

Personal Authentication Using Finger Images

Renuka Mahesh Jadhav

*Dept. of Electronics and Telecommunication Engineering
JSPM's Rajarshi Shahu College of Engineering
Pune, India
renukamjadhav@gmail.com*

Prof. Dr. D. S. Bormane

*Dept. of Electronics and Telecommunication Engineering
JSPM's Rajarshi Shahu College of Engineering
Pune, India
rscoe@jspm.edu.in*

Abstract— As the need for personal authentication increases, biometrics systems have become the ideal answer to the security needs. This paper presents a novel personal authentication system which uses simultaneously acquired finger-vein and finger texture images of the same person. A virtual fingerprint is generated combining these two images. The result of the combination i.e. the virtual fingerprint is then subjected to pre-processing steps including binarization, normalization, enhancement and Region of Interest (ROI) segmentation. Gabor filter is used to extract features. The feature extracted image is matched with the database. This proposed system is designed such that to achieve better performance in terms of matching accuracy, execution time, memory required and security.

Keywords — *Image pre-processing, Feature Extraction, Gabor Filter, Matching*

I. INTRODUCTION

With our progress toward a global information society, the average person's life has become threatened by heinous occurrences that can originate anywhere in the world. As a result, there is an intense need for personal authentication systems that can prevent spoofing and other criminal impersonation in such areas as financial (cash or credit card) withdrawals, passport and driver's license identification, entry into important facilities, apartment complexes or offices, access to IT equipment, and a broad range of other applications [18]. Biometrics systems have become the ideal answer to these security needs and are already being adopted worldwide.

Biometrics deals with identification of individuals based on their biological and/or behavioral features. These features include fingerprint, finger-vein, face, iris, voice, palm print, DNA, retina, signature, keystroke etc. Out of these, fingerprint techniques are widely used in authentication systems. Finger print and Finger Vein are growing and popular biometric identification and authentication technologies. They are used in large no. of commercial applications and applications of identity management. They are also used by forensic experts in criminal investigations.

Finger Print and Finger Vein identification is based on its uniqueness and persistence. The uniqueness of the fingerprints and veins is accepted over the time. The pattern of the friction ridges on each finger of an individual is unique. Even twins can be differentiated based on the finger prints. The pattern on the fingers is immutable. The finger surface injuries such as cut damage the finger pattern only temporarily but the original structure reappears after the injury heals i.e. the basic characteristics of fingerprints are persistent.

Finger-veins are internal characteristics of the finger. It is non-contacting and hidden structure. Finger-veins are visible only under Infrared light so it provides higher level of security as can't be stolen without the knowledge of an individual.

A lot of research has been done on the fingerprint and finger-veins in biometrics. An automated finger image matching framework which can reliably extract the finger vein and texture shape features and achieve much higher accuracy than previously proposed finger vein identification approaches is presented in [1]. A system for fingerprint privacy protection by combining two fingerprints into a new identity is introduced in [2]. This system has the advantage in creating virtual identity. Alessandra A. Paulino et al [3] proposed a fingerprint matching algorithm designed for matching latents to rolled/plain fingerprints which is based on a descriptor-based Hough Transform alignment which shows superior performance. Jinfeng Yang et al [13] proposed a new finger-vein image restoration method to improve the quality of finger-vein images.

In this paper, we propose a novel personal authentication system which uses simultaneously acquired finger vein and finger texture images of the same person. These two images are combined into a virtual fingerprint. The feature extracted templates of the virtual fingerprints are stored in the database for the authentication which requires two query fingerprints, finger vein and finger texture.

The mixing of finger vein and fingerprint has benefits in terms of storage and security. It can be used to generate large set of virtual identities. Even if this dataset is stolen it is highly impossible to separate these two images thus it is highly secure [19].

II. THE PROPOSED SYSTEM FOR PERSONAL AUTHENTICATION

Fig. 1 shows the block diagram [1] for proposed personal authentication system.

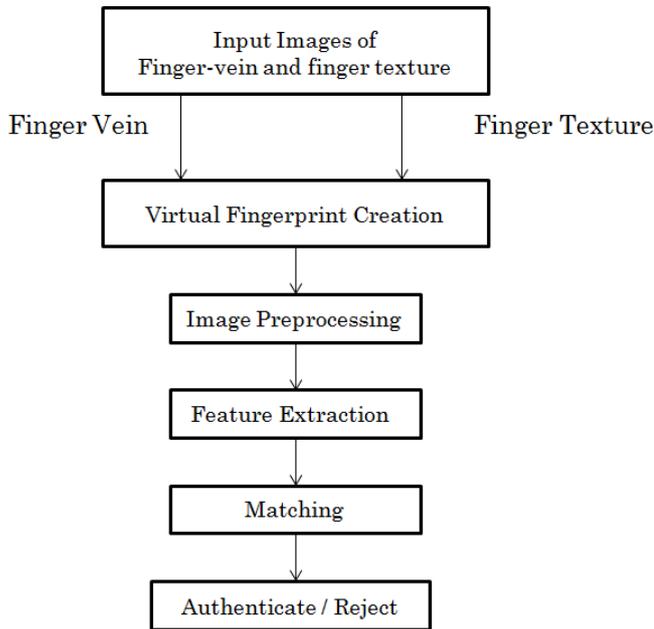


Fig. 1. Block Diagram for the proposed personal identification using finger-vein and finger texture combination

The system uses simultaneously acquired finger-vein and finger texture images. Fig. 2 shows the image samples.

As the finger texture images are captured using low resolution webcam, they are of low quality. These images do not contain minutiae or level-2 features.

The acquired finger images are noisy. Therefore these images are subjected to pre-processing steps. The pre-processing steps include image normalization, segmentation and enhancement.

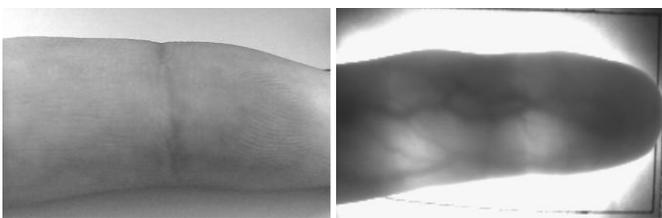


Fig. 2. Finger texture and Finger vein image samples

A. Generation of Virtual Fingerprint

The input finger vein and finger texture images are added to generate a virtual identity. This virtual fingerprint is then subjected to pre-processing steps for further processing.

B. Image Preprocessing

- 1) *Image Normalization*: In this, the image is subjected to binarization with global threshold value. The isolated and loosely connected regions in the binarized are eliminated by applying Canny Edge Detector to the image and subtracting the resulting edge map from the binarized image.
- 2) *Image Segmentation*: The obtained binary mask in image normalization is used to segment the ROI (Region of Interest) from the original finger-vein image. The orientation of the finger-vein image is determined from the orientation of the binary mask. The normalized 2nd order moments [1] are calculated as follows:

$$\alpha_{12} = \frac{\sum_{(x,y) \in R} (y - g_y)(x - g_x)I(x,y)}{\sum_{(x,y) \in R} I(x,y)}$$

$$\alpha_{11} = \frac{\sum_{(x,y) \in R} (y - g_y)^2 I(x,y)}{\sum_{(x,y) \in R} I(x,y)}$$

$$\alpha_{22} = \frac{\sum_{(x,y) \in R} (x - g_x)^2 I(x,y)}{\sum_{(x,y) \in R} I(x,y)}$$

Where I = Image

(g_x, g_y) = Position of centroid in the image

The orientation of the image is estimated as given below:

$$\omega = \begin{cases} \tan^{-1} \left\{ \frac{\alpha_{11} - \alpha_{22} + \sqrt{(\alpha_{11} - \alpha_{22})^2 + 4\alpha_{12}^2}}{-2\alpha_{12}}, \alpha_{11} > \alpha_{22} \right. \\ \left. \tan^{-1} \left\{ \frac{-2\alpha_{12}}{\alpha_{22} - \alpha_{11} + \sqrt{(\alpha_{22} - \alpha_{11})^2 + 4\alpha_{12}^2}}, \alpha_{11} \leq \alpha_{22} \right. \right. \end{cases}$$

This orientation is used for rotational alignment of the ROI of finger-vein image.

- 3) *Image Enhancement*: The ROI image is subjected to local histogram equalization. Histogram equalization is used to enhance the image and to improve the contrast and the details in the ROI of original image.

C. Feature Extraction

Gabor filter is used for image feature extraction. Gabor filters are known to achieve the maximum possible joint resolution in spatial and spatial-frequency domain. Gabor filters capture both local orientation and frequency information from a finger image. By tuning a Gabor filter to specific frequency and direction, the local frequency and orientation information can be obtained.

The Gabor with specified orientations are created and then convolved with the enhanced image to remove the unwanted regions. The analytical form of 2-D Gabor filter [1] is given by

$$h(x, y, \theta, f, \sigma_x, \sigma_y) = e^{-\frac{1}{2}\left(\frac{x_\theta^2}{\sigma_x^2} + \frac{y_\theta^2}{\sigma_y^2}\right)} \times e^{2\pi f x_\theta}$$

Where $x_\theta = x \cos \theta + y \sin \theta$

$y_\theta = -x \sin \theta + y \cos \theta$

f = Frequency of the sin wave

θ = Orientation of Gabor filter

σ_x = Standard deviations of the Gaussian envelope along the x axis

σ_y = Standard deviations of the Gaussian envelope along the y axis

The feature extracted image is subjected to morphological operations to enhance the patterns. The morphological top-hat operation is applied to the image. It performs morphological top-hat filtering on the grayscale or binary image. Top-hat filtering computes the morphological opening of the image and then subtracts the results from the input image. This corrects the uneven illumination when the background is dark. This is represented as [1] follow:

$$z(x, y) = f(x, y) - (f(x, y) \ominus b) \circledast b$$

Where \ominus = Gray-scale erosion

\circledast = Gray-scale dilation

b = Square structuring element

The result of the morphological operation is encoded [1] follows:

$$R(x, y) = \begin{cases} 255, & z(x, y) > 0 \\ 0, & z(x, y) \leq 0 \end{cases}$$

D. Matching

The features extracted from the virtual fingerprint are already stored in a database. The features of the combined image are matched with all the images in the database to check whether the input images are matched with any one of the images in the database.

The SURF detector-descriptor scheme is used for matching two feature vector templates. This detector uses the determinant of Hessian Matrix because of its good performance in computation time and accuracy. The Hessian

Matrix, H , is the matrix of partial derivatives of the function f given by

$$H(F(x, y)) = \begin{bmatrix} \frac{\partial^2 f}{\partial x^2} & \frac{\partial^2 f}{\partial x \partial y} \\ \frac{\partial^2 f}{\partial x \partial y} & \frac{\partial^2 f}{\partial y^2} \end{bmatrix}$$

The determinant of this matrix, known as the discriminant, is calculated by,

$$\det(H) = \frac{\partial^2 f}{\partial x^2} \frac{\partial^2 f}{\partial y^2} - \left(\frac{\partial^2 f}{\partial x \partial y}\right)^2$$

The value of this discriminant is used to detect the interest points. Once the interest points in both, the input feature vector and the database feature vector are detected, the Sum of Squared Differences, SSD, is used for matching.

If the resulting matching score is greater than the threshold then the input images and the person is authenticated.

III. EXPERIMENTAL RESULTS AND DISCUSSION

A. Database

The database used is The Hong Kong Polytechnic University Finger Image Database (Version 1.0) [16]. It consists of 6,264 images from 156 subjects. The finger texture images are captured using webcam having resolution of 75 dpi and the finger-vein images are captured using an infra-red camera and Light Emitting Diode [1].

B. Performance Evaluation

All codes are written in MATLAB. In this paper, we worked on 100 images of finger vein and finger texture each from the provided finger database. The feature extracted images of the virtual fingerprints are already stored in an enrollment database. The matching accuracy of the system is compared with the existing approaches.

Fig. 3 shows the results of Virtual Finger pre-processing and feature extraction. The last image in Fig. 3 shows the point matches of test and database image on the graph. The results show that the pre-processing performed on the vein and texture images has been effective in extracting the features. Gabor filters have both frequency and orientation selective properties so it extracts the features efficiently.

According to the work presented in [1], if the finger texture image is not matched due to its low quality then even if the finger vein image is matched the genuine person is rejected. We provide a solution to this by combining the vein and texture images. Our system provides matching accuracy of 96 %.

In terms of memory required and execution time, our system has improved performance than the system presented in [1]. Unlike in [1], we are storing feature extracted images of the virtual fingerprint only. So the database space required is reduced to 50% as we are generating the virtual fingerprint from finger vein and finger texture. The approach in [1] performs preprocessing and feature extraction on both finger vein and finger texture separately. In our system, only the virtual fingerprint is subjected to preprocessing and feature extraction so the execution time or the time required for the verification of a person is reduced to almost 50%.

C. Comparison with Previous Methods

The experimental results in table 1 illustrates that our approach performs significantly better than the existing approaches in [1] and [3] in terms of matching accuracy.

TABLE I
 PERFORMANCE EVALUATION IN TERMS OF MATCHING ACCURACY

Approach	Matching Accuracy (%)
Our method	92
Gabor Filter for score fusion of finger vein and finger texture [1]	90
Matched Filter [1]	86
Repeated Line Tracking [1]	77
Maximum Curvature [1]	73
Hough Transform [3]	75

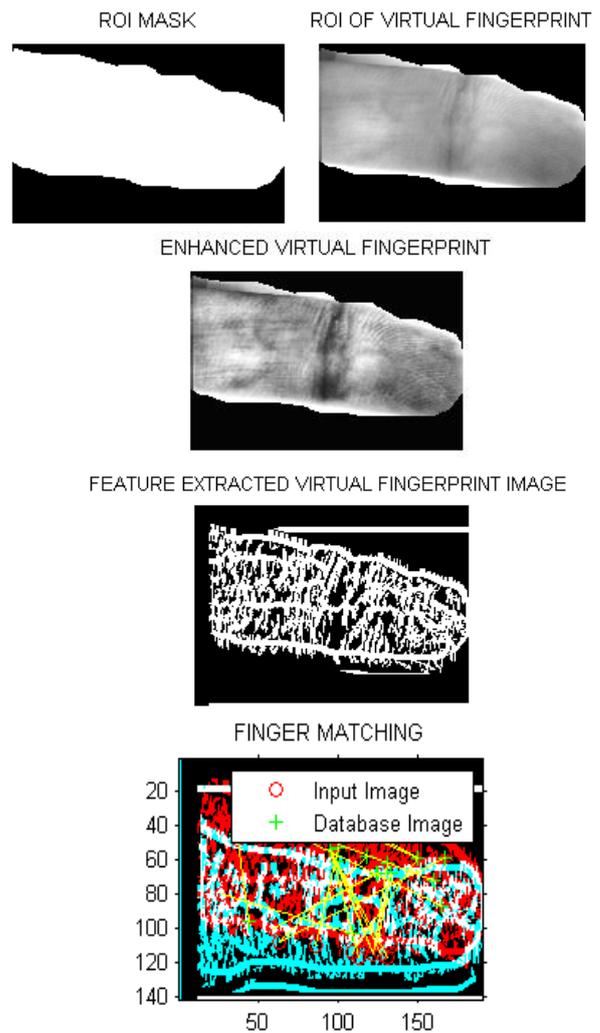
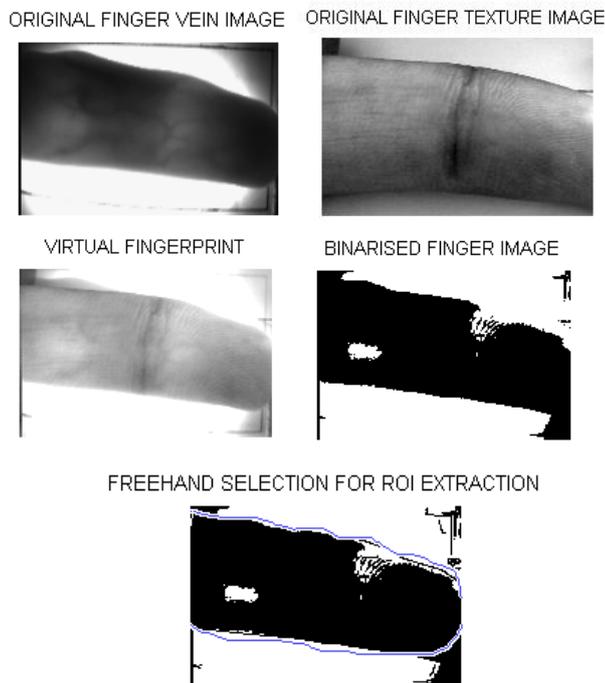


Fig. 3 Results of Virtual Finger pre-processing and feature extraction

IV. CONCLUSIONS

In this paper, we have discussed and implemented the personal authentication framework by using simultaneously acquired finger texture and vein images. We generated virtual fingerprint combining finger vein and finger texture image and used Gabor filter for feature extraction.

The experimental results show that our system provides improves matching accuracy of 92%.

The processing time for the verification of the person is approximately 20 to 25 seconds for the database of 100 persons. This is significantly lower than the existing approach in [1]. The memory requirement of our system is also reduced to 50% compared to the system in [1].

ACKNOWLEDGEMENT

We are very thankful to Dr. Ajay Kumar, Dept. of Computing, The Hong Kong Polytechnic University, for making available the Finger Image Database (Version 1.0).

REFERENCES

- [1] Ajay Kumar, Yingbo Zhou, "Human Identification using Finger Images", *IEEE Transaction on Image Processing*, vol.21, pp.2228-2244, 2012
- [2] Sheng Li, Alex C. Kot, "Fingerprint Combination for Privacy Protection", *IEEE Transactions On Information Forensics and Security*, Vol.8, No.2, pp.350-360, 2013
- [3] Alessandra A. Paulino, Jianjiang Feng, Anil K. Jain, "Latent Fingerprint Matching Using Descriptor-Based Hough Transform," *IEEE Transactions On Information Forensics and Security*, Vol.8, No.1, pp.31-45, 2013
- [4] Jucheng Yang, Athanasios V. Vasilakos, "Two-stage enhancement scheme for Low-Quality Fingerprint Images by Learning From the Images", *IEEE Transactions On Human-Machine Systems*, Vol.43, No.2, pp.235-248, 2013
- [5] Zhi Liu and Shangling Song, "An Embedded Real-Time Finger-Vein Recognition System for Mobile Devices", *IEEE Transactions on Consumer Electronics*, Vol.58, No.2, pp.522-527, 2012
- [6] Fengchun Zhang, Junyao Guo, Shuxu Guo, "Extraction for Finger Vein Pattern based on PDE", *International Conference on Audio, Language and Image Processing*, pp.651-656, 2012
- [7] Sepehr Damavandinejadmonfared, "Finger-vein recognition using Linear Kernel Entropy Component Analysis", *IEEE International Conference on Intelligent Computer Communication and Processing (ICCP)*, pp.249-252, 2012
- [8] Desong Wang, Jianping Li, Gokhan Memik, "User Identification Based on Finger-vein Patterns for Consumer Electronics Devices", *IEEE Transactions on Consumer Electronics*, Vol.56, No.2, 2010
- [9] Ntethelelo A. Mngenge, Nthatheni N. Nelufule, Fulufhelo V. Nelwamondo, Ntsika Msimang, "Fingerprint Pores Extractor", *National Conference on Computing and Communication Systems (NCCCS)*, pp.1-5, 2012.
- [10] Josef Strom Bartunek, Mikael Nilsson, Benny Sällberg, Ingvar Claesson, "Adaptive Fingerprint Image Enhancement With Emphasis on Preprocessing of Data", *IEEE Transactions On Image Processing*, Vol.22, No.2, pp.644-656, 2013.
- [11] Nazia Mastali, "A Novel Approach for Curvature Detection in Global Fingerprint Feature Extraction", *IEEE/OSA/IAPR International Conference on Informatics, Electronics & Vision*, pp.1059-1063, 2012.
- [12] Jinfeng Yang, Guangliang Bai, "Finger-vein Image Restoration Based on Skin Optical Property", *International Conference on Signal Processing*, pp.749-752, 2012.
- [13] P. Harsha, C. Subashini, "A Real Time Embedded Novel Finger-Vein Recognition System for Authenticated on Teller Machine", *International Conference on Emerging Trends in Electrical Engineering and Energy Management*, pp.271-275, 2012.
- [14] N. Miura, A. Nagasaka, and T. Miyatake, "Feature extraction of finger-vein patterns based on repeated line tracking and its application to personal identification," *Machine Vision. & Appl.* pp. 194-203, Jul., 2004.
- [15] N. Miura, A. Nagasaka, and T. Miyatake, "Extraction of finger-vein patterns using maximum curvature points in image profiles," *Proc. IAPR Conf. Machine Vis. & Appl.* pp. 347-350, Tsukuba Science City, May 2005.
- [16] The Hong Kong Polytechnic University Finger Image Database Version 1.0, Jul. 2010, <http://www.comp.polyu.edu.hk/~csajaykr/fvtDATABASE.htm> (Available Online)
- [17] K. Nandakumar, Y. Chen, S. C. Dass and A. K. Jain, "Likelihood ratio based biometric score fusion," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 30, pp. 342-347, Feb. 2008.
- [18] Junichi Hashimoto, "Finger Vein Authentication Technology and its future", *IEEE Symposium on VLSI Circuits Digests of Technical Papers*, 2006.
- [19] Asem Othman, Arun Ross, "On Mixing Fingerprints", *IEEE Transactions On Information Forensics and Security*, Vol.8, No.1, pp.260-267, Jan. 2013