Iris Image Biometric Technology for Identification #

#

Simren Ajrawat
IT 103, Section 011-Sanghera
George Mason University
October 4, 2013

Introduction

Imagine walking through an airport for screening before you board a flight. You are told to look at a camera lens that snaps an image of the unique structures of your eye's iris. This infrared image is scanned and then read by a system that then studies the patterns of the iris of your eye to get it recorded as a graphic. The patterns are studied, mathematical and statistical algorithms are run and a template is created. This result is then matched with databases of iris image templates searched by matching engines. Within the speed of 2 seconds the system cites your name, address, license and criminal record. The result, an identification of who you are is made. The Transportation Security Administration (TSA) system gives the airport security a prescreen of you and then a decision can be made to see if you need additional screening, need to be placed on the "No Fly Watch List" or if you are clear to get on board. This innovation is Iris Image Biometrics and is the future of our airline security for identification.

Biometrics is an emerging technology where the science of measuring physical or anatomical characteristics is mixed with technology to create identification systems (Corby et al., 2006). This new innovation of biometrics may be used soon by the United States Transportation Security Administration (TSA, 2013). This technology uses a database system connected to an Iris imaging system of the human eye. Iris recognition systems are currently being researched by the TSA for use because it is an identifier that is "unique to every person offering an alternative secure approach in validating who someone is" (TSA, 2013). The iris is stated to provide an ideal means of biometric identification for several important reasons. The iris is the perfect identifier because "it's randomly formed textural variation is unique to each individual, and it remains unchanged throughout life with 170 discriminators" (Webb, 1997). The iris is an organ that cannot be analyzed by the bare human eye so it becomes an excellent identification organ. Iris

image biometrics is an amazing new technology that will be used by airports around the country in the near future. The purpose of this paper is to showcase the advent of this new technology and its great benefits to the TSA, but also present the legal, ethical, social and security issues that arise from this innovation and its use.

Background

Iris image identification systems are being studied at a fast pace for use in the airline industry. This is not the only industry that can benefit, as other users of pin cards and passwords can also apply this technology. Iris image identification however links the image technology software to systems that house large amounts of data on the general population so identification can be made and validated.

A Cambridge University professor, John Daugman, began to develop iris identification software using math/algorithms in 1991. Daugman's patented software and algorithms used a "circular grid as a guide to select data from the iris image" (Webb, 1997). The algorithm is run, "selecting data points on the circular pattern at various angles..from the illuminating light source" (Webb, 1997). The optical fingerprint with a unique, detailed pattern, is then analyzed by algorithms and mathematical formulas; then each bit is given an abstract 256 byte digital code to store it as bar code (U.S. Patent Office, 2001). The software does a match search to millions of records to identify the person. Eye tracking technology currently "uses infrared light and cameras" (University of Wisconsin, 2013). Iris scans are then matched against law enforcement databases, intelligence terrorist databases, and criminal warrant databases.

Daugman further stated that "other systems first ask for a name and then this name is used in the system to help identify a person, whereas with this new technology the system tells you your name and identifies you, just by your eyes" (Essick, 1998). Future development of iris

recognition systems will now be linked into massive database systems of intelligence that allow prescreening and identification within seconds at airports. This new innovative technology has components that involve a camera that is sensitive to movement, a scanned image, mathematical formulas, algorithms, programming, links to search engines of thousands of data, and interpretation programs that are matched to produce a result. The result also has to be timely, quick and accurate.

Potential Benefits

The Transportation Security Administration states that "it exists to strengthen the security of the airlines in the United States for passengers" (TSA, 2013). As the threats to aviation become more sophisticated and advanced, TSA must also be on top of innovation and is a key user of information technology in screening passengers on the United States airlines. The disturbing memory of September 11, 2001 and the close scares of passengers boarding planes with bombs and dangerous devices, push the TSA to make passengers safe as "the most important concern for this government agency" (TSA, 2013). Information technology and new innovations like biometrics help the TSA to ensure safety of domestic and international air travel where identification and history of a person are available in seconds.

Intelligence information received from the systems at TSA must be accurate, updated around the clock, and real time. Use of biometric iris image identification has great benefits and allows the TSA to use these results to decide which flights need greater security of Federal Air Marshalls. Federal Air Marshalls are undercover officers placed with passengers on flights to protect travelers (TSA, 2013) . Information from this system can identify threats of danger and the need to send canine dogs at the airports (TSA, 2013). Intelligence information can also be used to allocate appropriate staffing of security officers at checkpoints, or see if changes to their

business are needed. Intelligence information serves most of all to help decide which passengers need to be identified on the "No Fly list" and be restricted from boarding a flight. The benefit of this information technology is immense and critical in protecting the security of passengers and the transportation system. Benefits are also to passengers who will feel greater safety using the airlines.

Finally, another benefit of iris image biometrics is that it offers greater advantages over "fingerprints which can dry or fade or smear" (Brown, July 2013) when being taken. The results therefore can be "inconclusive in identification but if it's used together with the iris image, there is greater accuracy" (Brown, July 2013).

Legal and Ethical and Social Issues

Use of intelligence raises invasion of privacy concerns of by consumers (Uppena & Finley, 2004). TSA staff is reviewing the information of the public and by having access to information there is a chance that this information can be abused, misused and maybe even compromised. This technology links to enormous amounts of information and intelligence on each person, so there is fear over who has access and who is looking at this information. To give a gauge, the FBI fingerprint system contained more than 40 million fingerprints (Scanlon, 2003). A second concern is data protection which is also a legal concern if data is lost or stolen. A third concern is the ethical challenge of holding so much information, on each person, with access from a single system. A fear is that other workers have access to information of so many people or if information can get in the wrong hands. People are fearful that this is too much invasion where the technology can be used to track their every-day lives (Bodor, 2001).

A fourth concern is an inaccurate result and thus embarrassment. A small glitch can cause embarrassment of possibly an innocent traveler who is either sent for additional screening

or posted on the "No Fly" list. This can also have legal implications of being falsely making someone misses their flight thus raising some liability issues for the TSA.

A sixth concern is that the iris could change with the aging process. This means the data must be updated. The National Institute of Standards and Technology states that there is no consistent change in the texture of irises for at least a decade (Brown, August 2013). Another concern, to gain social acceptance is "how humans interact with biometric devices is critically important for their future success…it must be efficient, accurate..and something that people trust, accept and don't get frustrated with" (University of Wisconsin, 2013). Finally, airport screening has overwhelmed travelers with fear of more delays with iris scanning (Uppena & Finley, 2004).

Security Concerns

There is a constant mix of security concerns for this technology related to data protection, protecting data from hackers/data theft, identify theft, data storage, integration with current systems, and the risks associated with trying to keep the data updated, speed, and scalability. Information is continually being attacked and challenged by hackers trying to access intelligence data around the world every second. Data protection, hackers, and data theft are concerns for once the iris image is saved as bar codes and is downloaded; also when match results are made. With this is also the security concern for identify theft. This system must be more than a camera and must sense eye movement and blinking, and further discriminate imposters or non-living things (U.S. Patent Office, 1991). This is to prevent a person from wearing a static lens in the image of another person much like contacts or eye lenses. Some measures need to be added to this technology to capture lenses or blinking so that a static fake image is recognized.

Another security concern is data storage for this large amount of data. Data storage features are being looked at where, when stored, the data and image are manipulated and then

reversed back when needed. Intentionally distorting the data is needed for better security. Finally integration ability and data update is needed to make this system successful. There are already systems in place at airports so this software has to have the ability to integrate with existing systems. Further, this technology must link to large sets of data from databases containing lots of information for every traveler in the country. To be successful this technology needs constant 24/7 updates, real time information is needed, with speed to prevent waits and scalability to allow the software to roll out millions of identities (Uppena & Finley, 2004). Veltek, a biometric developing company COO stated, "For biometrics to have a future, it needs to be non-intrusive" (Boder, 2001).

Conclusion

Biometric iris identification technology is in its infant stages for use by agencies like TSA but will be wide spread in just a few years. This type of technology brings a vast array of concerns ranging from legal issues, ethical issues, and security issues. There needs to be continual technological improvement in monitoring our airlines and ensuring passengers are safe with sound methods of identification systems. Terrorists and hackers alike will continue to try to damage our people and our systems. However, our technology will hopefully advance at even a faster pace. What we once saw in the old science fiction movies or James Bond movies is now almost a reality. With a blink of an eye and in seconds we can open doors, gain access and identify people. "We shouldn't risk hundreds of lives if an iris scan can identify a threat" (Hockersmith, 2013). Iris Biometric Technology is here and upon us so let's embrace this amazing innovation to protect us and our air travel but yet also prepare to make it accurate, timely, integrated, secure, non-intrusive and socially accepted by our populations.

ANNOTATED BIBLIOGRAPHY

1. Transportation Security Administration, Department of Homeland Security. (2013). *TSA: Security*. Retrieved on September 20, 2013 from http://www.tsa.gov/about-tsa/security-technologies#bio & http://www.tsa.gov/about-tsa/911-and-tsa

   This resource is a governmental organizational website for the Department of Homeland Security for the Transportation Security Administration. This site discusses technology used for passenger screening and baggage screening. Of interest is the discussion on the future use of biometric technology and retinal scans for identification. The TSA speaks of its mission and goals in keeping passengers safe. This is a reliable website from the Federal Department of Homeland Security who created TSA.

2. Brown, Evelyn. (2013, August 20). Study advances iris images as a long-term form of identification. *National Institute of Standards and Technology (NIST).* Retrieved on September 20, 2013 from http://www.nist.gov/itl/iad/iris-082013.cfm

   This resource article is from a governmental organizational website, the National Institute of Standards and Technology (NIST), an agency of the U.S. Department of Commerce. This agency publishes various articles on technological advances. This article is of particular importance for the study on the long term aging effect on an iris. This article cites a study and discusses the study itself, and results. Results show that there is little change to the iris for at least a decade. This is important because as technology databases are created, keeping information updated is critical. This is a reliable website as it belongs to the Federal Government. Only well documented and researched items are published.

3. Brown, Evelyn. (2013, July 12). Who are you- NIST Biometric Publication Provides Two New Ways to tell you Quickly. *National Institute of Standards and Technology (NIST).* Retrieved on September 21, 2013 from http://www.nist.gov/itl/iad/iris-071213.cfm

This resource article is from a governmental organizational website, the National Institute of Standards and Technology (NIST), an agency of the U.S. Department of Commerce. This agency publishes various articles on technological advances. This article is of particular importance for because it discusses how iris identification is a solution in lieu of smart cards, fingerprinting, PIN numbers and access codes. Of importance is the discussion on how iris identification is a better option than other methods. This is a reliable website as it belongs to the Federal Government. Only well documented and researched items are published.

4. University of Washington. (2013, July 13). Eye Tracking Could Outshine Passwords if Made User Friendly. *Science Daily*, 1-2. Retrieved September 26, 2013 from http://www.sciencedaily.com/releases/2013/07/130716132232

This is a scientific magazine resource that discusses advancements in the field of technology and science. Of particular importance is the discussion in this article about replacing passwords with biometric authentication. It speaks to the social factor on how in order for this technology to be successful, it cannot frustrate people. It suggests that in order for any technology to be successful it must have constant interface with the subjects that technology is being created for. This is a reliable scientific magazine and is a leader in ensuring reliable content and publications.

5. Scanlon, Lisa. (2003, June). Finger printing's Finger-pointing past. *MIT Technology Review*, 106, 80. Retrieved on September 27, 2013 from http://search.proquest.com/docview/195356154? accountid=14541

This is a scholarly magazine by MIT that tells of the latest advances in the technology industry. This article shows the importance of iris scanning and tells some history of the patent and software. This review discusses the history of fingerprints and forensic science and how these tools are critical in identification. This is a reliable scholarly publication from a well respected institution MIT.

6. Uppena, D., & Finley, L. (2004, Jun 29) Registered Traveler Program. *University of Wisconsin*, Retrieved on September 23, 2013 from http://www.uwosh.edu/faculty_staff/wresch/FPRegistered Traveler.htm

This is an educational institution's discussion on the use of iris technology by the TSA. It is of particular importance because it states that cost, labor, volume, terrorists, privacy, reliability and affordability are all concerns that need to be addressed. It speaks to funding constraints of the airline industry and how this impact emerging technology. This is a reliable publication from an educational university of the United States.

7. US Patent Office, Patent 5291560 A. (1991) Biometric personal identification system based on iris analysis. Retrieved on September 22, 2013 from http://patft.uspto.gov/netacgi/nphParser?Sect2=PTO1&Sect2=HITOFF&p=1&u=/netahtml/PTO/search-bool.html&r=1&f=G&l=50&d=PALL&RefSrch=yes&Query=PN/5291560

This resource is the patent from the U.S Patent Office for the written documents submitted for an iris identification patent. It describes the technology and claim of what it can do

giving also a background of the invention and functionality. This is a reliable source because it summarizes patents accepted by the Federal Government.

8. Essick, Kristi. (1998). Iris ID squares off against fingerprint and handprints. *InfoWorld*, 20 (26), 88. Retrieved on September 22, 2013 from http://search.proquest.com/docview/194328682? accountid=14541

   This resource is a technology magazine that writes on articles for information technology. The importance of this article is the history on iris recognition systems and how this technology works. IT also gives insight into how the software has to match records to conduct an identify match. This is a reliable magazine that is used by the industry to showcase new technology innovations.

9. Webb, Warren. (1997). High-tech security: The eyes have it. EDN, 42(26), 75-78. Retrieved on September 22, 2013 from http://search.proquest.com/docview/222393142? accountid=14541

   This source is an online publication that goes back to 1997 however it offers great insight into the same technology basics that are part of iris identification systems today. It states how many discriminators and eye has and speaks to how this technology differs from fingerprinting. This is useful in my paper because I am trying to understand exactly how this technology works and what the system has to do to capture the eye image. This is a reliable source from the research database of documentation history on this subject matter.

10. Corby, P. M., Schleyer, T. Spallek, H., Hart, T. C., & et al. (2006). Using biometrics for participant identification in a research study: A case report. *Journal of the American Medical Informatics Association, 13*(2), 233-5. Retrieved on September 27, 2013 from http://search.proquest.com/docview/220822552?accountid=14541

This is a scholarly journal publication which studies iris biometrics. It shows the use of biometrics on subjects with a case study on twins as a subject in helping with identification. It validates that this technology is very useful in helping with identification of individuals. This is a scholarly journal accepted and reliable for the cases that it presents with sound research.

11. Bodor, J. (2001, May 06). Sensing identity biometrics makes security a physical thing. *Telegram & Gazette*. Retrieved on September 27, 2013 from http://search.proquest.com/docview/268801104? accountid=14541

This is a newspaper article that helps point to the ethics nature of biometrics applications and gives a public perception. The article points to the potential intrusive nature of this technology and how it must be handled. It also cites NASA as a user of this and explains the technology in actual use. This is a reliable well known paper and source.

12. Hockersmith, Robert. (2013, September). Personal Communication Interview

This source is a personal communication interview of a Senior Developer/Programmer of databases at Fairfax County Government. This interview was important for me to try to understand the technology aspects of security, protecting data, saving data and risks from hackers. This is a reliable source from a high level individual working in a local government environment.