BIOMETRICS AS AN APPROACH TOWARDS IDENTIFICATION AND SECURITY

SUMAN RANI , BEANT KAUR

Abstract: With an increasing emphasis on security, automated personal identification based on biometrics has been receiving extensive attention over the past decade. The patterns are described be certain quantities, qualities, traits, notable features and so on. Each individual has a pattern which is different from the patterns of others. That's the reason why it is suitable for the fulfillment of emerging requirements of reliable and highly accurate personal identification in a number of applications like international border crossings, access to buildings, laptops and mobile phones. By using biometrics, it is possible to recognize a person based on who you are, rather than by what you possess like an ID card or what you remember likea password. Most of the authentication systems based onknowledge-based security like passwords and token-based security like ID cards can be easily violate when a password is disclosed to an unauthorized user or a card is stolen by a fraud. Biometric systems have addressed the security problems that plague traditional verification systems because they make use of a person's fingerprint, hand shape, iris, face and voice that are supposed to be uniqueto that person.

Keywords: Biometrics, identification, problems, security.

Introduction: Biometrics based solutions are able to provide for confidential, financial transactions and personal data privacy. The need for biometrics can be found in federal, state and local governments, in the military and in commercial applications. A biometric system is essentially a pattern recognition system, which makes personal identification by determining the authenticity of a specific physiological or behavioral features processed by the user. A biometric system can be either an identification system or a verification system such as biometric can be used to determine a person's identity even without his knowledge, is known as identification and it also can be used to verify a person's identity known as verification. Biometrics is unique identities. These are refers to automatic identification of people based on their distinctive physiological (eg. Face, fingerprints, iris, retina, hand geometry, signature, handwriting) and behavioral like voice characteristics, should be an essential component of security system because these can't be shared, misplaced and they represent individual's identity.

Biometric system components:

A. Sensor: collects data and convert the information to a digital format.

B. Signal Processing Algorithms: perform quality control activities and develop the biometric template.

C. Data Storage: keeps information that new biometric templates will be compares to.

D. Matching Algorithm: Compares the new biometric template to one or more templates in data storage.

E. Decision Process: Uses the results from the matching component to make a system level decision.

Biometric Technologies: There are many biometric technologies to suit different types of applications:

A. Fingerprints: Fingerprints are distinct to each person because of unique papillary features and are different even in twins. There are three major types of fingerprint scanners—capacitive, sweep and optical. The optical scanner is the reliable one. A fingerprint looks at the patterns found on a fingertip. There are a variety of approaches to fingerprint verification, such as traditional police method, using pattern-matching devices, and things like more fringe patterns and ultrasonic.

The method of Fingerprint recognition:

We used a commercial algorithm for fingerprint recognition. As shown in fig. 1, direction components in the captured fingerprint image are extracted. Next, thinning the image by using fingerprint direction components is performed. From that, fingerprint feature points such as minutia are located in the thinned image, and then fingerprint codes are acquired using the feature points [1].

B. Hand Geometry: This involves analysis and measuring the shape of the hand. It might be suitable where there are more users or where user accesses the system infrequently. Accuracy can be very high if desired and flexible performance tuning and configuration can accommodate a wide range of applications. Organizations are using hand geometry

C. Retina: a retina-based biometric involves analyzing the layer of blood vessels situated at the back of the eye. This technique involves using a low intensity light source through an optical computer to scan the unique patterns of the retina. Retinal scanning can be quite accurate but does require the user to look into a receptacle and focus on a given point. Even eyes of identical twins are found to have different retina patterns. It is therefore utilized in

situations where a high security biometric system is required. The system requires user cooperation and controlled environment for operation. The user must position the eye at a fixed distance from the camera, look directly into the lens and remain perfectly still while the retina is being scanned.
The proposed retinal recognition system consists of four stages i.e preprocessing, vascular pattern extraction, feature extraction and filtration and biometric pattern matching [3].

readers in various scenarios, including time and attendance recording. Overview of finger-vein recognition algorithm is shown in fig 2 below [1-2]:

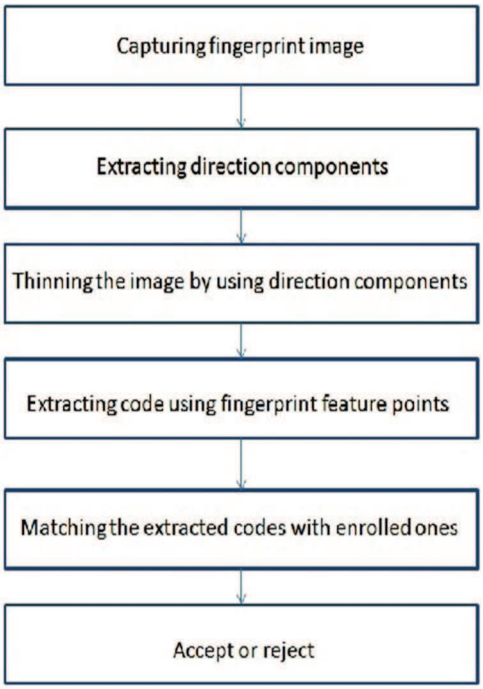

Fig. 1: Fingerprint Recognition Algorithm

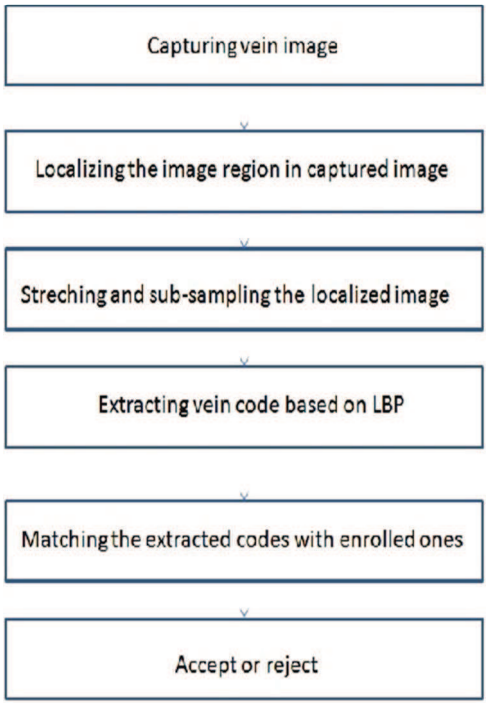

Fig. 2: Vein recognition algorithm

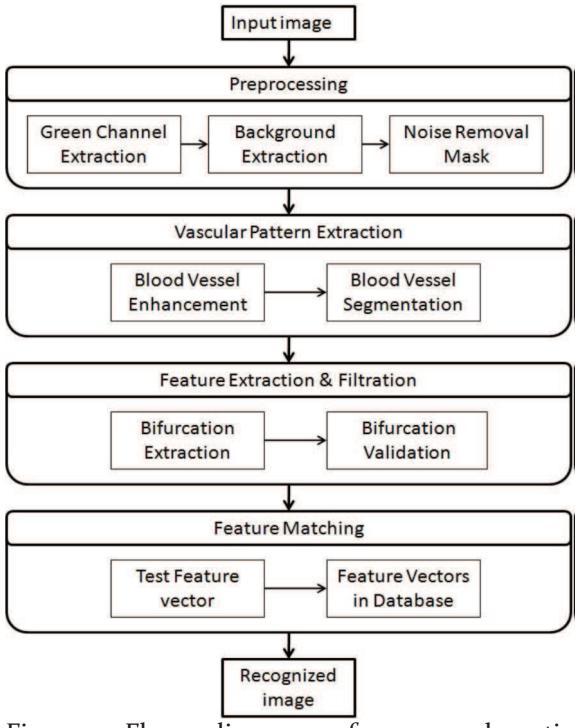

Fig. 3: Flow diagram of proposed retinal recognition system

D. Iris: an iris-based biometric involves analyzing features found in the colored ring of tissue that surrounds the pupil. This uses a fairly conventional camera element and requires no close contact between the user and the reader. Further, it has the potential for higher than average template- matching performance. The system requires user cooperation and controlled environment.
An iris recognition system is composed of three main stages [2].
I) Preprocessing Stage: which includes determining the boundary of the iris within the eye image, and

extract the iris portion from the image to facilitate its processing.

2)Feature Extraction Stage: consisting of the extraction of the features from the preprocessed iris image.

3) Recognition Stage: in which the feature of the iris pattern are compared with those of all patterns in the database.

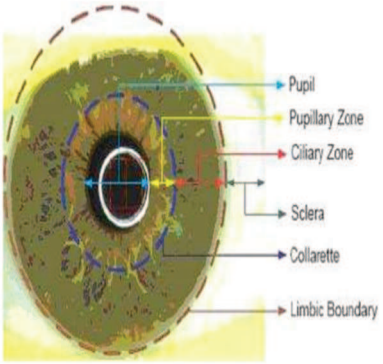

Fig. 4: Salient features in the anterior portion of the iris [4].

E. Face: Face recognition analyses facial characteristics. It requires a digital camera to develop a facial image of the user for authentication. Because facial scanning needs an extra peripheral thing that is not included in basic PCs, it is more of a niche market for network authentication. During identification, a facial recognition system automatically singles out and processes data that characterize the most distinctive facial features: nose, lips, eyebrows contours or distances between these features. These data are used to generate digital biometric templates that are subsequently used for matching.

The ability of Face recognition biometric system is expected to identify faces present in the images using biometric identification and the visual perception. The FRBS concentrates only on biometric identification of the face image subjected under various dark illuminations. Though the familiar systems like fingerprint identification, iris identification, gender, ethnicity, etc., are said to be biometric identifications, facial recognition plays an important role in the field of identifying a person. Such a FRBS system undergoes a three step process such as Preprocessor, Feature Descriptor and Recognizer. Figure3.1 depicts the conceptual model of the FRBS [1].

The face recognition biometric system undergoes some sequential steps to identify a matcher from the existing data set. The procedure for FRBS is as follows:

F. Handwriting: handwriting is unique and distinct for each person. To automatically (without human intervention) identify users by their handwriting, it is sufficient to have three text lines. Text sources can be as follows: hand-written applications, completed questionnaires, memo books, etc. handwriting samples are converted into an electronic format by using ordinary scanners, upon which digital handwriting templates are enrolled into a biometric identification system. Having received an identification request, a biometric system compares the previously enrolled biometric data with the newly produced handwriting samples and produces exhaustive search results.

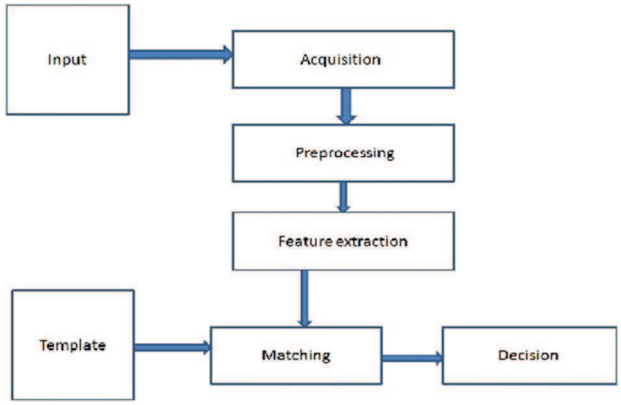

Fig. 6: Handwriting reorganization system[5]

Handwriting is unique to each individual [6].handwriting may be similar styles of some people acquired when these people learned to write by copying letters and words from handwriting, they tend to take on individual styles with age. One of the most important aspects of document analysis is the document segmentation. Straight segmentation [6-7] tries to decompose the image in a set of sub images, each one corresponding to a character. In segmentation-recognition strategies [8-10] the image is subdivided in a set of sub images (strokes) whose combinations are used to generate character candidates. The process of over segmentation is the number of sub images is greater than the number of characters of the ages.

No single handwriting feature proves anything specific or absolute by itself and a single feature can only identify a trend. It is show that the combination of features, and the interaction each other so that enable a full and clear interpretation [7].

G. Voice: Voice Recognition techniques are used in a number of application areas related to processing user requires by phone (such as call-centers), which allows faster servicing of clients and reduced operator workload. In high-value projects, voice recognition is good at supplementing other biometric technologies (mostly fingerprint biometrics). Human speech is divided into several segments, composed of several dominant frequencies called formants. These segments are then digitized, and the biometric templates, the so-called voice prints, are generated.

For identification, the previously enrolled voice prints and newly produced ones are compared for matching.

H. Signature: Signature verification analyses the way user signs his name. Signing features such as speed, velocity and pressure are as important as the finished signature's static shape. People are used to signatures as a means of transaction-related identity verification. It is a behavioral biometric. Automated systems can be both offline and online. Offline systems would have to work only using the characteristics of the signature. Online systems, on the other hand, can utilizes features obtained while providing the sample such as speed of writing, total time for signature, the pen pressure, pen inclination and number of pen up and downs, besides using the various characteristics of the signature itself.

I. Lips Print: The image data from a lip print is considered as a connective appearance with the directional local pattern. The local masks extract the information on the local patterns for a lip print, including the vertical, the horizontal, and the diagonal patterns. One of the advantages of the pattern kernels through the local masks is the small data required to represent unique personal information for recognition. The discrimination criteria either recognize a person from the input image from classes or reject him if the input image is unknown. The multi-resolution architecture is proposed in order to reduce both the noise and the false recognition rate [9].

Advantages of Biometrics: Enhanced Security, Convenient to control, Auditable trial, Accuracy, Reduced paperwork, Cost effective, Cannot be copied or shared, Cannot be lost.

Disadvantages of Biometrics: Adaptability to rate of change, Privacy concerns, Dangers to owners of secured items.

Future Aspects: There are always concerns about adapting to new technologies. The future of biometrics looks increasingly bright with the demand for security rising daily. Although companies are using biometrics for authentication in a variety of situations, biometric technologies are evolving and emerging towards a large scale of use.

Standards like the Common Biometric Exchange File Format, Biometric Assurance and Public-Key Infrastructure (PKI) are being developed to provide a common software interface to allow sharing of biometric templates.

India's Universal Identification (UID) programme seeks to provide a unique identity to all its residents. Now in initial stages, this UID programmes is the largest biometric identification programme in the world.

References:

1. Young Ho Park, "A Multimodal Biometric Recognition of Touched Fingerprint and Finger-vein", 2011 International Conference on Multimedia and Signal Processing, 978-0-7695-4356-7/11 $26.00 © 2011 IEEE.
2. Shimaa M. Elsherief, Mahmoud E. Allam, Mohamed W. Fakhr, "Biometric Personal Identification Based on Iris Recognition", 1-4244-0272-7/06/$20.00 ©2006 IEEE.
3. S. Zeenathunisa, "A BIOMETRIC APPROACH TOWARDSRECOGNIZING FACE IN VARIOUS DARKILLUMINATIONS",978-1-4577-1894-6/11/$26.00©2011 IEEE.
4. Ales Muron and JaroslavPospisil, "The human iris structure and its usages," Acta Univ. Palacki. Olomuc. Fac. Rerum Nat. Phys., vol. 39, pp. 87–95, 2000.
5. M. UsmanAkram_,AnamTariqy and Shoab A. Khan, "Retinal Recognition: Personal Identification using Blood Vessels", 978-1-908320-00-1/11, 2011, IEEE.
6. David A. Katz, Handwriting Analysis.
7. K. Pankaj, K. Asha, "Comparative analysis of offline Handwriting Recognition Using Invariant Moments with HMM and combined SVM-HMM classifier",2013 International Conference on Communication Systems and Network Technologies, 978-0-7695-4958-3/13 $26.00 © 2013 IEEE.
8. Kimura F. et al., Improvements of a Lexicon Directed Algorithm for Recognition of Unconstrained Handwritten Words. *Proc 2nd ICDAR* Tsukuba October 20-22 1993 pp. 18-22.
9. Cesar M. and Shingal R., Algorithm for segmenting handwritten postal codes. *Int'l J. Man Machine Studies* **33** (1) 1990 pp. 63-80.

***

Research Scholar (M.Tech), Department of ECE, Punjabi University, Patiala, INDIA
sumanrani002@gmail.com
Assistant Professor, Department of ECE, Punjabi University, Patiala, INDIA
sandhu.beant@gmail.com