International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611

Signature Authentication Using Biometric Methods

A. S. Syed Navaz[1], K. Durairaj[2]

[1]Assistant Professor, Department of Computer Science, Muthayammal College of Arts & Science, Namakkal, Tamilnadu, India

[2]Principal, Cheran Polytechnic College, Erode, Tamilnadu, India

Abstract: ***Signature identification using Biometrics methods is a well-studied problem in Biometrics. It involves the authentication of a person based on his signature. This paper is developed by using Vb.net as a front end Ms Access as backend. Our method validates the signature based on hand movement when a person signs his signature. Our method has a unique advantage over existing systems. A signature can be drawn easily by other unintended persons in important documents. But it is sure that only the original person can sign with the same fast movement and correct sequence. Since our method tracks the movement sequence and the speed with which the person signs his signature, it is highly accurate for authentication than any other existing system. One of the main advantages of our method is computationally inexpensive, that is it uses minimum system resources, less memory and hence offers a very high speed of recognition. Also, the signature identification cannot be duplicated unlike the existing methods where the passwords could be cracked using trail-and-error methods. We implement the system using the GUI tools of VB.NET. He has to draw his signature using the mouse in the panel and he/she is entered into the website based on the recognition result.***

Keywords: Biometric, Authentication**,** Signature, Palm, Scan

1. Introduction

A problem of personal verification and identification is an actively growing area of research. In our global information society, there is an ever-growing need to authenticate individuals. Biometrics-based authentication is emerging as a reliable method that can overcome some of the limitations of the traditional automatic personal identification technologies. Automated biometrics deal with physiological and/or behavioral characteristics, such as a fingerprint, signature, palm print, iris, hand, voice or face, which can be used to authenticate a person's claim to a certain identity or establish a person's identity from a large database. With the rapid progress made in electronics and Internet commerce and with the increased emphasis on security, there will be a growing need for secure transaction processing using biometrics technology. The methods are numerous, and are based on different personal Characteristics. Voice, lip movements, hand geometry, face, odor, fingerprint are the most commonly used authentication methods. All of these psychological and behavioral characteristics are called biometrics.

The biometrics is most commonly defined as measurable psychological or behavioral characteristic of the individual that can be used in personal identification and verification. The driving force of the progress in this field is, above all, the growing role of the Internet and electronic transfers in modern society. Therefore, considerable number of applications is concentrated in the area of electronic commerce and electronic banking systems. The general definition of signature is, According to American Heritage Dictionary signature can be defined as: “the name of a person written with his or her own hand; the act of signing one's name” Signature verification is the process used to recognize an individual's hand-written signature. Biometrics is expected to be incorporated in solutions to provide for Homeland Security including applications for improving airport security, strengthening our national borders, in travel documents, visas and in preventing ID theft. Now, more than ever, there is a wide range of interest in biometrics across federal, state, and local governments. There are many needs for biometrics beyond Homeland Security. Enterprise-wide network security infrastructures, secure electronic banking, investing and other financial transactions, retail sales, law enforcement, and health and social services are already benefiting from these technologies. A range of new applications can been found in such diverse environments as amusement parks, banks, credit unions, and other financial organizations.

Biometrics is automated methods of recognizing a person based on a physiological or behavioral characteristic. Among the features measured are; face fingerprints, hand geometry, handwriting, iris, retinal, vein, and voice. Biometric technologies are becoming the foundation of an extensive array of highly secure identification and personal verification solutions. Biometric-based solutions are able to provide for confidential financial transactions and personal data privacy. The need for biometrics can be found in federal, state and local governments, in the military, and in commercial applications. Enterprise-wide network security infrastructures, government IDs, secure electronic banking, investing and other financial transactions, retail sales, law enforcement, and health and social services are already benefiting from these technologies.

1.1 Physiological or Behavioral Biometrics

The physiological biometrics is based on measurements and data derived from direct measurement of a part of the human body. Fingerprint, iris-scan, retina-scan, hand geometry, and facial recognition are leading physiological biometrics. Behavioral characteristics are based on an action taken by a person. Behavioral biometrics, in turn, is based on measurements and data derived from an action, and indirectly measure characteristics of the human body. Voice recognition, keystroke-scan, and signature-scan are leading behavioral biometric technologies. One of the defining characteristics of a behavioral biometric is the incorporation

of time as a metric – the measured behavior has a beginning, middle and end. A biometric system is essentially a pattern recognition system which makes a personal identification by determining the authenticity of a specific physiological or behavioral characteristic possessed by the user. An important issue in designing a practical system is to determine how an individual is identified.

There are two different ways to resolve a person's identity: verification and identification. Verification (Am I whom I claim I am?) involves confirming or denying a person's claimed identity. In identification, one has to establish a person's identity (Who am I?). Each one of these approaches has its own complexities and could probably be solved best by a certain biometric system.

In day-to-day life most people with whom you do business verify your identity. You claim to be someone (your claimed identity) and then provide proof to back up your claim. For encounters with friends and family, there is no need to claim an identity. Identification (1:N, one-to-many, recognition) – The process of determining a person's identity by performing matches against multiple biometric templates. Identification systems are designed to determine identity based solely on biometric information. There are two types of identification systems: positive identification and negative identification. Positive identification systems are designed to find a match for a user's biometric information in a database of biometric information.

Positive identification answers the "Who am I?" although the response is not necessarily a name – it could be an employee ID or another unique identifier. A typical positive identification system would be a prison release program where users do not enter an ID number or use a card, but simply look at a iris capture device and are identified from an inmate database. Negative identification systems search databases in the same fashion, comparing one template against many, but are designed to ensure that a person is not present in a database. This prevents people from enrolling twice in a system, and is often used in large-scale public benefits programs in which users enroll multiple times to gain benefits under different names. Not all identification systems are based on determining a username or ID. Some systems are designed determine if a user is a member of a particular category. For instance, an airport may have a database of known terrorists with no knowledge of their actual identities. In this case the system would return a match, but no knowledge of the person's identity is involved. Verification (1:1, matching, authentication) The process of establishing the validity of a claimed identity by comparing a verification template to an enrollment template. Verification requires that an identity be claimed, after which the individual's enrollment template is located and compared with the verification template. Verification answers the question, "Am I who I claim to be?" Some verification systems perform very limited searches against multiple enrollee records.

For example, a user with three enrolled fingerprint templates may be able to place any of the three fingers to verify, and the system performs 1:1 matches against the user's enrolled templates until a match is found. One-to-few. There is a middle ground between identification and verification referred to as one-to-few (1:few). This type of application involves identification of a user from a very small database of enrollees. While there is no exact number that differentiates a 1:N from a 1:few system, any system involving a search of more than 500 records is likely to be classified as 1:N. A typical use of a 1:few system would be access control to sensitive rooms at a 50-employee company, where users place their finger on a device and are located from a small database.

1.2 Applications areas

Biometrics is a rapidly evolving technology which is being widely used in forensics such as criminal identification and prison security, and has the potential to be used in a large range of civilian application areas. Biometrics can be used to prevent unauthorized access to ATMs, cellular phones, smart cards, desktop PCs, workstations, and computer networks. It can be used during transactions conducted via telephone and internet (electronic commerce and electronic banking). In automobiles, biometrics can replace keys with key-less entry devices.

1.3 Biometrics Technologies

The primary biometric disciplines include the following:

Fingerprint (optical, silicon, ultrasound, touch less) Facial recognition (optical and thermal)

Voice recognition (not to be confused with speech recognition

- Iris-scan
- Retina-scan
- Hand geometry
- Signature-scan
- Keystroke-scan
- Palm-scan (forensic use only)

Disciplines with reduced commercial viability or in exploratory stages include:

- DNA
- Ear shape
- Odor (human scent)
- Vein-scan (in back of hand or beneath palm)
- Finger geometry (shape and structure of finger or fingers)
- Nailbed identification (ridges in fingernails)
- Gait recognition (manner of walking)

Application area for Motion based Signature recognition are:

- Time Attendance
- Access control
- Time Attendance
- Identification card
- Immigration checks
- Police records
- Customer identification, Loyalty programs
- Security systems

- Patient management in hospitals.

2. Problem Description

2.1 Existing System

The existing system recognizes the person with digital signature. This digital signature method is widely used and this is data encryption mechanism and concept of hash function. Both combined to produce the unique long encrypted number for signature. This system can also be affected by intruders who can misuse the data or information available.

2.1.1 Drawbacks

- Easily traceable by intruders
- Low reliability
- No unique identification

2.2 Proposed System

The biometrics have a significant advantage over traditional authentication techniques (namely passwords, PIN numbers, smartcards etc.) due to the fact that Biometric characteristics of the individual are not easily transferable, are unique of every person, and cannot be lost, stolen or broken.

2.2.1Advantages

The choice of one of the biometric solutions depends on several factors:

- User acceptance
- High Level of security required
- Accuracy High
- Cost and implementation time is Low

2.3 Description

The paper entitled as "Signature Authentication Using Biometrics methods" comprises of the following modules described below:

2.3.1New Person

The users who are new to this are asked to register themselves with the details such as name of the person, occupation, the desired ID of the person that is to be used in this paper are collected from the user while registering.

2.3.2Select Person

The person is selected with the help of the person ID that is already saved using the new person module. The list of the person ID's are displayed and the task of the user is to select the appropriate name and click on the "Select" button for further processes.

2.3.3New Sign

The signature of the new person is registered through this module. The person is given a name with person ID and with the help of the signature form, the person registers his/her signature. This form provides the space where the selected person can make his/her own handwritten signature with mouse. The coding is written for mouse drag event and so the signature is visible when the user leaves the mouse button. While drawing the signature the threshold value in X direction, Y direction and Time threshold are all checked and stored. This value can be used for recognition purpose. This form contains Clear button, through this particular person's signature can be deleted from the database table

For data store the OleDb.Connection object is used to connect to Access. The table contains the signature details in the form of XY Index, X, Y co-ordinate position, Direction and Interval values. So the pictorial information is stored in the form of numerical set of data.

2.4 Recognize Sign

This module is used to recognize the signature of the existing users and this sign is checked with the signature that is been already registered by the user. If both the signatures match, the users are allowed into the paper. It contains the space for drawing user's signature. First user has to draw the signature with mouse and then click the Recognize button. Here the form retrieves signature information from table. Now it calculates same numerical data for this signature. Now the comparison is made between the data already present and calculation made now in the point of view of the stroke in which the user signs and the time interval he has taken. If both signature's comparative status is displayed as result "Accuracy Direction % and Interval %".

3. System Implementation

Implementation includes all those activities that take place to convert from the old system to the new. The new system may be totally new, replacing an existing system or it may be major modification to the system currently put into use. This system "Motion Based Signature Recognition" is a new system. Implementation as a whole involves all those tasks that we do for successfully replacing the existing or introduce new software to satisfy the requirement.

The test case has performed in all aspect and the system has given correct result in all the cases

4. Conclusion

Our system is proposed to use Biometrics concept in Signature Recognition which eliminates the flaws in the existing system. This system makes use of user's behavior characteristic as tool for recognition. The application is developed successfully and implemented as mentioned above.

This system seems to be working fine and successfully. This system can able to provide the user to give their Specimen signature and later it is used for verification. The signature whether recognized or not is given in the form of accuracy result of comparison. The accuracy is in view of Direction and Interval in terms of percentage given as output display.

4.1 Future Enhancement

This paper done with detailed analysis of existing system and a careful design. So that future modifications can be done in efficient manner with minimum disturbance to the system.

- The system is very flexible and user friendly.
- In future by use of databases more efficient retrieval can be achieved.
- Later by use of some other techniques the system will achieve 100% accuracy.

References

[1] Richard Fairley,"Software Engineering Concepts", Tata McGraw hill publications, 1997.
[2] A.S.Syed Navaz, T.Dhevisri & Pratap Mazumder "Face Recognition Using Principal Component Analysis and Neural Networks" March -2013, International Journal of Computer Networking, Wireless and Mobile Communications. Vol No – 3, Issue No - 1, pp. 245-256.
[3] Elias.M.Award,"System Analysis And Design", Galgotia Publications 1997.
[4] Syed Fiaz A.S, Alsheba I, Meena R., "Using Neural Networks to Create an Adaptive Character Recognition System", Discovery - The International Daily journal, 37(168), 53-58, 2015.
[5] Shooman, "Software Engineering", Tata McGraw hill Publication 1997.
[6] Steven Holzner, "Visual Basic .Net Programming "Black Book - Dream Tech Press, New Delhi.
[7] G.Andrew Duthie, "Microsoft Visual Basic.Net version 2003".
[8] A.S.Syed Navaz & R.Barathiraja "Security Aspects of Mobile IP", Journal of Nano Science and Nano Technology, February 2014, Vol No - 2, Issue – 3, pp - 237-240.
[9] Harold Davis, "Visual Basic.Net for Windows", II Edition.
[10] A.S.Syed Navaz, C.Prabhadevi & V.Sangeetha"Data Grid Concepts for Data Security in Distributed Computing" January 2013, International Journal of Computer Applications, Vol- 61 – No 13, pp 6-11.

Author Profile

A.S.SYED NAVAZ received M.Sc in Information Technology from K.S.Rangasamy College of Technology, Anna University Coimbatore, M.Phil in Computer Science from Prist University, Thanjavur, M.C.A from Periyar University, Salem, PGDCA in Erode and Pursuing Ph.D in the area of Wireless Sensor Networks. He has researched and published 19 papers in International journals and working as an Editorial Board Member in 7 International Journals & Reviewer for 15 International journals including Springer. He is a Member of 13 International Social Bodies. His biography is listed in "Marquis Who's who in the World" 2015 & 2016 (32nd & 33rd Edition) USA. Currently he is working as an Assistant Professor in the Department of Computer Science at Muthayammal College of Arts & Science, Namakkal, India. His Research areas are Wireless Sensor Networks, Mobile Computing & Image Processing.

K. Durairaj received his BE in (CS) from Annai Mathammal Sheela Engineering College, Namakkal, He is having more than 8 years Experience in Teaching. Currently he is working as Principal in Cheran Polytechnic College at Namakkal. His Research areas are Networking.