Quantifying Privacy and Security of Biometric Fuzzy Commitment

Xuebing Zhou\textsuperscript{1,3}, Arjan Kuijper\textsuperscript{1}, Raymond Veldhuis\textsuperscript{2}, and Christoph Busch\textsuperscript{3}

\textsuperscript{1}Fraunhofer IGD, Fraunhoferstrasse. 5, 64295 Darmstadt, Germany
\textsuperscript{2} University of Twente, PO Box 217, 7500 AE Enschede, The Netherlands
\textsuperscript{3} Hochschule Darmstadt - CASED, Mornewegstrasse 32, Germany, 64293 Darmstadt

Abstract

Fuzzy commitment is an efficient template protection algorithm that can improve security and safeguard privacy of biometrics. Existing theoretical security analysis has proved that although privacy leakage is unavoidable, perfect security from information-theoretical points of view is possible when bits extracted from biometric features are uniformly and independently distributed. Unfortunately, this strict condition is difficult to fulfill in practice. In many applications, dependency of binary features is ignored and security is thus suspected to be highly overestimated.

This paper gives a comprehensive analysis on security and privacy of fuzzy commitment regarding empirical evaluation. The criteria representing requirements in practical applications are investigated and measured quantitatively in an existing protection system for 3D face recognition. The evaluation results show that a very significant reduction of security and enlargement of privacy leakage occur due to the dependency of biometric features. This work shows that in practice, one has to explicitly measure the security and privacy instead of trusting results under non-realistic assumptions.

1. Introduction

Biometrics is a convenient authentication method and binds a person and his/her identity together. Biometric applications grow rapidly and cover diverse areas such as physical or logical access control, border control, banking, e-Health, forensics etc. Meanwhile, related security risks and privacy concerns have been drawing a lot of attention. Biometric data may contain sensitive private information such as diseases, genetic information, etc. Therefore, the usage of biometrics can harm the privacy of users. Additionally, if stored biometric data is compromised, it can cause serious security problems. For instance, an adversary can use it to reconstruct a fake modality or to track activities of a victim in other applications and conduct identity fraud. Due to the uniqueness of biometric data, renewing and revocation of biometric templates are impossible. This security drawback limits the application of biometrics in identity management.

Biometric template protection has been developed to prevent exposure of biometric data and to redeem security weaknesses. It can convert biometric data into a secure form. On the one hand, the retrieval of biometric data from secure templates is hard or impossible. On the other hand, numerous independent templates can be derived from one biometric datum in order to prevent cross matching and enable renewing and revocation. Different template protection algorithms exist. In [9] Jain et al. gave an overview and classified the existing algorithms into transformation-based approaches and biometric cryptosystems. In the first category, transformation functions are used to distort biometric data. For instance, biometric encryption [18] and biohashing [3] utilize different randomization process, while cancelable biometrics [14] is based on non-invertable functions. In the second category, algorithms such as fuzzy extractor [6], fuzzy commitment [11], fuzzy vault [10] and fuzzy embedder [2], can bind a secret with biometric data.

Among them, fuzzy commitment is one of the most popular methods and has been successfully integrated for many biometric modalities. Despite this, a rigorous security and privacy assessment is still missing, especially for the evaluation of real systems. This paper focus on the quantitative assessment of fuzzy commitment in practice and has the following contributions: Firstly, we comprehensively summarize the evaluation criteria and compare different possible metrics. The distribution of biometric features has a strong influence on the security. Secondly, we introduce the second order dependency tree, which can efficiently characterise the dependency of biometric features. Thirdly, we strictly evaluate the proposed criteria in a fuzzy commitment scheme for 3D face recognition. The distribution of 3D face features is estimated. We show that the depen-
dency of features reduces the security and privacy significantly and increases privacy leakage.

The rest of paper is organised as follows: in Section 2 we introduce the fuzzy commitment scheme, give an overview of the related security analyses, and propose the evaluation criteria and the corresponding metrics for privacy and security assessment; in Section 3 we show an implementation of an existing fuzzy commitment scheme for 3D face recognition; in Section 4 we estimate the distribution of 3D face features and evaluate the protected system using information-theoretical metrics; in Section 5 we discuss the influence of feature dependency on the security and privacy and elaborate on the modelling of feature dependency. Moreover, the security requirements of fuzzy commitment in practice are expounded. Conclusions and future work are given in Section 6.

2. Security and Privacy Criteria and Metrics

The fuzzy commitment scheme was firstly proposed by Juels and Wattenberg in [11]. The main idea is to assign a random secret to a subject instead of using the biometric data itself. Authentication is performed through a correct regeneration of the secret with a biometric datum and some helper data, which attempts to compensate for errors between enrolled and queried biometric data. A block diagram of fuzzy commitment is shown in Figure 1.

![Figure 1. A block diagram of fuzzy commitment](image)

The encoder and the decoder of fuzzy commitment share the helper data $W$ and the two correlated biometric feature $X$ and $X'$. They try to extract exactly the same secret. The side information $W$ can be public and should reveal little information about $S$ or $X$:

$$W = C \oplus X$$ (1)

The error correction codeword $C$ corresponds to the secret $S$. Error correction coding is necessary, since biometric features are noisy. The stored secure template consists of the hash of the secret $h(S)$ and $W$.

If fuzzy commitment is information-theoretically (perfectly) secure, the helper data $W$ provides no information about the secret. In other words, the secret is expected to be uniformly independently distributed even given $W$ and an adversary can only perform a brute force attack. However, it is only an ideal case. In this section we will analyse the criteria and metrics towards empirical quantitative assessment.

2.1. Related Work

The security and privacy performance of fuzzy commitment is well analysed theoretically. In [19], Tuyls and Goseling showed secret extraction from biometric data is possible with helper data and the maximum achievable secret size is equal to the mutual information between enrolled and queried features. They also proved that perfect security is possible, if the bits extracted from biometric features are uniformly independently distributed. In [8], Ignatenko furthermore gave a boundary of possible secret rate and privacy leakage rate for the helper data scheme.

In [6], Dodis et al. proposed a $(\mathcal{M}, m, \tilde{m}, t)$- secure sketch for arbitrarily distributed feature $X$ in a space $\mathcal{M}$ with min-entropy $H_\infty(X) = m$. And $\tilde{m}$ is average min-entropy $H_\infty(X|W)$, which indicates the maximum probability recovering $X$ given $W$ on average. Entropy loss is defined as $m - \tilde{m}$, which is necessary to compensate for noise. Additionally, they proposed the statistical distance $SD$, which can evaluate the deviation of the distribution of $X$ from a uniform distribution regarding $W$.

Fuzzy commitment can be considered as a fuzzy extractor\(^1\) using code-offset or a special case of the helper data scheme. In [8], it is shown that fuzzy commitment has high privacy leakage and the optimal trade-off between secret size and privacy leakage can only be achieved by the maximum secret rate.

Fuzzy commitment has been successfully implemented in different biometric systems. Unfortunately, in most of the implemented fuzzy commitment systems, e.g. [1, 20, 21] etc, the distribution of the bits extracted from biometric data is not analysed, and a uniform and independent distribution is assumed in the security analyses. In [7], Hao et al. gave a more realistic security assessment for their iris fuzzy commitment scheme. With the efficient error correction coding method, a 140 bit long secret can be extracted at FRR of 0.47 and zero FAR. The interclass Hamming distance of the iris features is binomial distributed and their discriminative power is 249 bits. The coding scheme tolerates up to 27% bit error rates. With the sphere-packing bound, they calculated that searching the secret requires at least $2^{44}$ combinations, if an attacker knows the correlation properties of iris codes. However, they claimed that the system is secure enough, since “we really do not know how to correlate someone’s iris bits unless we know their iris code anyway.” In the rest of the section we will systematically propose the evaluation criteria and compare the possible metrics for a practical privacy and security assessment. In Section 4 we will show a simple way to analyse the dependency of biometric features and demonstrate how to give a rigorous assessment in practice.

---

\(^1\)In [6] other extractors, e.g. in a set different space, were also proposed.
### 2.2. Evaluation Criteria

Although the existing works indicate how to evaluate fuzzy commitment, they address only part of security and privacy requirements and comprehensive analyses are lacking. Recalling the security and privacy requirements on template protection, we propose the following evaluation criteria: security, privacy protection ability and unlinkability. For a fuzzy commitment scheme, security measures the hardness to retrieve the secret from a secure template. Privacy protection ability can be assessed regarding irreversibility and privacy leakage. Irreversibility shows the complexity to retrieve biometric features, while privacy leakage quantifies how much information about biometric data contained in a secure template. Another important criterion is unlinkability. Assume that an adversary obtains two secure templates. It should be difficult for him to verify whether they are generated from the same subject or not. Additionally, combining two secure templates should not be helpful to estimate secrets or to retrieve biometric features. In this paper we concentrate on the assessment of security and privacy. The related unlinkability analysis of fuzzy commitment can be found in [16, 12].

In order to measure those criteria, we also need to define the ability of an adversary. In this paper we apply Kerckhoffs’ principle and assume that an adversary has full knowledge about the system as well as the distribution of the biometric features.

### 2.3. Evaluation Metrics

The evaluation metrics are used to quantify the different criteria. In this section we summarize possible metrics and explain their meanings for security and privacy.

The security can be measured with average min-entropy, conditional entropy, conditional guessing entropy and statistical distance. The average min-entropy $H_{\infty}(S|W)$ corresponds to the probability of the most likely secret given $W$. It quantifies security performance in the worst case scenario and represents the lower bound of the security. Therefore, it is a very necessary metric in a strict evaluation. The conditional entropy $H(S|W)$ measures the uncertainty about $S$ given $W$. The conditional guessing entropy $G(S|W)$ shows the average number of the guesses needed using an optimal searching strategy till the true secret is found. The statistical distance $SD((S, W), (F_{L_S}, W))$ measures the deviation of the distribution $P(S, W)$ to the distribution $P(F_{L_S}, W)$, where $F_{L_S}$ is the uniformly distribution on $L_S$ bit binary strings and $L_S$ is the secret length. The closer $P(S, W)$ is to $P(F_{L_S}, W)$, the smaller is their $SD$ and the higher is the security.

The privacy protection ability consists of two aspects, irreversibility and privacy leakage. Irreversibility can be measured with the same metrics as in the security assessment. Due to the XOR used in fuzzy commitment, $X$ is totally compromised, if $S$ is known. It is proved in [8] that

$$H(S|W) = H(X|W)$$

The irreversibility evaluation can be combined with the security evaluation. On the other hand, it is known that privacy leakage is unavoidable in fuzzy commitment as proved in [17, 8]. Privacy leakage is caused by the redundancy in an error correction code. However, the leakage needs to be limited and even minimized, since large privacy leakage can cause cross matching of $W$ as shown in [16]. Privacy leakage can be measured with the entropy loss $H_{\infty}(X) - H_{\infty}(X|W)$ and the mutual information $I(X; W)$. The first one measures the leakage in the worst case scenario with the lowest security and the second one measures the average case leakage.

These metrics quantify the security and privacy performance from different aspects. The metrics using min-entropy or average min-entropy show the lower bound of security and privacy achieved with a system. The information-theoretical metrics quantify the performance with entropy. The statistic distance measures the randomness of extracted secrets regarding an ideal uniform distribution. Measuring these metrics requires the information about the corresponding distributions. Obviously, they are also important priori information for an adversary and are helpful to retrieve secrets or biometric data. Distribution estimation of a high dimensional variable can be very complicated. In the next section we will introduce a fuzzy commitment scheme for 3D face recognition. In Section 4 we will show how to estimate the distribution of biometric features empirically and evaluate the security and privacy with information-theoretical metrics in the introduced fuzzy commitment system.

### 3. A Fuzzy Commitment Scheme for 3D Face Recognition

In order to demonstrate the evaluation process, we take a fuzzy commitment scheme for 3D face recognition proposed in [21, 22] as an example. In this section we will briefly introduce the 3D face recognition algorithm and the relevant detail of the fuzzy commitment scheme. Additionally, the experimental results in the Face Recognition Grand Challenge database (FRGC) [13] will be shown.

The feature extraction algorithm uses the distribution of depth values of a face surface to characterize facial geometry. A 3D face image is normalized to a frontal view to compensate for pose variations. Then the facial region is divided into several disjoint horizontal stripes. The histogram of the depth values of the facial points in each stripe is calculated. The algorithm was detailedly described in [23]. In order to obtain uniformly distributed binary features, the resulting normalized histogram values are binarized using their interclass median.
The binary facial feature \( X \) are the input of the fuzzy commitment scheme. Here the BCH-code is used for error correction. The codeword length \( L_C = 2^n - 1 \), where \( n \geq 3 \) and \( n \in \mathbb{N} \). If the length of \( X \) is larger than \( L_C \), then only the \( L_C \) most reliable bits in \( X \) are selected so that the resulting binary string \( \tilde{X} \) is as long as the codeword \( C \). The selection of the reliable bits is based on their error probabilities, which are estimated during the enrolment. The robustness of the algorithm is improved further. The binarization and feature selection were detailedly shown in [21, 22]. We denote \( U \) as the position vector of the selected reliable bits. \( W \) is the bitwise XOR of \( \tilde{X} \) and \( C \). Only \( U \), \( W \) and \( h(S) \) are stored in data storage.

During the verification process, the binary string \( X' \) is extracted from a queried 3D image. \( \tilde{X}' \) is the reliable bits in \( X' \) selected with \( U \). A corrupted codeword \( C' \) is obtained by XOR of \( W \) and \( \tilde{X}' \). If the number of errors occurring in \( C' \) is within the error correction ability of the BCH-code, the correct secret can be calculated and a positive result can be given comparing its hash with the stored one.

The algorithm is tested in the FRGC databases [13]. Only the 380 subjects, that have more than 4 samples, are used in the experiment. 3 samples per subject are randomly chosen as enrolled samples and the rests are for the verification. The tests are repeated 4 times. We use different settings of the feature extraction and BCH coding. We choose the length of BCH-code of 255, which gives the best recognition performance. The resulting \( FMR \) and \( FNMR \) are shown in Table 1, where \(( L_C, L_S, t) \) stand for the codeword length, the secret length and the number of correctable bit errors respectively. \( L_X \) is the length of biometric feature \( X \) before the selection of the reliable bits. Since \( t \) is similar to the decision threshold comparing the Hamming distance of binary features, the \( FMR \) increases and the \( FNMR \) decreases with increasing \( t \). By the same setting of BCH-code, \( FMR \) of \( L_X = 476 \) is smaller than that of 884, meanwhile \( FNMR \) is larger.

<table>
<thead>
<tr>
<th>((L_C, L_S, t))</th>
<th>(L_X = 476)</th>
<th>(L_X = 884)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(255, 37, 45)</td>
<td>7.96% 3.21%</td>
<td>5.28% 4.68%</td>
</tr>
<tr>
<td>(255, 47, 42)</td>
<td>9.64% 2.75%</td>
<td>6.09% 4.03%</td>
</tr>
<tr>
<td>(255, 55, 31)</td>
<td>17.68% 1.32%</td>
<td>11.44% 2.04%</td>
</tr>
<tr>
<td>(255, 71, 29)</td>
<td>19.97% 1.12%</td>
<td>12.86% 1.73%</td>
</tr>
</tbody>
</table>

Table 1. \( FNMR \) and \( FMR \) at different coding settings and feature lengths.

In this section we show the recognition performance at different settings. Although a long secret can be extracted, without analysing the distribution of biometric features, we don’t know whether the secret size can represent the security of the system or not. In the next section, we will strictly evaluate the security and privacy of the system with the distribution analysis.

4. Quantitative Assessment on Privacy and Security

As shown in Section 2.3, the distribution of the extracted bits is indispensable for the assessment of security and privacy. In this section we will firstly analyse the distribution of the 3D face features and estimate their entropy. Secondly, we will make use of the feature distribution and quantify the privacy and security with information-theoretical metrics.

4.1. Distribution of Binary Features

We analyse the distribution of individual bits in the 3D facial features. If a bit is uniformly distributed, its probability being 1 or 0 is equal. We define a hypothesis test to evaluate whether a bit is uniformly distributed. The \( p \)-value is set to 0.05. Only 196 bits in 476 bit long features and 289 bits in 884 bit long features can be considered as uniformly distributed.

Theoretically, uniformity can be achieved, if real-valued features are binarized with their interclass median. However, binarization thresholds are normally obtained with a separate training process. The thresholds can be different from the interclass median of the testing data, if the training set is not sufficiently large. Additionally, many real-valued 3D features before binarization are skewly distributed and the uniformity of the resulting binary features is very sensitive to the thresholds. Therefore, a uniform distribution can be hard to achieve in practice.

We denote \( P(X) \) as the probability of feature \( X = [x_1, x_2, \ldots, x_{L_X}] \). Here we make a simplification and describe the distribution of \( X \) with the second-order dependency tree:

\[
\hat{P}(X) = \prod_{i=1}^{L_X} P(x_{u_i}|x_{u_{j(i)}}), \quad 0 \leq j(i) < i
\]

where \([u_1, u_2, \ldots, u_{L_X}]\) is a permutation of index \([1, 2, \ldots, L_X]\) and \( P(x_{u_i}|x_{u_{j(i)}}) \) is equal to \( P(x_{u_i}) \) by definition. Only the dependency of a bit to one of its previous bits is taken into account during the calculation. Chow and Liu analysed how to optimize this estimation in the sense of Kullback-Leibler distance [4]. Therefore, Eq. (3) is also called Chow-Liu representation. If \( \hat{H}(X) \) is the estimated entropy with \( \hat{P}(X) \), then with the chain rule of the joint entropy:

\[
\hat{H}(X) = H(x_{u_1}) + \sum_{i=2}^{L_X} H(x_{u_i}|x_{u_{j(i)}})
\]

\[
= \sum_{i=1}^{L_X} H(x_{u_i}) - \sum_{i=2}^{L_X} I(x_{u_i}, x_{u_{j(i)}})
\]
\begin{table}[h]
\centering
\begin{tabular}{|c|c|c|c|c|c|}
\hline
\textbf{m} & \textbf{H(X)} & \textbf{H(X)/L_X} & \textbf{H(X)} & \textbf{H(X)/L_X} \\
& \textbf{Training} & \textbf{Testing} & \textbf{Training} & \textbf{Testing} \\
\hline
476 & 153.7 & 1.51 & 175.6 & 1.45 & 0.323 & 0.370 \\
884 & 280.2 & 2.67 & 349.2 & 2.62 & 0.317 & 0.395 \\
\hline
\end{tabular}
\caption{The mean and standard deviation of the estimated entropy and the information rate for the training and testing set.}
\end{table}

It is shown in [4] that Kullback-Leibler distance between the real distribution of \(X\) and the second-order dependency tree is dependent on the following variables:

\[
D(P(X)||\hat{P}(X)) = \sum_{i=1}^{L_X} H(x_{u_i}) - H(X) - \sum_{i=2}^{L_X} I(x_{u_i}, x_{u_{j(i)}})
\]

The first two terms are constant and minimizing the estimation error is equivalent to maximize \(\sum_{i=2}^{L_X} I(x_{u_i}, x_{u_{j(i)}})\). In this case, the best estimation of the entropy is:

\[
\hat{H}(X) = \sum_{i=1}^{L_X} H(x_{u_i}) - \max_{\{u_1, \cdots, u_{L_X}\}} \left\{ \sum_{i=2}^{L_X} I(x_{u_i}, x_{u_{j(i)}}) \right\}
\]

In our experiments, the mutual information \(I(x_i, x_{i'})\) is calculated for all \(i, i' \in [1, 2, \cdots, L_X]\) and \(i \neq i'\). If \(x_i\) and \(x_{i'}\) are independent, \(I(x_i, x_{i'}) = 0\). If they are totally dependent on each other, then \(I(x_i, x_{i'}) = H(x_i) = H(x_{i'})\). Then the sum of the mutual information is maximized with the hierarchical clustering method based on the nearest neighbor and the corresponding permutation of feature vectors is obtained. The database contains 4 subsets generated with different enrolment samples. We take one subset to train the second order dependency tree. Then we apply the resulting tree structure to the remaining 3 subsets and calculated \(\hat{H}(X)\). The experimental results are shown in Table 2.

4.2. Assessment of Privacy and Security

In the protected 3D face recognition system (see Section 3), the BCH-code is used. It is a systematic code: the first \(L_S\) bits in the codeword is equal to secret \(S\) and the remaining \(L_C - L_S\) bits are redundant bits. We denote the selected binary feature as \(X = [x_{u_1}, \cdots, x_{u_{L_C}}] = X_{u_{1:L_C}}\). We can estimate the security as follows:

\[
H(S|W) \leq H(X_{u_1:L_C}|W) \leq H(X_{u_1:L_S})
\]

where equality \(a\) is derived from Eq. (2); equality \(b\) is valid since it is sufficient to retrieve \(S\), if the first \(L_S\) elements in \(X_{u_1:L_C}\) is successfully guessed; inequality \(c\) is valid because of the relation of the entropy and the conditional entropy. We measure \(H(S|W) = H(X_{u_1:L_S})\) as an approximation of the conditional entropy of \(S\) given \(W\).

Please note that \(H(X_{u_1:L_S})\) is a close upper bound of \(H(S|W)\). \(X_{u_1:L_S}\) corresponds to the secret bits in the BCH codeword. Other \(L_S\) bit combinations in the codeword exist, which can be used to determine the rest \(L_C - L_S\) bits. A closer bound can be given by finding the minimum of the entropy of their corresponding bits in the binary features.

During the experiment, the enrolled secure template is loaded. The secure template contains the position vector \(U = [u_1, u_2, \cdots, u_{L_S}, \cdots, u_{L_C}]\) of the \(L_C\) most reliable bits in \(X\) with \(L_C < L_X\). Then \(H(X_{u_1:L_S})\) is calculated using Eq. (6). Here we use the same datasets in the training and testing.

The variation of \(\hat{H}(X_{u_1:L_S})\) is shown with the boxplot in Figure 2. \(\hat{H}(X_{u_1:L_S})\) is not the half of \(L_S\). For the same \(L_S\), \(\hat{H}(X_{u_1:L_S})\) of \(L_X = 884\) is higher than \(L_X = 476\). The boxplot shows the large variation of \(\hat{H}(X_{u_1:L_S})\), since \(\hat{H}(X_{u_1:L_S})\) is dependent on which bits are selected. The minimum of \(\hat{H}(X_{u_1:L_S})\) is much lower than the average. It means that during the feature selection, not only the reliability of bits but also their joint entropy should be taken into consideration.
Table 3. Security, irreversibility and privacy leakage measurement at different $L_S$ and $L_X$

| $L_X$ | $L_S$ | Security $H(S|W)$ | Irreversibility $\hat{H}(X|W)$ | Privacy Leakage $\hat{I}(X;W)$ |
|------|------|------------------|------------------|------------------|
| 476  | 37   | 9.37             | 66.8             | 86.9             |
|      | 47   | 11.95            | 69.4             | 84.3             |
|      | 55   | 14.14            | 71.6             | 82.1             |
|      | 71   | 18.72            | 76.2             | 77.5             |
| 884  | 37   | 12.09            | 185.3            | 94.9             |
|      | 47   | 15.41            | 188.6            | 91.6             |
|      | 55   | 18.10            | 191.3            | 88.9             |
|      | 71   | 23.74            | 197.0            | 83.2             |

In Table 3, we can observe that security $H(S|W)$ decreases with increasing $L_S$, which means that the uncertainty of the secret reduces. Irreversibility $\hat{H}(X|W)$ and privacy leakage $\hat{I}(X;W)$ also increase with $L_S$, indicating higher information leakage. The irreversibility and privacy leakage are not directly related. For instance, a protected biometric system can be very safe and it is hard for an adversary to retrieve biometric data, meanwhile, it can have high privacy leakage. Privacy leakage can cause further security problems such as linkability. Therefore, it is important to analyse privacy leakage. We use the mutual information to assess privacy leakage:

$$I(X;W) = \hat{H}(X) - H(X|W)$$

This equation shows that the privacy leakage is only related to the selected binary feature $X_{u_iL}^c$.

Table 3 shows the experimental results of security, irreversibility and privacy leakage. The results are the average numbers over all the subjects. The estimated $H(S|W)$ grows linearly with $L_S$, but is much smaller than $L_S$. For each setting, irreversibility is higher than security. The binary feature is more secure than the secret, since several bits in binary features are discarded and are not used in the generation of secure templates. Irreversibility also increases with security. For the settings with the same feature size and codeword length, irreversibility increases and privacy leakage reduces with the increasing secret size. It shows that a high secret size can improve irreversibility and reduce privacy leakage. In [8], Ignatenko obtained the similar conclusion with the theoretical proof for the case of uniformly and independently distributed binary features.

If fuzzy commitment is perfectly secure, the uncertainty about the secret given the helper data $W$ is equal to the secret length. Our assessment shows that the fuzzy commitment scheme for 3D face recognition is far from perfect security. The security and irreversibility is poor. Privacy leakage is quite high.

### 5. Discussions

Our quantitative assessment shows that dependency of binary biometric features influences strongly security and privacy of fuzzy commitment. Biometric samples, for instance face images or iris images, contain inherent dependency. A feature extraction algorithm can convert samples into compact features for the sake of recognition. Many algorithms exploit local information of a sample, such as the histogram-based 3D face algorithm used in this paper, the Gabor filter for iris recognition [7], etc. Resulting features can preserve the dependency in the original biometric samples. Other algorithms, such as independent component analysis (ICA), principal component analysis (PCA) or linear discriminant analysis (LDA), give holistic description of samples. For PCA and LDA, if the samples are Gaussian distributed and training is representative for the data, resulting features can be independent. However, holistic methods have a poorer recognition performance in general, because they are more sensitive to illumination, expression, etc.

Fuzzy commitment takes binary features as input. Real-valued biometric features need to be binarized firstly. A straightforward binarization process is used in the fuzzy commitment system shown in this paper. The binary features inherit the dependency of the real-valued features, that reduces the security of the system. The relation between the correlation of real-valued features and binary features were analysed in [24]. An ideal binarization process should, on the one hand, preserve the recognition performance of biometric systems; on the other hand, it should produce uniformly and independently distributed (u.i.d.) binary features for the security reason. It can adapt distributions of biometric features. For instance, in the protected 3D face system, the strongly correlated features can be grouped and binarized together in order to reduce the dependency.

In fuzzy commitment, the helper data always leaks information about biometric features. In a perfectly secure system, the helper data exposes no information about the secret. Only in this case, the security can be measured with the
secret size. In many implementations of fuzzy commitment, e.g. [1, 20, 21], the assumption, that features are u.i.d., is made without careful investigation of the real distribution of biometric features, or it is taken that real security is only slightly smaller than the secret size. We demonstrate how seriously dependency can reduce the security. If features are not u.i.d., their distribution should be analysed and the security should be examined independent of the secret size.

If fuzzy commitment is used to protect dependent biometric features, additional process reducing the dependency can improve the security. However, in practice, perfect security is not sufficient. For instance, if the achieved secret size is too small, a system is not resistant to a hash inversion attack. Therefore, the searching complexity and space of secrets given helper data must be large enough in a secure system. Therefore, it is necessary to quantify the security. Whether a biometric system can achieve sufficient security with fuzzy commitment or not, can be estimated with e.g. secret capacity defined in [19]. The maximum number of random secrets, which can be extracted, is not larger than the mutual information between biometric data in enrolment and verification.

To evaluate a fuzzy commitment system, a randomness test of input binary biometric features can be firstly performed. Different kinds of tests are shown in [15], which can verify whether features are u.i.d. or not. If features are u.i.d., the security and privacy can be directly determined with the secret size and the codeword length. If not, the distribution of biometric features needs to be estimated.

In [5] Daugman proposed a simple way to determine the entropy of iris features. The binary features extracted with Gabor filter are uniformly distributed. Their interclass Hamming distance are perfectly binomially distributed. The entropy of iris features is equal to the number of Bernoulli trails of the corresponding binomial distribution. The 2048 bit long features contains 249 bit entropy. It shows that iris features are strongly correlated. In [7] Hao used this results to assess the security of the protected iris system. The method avoids the estimation the distribution of high dimensional features and can efficiently describe the dependency. However, not all features have binomially distributed interclass distance. Additionally, this method can estimate the entropy and the security, but the distribution of features is unknown. The distribution information can be used to retrieve secret or biometric features and is helpful to design binarization and coding processes in fuzzy commitment. We propose an alternative using the second order dependency tree to describe the distribution of binary features. Although only the dependency between two bits is considered, this method is more general and does not rely on a specific distribution. More accurate estimation is possible, if high order dependency of the features is analysed. The distribution estimated with this model can be used to crack fuzzy commitment by optimizing the search for the secret.

6. Conclusions and Outlook

This paper aims to quantify security and privacy of fuzzy commitment and enable rigorous assessment. We comprehensively propose the security and privacy criteria. The possible metrics to quantify security, irreversibility, and privacy leakage are introduced and compared. Additionally, we evaluate a system for 3D face recognition. The distribution of the binary features is characterized with the second order dependency tree. The entropy of the features is calculated. We give a quantitative measure using information-theoretical metrics. The achieved security is much smaller than the secret size. High privacy leakage is observed.

We show that the dependency of binary features has a strong influence on security and privacy. In a security analysis of fuzzy commitment, any assumption on distribution of biometric features must be made very carefully. If dependency of features is ignored, security can be highly overestimated. Moreover, we show how to quantify the security and privacy in practice. It is essential to give a provable security analysis of a real system.

Current research focuses on improving the distribution analysis with a more general model. Furthermore, we will extend our security and privacy assessment to other fuzzy commitment systems and other template protection algorithms and propose a generalised evaluation framework.

References


