

An Improved PCA based Zero Crossing Feature Extraction For Real- Time Biometric Iris Authentication In low Power Resource Constrained Mobile Devices

Sujithra. M* and Padmavathi. G**

**Assistant Professor, Dept of Computer Technology & Applications,
Coimbatore Institute of Technology, Coimbatore, India.*

Email: sujisrinithi@gmail.com

***Professor & Head, Department of Computer Science,
Avinashilingam Institute for Home Science and Higher Education for Women,
Coimbatore, India.*

Abstract

In an era of communication technology, mobile devices such as smart phones and tablets being smaller and powerful performs wide range of applications, as a result many users stores personal information and business data such as email addresses, contact numbers, credit card access numbers etc. As the functionality of mobile devices increases, there is a greater need to protect the data from unauthorized access and threats. User authentication is an essential security measure for protecting the information from unauthorized access. We proposed a framework for establishing a reliable authentication mechanism through implementing an Iris biometric user authentication. Experimental results are presented to validate this framework using iris, and the results show that the proposed system can be deployed on mobile phones to significantly reduce the false rates of a single biometric system. The proposed solution is implemented as an Android application.

Keywords: Biometric Iris, Mobile Device, security, Authentication

Introduction

Mobile device such as smart phones and tablets are given rise to many applications such as mobile banking, email, contactless payment, mobile marketing, social networking, financial services, healthcare services, corporate applications, and many others etc. This evolution of functionality increases serious threats to information security and user privacy. It is necessary to ensure the security to the data and information stored in the Mobile Devices. Authentication for mobile device provides increase security beyond secret-knowledge techniques, transparent authentication

which authenticates the user continuously/periodically throughout the day in order to maintain confidence in the identity of the user [3]. Identifying people and protecting access or privileges to specific resources are among current needs of modern society. Person identification security practices have involved the use of three authentication methods:

Knowledge-based: Something you know, which typically relies on a memorized password or a PIN. What a person knows, for example, a password or personal identification number

Object-based: Something you have or possess, which relies on a physical possession such as tokens, credit card.

Identity-based: Something you are, i.e. biometrics, which relies on the uniqueness of physical or behaviour characteristics of a person such as fingerprint, facial features, iris, or voice to identify individuals.

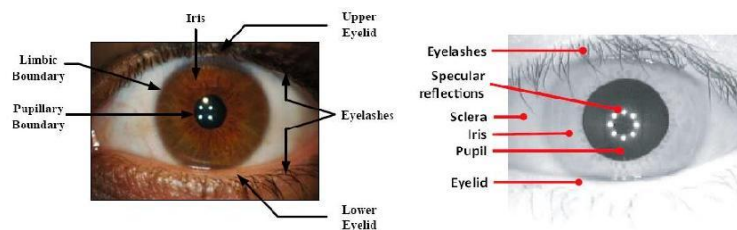


Figure 1: Iris images

Biometric verification has proven to be effective in verifying a person's identity without the possibility of forgetting a password. By adding strong security to mobile phones using unique individual features, biometrics on mobile phones will facilitate trustworthy electronic methods for commerce, financial transactions and medical services. Biometric systems are used for two purposes [1].

Verification: This is a process of confirming identity of any person by comparing the input data with ones existing in database. This is 1:1 authentication method. One is to verify that the user is genuine by comparing the acquired biometric trait with the one stored for that user.

Identification: In this case we are matching the input data with all samples in the database with a view to retrieving the data related for the person. This system represents the 1: N authentication model. The other purpose the biometrics are used is to identify a user in which case the acquired biometric trait is compared with a collection of the same traits from multiple users [2].

Biometric systems on Mobile devices is that the entire biometric system resides on the mobile device as a standalone system and it serves the purpose of preventing unauthorized access to mobile device personal information and business data. The physical characteristics of a person like finger prints, hand geometry, face, voice and iris are known as biometrics. Each biometric trait has its strengths and weaknesses. Except few from these traits, more number of biometric traits could be implemented on Mobile devices. Comparing all those traits, iris recognition is considered as the

best trait used for authentication in Mobile devices. Figure 1 represents iris images. Since iris patterns are unique in nature with high accuracy and robustness. Generally, several key factors should be considered when implementing such biometrics within Mobile devices. These factors will include user preference, accuracy and the intrusiveness of the application process. Table 1 illustrates the factors of biometric traits.

Table 1: Illustrates How These Factors Vary For Different Types of Biometrics

Attributes Vs Security Solutions	Fingerprint	Voice	Face	Iris	Gait
Types of Biometric	Image based	Voice based	Image based	Image based	Image based
Required Hardware	Fingerprint sensor hardware	Any standard telephone	Digital camera	Digital camera	Digital camera
Affecting Factors	Cleanliness and the pressure of the fingers. Severe injury of fingers	Ages and behave our like Cold& mood Surrounding noise/sound	Lighting, weather, and coverage of the face.	Usage of reading glasses, sun glasses, and health issue with eye scan affect Iris recognition	Drunkenness Injuries Speed of walking
Accuracy (Success Rate)	Higher very high (upto81%)	Medium (N/A)	Medium High(69%)	Very High (upto96%)	Medium
Limitations	The quality of fingerprint images	Input voice quality and users " speech patterns	Facial image quality	Capturing the iris image may need some practice.	Holding Accelerometers in different places and positions
Ease of Use	High	High	Medium	Low	Low
Cost	Low	Low	Low	High	High

This paper describes an approach to adapt iris recognition for resource-constrained mobile phones by reducing its computational complexity. Until now, iris recognition has been used in many fields. Recently, there have been attempts to adopt iris recognition technology for the security of mobile phones. Due to its complex texture, the iris has great potential as a biometric recognition modality. Iris Recognition has proved to be a reliable and nearly perfect biometric authentication technique. For more than 15 years now, researchers have developed a large number of different methods for IR which showed excellent performance. However, in a less constrained environment, such as capture by a low resolution camera of a mobile phone or PDA, or capture at a distance from a fixed surveillance camera, obtaining the image of an iris (which has a diameter of approximately 1 cm) of appropriate quality. The accuracy of iris recognition systems is proven to be much higher compared to other types of biometric systems like fingerprint, hand geometry, face, voice etc.

Related Works

Iris recognition in mobile devices is used to authenticate the users of the mobile device, by restricting the unauthorised access to the mobile device. Various approaches have been proposed by different authors for iris authentication in mobile devices based on their characteristics. Some of them are discussed below.

D. Cho et al considering the limited computing power of mobile devices, a new pre-processing method for iris localization is proposed. This uses the information of the pupil and iris along with its characteristics of the eye image. Experiment results shows that the proposed iris pre-processing method is performing well and stable across different iris databases.

K.R. Park et al based on corneal specular reflections for real-time pupil and iris detection method appropriate for mobile phones. Experimental results show a consequent accuracy of iris authentication.

Stan Kurkovsky et al proposed an approach to adapt iris recognition for resource-constrained mobile phones by reducing its computational complexity. Experimental results indicate adequate run time and quality of recognition that is comparable to other, more complex iris recognition systems developed for mobile devices with less EER rate.

Jin-Suk Kang analysed with a pre-processing method with noise detection in mobile device environment and provided good foundation towards developing an accurate portable Iris Recognition System. Classification accuracy is achieved by minimizing the false positive rate.

Qian Tao and Raymond Veldhuis use fusion, illumination, registration, verification. It produces face detection and registrations are still most time-consuming part, where, illumination normalization and verification components that are extremely fast.

Kremić, Emir and Abdulhamit Subaşi proposed a method in which PCA and Euclidean Distance are used this improves the security for mobile device authentication.

Iris authentication in mobile devices using different techniques and metrics is listed below. Table 2 summarizes the significant literatures reviewed for iris authentication in mobile devices.

Table 2: Literature Review on iris authentication in mobile devices

Sl. No.	Year	Author	Technique (s) used	Metrics Used	Observations
1	2006	D. Cho, K.R. Park, D.W. Rhee, Y. Kim, J. Yang	Threshold based binarization, Circular edge detection, Hough	Pixel Difference	The information of the pupil, iris and the characteristics of the eye images used to improve iris recognition performance.

			Transform		
2	2008	K.R. Park, H. Park, B.J. Kang, E.C. Lee, D.S. Jeong	On/off dual illuminator scheme, Ada Boost eye detector.	False accept rate (FAR), False reject rate (FRR), Equal error rate (EER)	Proposed a real-time pupil and iris detection method appropriate for mobile phones. But have to reduce processing time and to restore optical and motion blurred iris images.
3	2010	Stan Kurkovsky, Tommy Carpenter, Caleb MacDonald	Circular Hough transform, Gabor Filter, Hamming Distance.	False accept rate (FAR), False reject rate (FRR), Receiver Operating curve (ROC) Equal Error Rate (EER)	Adapt iris recognition for resource-constrained mobile phones. It has less computational complexity for implementing high accuracy iris recognition system.
4	2010	Jin-Suk Kang	Fixed focal length, Gaussian smoothing, BCH encoding function	Pupil Detection Rate, Iris Detection Rate, False Alarm Rate	Performance measured only using un-sharp masking algorithms. Not suitable for auto-focusing cameras in mobile devices.
5	2010	Qian Tao and Raymond Veldhuis	Haar Features, Adaboost, cascaded classifier	False acceptance rate (FAR) , False rejection rate (FRR)	Face detection and registration are still most time-consuming part, where, illumination normalization and verification components that are extremely complex.
6	2011	Kremić, Emir, and Abdulhamit Subaşi.	Principle Component Analysis & Euclidean Distance	Accuracy, Euclid distance measure	Improves the security of mobile devices with authorization and authentication in real time on Android Devices.

Iris Recognition Methodology

The ultimate aim of the proposed approach is to improve the overall authentication performance of mobile device security by using iris image and acquire better results than previous methods. The block diagram for the iris methodology is shown in Figure 2. In general, the process of iris recognition system consists of: Image acquisition, Image Pre-processing, Feature extraction and matching [5].

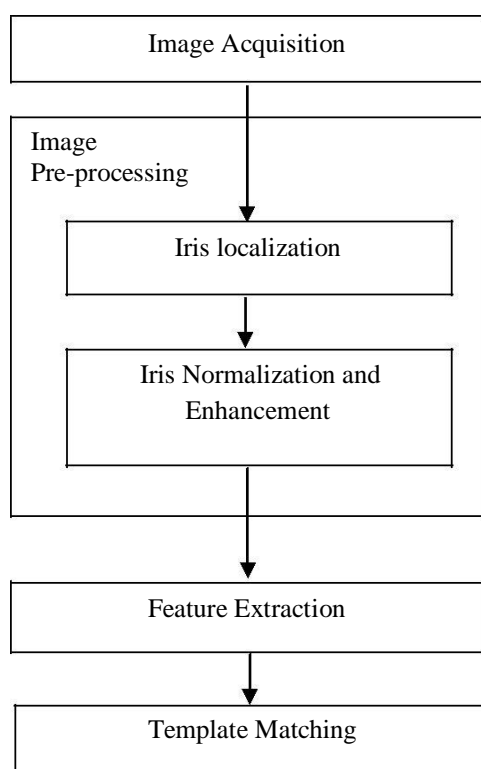


Figure 2: Iris Recognition

Image Acquisition

A biometric authentication system for a mobile phone will be used primarily in a verification mode when a biometric sample of the person trying to turn on or log in to the device is compared to that of a single rightful owner. With the integration of digital cameras that could acquire images at increasingly high resolution and the increase of cell phone computing power, mobile phones have evolved into networked personal image capture devices. The database used in the experiment was collected by the authors using a mobile phone equipped with 8 mega pixel photo camera. The motivation in collecting such a dataset is that there is no known publicly available iris

dataset acquired with the standard camera of a mobile phone. This dataset is called MSGP_Mobile Iris Database (MSGP_MID) and consists of 240 RGB colour images captured from 50 individuals enrolled using both eyes with 2 images/eye. The dimension of the images is 300 by 150 pixels and the iris diameter is around 100 pixels. The proposed solution is implemented here as an Android application. Its performances are evaluated on an own real time MSGP_Mobile Iris Database. The obtained experimental results indicate that the proposed method can be effectively employed to authenticate mobile phones users.

Image pre-processing

A high quality image of the iris has to be captured in order for the iris recognition system to work efficiently. The acquired image of the iris must have sufficient resolution and sharpness to support recognition. Besides, the acquired image also contains irrelevant parts (e. eyelid, eyelash, pupil, etc.) should be removed. For the purpose of analysis, the original image needs to be pre-processed. Iris image Pre-processing includes three stages, they are segmentation, normalization and contrast enhancement [6].

Iris localization

An eye image contains not only the iris region but also some parts that need to be separated from iris, such as the pupil, eyelids, and sclera. For this reason, at the first step, segmentation should be done to localize and extract the iris region from the eye image. Iris localization is the detection of the iris area between pupil and sclera. So it's needed to detect the upper and lower boundaries of the iris and determine its inner and outer circles. The first step in iris localization is to detect the outer radius of iris patterns [4]. The centre of iris can be used to detect pupil which is the black circular part surrounded by iris tissues. Because of the felicitous circular geometry of the iris the task of localizing the inner and outer boundary of the iris can be accomplished for a raw input image $I(x,y)$ by searching over the image domain (x,y) for the maximum in the blurred partial derivative, with respect to the increasing radius r , of the normalized contour integral of $I(x,y)$ along a circular arc ds of radius r and center coordinates (x_0, y_0) . Daugman (2002) proposed integro-differential operator to detect the centre and diameter of the iris and used the differential operators to detect the pupil. That is,

The Integro-Differential Operator is defined by the above equation

$$\max_{(r,x_0,y_0)} = G_\sigma(r) * \frac{\partial}{\partial r} \int_{r,x_0}^{y_0} \frac{I(x,y)}{2\pi r} ds \tag{1}$$

Where $I(x,y)$ is the Eye image, r is the radius, $G_\sigma(r)$ is a Gaussian Smoothing function, and s is the contour of the circle given by $(r,x_0 y_0)$. The operator searches for the circle path where there is maximum change in the pixel values by varying the radius and center x and y position of the circular contour. The integro differential operator is applied iteratively with the amount of smoothing progressively

reduced in order to attain precise localization and also eyelids are localized with the path of contour integration changed from circular to an arc.

Iris Normalization

The irises captured from the different people have different sizes. The size of the irises from the same eye may change due to illumination variations, distance from the camera, or other factors. At the same time, the iris and the pupil are non-concentric. These factors may affect the result of iris matching. In order to avoid these factors and achieve more accurate recognition, the normalization of iris images is implemented [7].

The homogenous rubber sheet model developed by Daugman remaps each point within the iris region to a pair coordinates (r, θ) where r is in the interval from 0 to 1 and θ is angle in the interval from 0 to 2π . The remapping of the iris region from (x, y) Cartesian coordinates to the normalized non-concentric polar representation is modelled as given by the equations 2, 3, and 4

$$I(x(r, \theta), y(r, \theta)) = I(r, \theta) \quad (2)$$

$$x(r, \theta) = (1-r) x_p(\theta) + r x_1(\theta) \quad (3)$$

$$y(r, \theta) = (1-r) y_p(\theta) + r y_1(\theta) \quad (4)$$

Where $I(x, y)$ is defined as the iris image, (x, y) are the original Cartesian coordinates, (r, θ) are the corresponding normalized polar coordinates, and the coordinates of the pupil and the iris boundaries along the θ direction as shown in Figure 3.

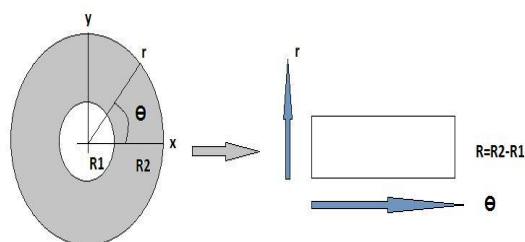


Figure 3: Rubber Sheet Model

This model takes into account Pupil dilation and size inconsistencies in order to produce a normalized representation with constant dimensions. The Iris region is modelled as a flexible rubber sheet anchored at the Iris boundary with the Pupil centre as the reference point. The segmented Iris image is normalized to a size 60×250 . Then the normalized image is given for enhancement. The normalized iris image obtained may not have uniform brightness due to position of light sources and also has low contrast. This may affect the subsequent processing in feature extraction and matching. Thus by enhancing the image by means of histogram equalization each of 32×32 regions produces compensation for the non-uniform illumination, as well as improves the contrast of the image. The enhancement process is done to make iris

visible clearly and to extract features from it. The histogram is produced for the iris image, which gives the detail of the dark and brighter part of the image. This is given for histogram equalization, where darker image pixels will be further darker and brighter image pixels becomes much brighter with a threshold value. This enhanced image is given for iris segmentation [8].

Proposed Methodology - Feature Extraction

Feature extraction is a special form of dimensionality reduction and contains more information about the original image. The input data which is to be processed is transformed into a reduced representation set of features. In order to recognize the individuals accurately, the most discriminating features that present in the region must be extracted. The significant features of the iris must be encoded so that comparisons between templates can be made. Iris provides abundant texture information. A feature vector is formed which consists of the ordered sequence of features extracted from the various representation of the iris images. Feature extraction identifies the most prominent features for classification [9].

A feature vector is formed which consists of the ordered sequence of features extracted from the various representation of the iris images. Some of the features are x-y coordinates, radius, shape and size of the pupil, intensity values, orientation of the pupil ellipse and ratio between average intensity of two pupils. The pseudo code for the proposed methodology is given in Figure 4.

```
Input: Eye image.  
Output: A unique feature vector represents the input eye image.  
  
Step 1: Eye image acquisition.  
Step 2: Iris localization.  
Step 3: Iris normalization.  
Step 4: Feature vector extraction using Zero crossing based 1-D wavelet.  
Step 5: Feature vector reduction using PCA.  
Step 6: Apply the pattern matching technique SVM with ED,  
{  
if the pattern exists in the iris DB:  
    Output the matching result (Authenticate the user)  
else  
    enroll the feature vector in the iris DB.  
}  
Step 7: End.
```

Figure 4: Pseudo Code - Proposed Methodology

The features are encoded to a format suitable for recognition. Feature extraction can be carried out using the following algorithms:

- Zero crossing based 1-D wavelet
- Colour Based Feature Extraction
- Principle Component Analysis

Zero Crossing Feature Extraction

This method represents features of the iris at different resolution levels based on the wavelet transform zero-crossing. The algorithm is translation, rotation and scale invariant. The input images are processed to obtain a set of 1D signals and its zero crossing representation based on its dyadic wavelet transform. The wavelet function is the first derivative of the cubic spline. The centre and diameter of the iris is calculated from the edge-detected image. The virtual circles are constructed from the center and stored as circular buffers. The information extracted from any of the virtual circles is normalised to have same number of data points and a zero crossing representation is generated. The representation is periodic and independent from the starting point on iris virtual circles. These are stored in the database as iris signatures. The dissimilarity between the irises of the same eye images was smaller compared to the eye images of different eyes. The advantage of this function is that the amount of computation is reduced since the amount of zero crossings is less than the number of data points [10].

$$\Delta I = \frac{\partial^2}{\partial x^2} I(x, y) + \frac{\partial^2}{\partial y^2} I(x, y) \quad (5)$$

Colour Based Feature Extraction

Feature extraction using colour based information of iris gives the colour saturation values which is different for each person's when detected absolutely. Here, Colour spaces used in Iris colour segmentation include YCbCr, HSV and RGB. Iris Colour Image is initially in RGB colour space then they are converted into HSV colour space and mean, standard deviation and variance are calculated. In this work, HSV (hue, saturation and value) colour representation is taken because it is compatible with human colour perception and it is obtained by the non-linear transformation of fundamental RGB colour space. Here use the cone representation of HSV colour space, where H, S and V are all normalised in the range [0,1]. The H and S components represent the chromatic information, while V represents the luminance information. This information is taken as a colour features taken with edge based features taken using Zero Crossing feature extraction given for the iris detection [11]. The R, G, B values are divided by 255 to change the range from 0.255 to 0.1:

$$R' = R/255$$

$$G' = G/255$$

$$B' = B/255$$

$$C_{\max} = \max(R', G', B') \quad (6)$$

$$C_{\min} = \min(R', G', B') \quad (7)$$

$$\Delta = C_{\max} - C_{\min}$$

$$\text{Hue calculation: } H = \begin{cases} 60^\circ \times \left(\frac{G' - B'}{\Delta} \bmod 6 \right), C_{\max} = R' & (8) \\ 60^\circ \times \left(\frac{B' - R'}{\Delta} + 2 \right), C_{\max} = G' & (9) \\ 60^\circ \times \left(\frac{R' - G'}{\Delta} + 4 \right), C_{\max} = B' & \end{cases}$$

Saturation calculation:

$$S = \begin{cases} 0, \Delta = 0 \\ \frac{\Delta}{C_{\max}}, \Delta <> 0 \end{cases} \quad (10)$$

Value calculation:

$$V = C_{\max} \quad (11)$$

Then for the conversion of RGB to YCbCr, YCbCr is an encoded nonlinear RGB signal used for image compression work. Colour is represented by luma computed from nonlinear RGB. RGB components convert to YCbCr by Equation:

$$\begin{aligned} Y &= 0.299R + 0.587G + 0.114B \\ Cb &= -0.169R - 0.332G + 0.500B \\ Cr &= 0.500R - 0.419G - 0.081B \end{aligned}$$

By obtained values for Y, Cb and Cr the YCbCr image is formed. And the best threshold result were found by using following rule for detecting the Iris pixels are:

$$\begin{aligned} 135 &< \square < 145 \\ 100 &< \sqcap < 110 \\ 140 &< \square \sqsupset < 150 \end{aligned}$$

The YCbCr colour space is obtained by multiplying the RGB region with some constant values. The constant values are given above and the threshold values for each colour space are also specified. The feature values in different colour space vary according to the image, so in order to extract the feature values the colour transformation is performed.

Principle Component Analysis

Principal Component Analysis is a linear transformation and it is used to identify the patterns in the phase information obtained from the dyadic wavelet transform with colour based approach encoded data. Computation of PCA involves subtracting the mean from the given data, calculating the covariant matrix, calculating the eigenvectors and eigenvalues of the covariance matrix and finally the transpose of feature vector formed from eigenvectors are multiplied to the left of the original data set transposed. Principal components analysis searches for k n-dimensional orthogonal vectors that can best be used to represent the data, where $k \leq n$. The

original data are thus projected onto a much smaller space, resulting in data reduction [12].

Given a set of data, PCA finds the linear lower-dimensional representation of the data such that the variance of the reconstructed data is preserved. Using a system of feature reduction based on a combined principle component analysis on the feature vectors that calculated from the wavelets limiting the feature vectors to the component selected by the PCA should lead to an efficient classification algorithm utilizing supervised approach. Therefore, the feature extraction process was carried out through two steps: firstly the wavelet coefficients were extracted by the dyadic wavelet transform with colour based approach and then the essential coefficients have been selected by the PCA. Figure 5 illustrates the flow of the proposed work.

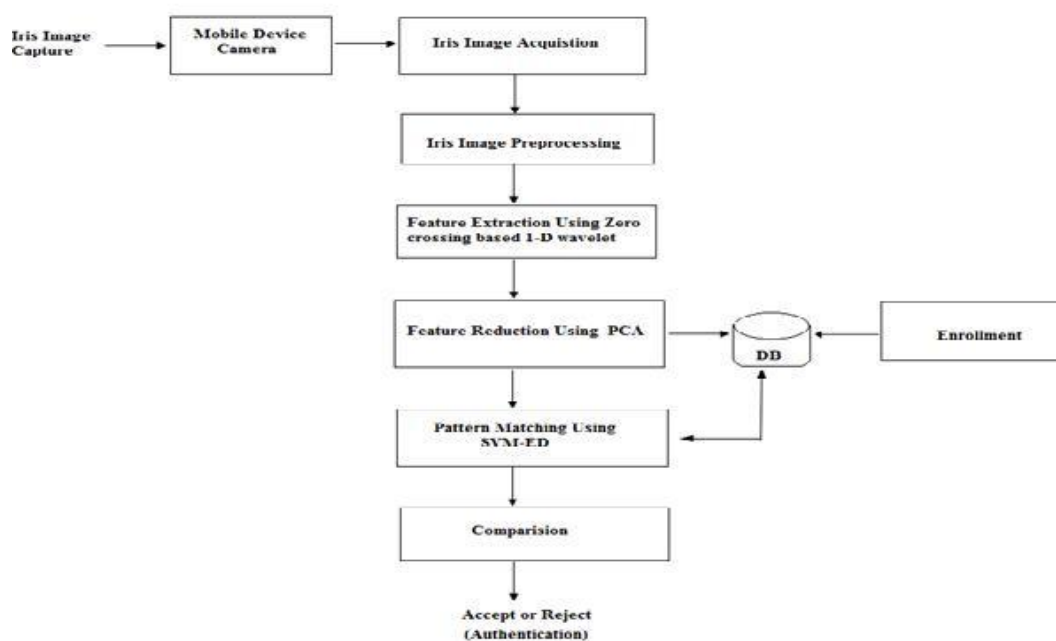


Figure 5: Flow Chart - Proposed Methodology

The obtained features dimensionality were further reduced by using principle component analysis (PCA), which drastically reduces the size of the iris database images and then improves the performance of the system. It minimizes the processing time and improves the accuracy in matching process by selecting the relevant features. So, the main idea behind using PCA in our approach is to reduce the dimensionality of the wavelet coefficients. This leads to more efficient and accurate classifier SVM with Euclidean Distance is used. This system show better result compared to other approaches. PCA effectively reduces the number of features and displays the data set in a low dimensional subspace [13]. The pseudo code for the PCA feature reduction is given in Figure 6.

Step 1: Get normalized data from the iris regions. 2-D iris image is represented as 1-D Vector by concatenating each row (or Column) into a long vector

Step 2: Subtract the mean image from each image vector. Step 3: Calculate the covariance matrix.

Step 4: Calculate the eigenvectors and eigenvalues of the covariance matrix.

Step 5: The eigenvectors are sorted from high to low according to their corresponding Eigenvalues. Choose components and forming a feature vector

Step 6: Deriving the new data set.

Figure 6: Pseudo code - PCA

Template Matching

Matching of an image to authenticate via identification (one-to-many template matching) or verification (one-to-one template matching), a template created by imaging the iris is compared to a stored value template in a database For the purpose of classification support vector machine was used as a main classifier while Euclidean Distance was used as a secondary classifier. The result of applying same feature for both the classifier (SVM and Euclidean Distance) has better recognition accuracy than using a single method.

The template matching compares the user template with the template from database using a matching metric. The matching metric compares similarity between two iris templates. When any iris comes into the system extract the important feature of that iris using zero crossing. These features are used for training and testing of the SVM. If correct classification is not done by SVM then Euclidean distance is used for further classification. For doing classification through SVM, various SVM models have been developed in training phase. If there are n classes then n SVM models are developed, one model for each class. Once training phase is completed, the testing or identification of human iris is done by testing the iris image against all n models [14].

The feature extracted values are split into training and testing. The splitting is done in the ratio of 50:50, 70:30, 60:40 (training and testing values) in the training phase the output of SVM will be a structured array. In the testing phase the results are produced for the given test data. The process is performed based upon the Euclidean Distance. This is distance measurement technique used here to find out the minimum distance between the feature and the SVM structure. The Euclidean distance between the points P and Q is the length connecting between them. In Cartesian coordinates if $P=(P_1, P_2, \dots, P_n)$ and $Q=(Q_1, Q_2, \dots, Q_n)$ are two points in Euclidean n-space, then the distance from P to Q or from Q to P is given by in equation:

$$d(P, Q) = \sqrt{(Q_1 - P_1)^2 + (Q_2 - P_2)^2 + \dots + (Q_n - P_n)^2} = \sqrt{\sum_{i=1}^n (Q_i - P_i)^2} \quad (12)$$

Which is used to find minimum distance between the testing feature and the structure, from this classification results are taken [15]. One of the methods used in SVM classification is one-against-all that has „n“ SVM models where „n“ represents the number of classes. The *i*th value in SVM is trained through all of the features in the *i*th class with positive labels, and the remaining with negative labels. Thus given one training data $(x_1, y_1), \dots, (x_l, y_l)$, where $x_i \in \mathbb{R}^n, i = 1, \dots, l$ and $y_i \in \{1, \dots, k\}$ is the class of x_i the *i*th SVM solves the following problem:

$$\min_{w^i, b^i, \xi^i} \frac{1}{2} (w^i)^T w^i + C \sum_{j=1}^l \xi_j^i (w^i)^T \tag{13}$$

$$(w^i)^T \phi(x_j) + b^i \geq 1 - \xi_j^i, \text{ if } y_j = i \tag{14}$$

$$(w^i)^T \phi(x_j) + b^i < -1 + \xi_j^i, \text{ if } y_j \neq i \tag{15}$$

$$\xi_j^i \geq 0, j = 1, \dots, l \tag{16}$$

Here, training data x_i will be mapped with the high dimensional space by the function ϕ and *C* is the penalty parameter.

Minimizing $\left(\frac{1}{2}\right) (W^i)^T W^i$ means maximizing $\frac{2}{\|w^i\|}$, and the margin between two data groups. When grouped data are not separable linearly, there is a penalty term $C \sum \xi^i (w^i)$ which can reduce the number of training errors. The fundamental conception behind SVM is to search for a balance between the regularization term $\left(\frac{1}{2}\right) (W^i)^T W^i$ and the training errors.

After solving (14), there are *n* decision functions

$$(w^1)^T \phi(x) + b^1 \dots \dots \dots (w^n)^T \phi(x) + b^n \tag{17}$$

Here *x* is in the class which has the largest value of the decision function class of $x = \text{argmax}_i ((w^i)^T \phi(x) + b^i)$ this process is carried out in

$$i = 1, \dots, \dots, \dots ((w^i)^T \phi(x) + b^i) \tag{18}$$

svm classification by means of training and testing phase where the input to the training and testing phase are the splitted data.

Experimental Results

The proposed method is evaluated using various parameters such as False Acceptance Ratio (FAR), False Rejection Ratio (FRR), Computational Complexity and Accuracy [16].

False Acceptance Rate (FAR)

The false acceptance rate is a unit used to measure the average number of false acceptances within a biometric security system. It measures and evaluates the efficiency and accuracy of a biometric system by determining the rate at which unauthorized or illegitimate users are verified on a particular system. It is calculated by the below equation

$$FAR(\%) = \frac{\text{Number of false acceptances}}{\text{number of total imposter attempts}}$$

The False Accept Rate (FAR) is the percentage of authentication decisions that allow access to an unauthorized user.

False Rejection Rate (FRR)

The False Rejection Rate is the probability that the system fails to detect a match between the input pattern and a matching template in the database. It measures the percent of valid inputs which are incorrectly rejected and it is calculated by below equation

$$FRR(\%) = \frac{\text{Number of false rejections}}{\text{number of total authentic attempts}}$$

The False Reject Rate (FRR) is the percentage of authentication decisions where an authorized user is denied access.

Accuracy:

$$Accuracy(\%) = \frac{TP + TN}{(TP + TN + FP + FN)}$$

It is calculated by the above equation, where True positive is correctly identified, False positive is incorrectly identified, True negative is correctly rejected and False negative is incorrectly rejected where TP is the Number of True Positive Instances, FN is the Number of False Negative Instances, FP is the Number of false Positive Instances, TN is the Number of True Negative Instances. Authentication accuracy indicates the possibility of correctly identifying an individual (including both imposters and legitimate users).

Computational Complexity:

It is the Time required to complete the whole process of a system. If the system takes much time, there the system will becomes complex system.

$$\text{Computational Complexity} = \text{Initial Time(ms)} - \text{Final Time (ms)}$$

Table 3: Parameters for Proposed Methodology

Parameters	Zero Crossing with SVM-ED	PCA - Zero Crossing with SVM-ED	Improvement (+/-)
Computational Complexity (ms)	53	50	3
FAR	0.0311	0.0225	0.0085
FRR	0.0335	0.0235	0.007
Accuracy (%)	95	97	2

Table 3 provide the comparison of parameters between existing Zero Crossing with SVM-ED and proposed PCA - Zero Crossing with SVM-ED. The given parameters are False Rejection Ratio (FRR) in (%), False Acceptance Ratio (FAR) in (%), Computational Complexity in (ms) and Accuracy in (%).

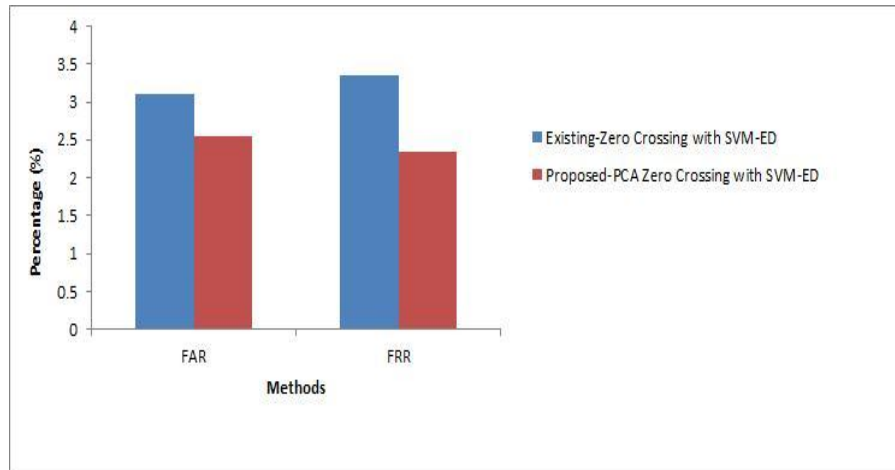


Figure 7: Comparison of FAR & FRR

The above Figure 7 illustrates the comparison between FAR and FRR for existing Zero Crossing with SVM-ED and proposed PCA - Zero Crossing with SVM-ED. It can be clearly observed that the proposed method of PCA - Zero Crossing with SVM-ED give better results compared to the existing method.

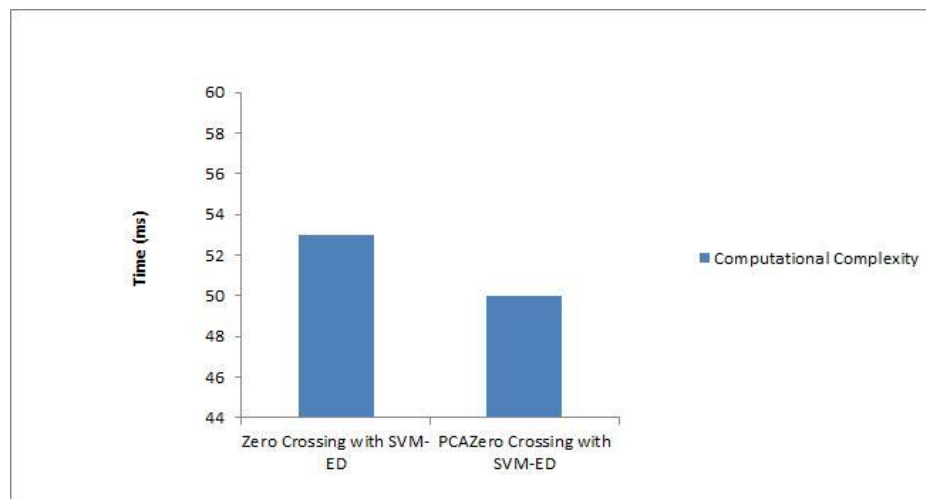


Figure 8: Computational Complexities

Figure 8 gives the Computational Complexity comparison between existing Zero Crossing with SVM-ED and proposed PCA - Zero Crossing with SVM-ED. From

Figure 8, it is clearly observed that the proposed PCA - Zero Crossing with SVM-ED provides improved 3ms result, that is less than existing method.



Figure 9: Overall Accuracy

Overall accuracy is shown in Figure 9 for existing Zero Crossing with SVM-ED and proposed PCA - Zero Crossing with SVM-ED. In this, accuracy attained by existing Zero Crossing with SVM-ED is 95 % and proposed PCA - Zero Crossing with SVM-ED is 97 %.

Conclusion

Mobile devices such as smart-phones, PDAs are vulnerable to theft and loss due to their small size and the environments in which they are used. Designing reliable user authentication on mobile phones is becoming an increasingly important task to protect user's private information and data. A robust algorithm has been introduced which reduces the size of the iris image database and correspondingly the computational cost with high accuracy. For Feature extraction and reduction Zero-crossing representation with PCA is used collectively. This feature vector of small size was inputted to SVM and Euclidean Distance classifier for the recognition purpose. The recognition accuracy for pattern classification is 97%.

The results obtained with the developed Android application, in real operating conditions are quite promising for a real time MSGP_ Mobile Iris Database (MSGP_MID) own made database. As the proposed system is mobile based, it is especially suited for scenarios, where there is a sudden or unexpected need to prove an identity or authenticate. The obtained results are encouraging and point out the feasibility of iris authentication in mobile phones. This work can be further extended in the aspect of providing authentication in unlocking the device using the iris of the user. From these experimental results have confirmed that the proposed method attain high performance in both speed and accuracy.

References

- [1] A.K. Jain and A. Kumar, "Biometrics of Next Generation: An Overview," *Second Generation Biometrics*, Springer, 2010.
- [2] Sujithra, M. and Padmavathi. G. Next generation biometric security system: an approach for mobile device security. In *Second International Conference on Computational Science, Engineering and Information Technology*, (New York, USA, 2012), ACM, 377 – 381.
- [3] M. La Polla, F. Martinelli, and D. Sgandurra, "A survey on security for mobile devices," *IEEE Communications Surveys and Tutorials*, vol. 15, no. 1, pp. 446-471, 2013.
- [4] Cho, D., Park, K. R., and Rhee, D. W.: Real-time iris localization for iris recognition in cellular phone. In *SNPD/SAWN*, pp. 254–259 (2005).
- [5] M. De Marsico, C. Galdi, M. Nappi, and D. Riccio, "FIRME: Face and Iris Recognition for Mobile Engagement," *Image and Vision Computing*, vol. 32, no. 12, pp. 1161-1172, 2014.
- [6] J. Daugman. High confidence visual recognition of persons by a test of statistical independence. *IEEE Trans. PAMI*, 15(11): 1148-1161, November 2007.
- [7] Zhaofeng He, Tieniu Tan, Zhenan Sun and Xianchao Qiu, "Toward Accurate and Fast Iris Segmentation for Iris Biometrics," *IEEE Trans on pattern analysis and machine intelligence*, vol.31,no.9, pp. 1676-1677,2009.
- [8] J. G. Daugman, "The importance of being random: statistical principles of iris recognition," *Pattern Recognition* 36, 279-291 (2003).
- [9] Q. M. Tieng, and W. W. Boles, Recognition of 2D Object Contours Using the Wavelet Transform Zero-Crossing Representation, *IEEE transactions on Pattern Analysis and Machine Intelligence*, vol. 19, no. 8, pp 910-916, August 1997.
- [10] C. Sanchez-Avila and R. Sanchez-Reillo, "Two different approaches for iris recognition using Gabor filters and multiscale zero-crossing representation," *Pattern Recognit.*, vol. 38, no. 2, pp. 231–240, Feb. 2005.
- [11] N. B. Puhan and N. Sudha. A Novel Iris Database Indexing Method using the Iris Color. In *ICIEA '08: Proceeding of IEEE Conference on Industrial Electronics and Applications*, pages 1886–1891, 2008.
- [12] Jin-Xin Shi; Xiao-Feng Gu, "The comparison of iris recognition using principal component analysis, independent component analysis and Gabor wavelets," *Computer Science and Information Technology (ICCSIT)*, 2010 3rd IEEE International Conference on, vol.1, no., pp.61,64, 9-11 July 2010.
- [13] Kumar, D.R.S.; Raja, K.B.; Nuthan, N.; Sindhuja, B.; Supriya, P.; Chhotaray, R.K.; Pattnaik, S., "Iris Recognition Based on DWT and PCA,"

- Computational Intelligence and Communication Networks (CICN), 2011 International Conference on , vol., no., pp.489,493, 7-9 Oct. 2011.
- [14] N. Cristianini and J. Shawe-Taylor, *An Introduction to Support Vector machines and other kernel-based learning methods*, Cambridge University Press, ISBN 0 521 78019 5, 2000.
- [15] Sayeed, F.; Hanmandlu, M.; Ansari, A.Q.; Vasikarla, S., "Iris Recognition Using Segmental Euclidean Distances," *Information Technology: New Generations (ITNG)*, 2011 Eighth International Conference on , vol., no., pp.520,525, 11-13 April 2011.
- [16] P. Grother and E. Tabassi, "Performance of Biometric Quality Measures," *IEEE Trans. Pattern Analysis and Machine Intelligence*, vol. 29, no. 4, 2007, pp. 531–543.

