A Finger Vein Recognition System Using Image Processing

[1]S. Nishanth, [2]P.Ponnilavan, [3]S.Bhuvana
[1, 2] UG Scholar, Department of CSE, Sri Krishna of Technology, Coimbatore.
[3] Associate Professor, Department of CSE, Sri Krishna of Technology, Coimbatore.

Abstract— The most vital requirement in today's world of spoofing attacks is the high security. The development in consumer electronics demands for high security with high accuracy and high speed of authentication. A human behavioural and physiological feature in biometrics has the large scope as a solution for security issues. However, the existing biometric systems are highly complex in terms of time or space or both, and thus not suitable in very high security. Thus an embedded finger-vein recognition system for authentication is proposed. The system is to be implemented using novel finger vein recognition algorithm and lacunae, fractal dimension and gabor filter are the algorithms used for feature extraction and the matching of the extracted feature is done using the distance classifier. The analysis is done using the various features from which the kurtosis, range shows large variation from person to person. Based on this analysis finger vein recognition becomes easier and reliable.

Keywords— vein, matching, scanning, feature extraction, biometric

I. INTRODUCTION

Image processing of images using mathematical operations by using any form of signal processing for which the input is an image ,a serious of images ,or a video, such as a photograph or video frame. Image processing may be either an image or an set of characteristics or parameters related to the image Conventional security and identification systems are either knowledge based – like a social security number or a password, or token based – such as keys, ID cards. The conventional systems can be easily breached by others, ID cards and passwords can be lost, stolen or can be duplicated. In other words, it is not unique and not necessary represent the rightful user. Therefore, biometric systems are under intensive research for this particular reason. Humans recognize each other according to their various characteristics for ages. People recognize others by their face when they meet and by their voice during conversation. These are part of biometric identification used naturally by people in their daily life. Any human physiological and/or behavioural characteristic can be used as a biometric characteristic as long as it satisfies the following requirements:

- Universality: each person should have the characteristic;

- Distinctiveness: any two persons should be sufficiently different in terms of the characteristic;
- Permanence: the characteristic should be sufficiently invariant (with respect to the matching criterion) over a period of time;
- Collectability: the characteristic can be measured quantitatively.

  However, in a practical biometric system there are a number of other issues that should be considered, including:
- Performance, which refers to the achievable recognition accuracy and speed, the resources required to achieve the desired recognition accuracy and speed, as well as the operational and environmental factors that affect the accuracy and speed.
- Acceptability, which indicates the extent to which people are willing to accept the use of a particular biometric identifier (characteristic) in their daily lives.

Circumvention, which reflects how easily the system can be fooled using fraudulent methods. In the verification mode, the system validates a person's identity by comparing the captured biometric data with her own biometric template(s) stored system database. In such a system, an individual who desires to be recognized claims an identity, usually via a PIN (Personal Identification Number), a user name, a smart card, etc., and the system conducts a one-to- one comparison to determine whether the claim is true or not (e.g., "Does this biometric data belong to Bob?"). Identity verification is typically used for positive recognition, where the aim is to prevent multiple people from using the same identity.

In the identification mode, the system recognizes an individual by searching the templates of all the users in the database for a match. Therefore, the system conducts a one-to-many comparison to establish an individual's identity (or fails if the subject is not enrolled in the system database) without the subject having to claim an identity (e.g., "Whose biometric data is this?"). Identification is a critical component in negative recognition applications where the system establishes whether the person is who she (implicitly or explicitly) denies to be. The purpose of negative recognition is to prevent a single person from using multiple identities.

- Identification may also be used in positive recognition for convenience (the user is not required to claim an identity). While traditional methods of personal recognition such as passwords, PINs, keys, and tokens may work for positive recognition, negative recognition can only be established through biometrics.

II. RELATED WORK

This section reviews several categories of existing solutions and explain their relationships to our work.

A. A Novel Design Of Finger Vein Recognition For Personal Authentication And Vehicle Security

Zhi Liu et al. [1] has proposed finger-vein recognition system for authentication on mobile devices. This system is implemented on a DSP platform and equipped with a novel finger vein recognition algorithm. In this work the system takes only about 0.8 seconds to verify one input finger vein sample and achieves an equal error rate (EER) of 0.07% on a database of 50 subjects. This proposed system qualified only for authentication on mobile devices. T. Y. V. BhanuKiranmai et al.

B. An Embedded Real-Time Finger-Vein Recognition System For Security Levels

This system consist of four hardware modules: radio frequency identification system, image acquisition module, embedded main board, and human machine communication module. RFID module will start the very initial communication between user and device. The image acquisition is used for collecting a finger vein image for user. The embedded main board is main chapter for security levels, it consists of microcontroller chip, memory (flash) and communication port is executed on FVRS algorithm. Caixialiu

C. A Study of Feature Extraction Techniques and Image Enhancement Algorithms for Finger Vein Recognition

Has proposed "study on finger vein feature extraction algorithm", according to the feature of human finger vein image, a finger vein feature extraction method based on improved adaptive black threshold segmentation algorithm is proposed. In this method, black window parameter and the correction factor, the image is enhanced by adaptive histogram equalization and filtering before feature extraction. This proposed system captures only 200 pixels and 500 pixels of finger vein images. Ajay Kumar et al.

D. Human Identification Using Finger Images

Has proposed human identification system simultaneously acquires the finger-vein and low resolution finger print. This system has investigates two new score level combination approaches, holistic and nonlinear fusion, for combining finger vein and finger texture. This model was too costly and was difficult to implement in all the circumstances.

E. An Authentication by Finger Vein Recognition System

In existing method, fingerprint method is used it is not more security. Additionally, for ATM centres they also provide automatic temperature control technique for detecting the fire, if the fire will happen in the centres it automatically ON the sprinkles. Using Tilt sensor and DC motor the shutter will automatically ON.

III.A FINGER VEIN RECOGNITION SYSTEM USING IMAGE PROCESSING

Private information is traditionally provided by using passwords or Personal Identification Numbers (PINs), which are easy to implement but is vulnerable to the risk of exposure and being forgotten. Biometrics, which uses human physiological or behavioural features for personal identification, has attracted more and more attention and is becoming one of the most popular and promising alternatives to the traditional password or PIN based authentication techniques There is a long list of available biometric patterns, and many such systems have been developed and implemented, including those for the face, iris, fingerprint, palm print, hand shape, voice, signature, and gait. Notwithstanding this great and increasing variety of biometrics patterns, no biometric has yet been developed that is perfectly reliable or secure. For example, fingerprints and palm prints are usually frayed; voice, signatures, hand shapes and iris images are easily forged; face recognition can be made difficult by occlusions or face-lifts and biometrics, such as fingerprints and iris and face recognition, are susceptible to spoofing attacks, that is, the biometric identifiers can be copied and used to create artefacts that can deceive many currently available biometric devices. The key methodology is to provide an improved security and accuracy in scanning the identity of a person with the help of various scanners. This model highly avoids the illegal authorization by making use of scanners. It is implemented with efficient algorithms for faster response time and security.

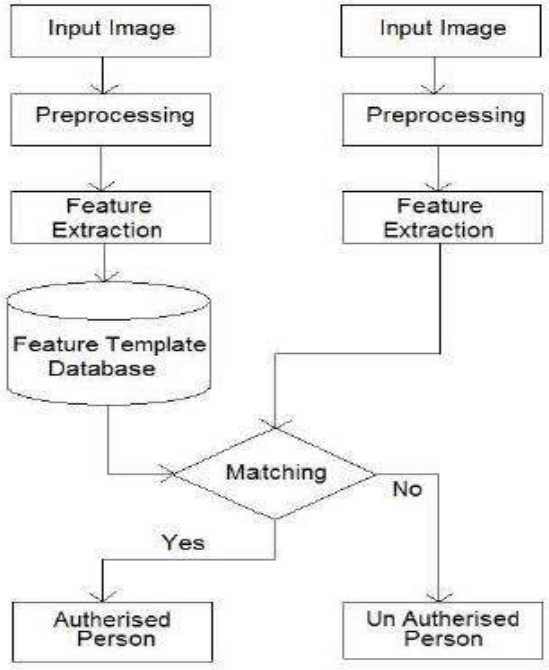

Fig 1. Model flow diagram

IV. IMPLEMENTATION AND RESULTS

A. IMAGE ACQUISITION: In image acquisition the finger vein is taken as an input. But the input image consist of blur and noise, so image clarity can be improved by removing

the blur and noise through pre-processing technique.

B.PRE-PROCESSING: Pre-processing is an improved the image data that suppress unwanted distortions or enhanced some image features important for further processing. The pre-processing method consists of image enhancement, image segmentation and feature extraction.

B. IMAGE ENHANCEMENT: Image Enhancement involves the adjustment of digital data for improving the image qualities with the aid of computers. The processing helps in enhancing the clarity, sharpness and details towards extracting information and further analysis. Enhancement distorts the digital value; therefore enhancement is doesn't initiate until the restoration process are completed. Image Enhancement alters the visual impact that the image has on the interpreter in a fashion that improves the information content 1. Contrast enhancement 2. Intensity, hue, and saturation transformation 3. Density slicing 4. Edge enhancement 5. Making digital varieties 6. Producing synthetic CD images

C. IMAGE SEGMENTATION: Image segmentation is the division of an image into sub images or categories, which correspond to different objects or parts of objects. Every pixel in an image is due to one of a number of these images. Segmentation contains, Pixels in the same category have similar grey scale of multivariate values and form a connected region, Neighboring pixels which are in different categories have different values.

D. FEATURE EXTRACTION: In feature extraction the required information can be extracted from the processed image for their requirement in the application Figure 1: Block Diagram C. Human Communication Module The extracted image has been taken from the human communication module.

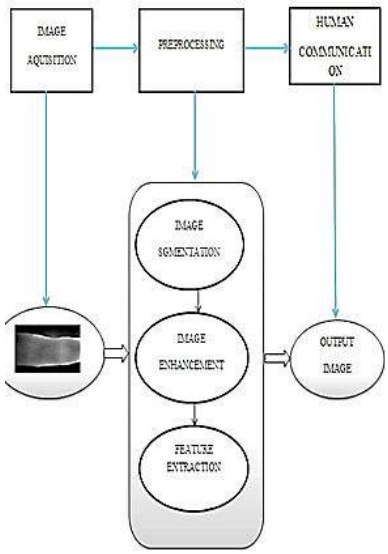

Fig 2. Feature extraction

F.*COMMUNICATION MODULE:* The communication module consist of LCD display, alarm and GSM (Global system for mobile). The main purpose of GSM in this work is to alert the

authorized vehicle user about the vehicle security. If an unauthorized person is trying to access the car, then an alert message "Access denied" message is sent to the authorized person through GSM, that is to provide a security information about the vehicle. The same message is also displayed in the LCD and also alarm will produce a beep sound and LCD display is displaying a message about "unauthorized is accessing a car" . This is a plug and play GSM Modem with a simple to interface serial interface. Use it to send SMS, make and receive calls, and do other GSM operations by controlling it through simple AT commands from microcontroller. It uses the highly popular SIM300module for all its operations. It comes with a standard RS232 interface which can be used to easily interface the modem to microcontroller and for developing embedded applications.

G.*CREATING A DATABASE:* To identify the authorized person, it is necessary to create a database of group of person's finger vein image. In this work a minimal of 12 image have been taken in to account the database. There are four steps for creating the database and are discussed in the following steps.

After pressing the start button in the index page, the next subpage will be opened and has seven buttons for various processes like creating , loading a database, capturing the image, segmentation, enhancement, feature extraction and for authenticating. There is one separate button for exit. For capturing the image, create database button needs to be pressed. The live video will be appeared in the second window and has one specific button to take picture and need to be pressed for the next stage. The captured image will be appeared in the input axes box.

s The next and final stage is an enrolment stage, and is represented as load database button. This stage includes all the processing like segmentation, enhancement and feature extraction .After completing all this process will be loaded in the database.

H. *MATCHING THE IMAGE:* Matching the finger vein image with the database image is the main stage to verify the person's authentication to access the car. This stage is discussed in the following steps.

While pressing the 'capture image button', the live video is appeared in the second window. And that second window also has one specific button to take the picture, and need to be pressed for the next stage. Newly captured finger vein image will be appeared in the input axes box. Press the segmentation button, which issued to cut the region of interest on rectangular shape of for the newly captured finger vein image.

Next press the enhancement button, this will enhance (resize) the newly captured finger vein image (verification stage). The vein is perceptible to the human eye.

Feature extraction for authentication is an important stage, press the feature extraction

button it will extracts the newly captured finger vein image features and feature extracted image is display in axes box. The next and final stage is authentication stage and is represented as authenticate button. Press the authenticate button, this will match the newly feature extracted image with the database image and it will display the matched feature extracted image in the axes box. And also if the finger vein image is matched perfectly with the database image then displays an authorized message in the static box as shown in the .The authorized person's details will be displayed in the word document. The vehicle get started only when the person is a authorized person.

V.CONCLUSION

In this paper, the implementation for improving the security and authentication based on biometric system. The developed system includes finger vein matching and controlling the application. The experimental result shows that it takes minimal time that is only 0.5 seconds to verify one input finger vein sample image which is significantly lower than the existing system methods. This system consumes low power and has less computational complexity and hence it is suitable for security applications in vehicle, home, banks and industry etc. Further enhancement involves in interfacing with image processing to provide better authorization and responsiveness.

REFERENCES

[1] Byung Jung Kang, Kang Ryoung Park: "Multimodal biometric authentication based on the fusion of finger vein and finger geometry", Optical Engineering Letters 090501-1, September 2009, vol 48(9).

[2] D. Wang , J. Li, and G. Memik, "User identification based on finger vein patterns for consumer electronics devices", IEEE Transactions on Consumer Electronics, vol. 56, no. 2, pp. 799-804, 2010.

[3] D. Mulyono and S. J. Horng, "A study of finger vein biometric for personal identification", Proceedings of the International Symposium Biometrics and Security Technologies, pp. 134-141, 2008.

[4] H. Lee, S. Lee, T. Kim, and HyokyungBahn, "Secure user identification for consumer electronics devices," IEEE Transactions on Consumer Electronics, vol.54, no.4, pp.1798-1802, Nov. 2008.

[5] Jiang Hong, GuoShuxu, Li Xueyan, QianXiaohua: "Vein Pattern Extraction Based on the Position-Gray-Profile Curve", 978-1-4244-4131-0/09/$25.00 ©2009 IEEE

[6] K. Jain, S. Pankanti, S. Prabhakar, H. Lin, and A. Ross, "Biometrics: a grand challenge", Proceedings of the 17th International Conference on Pattern Recognition (ICPR), vol. 2, pp. 935-942, 2004

[7] P. Corcoran and A. Cucos, "Techniques for securing multimedia content in consumer electronic appliances using biometric signatures," IEEE Transactions on Consumer

Electronics, vol 51, no. 2, pp. 545-551, May 2005.

[8] SeptimiuCrisan, Ioan Gavril Tarnovan, Titus Eduard Crisan: "Radiation optimization and image processing algorithms in the identification of hand vein patterns", Computer Standarts& Interfaces 32, 2010, pp 130-140

[9]. Y. Kim, J. Yoo, and K. Choi, "A motion and similarity-based fake detection method for biometric face recognition systems," IEEE Transactions on Consumer Electronics, vol.57, no.2, pp.756-762, May 2011