Implications of Bio-metric Identification in Healthcare

Noah Holt
University of Colorado, Colorado Springs
Email: nholt@uccs.edu

Abstract—**As computer and account hacking have become easier with the growth of root kits allowing more people to participate in such activities, so has the need for better security. One of the growing and most secure options to increase this security is the field of bio-metric identification. In this paper, what is bio-metric identification, how it can be used and improved, and what are some possible downfalls are what will be discussed.**

1. Introduction

The field I worked in before choosing to become a Computer Science student was medicine, both people and animal. While in this field, there were many good and bad things witnessed, but one of the things that seemed the biggest issue was patient identification. This was for various reasons such as uncooperative patients, patients that did not know who they were, or people trying to hide their identities thinking that we would call the cops.

Once I heard that there was research being done into alternatives such as bio-metric identification, it was interesting to say the least. My parents had just gotten back from a cruise and had reported that when coming back through customs they did not even need to show their passports as the local surveillance had already identified them and so the customs agents just waved them through. This showed that this technology could be trusted by the government to pass people through customs and showed its accuracy in identifying individuals despite them not knowing they were being subjected. In medical words, it was non-invasive.

This prompted further investigation into how bio-metric technologies were being used in medical settings. As a past emergency worker, it also raised some read flags as to how such technologies might work for patients who could be bleeding, swollen or injury and how such states of being may be taken into account.

The articles studied on the subject did not delve into the latter concern but show what bio-metric identification is, applications it can have, and some other areas of concern to consider.

2. Source Summaries

The papers chosen had many similarities and repetition that will be summarized here to avoid the same repetition within. Most began with an explanation of what bio-metric identification is. The consensus on the definition was generally a break down of the word into Latin roots (bio meaning life, metric or metrik meaning to measure) [1], and then broke bio-metrics down to 5-7 areas. Universality, so the trait to be measured must be shared by everyone so everyone could be measured [1]. Uniqueness, not only does everyone need it, but it must be unique to individuals [1]. Permanence implied that the trait or characteristic should not vary over time [1]. Reliability in the ability to measure it from a person [5]. Accuracy in the ability to identify an individual with the data collected [5]. Lastly, acceptability, in terms of how it is collected being easy and socially acceptable [5].

2.1. Mason's Investigation

Early on, Mason brought to light the case of John and Jane Doe and how when unable to obtain identification from patients, many go through the system under these aliases until identification can be obtained [1]. In these situations, it can be difficult for medical providers to assist patients in the case of pre-existing conditions due to this lack of information on the patient. Several cases even up with patients in worse states due to medications they should not have or allergies medical staff was unaware the patient had. Mason uses this type of situation as a basis for their argument for periocular (the region around and including the eyes) bio-metric identification [1]. Also pointing out the fact that with this type of scan being widely used in smart phones and tablets, that the technology is ready for other uses.

This article then dives deeply into how such a system should work. Mason breaks how the need for ”a template within the database” for collecting and comparing data [1]. The article gives a step by step walk through of a proposed plan of implementation. Key notes of take away being the collection process for know users, the need of large scale storage, and the process of comparison of which Mason recommends a values approach [1]. This values approach breaks down the different features into values per field or area and compares to the values in the system. The proposal of incorporating a deep learning engine to train and assist in identifying individuals was another possibility [1].

Some of the issues discussed is the connection to the current health care systems that use a master patient index (MPI) which is a number assigned to individuals and can track them with name and SSN to connect different visits to differnet doctors [1]. The issue of access to different providers was another factor mentioned [1]. With doctor's offices of rural communities or poor urban areas not able to afford some technologies, adding another high expense item to requirements of medical professionals could cause these offices financial issues.

2.2. Illusion of Choice

This dissertation began a discussion on currently connected surveillance systems that use bio-metrics and different viewpoints from nurses asked during the study. Baneville was also the only author to mention (though at a glance) some of the exclusions different groups face when dealing with bio-metrics [2]. For a long time, darker people were excluded from smart phone recognition due to biases in the testing of the systems. Other information on the topic will be mentioned in 2.8 Other Thoughts.

From the nurse's perspectives, the group in the study were aware of bio-metrics and were brought together to discus facial recognition [2]. These nurses believed that such technologies could be used but said that the technology was, "not necessarily used in day-to-day" [2]. With a seeming lack of public knowledge in the area may pose questions as to how these nurses were informed on the topic or how aware they were of the capabilities the technologies are seeing in areas like the customs story in the introduction.

Compliance was once again brought up to be an issue for when such technologies would be brought into healthcare with different patient rights and advocacy. The nurses thought that the technology "creates a sense of illusion that because the technology is assisting in healthcare facility, if the patients do not comply," then what is the point [2]. This issue would seem to be a healthcare specific issue due to the uses that different governments are using it without consent scanning high volumes of people hourly. In terms for healthcare, this raises questions as to how different HIPAA laws may need to be created for patient protection or the different types of information that can be accessed through bio-metric scans.

Data collection and storage was once again mentioned by this author as well as a legitimate concern. In this dissertation, the author did not purpose a central storage as Mason did, but instead simply raised the questions, "what data is collected, where is it stored, third party access" [2]? The first two of these questions would be for the business aspect, and to the point of where, the issue of data backups would need to be addressed with HIPAA outlining how long data needs to be held onto before it can be deleted. The third party access raises security concerns with more attack points introduced, and especially with data collection and regulation being an issue in the U.S., how would this data be protected from others.

2.3. Management Framework

The issue of third party access became more of an issue when analysis of the third article began. To start the article, Farid states that "access for dispersed clinical information," from IBM (I company who has sold healthcare data in the past) and Aetna (a health insurance company with 1.3 rating on google) [3]. Bringing up two companies like this in a paper discussing storage and access to healthcare information raised a red flag.

This article moved into bio-metrics as ECG and PPG scans that measure heart rate and volume and use your average to identify you. To begin, these types of metrics are variable and not necessarily unique and so how they could be used to identify individuals seems off. Though the authors bring up the point that these metrics are used by different fitness trackers and like devices (smartwatches mentioned in 3.1) [3]. The other point made for these metrics is how they can be used in remote health situations [3], though the point of cost savings and availability to many is not mentioned, it is another area to consider as well.

Something some of the other articles left out was the nature of bio-metric data. "Biometric information is considered confidential by nature" and so must be encrypted and therefore should limit the risk of data leakage [3]. This information was interesting as nothing in my research had brought in legislation like this. Encryption of data this large and needing to be access frequently, as a patient identity is could lead to much slow down during treatments. A process like this would now include a process of collecting data, comparing to templates as Mason discussed [1], and then decrypting to find a match.

2.4. Effective Biometrics

Slow downs in hospital and avoiding them can lead to serious consequences. Buhagiar begins their article with the statistic that "2.6 million people die each year [...] due to medical errors, including patient identification" [4]. The issues associated with these errors include, registration errors and time pressure [4]. These errors (especially time pressure) occur often so increasing time it takes to identify a patient (which needs to happen each separate interaction).

The current method of identification in most hospitals is wristband and DOB (date of birth) system where someone scans a barcode on a wristband and asks to confirm the DOB. This system has several flaws including people swapping wristbands and the fact that the DOB is printed on them. This system did increase correct identification of patients by 12-57% around the world [4].

Some concerns expressed by patients in this study were privacy and confidentiality leading to many patient refusing the use of bio-metric technologies [4]. The authors bring up the point that "safeguards must be set down for every step, from collection to retention of the data collected" yet gives no solution to the problem [4]. Most governments have security measures for databases such as this in place for confidential and classified data so it is possible. Having security measures like that on a large database with any number of random people who just need to make a single trip to the doctor to gain access is concerning. Once again we see a system with many points of access to confidential and private information open to the public.

2.5. Security and Privacy Concerns

Singh's article tries to address these security concerns. Singh declared that encryption for bio-metrics is weak [5]. The reason this is bad was the statement previously mentioned about time of access. Though not giving fixes on how to change the encryption method for the better, Singh relied on the fact that computers are increasing in capabilities daily and that ”this will help in finding the solution in very less time and calculations” [5]. Though this is true, the sit around and wait method is not typically good practice. An approach, even if only theoretical, would have been better.

The article then moves to advantages and disadvantages of using different bio-metric systems. Firstly mentioned was the sensitivity some of the scanners have and that a, ”few foreign particles like dust or moisture” could effect the scans [5]. This sensitivity brought the sliding scale of acceptability and false positives discussed in class to view and how allowances for foreign particles may allow for more incorrect matches. Another point was the ”increasing importance around the globe” of bio-metric systems for security in all fields [5]. With these two facts together, rapid improvements should be expected in the future.

2.6. Multimodal Authentication

The next topic was personal devices and their use in ECG and PPG [6]. The authors stated how deep learning models could be used to help in the efficiency of identifying individuals based on the bio-metric data collected [6]. AI and deep learning could be used to find patterns in the data and help quickly identify matches based on experience. The problem with that is if the data is stored encrypted then finding a match would still prove difficult. Thinking on HIPAA requirements, data only needs to be encrypted during transferring and does not need to be stored encrypted. No clear guidelines on bio-metric data, but if it ends up in a similar circumstance for encryption than the models could be inside as well.

This article also looked into different types of computer attacks and anaylized how each may effect the systems. Spoofing attacks were talked about first and brought to light how many such devices that already exist only check the identity at the beginning of the session and so if an attacker connects in the middle or end then they could have access. Injection attacks were another point. The authors mentioned how ”networks that adopt the proposed authentication approach [need to] also secure from an injection attack” [6]. So the hardening of the system and adjoining components as a whole is a requirement purposed. Attacks at the registration phase were also a concern of this author and another. The claim that, ”imposter can register a rough device into the network during registration” was mentioned and the solution to problems like this that we currently have in place is multi-factor authentication [6].

The authors for this took the time to explain how they did not go into other types of attacks such as DDoS attacks, side-channel attacks, or man in the middle attacks and so left room for future work to be developed. Though in this experiment conducted they did see high authentication and accuracy rates.

2.7. Bio-Ethics

A form of bio-metric data not mentioned by others was DNA analysis [7]. Much is still to be improved with DNA testing, but that which used to take years to examin is now able to be done in a matter of months. Testing and examination of DNA is an ever large field and is perfectly unique to a large majority of individuals with only identical twins sometimes (not always) having matching DNA.

This article also bring the topic back to healthcare and ethical implications that gathering and storing bio-metric data on patients may have. The need of “ensuring that personal health records are appropriately protected from unauthorized use and patient confidentiality s maintained” was a focus and large concern of the author [7]. During their experiment they also saw “confusion amongst some patients [. . .] about why they were supposed to have their fingerprints scanned” [7]. The patient of the Malawi community studied had perceived the scanning as a way for illiterate people in the community to receive care. This brought the point to how bio-metric scanning could help get more access to patients around the world who may be impaired or illiterate and so can now still give their identity.

Due to the limited knowledge of bio-metrics frm patients and staff alike, there seemed an disconnect in the study. The author also pointed to the power dynamic between patient and doctor to be a factor in the lack of questions [7]. In this community, there was also a concern as to what kinds of information was readily available to the staff upon obtaining their data [7]. In Malawi, patients are given healthcare passports and certain diseases such as HIV are prominent causing stigmas against the patients from the doctors [7]. These patients were expressing concern that only pertinent information could be accessed by personnel to keep unwanted or sensitive information private.

The author ends with the statement, “biometric identification would be welcomed and considered ethically appropriate, if undertaken in a manner that ensured that the benefits of implementation for patients outweighed potential harms” [7]. This statement of the importance of patient benefit anchored down how the difference of implementing bio-metric in the healthcare system would need to change or adjust to compared to what it is now to accommodate for the stricter circumstances.

2.8. Biometric Survey

Finishing on the strongest security oriented of the articles. The quote, ”To achieve robustness, high accuracy rates and difficult to spoof are the main factors that generally distinguish from the traditional methods for the security,” helps to emphasize the differences the last author brought up. Something unique to this article was the different types of bio-metric data as well. There is holistic class and features class [8]. Holistic was defined as looking at the whole and features was the differences in features and spacing and gaps between different parts [8]. They sounded quite similar with features taking the holistic maybe a step further assigning numerical values for easier computer comparisons.

Then it came back to advantages and disadvantages of bio-metrics for healthcare. Listing things like security, convenience and reliability as advantages [7]. Disadvantages included sensitivity as mentioned, identity leakage, privacy risks and the need for large sample sizes. These disadvantages in combination with flaws in current password and token systems in use led the author to offer bio-metrics as a source for multi-factor authentication. Stating ”biometric systems are not the replacement of authentication and security tools and technologies but combining biometric approaches with these tools can increase the security aspects” [8].

2.9. Other Thoughts

One topic none of the authors looked into was the issue of acceptability. The easy to obtain and socially acceptable part raised suspicion that none of the authors mentioned for differing cultures. In a different class (Culture and Health), this issue was the topic, mostly relating to disease and how different cultures view them, treat them, or may be prone to different ones. Having everyone (that is planned to be measured and stored) agree or not have religious differences to the area to be seasured will be an issue. In particular muslim cultures, were women are not able to show different parts of their body would be difficult to obtain consent to measure their features.

Another topic mentioned as a problem but never offered a solution was the database size and security that any system like this would need and the connectivity to other such systems for out of network patients. As mentioned, governments collect data like this and track different people through the streets with similar systems. Asking them to share that kind of research and development would get resounding ”no’s” without question. Having access to these systems is most likely top secret and releasing it (or even just something similar) for public data and access would bring their own systems security at risk.

3. Current Research and Future Work

Though mentioned or just gleamed from several of the articles summarized above, current applications of biometric identification have been in the works for a long time now. New improvements to such devices and compactness and affordability have been on the rise for such things as well.

3.1. Smart Devices

Since as early as 2004 phones have had bio-metric identification such as finger printing. Then in 2017, the introduction of facial recognition broke into the smart phone world as well. Even smart watches such as Fitbit and Apple Watch are sometimes able to identify and unlock with your ECG and PPG as discussed earlier. With such common place devices having such technologies and growing databases as well as finding better and more efficient ways to identify you (though many times they are only comparing to the one or two people that use them). This continued improvement and ingenuity is really the forerunner paving the way for these technologies to begin expanding into ohter fields.

3.2. Neuralink

The first thought on future research is the recently successful Neuralink. With technological implants that can allow a person to play chess online with only their brain, the applications are endless. Each one could be registered to an individual and (I would hope) with it being unable to extract by non professionals, could be used as ”Bio”-metric identification being a part of the person now and unique in terms of serial number or MAC address (or however it identifies itself). The problem with this is once again availability and patient compliance to get devices like this. With such technologies begining to be developed, a future like the one presented in the Netflix series ”Altered Carbon” is not too far away.

4. Conclusion

Many of these article discussed good and potential bad for implementing bio-metrics into healthcare systems. Most authors agreed that with technology growing and evolving as it is, bio-metrics have an increase to the security aspects of the field of healthcare. The fact that it could be used in poorer communities or as assistance to those who may not be able to speak or read has tremendous upsides.

The risk to security of the systems as a whole are not to be overlooked either. Most authors also agreed that any leakage would lead to identity theft of individuals and loss of private information of patients. Though some of the studies set up parameters and check against different attacks, none of them check against many, and there is always different vulnerabilities that are unaccounted for causing the need for patching systems often.

A design for a secure system may already be being used by some government entity or waiting to be discovered. With the research and view on the benefits that bio-metric data could have on the healthcare industry needs to be weighed measured and counter balanced to see just how good of a fit it might be.

Acknowledgments

First Note: This section is not really to do with my paper but more a reflection of how I think it went and some how the class went and thanks for the semester. Feel free to read this section or not.

Second Note: Overleaf (the editor that was recommended I use) did not like the word biometric and showed it as misspelled. That is why you see it changed to bio-metric throughout.

I would like to apologize, I was not really sure how to go about writing this paper. It was framed to be a research paper of sorts but with it just being a summary of other sources on a topic that I have a stake in of sorts having worked in the field of healthcare in the past. Also on the parts for current research and Future work where I was just brainstorming and didn't have resources or a plan, just ideas that came while writing. I feel as though it ended up a little more narrative in places than it should have been. Also with it being so short for summarizing eight sources and including the introduction, conclusion, and Current Research/future work sections, I feel I may have cut some source summaries short and others may be too long. My bad.

Since this is the last major assignment other than the final, I wanted to take the time to thank you for the semester. It was probably rough for you to do it last minute and still being new to teaching. If it helps I thought you did pretty well given that circumstance and though some of the materials you might not have known the most on, I feel like I got the opportunity to learn a lot from you and the class. So thanks for the great semester and I know you don't think you are doing the best but keep it up, you are one of the better teachers I have had (even though you grade things super rough sometimes), and there are way worse teachers at UCCS (you are not among them).

References

[1] Mason, J., Dave, R., Chatterjee, P., Graham-Allen, I., Esterline, A., and Roy, K. , *An investigation of biometric authentication in the healthcare environment*, Array, 8, 100042, 2020.

[2] Banville, M. C. , *AM I WHO I SAY I AM? THE ILLUSION OF CHOICE: BIOMETRIC IDENTIFICATION IN HEALTHCARE*, 2023.

[3] Farid, F., Elkhodr, M., Sabrina, F., Ahamed, F., and Gide, E. , *A smart biometric identity management framework for personalised IoT and cloud computing-based healthcare services*, Sensors, 21(2), 552., 2021.

[4] Buhagiar, E., and De Raffaele, C. , *An Effective Biometric Patient Identification System for Health Organizations.*, 2021.

[5] Singh, G., Bhardwaj, G., Singh, S. V., and Garg, V. , *Biometric identification system: security and privacy concern*, Artificial intelligence for a sustainable industry 4.0, 245-264, 2021.

[6] • Ahamed, F., Farid, F., Suleiman, B., Jan, Z., Wahsheh, L. A., and Shahrestani, S., *An intelligent multimodal biometric authentication model for personalised healthcare services*, Future Internet, 14(8), 222, 2022.

[7] Mwapasa, M., Gooding, K., Kumwenda, M., Nliwasa, M., Kaswaswa, K., Sambakunsi, R., ... and Desmond, N. , *"Are we getting the biometric bioethics right?"–the use of biometrics within the healthcare system in Malawi.*, Global Bioethics, 31(1), 67-80., 2020.

[8] Dargan, S., and Kumar, M. , *A comprehensive survey on the biometric recognition systems based on physiological and behavioral modalities*, Expert Systems with Applications, 143, 113114., 2020.