The Seybold Report

ISSN 1533-9211

DOI 10.5281/zenodo.7116039

A NOVEL APPROACH FOR DORSAL HAND VEIN RECOGNITION BY USING HYBRID CANCELABLE BIOMETRIC AUTHENTICATION SYSTEM

ANUP RITTI[1] and Dr. RAJAVARMAN.V.N[2]

[1]Research scholar, Department of Computer Science and Engineering, Dr. MGR Educational and Research Institute, Chennai, Tamilnadu, India. Email: anup.ritti66@gmail.com
[2]Professor, Department of Computer Science and Engineering, Dr. MGR Educational and Research Institute, Chennai, Tamilnadu, India. Email: rajavarman.vn@drmgrdu.ac.in

Abstract:

Biometric based authentication systems are being prominently used everywhere. The biometric data, popularly known as a biometric template, is generally stored on the database server in its unprotected form. Unlike passwords, once compromised, biometric data can never be recovered. Cancelable and hybrid biometric cryptosystems are two techniques used to offer protection against the security and privacy challenges faced by users of biometric authentication systems. Various cancelable biometric techniques have been proposed to maintain user data security. A cancelable biometric framework is introduced to satisfy user data security and keeping the original biometric template safe away from intruders. Biometrics like fingerprints and retinas are very vulnerable at the moment. Contactless, and thus impossible to counterfeit, has made the dorsal vein pattern a hot topic these days. This pattern can provide another more reliable biometric that is already in use. Currently, both the academic community as well as sector are paying attention to the results of hand vein patterns towards biometric authentication. This article provides details on the methodology of finding and using important points during data analysis based on different parameters. We would be able to examine the reliability of biometrics by examining hand vein patterns using Cancelable and hybrid biometric authentication system.

Index Terms: Biometrics, Privacy, Security, Hand vein, Cancelable biometrics

1) INTRODUCTION

Biometric recognition has been improved speedily and is almost used in our life daily. The biometric techniques recognize and verify the unique features accurately, rapidly, and appropriately to control the entry process in dedicated systems or applications [1]–[3]. It is essential to control the access process and prevent intruders from compromising or recognizing the original templates.

User Biometrics are divided into physical features and logical features [4], [5]. The unique physical features are defined as the face, iris, retina, palm print, and fingerprint, but the features, which are called logical or behavioural features, are measured by the behaviour of the body and its reaction against the different circumstances such as voice, signature, keystrokes pattern, and walking style.

The person's blood vessels network, known as hand veins, is the most noticeable part of the anatomy. The hand palm vein pattern classifies hand vein patterns. Just like twins do not have the same hand dorsal vein patterns, each individual's hand dorsal vein patterns are unique.

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7116039

Therefore, in order to design a biometric system utilizing the hand dorsal vein pattern, it is absolutely necessary to have this level of uniqueness.

Dorsal hand vein pattern, shown in Fig. 1, is the network of blood vessels under body's skin

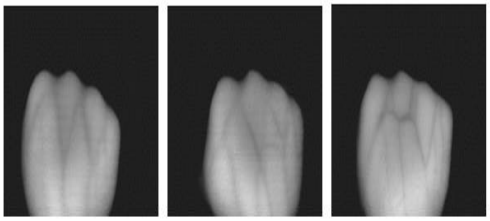

Figure. 1: Hand vein images

Biometric technology is one of the cutting-edge technologies in this digital age to fight cyber-security risk More than half of its biometrics generally dependent on the interaction between the subject and the sensor, for example fingerprints, retinas, or hand geometry. Biometrics parameters such as these were found to be readily traceable and have little dependability. Moreover, hand veins are within the skin, which has no impact on the biometric system's effectiveness. However, the hand dorsal vein pattern fingerprinting method requires physical touch. A common, fast, inexpensive, and accurate biometric system is required for identifying individuals with very little mistake. Biometric identification is competing with other authentication methods such as PIN, passcode, and RFID (or radio frequency identification, a.k.a. "RFID").The distinctive superficial vasculature with in human body is capitalized on using vein pattern feature techniques. Wrist and finger biometrics are less impacted by ageing. It is important to use infrared imaging equipment to properly see these venous patterns. Venous areas in the picture look darker than surrounding tissues because deoxyhemoglobin in the vein collects more infrared.

All of these biometric techniques measured traits or characteristics of our human body, which are employed to verify that no intruders can access or control the access to the services rendered [6]–[8]. Traditionally, tokens and passwords are applied to prevent the cryptographic key from being stolen or compromised for an adequate system or application. Same passwords have been used across various applications by most persons and never vary these tokens to make it easy when applying different long passwords for various applications. If an intruder tries to access the system and a piece of the private password is compromised, it may violate privacy for many services [9]. Institutions look forward to keeping their documents safe and improve a service network to dedicate illegal access to them. Verification and identification are used to confirm that the authorized entry can only get into the correct and secure position. Authentication by traditional techniques, specifically personal identification numbers (PINs) and passwords, has been applied over the years. Nowadays, we have been used magnetic cards and PINs for more safety [10]–[12]. Some disadvantages associated with the traditional ways come up because they identify some characters possessed by the owner rather than recognizing the owner itself, who indeed owned them. These tokens can be exposed by stolen or lost, so any intruder can easily be entered or controlled by the system. There is a new approach in

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7116039

authentication systems that exploit biometrics in various fields as governmental services, commercial applications, knowledge-based systems, tokens-based systems, and applications related to forensic evidence that depend on human-being supervision recognize biometric [13], [14].

Valuable security properties have been achieved by biometric-based authentication techniques, specifically in telemedicine services, to secure user information of offline password attacks [15]. In conventional biometric identification and authentication techniques, cross-matching (diversity) and cross-application invariance are the major challenges that make an obstacle towards these systems because all services and applications involved in user biometrics can be easily hacked, so the information of the users will be easily tracked [16], [17]. Therefore, biometric encryption techniques achieve high privacy with security and uniqueness for authorized individuals. Encryption keys provide increased protection to the biometric cryptosystems. In these cryptosystems, the genuine biometric features are not kept directly in the cloud, but they are initially processed and converted into deformed templates called noise templates (encrypted images) [18], [19].

Biometric template techniques are divided into helper data-based schemes and cancelable biometric schemes.

Biometric protection algorithms should achieve three main concepts for privacy, which are:

(1) Unlinkability, where various secured templates must be applied for various services to prevent cross-matching attacks,

(2) Irreversibility, to provide high protection against the recovery of the original biometric templates, and

(3) Confidentiality, which means that the authorized biometric feature must be secured against intruder access. In the helper-data-based method, user information is dependent on the authorized template. In addition to that, helper data provides the recovery and makes the secret key is accessible during the authentication operation.

The most famous techniques for cancelable biometric templates are fuzzy schemes, especially the fuzzy vault scheme involved in the helper-data methodology. In [20], the descriptors of the fingerprint are connected to provide high performance during the matching process and the privacy of a fuzzy fingerprint vault. The obstacles and restrictions that face the key binding scheme during the generation of the converted form of templates and the matches are obtained by exchanging the fuzzy commitment scheme with an error correction code (ECC). In cases of unauthorized attacks, renewability and revocability are the most widespread problems facing the biometric cryptosystems that effectively enter the system and identify the stored template features. Besides, biometric cryptosystems suffer from various attacks [21]. Transformations can be identified as repetitive alterations applied to the original biometric template to convert it to the unrecognized image before being stored. These transformations are one-way functions used for the extracted features that enhance the diversity and unlinkability properties. The same biometric template can be suffered from different

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7116039

transformations for various services to forbidden cross-matching between stored biometrics in various cloud datasets, [22]–[26]. Another type of cancelable biometric system is called a hybrid approach. It combines two or more template protection techniques [27]–[30]. One of the most advanced alternatives to produce a deformed biometric template is to apply data dependent cryptography.

2) LITERATURE REVIEW

Yang et al., [31] proposed a feature-adaptive random projection based method, in which the projection matrixes, the key to the ARM, are generated from one basic matrix in conjunction with local feature slots. The generated projection matrixes are discarded after use, thus making it difficult for the adversary to launch the ARM. Moreover, the random projection in the proposed method is performed on a local-feature basis. This feature-adaptive random projection can mitigate the negative impact of biometric uncertainty on recognition accuracy, as it limits the error to part of the transformed feature vector rather than the entire vector. The proposed method is evaluated on four public available databases FVC2002 DB1-DB3 and FVC2004 DB2. The experimental results and security analysis show the validity of the proposed method.

W. El-Shafai et al., [32] proposed a cancelable biometric framework is introduced to satisfy user data security and keeping the original biometric template safe away from intruders. Thus, our main contribution is presenting a novel authentication framework based on the evolutionary Genetic Algorithm (GA)-based encryption technique. The suggested framework produces an entirely unrecognized biometric template by hiding the whole discriminative features of biometric templates; this is with exploiting the outstanding characteristics of the employed Genetic operations of the utilized encryption technique. Firstly, the GA initiates its search from a population of templates, not a single template. Secondly, some statistical operators are used to exploit the resulting initial population to generate successive populations. Finally, the crossover and mutation operations are performed to produce the ultimate cancelable biometric templates. Different biometric databases of the face and fingerprint templates are tested and analyzed. The proposed cancelable biometric framework achieves appreciated sensitivity and specificity results compared to the conventional OSH (Optical Scanning Holography) algorithm. It accomplishes recommended outcomes in terms of the AROC (Area under the Receiver Operating Characteristic) and the probability correlation distribution between the original biometrics and the encrypted biometrics stored in the database. The experimental results prove that the proposed framework achieves excellent results even if the biometric system suffers from different noise ratios. The proposed framework achieves an average AROC value of 0.9998, an EER (Equal Error Rate) of $2.0243 \times 10{-}4$, FAR (False Acceptance Rate) of $4.8843 \times 10{-}4$, and FRR (False Rejection Rate) of $2.2693 \times 10{-}4$.

Huang et al. [33] proposed a method for dorsal hand vein identification. A new process integrating together holistic and local analysis then hierarchically joint with that from the surface modality, born by a reputable texture operator, that Local Binary Patterns (LBP), Binary Coding (BC) and graph for decision production by Factorized Graph Matching (FGM).

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7116039

Consequences attained are greater than the state-of-the-art ones so far described in works, which proves its efficiency.

Lee et al. [34] suggested a directional filter include different alignments that cutting hand vein patterns and encode hand vein features into binary code by the minimum directional filtering response (MDFR) and classification by Hamming Distance (HD). Also, there are many areas that not contain the vein in the image, which are not important for hand vein identification. To increase accurateness, the regions that not contain the vein are identified through calculating the modification of the minimum filtering. Their suggested approach achieves high accuracy that displays the method is effective for dorsal hand vein identification.

Trabelsi et al. [35] suggested a new hand vein pattern identification process for person recognition. Fixed static texture descriptor known as Circular Difference and Statistical Directional Patterns (CDSDP) is suggested to extract hand vein patterns and Artificial Neural Network (ANN), Feed forward Multilayer Neural Network (FMNN) for classification. The CDSDP is a neighboring circular change with weights combining the statistical directional data of vessels. Experimental display that descriptor depend on CDSDP has improved effective than the earlier descriptors that used in LBP.

Chuang et al. [36] suggested local feature-based hand vein image process depend on minutiae features extraction from venous networks to study the greatest discriminative areas and features of dorsal hand veins for recognition. These minutiae feature contain end points and the curve lines among the two end points as measured beside the edge of the area of attention. In addition, suggest a dynamic pattern tree (DPT) to speed up matching presentation and estimate the feature points discriminatory power for verifying an individual's identity.

3) PROPOSED WORK

The proposed research work is given below:

3.1 Cancelable biometrics

Cancelable biometrics can be defined as "an intentional, repeatable distortion of a biometric signal based on a chosen transform" [37]. The goal of cancelable biometrics is to provide diversity and unlinkability by using different transforms for different applications involving the same set of users. This prevents collision among templates of the same subjects stored in different biometric databases. The approach also provides revocability, which allows administrators to remove a compromised template and reissue a new one based on the same biometric data. Template revocability is achieved by changing the transformation parameters used for the previous enrolment. The security of transformed templates is guaranteed since decryption does not take place during authentication. Rather, the authentication process involves a comparison between the reference and the query templates in the transformed domain. The cancelable approach can be classified as non-invertible transforms and invertible transforms or biometric salting. Both methods apply specific transformation parameters to a biometric feature vector in order to obtain its transformed version.

ISSN 1533-9211

DOI 10.5281/zenodo.7116039

Cancelable Biometrics work by distorting the original biometric template. The comparisons during the authentication phase are performed on the protected or cancelable biometric templates such that no information regarding the original biometric templates is revealed. Cancelable biometrics are broadly classified into Salting and Non-invertible techniques. In Salting, a cancelable template is created by adding an artificial random pattern to the biometric template. GRAY-SALT and BIN-SALT [38] are the two salting approaches. A synthetic pattern is mixed with input iris image using pixel-wise addition or multiplication in the GRAY SALT. BIN-SALT is a similar approach that works on binarized iris images. The strength of noise can affect the performance rate, and security [39]. Jin et al. [40] introduced Bio– hashing. It uses two-factor authentication and combines unique tokens generated from a hash key and user biometric data to secure the biometric data. However, if that unique token is revealed, the security of the system is compromised. Jegede et al. [41] discusses various challenges and open research issues in cancelable biometrics as well as in the combination of cancelable biometrics with biocryptosystems. In [42], the bitwise encryption scheme and fuzzy extractor are combined to generate a cancelable template. High security is provided on the assumption that obtaining access to one biometric template by an attacker is equivalent to getting both biometric templates of the user. Bloom filters have been extensively used in the literature in the domain of biometric security. The application of Bloom filters in biometric template protection is first introduced in [43] and [44] where the Bloom filters based templates are created from the input biometric template. Gomez Barrero et al. [45] proposed a multi-biometric fusion based on the Bloom filter approach where the biometric templates are converted to Bloom filters. A boolean OR operation is performed between the corresponding Bloom filter arrays. An unlinkable and irreversible template protection scheme is proposed in [46] which is based on the Bloom filters. Based on a similar approach, Drozdowski et al. [47] proposed a row-wise permutation of iriscode using a system-generated key.

3.2 Hybrid biometric cryptosystems

Hybrid cryptosystems integrate two or more template protection schemes to create a single biometric cryptosystem. Hybrid techniques rely on the strengths of the component schemes to provide an integrated approach with better security and user privacy. A major drawback of hybrid schemes is that they have higher implementation costs and complexity of operation. A hybrid scheme was created by combining non-invertible transformation and secure sketch [48]. The scheme leverages on the error correcting capability of secure sketch to address low recognition accuracy of non-invertible transformation. The application of the technique to fingerprint yields FRR of 35% and FAR of 5.53%. It also improves the recognition performance without compromising the security of stored templates. Similarly, Bloom filter was also used to transform face templates before securing the transformed templates with the helper data. Bloom filters generate an irreversible template, which helps to increase the security of the scheme. That is, a compromise of the helper data will not reveal original biometric templates. However, the use of bloom filters lowers the recognition performance of the scheme. It is also possible to obtain a hybrid scheme by 'coupling' a fuzzy commitment scheme with fuzzy vault. This method provides good

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7116039

recognition performance (GAR = 95% and FAR = 0.01%) and offers a two-level protection for stored fingerprint templates. Security analysis shows that the hybrid approach increases the min-entropy (a measure of security) of the fuzzy vault from 31 bits to 47 bits. A related work first used fuzzy commitment scheme to encode the true fingerprint minutia before securing the encoded template in a fuzzy vault. Experimental results show that the scheme achieves GAR of 68.5% and FAR of 3.5%, which indicates improved performance accuracy over the baseline study. Template protection techniques such as enhanced biohash and key binding have been integrated to provide a hybrid scheme for securing face templates. Performance analysis shows that the scheme has genuine acceptance rate (GAR) of 97.79% and FAR of 8.32%. The use of BCH encoding as error correction method minimizes the success of brute force attack. In summary, the method achieves improved security, but with a minimal (1-2%) reduction in accuracy. A related work [49] used bio-hashing technique to create non-invertible fingervein templates, which are used as inputs for fuzzy commitment scheme and fuzzy vault. A separate evaluation of this technique on fuzzy commitment scheme and fuzzy vault reflects good recognition performance and security. However, the security and recognition accuracy becomes degraded when fuzzy commitment scheme is fused with fuzzy vault because they use different similarity measures. Face template protection was also performed using a scheme, which combines three techniques, namely random projection, discriminability-preserving transform, and fuzzy commitment scheme. Results from experiments show that scheme has EER of between 8.55% and 16.68%. It also provides cancelability, discriminability and an increase in recognition accuracy by 4 -15%. It is also resistant to masquerade, hill-climbing and brute force attacks. Other proposals for hybrid schemes are based on the integration of traditional encryption techniques. For example, RSA and simple symmetric algorithm were used to create a hybrid scheme, which has a maximum key length of 32 bits and supports biometric data of variable input sizes. The scheme also provides improved authentication speed (can handle up to 624 bytes per second) and security of stored templates. Similarly, a technique based on key generation and encryption was proposed to provide secure transmission of mosaic image [50]. The image is encrypted (prior to transmission) by using a key generated from fingerprint data. The encrypted image cannot be decrypted without the availability of the fingerprint data. However, it is difficult to obtain the fingerprint as it is not stored directly. The original image is discarded after the generation of the biometric key. Non-discriminability among stored templates which is a major weakness of the generic fuzzy vault was addressed by a hybrid scheme which uses password to provide an additional layer of security for fuzzy vault. An application of this technique to multibiometric (fused fingerprint, iris and retinal features) template shows that the use of password enhances user privacy by providing discriminability among protected templates. It also provides improved security by increasing the entropy of the vault by 18 to 30 bits. Similarly, user-specific transformation was applied on face biometric data before securing the transformed template in a fuzzy vault. This approach achieves minimum FRR and FAR of 23% and 15.38% respectively. It also improves the security of fuzzy vault by using a key generated from user-specific password to encrypt the vault. A related work [51] first applied noninvertible transformation to fingerprint data and then secured the transformed templates in a fuzzy vault. In another

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7116039

study, one way cryptographic hashing is used to create non invertible templates before securing the hashed template in a fuzzy vault [52]. This is similar to using random projection to obscure genuine palmprint chaff points before securing the protected points in a fuzzy vault [53]. This method achieves good recognition accuracy, cancelability and security. The FAR is always 0% and a reduction in FRR leads to a decrease in the security of the scheme. A secure and effective approach based on the integration of non-invertible transformation with key generation was proposed for fingerprint template protection. Non-invertible templates and keys were created by applying a one-way transformation to fingerprint minutiae before generating a unique key from the transformed template. A major shortcoming of the hybrid scheme is the complexity of its implementation and operation as well as an increase in the time required for authentication.

4) CONCLUSION AND DISCUSSION

This paper investigated an improved encryption algorithm for developing and building an efficient cancelable biometric authentication framework, which is more robust against hackers. Thus Dorsal Hand Vein Recognition is done using Hybrid Cancelable Biometric Authentication System

REFRENCES

1) N. F. Soliman, M. I. A. D. K. Algarni, S. Ismail, R. Marzouk, and W. El-Shafai, ‘‘Efficient HEVC steganography approach based on audio compression and encryption in QFFT domain for secure multimedia communication,’’ Multimedia Tools Appl., vol. 80, no. 3, pp. 1–35, 2020.

2) A. D. Algarni, G. El Banby, S. Ismail, W. El-Shafai, F. E. A. El-Samie, and N. F. Soliman, ‘‘Discrete transforms and matrix rotation based cancelable face and fingerprint recognition for biometric security applications,’’ Entropy, vol. 22, no. 12, p. 1361, Nov. 2020.

3) L. A. A. Elazm, S. Ibrahim, M. G. Egila, H. Shawkey, M. K. H. Elsaid, W. El-Shafai, and F. E. A. El-Samie, ‘‘Hardware implementation of cancellable biometric systems,’’ in Proc. 4th Int. Conf. I-SMAC (IoT Social, Mobile, Analytics Cloud) (I-SMAC), Oct. 2020, pp. 1145–1152.

4) A. Alarifi, S. Sankar, T. Altameem, K. C. Jithin, M. Amoon, and W. El-Shafai, ‘‘A novel hybrid cryptosystem for secure streaming of high efficiency H.265 compressed videos in IoT multimedia applications,’’ IEEE Access, vol. 8, pp. 128548–128573, 2020.

5) S. Ibrahim, M. G. Egila, H. Shawky, M. K. Elsaid, W. El-Shafai, and F. E. A. El-Samie, ‘‘Cancelable face and fingerprint recognition based on the 3D jigsaw transform and optical encryption,’’ Multimedia Tools and Applications, vol. 79, pp. 1–26, Feb. 2020.

6) A. K. Trivedi, D. M. Thounaojam, and S. Pal, ‘‘Non-invertible cancellable fingerprint template for fingerprint biometric,’’ Comput. Secur., vol. 90, Mar. 2020, Art. no. 101690.

7) M. Joshi, B. Mazumdar, and S. Dey, ‘‘A comprehensive security analysis of match-in-database fingerprint biometric system,’’ Pattern Recognit. Lett., vol. 138, pp. 247–266, Oct. 2020.

8) A. Sinha, ‘‘Image encryption by using fractional Fourier transform and jigsaw transform in image bit planes,’’ Opt. Eng., vol. 44, no. 5, May 2005, Art. no. 057001.

9) W. El-Shafai, I. M. Almomani, and A. Alkhayer, ‘‘Optical bit-panebased 3D-JST cryptography algorithm with cascaded 2D-FrFT encryption for efficient and secure HEVC communication,’’ IEEE Access, vol. 9,

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7116039

pp. 35004–35026, 2021.

10) O. S. Faragallah, A. Afifi, W. El-Shafai, H. S. El-Sayed, E. A. Naeem, M. A. Alzain, J. F. Al-Amri, B. Soh, and F. E. A. El-Samie, ‘‘Investigation of chaotic image encryption in spatial and FrFT domains for cybersecurity applications,’’ IEEE Access, vol. 8, pp. 42491–42503, 2020.

11) O. Enerstvedt, ‘‘Analysis of privacy and data protection principles,’’ in Aviation Security, Privacy, Data Protection and Other Human Rights: Technologies and Legal Principles, O. M. Enerstvedt, Ed. Cham, Switzerland: Springer, 2017, pp. 307–394.

12) X. Zheng, ‘‘The application of information security encryption technology in military data system management,’’ in Proc. Int. Conf. Man-Mach.- Environ. Syst. Eng. Singapore: Springer, Oct. 2017, pp. 423–428.

13) W. Yang, S. Wang, M. Shahzad, and W. Zhou, ‘‘A cancelable biometric authentication system based on feature-adaptive random projection,’’ J. Inf. Secur. Appl., vol. 58, May 2021, Art. no. 102704.

14) W. Yang, S. Wang, J. Hu, G. Zheng, and C. Valli, ‘‘A fingerprint and fingervein based cancelable multi-biometric system,’’ Pattern Recognit., vol. 78, pp. 242–251, Jun. 2018.

15) R. Jaichandran, ‘‘Biometric based user authentication and privacy preserving in cloud environment,’’ Turkish J. Comput. Math. Educ., vol. 12, no. 2, pp. 347–350, Apr. 2021.

16) V. R. Falmari and M. Brindha, ‘‘Privacy preserving biometric authentication using chaos on remote untrusted server,’’ Measurement, vol. 177, Jun. 2021, Art. no. 109257.

17) N. D. Sarier, ‘‘Efficient biometric-based identity management on the blockchain for smart industrial applications,’’ Pervas. Mobile Comput. vol. 71, Feb. 2021, Art. no. 101322.

18) Z. Xu, Z. Shao, Y. Shang, B. Li, H. Ding, and T. Liu, ‘‘Fusing structure and color features for cancelable face recognition,’’ Multimedia Tools Appl., vol. 80, no. 9, pp. 1–18, 2021.

19) M. Shahzad, S. Wang, G. Deng, and W. Yang, ‘‘Alignment-free cancelable fingerprint templates with dual protection,’’ Pattern Recognit., vol. 111, Mar. 2021, Art. no. 107735.

20) A. Nagar, K. Nandakumar, and A. K. Jain, ‘‘A hybrid biometric cryptosystem for securing fingerprint minutiae templates,’’ Pattern Recognit. Lett., vol. 31, no. 8, pp. 733–741, Jun. 2010.

21) C. Rathgeb and A. Uhl, ‘‘A survey on biometric cryptosystems and cancelable biometrics,’’ Eurasip J. Inf. Secur., vol. 2011, no. 1, p. 3, Dec. 2011.

22) V. M. Patel, N. K. Ratha, and R. Chellappa, ‘‘Cancelable biometrics: A review,’’ IEEE Signal Process. Mag., vol. 32, no. 5, pp. 54–65, Sep. 2015.

23) C. Moujahdi, S. Ghouzali, M. Mikram, M. Rziza, and G. Bebis, ‘‘Spiral cube for biometric template protection,’’ in Proc. Int. Conf. Image Signal Process. Berlin, Germany: Springer, 2012, pp. 235–244.

24) L. Zhang, H. Wang, and L. Tao, ‘‘One-factor cancelable fingerprint template protection based on feature enhanced hashing,’’ in Proc. 12th Int. Conf. Graph. Image Process. (ICGIP), Jan. 2021, Art. no. 1172017.

25) H. Mandalapu, A. Reddy P N, R. Ramachandra, K. S. Rao, P. Mitra, S. R. M. Prasanna, and C. Busch, ‘‘Audio-visual biometric recognition and presentation attack detection: A comprehensive survey,’’ IEEE Access, vol. 9, pp. 37431–37455, 2021.

26) A. Alarifi, M. Amoon, M. H. Aly, and W. El-Shafai, ‘‘Optical PTFT asymmetric cryptosystem-based secure and efficient cancelable biometric recognition system,’’ IEEE Access, vol. 8, pp. 221246–221268, 2020.

27) O. S. Faragallah, M. A. AlZain, H. S. El-Sayed, J. F. Al-Amri, W. El-Shafai, A. Afifi, E. A. Naeem, and B. Soh, ‘‘Secure color image cryptosystem based on chaotic logistic in the FrFT domain,’’ Multimedia Tools Appl., vol. 79, nos. 3–4, pp. 2495–2519, Jan. 2020.

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7116039

28) I. F. Elashry, W. El-Shafai, E. S. Hasan, S. El-Rabaie, A. M. Abbas, F. E. A. El-Samie, H. S. El-sayed, and O. S. Faragallah, ‘‘Efficient chaoticbased image cryptosystem with different modes of operation,’’ Multimedia Tools Appl., vol. 79, nos. 29–30, pp. 20665–20687, Aug. 2020.

29) O. S. Faragallah, H. S. El-sayed, A. Afifi, and W. El-Shafai, ‘‘Efficient and secure opto-cryptosystem for color images using 2D logistic-based fractional Fourier transform,’’ Opt. Lasers Eng., vol. 137, Feb. 2021, Art. no. 106333.

30) O. S. Faragallah, W. El-Shafai, A. I. Sallam, I. Elashry, E.-S.-M. El-Rabaie, A. Afifi, M. A. AlZain, J. F. Al-Amri, F. E. A. El-Samie, and H. S. El-sayed, ‘‘Cybersecurity framework of hybrid watermarking and selective encryption for secure HEVC communication,’’ J. Ambient Intell. Humanized Comput., vol. 710, pp. 1–25, Feb. 2021.

31) Yang, Wencheng & Wang, Song & Shahzad, Muhammad & Zhou, Wei. (2021). A cancelable biometric authentication system based on feature-adaptive random projection. Journal of Information Security and Applications. 58. 102704. 10.1016/j.jisa.2020.102704.

32) W. El-Shafai, F. A. H. E. Mohamed, H. M. A. Elkamchouchi, M. Abd-Elnaby and A. Elshafee, "Efficient and Secure Cancelable Biometric Authentication Framework Based on Genetic Encryption Algorithm," in IEEE Access, vol. 9, pp. 77675-77692, 2021, doi: 10.1109/ACCESS.2021.3082940.

33) D.Huang, X. Zhu, Y. Wang, and D. Zhang, "Dorsal hand vein recognition via hierarchical combination of texture and shape clues", Neurocomputing, Vol. 214, pp. 815-828, 2016

34) J. Lee, T. Lo, and C. Chang, "Dorsal hand vein recognition based on directional filter bank", Signal Image Video Process, Vol. 10, No. 1, pp. 145-152,2016.

35) R. Trabelsi, A. Masmoudi, and D. Masmoudi, "Hand vein recognition system with circular difference and statistical directional patterns based on an artificial neural network", Springer Multimedia Tools and Applications, Vol. 75, No. 2, pp. 687-707, 2014.

36) S. Chuang, "Vein recognition based on minutiae features in the dorsal venous network of the hand", Signal, Image and Video Processing, Vol. 12, No. 3, pp1-9, 2018.

37) Ratha NK, Connell JH, and Bolle RM (2001). Enhancing security and privacy in biometrics-based authentication systems. IBM Systems Journal, 40(3): 614-634.

38) Zuo, J., Ratha, N.K., Connell, J.H., 2008. Cancelable iris biometric. In: Pattern Recognition, 2008. ICPR 2008. 19th International Conference on, IEEE. pp. 1–4.

39) S. Patel, V.M., Ratha, N.K., Chellappa, R., 2015. Cancelable biometrics: A review. IEEE Signal Process. Mag. 32, 54–65.

40) S. Jin, A.T.B., Ling, D.N.C., Goh, A., 2004. Biohashing: two factor authentication featuring fingerprint data and tokenised random number. Pattern Recogn. 37, 2245–2255.

41) Jegede, A., Udzir, N.I., Abdullah, A., Mahmod, R., 2017. Cancelable and hybrid biometric cryptosystems: current directions and open research issues.

42) Chang, D., Garg, S., Hasan, M., Mishra, S., 2020. Cancelable multi-biometric approach using fuzzy extractor and novel bit-wise encryption. IEEE Trans. Inf. Forensics Secur. 15, 3152–3167.

43) Rathgeb, C., Breitinger, F., Busch, C., 2013. Alignment-free cancelable iris biometric templates based on adaptive bloom filters. In: 2013 international conference on biometrics (ICB), IEEE, pp. 1–8.

44) Rathgeb, C., Breitinger, F., Busch, C., Baier, H., 2014. On application of bloom filters to iris biometrics. IET Biometrics 3, 207–218.

45) Gomez-Barrero, M., Rathgeb, C., Li, G., Ramachandra, R., Galbally, J., Busch, C., 2018. Multi-biometric

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7116039

template protection based on bloom filters. Inf. Fusion 42, 37– 50.

46) Gomez-Barrero, M., Rathgeb, C., Galbally, J., Busch, C., Fierrez, J., 2016. Unlinkable and irreversible biometric template protection based on bloom filters. Inf. Sci. 370, 18–32.

47) Drozdowski, P., Rathgeb, C., Busch, C., 2018. Bloom filter-based search structures for indexing and retrieving iris-codes. IET Biometrics 7, 260–268.

48) Bringer J, Chabanne H, and Kindarji B (2008). The best of both worlds: applying secure sketches to cancelable biometrics. Science of Computer Programming, 74(1): 43-51.

49) Yang Y, Yu J, Zhang Q, and Meng F (2015). Improved hash functions for cancelable fingerprint encryption schemes. Wireless Personal Communications, 84(1): 643–669.

50) Dahake P and Nimbhorkar S (2015). Hybrid cryptosystem for maintaining image integrity using biometric fingerprint. In the International Conference on Pervasive Computing, IEEE, Pune, India: 1-5. https://doi.org/10.1109/PERVASIVE.2015. 7087177.

51) Chen H and Chen H (2010). A hybrid scheme for securing fingerprint templates. International Journal of Information Security, 9(5): 353-361.

52) Vo TTL, Dang TK, and Küng J (2014). A hash-based index method for securing biometric fuzzy vaults. In the International Conference on Trust, Privacy and Security in Digital Business, Springer, Cham, Switzerland: 60-71. https://doi.org/10. 1007/978-3-319-09770-1_6.

53) Liu H, Sun D, Xiong K, and Qiu Z (2014). A hybrid approach to protect palmprint templates. The Scientific World Journal, 2014: Article ID 686754, 9 pages. https://doi.org/10.1155/ 2014/686754.