Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 7.056

IJCSMC, Vol. 14, Issue. 3, March 2025, pg.39 – 47

Crypto-Biometric: An Overview

Solomon Sarpong[1]; Kwafo Awuah-Mensah[2]; Samuel Opuni-Basoa[3]

[1,2,3]Department of Physical and Mathematical Sciences
University of Environment and Sustainable Development, Somanya, Ghana
[1] ssarpong@uesd.edu.gh; [2] kaawuah-mensah@uesd.edu.gh; [3] sopbasoa@uesd.edu.gh

DOI: https://doi.org/10.47760/ijcsmc.2025.v14i03.005

ABSTRACT:
With the current advancement in computational technology, the security and privacy of information is under threat. The speed of data processing by modern computers is making traditional cryptographic techniques almost redundant. Cryptographic protocols which hitherto were deemed secure are under threat by bruteforce attack. In lieu of this, more secured cryptographic techniques are being sort to better protect data whether in transit or stationary. The quest for this pursuit has brought to the fore crypto-biometric – the use of biometric features of the user in addition to the traditional cryptographic techniques – techniques for information protection. Systems using biometric features for the protection of information is gaining popularity as there a unique and eternal relationship between a person and his/her biometric characteristics. Hence, harnessing the unique biometric features of an individual and the traditional cryptographic techniques will better protect users' information. This research paper seeks to highlight the benefits of the incorporation of biometric features and traditional cryptography.

Keywords: bruteforce, key management, cryptographic keys, electroencephalography, fuzzy extractor

I. INTRODUCTION

In order to prevent fraud, ensure compliance requirements, give better experience, manage risk, and response adequately to risks, systems usually ensure user verification and authentication. Traditionally, systems authenticate users by the provision of document, location detection, chat verification and passwords or passphrases. Humans at times have problems creating and remembering strong passwords. This difficulty makes their accounts vulnerable to attacks. In lieu of this, the use of biometric features of an individual for authentication gives user identity assurance as it is stronger than the traditional way.

For the purpose of this paper, the application of biometric technology refers to the identification and or authentication of a person using his/her biological and behavioral characteristics. The importance of the use of biometric features for the identification and authentication of a person(s) was initiated by Alphonse Bertillon. As a French police officer and a biometrics researcher, Bertillon applied anthropological technique of anthropometry to

law enforcement. By this, he created an identification system based on physical measurements, a system used by the police to identify criminals [1]. Bertillon can also be credited as the first person to have used fingerprint to solve crime.

Semi-automated facial recognition methods were developed in the 1960s. The semi-automated system required the analysis and extraction of usable facial features within an image by administrators. This is a manual method of biometric authentication. In 1969, the FBI became interested in biometric hence boosting its development. In the 1980s, National Institute of Standards and Technology (NIST) sought to develop speech recognition technology. This was a precursor to the voice command and recognition system in use today. The concept of the uniqueness of fingerprints and iris was proposed. Hence, by 1994, the first iris recognition algorithm was patented. By 1991, the technology for facial detection was developed hence enabling real time facial recognition possible. Despite its initial faults, by 2000s there were hundreds of biometric recognition algorithms that were functional or patented within the USA. This technology further found its applicability in commercial products.

Biometric technology works because each person is unique. There are physical and biological characteristics of individuals that distinguishes one individual from the other. It is based on these characteristics or traits that the different biometric systems seek to measure. Hence, the success of biometric techniques is based on how different the measurable characteristics or traits are in the different persons.

However, the usability of a particular biometric technique to a large extent depends on its ubiquitousness, distinctiveness, immutableness, acceptability, collectability and performance. Currently, the biometric techniques in use are fingerprint, eye (retina and iris), face, hand geometry, signature, voice, palmprint, gait recognition, body odor, ear shape, DNA, keystroke dynamics, and posture. These biometric features being used in the biometric technology can be classified as static and dynamic. The static features are usually physiological hence they are always present or do not change. The dynamic features are the behaviour of an individual.

The applicability of biometric technology depends on its intended use (verification or identification). The applicability of biometric technology depends on: willingness of the individuals to use the biometric technique and whether the collection of the biometric features covert or overt. There is a unique and eternal relationship between a person and his/her biometric characteristics hence, systems using biometric features for the protection of information is gaining popularity. Hence, this paper seeks to delve into the progress of development in this area of research and its prospects in the future.

A. Uses

In information security, the use of cryptography ensures the security of information whether in transit or stationary. Cryptographic keys are used to encrypt plaintext to cyphertext which can also be decrypted back to plaintext. In symmetric cryptography, same keys are used. However, in asymmetric cryptography, different keys are used. In symmetric cryptography, there is the problem of key distribution between the persons in the protocol. Key management (keeping all cryptographic keys safe) is another problem. Asymmetric cryptography on the other hand requires complex computation. In lieu of the issues with symmetric and asymmetric cryptography, some researchers advocate hybrid cryptographic technique - the use of both cryptographic techniques in a protocol. In the hybrid cryptography, symmetric cryptographic keys are shared using asymmetric cryptography whereas messages are encrypted or decrypted using symmetric cryptography. On the other hand, the hybrid cryptographic technique usually brings to the fore a third party to ensure that the protocol goes on smoothly making malicious and semi-malicious attacks less powerful. The

introduction of the third party also brings the fore the issue of repudiation - another important property of information security.

In cryptography, the longer the key the stronger the key (128 or 256 bits long) but the key is weak when it is short. Unfortunately, weak keys are easy to break and strong keys are difficult to remember due to its length. In order to overcome the problems of with the security of cryptographic keys, there is the use of another indicator: knowledge-based indicator (password) and possession-based indicator (smartcards). Passwords can be guessed through social engineering or dictionary attack. Smartcards on the other hand can be stolen or damaged. In the unfortunate event of any of these occurring, the problem of repudiation arises.

In traditional cryptography – symmetric, asymmetric and hybrid cryptography – there is either the issue of either the cryptographic keys being guessed, stolen, damage or the use of third party (bringing about repudiation). Key management is another problem with the traditional cryptographic techniques. Hence, this has brought to the fore the quest to integrate biometric features with traditional cryptography, referred to as crypto-biometric. The use of crypto-biometric addresses the problems relating to the traditional cryptography such the security of the cryptographic keys and repudiation. Crypto-biometric is the alternative to maintaining the privacy of cryptographic keys by using the user's biometric features. The use of biometric features in cryptography help prevent unauthorized access. Crypto-biometric helps to manage cryptographic keys by binding the traditional cryptographic keys to biometric features of the User hence ensuring non-repudiation, [2].

However, when the biometric feature used in the crypto-biometric become traumatized it becomes unusable as a form of authentication. Thus, different instances of the same biometric can result in error hence creating a serious problem in the crypto-biometric system. In such an instance, the biometric becomes useless forever especially if it was not transformed into revocable or cancellable template. This is due to the inherent characteristics of biometric features, as it usually uses non-cancellable template like password or smartcards. As a result of phishing attacks by hackers, persons are averse with biometric authentication as they are worried about what they are authenticating to.

The ability for a person to remember cryptographic key reduces when key is long (128 or 256 bits long). But the strength of a cryptographic protocol depends the length of the cryptographic keys used. This brings to the fore the use of biometric techniques due to the characteristics of the biometric features. The review of related literature is in section II. Storage of biometric data and the security of biometric data are in sections III and IV. The conclusion is in section V.

II. RELATED LITERATURE

Crypto-biometric system are either based on key release or key generation. The use of key release in biometric data is to ensure that, a randomly generated cryptographic key is secure and releases the secret only when a genuine biometric is presented [3], and [4]. On the other hand, in the key generation technique a random string is extracted from the biometric characteristics [5], [6], [3], and [7].

[3] proposed the use of fuzzy vault in binding cryptographic keys with biometric using the coordinates and the orientation of the minutiae points on the fingerprint. [8] proposed the fuzzy commitment scheme. By using the iris code, [6] proposed the use of fuzzy commitment scheme to protect the cryptographic key. Using fuzzy scheme with the coordinates of the minutiae points, [4] proposed a scheme that can hide the cryptographic secret key. While speaking a passphrase, [7] proposed a biometric based key generation technique for extracting the cryptographic key. By using online written signature, [9] proposed a biometric technique for extracting the cryptographic key.

[10] proposed the use of face a biometric feature for extracting the cryptographic key. The proposition for the generation of cancellable cryptographic template was made by [11]. Iris-based cryptographic key generation was proposed by [12]. Their proposal involved the use of binary bits derived from the iris for the detection in the cryptographic key generation. In order to make stronger cryptographic key, some researchers have proposed the use of multiple biometrics [5]. The use of the iris to generate cryptographic key was proposed by [13].

[14] proposed the usage of multibiometric (facial and fingerprint) features to create a random key for an individual. This random key can be used as an electronic number, passport identification, civil identification number e.t.c. The usage of the eye and ear features to generate cryptographic keys was proposed by [15]. They applied the Meerkat Clan key generation algorithm (MCKGA) for the key generation. With the usage of AES, they believed the generated key is unique for use in cryptographic systems. Key generation from multibiometric systems using Meerkat algorithm was proposed by [14]. They observed that, cryptographic key generated using the features of the eyes is stronger than that from the ears. [16] proposed biometric-based key generation scheme by using the Crow search algorithm (CSA). [17] used Laplacian filter to enhance fingerprint image and generate cryptographic keys for security and privacy in fingerprint identification, recognition and key generation. In order to enhance security and generate efficient cryptographic keys, [18] proposed the use of information from the retina.

A. Biometric System Architecture

Most biometric systems have subsystems such as: data collection, signal processing, matching, decision, storage and transmission. Figure 1 depicts the pictorial representation of a biometric system. *Data collection subsystem* – this constitutes the input devices or sensors for reading biometric information of a user into an appropriate form for processing by the other components of the input devices. As a requirement, in the initialization the user has to input the biometric feature a number of times. This is important so as to accommodate changes to the biometric feature. *Signal processing subsystem* – the biometric features are extracted and transformed into data that is usable by the matching subsystem after receiving the biometric data from the data collection subsystem. In order to make the biometric data usable, discriminating features are extracted and noise is removed by filtering. *Matching subsystem* – this receives information from the signal processing subsystem and measures the similarity between the new sample and the reference template using a distance measuring metric. *Decision subsystem* – it measures the match score by setting a threshold above which the user is authenticated by giving a binary output. In order to reduce the tendency of rejecting a legitimate claimant or accepting an imposter, this system fixes the maximum number of times a sample can be submitted for authentication by a claimant. *Storage subsystem* – this is usually a physically protected storage within the biometric device. It keeps the templates of enrolled users, usually more than one template per user. *Transmission subsystem* – even though this is usually a separate physical entity within the biometric system, it is integrated in others. It maintains security of the biometric data during transmission when it is most vulnerable.

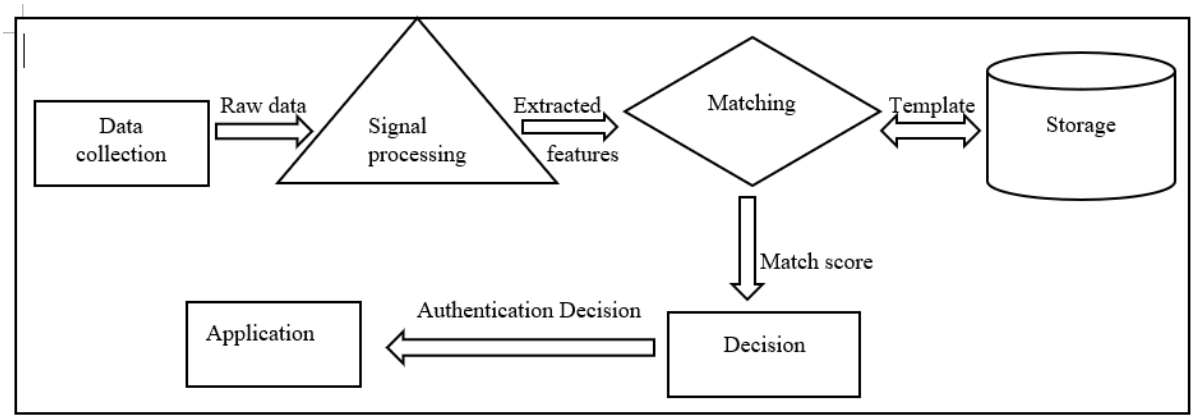

Figure 1: Pictorial representation of a biometric system

B. ***Protocol***

In order for a crypto-biometric system to be used, the enrolment should be secure – binding of the biometric template to the enrollee, and the checking of the quality of the template to facilitate the matching procedures should be done. These procedures entail the collection of the biometric feature, the binding of the identity of the User to the biometric template and the storage of the biometric template in a database.

During the enrolment in a crypto-biometric system, the biometric feature is used more than once on the input device. A distance function is used to calculate the distance between key feature in the biometric information. The distance between these key biometric features is set as the tolerance threshold for acceptance. When the tolerance threshold is too large, it causes type II error (an imposter is admitted); small tolerance threshold may result in a type I error (a legitimate user maybe rejected). Hence, there should be a balance between type I and type II errors.

Key generation and management are very essential in a biometric system. In a biometric system just like in the traditional cryptography, the exactness property can be compromised. In biometric system, this happens when there is variation in different instances of the same biometric feature. In order to prevent compromising a biometric feature and making it non-biometric usable, it can be transformed into revocable (or cancellable) template. However, the use of hash functions is not good in biometric systems as a small change in the biometric feature will result in vary large changes in the hash values. Hence, in order to protect biometric data, protocols such as: fuzzy commitment and fuzzy vault; fuzzy extraction; and secure multi-party computation can be used.

C. ***Fuzzy commitment and fuzzy vault***

The combination of cryptography and biometrics for authentication using fuzzy vault was proposed by [19]. Biometrics can be grouped into two main parts – conventional and cognitive. The conventional biometrics refer to physical and behavioral characteristics (fingerprint, voice, DNA, body-odor, iris, retina). On the other hand, cognitive biometrics refer to mental state signals such as electroencephalography (EEG).

A fuzzy vault, cryptographic construct, was proposed by [20]. In the fuzzy vault, a player gets to know the secret in the vault only when the length of the key being used to unlock the secret overlaps substantially with the key that was used to lock it. In 2005, [21] proposed combination of fuzzy vault and fingerprint minutiae to secure information. Using fuzzy vault, [22] demonstrated that the strength of security in multi-biometric is greater than uni-biometric. A cancellable fuzzy vault algorithm that uses the transformed fingerprint features of the user was proposed by [23].

[24] proposed the use of revocable fingerprint template in a crypto-biometric system to exchange randomly generated cryptographic key with user's fingerprint data using fuzzy commitment scheme. In order to hide the cryptographic secret keys, [4] proposed a protocol that uses the coordinates of the minutiae of a fingerprint. [3] proposed a protocol that uses the fuzzy vault in which the coordinates and the orientation of the minutiae points of the fingerprint used.

D. *Fuzzy extraction*

A protocol based on fuzzy extractor was proposed by [25]. This protocol is based on a secure sketch construction that uses set difference metric and pairwise independent hash function. A protocol that turns noisy information into keys that is reliable for authenticating biometric data was proposed by [26] using fuzzy extractors. Reusable fuzzy secrets in biometric data was proposed by [27] using fuzzy extractors. [28] proposed threshold reusable fuzzy extractor which finds application in storing and sharing sensitive data by smart contact on blockchain achieving access control using biometric information.

[29] proposed fuzzy extractors that work for binary strings with Hamming noise. Their protocol is computationally secure in digital lockers that is simple and tolerates near-linear error rates. A succinct fuzzy extractor scheme for both verification and identification of biometric information which satisfies security requirements with constant computational cost was proposed by [30].

D. *Secure multi-party computation*

[31] proposed secure multiparty computation protocols that give clues on the best practices for securing a biometric identification protocol. They proposed two biometric security protocols (biometric data retrieval and authentication) that is privacy preserving and secure using provable computation techniques. With authentication relying on both facial and iris biometrics, [32] proposed multimodal biometric recognition protocol that operates on encrypted data under the malicious security model.

The unique and eternal relationship between any individual and the biometric characteristics has made systems using biometric features for authentication and identification grow in popularity, [33]. Biometrics are increasingly gaining popularity and replacing passwords as they are not memorized and also hard to steal [34]. In order to guarantee that no sensitive information is exposed, an extension of the standard iris-based verification protocol was proposed by [35].

III. STORAGE OF BIOMETRIC DATA

In crypto-biometric system the biometric features used are not secret but the biometric data are sensitive information. Hence, there are strict laws governing its storage and use in some in different geographic locations. Singapore has Personal Data Protection Act (PDPA); California has California Consumer Protection Act (CCPA); European Union has General Data Protection Regulation (GDPR); and United Kingdom Data Protection Act (DPA). For instance, the GDPR laws refers to biometric data as 'Special Category Data' hence, consent from an individual is needed for its collection, processing and storage.

IV. SECURITY

With the use of biometric systems, these errors can be committed; *False accept/matching* – when two biometric features from different persons are matched as sample from one person. *False reject/non-matching* – assuming two biometric features from the same person as samples from different person. For a biometric system to achieve optimal authentication characteristics, there should be a good balance between false accept and false reject.

Biometric systems reduce these types of errors by introducing the biometric liveness technique, artificial detection for face recognition with the use of 3D cameras, saccade for recognition (iris biometric). However, it must be noted that, biometric features are not secret but biometric data are sensitive information. Unlike other forms of data that can be anonymized, biometric features cannot. With the use of personally identifiable information, a person can be tracked/deanonymized.

In a biometric system, the use of encrypted template to authenticate a biometric feature uses deterministic encryption. However, with the use of deterministic encryption security is limited as with the use of personally identifiable information an individual can be deanonymized (or tracked).

V. CONCLUSION

This research paper has taken a look at the application of biometric features in cryptography so as the enhance security. This also gives persons the opportunity to use their body parts (eye, fingerprint, ear etc.) to gain access to their homes, electronic devices etc. Hence, this removes the tendency of individuals remembering long passwords or passphrases which is at times forgotten.

REFERENCES

[1] R. D. Chaudhari, A. A. Pawar, and R. S. Deore, "The Historical Development Of Biometric Authentication Techniques: A Recent Overview," *International Journal of Engineering Research & Technology (IJERT)*, vol. 2, no. 10, pp. 1–8, 2013.

[2] S. Barman, S. Chattopadhyay, and D. Samanta, "Fingerprint based symmetric cryptography," *2014 International Conference on High Performance Computing and Applications, ICHPCA 2014*, no. February, 2015, doi: 10.1109/ICHPCA.2014.7045306.

[3] K. Nandakumar, A. K. Jain, and S. Pankanti, "Fingerprint-based fuzzy vault: Implementation and performance," *IEEE Transactions on Information Forensics and Security*, vol. 2, no. 4, pp. 744–757, Dec. 2007, doi: 10.1109/TIFS.2007.908165.

[4] S. Yang and I. Verbauwhede, "Automatic secure fingerprint verification system based on fuzzy vault scheme," *ICASSP, IEEE International Conference on Acoustics, Speech and Signal Processing - Proceedings*, vol. V, 2005, doi: 10.1109/ICASSP.2005.1416377.

[5] A. Jagadeesan and K. Duraiswamy, "Secured Cryptographic Key Generation From Multimodal Biometrics: Feature Level Fusion of Fingerprint and Iris," vol. 7, no. 1, pp. 296–305, 2010.

[6] F. Hao, R. Anderson, and J. Daugman, "Combining crypto with biometrics effectively," *IEEE Transactions on Computers*, vol. 55, no. 9, pp. 1081–1088, Sep. 2006, doi: 10.1109/TC.2006.138.

[7] F. Monrose, M. K. Reiter, Q. Li, and S. Wetzel, "Cryptographic key generation from voice," *Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy*, pp. 202–213, 2001, doi: 10.1109/SECPRI.2001.924299.

[8] A. Juels and M. Wattenberg, "Fuzzy commitment scheme," *Proceedings of the ACM Conference on Computer and Communications Security*, pp. 28–36, 1999, doi: 10.1145/319709.319714.

[9] H. Feng and C. C. Wah, "Private key generation from on-line handwritten signatures," *Information Management and Computer Security*, vol. 10, no. 4, pp. 159–164, 2002, doi: 10.1108/09685220210436949/FULL/XML.

[10] B. Chen and V. Chandran, "Biometric based cryptographic key generation from faces," *Proceedings - Digital Image Computing Techniques and Applications: 9th Biennial Conference of the Australian Pattern Recognition Society, DICTA 2007*, pp. 394–401, 2007, doi: 10.1109/DICTA.2007.4426824.

[11] S. V. K. Gaddam and M. Lal, "Efficient Cancellable Biometric Key Generation Scheme for Cryptography," *International Journal of Network Security*, vol. 11, no. 2, pp. 61–69, 2010.

[12] N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle, "Generating cancelable fingerprint templates," *IEEE Trans Pattern Anal Mach Intell*, vol. 29, no. 4, pp. 561–572, Apr. 2007, doi: 10.1109/TPAMI.2007.1004.

[13] C. Rathgeb and A. Uhl, "Special Issue: Future Trends in Biometric Processing Context-based biometric key generation for Iris," 2010, doi: 10.1049/iet-cvi.2010.0176.

[14] D. Salman, R. Azeez, and A. M. Hossen, "Key Generation from Multibiometric System Using Meerkat Algorithm," *Engineering and Technology Journal*, vol. 38, no. 3B, pp. 115–127, Dec. 2020, doi: 10.30684/ETJ.V38I3B.652.

[15] D. Salman, R. Azeez, and A. Abdul-hossen, "BUILD CRYPTOGRAPHIC SYSTEM FROM MULTI-BIOMETRICS USING MEERKAT ALGORITHM," *Iraqi Journal for Computers and Informatics*, vol. 45, no. 2, pp. 1–8, Dec. 2019, doi: 10.25195/IJCI.V45I2.46.

[16] Z. O. Ahmed and A. A. Khorsheed, "Biometric key generation using crow algorithm," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 21, no. 1, pp. 208–214, Jan. 2021, doi: 10.11591/IJEECS.V21.I1.PP208-214.

[17] Z. Ibrahim, A. Al-Rifaee, T. Z. Ismaeel, D. Samir, and I. Abood, "Cryptography based on Fingerprint Bio Metrics", doi: 10.58346/JISIS.2024.I4.025.

[18] Z. I. A. Alrifaee and T. Z. Ismaeel, "Cryptography based on retina information," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 28, no. 3, pp. 1697–1708, Dec. 2022, doi: 10.11591/IJEECS.V28.I3.PP1697-1708.

[19] F. M. Baqer, S. Albermany, F. M. Baqer, and S. Albermany, "EEG Authentication System Using Fuzzy Vault Scheme," Feb. 2022, doi: 10.5772/INTECHOPEN.102699.

[20] A. Juels and M. Sudan, "A fuzzy vault scheme," *Des Codes Cryptogr*, vol. 38, no. 2, pp. 237–257, Feb. 2006, doi: 10.1007/S10623-005-6343-Z.

[21] U. Uludag, S. Pankanti, and A. K. Jain, "Fuzzy vault for fingerprints," *Lecture Notes in Computer Science*, vol. 3546, pp. 310–319, 2005, doi: 10.1007/11527923_32.

[22] K. Nandakumar and A. K. Jain, "Multibiometric template security using fuzzy vault," *BTAS 2008 - IEEE 2nd International Conference on Biometrics: Theory, Applications and Systems*, 2008, doi: 10.1109/BTAS.2008.4699352.

[23] L. You, Y. Wang, Y. Chen, Q. Deng, and H. Zhang, "A novel key sharing fuzzy vault scheme," *KSII Transactions on Internet and Information Systems*, vol. 10, no. 9, pp. 4585–4602, 2016, doi: 10.3837/tiis.2016.09.030.

[24] S. Barman, D. Samanta, and S. Chattopadhyay, "Fingerprint-based crypto-biometric system for network security," *EURASIP J Inf Secur*, vol. 2015, no. 1, pp. 1–17, 2015, doi: 10.1186/s13635-015-0020-1.

[25] A. Arakala, J. Jeffers, and K. J. Horadam, "Fuzzy extractors for minutiae-based fingerprint authentication," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 4642 LNCS, no. October, pp. 760–769, 2007, doi: 10.1007/978-3-540-74549-5_80.

[26] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," *SIAM Journal on Computing*, vol. 38, no. 1, pp. 97–139, 2008, doi: 10.1137/060651380.

[27] X. Boyen, "This expanded," 2004.

[28] J. Ma, B. Qi, and K. Lv, "Threshold reusable fuzzy extractor and an application to joint access control via biometric information," *Inf Sci (N Y)*, vol. 579, pp. 525–540, Nov. 2021, doi: 10.1016/J.INS.2021.08.021.

[29] R. Canetti, B. Fuller, O. Paneth, L. Reyzin, and A. Smith, "Reusable Fuzzy Extractors for Low-Entropy Distributions," *Journal of Cryptology*, vol. 34, no. 1, 2021, doi: 10.1007/s00145-020-09367-8.

[30] N. Li, F. Guo, Y. Mu, W. Susilo, and S. Nepal, "Fuzzy Extractors for Biometric Identification," *Proc Int Conf Distrib Comput Syst*, pp. 667–677, Jul. 2017, doi: 10.1109/ICDCS.2017.107.

[31] J. Bringer, H. Chabanne, and A. Patey, "Privacy-preserving biometric identification using secure multiparty computation: An overview and recent trends," *IEEE Signal Process Mag*, vol. 30, no. 2, pp. 42–52, 2013, doi: 10.1109/MSP.2012.2230218.

[32] B. Sy, "Secure computation for privacy preserving biometric data retrieval and authentication," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 5376 LNCS, pp. 143–154, 2008, doi: 10.1007/978-3-540-89900-6_16/COVER.

[33] M. Barni, G. Droandi, R. Lazzeretti, and T. Pignata, "SEMBA: secure multi-biometric authentication," *IET Biom*, vol. 8, no. 6, pp. 411–421, Nov. 2019, doi: 10.1049/IET-BMT.2018.5138.

[34] M. Barni, G. Droandi, and R. Lazzeretti, "Privacy Protection in Biometric-Based Recognition Systems: A marriage between cryptography and signal processing," *IEEE Signal Process Mag*, vol. 32, no. 5, pp. 66–76, Sep. 2015, doi: 10.1109/MSP.2015.2438131.

[35] P. Strzelczyk, "Privacy Preserving and Secure Iris-Based Biometric Authentication for Computer Networks," *Journal of telecommunications and information technology*, 2011.

