

User Verification System

William Baker, Arthur Evans, Lisa Jordan, Saurabh Pethe
Under the guidance of Professor Cha

Abstract

Currently, small and large scale businesses are in need of advanced security measures to keep both customers and employees safe from today's possible dangers. An excellent method of security, which is almost essential, is to identify a person quickly, easily and accurately. This type of security hasn't been accomplished and proven through modern day technology up until now. We describe the technology which makes it possible to use cutting edge software and hardware to implement this particular type of security. The presented paper is an ongoing project in hybridizing multiple biometrics that include Handwriting, Voice, Fingerprinting and Face for verifying the user. The purpose is to develop a high-confidence user verification system that uses multiple biometrics that can be used to alleviate several practical problems which are associated with current personal identification methods. Biometrics are supposed to be possessed by each person in the target population but, in practice no biometrics truly is. For instance, every person has a fingerprint, but a small fraction of the population has a fingerprint which is not easily captured by the features adopted by a given system. A single biometric may not be acceptable to different sections of the target population and one could give users a choice of biometrics. . In addition, identifications from multiple independent biometrics offer increasingly irrefutable proof of the identity of a person, and reinforces confidence and reliability. This is why more than one biometrics were used in this system.

Introduction

Security is an important issue in the world that we live in today. It is a concern for various industries such as airlines, banks, government agencies, educational institutions among others. Many businesses rely on security as the number one factor for their customers. For example, customers would not want to fly on any commercial jet that belongs to an airline with inadequate or limited security. Law enforcement and security companies would also want to identify people accurately with the use of an advanced system that will quickly give them an answer to the person's true identity. This new system will the ability to authenticate a person using several techniques, which will be appealing to any company with the need to quickly identify a person. Similar uses have been accomplished by the police and law enforcement utilizing DNA, but none to recognize a particular person over another using the methods we have outlined herein.

Since the tragedy of 9/11 people in the US have been in a frenzy to regain a sense of security and sense of well-being. Companies can help this problem by using devices that would reduce the threat of terrorism and crime. Security products of this type will not only deter criminals from committing illegal acts, but will influence customers and people to feel secure in every day life. This type of computer system will provide a method to identify criminals and unauthorized personnel, and will actually authenticate their identity within seconds. Computer systems of this type will be appealing to many different business practices that would like to increase security and increase the faith and well being in customers.

Our intention is to provide a user verification system for industries that require extensive security. Our project, the User Verification System, will be comprised of a user verification system comprising several specific pattern recognition techniques using complex mathematical algorithms mainly, Artificial Neural Networks (ANN). This verification system consists of fingerprinting, handwriting, and voice input devices.

Biometric rate of change is one of the key elements that project the demand for this type of technology in the market. International Biometric Group's Biometric Market Report 2000-2005 is a comprehensive analysis of revenues, growth trends, and industry developments in the current and future biometric marketplace. The estimates and projected results are shown in Fig 1 [6].

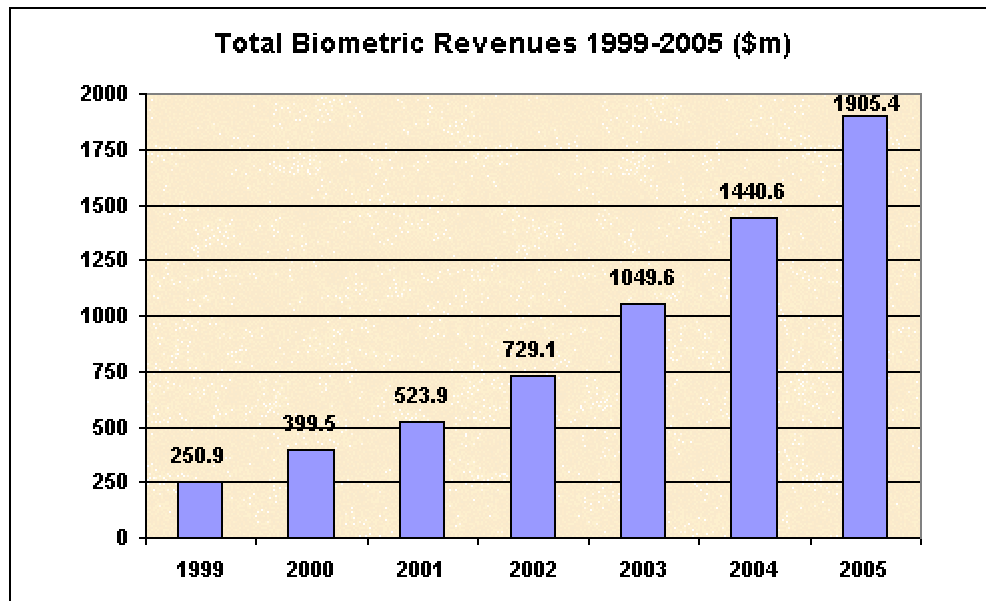


Fig 1. Total Biometric Revenues expected for the period of 1999-2005.

It is easy to see from the graph (Fig 1.) that biometric revenues will multiply in number over the next couple of years. In the search of a more secure world this type of technology appears that it may provide many solutions and it will be around for many years to come.

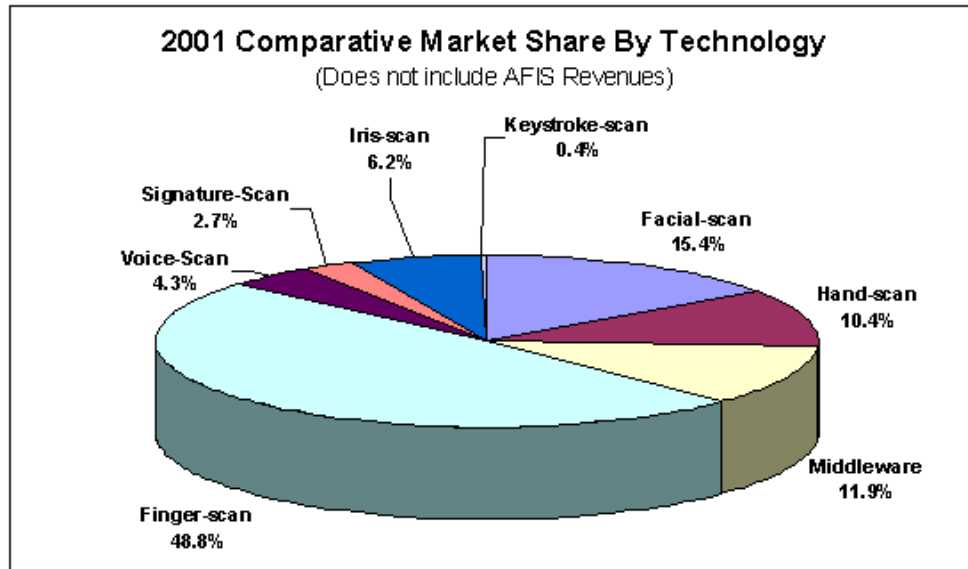


Fig 2. Market share by technology

From this figure (Fig 2)[6] we can say that the “ User Verification System” has nearly 70% of the market share which includes Finger-Scan, Voice-Scan, Facial-Scan, Signature-Scan, as of the year 2001 and will keep on growing.

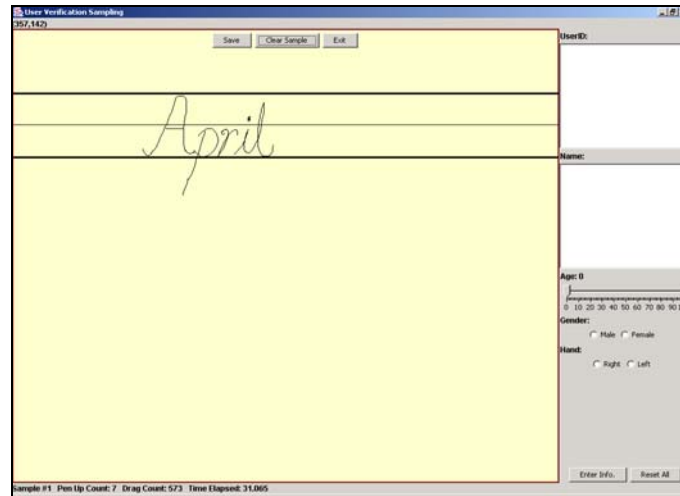
Besides the overwhelming statistics that show that this is a technology that will be in demand, here are advantages to having an advanced user verification system compared to the current practices:

1. Increased speed of determining a persons identity
2. Higher accuracy of determining an individual
3. Reliable or failsafe by having multiple recognition techniques or biometrics
4. Possibility of making this system portable
5. Increased security in companies
6. Appealing to customers and employees, knowing that the company invests in advanced security technologies
7. Reduced amount of time to identify a suspect or criminal for law enforcement
8. Difficult to challenge the system by forging names and mimicking voices making it virtually impossible to pass as someone else
9. Possible use in a court of law to prove criminal cases
10. Relatively inexpensive
11. Low maintenance software

User Verification Types

Handwriting

A Java applet is developed to provide a user interface. This is self explanatory and easy to use.



The user's details include Name, Age, Gender and Left/Right handed are entered. The user is provided with a user identification number (userid), for now which is entered manually by an administrator. The "EnterInfo" button will enter the information of the user and also create a folder in name of the userid. If there is any mistake a "Reset All" button is provided to clear all the user information. A prompt is provided for to the user to give his handwriting samples.

For collecting the handwriting samples we using a LCD pen Tablet. The specifications of this are:



- 1,024 levels of pressure
- Tablet resolution=2540 lpi
- Ergonomic grip pen
- Large active area.
- Size: 6X 8

When the user provides samples, the feature extractor class extracts specific features. The features that we are concentrating on are: width, height, pen-drag count, number of strokes, total stroke time, total stroke distance, total sample time, stroke direction sequence strings and acceleration. Along with this we are storing the raw the data, x and y co-ordinates of the entire sample from the first pen down to the last pen up.

Face

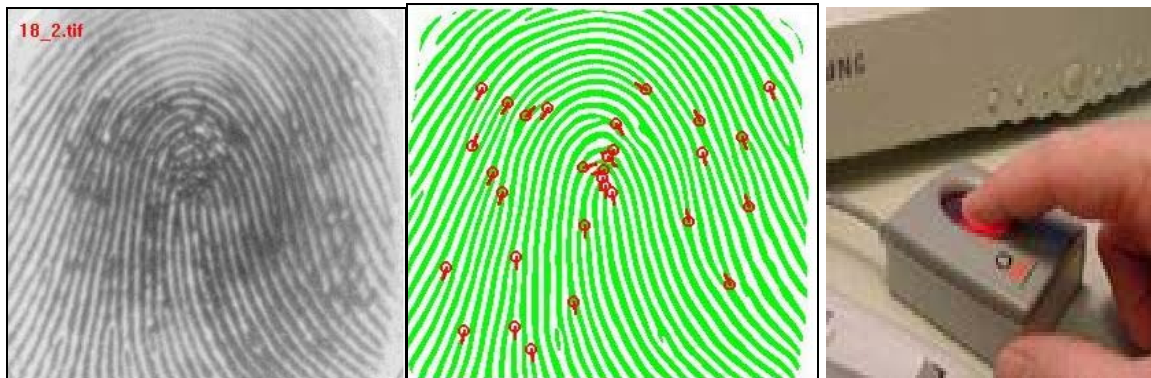
Faces are identified by comparing local features with those for faces stored in a database. Partial matches allow recognition though glasses, beards, and weight change. There are a number of applications for face recognition including surveillance, database lookup, video indexing, secure computer logon, and airport and banking security. Face recognition requires face images, which can be color or black and white, from video tape or pictures. We are using a small database of samples pictures captured by a digital camera in this project. The pictures are stored in flat files with a specified size 145x200 at 8bpp.

Voice

Voice biometrics relies on human speech, which is the primary modality in human-to-human communication, and provides a non-intrusive method for authentication. By extracting appropriate features from a person's voice and modeling the *voiceprint*, the uniqueness of the physiology of the vocal tract and articulator properties can be captured to high degree and used very effectively for recognizing the identity of the person.

Fingerprint

Fingerprints are a distinctive feature and remain invariant over a person's lifetime, except for cuts and bruises. Fingerprint authentication requires acquiring and digitizing a fingerprint impression. The digital image of the fingerprint includes several unique features in terms of ridge bifurcations and ridge endings, collectively referred to as minutiae. The next step is to locate the minutiae in the fingerprint image using an automatic feature extraction algorithm, which analyzes spatial relationships. Finally, a matching system attempts to arrive at a degree of similarity between the stored image and the fingerprint sample.



The figure shows the bifurcations and ridge endings.
We are using a biometrics fingerprint scanner to collect the samples.

Classifier

Artificial Neural Networks:

Artificial neural networks (ANN) are collections of mathematical models that emulate some of the observed properties of biological nervous systems and draw on the analogies of adaptive biological learning. The key element of the ANN paradigm is the novel structure of the information processing system. It is composed of a large number of highly interconnected processing elements that are analogous to neurons and are tied together with weighted connections that are analogous to synapses.

ANN technology gives computer systems an amazing capacity to actually learn from input data.

The purpose of using ANNs in this project is that they have many powerful properties which make them extremely useful and interesting. The first property ANNs are adaptive and flexible. A single ANN can approximate in principle and can learn it. We don't have to change ANN's architecture or learning rules: just change the teaching material. And more interestingly, to change the teaching material is essentially the same as to introduce a new environment. Therefore, ANNs are adaptive.

Their construction is also such that they are *holistic*. The function which they perform is distributed. This distribution offers tolerance for errors and noise. There can be errors or noise in the input when the network is still behaving correctly. This is because those errors either are so small or they are compensated by correct signals.

Dichotomy: Dichotomy is defining the problem in two classes, for example distinction between male and female, separate male class and female class. We use this concept for the User Verification System, we use separate class within and between.

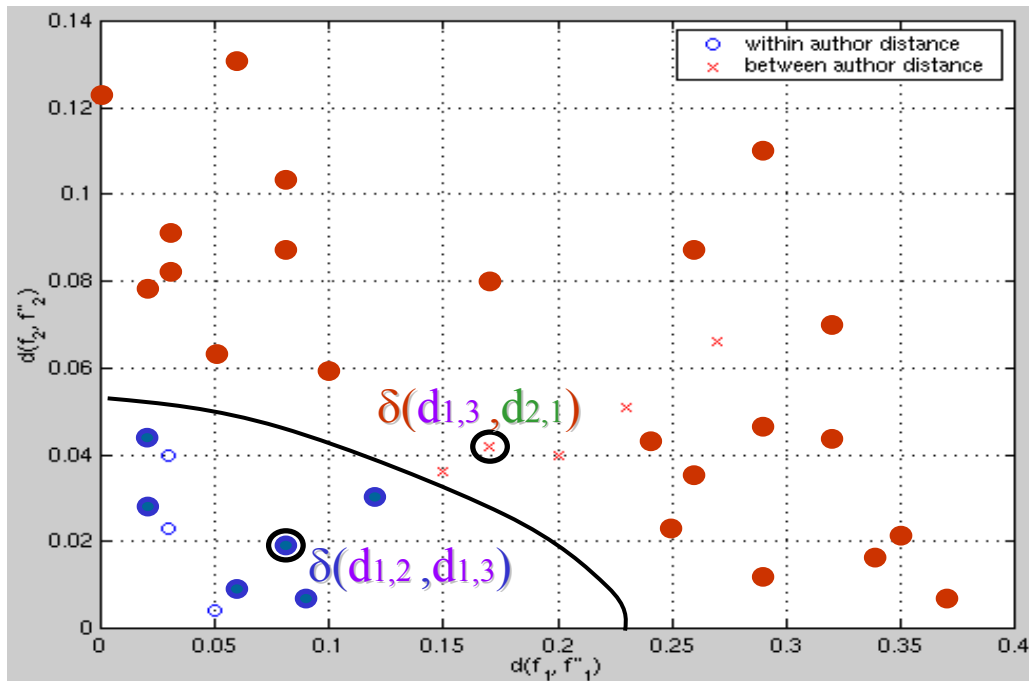


Fig 3

Fig 3. shows: O = Within a class
 X = Between classes
 $\delta(d_{1,2}, d_{1,3})$ = distance within the class1 of samples 2 and 3
 $\delta(d_{1,3}, d_{2,1})$ = distance between the class1, sample 3 and class 2, sample 1

To establish the inherent distinctness of the classes, i.e., validate individuality, we transform the many class problem into a dichotomy. This is done by, first normalizing the entire database of the features, calculating "distance" between two samples of the same class and those of two different classes.

Structure of ANN used for User Verification System:

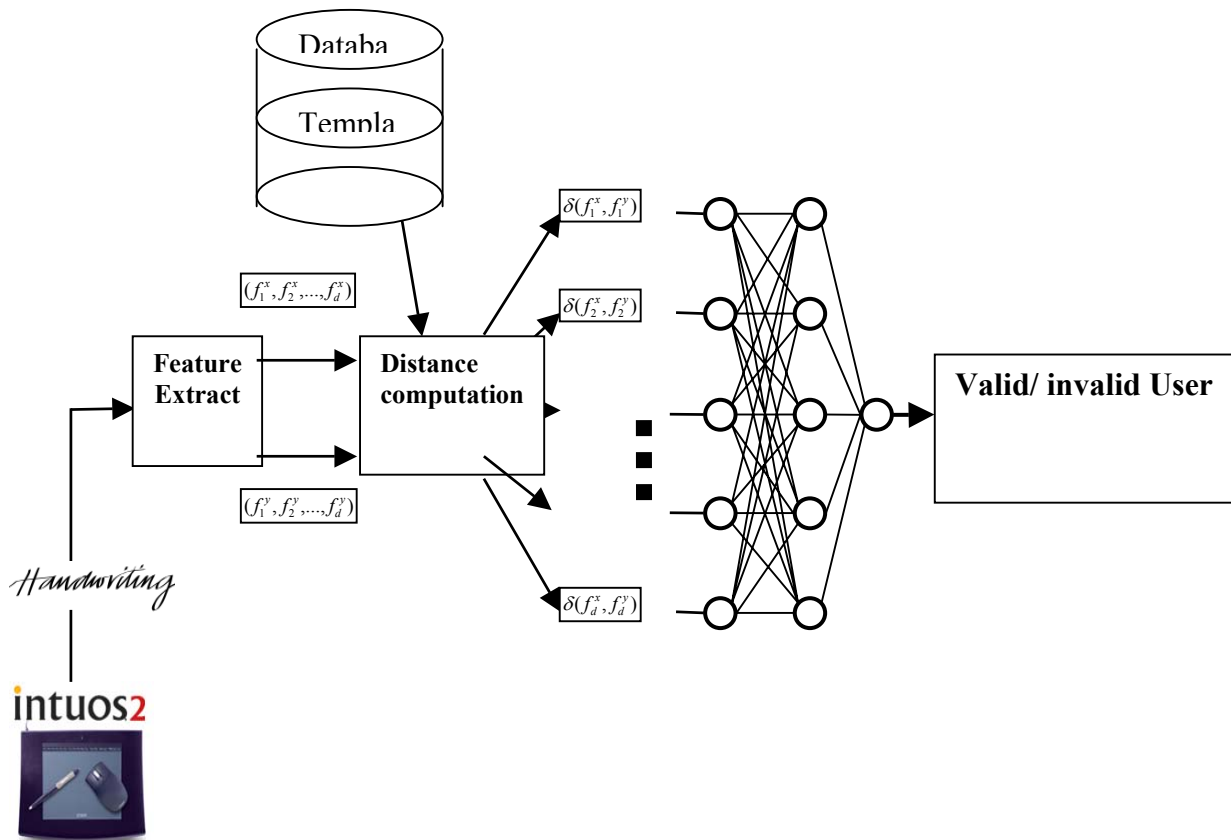


Fig 4. Artificial neural network

Fig. 4. represents the structure of artificial neural network that is being used for the system. This shows the verification system, the example is that for handwriting verification. The unknown user is asked for a handwriting sample using the Pen tablet

provided. Features from this sample are extracted. The template corresponding to this user is utilized from the database that has already been stored during the training process. This template and the template from the new sample, distance computation is done on each feature and then passed to the neural network. The structure of ANN is decided as to provide one of two types of outputs, valid or invalid.

Conclusion

From the data gathered about this technology it is easy to tell that this type of system will be in high demand for the years to come. A sense of security is one thing that is not easy obtain in today's world and with a user verification system it seems that we have a way to increase security and help put our minds at ease. Our high-confidence user verification system intends to provide security to institutions and others who are in the market for a verification system. It will enhance security for organizations and agencies that utilize this verification system and enhance the customer's sense of security towards a company that has this type of technology.

Some of the controversial issues that have come out of this project and should be explored. One of the issues that came up is that the recognition is not 100% accurate and may give a margin of error. This is a problem when using a single biometric but when used with multiple biometrics the accuracy increases tremendously. Another problem is that companies will have to make a decision on how close a biometric has to be to authenticate a person. Certain variances have to be established in order to make a standard for authentication. Having a system that is too sensitive might not validate a person and a system that is not sensitive enough might falsely validate a person. In addition people that have uncontrollable circumstances may not be able to access to system. ie) a person with a cold cannot be recognized by the system because their voice has changed. A person with a broken arm may not be able to sign their name the same. Again, a standard has to be in place for the business. Finally, acceptance of this new technology from the society is important and may drive the need for this technology up or down. If many similar products fail in the market it could prove to be a worthless technology in the publics view as a whole.

In the future we will attempt to broaden our scope of this project and by doing so appeal to a larger market. From the projections of the market we will expand the general ideas of the user verification to utilize the biometric technology to accommodate in future trends in the market. We intend to increase the accuracy of security by adding more features to the system such as, retinal scans, or iris scans and facial recognition, with enhanced features providing additional accuracy. The user verification system can expand it's adaptability to different situations and conditions, and will become increasingly versatile.

References:

- [1] Lawton, G.[George], Biometrics: A New Era in Security, Computer(31), No. 8, August 1998, pp. 16-18.
- [2] Kittler, J.V., Matas, J., Jonsson, K., Sanchez, M.U.R., Combining Evidence in Personal Identity Verification Systems, PRL(18), No. 9, September 1997, pp. 845-852.
- [3] Jain, A.K.[Anil K.], Bolle, R.M.[Ruud M.], Pankanti, S.[Sharath], Biometrics: The Personal Identification in Networked Society, KluwerAcademic, Norwell, MA, 1999.
- [4] Jain, A.K., Hong, L., Kulkarni, Y., A Multimodal Biometric System Using Fingerprint, Face and Speech, AVBPA99 (xx-yy).
- [5] Phillips, P.J.[P. Jonathon], Martin, A.[Alvin], Wilson, C.L., Przybocki, M.[Mark], An Introduction to Evaluating Biometric Systems, Computer (21), No. 2, February 2000, pp. 56-63.
- [6] www.biometricgroup.com International Biometric Group