# Efficient Approach for Retinal Biometric Template Security and Person Authentication using Noninvertible Constructions

M.Pabitha
Dept of CSE
Dr.Mahalingam College of Engineering & Technology
Pollachi, Tamilnadu, India

L.Latha
Dept of CSE
Kumaraguru College of Engineering & Technology
Coimbatore, Tamilnadu, India

## ABSTRACT

Cancelable biometrics is a good approach to address the security and privacy concerns on biometric authentication. The security of cancelable biometrics lies on non invertibility of the transformed templates. So the transforms should be noninvertible and the original biometric template cannot be recovered. Our proposed method initially involves segmentation process to identify blood vessel bifurcation points in the retina, and then the generation of template consisting of the bifurcation points in the blood vessels and the template is transformed using Noninvertible construction (NIC) algorithm and finally matching of the bifurcation points in different patterns. Our work mainly focused to provide the efficient person authentication and the secured biometric template, which has the unique patterns of blood vessels. The effectiveness of our proposed system is then verified with experimental results using a total of 603 retinal images from three different publicly available databases, namely DRIVE, VARIA and STARE. Also we have made a performance analysis, and found that the proposed retinal recognition method gives 100%, 98% and 93% recognition rates, 0%, 0.16%, 0.62% error rates for the above databases and analyzed the Genuine Acceptance Rate (GAR), False Acceptance Rate (FAR) and False Rejection Rate (FAR), Elapsed time respectively. The experimental results obtained using various databases shows that the application of Retinal feature extraction algorithm (RFEA) and NCI results in higher recognition rates and lower error rates.

**General Terms** – Retinal Biometric, security, Recognition rate

**Keywords** - Minucode, Bifurcation points, Retinal Feature Extraction, Template security, Noninvertible constructions.

## 1. INTRODUCTION

Reliable automatic recognition of persons has long been an important and attractive goal of scientific research. The recent upswing in technology and increasing concern related to security caused a boost in intelligent person authentication system based on retina biometrics. Retinal recognition is a relatively new approach, compared to other biometric features. It is one of the most accurate, more stable and most reliable of the biometric technologies. Since retinal patterns have highly distinctive traits, the features extracted from retina identify effectively persons, even among genetically identical twins. These characteristics make retinal recognition, a prominent solution to security in the near future. Retinal vessel tree pattern has been proved to be a valid biometric trait for personal authentication as it is unique, time invariant and very hard to forge, as showed by Marino et al. [12,13], who introduced an authentication system based on this trait. Fig.1 shows the blood vessels at the back of the eye have a unique pattern, from eye to eye and person to person. The blood vessel pattern of the retina allows up to 600 data points to be created. Security of the stored biometric templates has become one of the most damaging problems on a biometric system. Therefore, new privacy-preserving biometric recognition technologies are desired to work using secure templates without exposing the original information of the private biometrics.

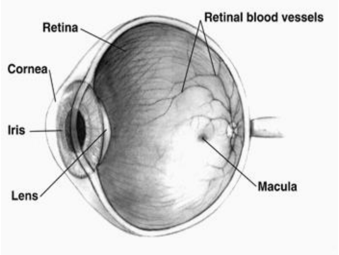


**Fig 1: Side view of the human eye**

It is used for access control in government and military environments that require very high security, such as nuclear weapons and research sites

## 2. PREVIOUS WORKS

Research based on retinal authentication and template security is very much limited, related to the retinal vascular patterns. The first retina based identification system named as Eyedentification 7.5 was introduced by EyeDentify Company in 1976 [1]. Retinal vessel detection methods are broadly classified into two categories, edge-based and kernel-based. Edge-based methods attempt to identify vessel edges with edge detector, such as Sobel operator [5] and Canny's method [6], morphological detector [7], directional matched differentiator template [4].Kernel-based methods work by convolving images with a filter kernel defined by the model of vessel cross-sectional profile. Blurred half-elliptical profile [8], Gaussian shaped profile [7, 9, 10], and simple rectangular profile [11] have been proposed for modeling profile cross-sections. Based on the idea of fingerprint minutiae [14, 15], a robust pattern was first introduced in [2], where a set of landmarks (bifurcations and crossovers of retinal vessel tree) were extracted and used as feature points. In [17] a pattern was defined using the optic disc as reference structure and using multi-scale analysis to compute a feature vector around it. The dataset size is 60 images, rotated 5 times each. [16] describes a retinal verification method characterized by adding semantic information to the biometric pattern. It reduces the computation load in the matching process as only points classified equally can be matched.

## 3. RETINAL RECOGNITION

Retinal recognition technology captures and analyzes the patterns of blood vessels on the thin nerves, on the back of the eyeball that processes light entering through the pupil. A robust representation for retina recognition must be invariant to changes in size, position and orientation of the vessel patterns. The size of the actual template is only 96 bytes, which is very small by any standards. Thus verification and identification processing times are much shorter than for other modalities. In this paper, our scheme contains five basic processes: segmentation, feature extraction, template generation, noninvertible transform, and matching as shown in Fig.2

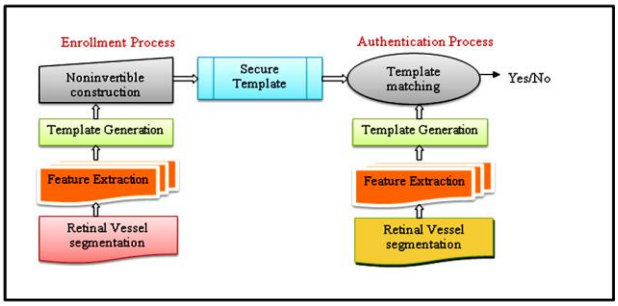


**Fig 2 System framework for Retinal Recognition Process**

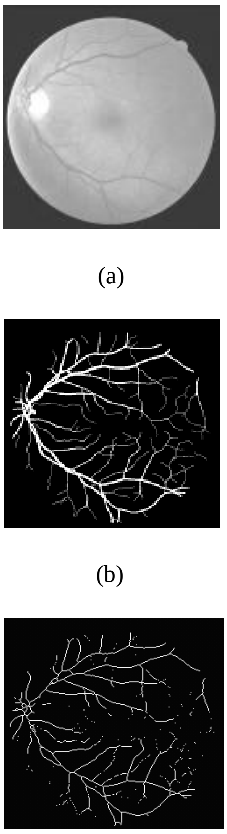
The strengths of retinal recognition include stability of blood vessel pattern over lifetime of an individual, interior location of retina that is not exposed to the threats, very small average feature vector size and quicker verification and identification processing times. The weaknesses include less accurate identification process of eyes affected by diseases such as hard glaucoma, cataracts, etc. Image acquisition involves more cooperation of the subject, entails contact with the eyepiece and this makes less public acceptance of retinal scan-based biometrics.

### 3.1 Retinal vessel Segmentation

Martinez-Perez et al.18 use a combination of scale space analysis and region growing to segment the vasculature. Two features are used to characterize the blood vessels, the gradient magnitude of the image intensity δI and the ridge strength both at different scales. The ridge strength is determined by calculating the absolute largest Eigen value £ of the matrix of second order derivatives of the image intensity. To account for the difference in vessel width across the retina both these features are normalized by the scale *s* over the scale-space while retaining only the local maxima. The local maxima of the gradient magnitude Gm and the local maxima of the ridge strength bs then become,

$$Gm=\max\,[\delta I(s)/s],\ bs = \max\,[\pounds(s)/s] \qquad (1)$$

The histograms of both features are used in the final region-growing step, in which the images pixels are divided into two classes, vessel and non-vessel. This is accomplished by alternating the vessel and background region growing and lowering the feature thresholds after each iteration. This continues until no new pixels are added to either of the two classes. Then the retinal feature is obtained by thinning the blood vessels.



(a)

(b)

(c)

**Fig 3: Retinal vessel Segmentation illustrated for one image from the test set. (a) Original test image. (b)Retinal Vascular tree (c) Retinal features**

### 3.2 Retinal Feature Extraction Algorithm

A pattern of landmarks such as bifurcations and crossovers of retinal vessel tree are extracted and are used as feature points called minutiae in our RFEA algorithm. Due to the eye movement during the image acquisition stage, patterns may suffer from deformations like translational, rotational displacements and non-linear distortion of blood vessels.

To deal with these distortions of retinal patterns, our RFEA algorithm first constructs a minutiae-centered region to avoid the translation error. Then polar coordinate conversion with respect to the corresponding core minutia can handle the rotation distortion. It takes the curvature of the image surface and performs the Hessian Tensor for finding bifurcation points in the image. Properties of such a surface can be used to detect features such as ridges, bifurcation points. The maximum principal curvature of the Hessian matrix of the intensity image is used for blood vessel extraction. Finally tessellation quantification is performed to work with the non-linear distortion effectively, by removing noise in retina image.

Each minutia in retinal image is represented as a 3-tuple T (a, b, θ), where a and b represents location and θ represents orientation attributes. A circular region *R*, of same radius, around each minutia is constructed. The center minutia is named as the core minutia and the others named as neighbor minutiae. Then each neighbor minutia with respect to the corresponding core minutia will be transformed into the polar co-ordinate system. They are represented as a new 3-tuple (α, β, γ), where α and β indicate the radial distance and radial angle and γ represents the orientation of the neighbor minutia with respect to the core minutia and β, γ ϵ [1 to 360 degree]. An illustration is given in Fig. 4.

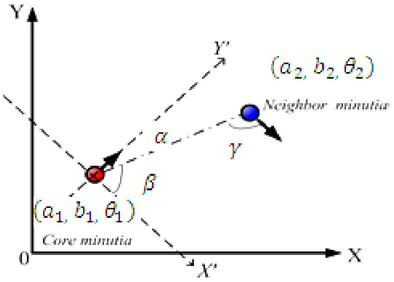


**Fig 4: Feature point centered region encoding**

The tessellation quantification is carried out on each of the neighbor minutiae by tessellating the region of interest that is centered at the core minutia. The 3-tuple (α, β, γ) in the polar coordinate system will be quantified into a rougher 3-tuple T (bt, ra, o).

$$bt = [\alpha / dbt]$$

$$ra = [\beta / dra] \qquad (2)$$

$$o = [\gamma / do]$$

Where dbt is the bandwidth of the region tessellation, dra is the distortion tolerable difference of radial angle, and *do* is the distortion tolerable difference of the orientation of the neighbor minutia with respect to the core minutia. Suppose there are *m* neighbor minutiae in a region P, then P can be represented as a set of T as

$$MC = \langle T_1, T_2 \ldots . T_m \rangle \qquad (3)$$

Where the set MC is called Minucode. The resultant retinal feature template is given by a set of minucode as

$$Temp = \{MC_1, MC_2, \ldots, MC_N\} \qquad (4)$$

Where N is the number of minutiae in a retinal image (Fig.5).

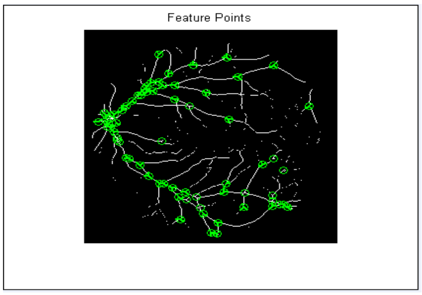


**Fig 5: Extraction of bifurcation points**

## 3.3 Template Generation

The blood vessel skeleton is removed from the input retinal image, by applying binary thresholding after the process of extracting the bifurcation points. These bifurcation points are collectively stored in a template. The template contains all extracted bifurcation points and also its coordinates. The generated template is shown in Fig. 6

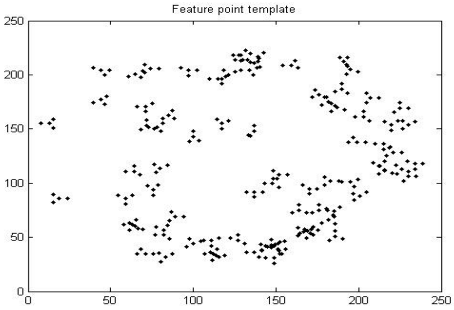


**Fig 6: A Template of Fig.5**

## 3.4 Noninvertible construction (NIC) Algorithm

The main problem in the privacy-preserving pattern recognition is to be set to transform functions that satisfy both noninvertibility and discriminability conditions simultaneously [21]. To deal with the security of cancelable biometrics problem, our proposed noninvertible scheme lies on non invertibility of the transformed templates. So the transforms should be noninvertible and the original biometric template cannot be recovered. Suppose a 3-tuples in a polar coordinate system *T*= (bt, ra, o) in the original minucode, a simple noninvertible construction algorithm can be constructed.

Step 1: Calculate the concatenated value *k* of the 3-tuple

$$K1=bt*R*R+ra*R+o \qquad (5)$$

Where R is a constant larger than all bt,*ra*,*o* and consider R=360.

Step 2: Generate a random string *RS*, encrypt *RS* with a block cipher E() ,using k1 as the cryptographic key

Step 3: Publish a new 2-tuple

$T_{new}$=(RS,$E_{K1}$(RS)) (6)

Where $E_{K1}$ (RS) is the encryption result of *RS* and NIC algorithm can preserve the discriminability, a different 3-tuple $T_{new}$ will lead to a different cryptographic key k1*'*, then result in EK1 (RS) ≠ $E_{K1'}$ (RS). So it is comparatively hard to compromise the cryptographic key k1 due to the difficulty of the plaintext attack.

## 3.5 Retinal Template Matching

This process describes a methodology for verification of individuals based on retinal patterns. Since patterns may undergo translational or rotational displacements, it is necessary to align the images to be matched. So the reference point detection method [6] is used to identify the blood vessel bifurcation points properly. The patterns compared could have a different number of points for the same individual, which is due to different conditions of illumination and orientation of the image in the acquisition process**.** Scaling is nearly constant for all images due to eye proximity to the camera. Also rotations are very slight as the eye orientation when facing the camera is very similar. Then matching of the bifurcation points is carried out. This system generates a safe confidence band in the similarity measure space between scores for patterns of the same individual and between different individuals. Each retinal template is subdivided into 8 x 8 sized sub regions. The matching of different templates [19] is measured by the closeness of feature points between the templates.

### 3.5.1 Template Matching algorithm

```
Step 1: Let the two templates to be matched as TP1 and TP2 and sub regions as SR1 and SR2.

Step 2: Initialize the total number of matched points in a template 'TMP' to be 0.

Step 3: For each sub region SR1 in TP1 and SR2 in TP2, perform:

  (i) Initialize the total number of matched points in a sub region 'MP' as 0.

  (ii) For each bifurcation point BP1 in SR1, perform:

        - Find the BP2 in SR2 and the 8 neighbor sub regions of SR2 which has minimum distance, Dmin with BP1.

        - If $Dmin \leq Dthresh$, distance threshold and BP2 is not already matched, then MP= MP +1.

        - Mark BP2 as matched.

  (iii) Find TMP = TMP + MP.

Step 4: Bifurcation point matching percentage is

 P = (2 * TMP / (TBP1 + TBP2)) * 100    (7)   where TBP1 is the total number of intersection points in TP1 and TBP2 is the total number of intersection points in TP2.

Step 5: Degree of Matching is given by

Maximum {Template Matching (TP1, TP2), Template Matching (TP2, TP1)}.
```

The distance threshold (Dthresh) represents the maximum offset by which, the same intersection point on different templates can be displaced. It is used in order to consider the quality loss and discontinuities arrived during the vessel extraction process that leads to dislocation of feature points by some pixels.

# 4. EXPERIMENTAL RESULTS AND DISCUSSION

Images from three publicly available databases, DRIVE, VARIA and the STARE databases are used to evaluate the proposed method. The proposed method is applied to a dataset [13] containing 40 retina images of 40 different persons, each having 3 samples. The database is tested for different threshold values that represent the degree of similarity between the compared images. The performance metrics used for our analysis are Genuine Acceptance Rate (GAR), False Acceptance Rate (FAR) and False Rejection Rate (FAR). On Windows XP, Pentium 4, CPU 3.06GHz, using MATLAB version 7.2, the computational time of the whole process of the algorithm takes approximately 29 seconds for comparing the features of two retinal images. The images are of size 512 x 512 for DRIVE, to get GAR, extracted features of each person are compared with other image samples of the same person. In all of the comparisons, if the similarity score is greater than the fixed threshold, then the person is accepted as a genuine user and if he is rejected, then it implies that a genuine person is not accepted i.e. falsely rejected. In this way find FRR. To get FAR, features of each person is compared with other persons' features in the database. In any of the comparison if the match score is more than the fixed threshold, then it implies that a false person is being accepted. All such comparisons are made on the database to compute GAR, FRR and FAR at fixed thresholds. The DRIVE [13] database contains only 40 normal retinal images. In order to increase the count, we have generated 2 synthetic images per user and used this along with the existing database. Our algorithm produced 100% recognition rate for DRIVE images with well separated inter distance between genuine users and imposters. VARIA [3] is the largest database and has 463 normal images. The proposed retinal authentication method gave 96.3% recognition rate for this database.

STARE database contains a mixture of normal and affected retinal images. Hence our algorithm produced only 90.1% recognition rate. We observed that the distance of separation between the two types of users is lesser in both VARIA and STARE databases.

In order to evaluate the influence of the system, in terms of EER, Recognition accuracy, and Elapsed time. A test is run where images with a biometric pattern size. Experimental results show high accuracy classification capability in terms of EER, Recognition rate, and elapsed time among similar images with different data sets.

**Table 1. Comparison of the performance representing GAR, FRR and FAR for different thresholds**

| **Drive Database** | | | | **Varia database** | | | | **Stare Database** | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Thres | GAR | FRR | FAR | Thres | GAR | FRR | FAR | Thres | GAR | FRR | FAR |
| 20 | 100% | 0% | 87.5% | 20 | 100% | 0% | 100% | 20 | 100% | 0% | 85% |
| 25 | 100% | 0% | 62.55 | 25 | 100% | 0% | 98.9% | 25 | 100% | 0% | 61.6% |
| 30 | 100% | 0% | 38.8% | 30 | 100% | 0% | 72.1% | 30 | 95% | 5% | 20% |
| 35 | 100% | 0% | 26% | 35 | 100% | 0% | 23.5% | 35 | 65% | 35% | 0% |
| 40 | 100% | 0% | 4% | 40 | 82% | 17.9% | 0% | 40 | 36.6% | 63% | 0% |
| 45 | 100% | 0% | 0% | 45 | 39.5% | 60.4% | 0% | 45 | 20% | 80% | 0% |
| 50 | 100% | 0% | 0% | 50 | 6.69% | 93.3% | 0% | 50 | 5% | 95% | 0% |
| 70 | 100% | 0% | 0% | 60 | 4.31% | 95.6% | 0% | 55 | 0% | 100% | 0% |
| 75 | 95% | 5% | 0% | 65 | 2.37% | 97.6% | 0% | 60 | 0% | 100% | 0% |
| 80 | 51% | 48.7% | 0% | 70 | 2.375 | 97.6% | 0% | 70 | 0% | 100% | 0% |
| 85 | 7.5% | 92.5% | 0% | 80 | 2.37% | 97.6% | 0% | 80 | 0% | 100% | 0% |
| 90 | 0% | 100% | 0% | 90 | 2.37% | 97.6% | 0% | 90 | 0% | 100% | 0% |

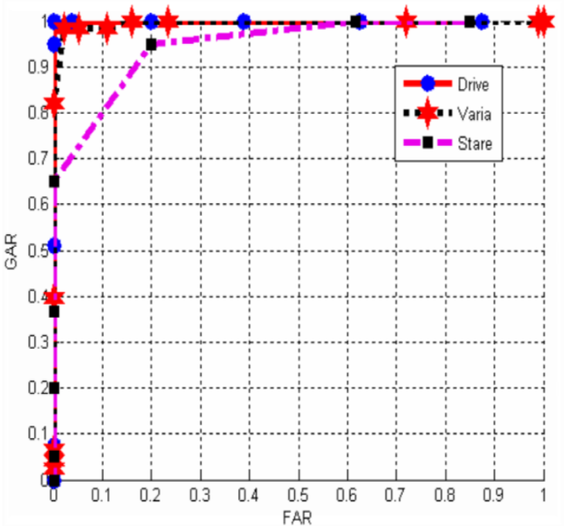


**Fig 7: ROC curve between FAR & GAR**

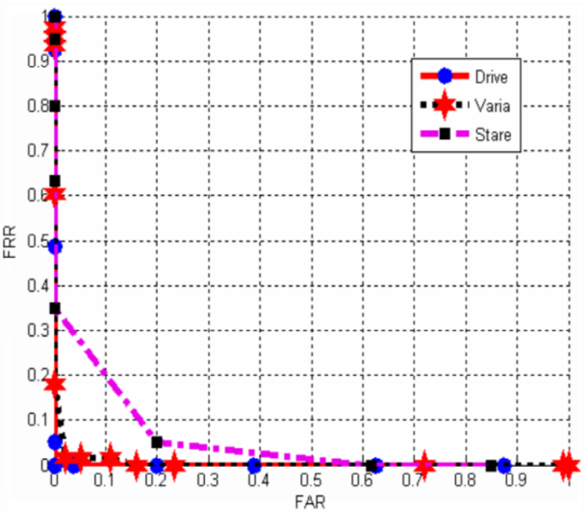


**Fig 8: ROC curve between FAR &FRR**

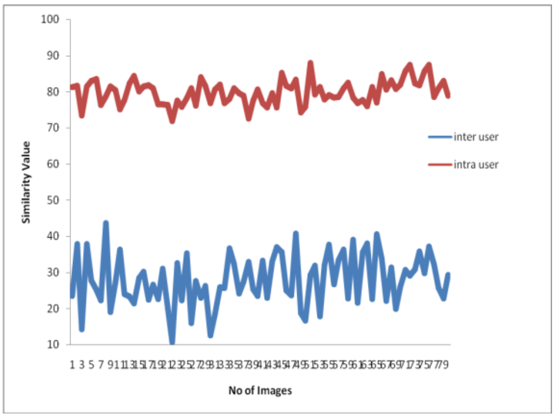


Fig 9: Inter and intra class variations for DRIVE

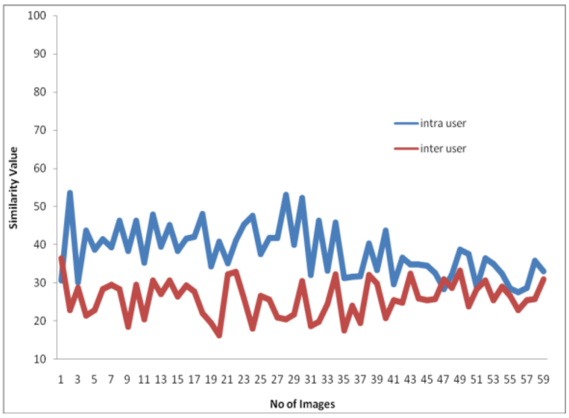
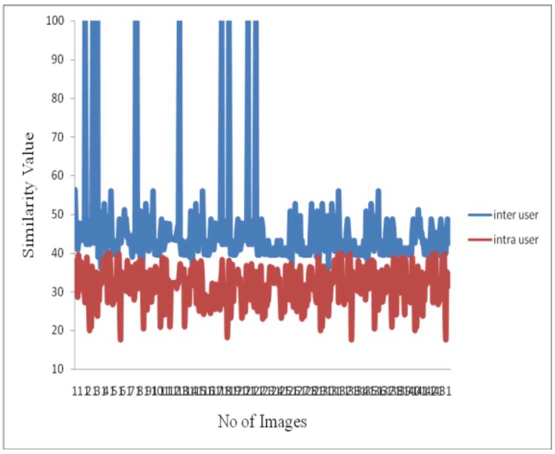


Fig 10: Inter and intra class variations for STARE



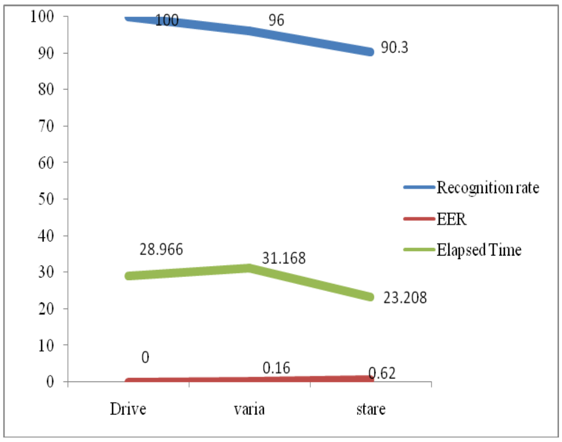


Fig 11: Inter and intra class variations for VARIA

Fig 12: Comparison of performance obtained for datasets

## 5. CONCLUSION AND FUTURE WORK

An automated retinal feature extraction algorithm for person authentication with template security has been implemented and this method involves blood vessel segmentation, feature extraction, generation of feature template consisting of the bifurcation points, non invertible transformations of the template, and then carried with anonymous matching of these feature points. The number of matched points is used to compute the degree of matching. We have made a performance analysis by using the publicly available databases, namely DRIVE, VARIA and STARE databases and found that the proposed retinal authentication method gives us 100%, 96.3% and 90.1% recognition rates for the above databases respectively. Experiments on the public domain datasets shows that this scheme provides better recognition accuracy and lower error rates along with the ability to protect the biometric template, thus becomes a promising solution for privacy trustworthy biometric applications. As a future work we will address the practical issues of the latency for recognition and the performance can also be verified for multimodal biometrics by using noninvertible transformations

## 6. REFERENCES

[1] R.B.Hill, Retinal identification, in Biometrics: “Personal Identification in Networked Society”, A.Jain, R.Bolle, and S.Pankati, Eds., p.126, Springer, Berlin, Germany, 1999

[2] M.Ortega, C.Marino, M.G. Penedo, M.Blanco, F.Gonzalez, “Biometric Authentication Using Digital Retinal Images,” in proceedings of the 5th WSEAS International Conference on Applied Computer Science (ACOS 06), pp.422427, Hangzhou, China, April 2006.

[3] VARIA, VARPA retinal images for authentication http://www.varpa.es/varia.htm

[4] Can A, Shen A, Turner J, Tanenbaun H, Roysam B. Rapid automated tracing and feature extraction from retinal fundus images using direct exploratory algorithms. IEEE Trans Info Technol Biomed 1999; 2:125–38.

[5] Chaudhuri S, Chatterjee S, Katz N, Nelson M, Goldbaum M. Detection of blood vessels in retinal images using two-dimensional matched filters. IEEE Trans Med Imag 1989; 8:263–9.

[6] Lalonde M, Gagnon L, Boucher M. Non-recursive paired tracking for vessel extraction from retinal images. In: Conf. vis. interface. 2000.

[7] Zana F, Klein JC. Segmentation of vessel-like patterns using mathematical morphology and curvature evaluation. IEEE Trans Imag Proc 2001; 10(7):1010–8.

[8] Miles EP, Nuttall AL. Matched filter estimation of serial blood vessel diameters from video images. IEEE Trans Med Imag 1993; 12:147–52.

[9] Hoover A, Kouznetsova V, Goldbaum M. Locating blood vessels in retinal images by piecewise threshold probing of a matched filter response. IEEE Trans MedImag 2000; 19:203–10.

[10] Gang L, Chutatape O, Krishnan S. Detection and measurement of retinal vessels in fundus images using amplitude modified second-order Gaussian filter. IEEE Trans Biomed Eng 2002; 49(2):168–72.

[11] Vermeer K, Vos F, Lemij G, Vossepoel A. Amodel based method for retinal blood vessel detection. Comput Biol Med 2004; 34:209–19.

[12]C.Marino,M.G.Penedo,M.Penas,M.J.Carreira,F.Gonzalez, ”Personal authentication using digital retinalimages”,PatternAnalysisandApplication(2006)21–33.

[13] DRIVE, “Digital retinal images for vessel extraction,” 2007.

[14] A.K. Jain, L. Hong, S. Pankanti, R. Bolle, An identity-authentication system using fingerprints, Proceedings of the IEEE 85 (9) (1997) 1365–1388.

[15] X. Tan, B. Bhanu, “A robust two step approach for fingerprint identification”, Pattern Recognition Letters 24 (2003) 2127–2134.

[16] Marcos Ortega, M.G.Penedo, J.Rouco and M.J.Carreira, “Personal verification based on extraction and characterization of retinal feature points”, Journal of Visual Languages and Computing, pages 80-90, 2009.

[17] H. Farzin, H. Abrishami-Moghaddam, and M.-S. Moin, “A novel retinal identification system,” EURASIP Journal on Advances in Signal Processing, vol. 2008, Article ID 280635, 10 pages, 2008.

[18] M. Martinez Perez, A. Hughes, A. Stanton, S. Thom, A. Bharath, and K. Parker, “Scale-space analysis for the characterisation of retinal blood vessels,” in *Medical Image Computing and Computer-Assisted Intervention - MICCAI’99*, C. Taylor and A. Colchester, eds., pp. 90–97 1999.

[19]L.Latha, M.Pabitha, S.Thangasamy, “A novel method for Person authentication using retinal images”, IEEE Explore, Feb 2010

[20] R.C.Gonzalez and R. E. Woods, Digital Image Processing, Pearson’s Education Inc., 2005 Second Edition.

[21]Jinyang SHI, Zhiyang YOU, Ming GU1,3, Kwok-yan LAM,” Biomapping :privacy Trustworthy biometrics using noninvertible and discriminable constructions, IEEE Explore 2008