ISSN 2047-3338

Emerging Trends in Wireless Multimedia Technologies: IRIS

S. Koteswari[1], Dr. P. John Paul[2], S. Indrani[3] and S. Srikanth Chetlapalli[4]
[1,3,4]Department of ECE, Andhra Pradesh, India
[2]Department of CSE, GATES Engineering College, Gooty, Ananthapur, Andhra Pradesh, India
eshwari.ngr@gmail.com, jppulipati@yahoo.com

***Abstract*– In the emerging trends in wireless multimedia services and technologies, the term biometrics is gaining increasing attention in these days. Security systems having realized the value of biometrics, specially, biometrics is used for two basic purposes to verify or identify users. The use of fingerprints, facial characteristics and other biometrics for identification is becoming more common. The paper overviews best of Biometric application for security management. The acquisition of biometric data introduces human research and privacy concerns that must be addressed by the organizations. Iris recognition has received increasing attention in recent years. The uniqueness and randomness of human iris patterns enable us to use it as quicker, easier and highly reliable forms of automatic human identification, where in the human iris serves as a type of biological passport, PIN or password. This paper tells about how the iris recognition system works and how it is a reliable approach to human identification. Iris recognition system comprises of iris image acquisition, image processing, feature extraction and pattern matching. This paper also focuses on how Iris is the best Biometric feature for identity Management.**

***Index Term*– Biometrics, Iris Recognition, Fingerprint and Wireless Multimedia**

I. INTRODUCTION

TODAY in our society, we have a lot of situations where we need to identify a person. Traditionally, the ways of identifying a person has been based on what the person knows, like passwords of what the person possesses ID cards, keys, frequency built activators (parking, door openers, etc) and so on. None of these methods are secure. Anything a person possesses might easily be lost or stolen by someone else. Because of this there has been a growing demand of other ways to identify persons, and scientists have started to explore identification based on biometric features. Biometrics is an emerging field of technology using unique and measurable physical, biological or behavioural characteristics that can be processed to identify a person. Biometric features are divided in two categories: behavioural like voice recognition and handwriting and physiological, like iris, retina, face and DNA and fingerprint recognition. Among all of these, the one of most secure method to identify a person is the iris recognition. It was proposed in 1936 by ophthalmologist Frank Burch, but it took more than 50 years to finally start researching it seriously, and first in 1994, Dr. John Daugman patented a set of algorithms that makes up the basis of all current iris recognition system.

The process of iris recognition is composed of four steps:

1. Iris image acquisition
2. Pre-processing of the image by locating the iris, normalising the iris and enhancing the image
3. Extracting the local features of the iris
4. Matching the iris-pattern with an already stored iris-pattern

This paper first gives a short introduction to the properties of the eye and then goes the four steps of iris recognition as well as some applications and advantages over other techniques.

The coloured part of the eye is called the iris. It controls light levels inside the eye similar to the aperture on a camera. The round opening in the centre of the iris is called the pupil. The iris is embedded with tiny muscles that dilate (widen) and constrict (narrow) the pupil size.

The iris's random patterns are unique to each other to each individual-a human "bar code" or living passport. No two irises are alike; each person has distinct patterns of filaments, pits and striations the coloured rings surrounding the pupil of each eye. In this pattern, scientists have identified about 250 degrees of freedom that is 250 non-related unique features of a person's iris. The following images demonstrate the variations found in iris.

II. THE EYE

Fig. 1. The EYE

Fig. 2. Different IRIS

III. IRIS RECOGNITION SYSTEM

Design and implementation of a system for iris recognition can be subdivided into three parts. The first part relates to image acquisition. The second part is concerned with localizing the iris from a captured image. The third part is concerned with matching an extracted iris pattern with candidate data base entries.

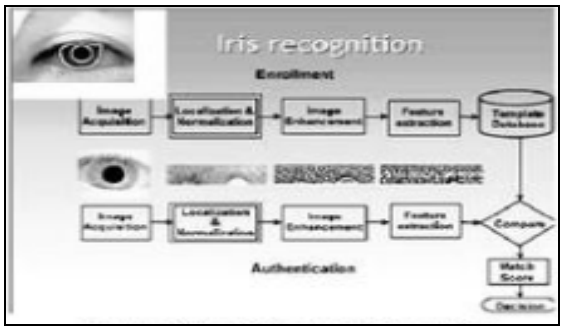

Fig. 3. The schematic diagram of IRIS recognition

There are two phases in process of recognition-enrolment and authentication enrolment is the first time when the iris of subject is scanned and stored in template database for future identification purpose. Authentication is the process in which iris of subject is scanned and compared with the sample in the data base.

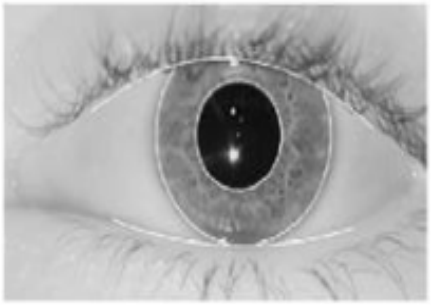

Fig. 4. Localization of the IRIS

A. IRIS Acquisition

The first step is location of the iris by a dedicated camera, not more than three feet from the eye. After the camera situates the eye, the algorithm narrows in from the right and left of the iris to locate its outer edge. This horizontal approach accounts for obstruction caused by the eyelids. It simultaneously loctes the inner edge of the iris (at the pupil), excluding the lower 90 because of inherent moisture and lighting issues.

B. Processing of the Image

IRIS localization: Image acquisition of the iris cannot be expected to yield and image containing only the iris. It will also contain data derived from the surrounding eye region. Therefore, prior to iris pattern matching, it is important to localize that portion of the image derived from inside the limbus (the border between the sclera and the iris) and outside the pupil. If the eyelids are occluding part of the iris, then only that portion of the image without the eyelids should be included.

The task of locating the iris consists of locating the inner and outer boundaries of the iris. Both of these boundaries are circular, the problem lies in the fact that they are not co-centric. Very often the pupil centre is nasal, and inferior, to the iris centre. Its radius can be displaced as much as 15%towards the noise from the centre of the iris. This means that the outer and inner boundaries must be calculated separately, as two independent circles.

Normalization: Now we have the iris located, but still one image of an iris normally will be very different from another image of the same iris. This might be for many reasons.

Size of the image: which is depending on the distance from the camera?

Size of the pupil: the pupil varies with the intensity of light, and so might Sketch or compress the iris tissue, interfering with matching of iris patterns

The orientation of the iris, depending upon the head, tilt, torsion eye rotation within its socket, and camera angles

As well, it is necessary to truncate the boundary zones of the iris. This is because what we have is the iris localized between two perfect circles, and as it turns out, the pupil is not a perfect circle. The outer boundary between the iris and the sclera sometimes is erroneous as a result of the subject using contact lenses. To normalize the representation of the iris, the image of the iris is converted from Cartesian to doubly dimensionless polar reference form.

Fig. 5. Transformation from Cartesian to polar reference form

Enhancement of Images: The image we are working with is not optimally sharp in contrast, and might have a non-uniform illumination because of the positioning of the light source when the image was captured. It is therefore necessary to enhance the image; otherwise reading of the iris pattern might

Figure 6: Texture image before enhancement.

Figure 7: Texture image after enhancement.

Fig. 8. IRIS-code generation

not be successful. The enhancements consist of sharpening the picture with a sharpening mask, and reduce the effect of non-uniform illumination.

Features Extraction: one of the important step in extracting is generating iris code. Iris recognition technology converts the visible characteristics into a 512 byte iris code, a template stored for future identification attempts. From the iris 11mm diameter, Daugman's algorithms provide 3,4 bits of data per square mm. This density of information is such that each iris can be said to have 266 'degree if freedom'. This '266' measurement is cited in most iris recognition literature; after allowing for the algorithm's correlative functions and for characteristics inherent to most human eyes, Daugman concludes that 173 "independent binary degrees of freedom" can be extracted from this algorithm. A key differentiator of iris scan technology is the fact that 512 byte templates are generated for every iris, which facilitates match speed (capable of matching over 500,000 templates per second).

Matching the IRIS Pattern: It is stored one after iris localisation, the final step is pattern matching of the iris image with other images from the database. First the iris image of the person to be identified is captured and then compared with the images existing in the database. After localizing and aligning the image containing the iris, the next task is to decide if this pattern matches with the one existing in the database. A particular user is declared as authenticated and valid only if a match is found.

To perform the recognition two iris codes are compared. The amount of difference between two iris codes is based on the Euclidean distance between the two corresponding Finger Codes and hence is extremely fast. We are able to achieve a verification accuracy which is only marginally inferior to the best results of statistically -based algorithms. Our system performs better than a state-of-the-art statistical -based system when the performance requirement of the application system does not demand a very low false acceptance rate. Therefore the key concept to iris recognition is failure of test of statistical independence.

IV. COMPARISON WITH OTHER TECHNIQUES

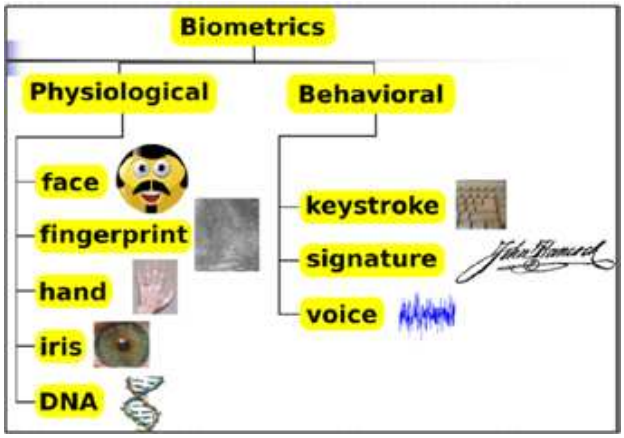

Fig. 9. Classification of biometrics

Face Recognition: It is an oldest recognition method and it is best done by human. Light intensity, age, glasses hairstyle, beard shape and face covering mask may change verification success rate.

Fingerprint Recognition: One of the most well-known biometric, unique for every human, even twins. But is is not as accurate as iris recognition. False accept rate is approximately one in one lakh.while iris recognition false accept rate is one in 1.2 million.

Voice Recognition: It identifies speaker from short utterance. The main threat in this system is the valiant imitate voice can deceive equipment. So, it appears to be weak biometric technology.

DNA is unique to every human, and can be obtained from many sources.also it doesn't change through the life, but there are some difficulties using this techniques viz.DNA are identical in twins, contamination can cause failure of test, cannot be implemented in real time. Hence iris recognition technique proves to be a most accurate and suitable biometric technique.

V. APPLICATIONS AND ADVANTAGES

Iris scan technology has been piloted in ATM environments in England, the US, Japan and Germany since as early as 1997. In these pilots, the customer's iris data became the verification tool for access to the bank account, thereby eliminating the need for the customer to enter a PIN number or password. When the customer presented their eyeball to the ATM machine and the identity verification was positive, access was allowed to the bank account. These applications were very successful and eliminated the concern over forgotten or stolen passwords and received tremendously high customer approval ratings. The system that enables fast and easy identity verification in order to expedite their path through passport control.

Other application include monitoring prison transfers and releases as well as projects designed to authenticate on-line banking, on-line voting and on-line stock trading to name just a few, iris scan offers a high level of user security, privacy and general peace of mind for the customer. A highly accurate technology such as iris scan has a vast appeal because the

inherent argument for any biometrics is, of course, increased security. The airports have begun to use iris scanning for such diverse functions as employee identification/verification for movement through secure areas and allowing registered frequent airline passengers:

1) The iris is a thin membrane on the interior of the eyeball. Iris patterns are extremely complex.
2) Patterns are individual (even in fraternal or identical twins)
3) Patterns are formed by six months after birth, stable after a year. They remain the same for life
4) Works even through the subject uses sunglasses or contact lenses,
5) Imitation is almost impossible
6) Patterns are easy to capture and encode.
7) Very resistant to false matching (1/1.2 million) and fraud.

Table I: Comparison of Techniques

Techniques	Misidentification rate	Security	Applications
Iris Recognition	1/1,200,000	High	High-security
Fingerprinting	1/1,000	Medium	Universal
Hand Shape	1/700	Low	Low-security facilities
Facial Recognition	1/100	Low	Low-security facilities
Signature	1/100	Low	Low-security facilities
Voice printing	1/30	Low	Telephone service

VI. CONCLUSION

The iris is one of the most unique, data rich physical structures on the human body, and one of the most robust ways to identify humans; it works even though the subject uses sunglasses or constant lenses. The properties of the iris that enhance its suitability for use in automatic identification include its natural protection from the external environment, impossibility of surgically modifying without the risk of vision. Physiological response to light that is unique (which makes sure that the eye that is scanned belongs to a living person) permanent features and case of registering its image at some distance. Biometrics is used for identification purposes. They are usually classified as physiological or behavioral. Sometimes a certain biometric can be classified as both. As we continue to progress into the future, more and more biometric schemes will become available. Also, more of the existing biometric schemes will advance further for a higher level of security. All biometrics have to go through a process which is capture, process, and comparison. As the need for security increases, so will the need for biometrics! It will definitely be interesting to see what the future holds for bioinformatics.

REFERENCES

[1] www.sciencedirect.com
[2] Dr. Mustafa H. Dahshan, Computer Engineering Department, College of Computer & Information Sciences, King Saud University.
[3] John Daugman, "How Iris Recognition Works", IEEE Transaction paper, Vol. 14, JANUARY 2004
[4] S. Kulkarni, Madhuri A. "Under The inbuilt password: iris", International Journal of Biometrics, Vol. 9, January 2004.
[5] www.wikipedia.com IRIS Recognition,
[6] www.cl.cam.ac.uk/~jgd1000/iris_recognition.htl
[7] Biometrics,scgwww.epfl.ch/courses/Biometrics-Lectures-2007-2008-pdf/07-Biometrics-Lecture-7-Part2-2-2007-11-05.pdf
[8] www.biometrics.gov/Documents/IrisRec.pdf
[9] Biometrics the Ultimate Reference by John D. Woodward-Jr., Nicholas M. Orlans, Peter T. Higgins (Dreamtech Press).

S. Koteswari

Dr. P. John Paul

S. Indrani

S. Srikanth Chetlapalli