Biometric Authorization for Building Security

Murphy, Brian
NYU Tandon, ISP Fall '21
New York University

NYC, USA
bpm9231@nyu.edu

***Abstract*—Protecting building assets, such as people, data, or devices is important for any organization. From a cybersecurity standpoint, impersonation attacks affect the confidentiality of building access, in that only authorized persons should enter. My hypothesis is that machine learning gait analysis models are more effective than humans. Specifically, in using cameras to detect attackers using impersonation attacks. Related research focused on voice recognition, electrocardiogram usage, and fingerprint scans for biometric authentication, respectively. The fourth focused on an IoT system using RFID cards and was looked at to compare as a non-biometric approach. Images and research from the CASIA-B dataset were used for the experiment.**

Keywords—building, biometrics, camera

I. Introduction

Breaching a building has high rewards for attackers. Employees, data, devices, and other assets are at risk of harm or theft. Therefore, cameras, security personnel, and scanners are commonly used to detect impostors. However, a determined attacker could evade or ignore these systems. An id card can be stolen or fabricated, a guard can be bribed, and ill-placed cameras can be bypassed.

Biometric authentication could be the answer to all of this. Biometrics cannot be easily fabricated, as they are unique to each person. A lot of research has already been done in the space, with pros and cons.

Mohamed and Martono's [1] research focused on using voice recognition to identify individuals. Their models were able to learn quickly and boasted 100% accuracy in identification. However, they collected 200 samples of audio from authorized persons to get that accuracy. In large organizations, or those with high turnover, this could be difficult. Furthermore, attacks using recorded audio of authorized persons could still work.

Zeng et al [2] focused research on an ECG card system, using electrical changes on skin to authenticate individuals. The system would have users touch a card to gather ECG data, transmit it to a device, and then compare it to stored ECG data. Compared to other methods, the data is unique and difficult to spoof. However, they show this can be affected by mental state, making availability harder. Users would also have to be comfortable with giving this information.

R. T Hans'[3] research focused on controlling vehicle access control using fingerprint scanners. His proposal replaces traditional cards with scanners used on entry and exit by authorized persons. A downside is similar to Zeng et al, where users would have to be comfortable giving that information up. Furthermore, in larger buildings this could cause long lines as people wait to authenticate themselves.

Finally, Bindu et al [4] focused on an IoT system on school buses. The system is designed with an RFID card for students, which activates when they get in range of a scanner. Notifications are sent to parents, teachers and bus drivers when they enter and exit the bus. A shortcoming of this system is the usage of physical cards, which can be lost or stolen. Further, a wireless system could be intercepted, and a duplicate card could be made.

My proposal solves these shortcomings. A person's gat can be used to uniquely identify a person, called gait recognition. Gait analysis models of this can be created using existing data from surveillance cameras. New employees could simply walk in front of a camera system, rather than having to speak one phrase hundreds of times. This avoids needing to collect and store extra data that users may not be willing to give. Finally, lack of physical user devices removes theft risk.

The organization of this paper is as follows: review of the dataset and previous work on it, the experiment, results, and future work.

II. Dataset and previous work

One of the largest gait datasets is provided by the Institute of Automation, Chinese Academy of Science. In this paper, we will focus on work related to CASIA-B, a subset. It was made by recording subjects and extracting silhouettes of 125 subjects at varying angles. Additionally, each walked using three poses: with Bags, wearing a Coat, and neither(Normal). Backs and fronts of subjects were also taken. Number of images was not uniform, as some were only one image, while others consisted of whole walks across frame.

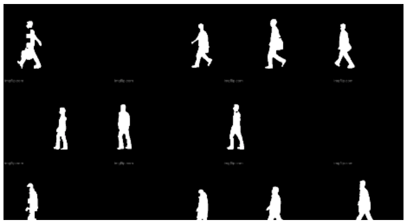
In the below table, there are some results from two papers published using this dataset, taken from a GitHub repository[7].

Paper	Normal	Bag	Coat	Avg
[5]	95	87.2	70.4	84.2
[6]	96.2	91.5	78.7	88.8

Attempts were made to recreate previous work, however due to time and resource constraints this was not possible. However, this does show the strength of gait recognition.

III. Experiment and Results

The core of my proposal is comparing humans to gait analysis machine learning models. To do this, 27 gifs using a subset of this dataset were prepared using the first 25 subjects. 8 of each type were made into gifs, while the 25th had all three types used. Regardless of pose, I used the 90 degree angle for all results. I used an online site Imgflip to convert the stills into gifs.



1. Sample of created gifs

Using a pure HTML/JS frontend, 6 or 9 were randomly shown to human subjects as authorized users. Once subjects felt confident in identification, 10 gifs were randomly selected, including ones not shown to them, and subjects asked to identify which are authorized and which are not. Results were displayed to subjects, then sent to a Python Flask API backend via the JavaScript fetch api. Both systems were implemented on Replit.

The experiment was run 20 times, generating 196 rows of data. Distribution by type is below.

Type	**Number**	**Percentage %**
Bag	66	33.67
Coat	54	27.55
Normal	76	38.78
Total	196	100

This shows that each type had about the same chance of being seen by subjects. Subjects got a total of 90 guesses correct, and 106 wrong.

Below are percentage of right and wrong results grouped by type.

Type	**Bag**	**Coat**	**Normal**	**Overall**
Right	39.39	55.56	44.74	45.92
Wrong	60.61	44.44	55.26	54.08

Here we see something interesting. When a Bag walker was shown, participants had a 39% chance of guessing correctly, worse than a coin flip. However, for Coats, they had a little better than a coin toss at 55% right, which reversed for Normal, with only 45% correct. This seems to show that coats were easier to identify or remember. However, overall, participants had 46% chance of being correct on any guess. When compared against the models cited above, it seems humans do in fact fair worse.

However, there were several issues. One was the data used. The available set was taken from one dataset, and only available in black and white. Additional datasets, and maybe color gifs would have helped. Further, only one angle was used, which may not have been the fairest to humans. Time subjects spent studying was not tracked, nor was time used to identify. This would have helped to compare against machine learning models, as I would have factored in training time.

Another was technical. Replit "sleeps" inactive apps, including my Flask API, so I may have missed some data. My frontend however always worked. Further, Javascript coding errors resulted in data loss of 4 rows, which is why I have 196. I also could not run or train the models myself, relying on other work and making me unable to test against the same subset as human subjects. If I were to do this again

A final issue was users. Three initial users reported the gifs were too similar and were shown 9 at a time. This made them feel the test was rigged or unwinnable. As a result, I edited it to 6 for the rest of the experiment. Users also had trouble understanding the experiment, as well as seeing the images, which prompted rewrites of the frontend. While most results were collected in-person, those sent the link would do unexpected things. One cheated by having the learning page and the identification pages open. Another ignored instructions and assumed they were supposed to stop anyone with a bag based on the gifs shown to them. More user testing could have gotten better results.

IV. Conclusion

My hypothesis was that building security could be achieved with gait recognition models watching cameras, which could outperform humans doing the same. Based on my results and previous research, this seems to be the case. However, data, technical, and user issues mean that a true conclusion cannot be drawn. Future work would have to address these issues.

References

[1] S. Mohamed and W. Martono, "Design of Fusion Classifiers for Voice-Based Access Control System of Building Security," 2009 WRI World Congress on Computer Science and Information Engineering, 2009, pp. 80-84, doi: 10.1109/CSIE.2009.983. J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[2] F. Zeng et al., "Biometric Electrocardiogram Card for Access Control System," 2011 Fifth International Conference on Genetic and Evolutionary Computing, 2011, pp. 373-376, doi: 10.1109/ICGEC.2011.92.

[3] R. T. Hans, "Using a biometric system to control access and exit of vehicles at Tshwane University of Technology," 2014 International Conference on Computer, Communications, and Control Technology (I4CT), 2014, pp. 230-233, doi: 10.1109/I4CT.2014.6914180.

[4] P. V. Bindu, K. D. Al-Hanawi, A. M. Al-Abri and V. Mahadevan, "IoT Based Safety System for School Children: A Contactless Access Control for Post Covid School Conveyance," 2021 2nd International Conference for Emerging Technology (INCET), 2021, pp. 1-4, doi: 10.1109/INCET51464.2021.9456314.

[5] H. Chao, K. Wang, Y. He, J. Zhang and J. Feng, "GaitSet: Cross-view Gait Recognition through Utilizing Gait as a Deep Set," in IEEE Transactions on Pattern Analysis and Machine Intelligence, doi: 10.1109/TPAMI.2021.3057879.

[6] C. Fan et al., "GaitPart: Temporal Part-Based Model for Gait Recognition," 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), 2020, pp. 14213-14221, doi: 10.1109/CVPR42600.2020.01423

[7] C. Fan et. al., "OpenGait GitHub Repository", hosted on GitHub, https://github.com/ShiqiYu/OpenGait

Links: Not part of official paper

[1] -https://ieeexplore-ieee-org.proxy.library.nyu.edu/document/5170665

[2] https://ieeexplore-ieee-org.proxy.library.nyu.edu/stamp/stamp.jsp?tp=&arnumber=6042804&isnumber=6042702

[3]-https://ieeexplore-ieee-org.proxy.library.nyu.edu/stamp/stamp.jsp?tp=&arnumber=6914180&isnumber=6914123

[4]- https://ieeexplore-ieee-org.proxy.library.nyu.edu/stamp/stamp.jsp?tp=&arnumber=9456314&isnumber=9456045

[5]: https://ieeexplore-ieee-org.proxy.library.nyu.edu/stamp/stamp.jsp?tp=&arnumber=9351667

[6]: https://ieeexplore-ieee-org.proxy.library.nyu.edu/stamp/stamp.jsp?tp=&arnumber=9156784

GitHub Link to papers 5,6 and Python Code: https://github.com/ShiqiYu/OpenGait