# Multi-Instance Cancelable Biometric System using Convolutional Neural Network

K N GANESH
NNM22MC030

# INTRODUCTION

- Cancelable or Revocable biometrics is a recent trend to safeguard a biometric system from a variety of attacks.
- We propose a cancelable system in which iris features are extracted through deep learning and then converted into a cancelable biometric template through random projection method.

# Unimodel v/s Multi-Instance

## Unimodel

- A unimodel biometric system utilizes a single biometric trait for identification or authentication
- It relies on a **single source** of biometric data
- The system extracts features from the chosen biometric trait and matches them against the stored templates

## Multi-Instance

- A multi-instance biometric system combines multiple biometric traits or sources
- It leverages **multiple sources** of biometric data- can be from the same biometric trait or different
- The system integrates the information from different sources to generate a more comprehensive and reliable representation

# Literature Review

| Year | Title | Author | Methodology | Findings/Result | Accuracy | conclusion |
|---|---|---|---|---|---|---|
| 2021 | Multi-instance Cancelable Biometric System using Convolutional Neural Network | Tanuja Sudhakar<br><br>Marina Gavrilova | CNN | High accuracy results due to poweful deep neural network architecture implemented. It is also found that random projection increases recognition rate considerably apart from providing biometric transformation. Various machine learning classifiers were compared for optimal performance in user verification. | 0.9803 | A multi-instance CB model has been explored using deep learning, random projection and machine learning. We find our system to be non-invertible, cancelable, differentiable and time efficient |
| 2015 | Cancelable Biometric | Vishal M. Patel<br><br>Nalini K. Ratha<br><br>Rama chellappa | Random Projection | Different Methods | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| 2022 | Block - XOR based cancellable template protection scheme for multi-instance iris biometric system | Shehla Rafiq<br><br>Arvind Selwal | Block – XOR | Able to generate different versions of cancellable templates by including different keys and by changing the block size i.e. by changing the number of bits taken per block. | 0.8873 | This paper meets the challenge of securing the important information extracted from the biological individuality like Iris before storage into the database. |
| 2021 | Privacy-preserving and verifiable multi- | Mahesh Kumar Morampudi Munaga | Public auditor | multi-instance iris authentication system, namely PviaPA is proposed to provide privacy to | 0.8002 | |

# Multi-Instance in Iris Biometrics

- A multi-model system can involve using multiple iris recognition algorithms that employ different approaches or feature extraction techniques.
- For instance, the system may combine algorithms based on texture analysis, phase-based methods, wavelet analysis, or deep learning architectures.
- Each algorithm can extract unique features from the iris images, and their results can be fused or combined to generate a more reliable and accurate identification or authentication decision.

# PROPOSED METHOD

- Deep learning architecture of Convolutional Neural Network (CNN) is utilized for iris feature extraction
- The proposed CNN greatly reduces number of feature dimensions from 16,384 to 256, thereby eliminating the need to use techniques like Principle Component Analysis (PCA) for dimension reduction.
- In our work, we propose to extract iris features from final ‘dense’ layer of the CNN. The ‘convolution layer’ along with ‘maxpool’ work together to generalize local features into more global features for better recognition. We optimize our CNN model using ‘RMS prop’ to monotonically decrease neural network's learning rate.

- We further use Random Projection (RP) and fuse the projection matrices to achieve a cancelable template that is hard to invert.
- We find that the CB template is computationally infeasible to invert even if an adversary possesses userkey, cancelable template or both.
- For user verification, we employ Support vector machines due to superior performance over K-Nearest Neighbor (kNN), Decision Trees (D-Trees) and Gaussian Naive Bayes classifiers.
- Results presented in the experimental section demonstrate that the proposed method increases recoverability and reliability of a CB system while preserving privacy.

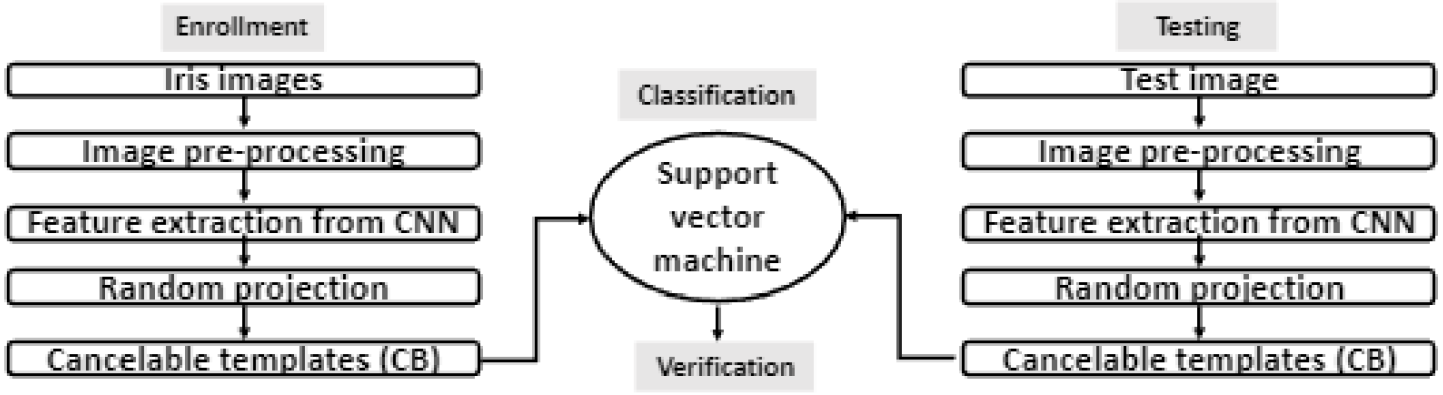



Figure 1: Flowchart of the proposed cancelable biometric system.

The proposed system has four major phases:

- Feature extraction: features of right and left irises are extracted using CNN. Feature extraction further comprises of five steps:
  - a) Rescaling
  - b) Pixelating
  - c) Normalization
  - d) CNN training and testing and
  - e) Feature extraction based on CNN.
- Transformation: RP is applied to the feature matrix to generate the cancelable template.
- Fusion and
- Testing phase.

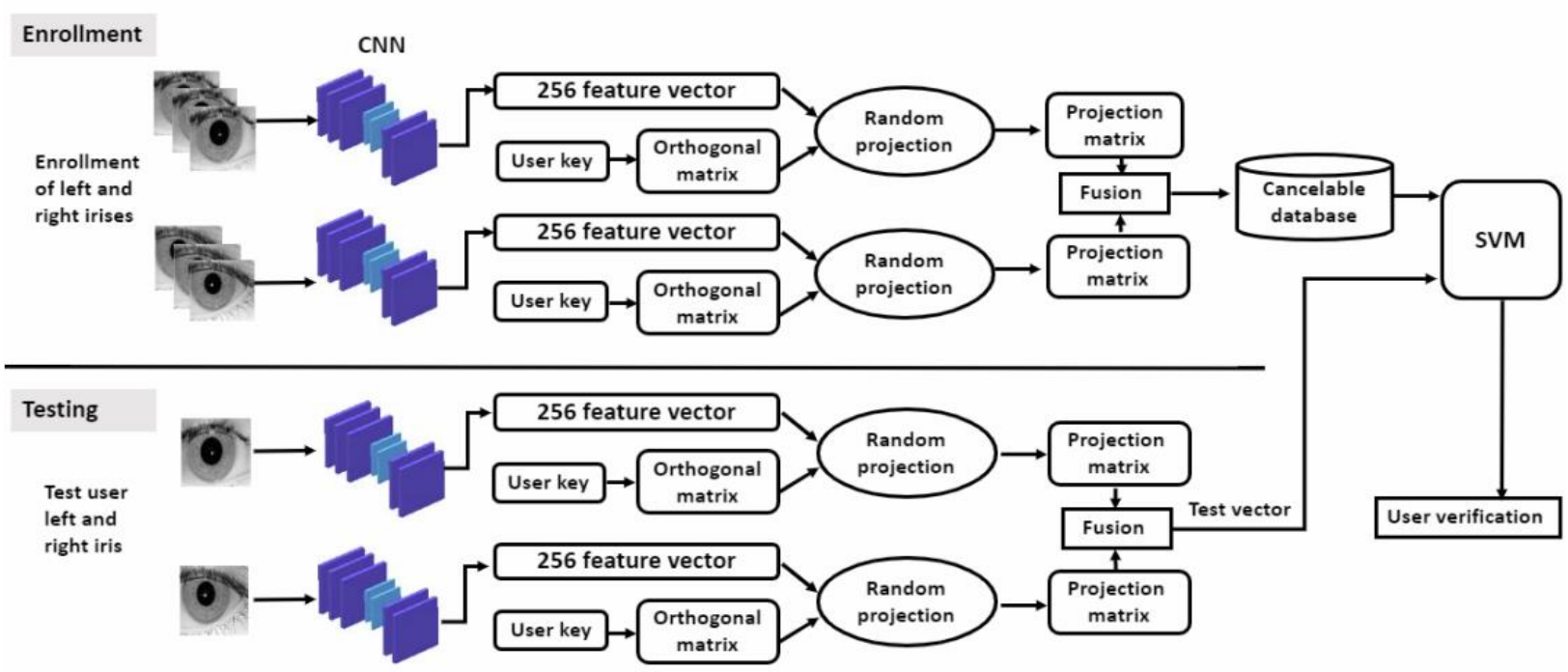



Figure 2: Overall architecture of the proposed cancelable biometric system.

Feature Extraction:

At the first stage, iris images of all users are converted to grey scale and rescaled to 128x128 pixels. Square shaped images are generally preferred for training to reduce errors and control shape of output.

Linear normalization of a digital grey-scale image is carried out using formula:

$IN = (I - Min)\ newMax - newMin\ /Max - Min + newMin$

It transforms a grey scale image,

$I : \{X \subseteq R\ n\} \rightarrow \{M\ in, \ldots, M\ ax\}$

with intensity values in the range(Min, Max), into a new image

$IN : \{X \subseteq R\ n\} \rightarrow \{newMin, \ldots, newMax\}$

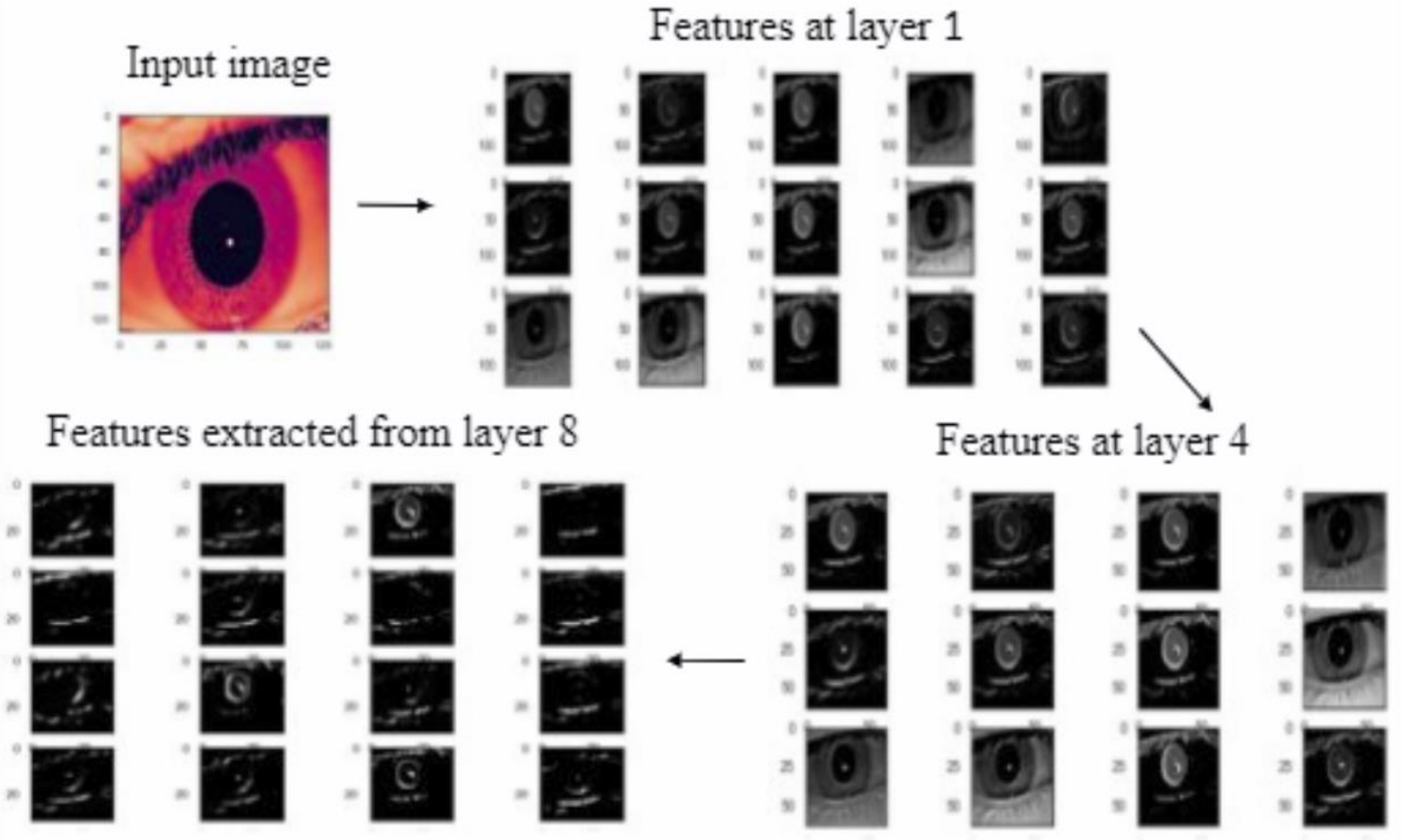



Figure 4: Features extracted at various stages of the neural network.

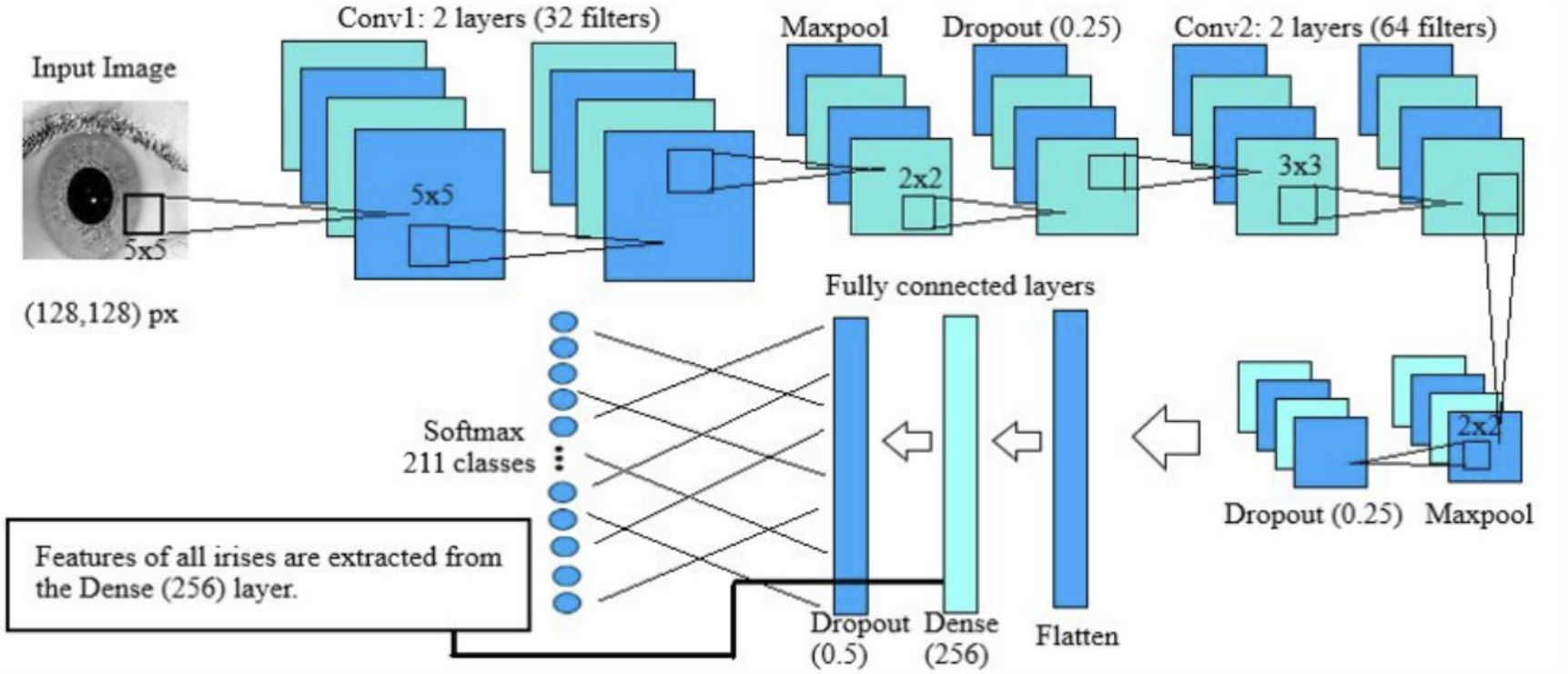



Figure 3: CNN architecture for feature extraction from irises.

## Random Projection (RP) :

RP has been utilized to create the cancelable template.

## Proposed technique comprises of three steps (Figure.5):

- a) Generation of an orthogonal matrix based on an userkey that is common for both left and right irises of a subject
- b) Multiplication of feature matrix to the orthogonal matrix to get a projection matrix and
- c) Multiplication of left and right iris projection matrices to obtain the cancelable template.

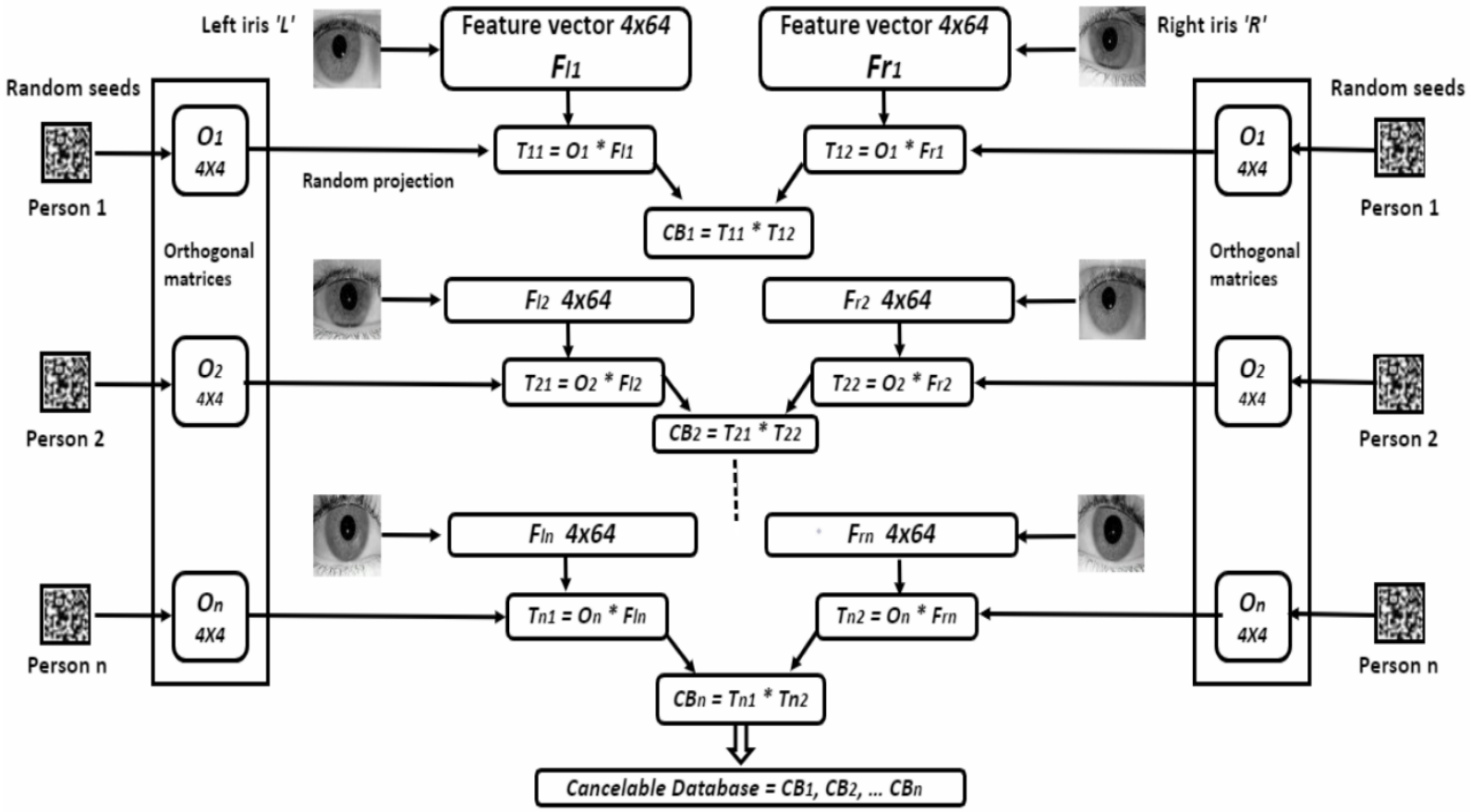



Figure 5: Generation of cancelable template using proposed random projection method.

## Process of Random Projection:

i) Let Fl and Fr be feature vectors where l and r denote left and right iris respectively.

ii)Let O be an orthogonal matrix generated from the userkey R.

The set of random matrices generated are

(O = O1, O2, O3 ... On).

The projection matrix for each user is given by

Tn1 = On * Fln and Tn2 = On * Frn

The two projection matrices are then multiplied

CBn = Tn1 * Tn2

to obtain the cancelable template for each user.

The final cancelable templates are then stored as the database

(CB = CB1, CB2, CB3 ... CBn).

## Classification:

- Performing  a comparative study of SVM, k-NN, D-Tree and Naive Bayes for user verification in the testing phase.
- Multi-class linear Support Vector Machine (SVM) is chosen due to its better performance compared to other classifiers.
- SVMs are supervised learning algorithms used for classification and regression analysis.
- SVM works by constructing hyperplanes to classify data into different sets.
- The model built by SVM assigns test data to one of the categories, making it a linear classifier.
- SVM is non-probabilistic in nature, meaning it does not provide probabilistic outputs.
- The optimal differentiator in SVM is a hyperplane that maximizes the gap between data clusters.
- The proposed linear SVM is implemented using Python's Scikit-Learn library.
- The performance of the linear SVM model is evaluated using 5-fold cross-validation.

# EXPERIMENTS:

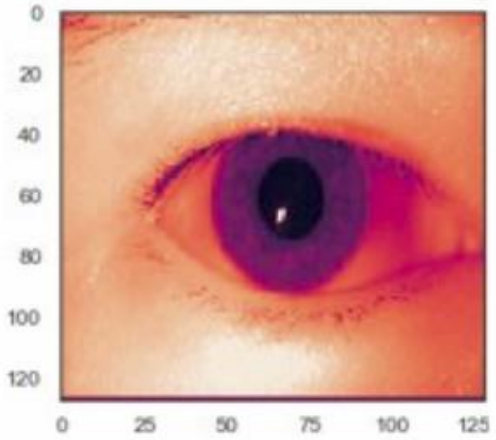
Experimental Setup:

Iris data was acquired from IIT Delhi Database (Version 1.0)

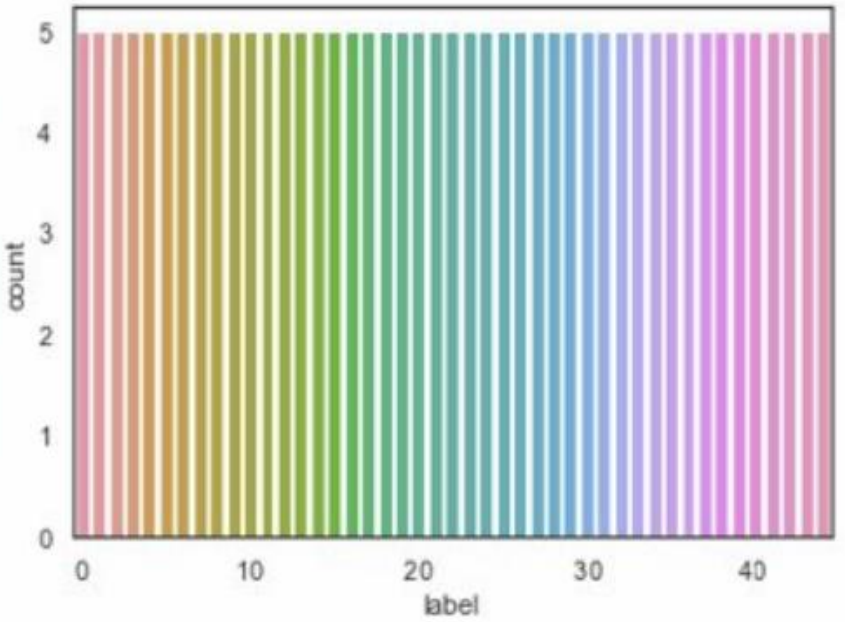
176 males and 48 females in the 14-55 age bracket were studied. Each image (320x240 pixels, 225kb) was resized to 128x128 pixels of 17kb each.

MMU was another dataset of 45 individuals obtained from Multi-media University .

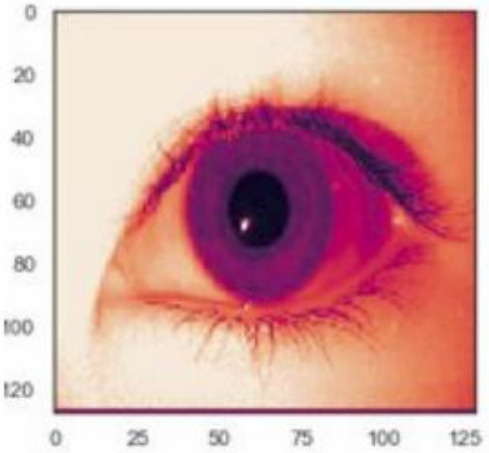
Images were pre-processed (grey scaled, rescaled and pixelated) and augmented by horizontal flips, vertical flips, random crops and rotations.



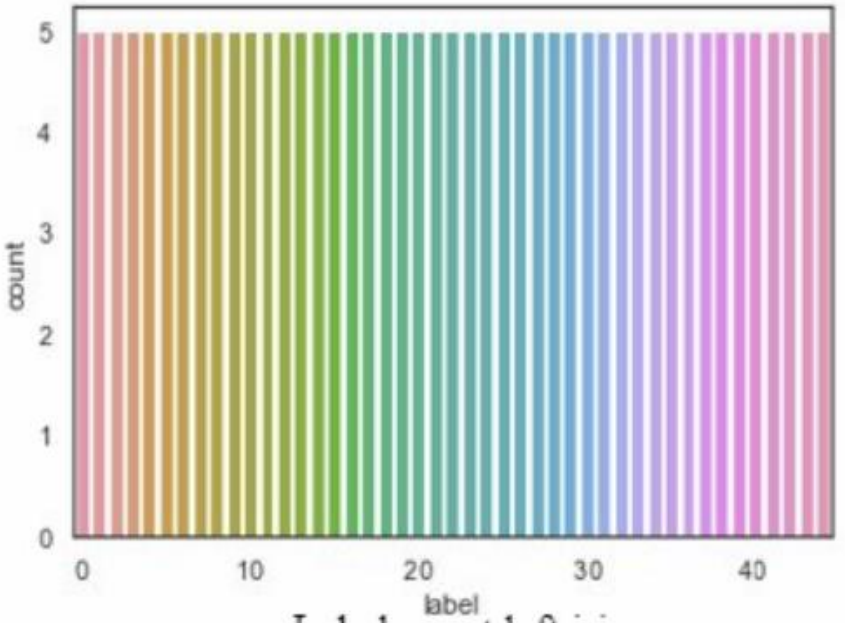

Sample right iris




Label count right iris




Sample left iris




Label count left iris

# Experimental Result:

Table I: CNN Performance - Accuracy and loss over 3 trails on IIT and MMU datasets.

| | Run 1 | | | | Run 2 | | | | Run 3 | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Epoch 1 | | Epoch 20 | | Epoch 1 | | Epoch 20 | | Epoch 1 | | Epoch 20 | |
| | Loss | Acc | Loss | Acc | Loss | Acc | Loss | Acc | Loss | Acc | Loss | Acc |
| Left Iris IITD | 6.5527 | 0.0032 | 0.1209 | 0.9600 | 6.5755 | 0.0011 | 0.1033 | 0.9663 | 6.8769 | 0.0074 | 0.0868 | 0.9737 |
| Right Iris IITD | 6.6336 | 0.0032 | 0.1046 | 0.9781 | 6.7087 | 0.0032 | 0.0582 | 0.9810 | 6.7919 | 0.0053 | 0.0587 | 0.9820 |
| Left Iris MMU | 4.3933 | 0.0141 | 0.1297 | 0.9507 | 4.6463 | 0.0001 | 0.1990 | 0.9607 | 6.3268 | 0.0070 | 0.0689 | 0.9859 |
| Right Iris MMU | 4.3281 | 0.0111 | 0.1620 | 0.9533 | 6.1432 | 0.0167 | 0.1159 | 0.9556 | 5.5189 | 0.0222 | 0.1195 | 0.9611 |

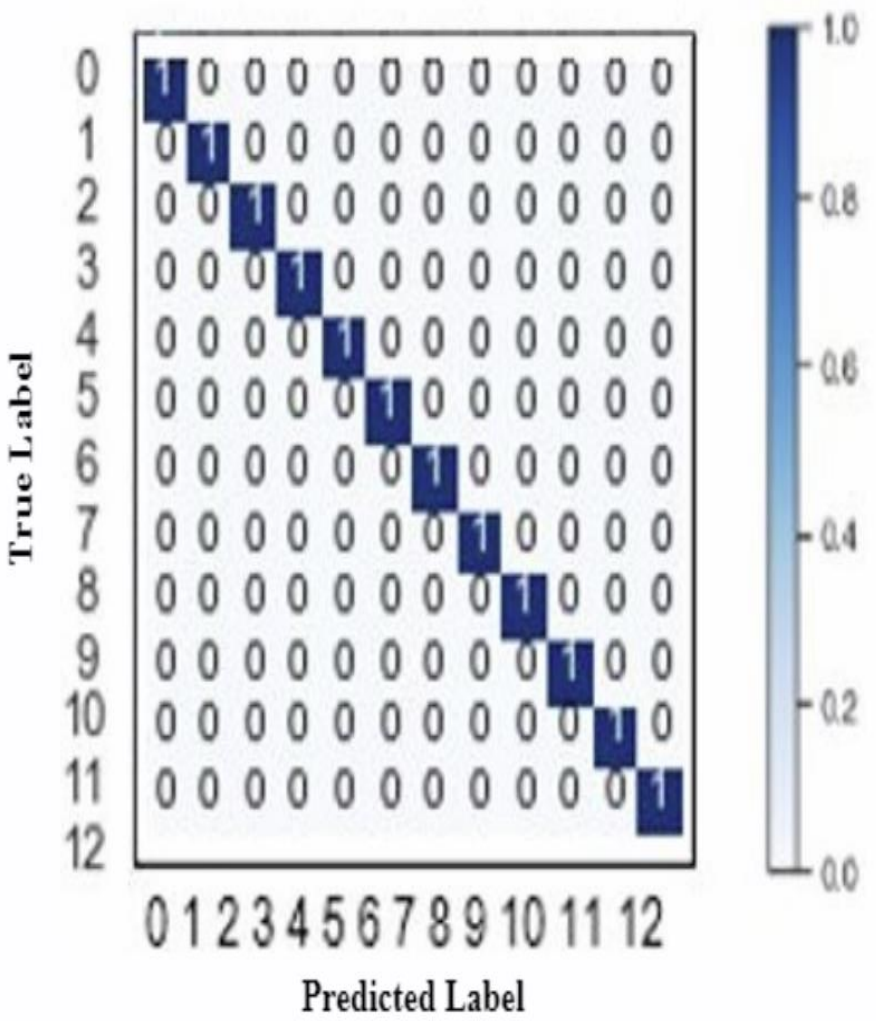
Table III: Results for SVM on IITD and MMU datasets.

| | IITD | | | MMU | | |
|---|---|---|---|---|---|---|
| | Precision | Recall | F1-score | Precision | Recall | F1-score |
| Micro-avg | 0.98 | 0.98 | 0.98 | 0.90 | 0.90 | 0.90 |
| Macro-avg | 0.98 | 0.98 | 0.98 | 0.86 | 0.84 | 0.84 |
| Weighted-avg | 0.98 | 0.98 | 0.98 | 0.96 | 0.90 | 0.91 |

Table IV: Comparison of four ML classifiers on cancelable biometric data.

| | EER IITD | EER MMU |
|---|---|---|
| Decision Tree | 0.35 | 0.45 |
| Gaussian Naive Bayes | 0.33 | 0.42 |
| k-Nearest Neighbor | 0.15 | 0.20 |
| **SVM (proposed)** | **0.12** | **0.15** |

Confusion matrix for first 12 labels IITD




Confusion matrix MMU

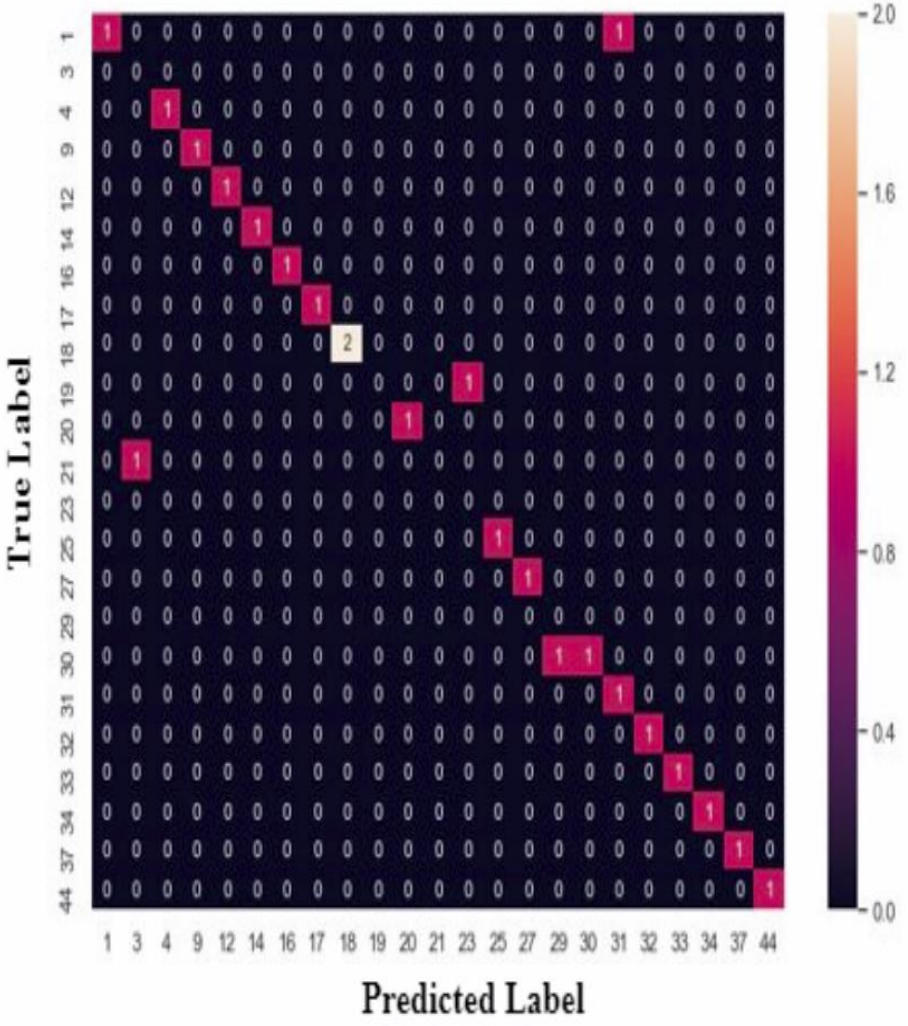
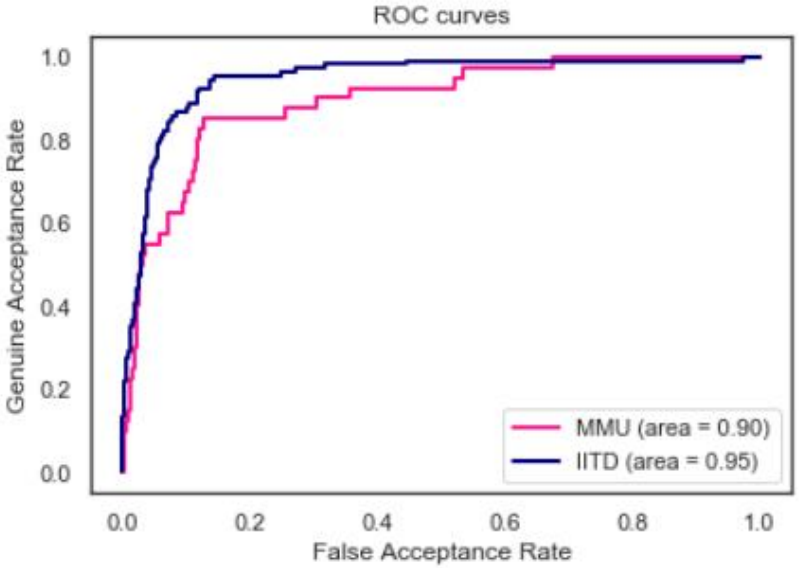
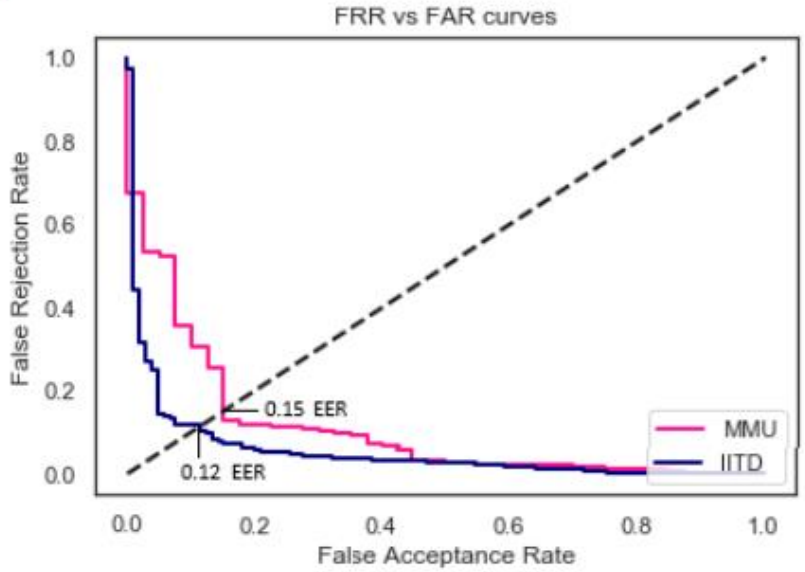


Table V: Comparison with other feature extraction methods.

| Dataset | Method | EER |
|---|---|---|
| IITD | Log Gabor [9] | 0.38 |
| | **Proposed method** | **0.12** |
| MMU | Raw Pixel Intensities [22] | 0.767 |
| | 5x5 Blocks of Avg Pixel Intensities [22] | 0.869 |
| | Gabor + PCA | 0.51 |
| | Log Gabor | 0.42 |
| | **Proposed method** | **0.15** |




(a) GAR vs FAR curves for MMU and IITD (on final cancelable dataset).




(b) FRR vs FAR and EER for MMU and IITD (on final cancelable

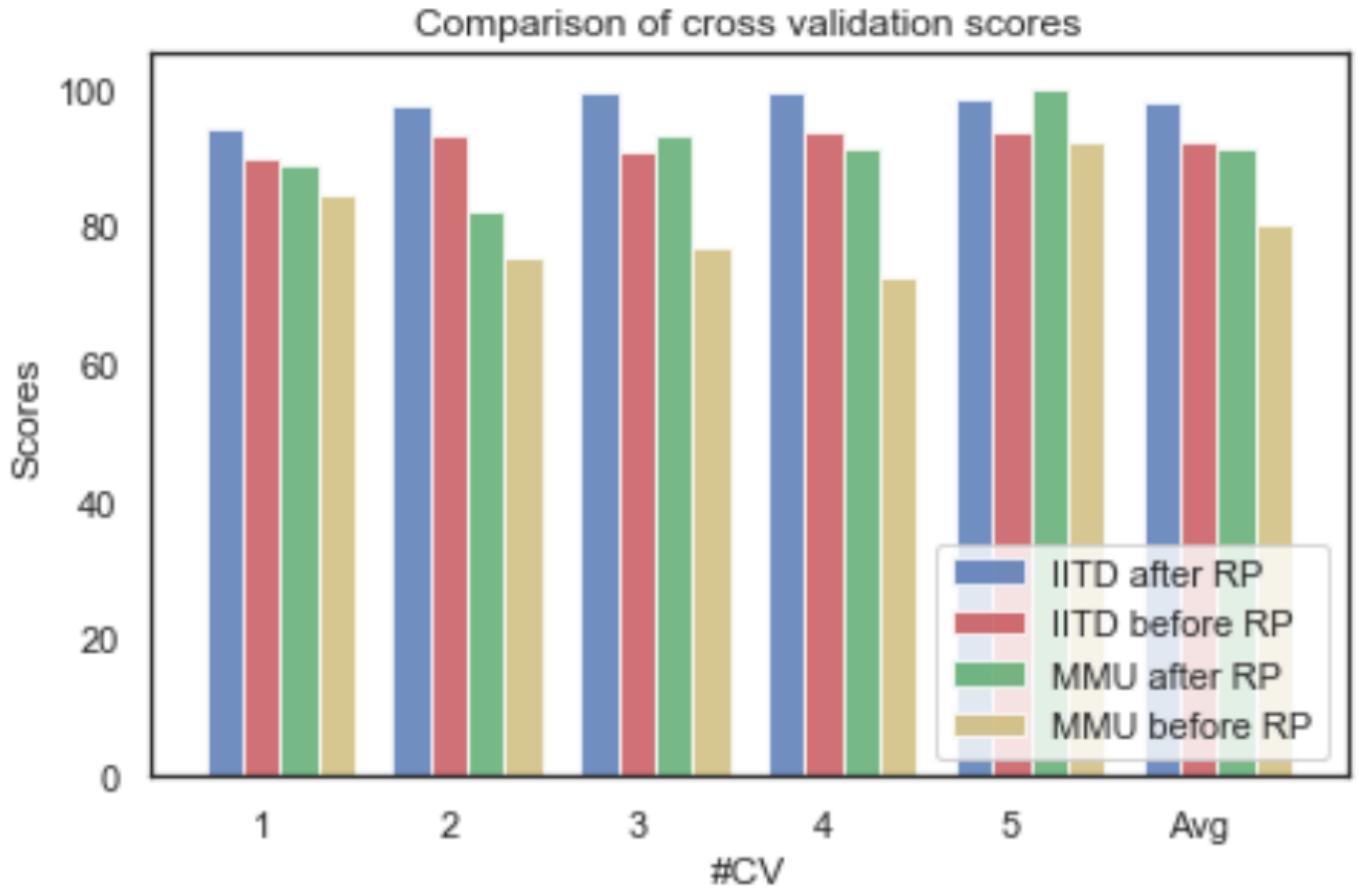



Figure 10: Cross validation scores for IITD and MMU datasets.

## Non-Invertibilty Analysis:

Reconstruction of (T11 and T12) of size (16x16) each is nearly impossible from a single matrix (CB1) of order (16x16). Number of possible combinations are huge due to decimal nature of the matrices .

Templates are also transformed by orthogonal transformation prior to the matrix multiplication (∇1) by means of an orthogonal matrix (also consisting of 10 digit decimal values in each cell) generated from userkey. It thus would be difficult to generate the exact orthogonal matrix even with the userkey. This combination of the two transforms ∇1 and ∇2 make it a secure technique with very little risk of template inversion.

## CONCLUSION:

A multi-instance CB model has been explored using deep learning, random projection and machine learning. We find our system to be non-invertible, cancelable, differentiable and time efficients. Future work will explore larger datasets with varied data quality as well as compare performance on diverse CNN architectures.

Thank -You