Multi-Modal and Multi-Instance Fusion for Biometric Cryptosystems

Johannes Merkle[1], Tom Kevenaar[2], and Ulrike Korte[3]

[1]secunet Security Networks AG, 45128 Essen, Germany
[2]GenKey, 5656 AE Eindhoven, Netherlands
[3]Bundesamt für Sicherheit in der Informationstechnik, 53175 Bonn, Germany

Abstract: Biometric cryptosystems allow cryptographic privacy protection for biometric reference data without storing a secret key. However, their security is inherently limited by the discriminative information content of the biometric feature data. Given the currently exploitable entropy of biometric features, one of the most promising approaches to achieve high privacy levels is to combine several biometric modalities or several instances of the same biometric modality. In this contribution, we theoretically analyze multi-biometric fusion strategies for biometric cryptosystems with respect to their impact on security and recognition accuracy. We also introduce *hash level* as a new fusion level. Furthermore, we give a more detailed analysis for the most prominent schemes, the Fuzzy Commitment Scheme and the Fuzzy Vault.

1 Introduction

Biometrics is increasingly used for secure identification throughout the world. However, biometric data that is collected and stored is, by definition, private and, therefore, demands rigorous protection from misuse. So-called *biometric cryptosystems* (also known as *biometric encryption*) are designed to combine the advantages of biometrics with proven cryptographic techniques so that biometric reference data, as in password-based authentication, is no longer stored in plain text but as a protected templates without the need to maintain secret keys for their decryption. The reconstruction of the biometric information from reference data is impossible unless a sufficiently similar feature data is provided for comparison. These schemes protect the biometric data by binding it to, or extracting from it, a secret string which is retrieved in case of successful verification and can, thus, also be used for biometrically protected key storage and release. Prominent examples of biometric cryptosystems are constructions based on the Fuzzy Commitment [JW99] or the Fuzzy Vault [JS02].

One factor limiting the security of biometric cryptosystems is the entropy of the biometric feature data. In most schemes, including the Fuzzy Commitment and the Fuzzy Vault, the private biometric data are recovered upon successful verification and, thus, an attacker can "decrypt" the protected template in an "FAR attack" by

repeatedly simulating the verification with random biometric samples (taken from a database or generated artificially) in 1/FAR trials on average. For instance, if a biometric cryptosystem has a False Accept Rate of 10^{-5} and each verification (incl. sample acquisition and feature extraction) takes three seconds, the attack could uncover the biometric data from a protected template in less than four days. Since biometric cryptosystems operate on concealed data, achieving very low FAR values is more challenging than for conventional biometric systems [CS09], [YBdG+11].

One of the most promising approaches to achieve low FAR values and, thereby, high privacy levels is to combine the information of several biometric modalities (e.g. fingerprints with finger vein, or face with iris) or several instances of the same biometric modality (e.g. several fingerprints or both irises). Different fusion approaches exist, combining the biometric information on different levels of the verification process. In this contribution, we investigate, how multi-modal or multi-instance fusion can be implemented for biometric cryptosystems and to what extent the recognition accuracy and privacy protection can be increased.

This paper is structured as follows: In Section 2, previous work on multi-biometric fusion for biometric template protection is discussed. In Section 3 we present a general description of biometric cryptosystems, and the Fuzzy Commitment and the Fuzzy Vault as important examples. In Section 4, we present possible multi-modal or multi-instance fusion approaches for biometric cryptosystems, and discuss their flexibility and impact on security in Section 5. Conclusions are drawn in Section 6.

2 Previous Work

Several publications proposed multi-biometric fusion for biometric template protection, e.g. [NJ08], [KBV+09], [KZB+09], [MNS+10], [YBdG+11], but did not provide an analysis of the impact of the fusion level on privacy protection. For instance, in [YBdG+11], Yang et. al. consider decision-level fusion for three template protection methods, one of which is based on the Fuzzy Commitment, but limit their analysis to biometric performance. In [FYLH09], two fusion approaches - biometric level and cryptographic level, roughly corresponding to feature-level and hash-level in our terminology - are theoretically investigated with respect to privacy and recognition accuracy but the privacy analysis is limited to entropy estimations and does not consider the effort of actual attacks; as our analysis will show, an increase of the entropy does not necessarily imply an equivalent increase of the minimum attack complexity. In [NNJ12], Nagar et. al. were the first to observe that decision-level fusion is less secure against exhaustive search attacks than feature-level fusion, and the authors present a feature-level fusion framework comprising algorithms for transforming templates into a common metric space and for fusion of the (transformed) templates.

3 Biometric cryptosystems

As any biometric authentication methods, biometric cryptosystems comprise procedures for enrollment and authentication.

- Enrollment. The biometric feature data X extracted from a reference sample are processed by the enrollment function of the biometric cryptosystem, which outputs a binary verification string R and helper data D to be used for error correction during verification. The verification string is hashed by a cryptographic one-way hash function. Both the helper data D and the hash value h of the verification string are stored as protected reference data.
- Verification. The biometric feature data Y extracted from a live sample and the helper data D are processed by the verification function of the biometric cryptosystem, resulting in a candidate verification string S. Provided that X and Y are sufficiently similar, S equals R. The equality of these strings is checked using the stored hash value h.

This high level work-flow for biometric cryptosystems is depicted in Figure 1.

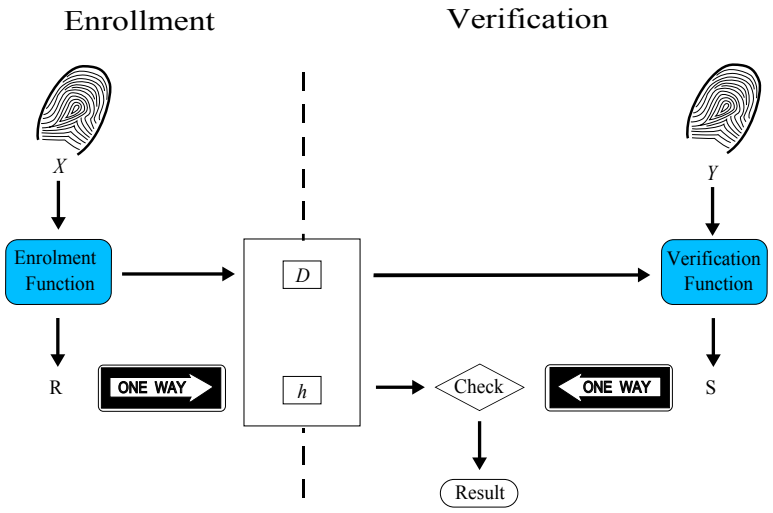

Figure 1: Processing in a biometric cryptosystem.

Prominent examples of biometric cryptosystems are the Fuzzy Commitment Scheme and the Fuzzy Vault. While the Fuzzy Commitment Scheme can correct errors that are bounded with respect to the Hamming metric, i.e. individual bit errors, the Fuzzy Vault works on an unordered set of features and is, thus, agnostic to permutations and tolerant to omissions an insertions of features. Further examples are quantization schemes with correction vector (e.g. [LT03] and [BDH+10]). An exhaustive survey is given in [CS09].

Unlike traditional biometric authentication methods, the verification procedure of biometric cryptosystems does not return a similarity score but just a one-bit *Accept/Reject* decision. However, if error correcting decoding is used, upon successful verification of the bit string, the original biometric feature data used at enrollment is recovered, and thus, the distance (with respect to some metric) of the biometric data provided for verification to the original feature data can be output as similarity score. While this a posteriori quantification of similarity allows flexible adjustment of the error rates without the need to re-enroll individuals, it has no impact on the level of privacy protection as an attacker trying to recover biometric data from the template would have succeeded already as soon as the error correction was successful.

Various types of attacks can be mounted on biometric cryptosystems, e.g. see [CS09] or [KKM+10]. In this publication, we only consider brute-force attacks on a single protected template resulting from multi-modal or multi-instance fusion. These include FAR attacks, which simulate the specified verification function, as well as attacks that directly exploit the information leakage from the helper data without simulating the verification function.

4 Multi-modal and multi-instance fusion strategies

In this section, fusion approaches for biometric template protection methods are described. For the ease of reading, we consider the case that two fingerprints are used, but the generalization to other modalities and more instances is straightforward. In Section 5, the impact on security and flexibility of the individual fusion strategies are discussed.

Multi-biometric fusion methods can be categorized according to the level in the processing where the information from the features is combined. Typically, three levels are distinguished: feature level, score level and decision level.[1]

The use of biometric template protection techniques, where reference data is only available in protected form, makes it necessary to reconsider how the data from different instances (of one or several modalities) can be combined. In particular, the usage of a hash value introduces a new level of fusion.

Feature-level Fusion In feature-level fusion, two feature vectors X_1 and X_2 obtained from two fingerprints during enrollment are combined to form a new feature vector X which is given as input to the enrollment function to compute the helper data D and the hash value h. Similarly, during verification, two feature vectors Y_1 and Y_2 are extracted from the two probe fingerprints and are combined

[1] Some text books like [RNJ06] also mention sensor (or sample) level fusion where the raw data is fused before any feature extraction is performed. With respect to biometric cryptosystems, this type of fusion can be considered equivalent to feature level fusion, because the biometric data is fused before given as input to the enrollment and verification functions.

to form a new feature vector Y. This feature vector Y, along with D, is given to the verification function, which computes the bit string S, which is then verified against the hash value h.

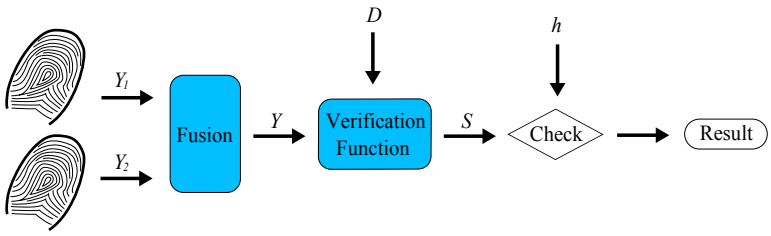

Figure 2: High-level processing of verification for feature level fusion

In case of the Fuzzy Commitment Scheme, a simple way to fuse two feature vectors, both represented as binary strings, is concatenation [KZB+09]. In the Fuzzy Vault, where feature vectors are represented as sets of attributes each encoding a feature component, the fusion can be most easily performed by either ordered concatenation of the sets [NJ08], or by appending to each attribute an index of the instance, and using the union of the sets of the individual instances [MNS+10]. For multi-modal fusion, it can be difficult to define feature representations for all instances and a fusion method so that the resulting feature vector can be processed by the biometric cryptosystem and the expected errors are bounded. In [NNJ12], several algorithms for transforming templates into a common metric space and for fusion of the (transformed) templates were proposed that facilitate feature level fusion for modalities with different error characteristics.

Hash-level Fusion Since biometric cryptosystems base the success decision on an equality check of a hash value, the multi-biometric fusion can also be implemented on the *hash level*. Precisely, the enrollment function is executed on the feature data of both instances individually, resulting in separate parts D_1 and D_2 of the helper data and two bit strings S_1 and S_2, which are concatenated before hashing. During verification, the stored hash value $h(S_1|S_2)$ is used to verify the correctness of the two strings S_1' and S_2' computed from the feature data from each instance and the corresponding part D_i of the helper data.

Score-level Fusion In score-level fusion, each instance is processed by the verification function separately (using separate helper data), resulting in two similarity scores which are then combined. For a biometric cryptosystem, score-level fusion is only possible if a score is computed by an a posteriori quantification of similarity of the feature vector (see Section 3). Since the score is only computed after successful verification of the string S, the bit strings for each instance can be either verified by separate hash values or a joint hash value. Thus, score-level fusion can be seen as a post-processing step after a match is achieved based on hash-level fusion or

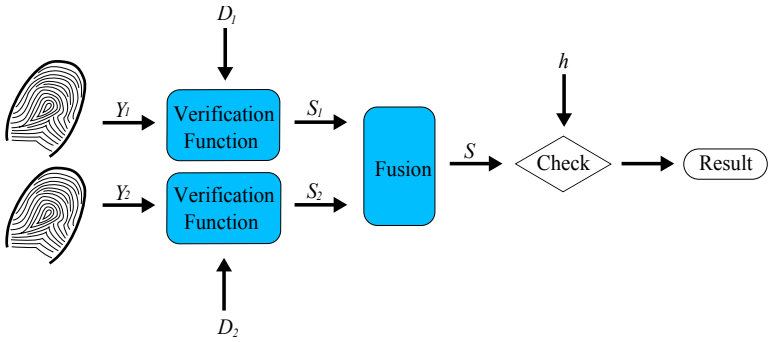

Figure 3: High-level processing of verification for hash-level fusion

decision-level fusion.

Decision-level Fusion For fusion at the decision-level, for each instance, separate helper data and hash values are stored. The binary results ("accept" or "reject") of the hash string verifications of both instances are combined at the Boolean level to obtain the final decision.

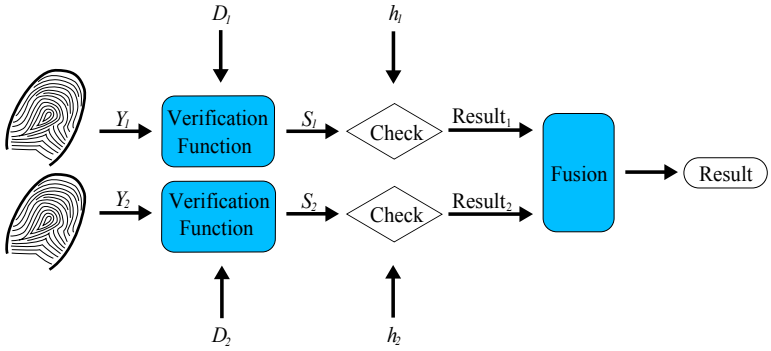

Figure 4: High-level processing of verification for decision-level fusion

5 Analysis of Fusion Strategies

Ideally, the security level - expressed by the minimum expected run time of attacks - resulting from the fusion of several instances of one or more biometric modalities would be the product of the security levels achieved for each single instance, which would imply an exponential increase of security with the number of instances used. However, there are two factors that can reduce the security of the fusion:

- The instances fused may not be statistically independent. For example, it is

known that the patterns types (left/right loop, whorl, arch, etc.) of different fingers of an individual are correlated [Way04]. In this case, the total entropy of all instances can be much lower than the sum of the entropies of the individual instances.

- Depending on the fusion approach taken and the biometric template protection method, an attacker may be able to attack each instance individually. Optimally, the success probability of an attacker trying to guess the features $X_1, \ldots, X_n$ of all instances as $x_1, \ldots, x_n$ is the product over the conditional probabilities $P(X_i = x_i | X_{i-1} = x_{i-1})$, and the average number of guesses needed by an exhaustive search attack is proportional to the inverse of the maximum of this product, which corresponds to the min-entropy of $(X_1, \ldots, X_n)$ [DORS08]. However, if the features of the individual instances can be guessed separately, i.e. if the attacker can verify the correctness of a guess $X_i = x_i$ independent of the other features X_j with $j \neq i$, the average number of guesses needed is only the sum of the inverses of the conditional probabilities. Even if the statistical dependence of the features is sufficiently small so that the total entropy increases linearly with the number of instances, the security gain against exhaustive search is not exponential but only linear if the instances can be attacked separately. Therefore, the security of biometric template protection methods applied to multi-biometric features heavily depends on the approach taken for combining the feature data.

In this section, the fusion approaches feature-level, hash-level, score-level fusion and decision-level are discussed with respect to their flexibility and impact to security for biometric cryptosystems.

5.1 Feature-level Fusion

Feature-level fusion does not allow an attacker to conduct an exhaustive search on a single instance, as the features are combined before the bit strings S are computed on which basis the correctness of the feature data is verified. The search spaces comprises all potential combinations of feature vectors from all instances, and therefore, the level of privacy protection is maximally increased: if the statistical dependencies of the instances are limited, feature-level fusion can induce an exponential increase of attack complexities with the number of instances.

On the other hand, the impossibility to verify the contributing instances separately may be considered a disadvantage in some circumstances. For example, when fusing several fingerprints on the feature-level, it is not possible to perform a comparison with latent fingerprint of only one finger. However, this inseparability is exactly what prevents efficient attacks on single instances.

Regarding maximum achievable recognition accuracy, in theory, combining feature vectors will lead to the best results. The high-dimensional combined feature space gives the optimal freedom to separate genuine feature vectors from impostor feature

vectors. This optimization, however, requires an accurate model of the probability distributions and obtaining such an accurate model might turn out to be difficult for fused feature vectors due to an insufficient amount of sample data. An inaccurate estimate of the model parameters might lead to over-training resulting in reduced accuracy for measurements that were not in the training set [RNJ06]. However, in a practical situation the simplifying assumption of statistical independence of the instances to be fused can be used to generate the combined model from the individual models. For example, this approach has been used in [MNS+10] for a Fuzzy Fingerprint Vault based on minutiae locations, which were assumed to be independent among different fingers. The assumption of statistical independence is much less problematic if the instances are from different modalities.

In schemes applying error correcting codes, feature-level fusion typically implies that the same code is applied to all instances. As compared to hash-level fusion or decision-level fusion, where different codes or even different schemes can be applied to each instance, this gives less flexibility in selecting the optimal error correction method with respect to the specific error distributions of the individual instances. This can be a particular disadvantage if the instances correspond to different modalities. As a special case, the Fuzzy Commitment Scheme could be implemented with a cascade of different codes, where at the first stage different codes are used to address the specific error distribution of each instance and the second stage applies a common code for the concatenated codewords of the first stage. However, such cascaded encoding has been shown to be vulnerable to attacks exploiting the logical structure of the individual codes used [SKvdV09].

5.2 Hash-level Fusion

Regarding maximum achievable recognition accuracy, hash-level fusion can be compared to decision-level fusion with the limitation that hash-level fusion inherently uses an AND rule which leaves less flexibility, and hence, may lead to a lower overall accuracy than decision-level fusion with other rules, or feature-level fusion.

Hash-level fusion leaves maximum flexibility to the error correction codes used, and it is even possible to apply distinct biometric cryptosystems to the individual instances before the resulting bit strings are fused. In particular for multi-modal fusion, this flexibility allows tailoring an optimal error correction mechanisms for different modalities. For example, the coefficients of the polynomial P from a Fuzzy Vault applied to a fingerprint could be hashed together with the random string S used in the Fuzzy Commitment Scheme for an iris.

The privacy protection of a biometric cryptosystem using hash-level fusion depends on the relation between feature vectors and helper data: for given helper data an attacker can therefor exclude those feature vectors that "do not fit" the helper data, i.e. from which the helper data could not have been computed. Since in hash-level fusion, the helper data is computed per instance, the exclusion of "unfitting" feature

vectors allows sequential attacking of the instances. For example, if the verification function returns an error for a large fraction of feature vectors, the attacker can drastically narrow the search space for each instance individually, which can result in an only linear increase of the attacker's effort as compared to attacking only one instance. If on the contrary, an attacker has no other means to verify the correctness of a candidate feature vector of an individual instance but to check the hash value of the resulting bit string, hash-level fusion can result in an exponential increase of security (provided that the statistical dependence among the instances is small).

In the Fuzzy Commitment Scheme, unless a perfect error correcting code (i.e. a code attaining the Hamming bound) is used, only a small fraction of possible strings can be decoded, which implies that an attacker systematically entering bit strings (e.g. extracted in an FAR attack from random biometric samples) to the verification function or directly to the decoder will in most cases observe a decoding failure indicating that the string does not match that one used during enrollment. Therefore, the attacker can exclude most of the candidate strings without checking the hash value. Unfortunately, there are very few perfect codes, all of which are limited in their dimension [Rot06], and hardly any of them is suitable for biometric feature verification. Implementations of the Fuzzy Commitment Scheme for biometric authentication, e.g. [TAK+05, KGK+07, KBV+09], often deploy BCH codes of length 127 - 511. As shown in Table 5.2, for these codes, the fraction of decodable bit strings can be negligible, which means that an attacker can exclude almost all incorrect candidate strings without considering the second finger, and thus, the security of a scheme using hash-level fusion only increases (at most) linearly with the number of instances.

Ref.	n	k	t	Q
[TAK+05]	511	85	31	2.710^{-79}
[TAK+05]	511	31	54	1.510^{-71}
[KGK+07]	127	36	15	5.410^{-9}
[KGK+07]	255	63	30	1.810^{-19}
[KBV+09]	255	21	55	1.710^{-14}
[KBV+09]	511	10	127	2.510^{-28}

Table 1: Code length n, message length k, number of correctable bits t and fraction Q of decodable words from the code space for BCH codes proposed for use with the fuzzy commitment scheme.

The Fuzzy Vault also allows verification of candidate polynomials P , e.g. interpolated from a subset of points in a polynomial reconstruction attack [MMT09] or in an FAR attack, without computing the hash value by checking if P is interpolated by exactly t points in the vault corresponding to this instance. As shown by Clancy et. al. [CKL03], for reasonable parameters, there exists a $k \leqslant \delta \leqslant t$ so that the expected number of spurious degree k polynomials interpolated by more than δ points is less than one. This implies that with overwhelming probability, the attacker can check the correctness of candidate polynomials by checking if they are

interpolated by δ (or t, if δ is unknown to the attacker) points in the vault. By this means, the attacker can apply the brute force attack to each instance individually and, hence, hash-level fusion can not result in an exponential increase of security.

5.3 Score-Level Fusion

Score-level fusion aims to separate the genuine and impostor scores in a low-dimensional space, the dimension of which equals the number of instances fused. As compared to decision-level fusion, this approach allows greater freedom in choosing the classification boundary and will therefore lead to better recognition accuracy as compared to hash-level fusion or decision-level fusion [RNJ06].

Since an attacker trying to recover the biometric data from a protected template can simply omit the a posteriori quantification of similarity, the evaluation of the score does not contribute at all to the privacy protection. If for each instance a separate hash value is stored as in decision-level fusion, the instances can be attacked individually resulting in only a linear increase of security. If, on the contrary, all strings are concatenated before being hashed, the privacy protection equals that of hash-level fusion. In any case, the privacy protection is not influenced by the threshold(s) applied to the score. For example, the success probability of an FAR-attack is given by the FAR value resulting from the minimum security level where no thresholds are applied at all.

5.4 Decision-level Fusion

Decision-level fusion gives more freedom to the matching rule (AND, OR, majority, etc.) applied for fusion than hash-level fusion, where the AND rule is inherently implemented. Thus, it allows more flexibility for the separation of genuine comparisons from impostor comparisons. Also, decision-level fusion leaves maximum flexibility to the error correction codes used and even allows to use distinct biometric cryptosystems for the individual instances.

However, decision-level fusion does not essentially increase the level of privacy protection: since the template protection method is applied to each instance separately, an attacker can determine the features of the individual instances separately, resulting in a running time that only grows linearly with the number of instances.

6 Conclusions

Our analysis has shown that score-level fusion and decision-level fusion only result in a linear increase of privacy and are, thus, not eligible for biometric cryptosystems

Fusion level	Security gain	Implementation difficulty
Feature level	high	can be high for different modalities
Hash level	high, if most inputs are decodable, else low	low
Score level	low	low
Decision level	low	low

Table 2: Summarizing comparison of feature levels

unless sufficient protection is already achieved with a single modality/instance. The new *hash-level fusion* approach has the potential to combine exponential privacy gain with great ease of implementation, allowing even the combination of different biometric cryptosystems. Unfortunately, for the most prominent biometric cryptosystems, the Fuzzy Commitment Scheme and the Fuzzy Vault, this fusion strategy does not yield an exponential gain of security. For these schemes, feature-level fusion is the only method that can give an exponential increase of privacy. However, feature-level fusion implies that a common error correction method is used for all instances, which gives less flexibility in tailoring the system to the error distributions of the individual instances. This restriction can make implementation of multi-modal biometric cryptosystems, where completely different error distributions of the instances are expected, quite challenging.

References

[BDH+10] I. Buhan, J. Doumen, P.H. Hartel, Q. Tang, and R.N.J. Veldhuis. Embedding renewable cryptographic keys into noisy data. *Int. J. Inf. Sec.*, 9(3):193–208, 2010.

[CKL03] C. Clancy, N. Kiyavash, and D. Lin. Secure smartcard-based fingerprint authentication. In *WBMA '03*, pages 45–52, 2003.

[CS09] A. Cavoukian and A. Stoianov. Biometric Encryption: The New Breed of Untraceable Biometrics. In *Biometrics: Theory, Methods, and Applications*, pages 655–718. John Wiley & Sons, Inc., 2009.

[DORS08] Yevgeniy Dodis, Rafail Ostrovsky, Leonid Reyzin, and Adam Smith. Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data. *SIAM Journal on Computing*, 38(1):97–139, 2008.

[FYLH09] B. Fu, S.X. Yang, J. Li, and D. Hu. Multibiometric cryptosystem: model structure and performance analysis. *IEEE Trans. Info. For. Sec.*, 4(4):867–882, 2009.

[JS02] A. Juels and M. Sudan. A Fuzzy Vault Scheme. In *ISIT 2002*, page 408, 2002.

[JW99] Ari Juels and Martin Wattenberg. A Fuzzy Commitment Scheme. In *ACM CCS 1999*, pages 28–36, 1999.

[KBV+09] E. Kelkboom, J. Breebaart, R.N. J. Veldhuis, X. Zhou, and C. Busch. Multi-Sample Fusion with Template Protection. In *BIOSIG 2009*, volume 155 of *LNI*, pages 55–67. GI, 2009.

[KGK+07] E.J.C. Kelkboom, B. Gökberk, T.A.M. Kevenaar, A.H.M. Akkermans, and M. Veen. "3D Face": Biometric Template Protection for 3D Face Recognition. In *Advances in Biometrics*, volume 4642 of *LNCS*, pages 566–573. Springer, 2007.

[KKM+10] T. Kevenaar, U. Korte, J. Merkle, M. Niesing, H. Ihmor, C. Busch, and X. Zhou. A Reference Framework for the Privacy Assessment of Biometric Encryption Systems. In *BIOSIG 2010*, volume 164 of *LNI*, pages 45–56. GI, 2010.

[KZB+09] E.J.C. Kelkboom, X. Zhou, J. Breebaart, R.N.J. Veldhuis, and C. Busch. Multi-algorithm fusion with template protection. In *BTAS 2009*, pages 1–8, September 2009.

[LT03] J.-P. Linnartz and P. Tuyls. New shielding functions to enhance privacy and prevent misuse of biometric templates. In *AVBPA'03*, pages 393–402. Springer, 2003.

[MMT09] P. Mihailescu, A. Munk, and B. Tams. The Fuzzy Vault for fingerprints is Vulnerable to Brute Force Attack. In *BIOSIG 2009*, volume 155 of *LNI*, pages 43–54. GI, 2009.

[MNS+10] J. Merkle, M. Niesing, M. Schwaiger, H. Ihmor, and U. Korte. Performance the Fuzzy Vault for Multiple Fingerprints (Short Version). In *BIOSIG 2010*, volume 164 of *LNI*, pages 57–72. GI, 2010.

[NJ08] K. Nandakumar and A.K. Jain. Multibiometric Template Security Using Fuzzy Vault. In *BTAS 2008*, pages 1–6, 2008.

[NNJ12] A. Nagar, K. Nandakumar, and A.K. Jain. Multibiometric Cryptosystems based on Feature Level Fusion. *IEEE Trans. Inf. For. Sec.*, 7(1):255–268, 2012.

[RNJ06] A.A. Ross, K. Nandakumar, and A.K. Jain. *Handbook of Multibiometrics (Int. Series on Biometrics)*. Springer, 2006.

[Rot06] R. Roth. *Introduction to Coding Theory*. Cambridge University Press, Cambridge, UK, 2006.

[SKvdV09] A. Stoianov, T. Kevenaar, and M. van der Veen. Security Issues of Biometric Encryption. In *TIC-STH 2009*, pages 34–39, 2009.

[TAK+05] T. Tuyls, A. Akkermans, T. Kevenaar, G.J. Schrijen, A. Bazen, and R. Veldhuis. Practical Biometric Authentication with Template Protection. In *5th Int. Conf. on Audio- and Video-Based Biometric Person Authentication (AVBPA)*, volume 3546 of *LNCS*, pages 436–446. Springer, 2005.

[Way04] J. Wayman. Multifinger Penetration Rate and ROC Variability for Automatic Fingerprint Identification Systems. In *Automatic Fingerprint Recognition Systems*, pages 305–316. Springer, 2004.

[YBdG+11] B. Yang, C. Busch, K. de Groot, H. Xu, and R.N.J. Veldhuis. Decision Level Fusion of Fingerprint Minutiae Based Pseudonymous Identifiers. In *ICHB 2011*, pages 1–6, 2011.