Biometric Authentication: IRIS image Capture, Storage and Processing

In this era of Information technology, we all have multiple accounts and use multiple passwords on host of computers and Web sites for checking e-Mail, managing bank accounts, online transactions etc. Maintaining and managing access while protecting both the user's identity and the computer's data and systems has become increasingly difficult. Central to all security is the concept of authentication - verifying that the user is who he claims to be.

MUKUL SAXENA
District Informatics Officer
NIC Faizabad
mukul.saxena@nic.in

Edited by
Anshu Rohatgi

Broadly speaking, in digital world we can authenticate and identity a person in three ways - by something the user knows (such as a password or personal identification number), something the user has (a security token or smart card) or something the user is (a physical characteristic, such as a fingerprint, called a biometric). Password, tokens and smart cards are perhaps the most commonly used techniques today. But all these methods are based on properties that can be forgotten, shared, lost or stolen. Biometric methods of verification, on the other hand, are based on distinctive anatomical and behavioral characteristics or identifiers such as (fingerprints, face, iris, voice palm geometry etc.) that cannot be easily misplaced forged or shared.

Even historically, finger prints (thumb impression) were taken on legal documents using the 'ink technique' where black ink was smeared on the thumb and pressed on the paper to authenticate and identify the subject. Biometric authentication has been widely regarded as the most foolproof system.

WHAT IS BIOMETRICS?

Biometrics is an automated method of identity verification or identification based on the principle of measurable biological characteristics of a person such as a fingerprint, an iris pattern or a voice sample. Biometric characteristics are permanent, unique and not duplicable or transferable. The Biometric characteristics are classified into two major groups - physiological and behavioral.

- Physiological Biometric data relates to the physical aspects of a person's body such as fingerprints, iris scan, face scan and also DNA test.
- Behavioral Biometric data relates to the behavior of a person such as hand writing matching, voice recognition, signature analysis.

ADVANTAGES OF BIOMETRICS:

- Biometric identification can provide extremely accurate, secured access to information; fingerprints, retinal and iris scans produce absolutely unique data sets when done properly
- Current methods like password verification have many problems (people write them down, they forget them, they make up easy-to-hack passwords)
- Automated biometric identification can be done very rapidly and uniformly, with a minimum of training
- Your identity can be verified without resort to documents that may be stolen, lost or altered.

TYPES OF BIOMETRICS

There are number of methods of biometric data gathering and reading worldwide. Some are less invasive, some can be done without the knowledge of the subject, and some are very difficult to fake. However, the selection of technology for proper identification depends upon number of factors like:

- Universal: All Persons must possess
- Unique: guarantee to identity
- Permanent
- Inexpensive

- Ease of Collection
- Analysis
- Technology
- Legal
- Socially accepted
- Based on these parameters some of the frequently used biometric technologies are
- **Face Recognition:** Face recognition system uses distinctive facial features, including upper outlines of eye sockets, areas around cheekbones, the sides of the mouth and the location of the nose and eyes. These numerical quantities are then combined in a single code that uniquely identifies each person.
- **Fingerprint Identification:** Fingerprints remain constant throughout life. Iit has been found that no two fingerprints are alike, not even those of identical twins. Fingerprint identification involves comparing the pattern of ridges and furrows on the fingertips, as well as the minutiae points (ridge characteristics that occur when a ridge splits into two, or ends).
- **Hand or Palm Geometry:** It uses the entire hand as an individual identifier. This method relies on devices that measure the length and angles of individual fingers.
- **Retina Scan:** Retina Scan uses the pattern of the blood vessels at the back of the eye, which is unique and stays the same for a lifetime. However, it requires about 15 seconds of careful concentration to take a good scan.
- **Signature Dynamics:** Signature dynamics is based on individual's signature. The biometric data is easy to gather and is not physically intrusive. Digitized signatures are sometimes used, but usually have insufficient resolution to ensure authentication.
- **Voice Recognition:** Like face recognition, voice biometrics provides a way to authenticate identity without the subject's knowledge. It is to verify the individual speaker against a stored voice pattern, not to understand what is being said.
- **Iris Scanning:** IRIS is the colored ring of tissue that surrounds the pupil of the human eye. The iris scan provides unique biometric data that is very difficult to duplicate as researches have shown that the possibility of having two similar iris patterns is very remote. Iris also remains the same for a lifetime of the person provided there is no physical injury and even the use of glasses or contact lens does not hamper the iris recognition. The technology is not sight dependent and can be used for blind persons also.
- Iris scanning is considered to be least intrusive of the eye-related biometrics, no bright light or lasers or contacts are used in order to protect the eyes from any harm or discomfort. The iris scanner mathematically analyses the random pattern visible within an eye from some distance and uses the technique of pattern recognition using computer vision and optics. In addition, iris scan has the potential for higher than average template-matching performance.
- **IRIS Images:** Iris scans create high-resolution images of the irides of the eye; IR illumination is used to reduce specular reflection from the cornea. Both iris images (left and right) are taken into consideration. To maintain the interoperability among the various e-governance applications it is necessary that standardized format is used for storing and transmitting the iris images.

IMAGE STORAGE FORMAT OF IRIS

- ISO and ANSI have defined several file formats for storing iris images. ISO 19794-6:2005(E) standard is widely accepted by Government of India.
- **Standard:** CBEFF (Common Biometric Exchange Formats Framework) defined in ISO/ IEC 19794-6. The image can be of type PNG or jpeg200.
- Standard Biometric Header (SBH) as defined in ISO/ IEC 19794-1 Biometric Data Block (BDB) for rectilinear iris image as defined in ISO/ IEC 19794-6.
- Image Data (Compressed/ Uncompressed)

IMAGE TYPES

- There are two types of iris images –
- Rectilinear - No Preprocessing of the image is done; 12-15 K space is required for storage.
- Polar - Image is preprocessed before storage and iris portion is converted to polar coordinates, very less space is required (2K).

IRIS RECOGNITION

It is the biometric identification technique which applies complex mathematical pattern recognition techniques on the video images of the iris of an individual's eyes. The complex random patterns inside the eyes are unique. The core algorithms for iris recognition were developed by Professor John Daugman (University of Cambridge) in 1990. Daugman's algorithms were the basis of all the commercially deployed iris recognition systems till 2008. Later some alternative algorithms were also studied upon and developed.

The majority of iris recognition cameras use Near Infra Red (NIR) by emitting 750 nm low power light. Most of the human eyes reveal rich patterns in the Infra Red light but much less in the visible band. Other reason for using this narrow band is that it reduces the effect of ambiance that bright light reflections may produce. But the infra red light is not sensitive to melanin (chromophore) present in the eyes and as result they do not appear in the captured image. So the alternative approach of iris scanning includes the fusion of the two.

ADVANTAGES OF IRIS SCAN IDENTIFICATION

Iris structure is stable throughout the

life after one year of age. It begins to form from the 3rd month of gestation. The structure is complete by eight months. The color and pigmentation completes in first year itself. Some advantages of iris include -

- Unique structure consisting of several layers.
- Protected (inner part of body).
- Taking iris image is easy like taking a photograph from some distance.
- Strong Algorithm.
- Iris has a very fine texture that remains stable for decades.
- In Indian context it is difficult to identify the poor people and people from rural background from fingerprints only because extensive physical labor always affects the quality of finger prints.

LIMITATIONS

Daughman's algorithm does not describe any tool for adjusting the focus. Some other image grabber software may be used to judge the focus quality by examining the successive images. It becomes more relevant if we do not have very much trained persons for grabbing the iris image. So the quality of the image depends on the instrument and the software.

DATABASE

An iris recognition database does not consist of actual images captured but the processed iris is stored. It is not possible to compress these iris templates as it may result in improper matching during identification process. Original images can be compressed. JPEG images can be effectively compressed using JPEG2000 compression techniques.

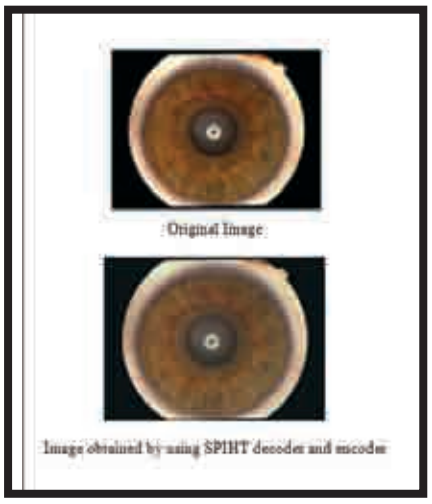
COMPRESSION

Compression reduces the space requirement for storing the images and bandwidth requirement for transmitting the images.

Two commonly used compression techniques are –

- Set Partitioning In Hierarchical Tree (SPIHT): It can be used for all bitmap images including png.
- Joint Photographic Experts Group (JPEG2000): It is new and more advanced image compression standard.

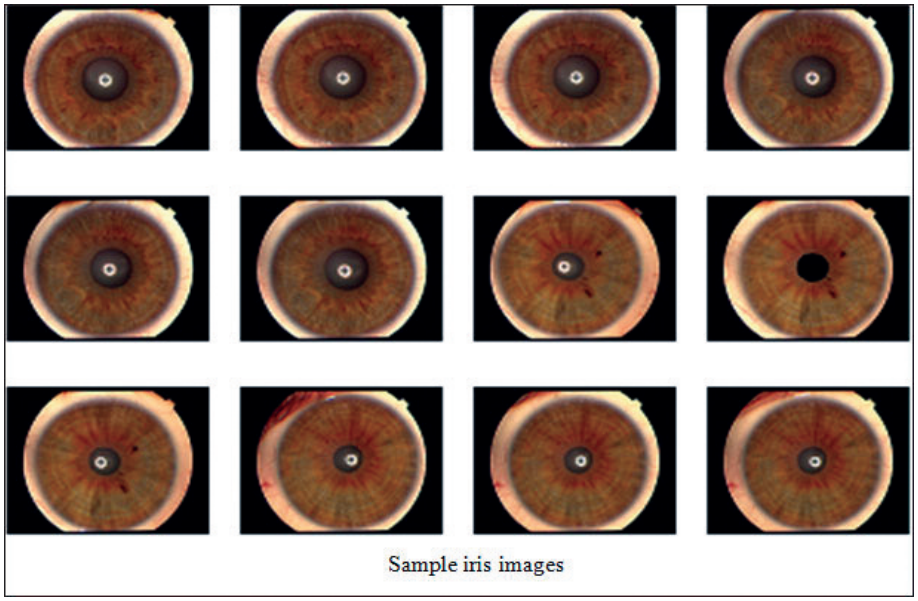
EFFECT OF COMPRESSION ON



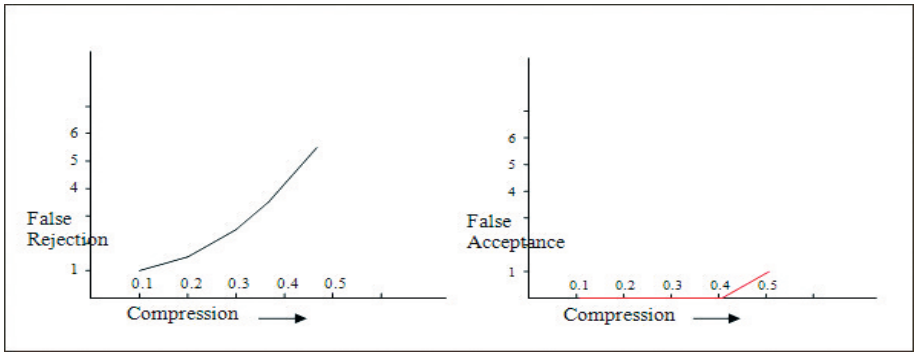
IRIS RECOGNITION

Effect on comparison of iris images using SPIHT based compression software were analyzed, it has been observed that possibility of accepting the invalid iris image is very low, even if compression of the image is very high.

Iris scan technology can be used for identification and de-duplication in any project that involves identification. Possibility of accepting duplicate iris is lesser than any other biometrics. The fusion of iris and fingerprint scanning or iris scanning with face scan may result in more cost effective techniques. Even in the Unique Identification (UID) project of Government of India Finger scanning & iris technologies have been used in conjunction as unique identifier for each citizen of the country.



Sample iris images



False Rejection -Acceptance of the image compressed by SPIHT