Pace University
DigitalCommons@Pace

CSIS Technical Reports

Ivan G. Seidenberg School of Computer Science and Information Systems

11-1-2005

Biometrics and Its Use in Forensics

Jason Bernard Thompson
Pace University, Ivan G. Seidenberg School of Computer Science and Information Systems

Follow this and additional works at: http://digitalcommons.pace.edu/csis_tech_reports

Recommended Citation
Thompson, Jason Bernard, "Biometrics and Its Use in Forensics" (2005). *CSIS Technical Reports*. Paper 22.
http://digitalcommons.pace.edu/csis_tech_reports/22

This Article is brought to you for free and open access by the Ivan G. Seidenberg School of Computer Science and Information Systems at DigitalCommons@Pace. It has been accepted for inclusion in CSIS Technical Reports by an authorized administrator of DigitalCommons@Pace. For more information, please contact rracelis@pace.edu.

SCHOOL OF COMPUTER SCIENCE AND INFORMATION SYSTEMS

TECHNICAL REPORT

Number 220, November 2005

Biometrics and Its Use in Forensics

Jason Bernard Thompson

PACE
UNIVERSITY
IVAN G. SEIDENBERG
SCHOOL OF COMPUTER SCIENCE
AND INFORMATION SYSTEMS

Jason Bernard Thompson holds a newly minted Bachelor of Science in Criminal Justice with a concentration in law enforcement. During his last two years at Pace, from 2003-2005, he was a Resident Assistant in Dow Hall, North Hall, Martin Hall, and New Dorm. In 2002-2003 he was the Vice President of the Resident Hall Association.

Jason has held internships with the New York Police Department and the United States Marshal Service. He is currently with the New Jersey State Police Department and anticipates service as a New Jersey State Trooper.

Biometrics and Its Use in Forensics

Jason Bernard Thompson
Dyson School of Arts and Science
Term Paper for Dr. Charles Tappert, CS 490, Summer I, 2005

Abstract

This paper describes how biometrics is used in Forensics. It first gives a general introduction to biometrics describing the main biometric techniques of fingerprinting, hand geometry, eye/iris scans, and DNA. Then it gives an introduction of forensics with an example criminal case. Finally it discusses how biometrics is used in forensics, including an interesting handwriting example from the Ted Bundy case.

Biometrics

Webster gives the scientific definition of biometrics as "the technique of studying physical characteristics of a person" [12], such as finger prints, hand geometry, eye structure/retinal scans, typing style, and voice prints. A person's physical characteristics, such as hand geometry and eye structure, cannot be easily changed without major surgery. Biometrics are the things that you see, hear, and feel when you meet or remember a person. Currently there is strong demand for security and passwords, and locks and keys, as well as computer passwords, are not going to be sufficient for most security purposes in the future. Although the idea of using biometrics for user authentication is not new, it is getting renewed interest with the increased demand for personal, corporate, and national security.

To harden passwords, several companies, such as Musicrypt.com [3] and NetNanny.com [3], have started to look at using keystroke biometrics because a person's keystroke patterns are difficult to duplicate. The way it works is as follows. The user types his

password on the keyboard, the system records the timing of key presses and key-press transitions and compares them to the person's enrolment data in the database, and then allows entry if they are sufficiently close. Because your password is something that you frequently key in, you tend to type it fast and without thinking with a particular pattern that is difficult to copy. This type of biometric is known as behavioral in contrast to the physical biometrics.

One of the most widely used biometric methods is fingerprints. Fingerprints are unique to the individual; no two fingerprints are the same even in identical twins. Fingerprints are identified or matched by using a series of ridges that consist of whirls, loops, and arches (Fig.1).

Figure 1. Fingerprint pattern examples: Whirls (top), Loops (bottom left) and arches (bottom right)

Of the fingerprint patterns, whorls tend to have the most amount of variation among them. Fingerprints are left behind on most surfaces when touched by someone with their bare hands. Fingerprints are one of the few ways that you can definitely identify one person from another. However, using fingerprints in criminal cases is an arduous task. For this reason law enforcement created IAFIS to help catalogue and identify fingerprints. IAFIS, the Integrated Automated Fingerprint Identification System, uses the national fingerprint database to obtain

positive matches of fingerprints found at crime scenes [7]. Although IAFIS is a high-tech way of identifying fingerprints, the way the fingerprints get into IAFIS is low tech. Each fingerprint recovered at a crime scene or taken by a creditable company is individually entered by hand by an operator. The only flaw in IAFIS is that it can't identify fingerprints that have not been previously entered into the database. Using your fingerprints as a way of gaining access to a computer or to a building is an excellent method because your fingerprints cannot be easily copied. Retinal scans or eye structure is also a good way to ensure that information is keep secure.

Like fingerprints your eyes are also unique, and corporations and government agencies with highly sensitive material might use them for access control. Retinal scanning analyses the layer of blood vessels at the back of the eye. This scanning involves using a low-intensity light source and an optical coupler and can read the patterns at a great level of accuracy. It does require the user to remove glasses, place their eye close to the device, and focus on a certain point. The way retinal scans work is that a user looks through a small opening in the device at a small green light. The user must keep their head still and eye focused on the light for 10 to 15 seconds during which time the device will verify his identity. Because there is no known way to replicate a retina and a retina from a dead person would deteriorate too fast to be useful, no extra precautions have been taken with retinal scans to be sure the user is a living human being.

Another biometric is a voice print allows someone to access material by using there voice. The way sound is produced is that it originates at the vocal cords. In between the vocal cords is a gap, and when we begin to speak, the muscles which control the vocal cords contract, and as a result, the gap narrows, and as we exhale, this breathe passes through the

gap, which creates sound. The unique pattern of an individual's voice is then produced by the shape of a person's vocal apparatus that consists of the laryngeal pharynx, oral pharynx, oral cavity, nasal pharynx, and the nasal cavity. It is these unique patterns created by the vocal apparatus that is used by voice recognition systems. The user has to give a sample of there voice usually by the user reading a passage or a predetermined document that the system recognizes. Voice recognition is both a physical and behavioral biometric. However, it is not as accurate as most pure physical biometrics.

Hand geometry is yet another option when it comes to biometrics security. Hand geometry involves the measurement and analysis of the shape of one's hand [2]. It is a fairly simple procedure and is surprisingly accurate. Though it requires special hardware to use, it can be easily integrated into other devices or systems. Unlike fingerprints, the human hand isn't unique. Individual hand features are not descriptive enough for identification. However, it is possible to devise a method by combining various individual features and measurements of fingers and hands for verification purposes. It works by the user placing the palm of his hand on a metal surface which has guidance pegs on it. The hand is properly aligned by the pegs so the device can read the hand attributes. The device then checks its database for verification of the user. The process usually takes less than 5 seconds. Since current hand geometry scanners do not have a way to detect whether a hand is living or not, the system can be fooled by a fake hand if pressure is applied to the plate correctly [2].

Biometrics can be the future to security for this country. It has many different applications and can be used in a lot of different situations. One of the key advantages of biometrics is that they cannot be forgotten like a password because you are born with these features and you use them everyday. If companies start using biometrics more often to secure

their information, the rest of America might follow because the government has been using this form of security for years and it will only be a matter of time before the general public adapts to this form of security [5].

Forensics

Whenever there are two objects that meet, there is always an exchange that occurs from something large like a gift to something as small as skin cells. For instance at a crime scene there is always evidence that is left behind by the suspect when he/she leaves the scene that can direct police and officials back to him or her. The evidence that is left behind is called forensic evidence and it is collected by forensic investigators. The amount and types of evidence that can be collected from a suspect at a crime scene can sometimes be surprising and numerous. This type of evidence includes fingerprints, blood, semen, skin, hair, fingernails, foot prints, voice recording, oils, and other fluids. These are all characteristics that are individual to each person and cannot easily be duplicated, and therefore can be used as forms of identification. Several of these characteristics, or in some cases just one, can catch a suspect involved in a crime.

Fingerprints are unique to every person, so when they are found at a crime scene they can be a good indicator of who committed the crime. However, being able to find fingerprints at a crime scene can be hard if the scene is cluttered with stuff, the scene is a large area, or the crime was committed elsewhere. Sometimes fingerprints can be seen, called visible prints, and sometimes they cannot be seen, called latent prints, that can be hard to find [4]. Sometimes the best way to find fingerprints is to think like a criminal and put yourself in the suspect's position to try and find out where they would put there hands. If that is successful

and you find some latent prints, you can lift them by using talcum powder or black powder (not explosive, this just describes the color), tape, and white or black paper. Once the fingerprints are lifted, or found, and processed they can then be entered into IAFIS to see if they get a positive match on a suspect. If the system doesn't come up with a positive match, then you might have to get more evidence to catch the suspect.

When fingerprints are not enough, then DNA might be used to help further the process of catching the suspect. There are different types of DNA samples that can be collected at a crime scene: blood, semen, hair, and skin. Blood found at a crime scene that doesn't belong, or is in an awkward spot, can lead officials in making an arrest. Every person gets there DNA submitted on record when they have blood taken. Sometimes blood, like latent fingerprints, cannot be seen, so investigators have to find it and make sure that it is blood. Blood may not be visible when someone tries to clean it up from a crime scene with a cleaning solution or solvent. When this occurs, you spray Phenolphalien on the suspected area and if blood is present it turns a fluorescent color. Blood can definitely identify a person and place them at the scene of the crime or at the time of the crime. Of course, if blood is not present, then other evidence has to be used.

Hair is a good piece of evidence at a crime scene that can be used to catch a suspect. Hair falls from a person's body all the time without them knowing it. If there is a struggle involved at a crime scene, then more then likely a hair or hairs will be present. If you have a hair fiber that still has the follicle attached, then you can pull DNA from it to find the suspect immediately. If there is no follicle attached, then you will have to compare it to either known samples you have taken in the past or to samples requested from a possible suspect [6].

Footprints are also valuable because they can give you the physical characteristics of a person: running or walking, direction from which they came in, or where they came from or have been. Shoe prints are important because, like fingerprints, shoeprints have unique wear and tear on them that is special on each shoe. If you find shoeprints at a crime scene then you can tell by the size of the shoe how tall someone was and by the depth of the impression the weight of the person. If you have a suspect then you can ask to see the bottom of his/her shoe to see if it matches the impression found at the crime scene. Also, every person walking on the ground picks up material after each step. If you find certain materials such as sand, dirt, paint, or certain types of liquids, you can tell where the suspect was or came from to help narrow your search.

Voice recording can be useful at a crime scene. If you are able to get a voice recording of a suspect planning a crime or committing the crime in question, then you can use this to get a match on a suspect. The instrument that investigators use to analysis voice recordings is called a spectrograph. Spectrographic examinations compare an unknown recorded voice sample to a known voice exemplar produced on a similar transmission and recording device, such as the telephone. However, because decisions regarding spectrographic voice comparisons are not conclusive the results of voice comparisons are provided only for investigative guidance [6].

Finally, there may be semen stains. Usually you don't find semen at a crime scene unless you are investigating a possible sexual assault or a sex crime such as rape, sex assault, or even a staking or peeping tom case. Semen contains DNA from the person that produced it and it can be used just like blood and fingerprints to convict a person. Semen can also be like fingerprints in the way that that they can be latent and not visible. When this occurs, you have

to perform an Acid Phosphatase test. Acid phosphatase is an enzyme secreted by the prostate gland that is present in large amounts in seminal fluid. It, like psa (prostatic specific antigen), is not unique to the prostate and can be found in other biological fluids, including vaginal secretions [10]. It is therefore considered a presumptive chemical test for the presence of semen, and semen must be confirmed by other means, such as sperm detection or psa detection using membrane test systems. Testing for the presence of acid phosphatase can be extremely helpful, however, in locating semen stains on clothing and for testing swabs from sexual assault cases. A strong positive reaction generally indicates that semen is present and that further testing is warranted [13].

Biometrics in Forensics

There have been many criminal cases that involve the use of biometrics. These cases may not have been solved solely based on biometric evidence but biometrics was able to profile, identify, or point authorities in the right direction. One case that used biometrics was the Ted Bundy case. Ted Bundy was a killer who stalked and killed at least 36 women on college campuses. Psychiatrists diagnosed him as having a personality disorder. Graphology was used to determine whether or not Ted Bundy showed any signs of being a serial killer. Graphology is the study of handwriting especially for the purpose of character analysis [8].

Two separate writing samples were taken from Ted Bundy in order to analyze his handwriting. His handwriting was rounded, which indicates a person who is graceful with imagination. Bundy also writes with certain lightness, indicating an ill-adjusted personality. His capital "A's" with a perfect oval and small letter "N" in place of a capital, signifies clarity of thought and simplicity. Bundy's "C's" are written indicating his sense of beauty, clarity,

and poetry. His capital "D" shows Bundy as having originality, and the great degree of swelling of this letter indicates his vanity. However, his small "d" linked to the next letter by a gracious curve shows that Bundy has a logical sequence of ideas. The written letter "H" indicates that Bundy has a sense of grandeur, strength, and liveliness. Ted writes his small letter "T's" in place of a capital one and heavily crossed shows a person with strong will power who is also domineering. A sample of Ted Bundy's handwriting is in the Appendix.

Ted Bundy's handwriting shows that he is an intelligent individual, with a slight personality disorder. He is a strong and domineering person, which was confirmed by his ex-girlfriend. Graphology does shed some light on what the psychiatrist said Bundy's personality was like [11].

Another example of biometrics helping in solving a case or further the process is a case of a murder that occurred in 1977. On June 3rd, 2000, in San Francisco, California, a previously convicted child molester was arrested after investigators matched his DNA with a semen sample found on a victim's shirt and sock. In 1977, a young girl, Lisa Marie Bonham, was kidnapped and killed in Reno, Nevada. The day after she was kidnapped, her clothing, stained with semen, was found in a garbage can. At the time, the findings had little value for forensic investigators, who could only use DNA technology to eliminate possible suspects. The technology at the time could not identify the perpetrator. However, as the years progressed, advances in DNA and computer technology were made. So in 1993, the police of the area took the semen sample and began checking them against a list of possible suspects, then against known sex offenders in Nevada, Northern California, and the Pacific Northwest. But no progress was made until the last week in May, when a direct match was found, linking Stephen Robert Smith to the little girl's disappearance. Smith had cooperated with his parole

officer by giving a DNA sample to the database. Smith had sexually assaulted the child before killing her, police said, and was sentenced to life in prison [9].

With biometrics gaining popularity, it is likely to be used more widely is the nation, and some think that it can help with the problem of national security. According to U.S. Senator Dianne Feinstein (D-CA), "Many experts believe that if we had been using biometrics for visa applicants and visa holders and at customs, baggage and passenger checkpoints at airports, we could have potentially forestalled the September 11 attack." With this in mind, government and aviation officials are considering various proposals that will improve airport security. Several programs are currently being installed and tested in airports throughout the United States [8]. There is a concern that as September 11th 2001 starts to become a distance memory all the security measures will begin to do the same. The concern for that is valid but law enforcement agencies have to consistently evolve with the new threats against the public, so even if the general public starts to slow down when it comes to implementing new biometrics technology law enforcement agencies have to try and stay one step ahead at all times.

References

1. Agaron L, "Show me some ID - Biometrics is leaving its fingerprints on the market with low-cost devices," PC Week, December 1998.
2. Biometrics and the Courts, "Hand Geometry," 2005, http://ctl.ncsc.dni.us/biomet%20web/BMHand.html, accessed June 2005.
3. CNet, "The Latest in Anti-Piracy Efforts: Keystroke Recognition," 2000, http://news.com.com/2100-1023-241792.html?legacy=cnet, accessed June 2005.
4. Coppock, C. (2001). Contrast: A Guide to Fingerprint Identification Concepts. Springfield: Charles C. Thomas.
5. Davies S. (1994) "Forget the passport, let's see your hand," The Independent, London, August 1994.
6. FBI, U.S. Department of Justice, "Handbook of Forensic Services," 2003, http://www.fbi.gov/hq/lab/handbook/forensics.pdf, accessed June 2005.
7. FBI, "Integrated Automated Fingerprint Identification System or IAFIS," 2005, http://www.fbi.gov/hq/cjisd/iafis.htm, accessed June 2005.
8. Forensic Biology, "Hair Evidence," 2005, http://www.bxscience.edu/publications/forensics/articles/hairandfiber/h-hair01.htm, accessed June 2005.
9. Forensic-Evidence.com, "In the New Millennium," 2005, http://www.forensic-evidence.com, accessed June 2005.
10. Gaensslen, R.E., Sourcebook in Forensic Serology, Immunology, and Biochemistry, Research Foundation of the City University of New York, 1983.
11. Law-Forensic.com, 2005, http://www.law-forensic.com, accessed June 2005.
12. Merriam-Webster Online, http://www.webster.com, accessed June 2005.
13. Midwestern Association of Forensic Scientist, "Forensic Detection of Semen," 2005, http://mafs.net/pdf/laux1.pdf, accessed June 2005.

Appendix – Ted Bundy Document

Ted Bundy
Florida State Prison
Box 747
Starke, Florida 32091

P.O. Box
San Rafael, California 94913

February 23, 1988

Dear

Thank you for your letter of January 25, 1988, and for the documents you enclosed with it. I also received in a separate mailing your "Cobb-Clark Case Synopsis."

There must be some need to send me the other material I requested in my last letter. I appreciate your willingness to send it, but I think I have enough information to form an opinion concerning your allegations about Carol Bundy and the Ulster book.

What I intend to address in this letter are two topics: Cobb's correspondence with me and the contention that she patterned the recent Trivis murders upon information contained in a book by Peter Ulster about Ted Bundy. As I understand it, you are interested in the letters Cobb wrote me because they may bolster the Ulster book connection in some way.

The Ivan G. Seidenberg
School of Computer Science and Information Systems
Pace University

Technical Report Series

EDITORIAL BOARD

Editor:
Allen Stix, Computer Science, Pace--Westchester

Associate Editors:
Constance A. Knapp, Information Systems, Pace--Westchester
Susan M. Merritt, Dean, CSIS--Pace

Members:
Howard S. Blum, Computer Science, Pace--New York
Mary F. Courtney, Computer Science, Pace--Westchester
Nicholas J. DeLillo, Mathematics and Computer Science, Manhattan College
Fred Grossman, Information Systems; Doctor of Professional Studies, Pace--New York and White Plains
Fran Goertzel Gustavson, Information Systems, Pace--Westchester
Joseph F. Malerba, Computer Science, Pace--Westchester
John S. Mallozzi, Computer Information Sciences, Iona College
John C. Molluzzo, Information Systems, Pace--New York
Pauline Mosley, Technology Systems, Pace--New York
Narayan S. Murthy, Computer Science, Pace--New York
Catherine Ricardo, Computer Information Sciences, Iona College
Judith E. Sullivan, CSIS Alumna, MS in CS from Pace--Westchester
Sylvester Tuohy, Computer Science, Pace--Westchester

The School of Computer Science and Information Systems, through the Technical Report Series, provides members of the community an opportunity to disseminate the results of their research by publishing monographs, working papers, and tutorials. *Technical Reports* is a place where scholarly striving is respected.

All preprints and recent reprints are requested and accepted. New manuscripts are read by two members of the editorial board; the editor decides upon publication. Authors, please note that production is Xerographic from your submission. Statements of policy and mission may be found in issues #29 (April 1990) and #34 (September 1990).

Please direct submissions as well as requests for single copies to:

Allen Stix
The Ivan G. Seidenberg School of Computer Science and Information Systems
Goldstein Academic Center
Pace University
861 Bedford Road
Pleasantville, NY 10570-2799