Cost-Effective Biometric Authentication using Leap Motion and IoT Devices

Louis-Philip Shahim, Dirk Snyman, Tiny du Toit, Hennie Kruger
School of Computer-, Statistical- and Mathematical Sciences
North West University,
Potchefstroom, South Africa.
e-mail:lp.shahim6@gmail.com; {dirk.snyman, hennie.kruger, tiny.dutoit}@nwu.ac.za

***Abstract* — Biometric authentication is a popular method for information security defense and access control. With the availability of small computing Internet of Things (IoT) devices in conjunction with a hardware peripheral that is able to track hand geometry, multifactor authentication becomes cost-effective and mobile. The proposed system would attempt to authenticate system users by combining both a user's hand geometry scan, along with a series of gestures while simultaneously using machine learning classification techniques for user classification. Cancelability will be insured with a novel steganography implementation for user biometric information.**

Keywords – biometrics; information security; internet of things (IoT); leap motion; multifactor authentication.

I. INTRODUCTION

Biometrics have long been used as an accepted user authentication method and have been implemented as a security measure in many real world systems including personal computers, mobile devices (cell phones and tablets), and also physical access control systems [1][2][3]. Biometrics are the digitalization and analysis of a person's innate physical or biological characteristics and the use thereof to distinguish between persons that are to be afforded access to specific systems, information or physical areas [1][3]. By encoding a person's physical attributes the disadvantages of traditional password based security, like passwords being lost or stolen, can be overcome [1][3]. One of the factors that hampers the acceptance of biometric authentication systems is that the cost of the development and implementation has traditionally been high due to factors such as biometric hardware, computational processing power, infrastructure integration, user training, and research and testing [1][3]. Cost still remains an ever present consideration for organizations when deciding to implement novel approaches over existing traditional methods. This factor raises the question whether traditional biometrics can be accomplished at a lower cost by using non-traditional methods and/or hardware.

With the current influx of new augmented computer interaction possibilities (i.e., new and non-traditional ways to control computers), a wide range of technological facets such as voice-, image- and movement control are receiving a lot of attention [3][4]. This leads to advancements in hardware capability and a definitive decrease in the cost of related hardware. Hardware peripherals (like the Leap Motion Controller (LMC)) that extend the basic functionality of computers to include support for the aforementioned facets are becoming more commonplace [2]. In order to facilitate these interactions, the hardware is implicitly working with information that can be harnessed for biometric identification. Chan *et al.* [2] mentions the possibility of partial sign language gesture recognition using the LMC. The recognition of simple gesture interactions could be implemented as a form of biometric identification due to the latent biometric information it conveys.

The advent of the IoT movement [5][6] presents a myriad of small computing systems that display reasonable processing power and connectivity capabilities at a cost point far lower than traditional computer systems. The IoT is the interaction of everyday objects over the internet or similar networks by embedding computer systems that add smart functionality or an implied "intelligence" to these objects [5][6].

By combining the two above mentioned paradigms, this paper proposes a system that would implement the required hardware and software in an environment that uses augmented user interaction techniques in order to authenticate system users. Using a LMC for advanced hand scanning, a user would be able to gain access to a system or physical area (interfacing with electronic components of traditional security systems to be controlled by the RPi) by having their hand geometry scanned, combined with a series of gestures to incorporate a technique called multifactor authentication [2] in an inexpensive way. Because the LMC requires no direct touch (compared to traditional fingerprint scanners), an applicable scenario for such a system could be to allow medical surgeons access to an operating theatre once they have disinfected their hands and would not like to touch any surfaces before entering. By simply gesturing towards the authentication system, access will be granted if the surgeon is duly authorized thereto.

The rest of this paper is structured as follows: Section II presents system design in terms of security, hardware, interpretation of biometric information, and advantages and disadvantages. The conclusion and future direction for this research is presented in Section III.

II. SYSTEM DESIGN

A. Security considerations

Literature [1][3] mentions a series of considerations (other than cost) that should be central to decision making relating to biometric systems and the biometric traits on which the system functions. Among others, these include:

1) Reliability – The system needs to be always operational and available and therefore hardware should be able to handle many interactions without fail.

2) Error incidence and accuracy – Errors may be introduced to the system by external factors like user aging or environmental changes. The accuracy of the system (false-acceptance vs. false-rejection rates) should be balanced to ensure security while promoting usability.

 ISBN: 978-1-61208-493-0

3) User acceptance – Users need to embrace the technology in order for the biometric authentication method to be successful. Unobtrusive technologies get accepted more easily.

4) Ease of use – The biometric technology should be easy to use, preferably without extensive training.

5) Security application – The choice of biometric authentication method should fit the level of security expected for the specific application.

6) Cancelability – Cancelable biometrics (CB) refer to the obfuscation of stored personal biometric information in such a manner that prohibits the reconstruction of said information by third parties using computational techniques [9]. This ensures the anonymity of users who submit their data to biometric authentication systems by ensuring that their specific information is difficult to decipher by any party other than the intended system. One the main categories of CB is that of biometric salting [9]. This entails the transform of biometric information using transform parameters native to the user in question. E.g., using hand information retrieved from the LMC as transform parameters.

7) Maturity of technology – Traditionally the maturity of the technology, i.e., the technology is often implemented and how well it is supported, determines its longevity. This is also based on prevailing standards that are expected of a proven technology. The LMC, when implemented as a biometrics device, should conform well to these factors mentioned above except for the maturity of the technology. Due to the novel nature of the application it is to be expected that the maturity level is to be quite low.

B. Hardware

With the LMC's advanced hand and finger tracking capabilities, the position, velocity and orientation, supplemented by hand geometry information, are reported upon with accuracy and reduced latency [8]. Chan *et al.* [2] present the implementation of an LMC to assume the role of a biometric authentication device by harnessing the abovementioned information. The low cost factor of this device makes this implementation even more favorable in situations where cost is of substantial concern. One drawback of this approach is that the LMC is a peripheral device that still requires a computer system to connect it to as the device cannot function in a standalone way. This disadvantage will add to the associated cost of implementation. However, because the IoT is such a phenomenon presently, many low cost alternatives to traditional computer systems have become commonplace. One of the most widely known computer systems for IoT development is the Raspberry Pi (RPi) platform [6][7]. The RPi presents a balance between size, connectivity, processing power and cost making it an ideal IoT device to serve as an electronic interface (e.g., for interaction with existing physical security systems) alongside traditional computers that drive peripheral devices like the LMC. The information from the LMC can be analyzed locally using methods such as those described by Chan *et al.* [2] but augmenting the result of the analysis by transmitting instructions to the RPi to effect remote digital electronics based tasks, for instance the arming or disarming of alarm systems across interconnected networks (like the Internet) where the RPi serves as an intelligent node for electronic systems interaction. The RPi can further be used for the communication with remote sensors such as movement- or sound sensors.

C. Interpreting biometric information

In order to interpret the implicit biometric information that is conveyed by the LMC and harness it in order to do biometric authentication, [2] proposes the use of machine learning techniques (see [8] for more examples on machine learning in biometrics). The readings obtained from the LMC (or other biometric devices) can be presented to a machine learning algorithm as features. The machine learning algorithms (each to their own internal structure) represent data that was gathered from users as a model against which to assess biometric access attempts at runtime. These models for biometric classification are usually biased to have a high precision, but low recall rate (i.e., to favor low false-acceptance rate at the expense of high false-rejection rates). The following algorithms are often implemented for biometric classification [2][8][11][12]: Naïve Bayes classifiers, Random Forrest classifiers, Support Vector Machines, Gaussian Mixture Models, and Artificial Neural Networks.

D. Advantages/Disadvantages

Advantages of the proposed approach to biometric authentication include: *a)* Ease of use and convenience. *b)* The low cost factor. *c)* Security aspects should be good when compared to passwords because authentication is based on gestures and hand information that cannot be stolen or guessed. *d)* Auditability in terms of being able to connect users to a specific event or activity. *e)* Well suited for environments where typing is difficult or unwanted (e.g., surgeon in theatre).

Disadvantages include: *a)* The technology is still in its infancy and is not mature. *b)* While accuracy of authentication is expected to be high for small organizations, it may pose a problem with many users. *c)* Error incidence due to changes in a person's hands due to injury, old age, or illness.

E. Comparison with literature

Table 1 presents a cursory summary of a selection of systems from literature in comparison to the idea proposed in this paper. The proposed novelty of this idea is the combination of the resulting LMC biometric authentication system with an environment where IoT devices interact with existing security infrastructure. The idea further proposes the inclusion of novel cancelability by employing a new steganography approach for the storage and retrieval of biometric user information. The steganography algorithm will include biometric information of each user as transform parameters. To further illustrate the approach, Fig. 1 presents a graphical representation of the proposed algorithmic framework.

 ISBN: 978-1-61208-493-0

TABLE 1: COMPARISON OF SYSTEMS FROM LITERATURE.

Biometric device	Biometric task	Cancelability	Algorithm	IoT	
LMC	3D signature recognition	None specified	Naïve Bayes/Support vector machine	No	[11]
LMC	Gesture based biometrics	None specified	*k*-nearest neighbor classifier	No	[12]
LMC	Hand geometry and gestures	None specified	Random forest classifier	No	[2]
LMC	Hand geometry and gestures	Stenographical encryption based on biometric information	Machine learning classification and novel steganography	Yes	[this paper]

III. CONCLUSION AND FUTURE WORK

This paper presented the proposed idea of a LMC as a low cost biometric authentication device by its combination with an RPi as an IoT device. The next stage in this research will be to investigate different implementation possibilities. Further investigation into the underlying hardware and software topics is warranted to gauge the feasibility of these technological aspects before experimental implementation can commence. Issues in terms of information security that need to be investigated are: Classification methods need to be researched to ensure the highest possible accuracy of implemented classifiers. The implementation of secure cancelable biometrics to ensure user anonymity. Dlamini *et al.* [10] present the encryption of user credentials in transit and rest by using steganography to "hide" user information in images rather than commonly used user databases. If a common user database is breached, all of the users' information contained therein may be exposed. Future work may include the incorporation of biometrics (read from the LMC) as parameters for use in such a steganography engine as implemented by Dlamini *et al.* [10]. This results in a steganography algorithm that encodes the user information in a picture based on their own unique traits rather than arbitrary encryption keys which may be computationally deduced. The premise is that even when one user's information is identified from the image, the fidelity of other users' information remains intact because the encryption parameters are unique to each user. Finally, extensive real world experimentation is planned with the resulting system to identify any inherent security flaws.

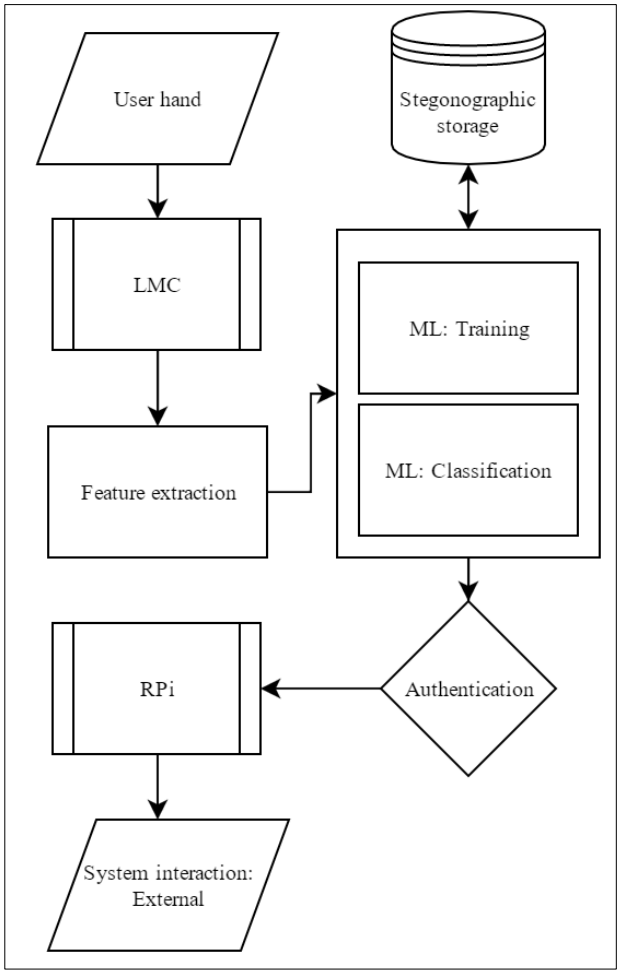

Figure 1. Graphic representation of the algorithm.

REFERENCES

[1] S. Liu and S. Silverman, "A practical guide to biometric security technology," IT Professional, vol. 3, no. 1, 2002, pp. 27-32.

[2] A. Chan, T. Halevi, and N. Memon, "Leap Motion Controller for Authentication via Hand Geometry and Gestures," In Human Aspects of Information Security, Privacy, and Trust, 2015, pp. 13-22.

[3] A. K. Jain, K. Nandakumar, and A. Ross, "50 Years of Biometric Research: Accomplishments, Challenges, and Opportunities," Pattern Recognition Letters, 2016. [Online]. Available from: http://www.sciencedirect.com/science/article/pii/S0167865515004365.2016.06.10.

[4] X. Wang, S. K. Ong, and A. Y. C. Nee, "A comprehensive survey of augmented reality assembly research," Advances in Manufacturing, vol. 4, no. 1, 2016, pp. 1-22.

[5] F. Xia, L. T. Yang, L. Wang, and A. Vinel, "Internet of things," International Journal of Communication Systems, vol. 25, no. 9, 2012, p. 1101.

[6] M. Maksimović, V. Vujović, N. Davidović, V. Milošević, and B. Perišić, "Raspberry Pi as Internet of things hardware: performances and constraints," Design issues, vol. 3, 2014, p. 8.

[7] MagPi, "Raspberry Pi 3 is out now! Specs, Benchmarks & More," 1 March 2016. [Online]. Available from: https://www.raspberrypi.org/magpi/raspberry-pi-3-specs-benchmarks/. 2016.03.01.

[8] G. Damousis and S. Argyropoulos, “Four Machine Learning Algorithms for Biometrics Fusion: A Comparative Study,” Applied Computational Intelligence and Soft Computing, vol. 2012, 2012, p. 6.

[9] C. Rathgeb and A. Uhl. “A survey on biometric cryptosystems and cancelable biometrics.” EURASIP Journal on Information Security 2011.1, 2011, pp. 1-25.

[10] M.T. Dlamini, J. Eloff, H.S. Venter, M. Eloff, K. Chetty, and J. Blackledge. “Securing cloud computing's blind-spots using strong and risk-based MFA,” In International Conference on Information Resource Management, 2016, pp. 58:1-28.

[11] I. Nigam, M. Vatsa, and R. Singh. “Leap signature recognition using hoof and hot features,” In 2014 IEEE International Conference on Image Processing (ICIP), 2014, pp. 5012-5016.

[12] M. Piekarczyk and M.R. Ogiela, “On using palm and finger movements as a gesture-based biometrics,” In 2015 International Conference on Intelligent Networking and Collaborative Systems (INCOS), 2015, pp. 211-216.

 ISBN: 978-1-61208-493-0