# A survey on face template protection methods

**Ena Barčić, Igor Tomičić, Mario Harjač**
Faculty of Organization and Informatics
University of Zagreb
Pavlinska 2, Varaždin, Croatia
{enbarcic, itomicic, mharjac}@foi.unizg.hr

***Abstract.*** *Biometric authentication has become one of the most popular ways of protecting information, with techniques such as "face unlocking" becoming more and more prevalent. For the purpose of authentication, a face image needs to be saved in the form of a template. To ensure that our information is protected, biometric face template protection methods have been created. In this paper we will present an overview of template protection methods, show their effectiveness and their uses.*

**Keywords.** Face template protection, Key Binding, Key Generating, Cancellable Biometrics, Hybrid Methods, Homomorphic Encryption

## 1 Introduction

In today's world, conventional forms of protection like PINs, passwords, tokens, etc. are stolen relatively easily, disclosed and reused by hackers (Sarkar, Singh 2020). To get the highest possible degree of security, biometric traits are often used as keys for unlocking information. Biometric attributes or biometric traits like fingerprint, iris, face (2D, 3D), etc. are extremely individual. The human face is one of the most distinct features, and also one of the most popular physiological characteristics used in commercial biometric systems.

In this paper, we will show the most common biometric facial template methods, determine which ones are the most commonly used today and present their advantages and disadvantages.

## 2 Biometrics and biometric templates

According to ISO/IEC 30136:2018 Information technology — Performance testing of biometric template protection (BTP) schemes (Shahreza et al. 2022), each scheme needs to include four main properties:

- Cancelability: if compromised, we have to be able to cancel the enrolled template and replace it with a new one.
- Unlinkability: There should be no link between different protected templates from the same unprotected (original) biometric template.
- Irreversibility: It should be difficult or impossible to recover the original biometric template from the protected one.
- Recognition Performance: The protected templates should allow for accurate recognition, without accuracy degradation.

Among most notable problems with biometrics are non-revocability and privacy compromises. Non-revocability means that biometric information in the form of a biometric database/template, if compromised, cannot be replaced or revoked. Privacy compromises consist of three categories: secrecy of biometric data, secrecy of biometric information and privacy of a user's identity. Secrecy of biometric data means that stored templates can be used for template recovery. Secrecy of biometric information means that various biometric traits can be stored together, so if one is compromised, another one can be used. Privacy of a user's identity means that biometric templates, stored in different biometric databases, can be used for cross matching.

Biometric systems are vulnerable to several types of attacks at different stages, the four most common ones being (Sarkar, Singh 2020):

1. Attacks at the user interface– the sensor is incapable of differentiating among fraudulent and real biometric traits.
2. Attacks between the interfaces between two modules – a strategically placed jammer block a wireless interface and intercepts or alters the template
3. Attacks on the software infrastructure – the modification of a module during its execution stage in a way that returns the values programed by an intruder.
4. Template database attacks – templates within databases are attacked. The most common attacks include replacement and spoofing.

The main advantage of biometric templates is that they are easy to use, convenient and reliable, but despite that, there still are some risks to security and privacy (Sandhya and Prasad 2017):

1. Impersonation: a thief gains access to a person's accounts/services.
2. Sensitivity: template contains a lot of personal and/or sensitive information.
3. Linkability: Cross matching of databases needs to be prevented.
4. Loss of biometrics is permanent: Theft can render the trait useless for the user's entire lifetime.

# 3 Performance estimation

False Acceptance Rate (FAR) is the percentage of times the authentication systems recognized an imposter as a legitimate user. This is also known as the false match rate (FMR) (Sarkar, Singh 2020).

$$\text{FAR}(\%) = \frac{\text{Number of false accept}}{\text{Number of imposters tested}} \text{x } 100 \quad (1)$$

False Rejection Rate (FRR) is the percentage of times the authentication systems recognized a legitimate user as an imposter. This is also known as false non-match rate (FNMR) (Sarkar, Singh 2020).

$$\text{FRR}(\%) = \frac{\text{Number of rejections}}{\text{Total number of users tested}} \text{x } 100 \quad (2)$$

Equal Error Rate (EER) shows that the balance of false acceptances is related to the balance of false rejections. To achieve the best possible performance of biometric authentication systems, the EER needs to be as small as possible (Sarkar, Singh 2020).

$$\text{EER} = \text{FAR where FAR} = \text{FRR} \quad (3)$$

Genuine accept rate (GAR) is the percentage of numbers of genuine registered users being recognized by the authentication infrastructure (Sarkar, Singh 2020).

$$\text{GAR}(\%) = \frac{\text{Number of geniune user accepted}}{\text{Total number of genuine trials}} \text{x } 100 \quad (4)$$

$$\text{GAR}(\%) = 100 - \text{FRR}(\%) \quad (5)$$

# 4 Research methodology and a literature overview

The scientific databases Web of Science, IEEE and Scopus were used in this paper. The main keywords used in the search were "biometric face template protection". The main keywords were also used in combination with the following additional keywords: Fuzzy Commitment, Fuzzy Vault, Quantization schemes, Secure sketch, Fuzzy extractor, Salting, Non-invertible Transforms, Hybrid Methods, Homomorphic Encryption and CNN. Additional criteria were also applied, mainly the number of citations and relevance to the topic of this paper. An additional criterion was that the searched approach needed to me the only method used or in cases where there wasn't a sufficient number of papers the searched method needed to be primary method with secondary methods being used to improve it. We also only considered papers that clearly show results. The publication year of the analysed papers was not restricted. The search for papers was carried out in the period from May 1 to June 1. Results of the search together with the relevant keywords are shown and summarized within Table 1.

**Table 1.** Search criteria

| Keywords | | WoS | Scopus | IEEE |
|---|---|---|---|---|
| Biometric face template protection | Base | 168 | 264 | 133 |
| | J/C* | 163 | 236 | 130 |
| | Eng | 163 | 230 | 130 |
| + Fuzzy Commitment | | 12 | 20 | 9 |
| + Fuzzy Vault | | 21 | 24 | 11 |
| + Quantization schemes | | 10 | 14 | 6 |
| + Secure sketch | | 8 | 11 | 6 |
| + Fuzzy extractor | | 10 | 12 | 4 |
| + Salting | | 2 | 3 | 3 |
| + Non-invertible Transforms | | 6 | 8 | 4 |
| + Hybrid Methods | | 5 | 7 | 1 |
| + Homomorphic Encryption | | 6 | 13 | 7 |
| + CNN | | 7 | 9 | 4 |

+ - The main keywords "Biometric face template protection" were combined with one of the additional keywords
J/C* – journal, conference

## 4.1 Biometric template protection

BTP is one of the most important tasks when creating a database. It can be secured at three different levels: hardware level, protocol level and software level (Kaur, Khanna 2016). At the hardware level, options like tamperproof hardware, smart cards, etc. can be used, while the protocol level options include private information retrieval, multiparty communication, and many more. This article focuses on the software level of BTP.

Biometric template security techniques must satisfy the following criteria (Sarkar, Singh 2020):

1. Diversity: The protected template should not permit comparison with other templates stored in the same database.

2. Revocability: Template protection techniques must be able to generate different templates based on the user's original biometric data and cancel old compromised templates.
3. Security: The authentic biometric template can never be obtained using the secured template.
4. Performance: Despite containing various strategies for BTP, the performance of the system should not suffer or slow down during the identification of the authenticated user.

BTP methods can be categorized into biometric cryptosystems, cancellable biometrics, hybrid methods, homomorphic encryption and others. In continuation we are presenting an overview of the methods, their accuracy and the databased they were tested on.

## 4.2 Biometric cryptosystems

Biometric cryptosystems are systems that bind a key to a biometric feature or generate it from a biometric feature (Sandhya, Prasad 2017). An important characteristic of biometric cryptosystems is their use of "helper data". Based on how "helper data" is derived, biometric cryptosystems can be further classified into key binding and key generating systems.

### 4.2.1 Key Binding Biometric Cryptosystems

In a key binding cryptosystem, the "helper data" is obtained by binding a user-specific chosen key to a biometric template (Sandhya, Prasad 2017). The combined key and biometric template from a secure template. Key binding cryptosystem can be further classified into fuzzy commitment schemes and fuzzy vault schemes.

#### 4.2.1.1 Fuzzy Commitment Schemes

Fuzzy commitment schemes combine cryptography and error correcting codes (ECC) (Sandhya, Prasad 2017). In the enrolment stage, a random key is chosen and encoded using ECC, generating a random code word. Next, a XOR operation is carried out between the biometric feature vector and a codeword, resulting in an encrypted template.

Wang et al. (Wang et al. 2015) present a multi-biometrics template protection scheme based on fuzzy commitment and chaotic systems. The authors capture thermal facial images and generate fuzzy commitmentfrom corporation of ECC and fusion binary features. They achieve EER = $1.163 * 10^{-1}$ on NVIE face.

Elrefaei and Mohammadi (Elrefaei and Mohammadi 2019) present a fuzzy commitment scheme combined with a machine vision gait-based biometric system to enhance system security. The proposed biometric cryptosystem has two phases: enrolment and verification. They achieve FAR = 0% and FRR = 0% on CMU MoBo and CASIA A.

Gilkalaye et al. (Gilkalayeet al. 2019) present a key-binding cryptographic template security scheme based on a lattice structure and sphere packing in Euclidean space. The proposed scheme can be applied to real-value feature vectors, making it more compatible with recent face recognition methods. They achieve TPR = 0.20-0.91 and FPR = 0.07-0.0004 on LFW and VGG.

#### 4.2.1.2 Fuzzy Vault Schemes

In fuzzy vault schemes (FVS), a key *k* is locked by an unordered set *A*, resulting in a vault *VA* (Sandhya, Prasad 2017). During the enrolment stage, a polynomial *p* encodes key *k*, *A* is projected onto *p* and chaff points are added. During the authentication stage, if another set *B* overlaps *A*, key *k* is reconstructed (Sandhya, Prasad 2017).

Wu and Yuan (Wu and Yuan 2010) propose a face-based FVS for online authentication. The transformed template and key are generated from a password and provided to the server. Fuzzy vault encoding is implemented using both the key and transformed template. They achieve FAR = 5.26%-15.38 and FRR = 23.0%-48.5% on ORL.

Nagar et al. (Nagar et al. 2011) show a feature-level fusion framework to simultaneously protect user's multiple templates as a single secure sketch. The authors achieve this by using fuzzy vault and fuzzy commitment and present a detailed analysis of the trade-off between matching accuracy and security. They achieve GAR = 75 on CASIA v1, FVC 2002 DB2 and XM2VTS.

Kaur and Sofat (Kaur and Sofat 2017) propose a multimodal biometric system security using face and fingerprint traits with fuzzy vault template security. The proposed system focuses on feature level fusion. They achieve FAR = 0 and FRR = 8.8%.

### 4.2.2 Key Generating Biometric Cryptosystems

Key generating cryptosystems directly generate keys through biometric templates (Sandhya, Prasad 2017). They are further classified into quantization schemes and secure sketches.

#### 4.2.2.1 Quantization Schemes

In quantization schemes helper data is quantized to obtain stable keys. In this scheme, intervals of feature elements are obtained by taking vectors of several biometric samples (Sandhya, Prasad 2017). Helper data consists of encoded intervals. During the authentication stage, features are calculated and mapped to the determined intervals.

Li and Chang (Li and Chang 2006) apply cryptographic operations on noisy data where objects are represented in a continuous domain, and further quantified to obtain a short authentication tag. The authors use two levels of quantization and heighten the sensitivity of the proposed framework.

Han et al. (Han et al. 2008) present a novel methodology for achieving BTP using an adaptive non-

uniform quantization (ANUQ) algorithm. This is used to eliminate the contradiction between the fuzziness of the biometric information and the hash function sensitivity. They achieve FRR = 1.07-1.58 and FAR = 0.11- 2.40

Wu et al. (Wu et al. 2010) propose a biometric cryptosystem based on face biometrics. The authors extract 128-dimensional PCA feature vectors from the face and obtain a128-bit binary vector. The distinguishable bits are selected to form a bio-key. They achieve FRR = 0.0%-97.0% and FAR = 0.0%-67.5% on ORL.

#### 4.2.2.2 Secure Sketch

Secure sketches are used to derive a consistent cryptographic key from noisy data (Chen et al. 2014). Two main components in a secure sketch scheme are the sketch generation algorithm (encoder) and the biometric template reconstruction algorithm (decoder).

Li et al. (Li et al. 2006) examine the relative entropy loss to determine optimal parameters of additional bits that could be extracted. They present a general scheme and show the relative entropy loss due to suboptimal discretization. They achieve FAR = 0.005 and FRR = 0.045 on Essex Faces94 database.

Sutcu et al. (Sutcu et al. 2007) study how secure sketch can be applied to protect the templates by identifying several practical issues and showing the subtleties in evaluating the security of practical systems on Essex Faces94 database.

Dang et al. (Dang et al. 2013) show the constructions of a face-based authentication systems where the stored templates are protected by a secure sketch. They achieve TRR = 100% on Essex Faces94 database.

#### 4.2.2.3 Fuzzy extractor

Fuzzy extractor is a cryptographic method that produces acryptographic key directly from different biometric features (Shahreza et al. 2022).

Blanton and Aliasgari (Blanton and Aliasgari 2013) present a study about the reusability of fuzzy sketches and extractors, as well as suggestsecurity improvements. The authors present the problem of safe reuse as well showcase improvements to the overall security.

Chen et al. (Chen et al. 2014) propose an optional multi-biometric cryptosystem based on fuzzy extractor and secret share technology.

Zhang et al. (Zhang et al. 2021) utilize dense packing feature of certain lattices to design a family of fuzzy extractors that docks well with existing neural network-based biometric identification schemes. They achieve FRR = 70% and FAR = $2.1 \times 10^{-7}$ on LFW.

### 4.2.3 Cancellable Biometrics

Cancelable biometric (CB) systems are systems that use a key-dependent transformation function (Sandhya, Prasad 2017). CB systems can be further classified into salting and non-invariable transforms.

#### 4.2.3.1 Salting

In salting, biometric features are transformed using an invertible function (Sandhya, Prasad 2017) and the stored key can be recalled by the user for authentication. The security of this method depends on the secrecy of the transformation key and the complexity of the transformation algorithm.

Kim et al. (Kim et al. 2007) propose a two-step method for boosting the verification performance of face biometric: using an efficient feature extraction transformation, and an error minimizing template transformation. To improve the feature extraction efficiency an extended random projection of face data is used. They achieve EER = 10.915 on AR face and BERC.

Wang et al. (Wang et al. 2007) propose an approach based on discretized random orthonormal transformation of biometrics features. The authors provide properties of zero error rate and generate revocable and non-invertible biometrics templates. They achieve FAR = 0, FRR = 0 and EER = 0 on ORL and GT.

Tarek et al. (Tarek et al. 2021) create unimodal-Bio-GAN, a reliable keyless biometric salting technique based on standard generative adversarial network (GAN). The authors use a random permuted version of biometric data as a salting key. They achieve EER = 2.1% on CASIA.

#### 4.2.3.2 Non-invertible Transforms

Non-invertible transforms (NT) apply a one-way and irreversible process to generate a transformed template from biometric data (Sandhya, Prasad 2017). Keys are produced during the authentication stage. NT can generally be further classified into geometric transforms, robust hashing, random projections, biometric filters and random permutations.

Kaur and Khanna (Kaur and Khanna 2019) propose a template protection approach for generating revocable binary features from phase and magnitude patterns of log-Gabor filters. They apply multi-level transformations at the signal and feature level to distort the biometric data using user specific tokenized variables. They achieve EER (%) = 2.40 ± 1.12 / 3.08 ± 2.11 on CASIA-Face V5 and EER (%) = 0.99 ± 0.46 / 1.19 ± 0.19 on ORL.

Sardar et al. (Sardar et al. 2020) present a novel cancelable FaceHashing technique based on non-invertible transformation with encryption and decryption template. The system consists of four components: face preprocessing, feature extraction, cancelable feature extraction followed by the classification and encryption/decryption of cancelable face feature templates. They achieve EER (%) = 0.0000 on CASIA, IITK, CVL and FERET.

Lee et al. (Lee et al. 2021) propose a data-driven cancelable biometrics scheme, named SoftmaxOut Transformation-Permutation Network (SOTPN). The SOTPN is a neural version of Random Permutation Maxout (RPM) transform, introduced for facial

template protection. EER (%) = 3.53 on LFW, YTF and FS.

#### 4.2.4 Hybrid Methods

Hybrid methods are a combination of cancelable biometrics and cryptosystems (Sandhya, Prasad 2017). They rely on the strengths of their component schemes and provide an integrated approach with a high degree of privacy (Jegede et al. 2017).

Sree and Radha (Sree and Radha 2016) present a system for multimodal biometric authentication based on the face and fingerprints. Biometric traits are transformed using distortion algorithm. They achieve FAR = 2%, FRR = 1.8%, GAR = 98.1%

Nguyen et al. (Nguyen et al. 2019) present a hybrid biometric template protection system which takes benefits of both feature transformation and biometric cryptosystems while preventing their limitations. The performance of the system can be maintained with a new random orthonormal project technique, reducing the computational complexity while preserving the accuracy. They achieve EER = 9%

BBousnina et al. (Bousnina et al. 2021) present a hybrid system for multimodal biometric template protection to provide robustness against template database attacks. Dual-Tree Complex Wavelet Transform Discrete Cosine Transform (DTCWT-DCT) based watermarking is employed to entrench a fingerprint sketch into a face image. EER = 0%, FRR = 0.0083 %, FAR = 0.2140%, GAR = 99.99 % on ORL & FVC2002 DB1 as well as EER = 0%, FRR = 0.0080 %, FAR = 0.2141%, GAR = 99.99 % on ORL & FVC2002 DB2 and EER = 0.12%, FRR = 0.0095 %, FAR =0.2074 %, GAR = 99.99 % on ORL & FVC2000 DB1.

#### 4.2.5 Homomorphic Encryption

Homomorphic encryption (HE) is a method characterized by allowing a limited subset of computation on the encrypted data (Sandhya, Prasad 2017). Biometric features are encrypted using a public key during the enrolment stage.

Boddeti (Boddeti 2018) proposes a fully homomorphic encryption-based framework to secure a database of face templates, designed to preserve user privacy and prevent information leakage, while at the same time maintaining their utility through template matching directly in the encrypted domain. They achieve TAR = 90.49 @ FAR = 0.01%, TAR = 96.74 @ FAR = 0.1%, TAR = 99.11 @ FAR = 1% on LFW, TAR = 23.13 @ FAR = 0.01%, TAR = 46.07 @ FAR = 0.1%, TAR = 73.71 @ FAR = 1% on IJB-A, TAR = 25.77 @ FAR = 0.01%, TAR = 48.31 @ FAR = 0.1%, TAR = 74.58 @ FAR = 1% on IJB-B and TAR = 86.48 @ FAR = 0.01%, TAR = 90.81 @ FAR = 0.1%, TAR = 93.83 @ FAR = 1% on CASIA.

Jindal et al. (Jindal et al. 2020) propose a method based on fully HE, using one-shot enrolment and supporting operations over real valued feature vectors without quantization and supporting packing of real valued feature vectors into a single cipher text. They achieve GAR = 99.33% @ FAR = 0.01% on LFW, FEI and GTF.

Kolberget et al. (Kolberget et al. 2020) present an efficiency analysis of post-quantum-secure face template protection schemes based on HE. The authors test if the approach is compliant with the ISO/IEC IS 24745 standards and their security. They achieve a false match rate less than 2% on FERET.

#### 4.2.6. Convolutional Neural Network (CNN)

DCNN is used to learn robust mapping from face images of users to unique binary codes (bit wise randomly generated) assigned to the users (Jami et al. 2019).

Jami et al. (Jami et al. 2019) propose a method for face template protection that improves the matching performance, provides a high level of template security and addresses re-enrolment. They compute identity/class specific perturbations to the input facial feature vectors as a function of gradients of mapping network as in targeted adversarial learning. They achieve GAR = 98% @ FAR =0% on CMU-PIE, FEI and FERET.

Mai et al. (Mai et al. 2020) present a randomized CNN to generate protected face biometric templates given the input face image and a user-specific key. Through user-specific keys, the authors introduce randomness to the secure template to strengthen its security. They achieve GAR = 78.2% @ FAR =0.1% and GAR = 81.9% @ FAR =0.1% on FRGC v2.0, CFP and IJB-A.

Kim et al. (Kim et al. 2021) present the IronMask, architecture, which can be combined with any face recognition system using angular distance metric. They achieve TAR = 99.79%, FAR = 0.0005% and TAR = 95.78%, FAR = 0% on CMU-Multi-PIE, FEI and FERET.

## 5 Discussion

Biometric cryptosystems can be divided in to Key-binding and Key generating biometric cryptosystems.

Key-binding biometric crypto system allows the users to bind external keys with biometric data, but matching has to be done using the ECC, making it prone to key leakage. This represents a broader category and can be further divided in to Fuzzy commitment and Fuzzy Vault Schemes. Fuzzy commitment and fuzzy vault methods are among the oldest and most reliable methods that provide consistently high template security (Wang et al. 2015 - Kaur and Sofat 2017). The methods have been upgraded including approaches like Euclidean-Distance Based Fuzzy Commitment (Gilkalaye et al. 2019) and Two-phase fuzzy vault (Kaur and Sofat 2017), providing even higher levels of security. They

are still commonly used today but not as the only form of template protection, rather they are integrated together with other approaches. There is a relatively large number of papers available for research in this fields.

Key generating biometric cryptosystems can be further divided in to Quantization Schemes, Secure Sketch and Fuzzy extractors. Using key generating, biometric cryptosystem keys can be generated directly from biometric data without any external mechanism and are cancelable, but the keys are not stable. Quantization, secure sketches and fuzzy extractor methods are often used together to provide additional security and are today often hybridized (Bousnina et al. 2021). Quantization is most commonly used with PCA (Wu et al. 2010) and non-uniform quantization (Han et al. 2008). Secure sketches are able to generate extremely low FAR, FRR and EER percentages (Kim and Toh 2007 - Tarek et al. 2021), while keeping a high level of security. Fuzzy extractor is sometimes used interchangeably with secure sketches (Sandhya, Prasad 2017) and achieves high FRR results, which can be further improved in combination with quantization and secure sketches (Blanton and Aliasgari 2013 - Zhang et al. 2021). While fuzzy extractors are still being used relatively commonly in biometric template protection and a good number of papers that use this method can be found, quantization schemes and secure sketches have a slightly lower number of papers that appeared in our searches and were more commonly used as primary methods that were being upgraded with other approaches.

Cancellable Biometrics can be divided in to Salting and Non-invertible Transforms. Cancelable biometrics in general are able to achieve low FAR percentages and generate multiple templates of the same user's biometric. However, they are user-specific and invertible in case of key loss. Salting is an older approach that is still being used and updated. If used with extended random projection (Kim and Toh 2007) and random orthonormal transformation (Wang and Plataniotis 2007), amongst others, the EER is kept low with a high FRR percentage. Today, salting can be combined with Unimodal-Bio-GAN (Tarek et al. 2021) and other neural networks for even better results. A very obvious trend with salting that can be noted is the decline of papers that use this method on its own or as a primary sores.

Non-invertible transformations are able to provide a greater diversity of biometric templates and offer cancelable biometric features, but NT features are hard to generate and it is possible to reconstruct the original trait from stored templates. The authors in (Kaur and Khanna 2019) present an example of random projection with low EER values. In (Sardar et al. 2020) the authors were able to achieve a 0% EER value using hashing and keep the FAR and FRR percentages low with a high GAR percentage in (Lee et al. 2021), using random permutation. The numbers of papers that use Non-invertible transformations I slightly higher then the number of papers that use salting but it can be seen that this is also an approach in decline.

Hybrid approaches are able to increase the template security by combining multiple schemes, but with a high chance of generating dissimilar values of the same feature set. Hybrid methods are currently the most popular ones. A good example is given in (Sree and Radha 2016), where authors present a fuzzy vault hybrid (Nguyen et al. 2019), presenting a fuzzy commitment hybrid updating older and reliable approaches and making them more secure. In (Bousnina et al. 2021), authors present a secure sketch hybrid combined with new transform approaches. Hybrid approaches are the most commonly used approaches today and the number of papers proves that.

HE is regarded as the easiest approach for complying with regulations. This approach enables user collaboration, but a disadvantage of the process time is relatively slow process time. HE is one of the most popular template protection approaches. This method constantly achieves low false match rates (Kolberg et al. 2020) and high GAR and TAR values (Boddeti 2018 - Jindal et al. 2020). HE has a consistent number of papers over the years, while the number of papers is not declining it is also nor rising rapidly, but it stays stable over the years.

CNN-based methods are the newest ones used for BTP. The most common approach for CNN based methods uses Deep CNN-s (Jami et al. 2019 - Kim et al. 2021). Their development requires larger training samples and experienced users, but produces highly secure templates achieving high TAR and GAR values (Jami et al. 2019 - Kim et al. 2021). CNN based approaches offer a great variaty of protection schemes with some examples beeing approaches that use identity/class specific perturbations for input facial feature vectors (Jami et al. 2019), randomized CNN-s (Mai et al. 2020) or an adaptable architecture that can be combined with other face recognition systems (Kim et al. 2021). CNN-based methods and their number has sharply increased over the last few years. There is a solid number of papers available that use this approach.

As can be seen from this paper, the best results are achieved using CNN and hybrid methods. An overall consensus is also that using just one protection scheme does not offer sufficient protection and combining methods is the way forward. Attacks on biometric templates are getting more and more sophisticated and to keep up with that template protection schemes need to adopt and offer better protection. New methods using AI and CNN-s are being developed daily, strengthened through hybridization, by combining them with the strongest and most secure aspects of different approaches

# 6 Conclusion

The aim of template protection is keeping biometric data safe. As using face images as a mean of

authentication becomes more prevalent, stronger and more robust templates need to be created to protect our biometric traits. The breach of a biometric template can have devastating consequences for the end user, as we cannot simply replace our own face.

In this paper we have given a brief overview of biometric facial template protection methods. From the presented works, we can conclude that the usage of some methods like steganography and watermarking lessens with each year, and new methods based on CNN and hybrid methods are becoming more common.

One major point we came across was the terminology problem, especially in the fields of secure sketch, fuzzy extractors and non-invertible transforms. Problems arose in some works where the terms secure sketch and fuzzy extractors were used interchangeably, as well as in non-invertible transforms and their sub-categories. We can conclude that a need for a standardized and well-defined terminology exists.

The field of template protection is still growing and evolving. With more and more people using biometric traits as authentication methods, it is conceivable that biometric authentication could replace security measures like PINs and passwords in the near future. Thus, the need for stronger template protection is greater than ever.

## Acknowledgments

This research was funded by the project "Development of CSTI platform for retrieval and analysis of structured and unstructured data". The project received funding from the European Regional Development Fund through OP Competitiveness and Cohesion 2014–2020 within the Call for Proposals "Development of the products and services arising from research and development activities Phase II", under grant number KK.01.2.1.02.0310.

## References

Shahreza, H. O., Hahn, V. K., & Marcel, S. (2022). MLP-Hash: Protecting Face Templates via Hashing of Randomized Multi-Layer Perceptron. arXiv preprint arXiv:2204.11054.

Kaur, H., & Khanna, P. (2016). Biometric template protection using cancelable biometrics and visual cryptography techniques. Multimedia Tools and Applications, 75(23), 16333-16361.

Sarkar, A., & Singh, B. K. (2020). A review on performance, security and various biometric template protection schemes for biometric authentication systems. Multimedia Tools and Applications, 79(37), 27721-27776.

Sandhya, M., & Prasad, M. V. (2017). Biometric template protection: A systematic literature review of approaches and modalities. Biometric security and privacy, 323-370.

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

Wang, N., Li, Q., El-Latif, A., Ahmed, A., Peng, J., Yan, X., & Niu, X. (2015). A novel template protection scheme for multibiometrics based on fuzzy commitment and chaotic system. Signal, Image and Video Processing, 9(1), 99-109.

Elrefaei, L. A., & Al-Mohammadi, A. M. (2019). Machine vision gait-based biometric cryptosystem using a fuzzy commitment scheme. Journal of King Saud University-Computer and Information Sciences.

Gilkalaye, B. P., Rattani, A., &Derakhshani, R. (2019, May). Euclidean-distance based fuzzy commitment scheme for biometric template security. In 2019 7th International Workshop on Biometrics and Forensics (IWBF) (pp. 1-6). IEEE.

Wu, L., & Yuan, S. (2010, September). A face based fuzzy vault scheme for secure online authentication. In 2010 Second International Symposium on Data, Privacy, and E-Commerce (pp. 45-49). IEEE

Nagar, A., Nandakumar, K., & Jain, A. K. (2011). Multibiometric cryptosystems based on feature-level fusion. IEEE transactions on information forensics and security, 7(1), 255-268.

Kaur, M., & Sofat, S. (2017, May). Fuzzy vault template protection for multimodal biometric system. In 2017 International Conference on Computing, Communication and Automation (ICCCA) (pp. 1131-1135). IEEE.

Li, Q., & Chang, E. C. (2006, September). Robust, short and sensitive authentication tags using secure sketch. In Proceedings of the 8th workshop on Multimedia and security (pp. 56-61).

Han, Q., Wang, Z., & Niu, X. (2008). An Improved Biometric Template Protection Method based on Non-Uniform Quantization. Journal of Digital Information Management, 6(2).

Wu, L., Liu, X., Yuan, S., & Xiao, P. (2010, October). A novel key generation cryptosystem based on face features. In IEEE 10th International Conference on Signal Processing Proceedings (pp. 1675-1678). IEEE.

Li, Q., Sutcu, Y., & Memon, N. (2006, December). Secure sketch for biometric templates. In International Conference on the Theory and Application of Cryptology and Information

Security (pp. 99-113). Springer, Berlin, Heidelberg.

Sutcu, Y., Li, Q., & Memon, N. (2007). Protecting biometric templates with sketch: Theory and practice. IEEE Transactions on Information Forensics and Security, 2(3), 503-512.

Dang, T. T., Truong, Q. C., & Dang, T. K. (2013, March). Practical construction of face-based authentication systems with template protection using secure sketch. In Information and Communication Technology-EurAsia Conference (pp. 121-130). Springer, Berlin, Heidelberg.

Blanton, M., & Aliasgari, M. (2013). Analysis of reusability of secure sketches and fuzzy extractors. IEEE transactions on information forensics and security, 8(9), 1433-1445.

Chen, C., Wang, C., Yang, T., Lin, D., Wang, S., & Hu, J. (2014, August). Optional multi-biometric cryptosystem based on fuzzy extractor. In 2014 11th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD) (pp. 989-994). IEEE.

Zhang, K., Cui, H., & Yu, Y. (2021). Facial Template Protection via Lattice-based Fuzzy Extractors. Cryptology ePrint Archive.

Kim, Y., & Toh, K. A. (2007, September). A method to enhance face biometric security. In 2007 First IEEE International Conference on Biometrics: Theory, Applications, and Systems (pp. 1-6). IEEE.

Wang, Y., & Plataniotis, K. N. (2007, September). Face based biometric authentication with changeable and privacy preservable templates. In 2007 Biometrics Symposium (pp. 1-6). IEEE.

Tarek, M., Hamouda, E., & El-Metwally, S. (2021). Unimodal-Bio-GAN: Keyless biometric salting scheme based on generative adversarial network. IET Biometrics, 10(6), 654-663.

Kaur, H., & Khanna, P. (2019). Random Slope method for generation of cancelable biometric features. Pattern Recognition Letters, 126, 31-40.

Sardar, A., Umer, S., Pero, C., & Nappi, M. (2020). A novel cancelableFaceHashing technique based on non-invertible transformation with encryption and decryption template. IEEE Access, 8, 105263-105277.

Lee, H., Low, C. Y., & Teoh, A. B. J. (2021, January). SoftmaxOut transformation-permutation network for facial template protection. In 2020 25th International Conference on Pattern Recognition (ICPR) (pp. 7558-7565). IEEE.

Sree, S. S., & Radha, N. (2016, January). Cancellable multimodal biometric user authentication system with fuzzy vault. In 2016 International Conference on Computer Communication and Informatics (ICCCI) (pp. 1-6). IEEE.

Nguyen, T. A. T., Dang, T. K., & Nguyen, D. T. (2019, January). A new biometric template protection using random orthonormal projection and fuzzy commitment. In International Conference on Ubiquitous Information Management and Communication (pp. 723-733). Springer, Cham.

Bousnina, N., Ghouzali, S., Mikram, M., Lafkih, M., Nafea, O., Al-Razgan, M., & Abdul, W. (2021). Hybrid multi-modal biometric template protection. IntellAutom Soft Comput, 27(1), 35-51.

Boddeti, V. N. (2018, October). Secure face matching using fully homomorphic encryption. In 2018 IEEE 9th International Conference on Biometrics Theory, Applications and Systems (BTAS) (pp. 1-10). IEEE.

Jindal, A. K., Shaik, I., Vasudha, V., Chalamala, S. R., Rajan, M. A., & Lodha, S. (2020, December). Secure and privacy preserving method for biometric template protection using fully homomorphic encryption. In 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom) (pp. 1127-1134). IEEE.

Kolberg, J., Drozdowski, P., Gomez-Barrero, M., Rathgeb, C., & Busch, C. (2020, September). Efficiency analysis of post-quantum-secure face template protection schemes based on homomorphic encryption. In 2020 International Conference of the Biometrics Special Interest Group (BIOSIG) (pp. 1-4). IEEE.

Jami, S. K., Chalamala, S. R., & Jindal, A. K. (2019, January). Biometric template protection through adversarial learning. In 2019 IEEE International Conference on Consumer Electronics (ICCE) (pp. 1-6). IEEE.

Mai, G., Cao, K., Lan, X., & Yuen, P. C. (2020). Secureface: Face template protection. IEEE Transactions on Information Forensics and Security, 16, 262-277.

Kim, S., Jeong, Y., Kim, J., Kim, J., Lee, H. T., & Seo, J. H. (2021). IronMask: Modular architecture for protecting deep face template. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (pp. 16125-16134).