IRIS SCANNER IN E-BANKING

P.Karthi, Assistant Professor, Department of ComputerTechnology, SNMV College of Arts & Science, Malumachampatti, Coimbatore -50, Tamil Nadu, India.

P. Ganesh,Assistant Professor, Department of Computer Science, Sri Vidhya College of Arts and Science, Sivakasi Main Road, P. Kumaralingapuram, Virudhunagar, Tamil Nadu, India.

ABSTRACT

Iris recognition is considered one of the most advanced methods of security, it is becoming the solution of choice for many banks, financial institutions, investment firms and payment systems. Using iris as a replacement for passwords, PINs, plastic cards, account numbers or paper-based credentials, etc would result in faster transaction time that leave the bank teller with more time to concentrate on the level of service provided to the customer.Furthermore, banks tend to adopt biometric technology which offers a kind of transformation in the banking industry around money laundering, fraud, financial inclusion that is able to properly identity customer. Not only it improves the entire confidence around which the bank system is built on but it also solves the problem that banks recently facing with is the large population of illiterates.Iris technology software enhances online banking system that needs a safe, secure and easy solution to manage user's money via the Internet. By utilizing users' iris images, customer can check account balance, make transactions and do most of their everyday banking from their house, a restaurant, or an office at any time.

Keywords : Iris and Biometric

Types of Biometric Security

There are two types of biometric security: physical and behavioral. Physical biometrics measure physical attributes such as facial features or fingerprints. Behavioral biometrics measure the behavioral traits of an individual, and unlike physical biometrics include the element of time. For example, when we sign our name, we begin at one point and end at another. Behavioral biometrics include signatures and speech patterns.

Physical Biometric Solution

Fingerprint Recognition:

Fingerprint biometrics cannot be faked or altered easily. The uniqueness of a fingerprint can be determined by the pattern of ridges and furrows on a fingertip as well as the minutiae points. A fingerprint sensor is an electronic device that captures a digital image of the fingerprint pattern. The captured image is called a "live scan." The live scan is digitally processed to create a biometric template which is stored and used for matching.

Disadvantages

- Probably most criticized method due to association with criminal identification
- Population coverage may be a problem with old age people or people with skin disease

- Performance can be fluctuate to dry, wet, dirty fingers

Hand Geometry

Hand geometry identifies users by the shape of their hands. It is the first biometric to achieve wide spread computerized use. A hand geometry system measures the physical characteristics of the fingers or the hands, including their length, width, thickness and surface area. It compares the results of a measurement to previous measurements stored in a file.Since a person's hands and fingers are unique, but not as unique as other traits, such as fingerprints or irises, this method of authentication and identification is not asrobust as some other alternatives. Unlike finger prints or irises, hand geometrics can change over time as a result of injury, weight change, or arthritis.

Disadvantages

- The hand geometry is not unique and cannot be used in identification systems
- Not ideal for growing children
- Jewelry,, limited dexterity, etc may pose a challenge in extracting the and geometry information
- The data size of hand geometry biometrics is large and is not ideal for using it in embedded systems

Facial Recognition

Facial recognition systems measure the structure, shape, and proportions of facial characteristics including the eyes, nose, and mouth. They can convert a photograph or video image into a code that describes a person's face. The most advanced method of facial recognition is three-dimensional (3-D) facial recognition. It uses 3-D sensors to capture information about the shape of a face and distinctive features on the face. Unlike 2-D methods, 3-D facial recognition is not affected by changes in lighting, and it can identify a face from a variety of angles. End users generally prefer facial recognition to other methods because it is hands-free and requires less effort than some other identification and authentication methods.

Disadvantages

- Since user consent is not required, may be used to surveil people
- 2D face recognition can be insecure and prone to spoofing
- Exposed biometric modality. People can be recognized from a distance, which can lead to privacy issues

Iris and Retina Scans

The iris is the colored, ring-shaped area surrounding the pupil. No two iris structures are alike, even in the case of identical twins. Iris recognition technology uses small, high-quality cameras to capture a black and white high-resolution photograph of the iris. Once the image is captured, it is analyzed, processed into an optical "fingerprint," and translated into a digital form.

The retina is the thin neural cell tissue at the back of one's eye. Its uniqueness remains constant throughout a person's lifetime. The blood vessels in the retina provide a unique pattern, which is used in retina recognition technology. A retinal scan is performed by casting an unperceived beam of low-energy infrared light into a person's eye as the user looks through the scanner's eyepiece. This beam of light traces a standardized path on the retina. Once

the scanner device captures a retinal image, specialized software compiles the unique features of retinal blood vessels into a template.

Disadvantages

- Intrusive
- Expensive to setup

Voice Recognition

The behavioral components of voice include movement, manner, and pronunciation. Voice verification technology works by converting a spoken phrase from analog to digital format and extracting the distractive vocal characteristics to create a speaker model or voiceprint. A template is then generated and stored for future comparison. Voice recognition is often used where voice is the only available biometric identifier, such as over the telephone.

Disadvantages

- Prone to spoofing with recorded or imitated voice sample
- May not be suitable for high security applications when used as only method of identification
- Since user consent is not required, may be used to surveil people
- Identity verification may take some time

Signature Recognition

The behavioral characteristics of a signature include the changes in the timing, pressure, and speed during the course of signing. While it may be very easy to duplicate the visual appearance of the signature, it is very difficult to duplicate the behavioral characteristics. Signature Recognition uses a pen and a specialized writing pad that are connected to a local or central computer for template processing and verification. Voice recognition is often used where voice is the only available biometric identifier, such as over the telephone.

THE IMPACT OF BIOMETRICS IN BANKING

The rapid digitization of banking services combined with the continued need to adopt stricter customer and employee identification protocols to prevent identity theft and fraud has set the table for biometric identification technology to become an integral and strategic part of financial service security platforms. Acting as a strong authentication tool to help secure ATM, brick and mortar, and online transactions, biometrics in banking also helps to increase customer trust and improve brand reputation. The necessity for a stronger authentication solution became inevitable in banking services because of the growing pace of sophisticated transactional technology adoption along with the unfortunate rise in fraud and security breaches due to reliance on traditional security systems such as passwords.

Biometric Technology in the Banking Sector

Biometrics are automated methods of recognizing customers through their biological characteristics and traits such as fingerprints, finger vein patterns, iris, and voice recognition. Biometric characteristics are unique for every individual and difficult to forge, which is why biometric verification and authentication is commonplace in immigration control, law enforcement, and forensic studies. Many banks worldwide are already using biometrics with their banking systems to authenticate employees and customers and among all banks utilizing biometrics,

52 percent are located in Asia. Japan has more than an estimated 15 million customers using biometric authentication for banking transactions. Banks in Mexico, South America, Africa, and the Middle East are also moving towards the use of biometric identification technology because of its popularity with consumers, and ability to offer more security than traditional personal identification numbers (PINs) and passwords.

Different Ways to Use Biometrics in Banking

Biometric technology is slowly replacing traditional passwords and token-based electronic access, signature-based branch service access, and PIN-based access in mobile banking and at ATMs. Here are ways that banks can use biometric technology to improve banking services and better protect customer assets:

Biometrics in Branch Banking

Financial service institutions are using fingerprint and finger vein biometrics in banking for customer identification in their branches because these two biometric authentication methods deliver fast results that are suitable for the busiest branches of a bank. Moreover, finger print and finger vein systems are user friendly, easy to use and ensure reliable security. When customers visit branches they can be authenticated at the counter through fingerprint and finger vein biometric scanners that match the customer's existing biometric template within the bank database, and after successful authentication, the customer will be allowed to move forward with their banking transactions.

Biometrics in Banking ATMs

Using biometrics in banking ATMs is popular in developed countries and the adoption rate is growing significantly. There are two approaches for customer authentication in ATMs — a customer using only biometrics and a bank card or a PIN along with biometric authentication. Therefore, facial recognition, fingerprints, finger vein patterns and iris recognition are the most suitable in ATMs as these biological traits can be easily authenticated in this environment. Furthermore, these types of biometric modalities also have other advantages such as flexibility, compactness, and accuracy.

Biometrics for Internet Banking

Many computers, laptops, and even smart phones already have webcams, microphones, and fingerprint scanners, offering flexibility for banks to easily adopt biometric authentication in online banking services with fingerprint, finger vein, facial, and voice recognition. When customers attempt to access their account, some banks now require them to provide a biometric credential first. Some banks require biometric authentication beside the traditional password to make authentication stronger, also known as a "multi-factor" authentication system. This helps banking institutions to protect customer identities from being compromised by cyber criminals and any others trying to illegally obtain sensitive customer information to commit a crime.

Biometrics in Mobile Banking

Mobile banking is growing rapidly worldwide, and according to Juniper Research, 400 million people performed a mobile banking transaction in 2013. Despite this large number, many bank customers still have a lack of trust over the security of mobile banking platforms and concerns over security. Banking transactions or customer services could be performed through a voice or speech recognition system where customers need to verify their identity using the microphone in their phones.

Single Sign on Solution for More Effective Password Management

Banks and financial institutions are suffering from network security and data breaches worldwide. According to a recent ACI Worldwide Survey, 44%of customer financial accounts have been compromised and 15% of breaches cause fraud. In a 2013 Ponemon Institute Survey, it was reported that an average cost of these types of incidents is $9.4 million. Banks can easily adopt biometric single sign on (SSO) solutions into their network for password management, identity management, data and network security, and two factor authentication. This system will eliminate vulnerable passwords and loopholes of a bank data security system and will protect both banks and customers from unauthorized access and data breaches. Furthermore, a biometric SSO system will mitigate other security risks and regulatory fines for government compliance.

BENEFITS OF USING BIOMETRICS IN BANKING

Protecting Banking Information

Biometric technology provides the strongest method of authentication that protects banking information from being compromised by unauthorized personnel.

Fast and Accurate Branch Banking

Biometric technology provides fast and accurate identification for the banking industry. Customers can be quickly authenticated in mere seconds through a fast biometric scan.

Protection Against Insider Fraud

Biometric identification of employees performing transactions on the back end is a crucial step to ensuring identity protection and reducing fraud. Biometrics in banking will help financial institutions to prevent insider fraud by establishing secure employee authentication, accountability and concrete audit trail of each transaction.

Secure Online Banking

Over the past years the banking sector has been suffering from massive online service cyber attacks. In most of these cases customers lose their money from the negative effects of identity theft. Biometrics in banking helps the bank to protect customer identities when using online banking services.

ATMs with Biometrics

Biometrics in banking for ATMs authentication brings outstanding benefits to both customers and banks. This system now gives customers flexibility to make transactions without bringing bank cards. Banks can avoid the costs and

liabilities of customer problems due to lost or stolen bank cards.

Audit Trails

Banks can easily track and monitor employee and customer activity in the system to create concrete audit trails with biometric technology solutions.

Fast, Secure and Accurate Customer Care Service

The banking sector is always in need of tighter security solutions to provide improved and more secure customer care service over the phone and internet. A biometric voice recognition system for example provides a secure and flexible solution to verify any customers executing transactions outside of a brick and mortar environment.

Conclusion

Based on the need for highly secured system in the banking sector in Nigeria, the CBN is proposing the used of fingerprint biometric measures in securing this systems thereby encouraging cashless economy in Nigeria. This will help to achieve strong banking systems security and also help in encouraging many customers in using these systems. However, because most fingerprint biometric can be cheated using artificial fingerprint, a multifactor biometric technique is recommended. The paper has presented a comprehensive conceptual multifactor biometric model suitable for implementing a secured platform for banking system. The full implementation of this model will help to achieve highly secured banking application and provide better banking services in the future.

References

1) Iris Recognition "An Identification Biometric system" by Abdul Basit.
2) "E-Banking and E-Commerce" by N. Subramani, M. Murugesan, D. Anbalagan, V. Ganesan.
3) "A Current Analysis of Biometric Technologies" by Jalaynea A.Cooper
4) "Biometrics: A Self-Service Viewpoint" by Gary Ross