, addressing key challenges in the current system. It features a two-step biometric authentication process, with temporary data storage. The first step involves fingerprint point matching using Aadhar card data through point detection modules. The second step is iris verification, conducted with an iris scanner and image processing algorithms. The system compares the scanned iris image with the stored database; if there is a match, the voter is allowed to vote. If not, a piezoelectric buzzer alerts the user to halt the voting process. If the same voter attempts to vote again, the system will recognize them during the first stage, preventing further processing. All data processing and analysis are managed by a PC, with image data captured through dedicated scanning and detection modules. The original iris template can be encrypted using Hyper Elliptic Curve Cryptography (HECC), a lightweight algorithm offering high security quickly. Unlike traditional elliptic curve cryptography, HECC overcomes key size and computational constraints due to its use of finite fields and algebraic structures. It employs Extended Complex Multiplication (ECM) over a high field (P) with a 64-bit key size, making brute-force attacks more complex. Figure 1 illustrates the integrated biometric authentication system.

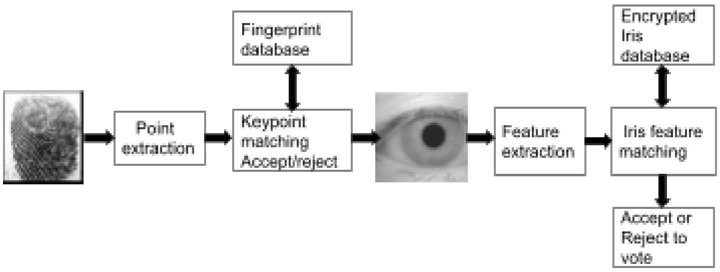


Fig.1 Multi Biometric e-voting system

The verification process includes iris image acquisition, preprocessing, and cypher template creation with HECC. The system compares the cypher template with the stored database template, and final authentication is performed using the FLANN algorithm. The authentication result is displayed via a web interface with pop-up dialogs for acceptance or rejection.

LITERATURE REVIEW

Multibiometric approach improves the security and accuracy of biometric systems compared to single-biometric systems that rely on one trait. Fuzzy combined with genetic algorithm handles imprecise information and uncertainities and helps to improve reliability in biometric authentication approach [1]. Traditional methods rely on texture-based features in iris, but incorporating stylometric features can significantly enhance recognition performance [2]. Hybrid techniques are employed in biometric recognition to combine various fusion strategies, thereby achieving superior performance in the identity verification process compared to unimodal systems [3][4]. Innovative technique to assist physically disabled individuals by enabling robotic control through iris movement and improve reliability in iris based system [5] , further integrating detection and segmentation using deep learning framework improves accuracy [6] . Artificial intelligent models with self customization discuss the difficulties with iris recognition in partially obscured images [7] and various feature extraction methods enhance performance [8] [9]. Neural network based models helps in classification of iris patterns effectively [10] [11]. When template matching technique is integrated with the network model iris recognition on mobile devices is enhanced [12]. In real-time image processing for finger print systems, the CNN model performs accurate segmentation in less training time [13] [14]. The proposed system uses both finger print and iris based recognition system and offers high accuracy, significantly reducing the equal error rate. This leads to lower time and energy consumption compared to manual verification systems, as it requires minimal computational time. Together, these factors enhance the efficiency of the voting ecosystem in every election.

IMPLEMENTATION

A. FINGERPRINT RECOGNITION SYSTEM

Fingerprint recognition is achieved using SIFT and FLANN algorithms. SIFT algorithm detects and fixes the curves and edges by identifying the ridges and valleys in the fingerprint image. FLANN matcher uses the function of comparison and matches the fixed keypoint descriptors using features of the fingerprint images in the database. After preprocessing, during finger print recognition the descriptor is extracted and point matching is done.

1. Scale Invariant Feature Transform (SIFT)

i) Scale-space local extreme detection: Sites are identified by looking for traits that remain stable across sizes using the continuous scale function known as scale space. A(i1,j1,$\boldsymbol{\sigma}$) is convolution operation which is formulated in equation (1), where Gaussian variable scale is G(i1,j1,$\boldsymbol{\sigma}$). With the input image h(i1, j1), for two nearby scales of the image, the DoG is computed as represented in equation (2), where m is a constant multiplicative factor to change scale and i1,j1 are the direct coordinates of a pixel in image h. ii) Accurate Key-point Localization: Images are evaluated by computing local maxima and minima across several scales to find significant locations. A thorough fit is conducted after keypoint identification to ascertain the location, major curve percentage and scale. Low contrast keypoints are disregarded and the interpolated location of the maximum is determined using a 3D quadratic operator. Sample point derivatives V_m are formulated as in Equation (3). By taking the derivative with respect to x and tracking down towards zero, the location of extremum e is obtained as given in Equation (4).

$$(i1,j1,\boldsymbol{\sigma}) = h(i1,j1) * G(i1,j1,\boldsymbol{\sigma}) \qquad (1)$$

$$D(i1,j1,\boldsymbol{\sigma}) = h(i1,j1) * \ (G(i1,j1,m\boldsymbol{\sigma}) - G(i1,j1,\boldsymbol{\sigma})) \qquad (2)$$

$$V_m(x)=V+(\partial^{2}V^{-1}{}_{m}/\partial z)*(\partial V_m/\partial z) \qquad (3)$$

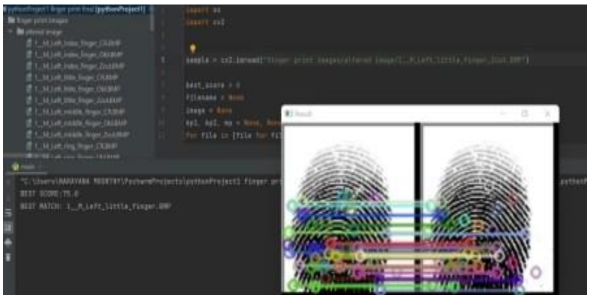
$$e=(-\partial^2 D-1 \ / \ \partial e^2) * (\partial D/\partial e) \qquad (4)$$

iii) Orientation Assignment**:** The deviation offset point is compared to a predefined threshold value after which it implies that e is close to some different sample point. Then sample point is varied and interpolation is operated about that point. iv) Key-Point Descriptor: By examining gradient orientations and magnitudes, a key-point descriptor is defined. Samples are concatenated into 4×4 sub-region histograms, and the descriptor is used to identify matching fingerprint features. The Figure 2 depicts the construction of key-point descriptors

$$\theta(i.j)=tan^{-1}((L(i,j+1)-L(i,j-1)) \ / \ (L(i+1,j)-L(i-1,j))) \qquad (5)$$

2. Fast Library for Approximate Nearest Neighbour (FLANN)

FLANN performs approximate nearest neighbor search in image. The features are extracted and represented as a set of feature descriptors, where each descriptor represents a unique feature in the image. FLANN uses an indexed data structure to quickly find approximate nearest neighbors of an image's feature descriptors. It measures similarity using a distance metric and selects the best matches with lowest distances. To reduce false matches and to provide approximate matches, filtering is applied. The Figure 3 depicts matching of keypoint matching, unique descriptor features of the database images are compared with the test image keypoints and scores are generated.



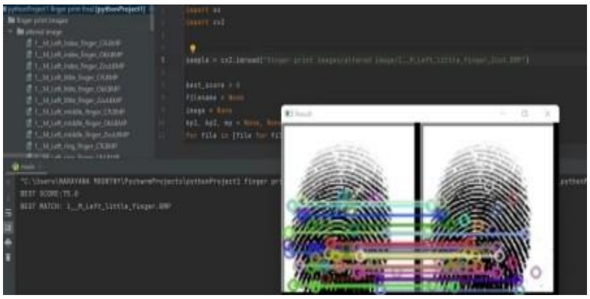
```
import os
import cv2

sample = cv2.imread("finger print images/altered image/1__M_Left_little_finger_Zcut.BMP")

best_score = 0
filename = None
image = None
kp1, kp2, mp = None, None
for file in [file for fi
```

```
BEST SCORE: 75.0
BEST MATCH: 1__M_Left_little_finger.BMP
```

Fig.2 Construction of keypoint descriptors



```
import os
import cv2

sample = cv2.imread("finger print images/altered image/1__M_Left_little_finger_Zcut.BMP")

best_score = 0
filename = None
image = None
kp1, kp2, mp = None, None
for file in [file for fi
```

```
BEST SCORE: 75.0
BEST MATCH: 1__M_Left_little_finger.BMP
```

Fig. 3 Fingerprint matching with FLANN

B. IRIS RECOGNITION SYSTEM

1. Preprocessing of Iris

Iris preprocessing includes normalization to minimize noise and localization to determine the region of interest. i) Iris Localization: Locates the iris boundary internally and externally using the Circular Hough Transform Algorithm (CHTA). Canny Edge Detection identifies the edge map, and CHTA determines the inner and outer iris circles. Localizes and segments the iris as a distinct biometric feature. Figure 4 and 5 represents iris region.

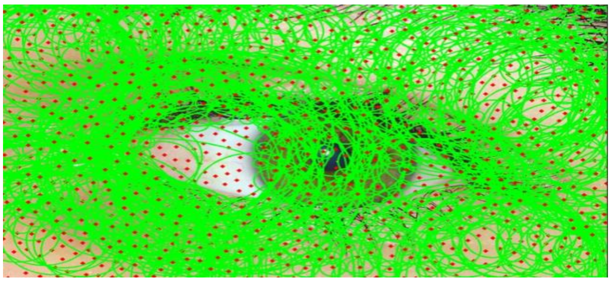


Fig. 4 Localization of iris region using CHTA

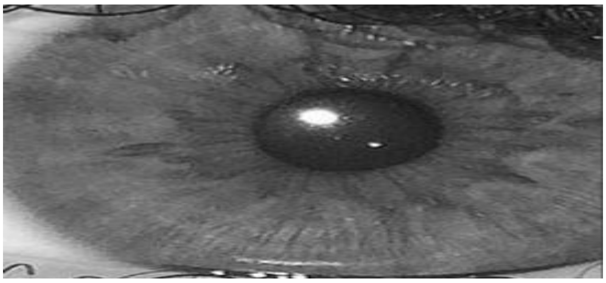


Fig.5 Segmented iris region

ii) Iris Normalization: Using Daugman's model, the iris image is normalized to polar coordinates. The focal point and radius of the pupil are determined by iris segmentation. Based on the IITD Iris dataset, the iris component is separated into 50 pixels, where s is the scaling factor, θ is the rotation angle, and (i center, j center) is the center of the normalized iris image.

$$i' = s * ((\theta) - j\sin(\theta)) + icenter \quad (6)$$

$$j' = s * ((\theta) + j\cos(\theta)) + jcenter \quad (7)$$

2. Feature extraction

Gabor kernel filters, which are used for feature extraction, apply multiple filters with varying orientations, frequencies, and bandwidths to the input image. The formula for spatial domain is:

$$G(i,j) = \exp(- i'^{2} + \boldsymbol{\gamma}^{2} * j'^{2}) / (2 * \sigma^{2})) * \cos(2 * \pi * frequency * i' + phase) \quad (8)$$

where i and j are filter coordinates, i' and j' are rotated coordinates, $\boldsymbol{\gamma}$ is aspect ratio that controls the ellipticity of the filter, $\boldsymbol{\sigma}$ is the standard deviation. Figure 6 and 7 holds normalized and extracted iris region Input image is convolved with Gabor filters, producing response maps that highlight areas matching the filter features. Features are extracted by selecting the maximum or average values from these maps. The image is smoothened, reducing noise, emphasizing key features for analysis and matching. The Figure 8 shows matching iris feature and Figure 9 iris processing.

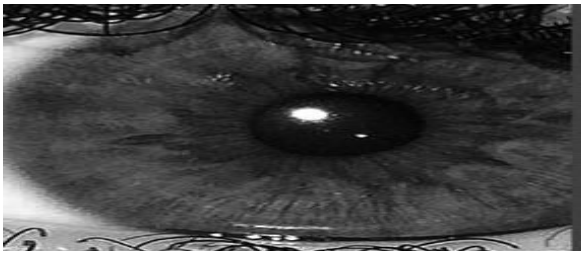


Fig. 6 Normalized iris region in polar coordinates

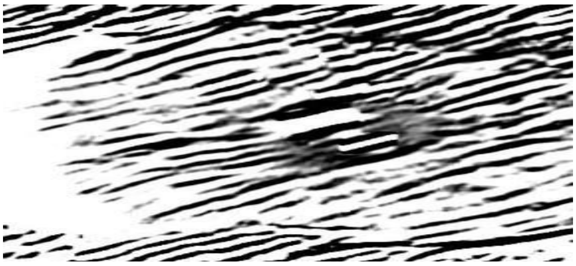
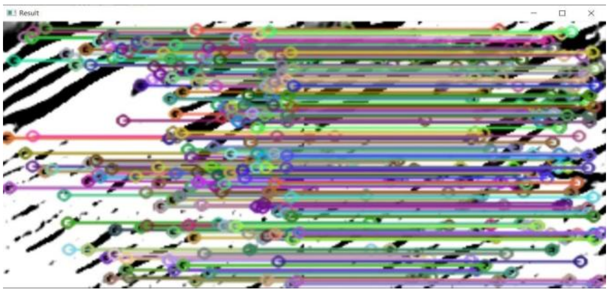


Fig. 7 Extraction of features after Gabor channels

Smoothening the iris region



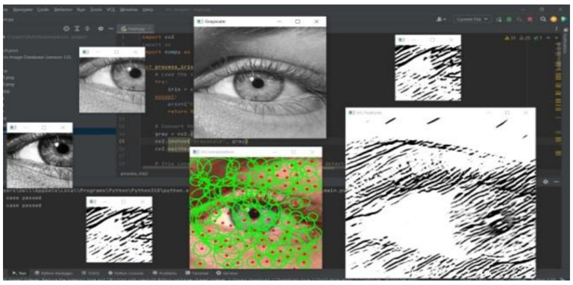


Fig. 8 Matching iris feature points through FLANN matcher

Fig. 9 Iris image processing stages of sample test image

3. Hyper Elliptic Curve Cryptography

HECC encrypts biometric templates using cryptographic primitives with an 80-bit key size, offering strong security and fast processing for real-time applications. It includes stages such as Extended Complex Multiplication: selects the curve with N cardinality b) Restricted Iris Template: reduces size of template c) Point - Divisor Conversion (PDC): converts HEC points in to divisors d) Randomized Divisor Construction: generates random divisors using PDC results and the Cantor Algorithm (DACA) e) Divisor - Point Conversion (DPC): transforms divisors into cipher points, forming the final encrypted template. The algorithm followed in HECC is as follows:

Input: Initial iris template A

Output: Iris template in encrypted form A'

Method: Use ECM to choose genus 2 HEC

Transform the initial iris template into hyperelliptic curve points and Apply PDC to map HEC points to corresponding divisors

Using the RCD algorithm, select a random divisor d11 and choose the public key $\in \{2, 3, 4 \ldots p - 1\}$

For 4 sequential samples (M1, M2, M3, M4) do

Apply the RCD algorithm to generate a random divisor d1

Calculate $c'_i = c + (k * d1)$ *with cantor algorithm*

Output the calculated divisors in cipher form c'_i

Apply DPC to convert divisors to points (cipher) & then convert points into the template (cipher) A'

Save the templates (cipher) - A'

RESULTS AND DISCUSSION

The IITD Iris Dataset was used to assess the performance of the proposed technique. A set of 100 iris samples was gathered and accuracy were calculated at various threshold values to assess the viability of the approach. The analysis of the IITD iris data revealed a maximum TAR of 100%. At a threshold of 0.75, an EER of 2.5% was observed with a TAR of 98%. The total recognition time for authentication was just 4 seconds, which is twice as fast as existing biometric systems without cryptography. The integration of algorithms used in fingerprint and iris recognition, along with the encryption scheme applied in the voting system, highlights the performance benefits of biometric e-voting systems. These systems play a crucial role in enhancing security and protecting the integrity of votes during elections. The performance metrics were computationally effective, with different threshold illustrated graphically in Figures 10 and 11, offers a clear evaluation of the performance of algorithm during implementation at different stages.

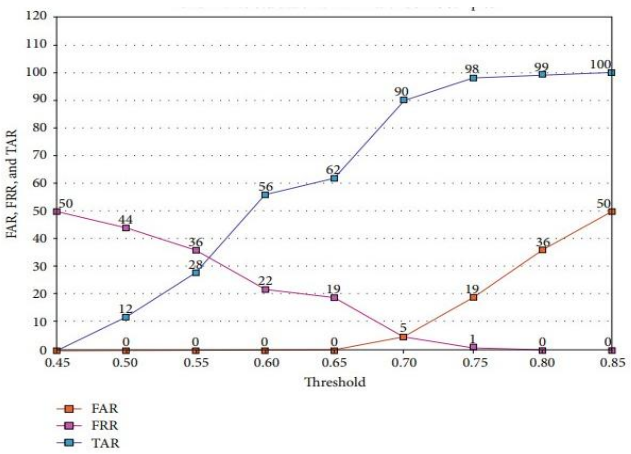


Fig. 10 Performance metrics evaluation against different thresholds for 50 samples

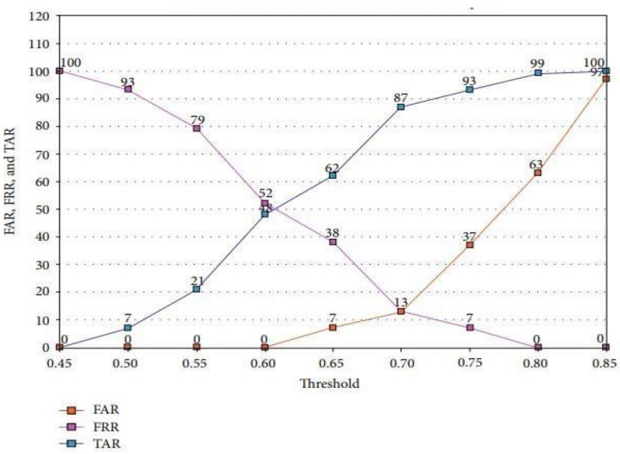


Fig. 11 Performance metrics evaluation against different thresholds for 100 samples

The performance of the samples from the IITD iris dataset was assessed based on specific parameters using Python 3.10 on PyCharm IDE 22.2.3. An R307 optical fingerprint reader was used as the fingerprint scanner module. The performance parameters evaluated are: FAR (False Acceptance Rate): Chance of wrongly accepting an unauthorized user. FRR (False Rejection Rate): Chance of wrongly denying an authorized user. TAR (True Acceptance Rate): Probability of correctly identifying an authorized user.

CONCLUSION

Multibiometric e-voting with cryptography is a secure, user-friendly system that gradually integrates multiple biometric authentication methods for voter identification and verification at polling booths. The data is securely encrypted with hashed, lengthy keys, making it difficult for intruders to breach. The proposed system witnessed a true acceptance rate of 98% and with 2.5% of equal error rate with highest accuracy of 95%, the minimum recognition time achieved is 4 seconds. Even though block chain voting approach has come a long way in its own deployment model for the voting process, still it hasn’t achieved certain regulations and control over the implementation stand point of view in real world scenarios. Automation of e-voting can reduce the manual operation and maintenance cost drastically by deploying an authentic, self-sustained and secured voting model which is suggested in the proposed system. Additionally, the proposed system is eligible for implementation in different sectors like military applications, banking sector and avoidance of fake candidates in the entrance exams. Application of biometric secured systems in future prospects can help in protecting the democracy and rights of the people from a broader perspective in the years to come as technology stays evolving all the time.

REFERENCES

[1] N. Malarvizhi, P. Selavarani and P. Raj. “Adaptive fuzzy genetic algorithm for multi biometric authentication”. Multimedia Tools and Applications, vol. 79, no.2 (2020), pp. 9131– 9144. DOI: 10.1007/s11042-019-7436-4.

[2] S. Adamovic, V. Miskovic, N. Macek, et al. “An efficient novel approach for iris recognition based on stylometric features and machine learning techniques”. Future Generation Computers Systems, vol. 107 (2020), pp.144–157. DOI:10.1016/j.future.2020.01.056

[3] R. Lavanya and N. R. Shanker. “Thermal Image Based Occupant Count Measurement Model using Human Body Temperature for Smart Building”. Indian Journal of Science and Technology, vol.17, no.26 (2024), pp.2683-2690. DOI://doi.org/10.17485/IJST/v17i26.1647

[4] S. Velmurugan and S. Selvarajan. “A multimodal authentication for biometric recognition system using hybrid fusion techniques”. *Cluster Computing*, vol. 22, no.6 (2019), pp. 13429– 13436. DOI:10.1007/s10586-018-1952-2

[5] S Viriri and J. Tapamo, “Iris pattern recognition based on cumulative sums and majority vote methods”, International journal of Advanced Robotics Systems, vol. 14, no. 3 (2017), pp.1-9. DOI:10.1177/172988141770393

[6] Z. Zhao and A. Kumar. “A deep learning based unified framework to detect, segment and recognize irises using spatially corresponding features”. *Pattern Recognition, vol.* 93, no. 2 (2019), pp.546–557. DOI: 10.1016/j.patcog.2019.04.010

[7] I. A. Qasmieh, H. Alquran and A.M. Alqudah. “Occluded iris classification and segmentation using self-customized artificial intelligence models and iterative randomized Hough transform”. International Journal of Electrical & Computer Engineering, vol. 11, no.5 (2021), pp.4037-4049. DOI: 10.11591/ijece.v11i5.pp4037-4049

[8] R. Lavanya, C. Murukesh and N.R. Shanker. “Microclimatic HVAC system for nano painted rooms using PSO based occupancy regression controller”. Energy. Vol. 278, 127828 (2023). pp. 1-12. DOI:10.1016/j.energy.2023.127828.

[9] T.O. Aro, O. Matiluko and I.S. Olatinwo. “Dual feature extraction techniques for iris recognition system”. International Journal of Computer Systems & Software Engineering. Vol. 5, no. 1 (2019), pp. 1–15. DOI: 10.15282/ijsecs.5.1.2019.1.0051

[10]F. Mary Harin Fernandez, A. Ganesh Ramachandran, S. K. Saravanan, M. Bhanumathi et al. "Advancements in Object Detection for Accurate and Efficient Visual Recognition Using Machine Learning". Second International Conference on Advances in Information Technology (ICAIT), (2024), pp. 1-6, DOI: 10.1109/ICAIT61638.2024.10690296.

[11] R.Sarasu, Sunil Kumar, M. Thomas, L. Shymala et al. “Optimizing Healthcare Service Delivery using Improvised Fuzzy Logic Algorithm”. Informing Science: International Journal of Emerging Trans discipline, Vol. 28, no. 1 (2025), pp. 1-15. DOI: 10.28945/541

[12]A.F.M. Raffei, S.Z. Dzulkifli and N.S.A. Rahman. “Template matching analysis using neural network for mobile iris recognition system”. IOP Conference Series: Materials Science and Engineering, 769 (2020), 012024. DOI:10.1088/1757-899X/769/1/012024

[13]Reena Garg, Gunjan Singh, Aditya Singh and Manu Pratap Singh. “Fingerprint recognition using convolution neural network with inversion and augmented techniques”. Systems and Soft Computing, vol. 6, (2024), 200106. DOI: 10.1016/j.sasc.2024.200106

[14] S. Aghalya, R. Sarasu, N. Mishra, Arunachalam et al. “Tele-Rheumatology-Advanced Neural Network Model for Remote Assessment and Management of Rheumatic Conditions”. In 2024 10th International Conference on Communication and Signal Processing (ICCSP), (2024), pp. 453-458, IEEE. DOI: DOI: 10.1109/iccsp60870.2024.10543749