FSIS Security in e-Governance

[1] **Anil Rajput,**
[1]Bhabha Engineering Research Institute – MCA, Bhopal (M.P.) India
[2] **Manmohan Singh**
[2]Asst. Prof, Department of Computer Science, BIST, Bhopal (M.P.) India
[3]**Meghna Dubey**
[3]Asst. Prof, Department of Computer Application, SCOPE, Bhopal (M.P.) India
[3]**Nidhi Chandel**
[3]Asst. Prof, Department of Computer Application, Career College, Bhopal (M.P.) India

Abstract:
When used for personal identification, E-Governance measure and analyze human physiological and behavioral characteristics. Identifying a person's physiological characteristics is based on direct measurement of a part of the body signature s, speech, face and irises. E-Governance the corresponding technologies are fingertips, speech face and irises. Identifying behavioral characteristics is based on data derived from actions, such as speech and signature, the corresponding E-Governance being speaker recognition and signature recognition. Unlike conventional identification methods that use something you have, such as an identification card to gain access to a building, or something you know, such as a password to log on to a computer system, these characteristics are integral to something you are.
Keywords:
E-governess, AI, data mining, iris, cryptography and parallel,

Introduction

E-governance becomes very widely used; there is increased risk of forgery in unattended operation: speech synthesizers, photographs of irises, fingerprint molds, and even good old-fashioned forged signatures must all be thought of in system design. These do not rule out the use of E-governance, as traditional methods such as Signatures are usable in practice despite very high error rates. E-governance is usually more powerful in attended operation, where, with good system design, the relative strengths and weaknesses of the human guard and the machine recognition system may complement one another.

Public key cryptography

- Each entity is assigned a pair of keys – *private* - known only by the owner *public* -known by everyone
- Information encrypted with the private key can only be decrypted by the corresponding public key & vice versa
  - Digital Signatures
  - Signing using the sender's Private key
  - Speech recognizationand its authentication
  - Face recognization and its authentication
  - IRIS Authentication
  - Verification using the sender's Public key
- Ensures
  - Authentication
  - Non Repudiation
  - Integrity
  - Face using sender Private Key
  - Iris using sender's private key
  - Speech
- Encryption
  - Encryption using the Public key of the recipient

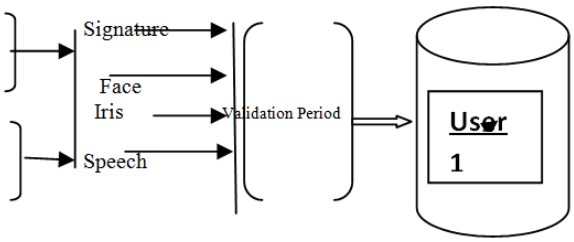

Figure 1.1.1 data base

1.1 Face

Face recognition also satisfies most of the criteria for the ideal -governance solution. It's easy to perform, fast, moderately convenient, and nonintrusive, except perhaps to the camera-phobic. Video camera hardware is relatively inexpensive; and some monitor manufacturers build camera lenses into their display screens to accommodate videoconferencing. With to day faster processors, even a low quality digital camera can do a pretty good job of reading digital video and can recognize individuals 78 percent of the time. These factors contribute to making face recognition one of the fastest-growing niches. However, the technology is subject to spoofing; and

Manuscript received October 5, 2010
Manuscript revised October 20, 2010

lighting can affect authentication. Face-recognition systems can also work with people still at a distance. As one approaches, the system could recognize the face and activate the system, such as turning on a computer or unlocking a door. Some applications are focusing on a person's smile as a replacement for a security password. Other techniques based on ear or lip shape and knuckle creases are in the conceptual stages; and one startup company is trying to recognize a person's identity by body odor. Eye scanning is probably the fastest growing area of biometric research because of its promise for high scan accuracy and great difficulty to fool. There are two types of eye scanning: retinal scanning and iris scanning. Retinal scanning uses lasers that focus on the back of the eye, while iris scanning zooms in on the front. The retina is considered unique even among identical twins. Likewise, the iris is the most feature-rich part of the human anatomy that is constantly on view. The iris can have more than 250 distinct features, compared with 40 or 50 points of comparison in fingerprints; so iris scanning is an order of magnitude more accurate than fingerprints or even DNA analysis. Also, unique patterns in the human iris stabilize within one year of birth and remain constant throughout one's lifetime, unlike other biometrics. However, contact lens wearers or people with optical diseases like glaucoma may not easily pass an eyeball scan. It is also impossible to counterfeit the distinct iris pattern with

$$\begin{bmatrix} Y \\ C_b \\ C_r \end{bmatrix} = \begin{bmatrix} 0.299 & 0.587 & 0.114 \\ -0.169 & -0.331 & 0.5 \\ 0.5 & -0.419 & -0.081 \end{bmatrix} \begin{bmatrix} R \\ G \\ B \end{bmatrix} + \begin{bmatrix} 16 \\ 128 \\ 128 \end{bmatrix}$$

Binary Image Processing

Depending on the Cb and Cr threshold values a binary image is obtained with the skin regions masked in white and the non skin regions masked in black. This mask is further refined through morphological operators.

Figure 1.1.1 Face Recognition database.

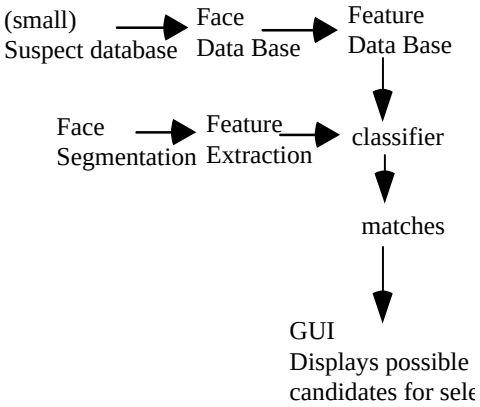

Figure 1.1.2 Face Identification System

2.1 Finger/Hand

Fingerprint technology is the most commonly used biometric because it has been used in law enforcement for over a hundred years. However, prisons and law-enforcement populations are comprised mostly of relatively uniform populations of males between the ages of 18 and 36 whose fingerprints are in relatively good condition. Some people have fingerprints that are harder to image. About 2% of the general population's fingerprints baffle computers. It's often difficult to image fingerprints from people with very small hands and fingers, people who work with their hands, or those who have injuries or scars. Also, as people age, they often lose the lipid (fat) layer in their skin and their fingerprints become worn and difficult to image. Fingerprint scanners could work fine in a private security application where it may suffice to match a few locally stored prints. They are more difficult to fool than face-recognition systems because they measure the unique and complex swirls on a person's fingertip and some can even accommodate cuts. However, a public security setting, where potentially anyone's prints would need to be matched, could pose problems because current methods require large central databases. For example, if a customer makes a purchase with a credit card, his or her fingerprints might have to be matched against everyone who owns tha particular card unless there is a tamper-proof way of storing prints locally. Also, cuts and dirt can distort images. If a previous user leaves an oily latent image on the scanner, a false rejection may occur or someone with a fine brush and dry toner could "lift" fingerprints with adhesive tape. Palm/hand scanners, a variation of the fingerprint scanners, are better suited to sites in which the users may be working with their hands. They measure creases and/or geometry that will not be substantially altered by grime or nicks. However, these devices are also more expensive and less accurate than the

fingerprint scanners, especially at sites with a large number of users. Some manufacturers rely on smart cards to control access, particularly to notebook PCs. They encode fingerprint data (128 to 512 bytes) in the smart card's microprocessor.

3.1 Signatures

Forged signature will be accepted as genuine mainly depends on the amount of care taken when examining it. Many bank card transactions in stores are accepted without even a glance at the specimen signature on the card so much so that many Americans do not even bother to sign their credit cards. But even diligent signature checking doesn't reduce the risk of fraud to zero. An experiment showed that 105 professional document examiners, who each did 144 pairwise comparisons, misattributed 6.5% of documents. Meanwhile, a control group of 34 untrained people of the same educational level got it wrong 38.3% of the time [1] and the nonprofessionals' performance couldn't be improved by giving them monetary incentives. Errors made by professionals are a subject of continuing discussion in the industry, but are thought to reflect the examiner's assumptions and preconceptions [5]. As the participants in these tests were given reasonable handwriting samples rather than just a signature, it seems fair to assume that the results for verifying signatures on checks or credit card vouchers would be significantly worse. So signatures are surrounded by a number of conventions and special rules which vary from one country to another. For example, to buy a house in England using money borrowed from a bank of which you're not an established customer, the procedure is to go to a lawyer's office with a document such as a passport, sign the property transfer and loan contract, and get the contract countersigned by the lawyer. The requirement for government-issued photo-ID is imposed by the mortgage lender to keep its insurers happy, while the requirement that a purchase of real estate be in writing was imposed by the government some centuries ago in order to collect stamp duty on property transactions. Other types of document (such as expert testimony) may have to be notarized in particular ways. Many curious anomalies go back to the nineteenth century, and the invention of the typewriter. Some countries require that machine written contracts be initialed on each page, while some don't; and these differences have sometimes persisted for over a century. Clashes in conventions still cause serious problems.

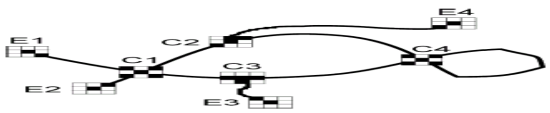

Figure 3.1.1. Machine written

Company went bust as a result. In most of the English-speaking world, however, most documents do not need to be authenticated by special measures. The essence of a signature is the intent of the signer, so an illiterate's "*X*" on a document is just as valid as a monarch's flourish. In fact, a plaintext name at the bottom of an email message also has just as much legal force, except where there are specific regulations requiring the transaction to be in writing. There may be thousands of such in each very rare for signatures to be disputed in court cases ally very rare for signatures to be disputed in court cases, as the context generally makes it clear who did what. So we have a very weak biometric mechanism that works quite well in practice except that it's choked by procedural rules that vary by country and by application. Sorting out this mess, and imposing reasonably uniform rules for electronic documents, is a subject of much international activity, with an analysis by country in [5], and I'll discuss some of the issues further in Part 3. There is one application, though, where effective automatic recognition of signatures could be very valuable. In a bank's check processing center, it is typical practice that you only verify signatures Verifying checks for small amounts is not economic unless it can be automated, so a This turns out to be a very difficult image-processing task because of the variability between one genuine signature and another. A much easier option is to use a *signature tablet.* This is a sensor surface on which the user does a signature; it records not just the shape of the curve but also its dynamics.

- **Vertical center of the signature.** The vertical center Cy is given by

$$C_y = \frac{\sum_{y=1}^{y\max} y \sum_{x=1}^{x\max} b[x,\ y]}{\sum_{x=1}^{x\max} \sum_{y=1}^{y\max} b[x,\ y]}.$$

- **Horizontal center of the signature.**

The horizontal center Cx is given by

$$C_x = \frac{\sum_{x=1}^{x\max} x \sum_{y=1}^{y\max} b[x,\ y]}{\sum_{x=1}^{x\max} \sum_{y=1}^{y\max} b[x,\ y]}.$$

4.1 Iris

We turn now from the very traditional ways of identifying people to the modern and innovative. Recognizing people by the patterns in the irises of their eyes is far and away the technique with the best error rates of automated systems when measured under lab conditions. It appears to be the most secure possible way of controlling entry to

premises such as plutonium stores. As far as is known, every human iris is measurably unique. It is fairly easy to detect in a video picture, does not wear out, and is isolated from the external environment by the cornea (which in turn has its own cleaning mechanism). The iris pattern contains a large amount of randomness, and appears to have many times the number of degrees of freedom of a fingerprint. It is formed between the third and eighth month of gestation,

And (like the fingerprint pattern) is *phenotypic* in that there appears to be limited genetic influence; the mechanisms that form it appear to be chaotic. So the patterns are different even for identical twins (and for the two eyes of a single individual), and they appear to be stable throughout life. A signal processing technique (Gabor filters) has been found which extracts the information from an image of the iris into a 256-byte *iris code*. This involves a circular wavelet transform taken at a number of concentric rings between the pupil and the outside of the iris (Figure 4.1.1), and has the beautiful property that two codes computed from the same iris will typically match in 90% of their bits [6]. This is much simpler than in fingerprint scanners where orienting and classifying the minutiae is a hard task. The speed and accuracy of iris coding has led to a number of commercial iris recognition products. Iris codes provide the lowest false accept rates of any known verification system—zero, The equal error rate has been shown to be better than one in a million, and if one is prepared to tolerate a false reject rate of one in ten thousand, then the theoretical false accept rate would be less than one in a trillion. The main practical problem facing deployment of iris scanning in the field is getting the picture without being too intrusive. The iris is small (less than half an inch) and an image including several hundred pixels of iris is needed. A cooperative subject can place his eye within a few inches of a video camera, and the best standard equipment will work up to a distance of two or three feet. Cooperation can be assumed with entry control to computer rooms, but it is less acceptable in general retail applications, as some people find being so close to a camera uncomfortable. There's no technical reason why a camera could not acquire the iris from a distance of several feet given automatic facial feature recognition, pan and zoom it would just cost a bit more—but that brings Orwellian overtones of automatic recognition of individuals passing in a crowd. (In Europe, data protection law would be a potential show-stopper.) Secondary problems include blinking, eyelashes obscuring the eye, and sunglasses. Possible attacks on iris recognition systems include in unattended operation at east—a simple photograph of the target's iris. This may not be a problem in entry control to supervise sad premises, but if everyone starts to use iris codes

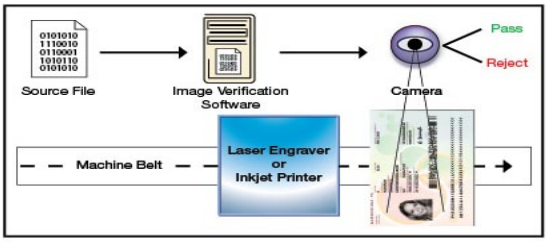

Figure 4.1.**1** iris recognition

Control to supervised premises, but if everyone starts to use iris codes to authenticate bank card transactions, then your code will become known to many organizations. As iris codes can be compared rapidly (just exclusive-or them together and count the number of zero bits), they may start to assume the properties of names, rather than being Passwords (as in current systems). So it might be possible to use your iris code to link together your dealings with different organizations. Image obtained after extracting the part with highest intensity. Boundary of the image cannot be obtained exactly in this step.

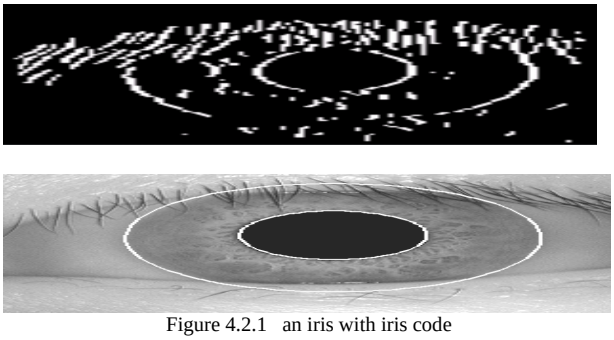

Figure 4.2.1 an iris with iris code

A possible solution to the impersonation problem is to design terminals that measure *hippus*—a natural fluctuation in the diameter of the pupil which happens at about 0.5 Hz. But even this isn't infallible. One might try, for example, to print the target's iris patterns on contact lenses (though existing vanity contact lens printing techniques are so coarse-grained that they are detectable). Despite the difficulties, iris codes remain a very strong contender as they can, in the correct circumstances, provide much greater certainty than any other method that the individual in question is the same as the one who was initially registered on the system..

5.1 Speech Recognition

Speech recognition—also known as *speaker recognition*—is the problem of identifying a speaker from a short utterance. While *speech recognition* systems are concerned with transcribing speech and need to ignore speech idiosyncrasies, voice recognition systems need to

amplify and classify them. There are many sub problems, such as whether the recognition is text-dependent or not, whether the environment is noisy, whether operation must be real time, and whether one needs only to verify speakers or to recognize them from a large set. In *forensic phonology*, the objective is, usually, to match a recorded telephone conversation, such as a bomb threat, to speech samples from a number of suspects. Typical techniques involve filtering and extracting features from the spectrum; for more detailssee [2]. And that achieves an equal error rate of about 5%. This is primitive compared with what can now be done with digital signal processing. Some informed observers expect that within a few years, there will be products available which support real-time voice and image forgery. Crude voice morphing systems already exist, and enable female victims of telephone sex pests to answer the phone with a male sounding voice. Better ones will enable call centers to have the same 'person' always greet you when you phone. With that sort of commercial pressure driving the technology,

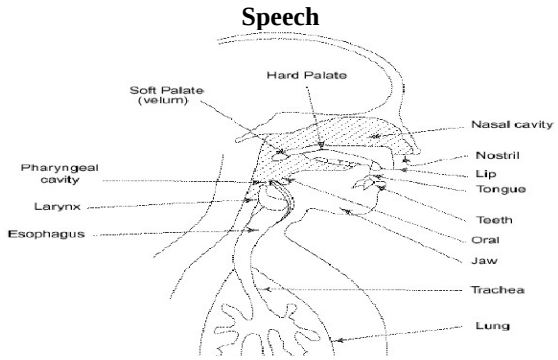

Figure 5.1.1 speech

Recognition Basics: Speech recognition is the process by which a computer (or other type of machine) identifies spoken words. Basically, it means talking to your computer, AND having it correctly recognizes what you are saying. The following definitions are the basics needed for understanding speech recognition technology.

Utterance: An utterance is the vocalization (speaking) of a word or words that represent a single meaning to the computer. Utterances can be a single word, a few words.

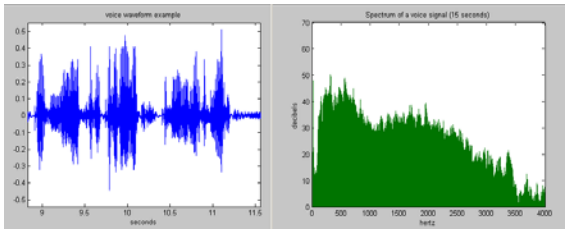

Figure 5.1.2 Voice Waveform & Spectrum

Speaker Dependence: Speaker dependent systems are designed around a specific speaker. They generally are more accurate for the correct speaker, but much less accurate for other speakers. They assume the speaker will speak in a consistent voice and tempo. Speaker independent systems are designed for a variety of speaker.

Conclusion

E-governance measures of one kind or another have been used to identify, with signatures, face features, iris and speech being the traditional methods.

This System has been built that automate the task of recognition, using all these methods and newer ones: Hand geometry, Voiceprints, Facial and Iris patterns.

This system has different strengths and weaknesses. In automatic operation, most have error rates of the order of 5% (though iris recognition is better, hand geometry slightly better, and face recognition worse). There is always a trade-off between the false accept rate (the fraud rate) and the false reject rate (the insult rate).

Finally, Our FSIS systems achieve most or all of their result by deterring criminals rather than being effective at identifying them.

References:

[1] Citizenship & Immigration Canada (2003). Tracking public perceptions of biometrics. http://www.cic.gc.ca/english/press/03/poll-biometrics-e.pdf (accessed Oct. 24, 2003)

[2] Coventry, L. (2004). Fingerprint authentication: The user experience. Paper presented at the DIMACS Workshop on Usable Privacy and Security Software, July 7 - 8, Rutgers University, and Piscataway, NJ. (http://dimacs.rutgers.edu/Workshops/Tools/program.html)

[3] Sasse, M.A. (2004). Usable security: Beyond the interface. Paper presented at the DIMACS Workshop on Usable Privacy and Security Software, July 7 - 8, Rutgers University, and Piscataway, NJ. (http://dimacs.rutgers.edu/Workshops/Tools/program.html)

[4] Sasse, M.A., Brostoff, S., & Weirich, D. (2001). Transforming the 'weakest link': A human/computer interaction approach to usable and effective security. BT Technology Journal, 19, 122-131.

[5] L. De Lathauwer, B.D. Moor, J. Vandewalle, A multilinear singular value decomposition, SIAM Journal on Matrix Analysis and Applications 21

[6] A. Haiping Lu, K.N. Plataniotis, Venetsanopoulos. Multilinear principal component analysis of tensor objects for recognition, in: 18th International Conference on Pattern Recognition, ICPR 2006, vol. 2, 2006, pp. 776–779.

[7] A. Kumar, T. Srikanth, Online personal identification in night using multiple face representations, in: 19th International Conference on Pattern Recognition, ICPR 2008, vols. 1–4, December 2008

Dr. Anil Rajput, PhD from BU Bhopal in 1993. He was born in Bareli (Raisen), India on 12 July 1965. He has 23 years teaching and 17 years research experience. 12 students are awarded PhD under his guidance.

Mr.Manmohan Singh, M.Tech Form RGPV Bhopal He was born in Betul, India on 25 Sep 1982 .There after he joined as a Lecturer in BIST College of Technology till 2010. Now he is working as a.

Mrs. Meghna Dubey is having a Teaching Experience of Ten Years in teaching.She is Persuing her P.hd Under the guidance of Dr. Anil Rajput in Computer Science from Barkatullah University Bhopal .She is working as HOD M.C.A in Scope . College till Now.

Mrs. Nidhi Chandel is having a Teaching Experience of TwoYears in teaching. She is Persuing her P.hd Under the guidance of Dr. Anil Rajput in Computer Science from Barkatullah University Bhopal.She is working as Assistant Professor in Career .College till Now.