Acoustic Ear Scanning With Fingerprint Technology

[1,]S. Niveda , [2,]K. Dhavamani
[1,]*Department of Information Technology*
[2,]*Manakula Vinayagar Institute of Technology*

ABSTRACT:

We often hear about the theft of our valuable devices. Day-by-day it is increasing too. So, in order to control the theft of electronic devices such as iPod, smart phones, scientists have introduced a new technology called "acoustic ear scanning technology" for their security. The predecessor for this technology is fingerprint scanning, face recognition, etc., but these all have a common disadvantage. And to overcome that disadvantage, we have introduced finger print scanning along with it in our paper.

KEYWORDS: iPod, smart phones, earphone, biometric template.

I. INTRODUCTION:

This is mainly to protect the electronic and portable devices from theft. The basis of this acoustic ear scanning technology is that the new scan sends sound through earphones. Sound returns from the ear chamber's "finger print ". Scientists have found a way of using the "acoustic fingerprint" of a person's ear to ensure no one else can operate their iPods, mobile phones and other personal portable device. The technology can be extended to protect bank accounts and passports.

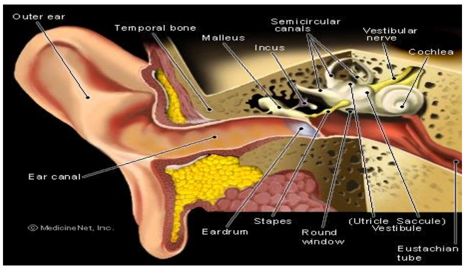


Figure 1

Overseas researchers have discovered that they can identify individuals from the unique sound of the ear chamber. The biometric "pin number" would be instantly detected by an iPod, mobile phone or any other device fitted with an anti-theft acoustic fingerprint detector. Acoustic fingerprint can be used to pay bills or do banking transactions securely with confirmation of identifying as easy as by simply wearing a headphone in the ear. Electronic engineer, Arthur Rapos of the Elektra Company, believes biometric mapping will eventually lead to microchip implants in humans. It isn't a flight of fancy to imagine someone being implanted with a removable microchip that records that person's unique biological feature before travelling overseas."The sound the inside of our ear makes is not the only unique things about an individual's".

II. PRINCIPLES:

The working principle of this technology is

- **Biometric**
- **Image processing**

2.1 BIOMETRIC:

Biometric recognition, or biometric refers to the automatic identification of a person based on his/her anatomical (e.g., fingerprint) or behavioral (e.g., signature) characteristics or traits. This method of identification offers several advantages over traditional methods involving ID cards (token) or pin numbers (passwords) for various reasons:

[1] The person to be identified is required to be physically present at the point-of-identification.
[2] Identification based on biometric techniques obviates the need to remember a password or carry

a token with the increased integration of computers and the internet into our everyday lives, it is necessary to protect sensitive and personal data by replacing PINs (or using biometrics in addition to PINs), biometric techniques can potentially prevent unauthorized access to cell phones laptops, and computer networks. Biometrics are used in computer science as a form of identification and access control. It is also used to identify individuals in groups that are under surveillance.Biometric identifiers are the distinctive, measurable characteristics used to label and describe individuals. Biometric identifiers are often categorized as physiological versus behavioral characteristics. A physiological biometric would identify with one's voice, DNA, hand print or behavior. Behavioral biometrics are related to the behavior of a person, including but not limited to: typing rhythm, gait, and voice. In verification mode the system performs a one-to-one comparison of a captured biometric with a specific template stored in a biometric database in order to verify the individual is the person they claim to be.
Three steps involved in person verification.

- In the first step, reference models for all the users are generated and stored in the model database.
- In the second step, some samples are matched with reference models to generate the genuine and impostor scores and calculate the threshold.

- Third step is the testing step.

This process may use a smart card, username or ID number (e.g. PIN) to indicate which template should be used for comparison. 'Positive recognition' is a common use of verification mode, "where the aim is to prevent multiple people from using same identity". In Identification mode the system performs a one-to-many comparison against a biometric data base in an attempt to establish the identity of an unknown individual.

Figure 2

The system will succeed in identifying the individual if the comparison of the biometric sample to a template in the database falls within a previously set threshold. Identification mode can be used either for 'positive recognition' (so that the user does not have to provide any information about the template to be used) or for 'negative recognition' of the person "where the system establishes whether the person is who she (implicitly or explicitly) denies to be". The latter function can only be achieved through biometrics since other methods of personal recognition such as passwords, PINs or keys are ineffective.The first time an individual uses a biometric system is called enrollment. During the enrollment, biometric information from an individual is captured and stored. In subsequent uses, biometric information was detected and compared with the information stored at the time of enrollment. Note that it is crucial that storage and retrieval of such systems themselves be secure if the biometric system is to be robust.

- The first block (sensor) is the interface between the real world and the system; it has to acquire all the necessary data. Most of the times it is an image acquisition system, but it can change according to the characteristics desired.
- The second block performs all the necessary preprocessing: it has to remove artifacts from the sensor, to enhance the input (e.g. Removing background noise), to use some kind of normalization, etc.

A sensor (also called detector) is a convertor that measures a physical quantity and converts it into a signal which can be read by an observer or by an (today mostly electronic) instrument. A sensor is a device which receives and responds to a signal when touched. A sensor's sensitivity indicates how much the sensor's output changes when the measured quantity changes. In the third block necessary features are extracted. This step is an important step as the correct features need to be extracted in the optimal way. A vector of numbers or an image with particular properties is used to create a template. A biometric template (also called *a template*) is a digital reference of distinct characteristics that have been extracted from a biometric sample. Templates are used during the biometric authentication process. A template is a synthesis of the relevant characteristics extracted from the source. Elements of the biometric measurement that are not used in the comparison algorithm are discarded in the template to reduce the file size and to protect the identity of the enrollee.

If enrollment is being performed, the template is simply stored somewhere (on a card or within a database or both). If a matching phase is being performed, the obtained template is passed to a matcher that compares it with other existing templates, estimating the distance between them using any algorithm (e.g. Hamming distance). In coding theory Hamming (7,4) is a linear error -correcting code that encodes 4 bits of data into 7 bits by adding 3 parity bits. It is a member of a larger family of hamming codes, but the term Hamming code often refers to this specific code that Richard W. Hamming introduced in 1950. At the time, Hamming worked at Bell Telephone Laboratories and was frustrated with the erroneous punched card reader, which is why he started working on error-correcting codes. The matching program will analyze the template with the input. This will then be output for any specified use or purpose. Selection of biometrics in any practical application depending upon the characteristic measurements and user requirements. We should consider Performance, Acceptability, Circumvention, Robustness, Population coverage, Size, Identity theft deterrence in selecting a particular biometric. Selection of biometric based on user requirement considers Sensor availability, Device availability, Computational time and reliability, Cost, Sensor area and power consumption.

2.2 IMAGE PROCESSING:

Image processing refers to the processing of a 2D picture by a computer. An image is considered to be a function of two real variables, for example, a (x, y) with a as the amplitude (e.g. Brightness) of the image of the real coordinate position (x, y). Modern digital technology has made it possible to manipulate multi-dimensional signals with systems that range from simple digital circuits to advanced parallel computers.

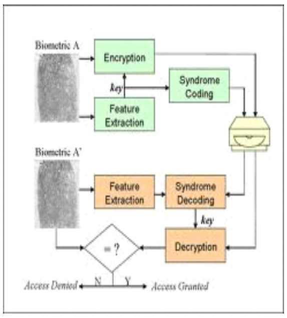


Figure 3

The most requirements for image processing of images is that the images are available in digitized form, that is, arrays of finite length binary words. The digitized image is processed by a computer. To display a digital image, it is first converted into an analog signal, which is scanned onto a display. Before going to processing an image, it is converted into a digital form. Digitization includes sampling of images and quantization of sampled values. After converting the image into bit information, processing is performed. This processing technique may be, Image enhancement, Image reconstruction, and Image compression

2.2.1 IMAGE ENHANCEMENT:

It refers to accentuation, or sharpening, of image features such as boundaries, or contrast to make a graphic display more useful for display & analysis. This process does not increase the inherent information content in data. It includes gray level & contrast manipulation, noise reduction, edge christening and sharpening, filtering, interpolation and magnification, pseudo coloring, and so on.

2.2.2 IMAGE RESTORATION:

It is concerned with filtering the observed image to minimize the effect of degradations. Effectiveness of image restoration depends on the extent and accuracy of the knowledge of degradation process as well as on filter design. Image restoration differs from image enhancement in that the latter is concerned with more extraction or accentuation of image features.

2.2.3 IMAGE COMPRESSION:

It is concerned with minimizing the no of bits required to represent an image. Application of compression is on broadcast TV, remote sensing via satellite, military communication via aircraft, radar, teleconferencing, facsimile transmission, for educational & business documents , medical images that arise in computer tomography, magnetic resonance imaging and digital radiology, motion , pictures ,satellite images, weather maps, geological surveys and so on.De-essing is any form of signal processing for which the input is an image, such as a photograph or video frame; the output of image processing may be either an image or a set of characteristics or parameters related to the image. Most image-processing techniques involve treating the image as a two-dimensional signal and applying standard signal-processing techniques to it. Image processing usually refers to digital image processing, but optical and analog image processing also is possible. This article is about general techniques that apply to all of them. The acquisition of images (producing the input image in the first place) is referred to as imaging. In modern sciences and technologies, images also gain much broader scopes due to the ever growing importance of scientific visualization (to often large-scale complex scientific/experimental data). Examples include microarray data in genetic research, or real-time multi-asset portfolio trading in finance.

III. EXISTING SYSTEM:

Acoustic ear scanning technology has been implemented to prevent the theft of iPods, mobile phones. It works by, for the first time of using the device, an ear phone should be put into the ears. A minute sound is sent into the ears. The microscopic hairs inside the ear responds the sound by producing its own sound. This happens by, the sound that passes through the air after entering the ear, passes through the liquid medium. During this time, the microscopic hair cells in the inner ear, bends to produce its own sound. The sound is unique for each person varying according to the ear drum, ear bones, etc.,. The sound is then processed in digital form and saved into a biometric template. Biometric template is a place where the digital form of the sound gets stored.Now, whenever a person uses it for the second time, it insists the user to wear earphones. Once we wear the earphone, a minute sound is sent in order to make hair cells produce their own sound. This sound is the converted to digital form and compared with the standard biometric template. If they are same, the access will be granted else the access is denied.

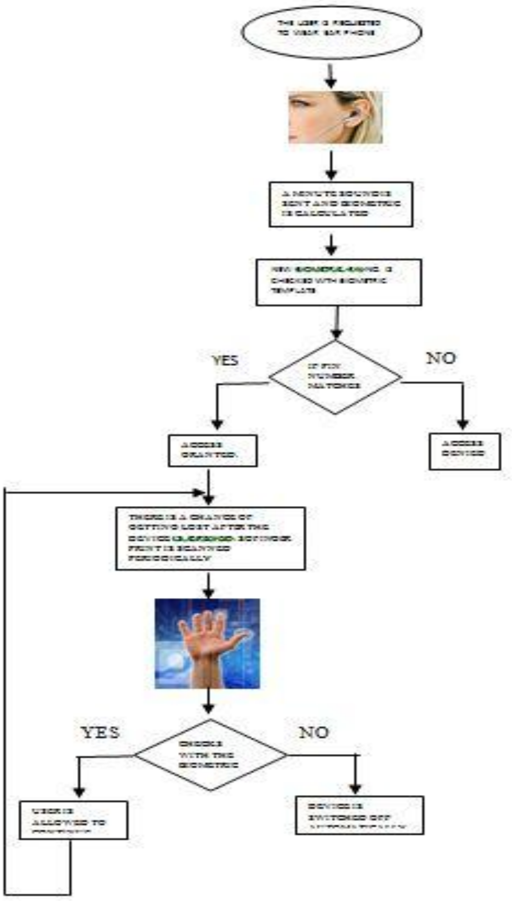
3.1 CONVERSIONS OF SOUND INTO DIGITAL FORM:

An analogue or acoustical input source such as microphone converts air pressure variation into an electrical signal. An analog-to-digital convertor converts the signal into digital data by repeatedly measuring the signal of the changes in voltage.

IV. PROPOSAL:

This overcomes the disadvantage of ear scanning technology. It can be applied to systems also.
STEP 1: for the first time, when the user uses the device, a biometric of the fingerprint and ear sound is stored in a database.
STEP 2: The user is requested to wear an ear phone while switching on the mobile.
STEP 3: Once the earphone is worn, a minute sound is sent to our ears which will be then converted into biometric.
STEP 4: If the biometric matches with the template stored already, the access is granted.
STEP 5: Since this process provided security only at the time of opening, there might a chance of getting lost after opened.
STEP 6: Hence, we introduced finger print technology along with it.
STEP 7: For every particular time period, the fingerprint is being scanned again and compared with the biometric template of it.
STEP 8: If the biometric matches, the user can continue. Otherwise, it gets shut down automatically.
STEP 9: Once the device is switched off, again the user has to start from first.
STEP 10: This can be applied in the same way to systems, where the finger print has been implemented in most used keys.

V. CONTROL FLOW DIAGRAM:


THE USER IS REQUESTED TO WEAR EAR PHONE
A MINUTE SOUND IS SENT AND BIOMETRIC IS CALCULATED
NEW IS CHECKED WITH BIOMETRIC TEMPLATE
YES
NO
IF PIN NUMBER MATCHES
ACCESS GRANTED.
ACCESS DENIED
THERE IS A CHANCE OF GETTING LOST AFTER THE DEVICE SO FINGER PRINT IS SCANNED PERIODICALLY
YES
NO
CHECKS WITH THE BIOMETRIC
USER IS ALLOWED TO
DEVICE IS SWITCHED OFF

VI. CONCLUSION:

Thus we proposed an idea which will be helpful in protecting the electronic devices even though the device is kept opened. Acoustic ear scanning technology is a recent technology introduced to protect electronic devices. Since it can provide security only at the time of opening, we introduced finger print scanning which will not allow unauthorized access to it.

REFERENCES:

[1] S. Prabhakar, S. Pankanti, A. K. Jain, "Biometric Recognition: Security and Privacy Concerns", IEEE Security & Privacy, March/April 2003

[2] D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman, A. K. Jain, "FVC2002: Fingerprint verification competition" in Proc. Int. Conf. Pattern Recognition (ICPR), Quebec City, QC, Canada, August 2002

[3] Samir Nanvati, (2002), Biometrics: Identity Verification in a Networked World, New York: Wiley and Sons, Inc.

[4] Wayne Penny, (2002), Biometrics, A Double-Edged Sword

[5] Jensen, J.R. 1996. Introduction to Digital Image Processing : A Remote Sensing Perspective.Practice Hall, New Jersey