PROJ 102 Project Proposal

Project #029
Is this a real signature or not?

Group #048
Serhan Tutar
Enes Tever
Hasan Gönen

Supervised by:
Ayşe Berrin Yanıkoğlu
Mustafa Berkay Yılmaz

October, 25, 2012

Spring 2011-2012
Sabancı University

Abstract

In this project we will perform experiments in order to get data of the human success rate at detecting the forgery of signature. To do the experiments we will use computer software. In this software we will be given 5 reference signatures and a query. During the project we will learn more about the signature verification and see if it makes changes in our success rates. Our false rejection/ false acceptance rates will be compared with the signature verification software's rates. The result of comparison will show the reliability of the software based signature verification.

1. Introduction

Biometrics is recognizing people with automated system based on people's physiological and behavioral traits (Vacca, 2007).These traits include hand and fingerprint images, facial characteristics, iris, signature, voice of a person. Biometric systems are becoming more and more extensive in secure identification and verification. There are few steps of a biometric system. The first step of biometric system is enrollment. A subject gives a reference for a database such as an image of fingerprint, image of subject subject's iris or subject's signature's on a tablet, etc. This reference is recorded at a database and the reference will be used for comparison in future quires. On further step, when a query is made, software will take this input and compare it with references recorded in the database. Based on findings of comparison with the database, software will reject or accept of authenticity of the input. But this process could be problematic; sometimes software could give some false rejections and false acceptances. Our focus in biometrics will be the signature verification part.

Signature verification is the process used to recognize an individual's handwritten signature. Today there are two methods of signature verification. One of them is the static verification and the other one is the dynamic verification. The difference of them lies in the input values. While the static one uses only the image of the signature, the dynamic method uses several input values such as, (x, y) coordinate, time stamp, pressure, pen inclination, curvature and acceleration. For example a banker, who checks the signs of his/her clients using reference signature that he possesses, is actually an example for the static method. On the other hand a person, who signs on a pressure-sensitive tablet, is an example for the dynamic method. In comparison to the static method, which is more common but easy to forge, the dynamic method is more unique and has an error rate under 2% with the development of the new technologies. This successful rate encouraged the companies to use the dynamic signature verification as security systems in the building entrances, laptops, PDAs, online banking and also as an employee tracking system.

There are two possible error rates in the dynamic signature verification which determines if the biometric software is effective or not. These are,

False Acceptance Rate: It is the rate that determines how often an forger can pass the biometric authentication. If this rate is low, the authentication system is secure.

F.A.R = NUMBER OF ACCEPT / NUMBER OF IMPOSTOR

False Rejection Rate: It is the rate that determines how often a real user will not pass. A high rate causes usability problems.

F.R.R = NUMBER OF REJECT / NUMBER OF GENUINE

There are some advantages and disadvantages of dynamic signature. Dynamic signature verification is more secure because by using a cheap hardware you can detect if the signature is the original or not. The system can detect the forger in short time and response quickly. However there are also some disadvantages. These systems also record that how long does it take to sign and if you have a muscular illness and if it takes a long time to sign, then the system will not accept your signature.

2. Definition and Scope

Our aim is to measure the ability and the improvement of the human in biometrics, specifically in recognizing forgery of signature if he/she is given a short or long time. The participants of the test are our entire group members. We are going to participate in 6 tests, each of them including 50 – 100 signatures. During the tests we will be shown 5 reference signatures of one person and other several signatures, either a fake or a genuine one, which are claimed to belong this person. The time until we end up with a decision is going to be either short (10 seconds) or long (a few minutes). All of the tests will be done and recorded by software. After each test we will be given lessons on recognizing the forgery. So at the end we will analyze the results if there was a contribution of the lessons or if there was a change, when we were given longer time.

2.1. Project Objective Statement

We are predicting to reach a success rate above the half. During the object we will use MATLAB which is computer software. We plan to finish the project before January 5, 2012.

2.2. Deliverables

At the end of this project, we will have created various statistics about the human's ability to recognize the forgery of signature. These statistics will contain the criteria like the given time, the effect of the lessons on recognizing the forged ones and if we would be given the information about the timing of the signature. The results of the whole project will be used as a reference about the articles regarding the biometrics, especially the signature verification.

2.3. Milestone

The first milestone of our project is learning the biometrics in general. Then we will learn briefly signature verification methods. Lastly we will learn in a more detailed way human based signature recognition which will be taught us fragmentary after each experiment.

3. Project planning

3.1. Work breakdown structure

3.1.1 Learning the biometrics in general (1 Week)

3.1.2 Learning the signature verification methods (1 Week)

3.1.3 Performing the experiments and learning how to recognize the forgery of signature (6 Weeks)

3.1.4 Collecting and analyzing all the data recorded (1 Week)

3.1.5 Concluding the data to an idea about the signature verification (1 Week)

3.2. Organizational structure

Since we all are doing the experiments as individuals, all of us have to come to the lessons and perform the experiments on their own. So we will be working on the same things at the same time. But at the end we will bring our results/data together and come to a conclusion as a group.

We will meet with our supervisors at a time which we will arrange later. At home each group member will spend approximately 1 – 1,5 hours at each experiment, which will last for 6 weeks.

3.3. Time and Resource Plan

Tasks	WBS Code	Description	Duration (week)	Number of Precedents	Start	Finish
1	1,1	Learning the biometrics in general	1	3	0	1
2	1,2	Learning the signature verification methods	1	3	1	2
3	1,3	Performing the experiments and learning how to recognize the forgery of signature	6	3	2	8
4	1,4	Collecting and analyzing all the data recorded	1	3	8	9
5	1,5	Concluding the data to an idea about the signature verification	1	3	9	10

References

Vacca, J. R., (2007). *Biometric technologies and verification systems*. Boston: Butterworth - Heinemann/Elsevier. 3-15, 169-180.