Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 2, Issue. 5, May 2013, pg.232 – 237

SURVEY ARTICLE

Literature Survey on Automated Person Identification Techniques

Sruthy Sebastian[1]

[1]Department of Computer Science and Engineering, Nehru College of Engineering and Research Center, Kerala

[1] *sruthyksebastian@gmail.com*

Abstract— A wide variety of organizations are using automated person identification systems to improve customer satisfaction, operating efficiency as well as to secure critical resources. This paper gives a literature survey on the recent developments in person identification techniques and the survey highlight on two major approaches for automatic human identification, namely biometric identification and gait identification. Gait identification provides a way to automatic person identification at distance in visual surveillance and monitoring applications.

Key Terms: - biometric recognition; gait recognition; visual surveillance

I. INTRODUCTION

Automated person identification is highly researched in recent years because of its applications, like protected access to computer systems, buildings, cellular phones, ATMs and video surveillance. Person identification is the process of associating an identity to an individual. Person identification techniques are broadly classified into three, namely knowledge based, token based, and biometric based. A knowledge-based approach depends on something an individual knows to make a personal identification, like a password or a personal identification number (PIN). Token-based approaches are based on something an individual have to make a personal identification like a passport, driver's license, ID card, credit card, or keys. These two approaches have several demerits: tokens may be stolen, lost, forgotten or misplaced. The password or PIN code can be forgotten by an authenticated person or predicted by an attacker. The biometric systems use physiological or behavioural features of an individual for identification and it cannot be stolen or lost.

The biometric identification method consists of three operations; they are firstly capture biometric sample of the person and make a digital representation of the sample, then extract distinctive features from the digital representation using feature extractor, and finally compare the extracted feature set against the template set in the database.

Generally automatic gait recognition consists of following operations: subject detection, silhouette extraction, feature extraction, feature selection, and classification. Once moving subjects are seized, individuals will be discovered and separated from the image background. After individuals have been alienated from the background, characteristics that can be used for recognition are extracted from these segmented walking persons.

The rest of the paper is organized as follows: Section 2 gives a literature review on recent advances in biometric identification systems. Section 3 gives a literature review on developments in automated gait identification schemes Section 4 gives an abstract view of activity based person identification. Section 5 compares the different automated identification schemes based on certain performance criteria. Finally concluding remarks are given.

II. LITERATURE REVIEW ON BIOMETRIC SYSTEMS

In this section we will be describing the various approaches that were used in person identification using biometric systems. A biometric system is 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

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 shinning, 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.

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.

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. Colour 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.

e. Keystroke

It is estimated that each person types on a keyboard in a distinctive way. Keystroke dynamics is a behavioral biometric; for some individuals, we can observe large variations in typical typing patterns. Further, the keystrokes recognition can be done unobtrusively when the person is keying in information. Behavioral characteristics measured by keystroke recognition include: the cumulative typing speed, the time that elapses between consecutive keystrokes, the time that each key is held down, the frequency with which other keys, such as the number pad or function keys, are used and the sequence used to type a capital letter

f. Signature

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 parson 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.

g. 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.

III. LITERATURE REVIEW ON GAIT RECOGNITION

Gait recognition is based on a person's style walking. Gait recognition has several unique features. The supreme feature is its unobtrusiveness, which does not require observed subjects' attention and cooperation. Also, human gait can be captured at a far distance without requiring physical information from subjects. Technically gait recognition can be classified into three, namely machine vision (MV) based, floor sensor (FS) based and wearable sensor (WS) based.

a. Machine vision (MV) based gait recognition

In this category, gait (an individual's way of walking) is captured using a video-camera from distance. Video and image processing techniques are employed to extract gait features for recognition purposes. Features used for person verification can be stride and cadence or static body parameters like height, the distance between head and pelvis, the maximum distance between pelvis and feet, and the distance between feet. Stride and cadence are based on body height, weight, and gender, and we use these biometrics for identification and verification of people. The cadence is measured using the periodicity of a walking person. Using a calibrated camera system, the stride length is measured by first tracking the person and computing their distance travelled over a period of time. Most of the MV based gait recognition algorithms are based on the human silhouette. That is the image background is removed and the silhouette of the person is extracted and analyzed for recognition. Application areas for machine vision based gait recognition are usually surveillance and forensics. In robbery cases, the criminal uses a mask to hide his face and puts gloves on his hand, so that no face or fingerprints can be captured or left, but cameras can record the gait of the criminal.

b. Floor sensor based gait recognition

In floor sensor based approach, a set of sensors or force plates are installed on the floor. Such sensors enable to measure gait related features, when a person walks on them. Examples of the gait related features include max, time value of heel strike, max, amplitude value of the heel strike, Stride length, stride cadence and time on toe to time on heel ratio for recognition.

One of the main advantages of floor sensor based gait recognition is in its unobtrusive data collection. The floor sensor based gait recognition can be used in access control application and is usually installed in front of doors in the building. In addition to providing identity information, the FS-based gait system can also indicate location information within a building

c. Wearable sensor based gait recognition

In wearable sensor based gait recognition, gait is collected using body worn motion recording (MR) sensors. The MR sensors can be worn at different locations on the human body. The acceleration of gait, which is recorded by the MR sensor, is utilized for authentication. The MR sensor can attached to the belt of the subjects, around the right hip, lower part of the leg or the MR sensor can carried in the trousers pocket.

One of the main advantages of the wearable sensor based gait recognition is its unobtrusive data collection. The wearable sensor based approach was proposed for protection and user authentication in mobile and portable electronic devices. In the recent future it is feasible to integrate the MR sensor as one of the components in personal electronic devices.

IV. ACTIVITY BASED PERSON IDENTIFICATION

In this persons are identified based on the way they perform different activities. One disadvantage of gait recognition is the assumption that the person under investigation walks, which is not always the case. Most methods proposed in the literature would probably fail in the case where the person performs a different activity, for example if he/she bends. Thus, the activity information should be taken into account in order to provide the correct person ID.

Dynamics observed in different activities may be very distinctive. That is, although people walk in quite a similar way, they may perform other activities, like eating, quite differently. This means that it is more probable to achieve good identification performance if we exploit several, possibly all, different activities a person performs. Indeed, other activities, besides walk, may contain more discriminant information for person identification, as execution style of one activity may uniquely describe a person. A multi-camera setup is used to capture the human body from different viewing angles. This method removes the viewing angle problems of other biometric systems by taking multi-view information from different cameras.

V. COMPARISON

Method	Security level	User Acceptance	Ease of use	Low cost	Errors	Hardware
Fingerprint recognition	▶▶▶	▶▶	▶▶▶	✓	dryness, dirt, age	Special, cheap
Facial recognition	▶▶	▶▶	▶▶	✓	lighting, age, glasses, hair	Common, cheap
Hand geometry	▶▶	▶▶	▶▶▶	✗	hand injury, age	Special, mid-price
Speaker recognition	▶▶	▶▶▶	▶▶▶	✓	noise, weather, colds	Common, cheap
Iris scan	▶▶▶	▶▶	▶▶	✗	poor lighting	Special, expensive
Signature recognition	▶▶	▶▶	▶▶▶	✓	Changing signatures	Special, mid-price
Keystroke recognition	▶▶	▶▶	▶▶▶	✓	Changing speed, characters	Special, cheap
Machine vision based gait recognition	▶▶	▶▶	▶▶▶	✓	viewing angles, clothes, shoe type	Special, cheap
Floor sensor based gait recognition	▶▶▶	▶▶	▶▶▶	✗	viewing angles, walk surface, cloths	Expensive
Wearable sensor based gait recognition	▶▶▶	▶▶	▶▶	✓	Lighting, viewing angles	Special, cheap

VI. CONCLUSION

This paper presents a literature survey on the various techniques involved in person identification. The survey emphasizes on biometric recognition system and gait based recognition systems. Biometrics is reliable way for identification because it is based behavioural or physiological characteristics of a person. Gait based systems provide recognition at a far distance and provide good results in low resolution images where other biometrics are failed. Activity based person identification removes the drawbacks of gait recognition like viewing angle differences, clothes or shoe type differences and walking surface differences because it is based on a set of activities which are view invariant also.

REFERENCES

[1] A. K. Jain, A. Ross, S. Prabhakar, "An Introduction to Biometric Recognition", IEEE Trans. on Circuits and Systems for Video Technology, Vol. 14, No. 1, pp 4-19, January 2004

[2] Matthew A. Turk, Alex P. Pentland, "Face recognition using Eigen faces" Proc. IEEE Conference on Computer Vision and Pattern Recognition: 586–591. 1991.

[3] A. Jain, A. Ross, S. Prabhakar, "Fingerprint matching using minutiae and texture features", International Conference on Image Processing (ICIP), Thessaloniki, Greece, 2001, pp. 282–285.

[4] X. Tan and B. Bhanu, "Fingerprint matching by genetic algorithms," Pattern Recognition, vol. 39, no. 3, pp. 465– 477, 2006

[5] J. Daugman, "Recognizing persons by their Iris patterns," in Biometrics:Personal Identification in a Networked Society, 1999, pp. 103–121.

[6] Lawrence Rabiner, Biing Hwang Juang, "Fundamental of Speech Recognition", Copyright 1993 by AT&T.

[7] Mathias De-Wachter et.al. "Template based continuous speech recognition" IEEE transactions on Audio, speech and Language processing, Vol.15, No.4, May 2007.

[8] C. BenAbdelkader, R. Cutler, and L. Davis. "Stride and cadence as a biometric in automatic person identification and verification", In Fifth IEEE International Conference on Automatic Face and Gesture Recognition, pages 357–362, May 2002.

[9] Amos Y. Johnson and Aaron F. Bobick. "A multi-view method for gait recognition using static body parameters", In Third International Conference on Audio- and Video-Based Biometric Person Authentication, pages 301–311, June 2001.

[10] Lee Middleton, Alex A. Buss, Alex Bazin, and Mark S. Nixon. "A floor sensor system for gait recognition".In Fourth IEEE Workshop on Automatic Identification Advanced Technologies (AutoID'05), pages 171–176, 2005.

[11] A. Iosifidis, A. Tefas, and I. Pitas "Activity-Based Person Identification Using Fuzzy Representation and Discriminant Learning" IEEE transactions on information forensics and security, vol. 7, no. 2, april 2012

