



International Journal of Engineering, Business and Enterprise Applications (IJEBA)

www.iasir.net

AN EMBEDDED REAL TIME FINGER VEIN RECOGNITION SYSTEM FOR ATM

Sonu.p.sam

ME Embedded System Technologies

Anna University

Nehru Institute of Engineering and Technology, Coimbatore, Tamil Nadu, India

Abstract: In consideration of emerging requirements for information protection, biometrics, which uses human physiological or behavioral features for personal identification, has been extensively studied as a solution to security issues. However, most existing biometric systems have high complexity in time or space or both, and are thus not suitable for mobile devices. In this paper, we propose a real-time embedded finger-vein recognition system for authentication on ATM. The system is implemented on embedded platform and equipped with a finger-vein recognition algorithm. We have described and implemented an algorithm for finger-vein recognition system using image processing. In the pc we have database where the authentication the matching will be done & the pc will match the two images until it provides the information to the GSM modem. The GSM modem is used to generate the one time password to the user.

Keywords: ATM, Embedded, Image processing, GSM

I. Introduction

The traditional way to provide private information is by the use of passwords or Personal Identification Numbers (PIN), magnetic swipe cards, keys and smart cards that are easy to implement but are subjected to risk of exposure or being forgotten and are hence unreliable. As a result, biometrics that involve analysis of human biological, physical and behavioral characteristics have been developed to provide more reliable security. A long list of biometric patterns is available. Many systems using these have been developed and implemented, namely face, iris, finger print, palm print, hand shape, voice, signature, gait and so on. Irrespective of this variety of biometric patterns, none of them are completely reliable and secure. In case of fingerprint, the condition of the finger surface (e.g. dryness, sweat) and skin distortion degrades the recognition accuracy. Performance for face recognition depends hugely on facial expressions and illuminations, which can change by occlusions or face-lifts. The biometrics like fingerprint, iris, signature, hand shape, voice, and face do not necessarily provide confidentiality since the features used in the methods are exposed outside the human body. These methods are hence susceptible to forgery. From the point of view of security and convenience, the finger-vein is a promising biometric pattern for personal identification.

II. Literature Survey

In this section we will be describing the various approaches that were used in person identification using biometric systems. A biometric system uses the specific physiological or behavioral features possessed by the user for identification and these features are unique, universal and persistent. These systems include face recognition, fingerprint technology, iris recognition, hand geometry, keystroke, signature and speech recognition.

A. Face Recognition

Facial images are the common biometric feature used for personal identification. Face recognition is mainly performed by two approaches, they are Eigen face based recognition and 3D face recognition. The Eigen face based recognition works by analyzing face images and computing Eigen faces which are faces composed of eigenvectors. The comparison of Eigen faces is used to identify the presence of a face and its identity. The Eigen face technique is straightforward, efficient, and yields generally good results in controlled circumstance. There are also some limitations of Eigen faces. There is limited robustness to changes in lighting, angle, and distance. 2D recognition systems do not capture the actual size of the face, which is a fundamental problem. These limitations affect the technique's application with security camera. 3D face recognition systems make 3D models of faces and compare the 3D faces for recognition. These systems are more accurate because they capture the actual shape of faces. The acquisition of 3D data is one of the main problems for 3D systems. Another face identification technology, Facial thermo grams, uses infrared heat scans to identify facial characteristics. This non-intrusive technique is light-independent and not vulnerable to disguises. Even plastic surgery, cannot hinder the technique. This technique delivers enhanced accuracy, speed and reliability with minimal storage requirements. To prevent a fake face or mold from faking out the system, many systems necessitate the person to smile, blink, or otherwise move in a way that is human before verifying.

1. 2D recognition is affected by changes in lighting, the person's hair, the age, and if the person wears glasses.

2. Requires camera equipment for user identification; thus, it is not likely to become popular until most PCs include cameras as standard equipment.

B. Fingerprint Technology

A fingerprint is the pattern of ridges and grooves on the surface of a fingertip. The fingerprints are highly stable and unique. The uniqueness of fingerprint is determined by global features like valleys and ridges, and by local features like ridge endings and ridge bifurcations, which are called minutiae. The recent studies reveal that probability of two individuals, having the same fingerprint is less than one in a billion. There are various fingerprint matching algorithms like minutiae based matching correlation based matching, genetic algorithms based. Among these, minutiae based matching is the dominated one. In minutiae based matching the similarity of two fingerprints is determined by computing the total number of matching minutiae from the scanned fingerprints. Extraction of minutiae features before matching needs a series of processes, containing alignment computation, image segmentation, image enhancement, and ridge extraction and thinning, minutiae extraction and filtering. Correlation based matching uses one to one correlation between fingerprints. This method gives poor results in fingerprint recognition because correlation cannot recognize elastic-distorted versions of the same fingerprint. In neural network based approach the finger prints are classified by using HAVNET. The number of output nodes of HAVNET was equal to number of enrolled fingerprints. The method was not able to distinguish fingerprints of similar shapes the genetic algorithm based methods try to identify the optimal global alignment between two fingerprints. The process is highly time consuming one.

1. For some people it is very intrusive, because is still related to criminal identification.
2. It can make mistakes with the dryness or dirty of the finger's skin, as well as with the age (is not appropriate with children, because the size of their fingerprint changes quickly).
3. Image captured at 500 dots per inch (dpi). Resolution: 8 bits per pixel. A 500 dpi fingerprint image at 8 bits per pixel demands a large memory space, 240 Kbytes approximately → Compression required (a factor of 10 approximately).

C. Iris Recognition

Iris recognition systems make use of the uniqueness of the iris patterns to identify a person. This system uses a high-quality camera to capture a black-and-white, high-resolution image of the iris (the colored ring surrounding the pupil). Iris recognition consists of five operations; they are image acquisition, iris localization or segmentation, iris normalization and unwrapping, feature encoding, and matching algorithm. In image acquisition step the system takes a high-quality image of the iris, Iris localization takes place to detect the edge of the iris as well as that of the pupil; thus extracting the iris region, Normalization is used to transform the iris region to have fixed dimensions, and hence removing the dimensional inconsistencies between eye images, The normalized iris region is unwrapped into a rectangular region. The feature encoding is used to extract the most discriminating feature in the iris pattern so that a comparison between templates can be done. Finally a decision can be made in the matching step

1. Intrusive.
2. A lot of memory for the data to be stored.
3. Very expensive

D. Hand Geometry

Hand geometry recognition systems use a number of measurements taken from the human hand, including its shape, size of palm, and lengths and widths of the fingers. The technique is very simple, relatively easy to use, and inexpensive. Hand geometry based identification consists of following steps, image capturing and pre-processing, measurements and feature selection and finally classification and verification. The imaging equipment used for hand geometry recognition is simple and it includes a platform where the hand should be placed and a camera. The hand image should be pre-processed to extract the features. Color image is converted into grey scale image with background subtracted. The measured features in hand geometry are finger length, width and palm dimensions. Once the features are measured a statistical analysis is performed for selecting significant features. The extracted features are compared using common distance measures like Euclidean or Hamming distance. Comparison is done by normalized correlation between sample and template feature vectors. If the correlation exceeds the pre-defined threshold, the identity indicated by the user is verified.

1. Very expensive
2. Considerable size.
3. It is not valid for arthritic person, since they cannot put the hand on the scanner properly.

E. Signature Recognition

Signature recognition is based on the way a person signs his or her name. Signatures are a behavioral biometric that change over a period of time and are influenced by physical and emotional conditions of the persons. Professional forgers may be able to reproduce signatures that fool the system. Biometric signatures are used in banking and finance industry in order to restrict duplicate signature frauds. Dynamic signature verification technology is used, where the person make signatures on contact sensitive devices like PDA or tablet PC. This technology is also installed in mobile phones to prevent illegal access, although the device is lost or stolen.

F. Speech Recognition

Speech Recognition (is also known as Automatic Speech Recognition (ASR) or computer speech recognition) is the process of converting a speech signal to a sequence of words, using a computer program. Speech recognition technology was increasingly used within telephone networks to automate as well as to enhance the operator services. Generally there are three approaches to biometric speech recognition; they are Acoustic Phonetic Approach, Pattern Recognition Approach and Artificial Intelligence Approach. Acoustic Phonetic Approach was based on finding speech sounds and providing appropriate labels to these sounds. The pattern-matching approach contains two steps namely, pattern training and pattern comparison. This approach uses a well formulated mathematical framework and establishes consistent speech pattern representations, for reliable pattern comparison, from a set of labeled training samples via a formal training algorithm. The Artificial Intelligence approach is a hybrid of the acoustic phonetic approach and pattern recognition approach.

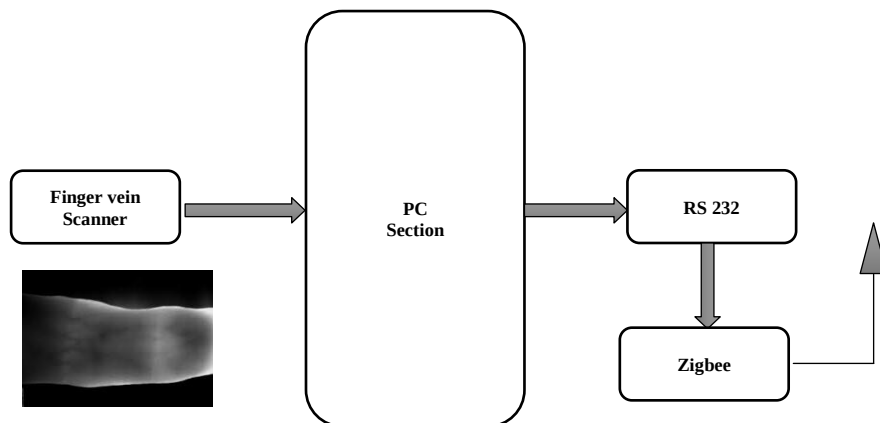
From the point of view of security and convenience, the finger-vein is a promising biometric pattern for personal identification. The finger-vein has following advantages over other biometrics

1. Every individual has a unique pattern of veins and it is even different in case of identical twins. As the individual grows, the veins do become larger, but the position and number of veins do not change from infancy.
2. As the vein structure is underneath the skin, it is invisible to the naked eye and is very complex that it cannot easily spoof the system.
3. It is more acceptable by user because non- invasive and contactless capture of finger-vein provides convenience and hygiene.
4. It is a natural and convincing proof that the person whose finger- vein is captured is alive, since finger-vein pattern can only be taken from a live body.

III. System Analysis

Analysis of finger-vein based biometric security system has been carried Operating System using MATLAB. From each people the forefinger, middle finger, and ring finger of both hands are considered. The image which is obtained from the real- time camera. The image after preprocessing, while matching two types of errors results in the finger-vein based biometric verification security system. The errors are false rejection rate and the false acceptance rate. False rejection is a claim that a genuine image is considered as impostor. False acceptance is a claim that an impostor image is considered as genuine. When the false rejection rate and the false acceptance rate are equal, then the performance of the system is evaluated as equal error rate. This system is suitable for mobile device applications with low computational complexity. Although MATLAB is intended primarily for numerical computing, an optional toolbox uses the MuPAD symbolic engine, allowing access to symbolic computing capabilities. An additional package, Simulink, adds graphical multi-domain simulation and Model-Based Design for dynamic and embedded systems. MATLAB's Graphical User Interface Development Environment (GUIDE) provides a rich set of tools for incorporating graphical user interfaces (GUIs) in M-functions. Using GUIDE, the processes of laying out a GUI (i.e., its buttons, pop-up menus, etc.) and programming the operation of the GUI are divided conveniently into two easily managed and relatively independent tasks

Figure 1 Finger vein scanner & pc section



IV Methodology

A Finger-Vein recognition system consists of two stages - enrollment stage and verification stage. Both stages consist of following steps.

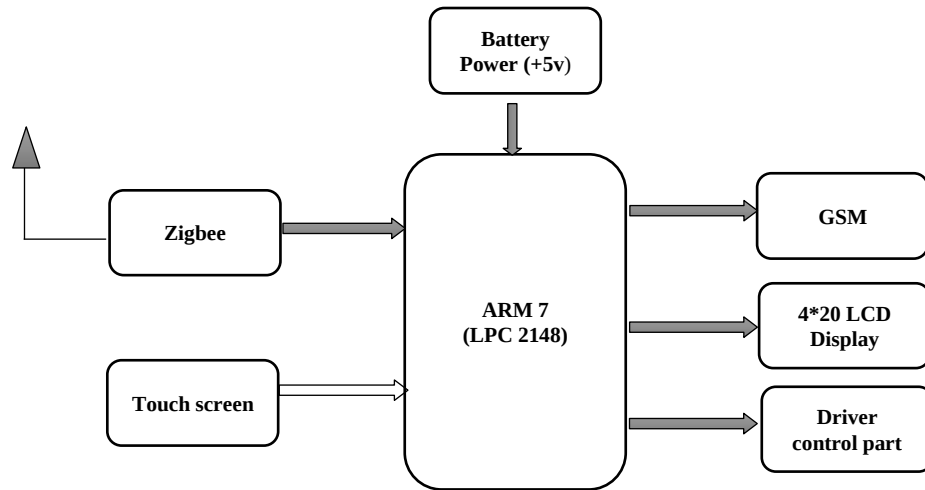
A Image Acquisition

Image acquisition is of two type off-line and on- line. In image acquisition, we are using off-line images. On-line images are the images which are taken real time and off-line images means the images which are taken from already created database.

1) Resizing

By this, the dimensions of the image are changed to the required new width and height

Figure 2 Receiver Section



Resize an image

Syntax

`B = imresize(A,m,method)`

`B = imresize(A,[mrows ncols],method)`

`B = imresize(...,method,n)`

`B = imresize(...,method,h)`

Description

`imresize` resizes an image of any type using the specified interpolation method. `method` is a string that can have one of these values:

1. 'nearest' (default) uses nearest neighbor interpolation.
2. 'bilinear' uses bilinear interpolation.
3. 'bicubic' uses bicubic interpolation.

If you omit the `method` argument, `imresize` uses the default method of 'nearest'.

`B = imresize(A,m,method)` returns an image that is `m` times the size of `A`. If `m` is between 0 and 1.0, `B` is smaller than `A`. If `m` is greater than 1.0, `B` is larger than `A`.

`B = imresize(A,[mrows ncols],method)` returns an image of size `[mrows ncols]`. If the specified size does not produce the same aspect ratio as the input image has, the output image is distorted.

When the specified output size is smaller than the size of the input image, and `method` is 'bilinear' or 'bicubic', `imresize` applies a lowpass filter before interpolation to reduce aliasing. The default filter size is 11-by-11.

You can specify a different order for the default filter using

`[...] = imresize(...,method,n)`

`n` is an integer scalar specifying the size of the filter, which is `n`-by-`n`. If `n` is 0 (zero), `imresize` omits the filtering step.

You can also specify your own filter `h` using

`[...] = imresize(...,method,h)`

`h` is any two-dimensional FIR filter (such as those returned by `ftrans2`, `fwind1`, `fwind2`, or `fsamp2`).

B. Image Enhancement

Image enhancement is used to improve the quality of an image. It is used to improve image contrast and brightness characteristics as well as to reduce noise contents. It highlights certain features of interest in an image. Histogram equalization is a technique for adjusting image intensities to enhance contrast. Let f be a given image represented as a m_r by m_c matrix of integer pixel intensities ranging from 0 to $L - 1$. L is the number of possible intensity values, often 256. Let p denote the normalized histogram with a bin for each possible intensity. So p_n = number of pixels with intensity n / total number of pixels "image histogram" is a type of histogram that acts as a graphical representation of the tonal distribution in a digital image. It plots the number of pixels for each tonal value. By looking at the histogram for a specific image a viewer will be able to judge the entire tonal distribution at a glance. Image histograms are present on many modern digital cameras.

Photographers can use them as an aid to show the distribution of tones captured, and whether image detail has been lost to blown-out highlights or blacked-out shadows. The horizontal axis of the graph represents the tonal variations, while the vertical axis represents the number of pixels in that particular tone. The left side of the horizontal axis represents the black and dark areas, the middle represents medium grey and the right hand side represents light and pure white areas. The vertical axis represents the size of the area that is captured in each one of these zones. Thus, the histogram for a very dark image will have the majority of its data points on the left side and center of the graph. Conversely, the histogram for a very bright image with few dark areas and/or shadows will have most of its data points on the right side and center of the graph.

C. Wavelet Transform

In order to analyze signals of very different sizes, it is necessary to use time- frequency atoms with different time supports. The wavelet transform decomposes signals over dilated and translated functions called wavelets, which transform a continuous function into a highly redundant function

D Feature Extraction

In pattern recognition and in image processing, feature extraction is a special form of reduction. When the input data to an algorithm is too large to be processed and it is suspected to be very redundant (e.g. the same measurement in both feet and meters, or the repetitiveness of images presented as pixels), then the input data will be transformed into a reduced representation set of features (also named features vector). Transforming the input data into the set of features is called feature extraction. If the features extracted are carefully chosen it is expected that the features set will extract the relevant information from the input data in order to perform the desired task using this reduced representation instead of the full size input. One very important area of application is image processing, in which algorithms are used to detect and isolate various desired portions or shapes (features) of a digitized image or video stream. It is particularly important in the area of optical character recognition.

V Conclusion

In this paper, we presented a finger-vein based biometric security system that can be used for security based electronic devices. The method can extract the finger-vein feature for recognition from the NIR images. This method uses single sample and is convenient to the application. This work can be extended with increasing the database for further verification. The project has demonstrated and proved the capability of personal identification based on vein patterns. Although the scale is small, other applications can be extended by solutions which are used in this project. For large applications, some modules should be done in hardware in order to improve the speed of the whole system. If problems of accuracy and speed are solved there is a huge market waiting for the system such as ATMs, cars, houses, cell phones, entrance doors, etc

VI References

- [1] A. 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)
- [2] ATM security System using fingerprint biometric identifier: An Investigative Study, By- Saatci, V avsanogh, M. Purser. Year of publishing paper 2009-2010 IEEE.
- [3] 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.
- [4] D. D. Hwang and I. Verbauehede, "Design of portable biometric authenticators - energy, performance, and security tradeoffs," IEEE Transactions on Consumer Electronics, vol. 50, no. 4, pp. 1222-1231, Nov. 2004.
- [5] 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 Application, vol. 15, no. 4, pp. 194-203,
- [6] H. Lee, S. Lee, T. Kim, and Hyokyung Bahn, "Secure user identification for consumer electronics devices," IEEE Transactions on Consumer Electronics, vol. 54, no. 4, pp. 1798-1802, Nov. 2008
- [7] Novianto, Suzuki, and Maeda, "Optimum estimation of local fractal dimension based on the blanket method," Transactions of the Information Processing Society of Japan, vol. 43, no. 3, pp. 825-828
- [8] 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 2010
- [9] P.K. Amurthy and M.S. Reddy, "Implementation of ATM Security by Using Fingerprint recognition and GSM", International Journal of Electronics Communication and Computer Engineering vol. 3, no. 1, pp. 83-86, 2012.
- [10] "Smart Card & Security Basics"-CardLogix, paper no.: 710030 www.cardlogix.com [2] "Smart card based Identity Card And Survey"-White Paper JKCSH (Jan Kremer Consulting Services).
- [11] W. Song, T. Kim, H. C. Kim, J. H. Choi, H. Kong and S. Lee, "A finger-vein verification system using mean curvature", Pattern Recognition Letters, vol. 32, no. 11, pp. 1541-1547, 2011.
- [12] Y. Kim, Y. 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
- [13] Y. G. Dai and B. N. Huang, "A method for capturing the finger-vein image using non uniform intensity infrared light", Image and Signal Processing, vol. 4, pp. 27-30, 2008.
- [14] Z. Liu, Y. Yin, H. Wang, S. Song, and Q. Li, "Finger vein recognition with manifold learning", Journal of Network And Computer Applications, vol. 33, no. 3, pp. 275-282, 2010