# Encryption Keys Generation Based on Bio-Cryptography Finger Vein Method

Tomas Trainys
Computer Department,
Kaunas University of Technology,
Kaunas, Lithuania
tomas.trainys@ktu.edu

Algimantas Venčkauskas
Computer Department,
Kaunas University of Technology,
Kaunas, Lithuania
algimantas.venckauskas@ktu.lt

***Abstract*— Bio-cryptography is a field that combines cryptography with biometrics. The use of biometric methods in cryptography is a widely researched area. The main goal of bio-cryptography is a derivation of stable encryption keys from biometric data. This article is initial phase for developing method based on multiple representations of finger vein modality patterns combined with a pseudo password is discussed in this article for Cryptographic Key generation. Finger veins are hidden biometric attributes that resides under the skin surface which are invisible to the naked eye. The desirable characteristics of finger vein such as universality, distinctiveness, permanence and acceptability makes it a suitable biometric for the key generation process. Cryptographic key generated from the biometric template of an individual can be used as a personal key to encrypt and decrypt information for secure transmission. The key idea of the discussed method is to generate permanent keys from the finger vein network that could be combined into sequences and applied to data encryption. These keys can be used in many real time applications for secure data transmission or authentication.**

***Keywords - Bio - cryptographic, Information security, Biometrics, Finger Vein, Fuzzy vault and password hardening schema, Key generation.***

## I. INTRODUCTION

Nowadays information security is essential to ensure data secrecy and authenticity of messages to prevent it from undesirable users and intruders. Cryptography plays an important role for information security during transfer or storing with the help of cipher keys. Simple keys (password, PIN) are very easy to memorize as well as easy to crack. Complex keys provide more security and they are difficult to crack. However, such keys must be stored in protected, secure storage as it is difficult to remember them. Therefore, there is a risk of losing such keys, they may be stolen or illegally transferred to third parties [1].

One of the solutions to these problems are bio - cryptography techniques, which are the combination of biometrics and cryptography [2].

Biometric methods are based on the human body's permanent and unique physiological characteristics, such as fingerprint, palm geometry, hand vein, iris, finger vein, or face features. Behavioral traits such gait, typing, speech, signature writing characteristics and keys stroke dynamics are the ones that an individual can have [2], [3]. Those characteristics holds identity of each individual witch are embedded in a human's body. Todays, biometric methods are widely used for security purposes for symmetric and asymmetric crypto systems (bioPKI) [4], [5] as well as data encryption, key generation or authentication and identification [6], [7], as it is more secure and convenient to use.

Biometrics increases the security of the system and offers advantages over knowledge and possession based approaches because there is not needed to remember, biometric attributes cannot be lost, stolen, it offers better security due to the fact that biometric features are hard enough to forge and require the presence of the genuine user to grant access to a particular resource [2], [8].

The bio-cryptographic approach gives an opportunity to increase security and convenience to use it in many applications like access control, financial transactions, mobile devices, ATMs, etc.; it ensures biometric systems overarching security policy and architecture [9].

Biometric cryptosystems are mainly categorized in to two groups: key generation system or a key binding system. In a key binding case, the system randomly generates cryptographic keys and binds them to the biometric template. Key generation systems produce a cryptographic key from certain acquired biometric data [7]. It covers a high level of security provided by cryptography and non-repudiation provided by biometrics. Bimodality systems are categorized in the unimodal and multimodal. In unimodal system architecture a single biometric sample is used which typically is acquired from one type of sensor. Multimodal combines at least two modalities i.e. finger vein and finger print, face and eye etc. in other words they could be called multi sensor systems [10]–[12]. According to the latest research multi sensor systems are operational and offer several additional security advantages such as good entropy when used to derive encryption keys, non-repudiation and negative recognition, improves matching accuracy, more resistant to spoofing [9], [13], [14], reduces

noisy data, reduces false rejection rate (FRR) and false acceptance score (FAR) [15].

The main components of biometric systems are: Sensor module – typically a camera to obtain raw data from the user, in case of blood vessels, this is done by illuminating blood vessels and capturing the image.

Feature extraction module – to obtain the minutiae point from an acquired image [16], [17]; Storage module, for storing biometric data; Matching and decision module – to perform verification of the user and make decision based on defined scores [18], [19].

In order to implement biometrics systems, the main focus is solving security issues such as integrity, and reliability of the system. Systems should provide enough entropy and stabile bio-keys. According to different researches related to security issues of biometric systems, most prevent attacks are based on the presentation of fake biometrics, the replay of previously captured biometric samples and stolen data [20], [21].

The main problem of Bio-cryptography is to generate a random cryptographic key with sufficient length and entropy [22]. It is related to the quality of the vein image witch effects recognition performance, i.e. blur of sample, what is related to the strong noise, it makes significant effect to the accuracy. For instance the main issue with the Finger vein method are: susceptibility to the environmental conditions such as fluctuation of temperature, dust, shading etc. [23], image quality. To solve it an implementation of a mechanism for eliminating loss of data during the data processing stage is needed [24], [25]. Therefore stabilization and error control mechanisms are needed to be implemented [24], [25]. Moreover, recognition performance is related to skin properties such as pigmentation, illumination, positioning. The finger veins method has advantages: it is non-contact; finger vein patterns are not influenced by surface conditions; non-invasive and contactless data capture; convenience to use; acceptable for the user; safe - finger vein patterns can only be identified on a live body and it is patterns are internal features that are difficult to forge; small device size.

The main issues we are going to solve are: achieve high Key entropy, generation of strong cryptographic keys resistant to brute-force attacks, aggregating features and parameters from individuals with not less than 256 bits, GAR 99.9 %.

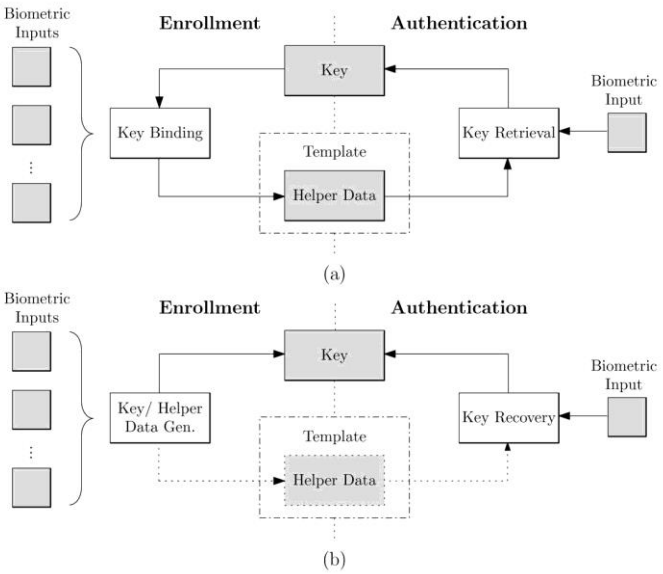
In this paper there is considered new key generation method based on Fuzzy vault and password hardening schema, using multiple representation of finger vein patterns combined with a password (password hardening technique) to generate a cryptographic key, which could be used as for data encryption as well as for authentication. This paper covers the news method (last five years) as an investigation for a further research. This stage covers the only review of biometric systems, methods for generating crypto key based on biometric modalities. We are summarizing our previous work and setting goals for a feature investigation.

The parts of the paper are organized as follows. An overview of biometric cryptosystems and key generation methods are discussed in Section II. The survey of related works methods provided in Section III. Our proposed methodology for the generation of cryptographic key in Section IV. Conclusion of this paper is provided in Section V. Future work in section VI.

## II. BIOMETRIC CRYPTOSYSTEMS

Biometric encryption is a method which combines cryptography with biometric by storing the cryptographic key in a trusted container. In such systems cryptography provides different security levels for non-repudiation, identity verification, and key release. In other words it is pattern recognition applications that acquire biometric data from an individual, extract feature sets, compare this feature set against the feature set stored in the database, and gives the result of the comparison [7]. The key can be released the only after successful biometric verification and then enters a cryptosystem. In other words, biometric encryption is a double-layered security scheme, in which biometric data is used as the key to grant access to the cryptographic key in the first layer and then the cryptographic key is used to unlock the second layer of the security system [1]. Such as techniques provides a binding between a cryptographic key and a biometric vault scheme [26]. The functioning of different schemas presented in Fig. and comparison in Table I.

Figure 1. Key binding (a), Key generation (b) schemas, *(obtained from [7])*




### A. *Key-binding Biometric Cryptosystem*

Key-binding schema uses techniques to create secure template from bio modality template. An approach is called key-binding because it uses the independent secret key which is linked to the biometric data (Fig. 1). That key in the system is presented as a helper data. Helper data – it is user specific key and it's independent from the biometric data. During a key derivation process the helper data Crypto keys are revocable because they are not associated to biometric information. This is called biometric encryption. It is impossible to extract secret

key or biometric data from templates stored in such systems [7], [27]. When entering a user's data, a new key is generated in the system, so the user does not need to remember it. As key is not in related to biometric data, it can be changed.

In case of loss it does not reveal information about the secret user biometric properties. After creating a user's private template that holds a secret key and biometric data, the original biometric template and generated key are no longer needed and can be destroyed.

### *B. Key generation Biometric Cryptosystem*

The key-generating scheme (Fig. 1) is a method based on helper data, is allows derivation and generation of keys from the helper data. System doesn't store real template but the only intermediate data, which is called Helper data. It is the only associated biometric data to the real template. Helper is generated during template enrolment phase. The cryptographic keys are generating from the created helper data. There are proposed two schemes Fuzzy extractors and Secure sketches which allow secure keys to be generated from the helper data [24], [28]. Secure sketch [29] is a method mainly for decreasing fall tolerance to the errors. Fuzzy extractor [24] solves incapability and error tolerance issues. It is applicable for generating random bit string from the enrolled biometric template and controls errors.

### *C. Hybrid Biometric Cryptosystems*

Hybrid schemas are used as a combination of different schemas; it provides higher privacy and security. For instance Cancellable [30] and Secure sketch [31] applying secure sketch error correction mechanism to the transformed templated, authors of an article have achieved better performance and security results. Another instance [32] for hardening Fuzzy vault with password solution enhanced security for authenticating users and gives better protects from brute force attacks if an attacker will grands rights to overlap two different versions of the fuzzy vault of the same person performing statistical analysis. Authors [33] Cai et. al. demonstrate how to combine Fuzzy vault and Cancellable biometric schemas, transforming minutiae structures before coding. Combination of two mentioned schemas provides enhancement of the features and protection against cross matching attacks.

TABLE I. COMPARISON OF EXISTING METHODS

| **Type** | ***Method*** | ***Operation mode*** | ***Strength/Weakness*** |
|---|---|---|---|
| Key-binding | Bio-encryption [1] | Template matching | Strength: Encrypted template; Weakness: possible substitution attacks |
| | Fuzzy commitment [34] | Key binding and release; Helper data | Strength: high protection of bio-data; ECC codes [24] Weakness: reconstruction of bio-data form template if secret key is disclosed |
| | Fuzzy vault [26] | Secret key; Minutiae points | Strength: ECC code, Polynomial encoding; Weakness: Brute force attacks |
| | Shielding function [7] | Helper data; Random key | Strength: Hash function; Weakness: Brute force attacks |
| Key generation | Fuzzy extractor [1] | Helper data; Random keys | Strength: eliminates template; secure bio-data Weakness: no revocable keys |
| | Secure sketch [29] | Helper data; Quantization of features | Strength: do not stored template Weakness: attacks via records |
| Hybrid | Fuzzy vault and password hardening [32] | Secret key | Strength: improved vault security, higher entropy |
| | Cancellable and Secure sketch [31] | Template transform | Strength: ECC code, features transform |
| | Fuzzy vault and Cancellable [33] | Regional transform; Feature vector | Strength: ECC code, features transform, higher entropy |

## III. RELATED WORKS

This section provides an assessment of different latest key generation methods proposed by authors. Analyzed works related to the various modalities, provided results of their achievement (Table II).

Ushmaev et. al. [35] proposed Topological fingerprint pattern minutiae point neighborhood descriptors method based approach. Topological descriptors are very stable fingerprint features; it doesn't depend on finger alignment and elastic deformations. The approach allows varying decryption rates and key lengths. Key length up to 512 bit. GAR 97, 25%.

Method proposed by Hu et al. [36] generates cryptographic keys from uncertain biometrics. For testing authors have used fingerprint modality. After testing has been found, that information integrity of the original fingerprint image can be significantly compromised by image rotation transformation process. Quantization and interpolation process can change the fingerprint features significantly without affecting the visual image.

Venčkauskas et. al. [22] propose method for generating complex cryptography keys from finger vein minutiae points using several instances of finger vein patterns and combining them with a password. Moreover authors proposed algorithms for vessel beginnings and end points detection coordinates detection and contour tracing.

R. Ranjan et. al. [37] proposed Divide and Conquer method for key generation from fingerprint. Method can be extended to any kind of biometric key or template matching. Proposed algorithm instead of comparing the whole key or template compares the threshold of the sub-key or sub-template. This approach increases the security as well as decreases the effect of biometric variation and does not require fingerprint alignment during authentication. For example if some parts of the person's fingerprint is damaged, or dirty it can be still be processed.

Sheng et.al. [38] developed scheme uses variations on both single features and feature subsets with the purpose of recovering a large number of consistent and discriminative feature elements for key generation based on handwritten signatures modality. This can be used together with the bio salting (password) technique by adding with other information (e.g., PIN, user name, email etc.) to make them even harder to decode.

Panchal et. al. [39] proposed method to generate randomness in cryptography. The method provides better security. Authors have reached 97,25% GAR result. This approach is based on quantization schema; it creates every time different keys based on the impression captured from the scanner. Authors got the same biometric cryptography key from the fingerprints captured from different scanners with different quality. Proposed method not generates high entropy keys and do not store the original biometric data, therefore it prevents to recover the biometric data even if the system is opened to an attacker.

Proposed FVHS method by Wu et. al. [40] is based on machine learning technique, mining feature vector from finger vein patterns. The main advantage of algorithm that it performs correlation between each of biometric feature, self-stabilization and provides high dimensional space to generate key. Method allows generating stabile bio-keys with GAR more then 99, 9% and FAR less than 0, 8%. Key strength is up to 256 bits.

The method proposed by Abuguba et. al. [41] is based on a multimodal approach using iris and face modalities. For features extraction authors used PCA for face and 2-D real Gabor filters for iris. Crypto key generated from iris and face biometric reached 256 bits length.

Panchal et. al. proposed a method [42] based on cancellable biometrics template, code-word generation using Reed-Solomon encoding. Reed-Solomon encoding has been used to maintain the code-word and generation of the key and SVM based ranking mechanism for user verification. In this approach, fingerprint features and the sketch data is stored in a server. The key is generated and bound during encoding phase. The length of the key is 1024 bits, GAR 99.27%, FAR 0, 14%. This method can be used for key generation and authentication.

An approach based on the Fuzzy commitment schema [43] shows that a key with the length of 400 bits per iris, FRR 3.75% and FAR can be generated. Authors Adamovic et. al. use Reed Salamon code for error detection and correction, interleaving permutation is demonstrated in their proposed fault tolerant schema.

Authors Zainon et. al. [44] proposed a new method for a master and child key generation based on Bitcoin Improvement Proposal 32(BIP32) - Ed25519 scheme [45], using the palm vein network, their proposed method will be applicable for authentication purpose. For each instance of use, a new child key will be generated. Such key release method will prevent form spoofing and reply attacks.

Verma et. al. [46] proposed a one-time key use method based on a direct key generation approach, using hash functions (MD5, SHA-512) for key generation. The authors have conducted verification of the method and have achieved 512 bits length key using fingerprint modality minutiae points. After comparison of the key generation from alphanumeric and biometric, results indicate that entropy Mean Square Error rate is 2-3% higher when the key is generated from biometric minutiae points.

TABLE II. COMPARISON OF EXISTING WORKS

| **Article** | ***Modality*** | ***Key generation methods*** | ***Results*** |
|---|---|---|---|
| Ushmaev et al. [35] | Fingerprint | Random | Key length 512 bit. GAR 97, 25% |
| Hu et al. [36] | Unimodal | Key binding and release | Method |
| R. Ranjan et. al. [37] | Fingerprint | Random key binding | Method |
| Venčkaus kas et. al. [22] | Finger vein | Random key | Method |
| Sheng et.al. [38] | Handwritten signatures | Clustering, bio-salting | Method |
| Panchal et. al. [39] | Fingerprint | Key binding | GAR 97,25% |
| Wu et. al. [40] | Finger vein | Key binding and release | GAR 99.9%, FAR 0.8, Key length 256 |
| Abuguba et. al. [41] | Iris, face | Key binding and release | Key length 256 |
| Panchal et. al. [42] | Fingerprint | Secret key | GAR 99.27%, FAR 0.14%, Key length 1024 bits. |
| Adamovic et. al. [43] | Iris | Random key | FRR 3.75%, FAR 0.14%, Key length 400 bits. |
| Zainon et. al. [44] | Palm vein | Random, Master and child keys | Method, RIO accuracy 98.3% |
| Verma et. al. [46] | Fingerprint | Random | Method, key length 512 bits |

## IV. PROCESS FOR KEY GENERATION FROM FINGER VEIN NETWORK

In this section we present a process of key generation which is based on Fuzzy vault schema and ostensible password hardening techniques. In this solution the multiple representations of the same modality - finger vein patterns combined with a password hardening technique are foreseen to be used. The solution is going to be based on a Hybrid type implementing Fuzzy vault and password hardening techniques (Table III). The expected result – a generated cryptographic key, 256 bits in length, which could be used for data encryption as well as for authentication.

TABLE III. DESCRIPTION OF METHOD

| **Bio-Crypto System** | ***Method*** | ***Operation mode*** | ***Strength/Weakness*** |
|---|---|---|---|
| Hybrid | Fuzzy vault and password hardening | Secret key | Strength: improved vault security, higher entropy, one type of sensor. |

The password is emulated by providing different finger sequences to the system. The system will be designed for 10 different finger vein patterns, extracting minutiae points, fusing them to one feature vector and storing it to the system vault which allows the usage of key generation. Since it is intended

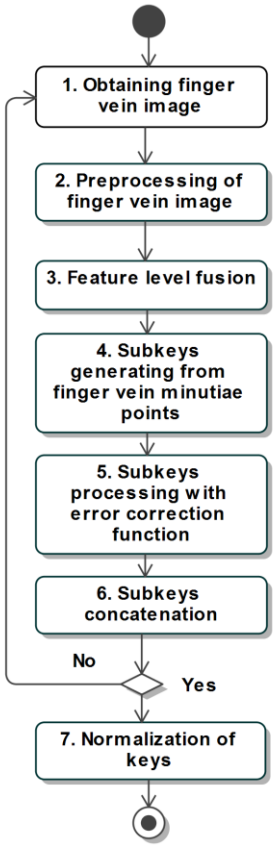
to use up to ten instances of the same modality, this should allow for a higher level of entropy key to be generated.

Method for key generation is obtained and extended from previous article [22], this work part is an extension .

A schematic representation of process for cryptographic key generation from finger vein patterns is presented in Figure 2. The process consists of seven steps:

1. Finger vein image is acquired by capturing image with image sensor. Because deoxygenated hemoglobin in the veins absorbs light, veins will appear darker in all region [47]. Ten fingers can be used to compose a set of images for obtaining finger vein patterns. Finger has a number from 1 to 10, by finger sequence to the system; fingers are mapped to the numbers. Such a pseudo identification number is emulated. Further process contains: extraction of center of position of veins; calculation of curvatures; detection of vein centers and assigning scores to the center position; calculating veins endings. Finally, calculation of all profile for feature set acquisition. For experimentation finer vein database FV-USM [48] will be used.
2. Obtained vein samples application for the digital image preprocessing operations which make images more suitable for features extraction. In this step these operations are performed: de-noising, smoothing, background subtraction, lines detection, pattern normalization segmentation and pattern extraction operations [49]. For that purpose *Repeated Contour Tracing Algorithm, Gabor filter, Maximum Curvature, Wide Line detector and Scale Invertible Feature Transforms* methods are going to be implemented.
3. Extracted features are fused to one feature vector at Feature level by adopting *Support Vector Machine* approach. The approach allows ranking and combining heterogeneous feature sets to the one vector [10]. Fused feature sets are used for generating partial subkeys.
4. Subkeyes are obtained using key derivation function (KDF) which uses input data to derive key material for cryptographic algorithm [50]. The process consists of performing key derivation rounds by applying operations such as XOR, Transpose and shifting.
5. *Error Correcting Code* (ECC) [24] method is used to reduce the variability of biometric data. This mechanism is necessary because of the leading errors in the information transmission channel, in this case by scanning the finger vein network. This usually occurs due to finger positioning or lighting and reflections. Using error correction codes, we can restore damaged pieces of information. The most commonly used algorithm for calculating the minimum distance between any two code units is the application of the BCH [24] code correction algorithm for solving this problem. BCH algorithm solves errors at the bit level.
6. Partial cryptographic keys are concatenated to combine a final cryptographic key by applying KDF operations for generating symmetric key. [50].
7. Generated variable length cryptographic key is normalized using key derivation functions [51]

Figure 2. Process diagram of Cryptographic key generation using finger vein patterns




## V. INVESTIGATION AND DISCUSSION

Steps 1 and 2 for proposed cryptographic key generation have been implemented and tested in the previewed work [22], a set of feature points in the vascular pattern were calculated. In this article we are providing insights for the future work.

Looking from the perspective of security and the cost of implementation of the solution, the advantages are ease of use, since the scanner is compact, without the need for additional hardware (keyboards) to enter numerical values. The solution fulfills the European Union security requirement for the personal data protection [52]. In the case of realizations of this solution, this regulation would be ensured because the finger vein images that provide unique information about person would not be stored but only the feature sets obtained during the processing phase. In case of system's compromise, when a third party gets data there is no way to restore the original biometric data. It allows usage of several factors for identification: what I know; what I have and what I am and only one device is needed.

## VI. CONCLUSION AND FUTURE WORK

In this article the latest conducted research in the bio-cryptography field related to the task of this article were analyzed. Different Bio Cryptography approaches were analyzed and differences between functionality modes, strengthens and weaknesses were discussed. A solution described in this article has advantages because we can use it like a multimodal solution - it needs less equipment, each finger can represent a number thus no keyboard is needed. There is no need to implement liveness detection mechanism because veins can be only be detected in the live body and that's difficult to forge.

In further research it is envisaged to analyze fusion modes at the data level, decision methods, to build a prototype for combining feature level features vector with a password and to create an algorithm for automating the processes and conduct experiment.

## REFERENCES


[1] N. I. Udzir, A. Abdullah, and R. Mahmod, "State of the Art in Biometric Key Binding and Key Generation Schemes," *International Journal of Communication Networks and Information Security (IJCNIS)*, vol. 9, no. 3, 2017.

[2] J. A. Unar, W. C. Seng, and A. Abbasi, "A review of biometric technology along with trends and prospects," *Pattern Recognition*, vol. 47, no. 8, pp. 2673–2688, Aug. 2014.

[3] A. Lumini and L. Nanni, "Overview of the combination of biometric matchers," *Information Fusion*, vol. 33, pp. 71–85, Jan. 2017.

[4] D. B. Ojha and A. Sharma, "A fuzzy commitment scheme with McEliece's cipher," *Survey in Mathematics and Its Application*, vol. 5, pp. 73–83, 2010.

[5] C.-J. Chae, K.-N. Choi, K. Choi, J.-S. Kim, and Y. Shin, "Enhanced biometric encryption algorithm for private key protection in BioPKI system," *Journal of Central South University*, vol. 21, no. 11, pp. 4286–4290, Nov. 2014.

[6] M. Khalil-Hani, M. N. Marsono, and R. Bakhteri, "Biometric encryption based on a fuzzy vault scheme with a fast chaff generation algorithm," *Future Generation Computer Systems*, vol. 29, no. 3, pp. 800–810, Mar. 2013.

[7] C. Rathgeb and A. Uhl, "A survey on biometric cryptosystems and cancelable biometrics," *EURASIP Journal on Information Security*, vol. 2011, no. 1, p. 3, Sep. 2011.

[8] C. Champod and M. Tistarelli, "Biometric Technologies for Forensic Science and Policing: State of the Art," in *Handbook of Biometrics for Forensic Science*, M. Tistarelli and C. Champod, Eds. Cham: Springer International Publishing, 2017, pp. 1–15.

[9] M. I. Gofman, S. Mitra, T.-H. K. Cheng, and N. T. Smith, "Multimodal biometrics for enhanced mobile device security," *Communications of the ACM*, vol. 59, no. 4, pp. 58–65, 2016.

[10] L. M. Dinca and G. P. Hancke, "The Fall of One, the Rise of Many: A Survey on Multi-Biometric Fusion Methods," *IEEE Access*, vol. 5, pp. 6247–6289, 2017.

[11] A. Razaque, P. S. Sreeramoju, F. H. Amsaad, C. K. Nerella, M. Abdulgader, and H. Saranu, "Multi-biometric system using Fuzzy Vault," 2016, pp. 0122–0126.

[12] A. K. Jain, K. Nandakumar, and A. Nagar, "Biometric Template Security," *EURASIP Journal on Advances in Signal Processing*, vol. 2008, no. 1, p. 579416, 2008.

[13] R. Gad, N. El-Fishawy, A. El-Sayed, and M. Zorkany, "Multi-Biometric Systems: A State of the Art Survey and Research Directions," *International Journal of Advanced Computer Science and Applications*, vol. 6, no. 6, 2015.

[14] W. Yang, S. Wang, J. Hu, G. Zheng, and C. Valli, "A fingerprint and finger-vein based cancelable multi-biometric system," *Pattern Recognition*, vol. 78, pp. 242–251, Jun. 2018.

[15] S. Abuguba, M. M. Milosavljevic, and N. Macek, "An efficient approach to generating cryptographic keys from face and iris biometrics fused at the feature level," *International Journal of Computer Science and Network Security (IJCSNS)*, vol. 15, no. 6, p. 6, 2015.

[16] R. Rajan and M. G. Indu, "A novel finger vein feature extraction technique for authentication," 2014, pp. 1–5.

[17] I. Malik and R. Sharma, "Analysis of different techniques for finger-vein feature extraction," *Int. J. Comput. Trends Technol.(IJCTT)*, vol. 4, no. 5, 2013.

[18] Hyung Hong, Min Lee, and Kang Park, "Convolutional Neural Network-Based Finger-Vein Recognition Using NIR Image Sensors," *Sensors*, vol. 17, no. 6, p. 1297, Jun. 2017.

[19] G. Yang, R. Xiao, Y. Yin, and L. Yang, "Finger Vein Recognition Based on Personalized Weight Maps," *Sensors*, vol. 13, no. 12, pp. 12093–12112, Sep. 2013.

[20] H. Zhang, W. Han, X. Lai, D. Lin, J. Ma, and J. Li, "Survey on cyberspace security," *Science China Information Sciences*, vol. 58, no. 11, pp. 1–43, Nov. 2015.

[21] A. K. Jain, K. Nandakumar, and A. Nagar, "Biometric template security," *EURASIP Journal on advances in signal processing*, vol. 2008, p. 113, 2008.

[22] A. Venckauskas and P. Nanevicius, "Cryptographic key generation from finger vein," 2013.

[23] Hyung Hong, Min Lee, and Kang Park, "Convolutional Neural Network-Based Finger-Vein Recognition Using NIR Image Sensors," *Sensors*, vol. 17, no. 6, p. 1297, Jun. 2017.

[24] H. S. G. Pussewalage, J. Hu, and J. Pieprzyk, "A survey: Error control methods used in bio-cryptography," 2014, pp. 956–962.

[25] A. B. J. Teoh and J. Kim, "Error Correction Codes for Biometric Cryptosystem", vol. 32, no. 6, pp. 39–49, 2015.

[26] A. Juels and M. Sudan, “A fuzzy vault scheme,” *Designs, Codes and Cryptography*, vol. 38, no. 2, pp. 237–257, 2006.
[27] N. Wang, Q. Li, A. A. Abd El-Latif, J. Peng, X. Yan, and X. Niu, “A novel template protection scheme for multibiometrics based on fuzzy commitment and chaotic system,” *Signal, Image and Video Processing*, vol. 9, no. S1, pp. 99–109, Dec. 2015.
[28] E. Chandra and K. Kanagalakshmi, “Cancelable biometric template generation and protection schemes: A review,” 2011, pp. 15–20.
[29] Y. Sutcu, Q. Li, and N. Memon, “Secure Sketches for Protecting Biometric Templates,” in *Security and Privacy in Biometrics*, P. Campisi, Ed. London: Springer London, 2013, pp. 69–104.
[30] W. Yang, S. Wang, J. Hu, G. Zheng, and C. Valli, “A fingerprint and finger-vein based cancelable multi-biometric system,” *Pattern Recognition*, vol. 78, pp. 242–251, Jun. 2018.
[31] J. Bringer, H. Chabanne, and B. Kindarji, “The best of both worlds: Applying secure sketches to cancelable biometrics,” *Science of Computer Programming*, vol. 74, no. 1–2, pp. 43–51, Dec. 2008.
[32] F. Benhammadi and K. Beghdad Bey, “Password hardened fuzzy vault for fingerprint authentication system,” *Image and Vision Computing*, vol. 32, no. 8, pp. 487–496, Aug. 2014.
[33] C. Li and J. Hu, “A security-enhanced alignment-free fuzzy vault-based fingerprint cryptosystem using pair-polar minutiae structures,” *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 3, pp. 543–555, 2016.
[34] A. Juels and M. Wattenberg, “A Fuzzy Commitment Scheme,” 2013.
[35] O. Ushmaev, V. Kuznetsov, and V. Gudkov, “Extraction of Binary Features from Fingerprint Topology,” 2011, pp. 1–6.
[36] P. Zhang, J. Hu, C. Li, M. Bennamoun, and V. Bhagavatula, “A pitfall in fingerprint bio-cryptographic key generation,” *Computers & Security*, vol. 30, no. 5, pp. 311–319, Jul. 2011.
[37] R. Ranjan and S. K. Singh, “Improved and innovative key generation algorithms for biometric cryptosystems,” 2013, pp. 943–946.
[38] W. Sheng, S. Chen, G. Xiao, J. Mao, and Y. Zheng, “A Biometric Key Generation Method Based on Semisupervised Data Clustering,” *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 45, no. 9, pp. 1205–1217, Sep. 2015.
[39] G. Panchal and D. Samanta, “Comparable features and same cryptography key generation using biometric fingerprint image,” 2016, pp. 691–695.
[40] Z. Wu, L. Tian, P. Li, T. Wu, M. Jiang, and C. Wu, “Generating stable biometric keys for flexible cloud computing authentication using finger vein,” *Information Sciences*, 2016.
[41] S. Abuguba, M. M. Milosavljevic, and N. Macek, “An efficient approach to generating cryptographic keys from face and iris biometrics fused at the feature level,” *International Journal of Computer Science and Network Security (IJCSNS)*, vol. 15, no. 6, p. 6, 2015.
[42] G. Panchal and D. Samanta, “A Novel Approach to Fingerprint Biometric-Based Cryptographic Key Generation and its Applications to Storage Security,” *Computers & Electrical Engineering*, Feb. 2018.
[43] S. Adamovic, M. Milosavljevic, M. Veinovic, M. Sarac, and A. Jevremovic, “Fuzzy commitment scheme for generation of cryptographic keys based on iris biometrics,” *IET Biometrics*, vol. 6, no. 2, pp. 89–96, Mar. 2017.
[44] N. A. F. M. Zainon and S. A. Razak, “Master and child key generation from palm vein,” 2017, pp. 37–41.
[45] D. Khovratovich and J. Law, “BIP32-Ed25519: Hierarchical Deterministic Keys over a Non-linear Keyspace,” in *Security and Privacy Workshops (EuroS&PW), 2017 IEEE European Symposium on*, 2017, pp. 27–31.
[46] I. Verma and S. Jain, “Biometric based key-generation system for multimedia data security,” in *2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom)*, 2016, pp. 864–869.
[47] N. Miura, A. Nagasaka, and T. Miyatake, “Extraction of finger-vein patterns using maximum curvature points in image profiles,” *IEICE TRANSACTIONS on Information and Systems*, vol. 90, no. 8, pp. 1185–1194, 2007.
[48] M. S. Mohd Asaari, S. A. Suandi, and B. A. Rosdi, “Fusion of Band Limited Phase Only Correlation and Width Centroid Contour Distance for finger based biometrics,” *Expert Systems with Applications*, vol. 41, no. 7, pp. 3367–3382, Jun. 2014.
[49] B. Huang, Y. Dai, R. Li, D. Tang, and W. Li, “Finger-vein authentication based on wide line detector and pattern normalization,” in *Pattern Recognition (ICPR), 2010 20th International Conference on*, 2010, pp. 1269–1272.
[50] C. Percival, “Stronger key derivation via sequential memory-hard functions,” *Self-published*, pp. 1–16, 2009.
[51] C. J. Mitchell and A. W. Dent, “International standards for stream ciphers: A progress report,” *SASC-The State of the Art of Stream Ciphers. Brugge, Belgium: Novotel Brugge Centrum*, pp. 14–15, 2004.
[52] EU Parliament, “Regulation (EU) on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).” 27-Apr-2016.
[53] F. Beritelli, G. Capizzi, G. Lo Sciuto, C. Napoli, and F. Scaglione, "Automatic heart activity diagnosis based on gram polynomials and probabilistic neural networks." Biomedical Engineering Letters, vol. 8, issue 1, pp.77-85, 2018.