A Survey on Face-based Cryptographic Key Generation

Thao Dang*, Deokjai Choi**

Abstract

Derivation cryptographic keys from human biometrics opens a new promising research area when it can be used efficiently for not only verification or recognition tasks, but also symmetric-key based applications. Among existing biometric traits, face is considered as the most popular biometrics since facial features are informative and discriminative. In this paper, we present a comprehensive survey of Face-based key generation (FKGS). First, we summarize the trend of FKGS researches and sum up the methods which play important roles in the proposed key generation systems. Then we present the evaluation and the general performance analysis; from that, we give a discussion about the advantages and disadvantages of surveyed studies to clarify the fundamental requirements and the main challenges when implementing FKGS in practice. Finally, an outlook on future prospects is given.

Keywords : biometrics template protection | face-based cryptosystems | key generation

I. INTRODUCTION

Biometrics, human biological or behavioral characteristic, is suitable to recognize or verify the identity of an individual person. The main advantage of using biometrics over using a password or token is that the approach helps people escape from remembering complicated random strings or carrying physical devices. However, biometric data is difficult to represent as a deterministic string because of its less-discrimination and high-varication properties.

Overall, FKGS is a two-phase system: key generation and key reproduction. In the generation phase, given the original raw biometrics of genuine user, the system derives a biometric key and generates helper data which will be used to reconstruct the cryptographic key in the second phase. The attacker learns nothing about the key and biometric features from that auxiliary information. In the key reproduction phase, thanks to the helper data, when providing another biometric sampling of registered users, a biometric-dependent key can be generated the same with the one extracted in the first stage.

FKGS is a multifunctional approach when the generated key is not only used in identifying human characteristics but also can be used as a secret key in symmetric encryption, which supports combining biometrics scheme with cryptosystem.

FKGS is a multifunctional approach when the generated key is not only used in identifying human characteristics but also can be used as a secret key in symmetric encryption, which supports combining biometrics scheme with cryptosystem.

Machine learning roles in FKGS are going to replace by deep learning approaches because of its robust ability to learn valuable features from the input images. Deep learning reached a new milestone in image recognition when AlexNet was first introduced in the ImageNet Large Scale Visual Recognition Challenge on September 30, 2012. Since then, the most considerable works in face recognition are DeepFace [21] and FaceNet [22]. Therefore, we categorize FKGS according to the methodologies of featurization into machine learning-based and deep learning-based approaches.

* This research was supported by NRF-2017R1D1A1B03035343
* Student Member, **Member, Professor, Chonnam National University

Manuscript : 2019. 09. 02
Confirmation of Publication : 2019. 11. 06
Corresponding Author : Deokjai Choi,
e-mail : dchoi@jnu.ac.kr

In terms of machine learning, we present the historical sequence of the scheme called BioHash which introduced by Teoh et al. [5] and its descendant [20] to illustrate the changing trend of machine learning approaches in FKGS. On another hand, we introduce two main approaches in the deep learning-based method. The first one uses deep models to extract facial features and then convert these into stable strings which can be used as cryptographic keys. The second one is different completely from the above-mentioned case when condensing all steps into a concentrated system that tries to learn the representation of input images and then maps those distinct features to the predetermined key of each individual user (learning to map approach). To complete the entire picture about FKGS, we introduce more three studies using distinct methods to convert biometric features from Euclidean space into Hamming space.

We organize the remaining sections of this paper as follows. Section II provides a background related to FKGS. In Section III, we summarize 10 related studies (4 machine learning-based studies and 6 deep learning-based studies) in FKGS. In Section IV and V, we point out the advantages and disadvantages of surveyed studies and discuss some potential approach may be used in the future to enhance both performance and security perspectives of the system. Finally, the conclusions were given in Section VI.

II. BACKGROUND

The main objective of FKGS is that the systems extract exactly a deterministic and different key for a different user. However, biometric data is noisy and unstable; so that FKGS needs to store some additional information called a helper data which helps to reduce variations and to correct errors in order to extract the same key from different biometric sampling time. In this section, we clarify the remaining challenges and vital requirements in implementing a FKGS.

1. Objectives and Challenges

Basically, implementing a FKGS has two primary challenges: retrieving a deterministic key from the unstable noisy biometric source and revoking the extracted key when it is compromised.

- Biometric data is noisy data that contains variations that can be caused by various factors such as environmental conditions, limitations of data acquisition devices/ techniques, and the mood changing of users. While the biometric key is required to be deterministic and unique, eliminating the variations to get stable information and extracting the key from raw biometrics is considered as the main challenge in implementing the key generation scheme.

- Revoking the new instance of the extracted key from the same biometrics is needed when the old one is compromised. However, the biometric properties of an individual are likely to remain unchanged in a long time period. Therefore, cancellable biometrics is another crucial topic in implementing biometrics-based cryptosystems.

2. Requirements and Evaluation Metrics

In FKGS, there are three main requirements when establishing a generating scheme.

- Irreversibility: From the public helper data, the attackers cannot reverse to the original biometric features or the biometric template.
- Revocability: When the current key is compromised, it should be feasible to revoke a compromised key. This requirement is applied also in the scenario that users can generate several different biometric keys for different systems from the same biometric input.
- Unlinkability: From two or several instances, it should be impossible to distinguish whether the keys were generated from the same biometric input or not. It means the two deriving keys from the same person are completely distinct and there is no correlation between them.

Some common metrics to evaluate the performance of verification/ authentication/ recognition tasks:

- False Acceptance Rate (FAR): False acceptance in the FKGS may mean that the attacker can produce the same key from the attacker's biometric features as for the victim. FAR is the probability that the systems reproduce the same key compared to the stored one. Cryptographically, FAR is considered as the metric to evaluate the security level of the system.
- False Rejection Rate (FRR): False rejection in the FKGS may mean that the key generated by the genuine user is rejected by the system. FRR is the probability that the systems cannot reproduce the same key in different sampling time.
- Equal Error Rate (EER): EER is the value when FAR equals FRR. Reducing EER value means increasing both security (FAR) and

user-friendliness (FRR) level of the system, simultaneously.

- Genuine Acceptance Rate (GAR): This is defined as a percentage of genuine users accepted by the system. It is given by GAR = 100 - FRR.

Additionally, the security strength of the FKGS is also reflected by the length of the extracted key which is required to be long enough to resist against brute force attack. Assume that the extracted key is represented in binary form, another requirement of a strong key is the randomness of the occurrence of bit 1 and 0 along with the key horizontally, and the entropy of that occurrence vertically among the user population.

III. FACE-BASED KEY GENERATION

In this section, we first present face datasets which were used in the surveyed studies. Then, we introduce the overall framework of almost related works to extract the biometric key. Finally, we compare in detail the methodologies that were used and the received results of those studies.

1. Dataset

We provide a short description of each dataset that was used in the surveyed studies. In addition, we present one more dataset that is widely used for face recognition tasks.

- AT&T "The database of faces" [24] (formerly "The ORL database of faces" [19]): There are 40 subjects, 10 grayscale images for each subject. All the images are frontal but varying in lightings and facial expressions.
- FERET [17]: The dataset is collected in 15 sessions. It contains 14,126 images of 1199 identities.
- Faces94 [25]: There are twenty different color images of each of 153 subjects (20 female and 133 male volunteers). The subjects sit at a fixed distance from the camera and are asked to speak, whilst a sequence of images is taken. The speech is used to introduce facial expression variation.
- LFW (Labeled Faces in the Wild) [26]: The dataset contains more than 13,000 face images downloaded from the Internet.
- Extended Yale Face Database B [27]: The dataset contains 16,128 grayscale images of 28 human subjects under 9 poses and 64 illumination conditions. The pose 0 is the frontal pose. Poses 1, 2, 3, 4, and 5 were about 12 degrees from the camera optical axis (i.e., from Pose 0), while poses 6, 7, and 8 were about 24 degrees.
- AR [28]: There are more than 4,000 face images of 126 subjects (70 men and 56 women). The images are taken in two sessions. All of the images are frontal but varying in illumination conditions, facial expressions, and occlusions. No restrictions on wear, make-up, hairstyle, etc. were imposed on participants.
- CMU PIE (Pose, Illumination, and Expression) [29]: There are 41,368 images of 68 individuals. The database is taken under 13 different poses, 43 different illumination conditions, and with 4 different expressions.
- CMU Multi-PIE [30]: The CMU Multi-PIE face database contains more than 750,000 images of 337 people recorded in up to four sessions over the span of five months. Subjects were imaged under 15 viewpoints and 19 illumination conditions while displaying a range of facial expressions. In addition, high-resolution frontal images were acquired as well.
- CASIA-WebFace [31]: It is a collection of 494,414 color facial photographs of 10,575 subjects. The face images in the database are crawled from the Internet by the Institute of Automation, Chinese Academy of Sciences (CASIA). CASIA-WebFace database is used for scientific research of unconstrained face recognition.
- FEI [32]: There are 2800 color images of 200 people (14 images for each subject). The age range of the volunteers is between 19 and 40 years old. The numbers of male and female identities are equal to 100.
- Color FERET [33]: The dataset is a 24-bit color version of FERET [17] dataset. There are 2,413 still facial images, representing 856 individuals.
- UMD-Faces [34]: The dataset is divided into two parts: still images with 367,888 face annotations for 8,277 subjects, and video frames with over 3.7 million annotated video frames from over 22,000 videos of 3100 subjects.
- IJB-A [35]: The dataset contains 500 subjects with manually localized face images. IJB-A consists of a total of 5,712 images and 2,085 videos, with an average of 11.4 images and 4.2 videos per subject. The dataset has been developed using 1,501,267 million crowd sourced annotations.

- IJB-C [36]: IJB-C includes a total of 31,334 (21,294 faces and 10,040 non-face) still images, averaging to around 6 images per subject, and 117,542 frames from 11,779 videos, averaging to around 33 frames and 3 videos per subject.
- WVU multimodal dataset [41]: The was collected at West Virginia University in year 2012 and 2013. The data for the year 2013 and 2012 containing 61,300 and 70,100 facial images in different poses corresponding to 1063 and 1200 subjects, respectively.

Even though VGGFace2 [39] is not been used in the surveyed papers, it is widely used in face recognition as training data due to its large-scale size. Images are downloaded using Google Image Search and have huge variations in pose, age, illumination, ethnicity, and profession. There are around 3.3 million face images are captured "in the wild" from more than 9 thousand identities.

2. General Key Generation Architecture

The processes to retrieve cryptographic keys in almost published studies are quite similar [42]. The main steps of FKGS are generally sketched in Figure 1.

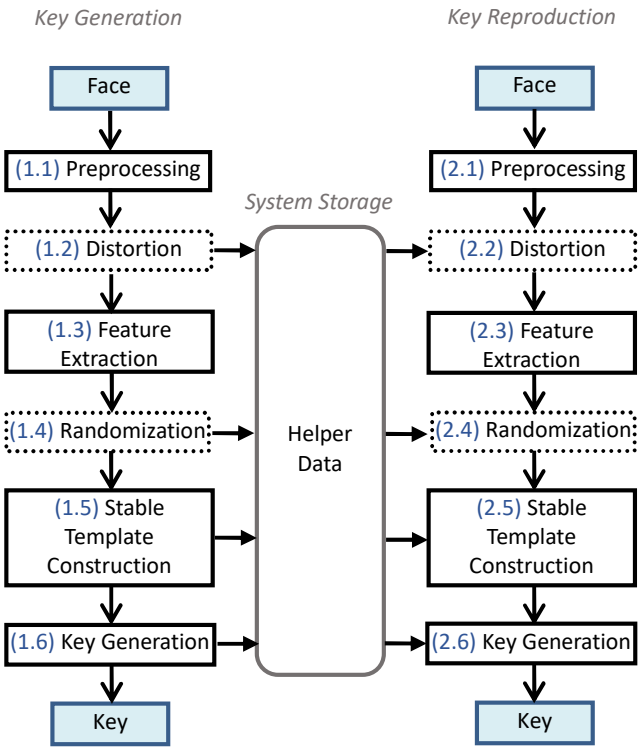


Fig. 1. The overall structure of Face-based key generation scheme

- Enrollment phase: Given the training face data set, the key generation phase starts with preprocessing the variations of input face images. The popular preprocessing method is eye locations-based face alignment [18]; more sophisticated preprocessing methods for face images could be found in [43][44]. There are two options to adopt cancellable methods in the system: before extracting biometric features (Step 1.2), and after extracting biometric features (Step 1.4). After using feature extractor to retrieve biometric features (Step 1.3), those high-uncertainty features will be converted to reliable templates (Step 1.5) which are more stable and discriminative than original biometric features. Finally, the system performs key generation algorithms to eliminate the remaining variations in reliable templates to extract a deterministic and zero-uncertainty key (Step 1.6). The auxiliary data extracted in this phase are stored publicly and reused in the key reproduction phase.
- Testing phase: Given the testing data set, the system repeats same steps at key generation stage. The basic idea is that if the input of key reproduction phase is "close" enough with ones in the enrollment process, the system will generate the same key.

3. Related Works Summarization

There are two main approaches to extract features in FKGS: machine learning-based approach and deep learning-based approach. In the first group, common algorithms such as PCA, LDA, and ICA are usually used as the means to extract facial features. The studies in [20] and [7] used their own algorithms which based on Gabor and Local Binary Pattern (LBP), respectively, as feature extractors of the systems. In the second group, all of the surveyed studies used Convolutional Neural Networks (CNNs) as a feature extractor due to its ability of object recognition in image data. In deep learning-based group, there are two main approaches to derive cryptographic key. The first one has the general process as we presented in Section III.1 (Figure 1). It has a small improvement when using deep neural networks instead of machine learning methods as feature extractors. On another hand, the second approach tries to make a compact system in which the cryptographic keys are not derived from user's

biometric features, but the system is trained to map each user's template to a predetermined cryptographic key. The advantage of this method is managing easily the entropy, randomness and the length of the keys. However, it is difficult to prove the irreversibility property of the system since this method cannot be analyzed as machine learning algorithms. In addition, the trained system is not flexible and scalable, which means it needs to be retrained when there is any change in the system (number of users, changing key length, reissuing new key, etc.). Figure 2 illustrates the overall structure of the mapping approach.

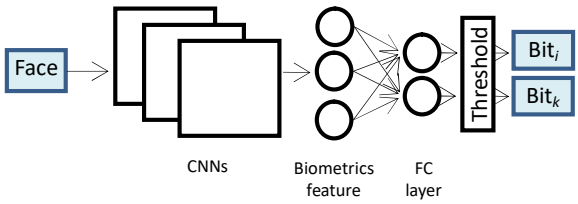


Fig. 2. The overall structure of learning to map approach in [8][10]

Learning to hash is quite similar with mapping approach; however, this approach did not learn to map the biometrics feature of users to the determined result. But it tried to learn the semantic information of given images and then encoded the biometrics feature into the unique hashing code. The advantage of this method is providing zero-shot learning ability. However, the hashing code of this method cannot be revoked, which is the main drawback of Learning to hash approach. Figure 3 presents the overall structure of the hashing method.

All Face-based key generation studies are summarized in Table 1 which describes the key extraction process, whether the key is dependent on biometrics characteristics, and whether the proposed system allows revoking the new key. We arrange all studies by year of publishing and type of approaches (machine learning or deep learning). Until now, no study in this research field evaluated the proposed system in realistic conditions.

Quantization and binary histogram are popular methods for discretization. Distorting the raw input and projecting the biometric features to another space are usually used as a means to cancel the biometrics. The popular metrics for measuring system performance were FAR/FRR and EER combining with key length measured by bits number [5-6,8,10-11,40]. The study in [20] extracted integer value key, which helps to increase the hardness of key guessing attacks. On the other hand, some studies attempt to map the extracted biometric features to predetermined stable strings which could be used in biometric cryptosystems as secret key in studies [8,10,45]. In terms of the main three requirements of FKGS, only machine learning-based studies can prove the irreversibility property. The study [9] used asymmetric encryption to protect biometric features; so that this study does not need to prove the irreversibility demand. Among 10 surveyed FKGS studies, none of them provided a measurement about unlinkability; therefore, we present [1-4] to clarify property of this requirement and methodologies to measure it in Section IV. Since the surveyed papers were evaluated by different conditions among various dataset, and feature extraction is one of the important parts of FKGS; we summarized the feature extraction methods were used, and then compared them using LFW dataset to give a general viewpoint about the performances of those papers. Figure 4 illustrates the milestone of face representation for recognition of surveyed papers.

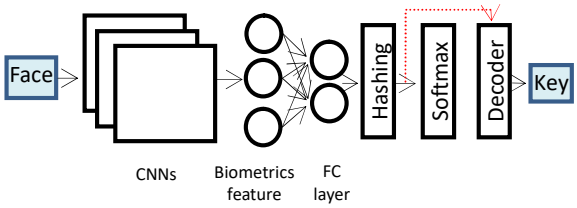


Fig. 3. The overall structure of learning to hash approach in [40]

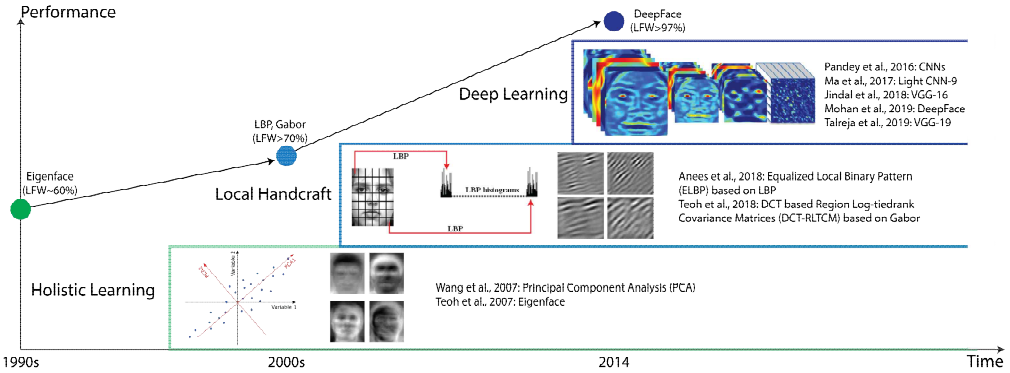


Fig. 4. Milestones of face representation for recognition. The holistic approaches dominated the face recognition community in the 1990s. In the early 2000s, handcrafted local descriptors became popular. In 2014, DeepFace [21] achieved a breakthrough on state-of-the-art performance, and research focus has shifted to Deep learning-based approaches

Table 1. The summarization of key generation methodologies of related works.

Studies	Key generation process	Cancellable method	User-dependent information
Machine learning-based approach			
Teoh et al., 2007 [5]	1. EigenFace [16] played as a biometric feature extractor. 2. The random projection matrix is generated based on the user's information TRN. 3. BioHash template is computed by using the predetermined threshold and values of product operation between token and biometric features.	The random projection matrix is generated by using the user's token. Changing the token helps to cancel the compromised biometrics.	Tokenized random numbers (TRN).
Wang et al., 2007 [6]	1. PCA is adopted as the feature extractor. 2. The extracted features are then quantized and mapped to binary representation using the proposed method in [6]. 3. The fuzzy vault scheme is used to bound the produced binary features and the randomly generated key.	The binary form of facial feature is generated by using 2 random orthogonal matrices. Changing those matrices helps to cancel the compromised biometrics.	2 random orthogonal matrices (user-dependent mode).
Anees et al., 2018 [7]	1. The proposed method, Equalized Local Binary Pattern (ELBP), is used as a feature extractor. 2. The extracted facial features are quantized to reduce the variations of the sampling biometrics. 3. The first 256 bits of the quantized features are considered as the cryptographic key.	NO	NO
Teoh et al., 2018 [20]	1. DCT-RLTCM [37] is used to extract facial features. 2. The proposed method, Random Permutation Maxout (RPM), is used to converts a continuous facial feature vector	Changing the permutation matrix helps to cancel the extracted key.	User-specific permutation matrix

	into a max ranked indices vector as a cancellable template.		
Deep learning-based approach			
Pandey et al., 2016 [8]	1. The end-to-end CNN model is trained to map user images with their predetermined Maximum entropy binary codes. Those codes are considered as cryptographic keys.	Changing the Maximum entropy binary (MEB) code.	NO
Ma et al., 2017 [9]	1. CNN is trained to extract facial features. 2. Sign function is used to binarize the extracted features (the output of this step is the cryptographic key).	The study did not provide any cancellable method due to using the homomorphic encryption to protect the biometric features.	NO
Jindal et al., 2018 [10]	1. The end-to-end CNN model is trained to map user images with their predetermined binary codes. Those codes are considered as cryptographic keys.	Changing the assigned code.	NO
Jindal et al., 2019 [45]	1. CNN is trained to extract facial features. 2. Random Projection is used to reduce redundant features. 3. Fully connected layer is used to map user reduced features with the predefined binary code. This code is considered as cryptographic key.	Changing the assigned code.	NO
Mohan et al., 2019 [11]	1. DeepFace [21] played as a feature extractor. 2. Significant Binary Representation (SBR), is used to extract significant binary vector (the output of this step is the cryptographic key).	Changing the randomly generated valid codeword of Fuzzy commitment scheme.	NO
Talreja et al., 2019 [40]	1. The end-to-end CNN model is trained to encode user images to into their semantic hash codes. Those hashing codes are considered as cryptographic keys.	NO	NO

IV. CANCELLABLE BIOMETRIC KEY

There are two ways to adopt cancellable methods in a general face-based key generation cryptosystem: early canceling and late canceling.

1. Early Canceling

The early canceling approach transforms the raw original face into a cancellable face image (Step 1.2 in Figure 1) and then, those transformed images are used to retrieve cancellable features.

Ratha et al. first presented the idea of cancellable biometrics using distorted images in studies [4] and [2]. Distorted images return different biometric features compared to features extract from the original images. However, there is a high correlation between the morphed cancellable face images and the original data, which violates irreversibility and unlinkability requirements simultaneously. In Figure 5, the original image is shown with a cover grid aligned with the features of the face. In the adjacent image, the grid is bent, and the face is morphed.

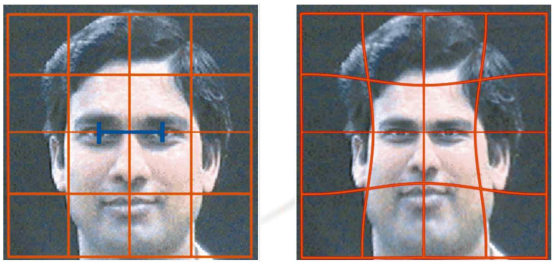


Fig. 5. Distortion transform based on image morphing [4]

Dabbah et al. proposed a new technique that transformed non-linearly original facial images by using a polynomial function whose parameters can be altered accordingly to the issuing version of the secure cancellable template. This method uses co-occurrence matrices in the transform also to generate a distinctive feature vector which helps to increase both security and recognition accuracies. The final cancellable template is constructed by the Hadamard product [1]. The proposed cancellable biometric images are presented in Figure 6. It does not have any readable information. It does not contain any frame as the morphed images in [2] and looks like a random sequence, which makes them misinterpreted by humans. In this study, the authors proved that their proposed method could be satisfied with the irreversibility requirement. The author proved the unlinkability of the system by calculating the correlation values of all original images with their corresponding cancellable versions.

- Irreversibility: The proposed method of [1] is quite similar to random projection-based algorithms in [5] and [6]; therefore, [1] satisfies irreversibility property due to the inheriting benefit from random projecting. Morphed cancellable images in [4] remain high correlation with the original raw source; so that the distorted method in [4] and [2] cannot meet the demand about irreversibility.

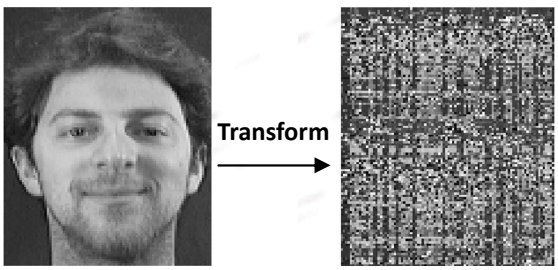


Fig. 6. Cancellable face images of a subject in [1] from the ORL database [19]

- Revocability: Both studies [1] and [4] can change biometric keys by distorting the original face images.

- Unlikability: [1] proved the unlinkability property by computing correlation scores between its distorted images with the corresponding raw images. Moreover, the study analyzed that correlation scores in [4] also and pointed out that [4] cannot reach the requirement about unlinkability. However, the method to measure the unlinkability level in [1] is quite coarse. The study in [3] introduced a framework for the evaluation of biometric templates' unlinkability. They defined two different measures for the linkability of biometric templates: local measure and global measure. For more background information, we refer to the mentioned paper [3].

2. Late Canceling

The late canceling approach first extracts the raw biometric features from the original face image, then transforms those features into cancellable features (Step 1.4 in Figure 1). The biometric key is extracted from the cancellable features.

Teoh et al. proposed a two-factor authentication approach called BioHash which joins a set of user-specific random vectors with biometric features. The random vectors are orthogonal random vectors which were constructed by user's tokenized random numbers (TRN). With user-specific data, there is a large uncorrelation between the cancellable templates generated from the same biometric features, which is considered as unlinkability. Changing the token helps to cancel the extracted key. However, the weakness of this scheme is that the users need to carry their tokens for identifying; the inconvenient in terms of practicality may incur.

In the study [20], Teoh et al. used proposed the algorithm called Random Permutation Maxout (RPM) which used the hashing property of Locality Sensitive Hashing (LSH) to increase the system's performance and security level. RPM can be canceling function and discretization function simultaneously. Because of the properties of LSH, RPM is able to transform the correlation of biometric features into a new irreversible relationship. Furthermore, the architecture of RPM helps to lengthen the length of extracted keys and

strengthen the security level when representing the cryptographic key in integer [1..k] space instead of binary form.

- Irreversibility: Both BioHash [5] and its descendant [20] used the property of random projecting method to provide the irreversibility.
- Revocability: These studies used the token as a means to cancel the biometrics.
- Unlinkability: Both two studies did not measure this requirement.

V. DISCUSSION

In this section, we discuss about popular methods in FKGS and their replacements in the future; and forecast new approaches could be applied in key generation scheme.

Famous algorithms such as LDA, PCA, and ICA are replaced by deep neural networks as feature extractors. With the face input, DeepFace [21] and FaceNet [22] are popular among the existing deep models. Quantization is still a common choice in the discretization step due to its simplicity and reducing variations ability. However, LSH is started to be concerned [20] since LSH-based methods can fulfill the requirements of cancellable biometrics function and discretization function at the same time. Like feature extraction, there are two main groups of hashing algorithms that can be classified as machine learning-based approach and deep learning-based approach: LSH and learning to hash, respectively. LSH is data-independent while learning to hash, conversely, is data-dependent. Learning to hash attempts to learn hash functions from the given input, which yields to the nearest search result in the hash coding space is as similar as possible to the search in the original space; so that the similarity is preserved [38].

Learning to map is a new approach in FKGS, however, there are some existing problems which makes this method is not feasible in real-life schemes. Personally, we forecast that triplet loss-based learning to hash is a promising approach due to its scalability and one-shot learning property. If early canceling functions combine with this approach, it is unnecessary to have discretization function in the system. However, proving irreversibility in learning to hash method is still big challenge in mathematic viewpoint. We summarize the three main needed functions of FKGS, and methodologies were used in the past, present, and future in Table 2.

Table 2. The summarization of feature extraction, discretization, and cancellable methods. The trending methods are set in bold type

Function	Methods
Feature extraction	PCA, LDA, ICA **Deep neural networks: CNNs**
Discretization (binarization)	Quantization Significant binary representation **Learning to map, Locality sensitive hashing, Learning to hash**
Biometrics cancellation	Token, random projection **Locality sensitive hashing**

VI. CONCLUSIONS

In this study, we summarize state-of-the-art studies and the requirements when implementing a FKGS. Deep learning-based methods replace machine learning-based methods such as PCA, LDA, and ICA in extracting informative biometric features. However, establishing an end-to-end deep model as the key generation cryptosystem is difficult since there is no practical method to prove the irreversibility of "black box" deep neural networks.

REFERENCES

[1] M. A. Dabbah; W. L. Woo; S. S. Dlay; "Secure Authentication for Face Recognition," *2007 IEEE Symposium on Computational Intelligence in Image and Signal Processing*, Honolulu, HI, 2007, pp.121-126

[2] R. M. Bolle; J. H. Connell; N. K. Ratha; "Biometric perils and patches," *Pattern Recognition*, vol.35, no.12, pp.2727-2738, 2002

[3] M. Gomez-Barrero; J. Galbally; C. Rathgeb; C. Busch; "General Framework to Evaluate Unlinkability in Biometric Template Protection Systems," *IEEE Transactions on Information Forensics and Security*, vol.13, no.6, pp.1406-1420, 2018

[4] N. K. Ratha; J. H. Connell; R. M. Bolle; "Enhancing security and privacy in biometrics-based authentication systems," *IBM Systems Journal*, vol.40, no.3, pp.614-634, 2001

[5] A. B. J. Teoh; Y. W. Kuan; S. Lee; "Cancellable biometrics and annotations on BioHash," *Pattern Recognition*, vol.41, no.6, pp.2034-2044, 2008

[6] Y. WANG; K.N. Plataniotis; "Fuzzy Vault for Face Based Cryptographic Key Generation," *2007 Biometrics Symposium*. IEEE, 2007. pp.1-6, 2007

[7] A. Anees; Y. P. Chen; "Discriminative binary feature learning and quantization in biometric key generation," *Pattern Recognition*, vol.77, pp. 289-305, 2018

[8] R. K. Pandey; Y. Zhou, B. U. Kota and V. Govindaraju, "Deep Secure Encoding for Face Template Protection," *2016 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*, Las Vegas, NV, pp.77-83, 2016

[9] Y. Ma; L. Wu; X. Gu; J. He; Z. Yang; "A Secure Face-Verification Scheme Based on Homomorphic Encryption and Deep Neural Networks," *IEEE Access*, 5, pp.16532-16538, 2017

[10] A. K. Jindal; S. Chalamala; S. K. Jami; "Face Template Protection Using Deep Convolutional Neural Network," *IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*, Salt Lake City, UT, pp.575-5758, 2018

[11] D. D. Mohan; N. Sankaran; S. Tulyakov; S. Setlur; V. Govindajaru; "Significant Feature Based Representation for Template Protection," *IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*, Long Beach, CA, 2019

[12] C. Rathgeb; A. Uhl; "A survey on biometric cryptosystems and cancelable biometrics," *EURASIP Journal on Information Security*, 2011

[13] Y. Dodis; L. Reyzin; A. Smith; "Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data," *Advances in Cryptology (EUROCRYPT)*, pp. 523-540, 2004

[14] A. Juels; M. Wattenberg; "A Fuzzy Commitment Scheme," Proc. of the 6th ACM Conference on Computer and Communications Security (CCS), pp. 28-36, 1999

[15] A. Juels; M. Sudan; "A Fuzzy Vault Scheme," *Designs, Codes and Cryptography*, vol.38, no.2, pp.237-257, 2006

[16] M. Turk; A. Pentland; "Eigenfaces for recognition," *Journal of Cognitive Neuroscience*, vol.3, no.1, pp.71-86, 1991

[17] P.J. Phillips; H. Wechsler; J. Huang; P. J. Rauss; "The FERET database and evaluation procedure for face-recognition algorithms," *Image and Vision Computing*, vol.16, no.5, pp. 295-306, 1998

[18] P. Wang; M. B. Green; Q. Ji; J. Wayman; "Automatic Eye Detection and Its Validation," *IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*, San Diego, CA, pp.164-164, 2005

[19] ATT Laboratories Cambridge, ORL face database, http://cam-orl.co.uk/facedatabase.html (accessed Apr., 03, 2020).

[20] A. B. J. Teoh; S. Cho; J. Kim; "Random permutation Maxout transform for cancellable facial template protection," *Multimedia Tools and Applications*, vol.77, no.21, pp.27733-27759, 2018

[21] Y. Taigman; M. Yang; M. Ranzato; L. Wolf; "DeepFace: Closing the Gap to Human-Level Performance in Face Verification," *IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, Columbus, OH, pp.1701-1708, 2014

[22] F. Schroff; D. Kalenichenko; J. Philbin; "FaceNet: A unified embedding for face recognition and clustering," *IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, Boston, MA, pp.815-823, 2015

[23] S. Xie; R. Girshick; P. Dollar; Z. Tu; K. He; "Aggregated Residual Transformations for Deep Neural Networks," *IEEE Conference on*

Computer Vision and Pattern Recognition (CVPR), Honolulu, HI, pp.5987-5995, 2017

[24] F. S. Samaria; A. C. Harter; "Parameterisation of a stochastic model for human face identification," Proc. of IEEE Workshop on Applications of Computer Vision, Sarasota, FL, USA, pp.138-142, 1994

[25] D. Hond; L. Spacek "Distinctive Descriptions for Face Processing," Proc. of the 8th British Machine Vision Conference (BMVC), Colchester, England, pp. 320-329, 1997

[26] E. Learned-Miller; G. B. Huang; A. R. Chowdhury; H. Li; G. Hua; "Labeled Faces in the Wild: A Survey," *Advances in Face Detection and Facial Image Analysis*, pp.189-248, 2016

[27] A. S. Georghiades; P. N. Belhumeur; D. J. Kriegman; "From few to many: illumination cone models for face recognition under variable lighting and pose," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol.23, no.6, pp.643-660, 2001

[28] A.M. Martinez; R. Benavente; "The AR face database," *CVC Tech Rep*, 24, 1998

[29] T. Sim; S. Baker; M. Bsat; "The CMU Pose, Illumination, and Expression (PIE) Database," Proc. of IEEE International Conference on Automatic Face and Gesture Recognition, pp. 53, 2002

[30] R. Gross; I. Matthews; J. Cohn; T. Kanade; S. Baker; "Multi-PIE," *IEEE International Conference on Automatic Face and Gesture Recognition*, Amsterdam, pp.1-8, 2008

[31] D. Yi; Z. Lei; S. Liao; S. Z. Li; "Learning face representation from scratch," (2014)https://arxiv.org/abs/1411.7923 (accessed Apr. 20, 2020).

[32] C. E. Thomaz; G. A. Giraldi; "A new ranking method for principal components analysis and its application to face image analysis." *Image and Vision Computing*, vol.28, no.6, pp.902-913, 2010

[33] P. J. Phillips; H. Moon; S. A. Rizvi; P. J. Rauss; "The FERET evaluation methodology for face-recognition algorithms," *IEEE Transactions on pattern analysis and machine intelligence*, vol.22, no.10, pp.1090-1104, 2000

[34] A. Bansal; A. Nanduri; C. D. Castillo; R. Ranjan; R. Chellappa; "Umdfaces: An annotated face dataset for training deep networks," *Biometrics IEEE International Joint Conference (IJCB)*, pp. 464-473, 2017

[35] B. F. Klare; B. Klein; E. Taborsky; A. Blanton; J. Cheney; K. Allen; P. Grother; A. Mah; A. K. Jain; "Pushing the Frontiers of Unconstrained Face Detection and Recognition: IARPA Janus Benchmark A," *IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 2015

[36] B. Maze; J. Adams; J. A. Duncan; N. Kalka; T. Miller; C. Otto; A. K. Jain; W. T. Niggel; J. Anderson; J. Cheney; P. Grother; "IARPA Janus Benchmark - C: Face Dataset and Protocol," *International Conference on Biometrics (ICB)*, Gold Coast, QLD, pp.158-165, 2018

[37] C. J. Ng; A. B. J. Teoh; C. Y. Low; "DCT based region log-tiedrank covariance matrices for face recognition," *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pp.2099-2103, 2016

[38] J. Wang; T. Zhang; J. Song; N. Sebe; H. T. Shen; "A Survey on Learning to Hash," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol.40, no.4, pp.769-790, 2018

[39] Q. Cao; L. Shen; W. Xie; O. M. Parkhi; A. Zisserman; "VGGFace2: A dataset for recognising face across pose and age," *International Conference on Automatic Face and Gesture Recognition*, 2018

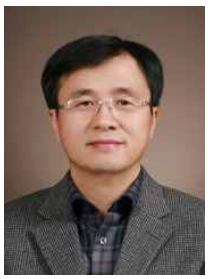
[40] V. Talreja; M. Valenti; N. Nasrabadi; "Zero-Shot Deep Hashing and Neural Network Based Error Correction for Face Template

Protection," *IEEE International Conference on Biometrics: Theory, Applications and Systems (BTAS)*, 2019
[41] WVU multimodal dataset, http://biic.wvu.edu/ (accessed Apr., 20, 2020).
[42] Lam Tran Ha; Deokjai Choi; "Biometrics-based Key Generation Research : Accomplishments and Challenges," *Smart Media Journal*, vol.6, no.2, pp.15-25, 2017
[43] Hong Tai Tran; In Seop Na; Young Chul Kim; Soo-Hyung Kim; "Human Face Tracking and Modeling using Active Appearance Model with Motion Estimation," *Smart Media Journal*, vol.6, no.3, pp.49-56, 2017
[44] Do Nhu Tai; Soo-Hyung Kim; Guee-Sang Lee; Hyung-Jeong Yang; In-Seop Na; A-Ran Oh; "Tracking by Detection of Multiple Faces using SSD and CNN Features," *Smart Media Journal*, vol.7, no.4, pp.61-69, 2018
[45] A. K. Jindal; S. Rao Chalamala; S. K. Jami; "Securing Face Templates using Deep Convolutional Neural Network and Random Projection," *2019 IEEE International Conference on Consumer Electronics (ICCE)*, Las Vegas, NV, USA, 2019, pp. 1-6

Authors

Dang Mai Thao

Received the B.S. degrees in Information Technology from Ho Chi Minh University of Science in 2017.



Deokjai Choi

Received BS degree in Department of Computer Engineering, Seoul National University, in 1982. He got MS degree in Department of Computer Science, KAIST, South Korea in 1984. He got PhD degree in Department of Computer Science and Telecommunications, University of Missouri Kansas City, USA in 1995. He is currently Full Professor in the School of Electronics and Computer Engineering at the Chonnam National University, South Korea.