Biometrics in cyber defense

Gabriela Mogos*

Computer Science and Software Engineering Department, Xi'an Jiaotong-Liverpool University, 111 Ren'ai Road, Suzhou, China

Keywords: Cryptography, Biometric identification, Iris recognition.

Abstract. Biometric identification is an up and coming authentication method. The growing complexity of and overlap between smart devices, usability patterns and security risks make a strong case for securer and safer user authentication. This paper aims to offer a broad literature review on iris recognition and biometric cryptography to better understand current practices, propose possible future enhancements and anticipate possible future usability and security developments.

1 Introduction

Typically, access credentials are established, practiced and recovered using passwords. In earlier computing ecosystems, passwords represent a high security wall against possible hacking and/or guessing activities. Unsurprisingly, earlier computing systems are underdeveloped, non-integrated, minimally web-enabled, of much lower processing speeds and process much less data volumes. This is not to mention, of course, lesser adoption and usability patterns. These factors, only a handful, justify why security, let alone privacy, was a lesser priority in earlier computing ecosystems.

A few decades later, however, not only have security become a first priority across different industries and usability patterns (expert, professional and average user) but has required, more critically, far more measures to maintain.

As computing processing power (e.g. quantum computing), device/application variety (e.g. laptops, smartphones, iPads, cloud-based platforms, virtual servers, etc.) and data volumes (e.g. Big Data) continue to evolve in speed, capabilities and size, respectively, security measures assume even more critical priority. In recent years, a number of security measures has emerged, in addition to or replacement of, password-based access. For current purposes, biometric identification is of central interest.

The adoption of biometric identification methods has become more mainstream in recent years. Primarily for security reasons, biometric identification has come to be replace password-based access across industries, devices, platforms and/or applications. Of specific interest is iris recognition innovations, now deployed at rapid adoption patterns. To better understand how iris recognition – and, more broadly, biometric cryptography – is changing

* Corresponding author: Gabriela.Mogos@xjtlu.edu.cn

current usability and security practices, a closer examination is required of current literature and state-of-art practices.

This research paper discusses, accordingly, how biometric identification, particularly iris recognition, has received growing attention in literature and practice.

2 Current situation

The need for more enhanced security methods has grown by leaps and bounds in recent years. As noted, rapidly developing computing capabilities, combined by unprecedented evolution of new generations of smart devices and virtual applications, have made password-based authentication methods increasingly outdated, if not outright risky. The attention to securer and safer authentication methods is documented early in literature [3]. The shift – which, in fact, is both practical and conceptual – from password-based to biometric authentication is informed by a broad range of developments in information management and security precautions in computing ecosystems. Given current research focus, iris recognition is central to a discussion about biometric identification methods.

Five main areas emerge, under current literature on iris recognition and biometric identification: Mobility, Methods, Big Data, Open Source and Challenges.

The Mobility research and practice area highlights growing needs for biometric identification and authentication methods in response to growing risks due to using password-based authentication methods in smartphones.

The Methods research and practice area reports specific methods used to develop iris recognition capabilities.

The Big Data research and practice area discusses opportunities and challenges of adopting biometric cryptography methods for vast data volumes.

The Open Source research and practice area highlights a growing need for "free" resources to develop and benchmarks for iris recognition and biometric identification methods.

The Challenges research and practice area discuses one major challenge for iris recognition and barometric identification. These research and practice areas are discussed in depth as follows:

2.1 Mobility

The emergence of smartphones as multiple-purpose device is becoming increasingly undisputed. The convenient portability, global access and multiple features (e.g. mobile-custom apps and photo capturing, storage and recovery features) of smartphones make mobile phones indispensable for professional, social and personal applications. Interestingly, however, access to and authentication methods for smartphones appear to lag much behind built-in and add-on mobile capabilities. According to a 465-participant survey [2], participants report consistent need for stricter security measures and securer authentication methods compared to current password-based ones. In response, Ben-Asher et al. propose a dual-layer security model for mobile phones, including biometric cryptography. By "multiplying" security layers, security practices show, attempts to intrude, sniff and/or penetrate are considerably reduced, if not eliminated.

The surprising paradox one notes from recent exponential growth and development of smartphones – and, for that matter, mobility in general – is that, while mobile devices, including smartphones, are characteristically personal properties, means to personalize authentication methods remain, largely, standardized. If anything, iris recognition and biometric cryptography are not only securer and safer user-authentication methods but, from a

user-centered approach, are more personal and unique. The adoption of more personalized authentication methods at mass scale has, moreover, broad implication for mobility markets and business. Notably, a more personalized and customized approach to authentication, particularly using iris recognition methods, is apt to create new niche markets for mobile security across devices, platforms and applications.

2.2 Methods

The growing needs for non-password-based authentication methods has given rise to a plethora of alternatives to secure access. Notably, iris recognition has become increasingly adopted across different user segments, usability patters and devices.

The [4] offers, for instance, an innovative method to adopt iris recognition. More specifically, Moi et al. propose an approach by which a secure cryptographic key is generated from Iris Template. More specifically, available iris images are processed such as to generate Iris Template or Code utilized for encryption/decryption activities.

The experimental results show, interestingly, low false rejection and false acceptance rates. This proposed method does not only enable users to authenticate access more securely but, more critically, to generate a cryptographic key whose authentication is accepted or not based on more complex visual identification analysis compared to a password-based authentication method.

The implications for biometric identification methods using iris recognition are far-reaching. In addition to securer and safer accessibility, iris recognition methods introduce radical shifts in human-machine interactions. In contrast to a conventional hand-keyboard interaction mode, iris recognition redefines how users (so far, human) gain access to one or more device, platform and/or application using a human part, i.e. eyes. For users long used to hand-keyboard interactions, iris recognition, apparently convenient and effortless, might involve some accessibility challenges, if not outright resistance, from users. The user acceptance of iris recognition is, probably, an area which requires further research for better practice and adoption patterns.

2.3 Big data

The scope and quality of data authenticated by biometric systems highlights parallels between biometric identification methods and Big Data systems. According to [6], biometric systems, much like Big Data, are required to offer effective solutions to Four V Challenges:

Volume, i.e. vast enrollment database size,

Velocity, i.e. rapid processing response-time,

Veracity, i.e. requirements using potentially noisy, fraudulent data, and

Variety, i.e. multiple biometric identifiers. The growing complexity and size of enrollment data, as in Big Data, makes biometric identification and authentication methods, including iris recognition, accordingly, not only preferable but a necessity.

As noted, multiple-layer authentication has become mainstream due to emerging risks resulting from growing capabilities in devices and unauthorized access.

2.4 Open source

The evolution of iris recognition systems and applications is rapid and constant. As discussed above, methods of iris recognition continue to change response to emerging risks and usability patterns across devices, platforms and applications. Similarly, biometric identification, including iris recognition, methods face challenges comparable to Big Data.

More broadly, open source systems, platforms and applications are becoming increasingly adopted across industries, user segments and devices.

This is justified by several factors:

First, open source software offers far more modularity options compared to commercial and/or closed systems.

Second, open source software is cost-effective.

Third, open source software involves constant collaboration inputs from multiple developers and/or users, or community members and hence far more efficiencies and far less vulnerabilities.

Fourth, open source software is fairly easily deployable across platforms.

Unsurprisingly, a growing number of efforts is attempted to develop more effective iris recognition applications. The paper [5] discusses, for example, how OSIRIS, an open source iris recognition system, in different developed versions (i.e. OSIRISV2, OSIRISV4, and OSIRISV4.1), do not only offer higher verification rates but also a reliable baseline, or benchmark, against which different algorithms used for iris recognition could be compared and, possibly, optimized.

Needless to say, benchmarking remains a highly valuable, albeit missing, criterion based on which evolution of different versions of emerging applications are assessed. For iris recognition applications, a community/industry/practitioner universal standard is, indeed, a necessary requirement.

The adoption of open source iris recognition software for biometric authentication becomes, for all four (and more) reasons mentioned above, strongly recommended.

2.5 Challenges

Fuzziness is, perhaps, one most recurring challenge in iris recognition. In response, a broad range of solutions using more precise extraction methods, are proposed in literature. The [1] proposes, for instance, a highly effective extraction method by which more effective development systems of cryptographic key generation (up to 400 bits per iris) are enabled. The growing size of image database, combined by large scale deployment challenges, makes more effective methods to extract images data, particularly from regions of high entropy, a necessity.

Practically, growing numbers of passengers flying across borders, crowds in public spaces and, not least, terror-related risks – all make image processing using iris recognition methods at increasing speeds a growing necessity. For one, a broad range of adopters are concerned including, but may not be limited to, security agencies, smart device developers, smart home manufacturers and, not least, end users becoming more and more aware of security and privacy issues.

3 Discussions

The biometric authentication, including iris recognition, is a promising security area. Offering more security and safer access, iris recognition shifts authentication from password-based to biometric recognition. This shift has several implications along dimensions of security, usability, marketability, and deploy ability.

For security, safer authentication practices are expected. As noted, multi-layer authentication approach appears to gain further grounds. This should spill over to system management and user awareness. That is, by adopting a multi-layer authentication method, system administrators are better able to identify, mitigate and recover from security risks.

Moreover, a multi-layer authentication method is apt, hopefully, to raise user awareness of security and privacy risks by making harder access to personal or valuable data.

For usability, shifting authentication to iris recognition changes human-machine interactions in numerous ways. As noted above, users having biometric access to own/rented devices are more likely to exhibit ease or difficulty in accepting new methods. The user acceptance is, needless to say, a significant consideration system administrator, app developers are device manufactures often pay attention to.

For marketability, iris recognition authentication offers valuable market expansion methods. As noted above, iris recognition is, by definition, a highly personal authentication method. Tapping into almost limitless options for customization, app developers and device manufacturers might market and promote apps and device based on more personalized, iris-recognized features.

For deploy ability, iris recognition – and for that matter, biometric authentication in general – bypasses several security issues associated with password-based authentication.

In contrast to conventional password-based authentication, credentials are shifted from machines to users. More specifically, while password-based authentication might change slightly according to used device or location (both relatively easy to falsify by, saying, changing IP address), iris recognition, highly image-dependent and multi-layer-authenticated, is user-centric. Thus, users – not devices, ISPs, device manufacturers and/or app developers – have more control over authentication. Interestingly, future iris recognition methods might include open source applications enabling users to (un)lock biometric authentication for limited periods or permanently.

4 Conclusions

On iris recognition and biometric identification five major areas are identified as of primary significance in current – and, more likely, in future – practice: Mobility, Methods, Big Data, Open Source and Challenges.

For Mobility, a shift in authentication practices is noted. In contrast to password-based authentication, users are shown to express more interest in stricter authentication methods, including biometric ones. The proposition of dual-layer authentication by [2] reflects a growing shift to multi-layer, non-password-based authentication.

For Methods, generation of more effective cryptographic keys is a case in point. As systems grow smarter, data migrates more frequently across networks and platforms and security risks increase, stronger cryptographic keys, based on Iris Templates, become a natural response.

For Big Data, biometric systems appear to exhibit striking parallels. As shown by Ratha et al. [6], biometric systems and Big Data share all Four V Challenges of: (i) Volume (ii) Velocity, (iii) Veracity, and (iv) Variety.

As data complexities increase, biometric identification becomes, apparently, more about Big Data management. This requires, perhaps, more innovative methods to ensure processed data is accurately, verifiably, and rapidly processed for more effective authentication.

For Open Source, iris recognition appears to gain more verifiability using collaborative software. The OSIRIS system offers, for example, numerous ways by which updated standards could not only enhance authentication but also to provide a reliable benchmark against which current and future iris recognition applications are assessed and, hopefully, better developed.

For Challenges, fuzziness remains a central issue in iris recognition. The constant evolution of extraction methods is apt to result in more effective development systems of cryptographic key generation.

References

1. S. Adamovic, M. Milosavljevic, M. Veinovic, M. Sarac, & A. Jevremovic, Fuzzy Commitment Scheme for Generation of Cryptographic Keys Based on Iris Biometrics. IET Biometrics, 6(2), 89 – 96. IET Digital Library. (2017)
2. N. Ben-Asher, N. Kirschnick, H. Sieger, J. Meyer, A. Ben-Oved & S. Möller, On the Need for Different Security Methods on Mobile Phones: Proceedings of the 13th International Conference on Human Computer Interaction with Mobile Devices and Services, Stockholm, Sweden. (2011)
3. P. Li & R. Zhang, The Evolution of Biometrics, International Conference on Anti-Counterfeiting, Security and Identification. (2010)
4. S. Moi, N. Abdul Rahim, P. Saad, P. Sim, Z. Zakaria & S. Ibrahim, Iris Biometric Cryptography for Identity Document. Paper presented at International Conference of Soft Computing and Pattern Recognition. (2009)
5. N. Othman, B., Dorizzi & S. Garcia-Salicetti, OSIRIS: An Open Source Iris Recognition Software. Pattern Recognition Letters, 82(2), 124-131. (2016)
6. N. Ratha, J. Connell & S. Pankanti, Big Data Approach to Biometric-Based Identity Analytics. IBM Journal of Research and Development, 49(2/3), 1-11. (2015)