

Evaluation of a template protection approach to integrate fingerprint biometrics in a PIN-based payment infrastructure

Jeroen Breebaart^a, Ileana Buhan^b, Koen de Groot^c, Emile Kelkboom^c

^a*Civolution, HTC9, NL-5656 AE Eindhoven, The Netherlands*

^b*Riscure, Delftechpark 49, Delft, The Netherlands*

^c*Philips Research, HTC34, NL-5656 AE Eindhoven, The Netherlands*

Abstract

Biometric authentication has a great potential to improve the security, reduce cost, and enhance the customer convenience of payment systems. Despite these benefits, biometric authentication has not yet been adopted by large-scale point-of-sale and automated teller machine systems. This paper aims at providing a better understanding of the benefits and limitations associated with the integration of biometrics in a PIN-based payment authentication system. Based on a review of the market drivers and deployment hurdles, a method is proposed in which biometrics can be seamlessly integrated in a PIN-based authentication infrastructure. By binding a fixed binary, renewable string to a noisy biometric sample, the data privacy and interoperability between issuing and acquiring banks can improve considerably compared to conventional biometric approaches. The biometric system security, cost aspects, and customer convenience are subsequently compared to PIN by means of simulations using fingerprints. The results indicate that the biometric authentication performance is not negatively influenced by the incorporation of key binding and release processes, and that the security expressed as guessing entropy of the biometric key is virtually identical to the current PIN. The data also suggest that for the fingerprint database under test, the claimed benefits for cost reduction, improved security and customer convenience do not convincingly materialize when compared to PIN. This result can in part explain why large-scale biometric payment systems are virtually non-existent in Europe and the USA, and suggests that other biometric modalities than fingerprints may be more appropriate for payment systems.

Keywords: Biometrics; authentication; payment systems; PIN; smart card; ATM; point of sale; EMV

1. Introduction

Biometrics have often been identified as the next-generation identity verification method in a variety of applications such as border control, building access, computer login, municipal services, healthcare services and commerce. Some of the driving forces behind biometrics that are often mentioned are an enhanced identity proof, a higher level of customer convenience, and cost savings. The latter is often explained by a supposedly faster transaction or authentication process compared to conventional identity verification methods using tokens, personal identification numbers (PINs), passwords, signatures, and alike.

A large amount of trials and fully operational systems have been installed for biometric payment. For example, Japan has introduced finger and palm vein recognition (Ogata, 2009) in a wide range of ATMs in 2005 to counter their substantial problem of unauthorized cash withdrawals (Jones, 2006). The US-based company Pay by Touch enabled customers to pay for goods with a swipe of their finger (Boyle, 2006; Williams, 2008). In Singapore, Citibank launched

a new fingerprint authentication payment service for credit card customers, installed in 9 merchant locations such as music and IT stores, clubs, restaurants and cinemas (Tan, 2009). In The Netherlands, supermarket chain Albert Heijn together with payment processing company Equens initiated a trial for fingerprint-based payment authentication (van Hooren, 2009). Also in emerging economies, biometrics have found their way into payment systems. The Mexico-based Banco Azteca registered the fingerprints of about 8 million customers in 2007 for payment authentication (Jones, 2007). Similar roll out plans for financial applications have been revealed for the Indian subcontinent, the middle east, Brazil, and others (see International Biometric Group, 2005; McIntosch, 2009, for an overview).

Despite these relatively small-scale successes, biometric authentication has not yet been adopted by large-scale point-of-sale (PoS) and automated teller machine (ATM) systems such as EMV (Europay, Mastercard, VISA (EMVCo), 2008). This could in part be the result of the major challenges that are associated with the adoption of biometrics, such as the proper pro-

tection of biometric data for security and privacy reasons. Furthermore, if an application requires a certain degree of interoperability, for example in a biometric-enabled payment system that should work in different geographic areas, the storage, transfer, exchange and processing of biometric information should be agreed upon between all involved parties. Another explanation for the absence of large-scale biometric payment systems could be that the claimed benefits of biometric authentication do not really materialize in practice, or are subject to unforeseen tradeoffs.

This paper aims at providing a better understanding of the benefits, challenges, possibilities and limitations associated with the integration of biometrics in a PIN-based payment authentication system. The resulting insights may in part explain why such large-scale biometric systems are currently virtually non-existent, and what further actions are required to alleviate any hurdles that may hamper the introduction of such systems. In terms of potential benefits and challenges, we mostly limit the scope to security, cost, customer convenience and acceptance, and system integration aspects. We only consider existing payment systems employing PIN authentication based on conventional magnetic stripe cards or smart cards with an integrated microprocessor (i.e., the majority of debit and credit cards used throughout Europe, de USA, and large parts of Asia). For transaction authentication, we focus on money withdrawals at automated teller machines (ATMs) as well as point-of-sale (PoS) terminals (e.g. retail). We also assume that fingerprints are the biometric of choice for this application, and that both online (in a central facility) as well as offline (by a smart card) authentication are required.

The paper is structured as follows. In Section 1.1, the main benefits and drivers for biometrics are reviewed in more detail, followed by an overview of deployment hurdles in Section 1.2. From the identified hurdles we conclude that it is unlikely that biometric authentication can replace a PIN, and an alternative, integrated approach in which both authentication means are available in parallel is propounded in Section 2. A qualitative analysis of the proposed approach in terms of customer convenience (e.g. false non-match rates), system security (e.g. cryptographic key size and biometric false match rates) and transaction time (e.g. the number of authentication attempts) is provided in Section 3. The claimed benefits associated with biometrics are reconsidered in retrospect in Section 3.5, followed by conclusions in Section 4.

1.1. Potential benefits of biometric technology

1.1.1. Improved identity verification

Authentication that includes something “you are” (e.g. a biometric characteristic) can provide a more trustworthy identity verification than something “you

have” (such as a bank card) or something “you know” (a PIN or password) alone. Recent figures on identity fraud indicate a need for such improvement. According to the Identity theft website (2008), the estimated number of compromised identity data records in the US amounts to about 48 million per year. In a 2008 survey conducted by the Identity theft resource center (2008), 73% of the respondents that were subject to identity compromise reported that their identity was used in financial crime. Credit and debit card fraud are the most frequently occurring financial crime (Federal trade commission, 2009). Especially charges on stolen credit or debit cards (that do not require a PIN) was reported to increase from 8.1% in 2004 to 39% of all reported identity fraud cases in 2008 (Identity theft resource center, 2008). Within the UK, a 25% rise in fraudulent use of credit and debit card was reported for 2007, with losses amounting to 535 million pounds (BBC news, 2008) and 609 million pounds in 2008 (The UK payments association, 2009). The U.S. secret service estimated that annual losses from automated teller machines (ATMs) fraud totalled about USD 1 billion in 2008 (ENISA, 2009). The observed increase in ATM fraud can largely be attributed to card skimming and on-line credit card data compromise (i.e., in so-called card-not-present transactions). During 2008, a total of 10,302 skimming incidents were reported in Europe.

In Europe, credit and debit cards require a PIN to authenticate a transaction. Such knowledge-based authentication was introduced to decrease the risk of fraudulent charges on the associated cards. The PIN is verified either “online” or “offline”. Online PIN verification is used for ATM withdrawals and point-of-sales (PoS) transactions. The secret number entered by the customer is transformed into a derivative (e.g., the PIN verification value, or PVV) and compared to a reference stored at the issuing bank. When both derivatives are equal, the transaction is authenticated. Offline PIN verification, on the other hand, is performed by the terminal (in case of magnetic stripe cards) or by the bank card (in case of a smart card). To allow offline authentication of a PIN using a magnetic stripe card, the PVV is stored on the card and read by the terminal. The fact that this information can be easily copied makes the system vulnerable to skimming (Bhatla et al., 2003; ENISA, 2009) and presumably PIN cracking attacks (Berkman and Ostrovsky, 2007). The new “Chip-and-PIN” system, which is the brand name of cards that comply with the Europay, Mastercard, VISA (EMVCo) (2008) protocol performs offline PIN verification for PoS terminals by the bank card itself. The card contains a small integrated chip (e.g. a so-called smart card), which makes copying information from the card very difficult (Murdoch et al., 2010). The card itself has to prove its genuineness to the terminal through dynamic data authentication

(DDA) or static data authentication (SDA), resulting in a two-factor authentication (i.e. possession of the card and knowledge of the associated PIN). The card with PIN can however still be subject to theft. Additionally, weaknesses in the communication protocol between card and terminal have been identified (Murdoch et al., 2010), and hence there is still an expected benefit from authenticating the subject through the use of biometrics.

1.1.2. Customer convenience

The card fraud events described above will require a card to be revoked, resulting in a period that the customer cannot authenticate electronic payment transactions. Since many financial institutions strongly depend on customer trust and convenience (cf. McIntosh, 2009), biometrics can play an important role to prevent the inconvenience that results from card fraud, and have the potential to increase trust for electronic payments.

A second convenience-related motivator to use biometrics that has often been mentioned is not having to remember a PIN, or even not having to present a debit/credit card. For many people and particularly elderly, PINs can be difficult to remember, especially if different PINs have to be remembered for different cards. This in turn results in a security risk of customers writing down their PINs on a card or on a small piece of paper kept in their wallet. It has also been shown that if people are permitted to choose their own passwords or PINs, they tend to select ones that are easily guessed or are the same across bank cards (Gong et al., 1993).

1.1.3. Cost reduction

A third benefit of biometrics that is often being reported is the one of cost reduction. Point-of-sale terminals may decrease their transaction time, resulting in a faster throughput of customers. Suggested reduction of transaction times between 10% up to 70% have been reported in the past (Banking automation bulletin, 2009; Boyle, 2006). Furthermore, cost associated with forgotten PINs and associated cards that have to be renewed may be reduced.

1.2. Deployment hurdles

1.2.1. Investment in terminals, cards, and enrollment facilities

The integration of biometrics in an ATM/PoS payment system requires significant investments in terminals and cards. During the last decade, banks and retailers have been forced to keep up with industry initiatives such as an EMV compliant smart card. It has been estimated that in 2008, there were about 400 thousand ATMs in Europe and about 1.5 million around the world (ENISA, 2009; European Central Bank, 2010)

and these numbers increase by about 6% per year. The number of point of sales (PoS) terminals is even larger; within Europe alone the total number of PoS terminals amounted to 8 million in 2008 (European Central Bank, 2010). Extending PIN-based PoS and ATM terminals with biometric functionality requires significant investments and hence banks have only a limited appetite for biometrics without a strong customer pull. The only feasible route of integration seems therefore during renewal of old terminals, and thus from a financial point of view, biometrics and PIN would need to co-exist until the majority of terminals has been replaced which can take several years if not longer.

On top of the required hardware investments, banks would need to invest in enrollment facilities as well. Because the security of a biometric system depends to a large extent upon the identity proof of customers during such enrollment phase, this process is typically performed at the bank itself in a supervised manner. This means that dedicated enrollment equipment and services need to be installed, and qualified personnel should be present.

1.2.2. Infrastructural changes for biometric interoperability

Besides the required changes in the PoS/ATM terminals and bank cards, the authentication communication infrastructure may need to change as well (von Graevenitz, 2007). For example, in an online PIN authentication protocol, a merchant sends transaction information accompanied by an encrypted PIN entered by the customer to the merchant's acquiring bank, which in turn requests authorization from the customer's issuing bank. The authorization depends among other things upon equality or inequality of the entered PIN against a reference stored at the issuing bank, and the authorization outcome is returned to the merchant via the acquiring bank. If such protocol is to be extended with biometrics, the biometric modality and data exchange formats that are to be exchanged between banks need to be agreed upon, and measures to ensure the security of the system and the privacy of its subjects need to be in place. Without consensus among all involved parties on these aspects there is a substantial risk that biometric authentication will only be available at terminals of the issuing banks.

1.2.3. Service costs resulting from false non-matches

Besides cost benefits resulting from shorter transaction times, it has also been argued that the use of biometrics may increase cost. Any biometric system is prone to errors by definition. The intrinsic failure is expressed as false non-match and false match rates, which are subject to a design trade-off. Depending on the modality that is being used and the quality of the biometric data samples, realistic false non-match rates (expressed as proportion of the number of

authentication attempts) are typically in the order of 0.1 to 5% (cf. Phillips et al., 2005, 2007; Toth and Mansfield, 2006; Cappelli et al., 2006; University of Bologna, 2006). In a payment authentication system dealing with millions of transactions a day (European Central Bank, 2010), however, such false non-match rate is not really acceptable given the large number of resulting service calls and the associated cost.

1.2.4. *Biometric system security*

Another concern for the adoption of biometrics in a payment system is related to biometric security. Various potential vulnerabilities of biometric systems have been described in the past (see Jain et al., 2008, for an overview) which require dedicated countermeasures to mitigate such risks. Examples of vulnerabilities include spoofing of a sensor (for example by the use of gummy fingers), replay attacks and other channel-interception based methods. Especially for a payment system involving unattended terminals (such as ATMs), malicious persons may be able to modify the operation of a sensor, or make several authentication attempts using spoof biometrics or cards. In the unfortunate case that a security breach occurs, and biometric template information becomes compromised, that biometric information will be compromised forever. The ability to revoke and renew biometric references is therefore an important requirement for biometric systems (cf. ISO/IEC JTC1 SC27, 2010), which requires dedicated technology and/or procedures to facilitate such renewal.

But even in normal operation (without malicious actions), a biometric system has a non-zero false match rate. Independent tests on a variety of biometric modalities often indicate false match rates in the order of 0.1 to 1% (cf. Phillips et al., 2007, 2005; University of Bologna, 2006). On the other hand, biometric vendors themselves often report more optimistic performance numbers, and the discrepancies in performance indicators may lead to skeptical expectations for biometrics (Moss, 2009). If a payment system would only rely on biometrics to identify and authenticate a subject, any non-zero false match rate will result in a certain proportion of transactions that will be associated with the wrong identity. As such, it is unlikely that a large-scale payment system can operate on biometrics alone, and most likely will rely on other authentication means as well (such as the possession of a bank card, or knowledge of a secret PIN).

1.2.5. *Biometric information privacy*

Biometric information privacy refers to the right to control over ones own biometric information in its life cycle of collecting, transferring, using, storing, archiving, disposal and renewal. The protection of individuals with regard to the processing of personal data is underlined in various legal documents and standards

(cf. European Parliament and European Council, 1995; ARTICLE 29 - Data Protection Working Party, 2003; ISO/IEC JTC1 SC27, 2010). Because biometric characteristics are (almost) unique for a subject, and often contain information beyond what is needed for authentication, biometric data is regarded as personal data and is vulnerable to unlawful use. Examples of unlawful processing include cross-linking of subjects across databases, the assessment of the subject's ethnic background or the analysis of medical data from biometric measurements. As a result, it is often disputed whether biometric data can or cannot be stored in a centralized database. Although the final answer is yet unknown, it is clear that the benefits of centralized data storage should be proportional to the resulting privacy risks.

1.2.6. *Customer acceptance*

In terms of customer acceptance, we can identify 4 categories of subjects that are not necessarily mutually exclusive.

1. Subjects that find biometrics more convenient and safe than PIN and experience no practical problems during operation. This is the target group to embrace biometrics. Surveys indicate that between 60 to 92% of the population belongs to this group (ORC, 2001; TNS/TRUSTe, 2005; Tan, 2007; Logica CMG, 2006; van Hooren, 2009).
2. Subjects that object against the use of biometrics in payment systems for a variety of reasons, such as a lack of trust in futuristic technology (Coventry et al., 2003), mis-use of personal data, health and hygiene risks associated with biometric sensors, associations with crime (e.g. fingerprints), and alike. US surveys between 2001 and 2005 revealed a percentage of 6-10% of Americans that found the use of finger and hand scan biometrics for law enforcement and governmental applications unacceptable (ORC, 2001; TNS/TRUSTe, 2005). In the area of payment, a similar proportion found it not acceptable to use biometrics for ATMs (Logica CMG, 2006).
3. Subjects that fail to enroll due to an absence of reliable biometric characteristics. Depending on the biometric modality, this group of subjects represents about 1 to 3% of the population (Mansfield et al., 2001; Toth and Mansfield, 2006; Ogata, 2009).
4. Subjects that enroll correctly but experience a disproportional false non-match rate during operation. This subgroup of a population is often referred to as "goats" (Doddington et al., 1998). There is evidence that goats indeed exist for certain biometric modalities and corpora (Bolle et al., 2000; Wittman et al., 2006; Maio et al., 2006; Modi and Elliott, 2006; Yager and Dunstone, 2007; Breebaart et al., 2009).

2. Biometric template protection to integrate biometrics in a PIN infrastructure

2.1. Rationale

Given the deployment hurdles described in the previous section, it seems highly unlikely that biometrics will completely replace PIN. The PIN is likely to be required as fallback in the case that a payment terminal does not support biometric authentication, or when a client does not want to or cannot use biometrics. We therefore propose an integrated approach, in which PIN and biometric authentication co-exist. To allow for a seamless integration of both authentication means, and to ensure a sufficient level of data privacy, we propound the use of so-called “biometric template protection” techniques employing key binding and key release principles. The properties of such techniques, and their benefits in the context of a payment system are outlined in the next sections. The proposed method will subsequently be subject to a security and customer convenience analysis by means of simulations in Section 3.

2.2. Key binding and key release methods

During the last decade, a variety of techniques to enhance the security and privacy of biometric systems have been proposed and evaluated (see Breebaart et al., 2008, for a non-exhaustive list). These methods are often denoted as “template protection” methods because of their aim to protect the biometric reference data (e.g. the template) against tampering and unauthorized processing during storage and transmission. Their operation is in many cases based on transforms that convert biometric data into a representation that is renewable, unlinkable and irreversible (ISO/IEC JTC1 SC27, 2010). The use of such methods is regarded as best practice according to the European data protection supervisor (EDPS, 2011). One class of such template protection algorithms employs principles of key binding and key release. Embodiments of such key binding and key release principles are referred to as fuzzy commitment schemes (Juels and Wattenberg, 1999), helper data systems (Linnartz and Tuyls, 2003; Kelkboom et al., 2007), fuzzy vaults (Juels and Sudan, 2006; Nandakumar et al., 2007) and fuzzy extractors (Dodis et al., 2004, 2008). Figure 1 provides a schematic overview of the important processing elements. During enrollment, a key binding method combines a (secret) key with a biometric sample into so-called “auxiliary data” (AD). The auxiliary data should not reveal the key nor the biometric characteristic. Additionally, the key is processed by a cryptographic one-way function and the hash of the key is stored as the “pseudonymous identifier” (PI). The processing stage that generates AD and PI is referred to as pseudonymous identifier encoder (PIE). During verification, the key is reconstructed (released) with the help of the auxiliary data and a new

biometric sample by means of a pseudonymous identifier recorder (PIR), and the candidate pseudonymous identifier (PI*) is obtained as the hash of the released key.

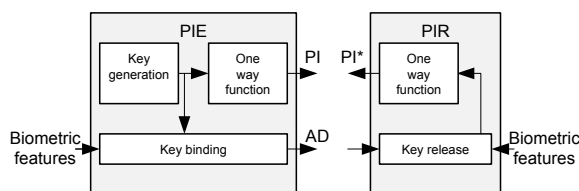


Figure 1: Schematic overview of the PIE and PIR modules employing key binding and key release principles.

The use of pseudonymous identifiers solves several challenges related to the security and privacy of biometric data. In contrast to biometric characteristics, PIs are renewable which is an important benefit in the case of identity fraud ISO/IEC JTC1 SC27 (2010). Furthermore, the PI does not reveal any information that is not strictly required for authentication, reducing the risk for unlawful processing of biometric data. The privacy risks and the corresponding legislation associated with centralized biometric databases have often been the reason to argue for comparison-on-card biometric solutions (von Graevenitz, 2007). Besides these security and privacy benefits, the deployment of PIs also has benefits in terms of system integration, as will be explained in the next section.

2.3. System integration

One of the interesting analogies between biometric pseudonymous identifier and PIN authentication is that both methods rely on the comparison of an encrypted or hashed secret key. This similarity allows for a relatively simple system integration of biometrics compared to conventional biometric authentication methods. Biometric systems not incorporating biometric template protection require the transmission of biometric data from a sensor (presumably integrated in a PoS or ATM terminal) to the bank that issued the payment card for biometric verification. If the ATM or PoS terminal is operated by a different (acquiring) bank, the data has to be transmitted between banks. Such exchange of biometric data is difficult to realize for several reasons. Firstly, it requires banks to reach consensus on biometric modalities and exchange formats to be used. Secondly, the authentication infrastructure needs to be extended to support such exchange of biometric data. The concept of pseudonymous identifiers solves these hurdles to a large extent by transforming a biometric sample into a fixed binary string that can readily function as a PIN. In the following two subsections, two examples of the integration of pseudonymous identifiers in a payment infrastructure are outlined. In these examples, we focus on the information

flow related to biometric data, and do not specifically outline additional procedures to ensure confidentiality and authenticity of transmitted data, cards and terminals. These properties are assumed to be provided by off-the-shelf cryptographic techniques such as data encryption and the use of signatures.

2.3.1. Online biometric verification

In this scenario, the customer has a bank card that only stores information and has no processing or cryptographic capabilities. We consider ATM withdrawals and point-of-sales (PoS) terminals that read information stored on the card, are equipped with a biometric sensor, and rely on online (biometric) verification by the issuing bank. The information flow is outlined in Fig. 2. The bank card contains cardholder information (CI) such as the account number, card holder’s name, and expiry date, as outlined in ISO/IEC (2006). Additionally, the biometric auxiliary data are stored on the card. Upon transaction, both CI and AD are read from the card by the terminal. The cardholder also presents his/her biometric. From the combination of AD and biometric sample, a candidate PI^* is created by the terminal. Part of the cardholder data, the candidate PI^* , and the transaction data are subsequently transmitted to the issuing bank for verification. A pseudonymous identifier comparator (PIC) compares the generated PI^* with the reference PI stored in the database (DB) of the issuing bank. When the PI^* is authenticated, the payment will be settled.

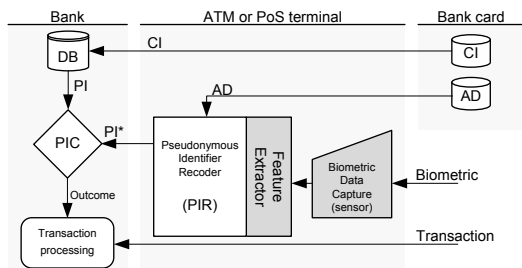


Figure 2: Scenario for online biometric transaction authentication based on a bank card with storage facilities.

2.3.2. Offline biometric verification

The biometric information flow for an offline smartcard based biometric verification is outlined in Fig. 3. The card first provides the auxiliary data to the terminal. Subsequently, the terminal recreates a candidate PI^* from the captured biometric sample and transmits it to the card, which verifies its value. The verification result is published to the terminal to proceed with or to reject the transaction. When the genuineness of the cardholder has successfully been verified by the card, the transaction information is typically signed by the card (via a message authentication code, or MAC) and

send to the issuing bank to settle the payment. If no live connection with the issuing bank can be established, the terminal may store the transaction data temporarily until the connection is re-established.

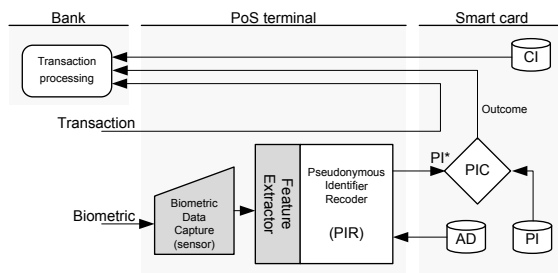


Figure 3: Scenario for offline, smartcard-based biometric transaction authentication employing storage of AD and PI on the card, and comparison on the card.

This scenario can even be extended towards a biometric challenge-response method. If biometric *features* (BF) that are used as input for PIE and PIR modules are stored on the card in a secure manner, the card can be equipped with a pseudonymous identifier encoder (PIE) that generates a new PI and corresponding auxiliary data for each authentication session (see Fig. 4). By doing so, the required PI^* generated by the terminal is different for each session hence preventing potential replay attacks.

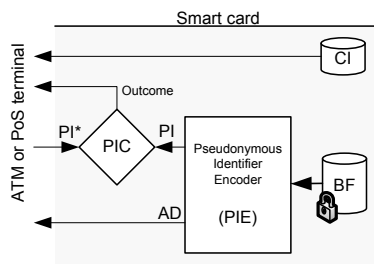


Figure 4: Smartcard-based biometric transaction authentication employing a challenge-response protocol based on stored biometric features (BF) in a secure area of the smart card.

3. Performance evaluation based on fingerprint biometrics

In this section a simulation study is described in which the integration of biometrics in a card-based payment system is evaluated from a technical perspective. The study is based on the assumptions that (1) biometrics and PIN co-exist, (2) biometric authentication employs the concept of PIs that function as PIN, and (3) subjects have the freedom to select PIN or biometric authentication. In particular, this section:

- Compares biometric performance with and without the incorporation of biometric template protection;

- Compares the maximum entropy of the biometric key to the entropy of a 4-digit PIN;
- Evaluates the effect of multiple authentication attempts as typically exist in PIN-based systems, and
- Simulates the removal of “goats” (cf. Section 1.2.6) from the biometric population on the biometric performance, assuming these subjects will revert to PIN-based authentication if a series of initial attempts to use biometrics were not successful.

3.1. Feature extraction

The following procedure was employed to create PI and AD data elements from fingerprint images. First, for each fingerprint sample in the database, a set of minutiae was extracted using a commercially-available software solution (Neurotechnology VeriFinger SDK version 5). Each set of minutiae was transformed into a (partially) rotation and translation-invariant feature representation to result in a first set of features. Furthermore, directional field and Gabor responses were extracted of each fingerprint image as described in Tuyls et al. (2005) and combined (concatenated) to the features extracted from the minutiae set. The combined feature set had a fixed length of 1400 real-valued features. These features were created such that they adhered to the following requirements:

- The expected mean feature vector across a large population of subjects amounted to zero;
- The features did not have any significant (first-order) correlations;
- The individual features had (approximately) unit variance across the population.

These properties were obtained by applying a combination of a principal component and linear discriminant analysis (Duda and Hart, 1973) on the set of features from our feature extraction algorithm. The matrix coefficients required for this transformation were obtained from an independent *training* set (see Sec. 3.3 for details).

3.2. Key binding and key release model

The PI encoder and recoder as outlined in Fig. 1 were modeled following the approach by Kelkboom et al. (2010), which comprised:

1. A quantizer, which transforms each individual feature from the enrolment and verification feature vector into a one-bit binary representation by thresholding;

2. A Hamming-distance classifier operating on the difference between two binary feature vectors in which the maximum size of the secret key depends on the Hamming-distance classifier threshold.

3.3. Procedure

The publicly available MCYT fingerprint database (Ortega-Garcia et al., 2003) was used to evaluate the PIE and PIR scheme. This database contains 12 images of all 10 fingers from 330 subjects that were located in four different institutions, and were all sampled using 2 different sensors (i.e., one optical and one capacitive sensor). For the test described, we only used the first two fingers acquired using the optical sensor. In a first step, we randomly split the feature vectors by subject in a training set (comprising 80% of the subjects) and a test set (comprising the remaining 20%). The training set was used to determine the principal component analysis (PCA) and linear discriminant analysis (LDA) matrix coefficients. Subsequently, the PCA/LDA transformation was applied to all feature vectors of the test set. From this transformed test set, 4 feature vectors were randomly selected from each subject and converted to a single feature vector by averaging. This averaged feature vector was used for enrollment. The remaining 8 images were used as individual genuine comparison samples. For imposter comparisons, we randomly sampled one in five of all imposter combinations. The process of random selection for enrollment and verification was repeated 5 times resulting in a total of $0.2 \times 2 \times 330 \times 8 \times 5 = 5280$ genuine comparison scores. The process of randomly splitting training and test sets was employed 10 times to result in a pooled 52800 genuine comparison scores, from which we constructed detection error trade-off (DET) curves. A maximum key entropy was obtained based on the number of errors to be corrected for a discrete set of operating points on the DET curve (Kelkboom et al., 2010).

For reference (as baseline condition), we also constructed DET curves based on real-valued feature vectors (i.e., without quantization and PIE/PIR processing) to investigate potential performance differences induced by the PIE and PIR processes. The process of feature splitting and PCA/LDA transformation was identical as employed for the PIE/PIR configuration. We used (one minus) the normalized correlation coefficient ρ as comparison score D between two feature vectors f_1 and f_2 :

$$D = 1 - \rho = 1 - \frac{f_1 \cdot f_2}{\sqrt{(f_1 \cdot f_1)(f_2 \cdot f_2)}}, \quad (1)$$

with $(a \cdot b)$ the dot product of vectors a and b .

In a payment system that provides PIN as fallback option, it is likely that the group of biometric “goats”

will stop to use biometric authentication at some point in time (after a series of false non-matches) and will solely rely on PIN authentication. We simulated this phenomenon using the procedure of Breebaart et al. (2009) to filter out goats from the population:

- We calculated the mean comparison score across all genuine comparisons for each subject in the test set.
- We sorted these comparison scores and identified the 5% of the population with the lowest average comparison score.
- We removed all measurements from the subjects that were identified in the previous step.

3.4. Results

The biometric system performance expressed as DET curve is provided in Fig. 5. The baseline condition based on real-valued features is shown by the dotted line. For a false match rate (FMR) of 0.1%, this configuration reaches a false non-match rate (FNMR) of approximately 1.5%, which decreases to about 0.7% for a FMR of 1%, while the equal-error rate (EER) point amounts to 0.8%.

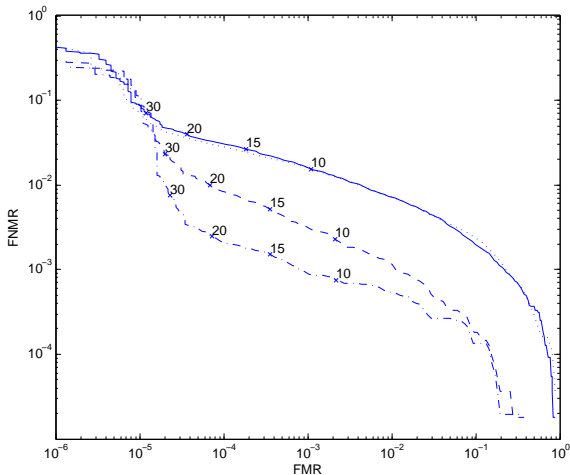


Figure 5: DET curve for the PIE/PIR approach (solid line), real-valued feature vectors (dotted line), PIE/PIR approach based on two attempts for each verification (dashed line), and the PIE/PIR approach based on two attempts after removing “goats” (dash-dotted line). The crosses indicate the key size.

The performance for the PIE/PIR system (as indicated by the solid line) is very similar to that of the baseline condition based on real-valued feature vectors. Hence for the current biometric database and employed feature extraction algorithm, the incorporation of feature quantization and key binding and release

processes was not found to have any significant positive or negative impact on the biometric system performance. The maximum entropy of the key (in bits) for a discrete set of operating points is provided by the crosses on the solid line, ranging from about 30 bits at a FMR of 0.001% down to 10 bits at a FMR of 0.1%.

The DET curve for two verification attempts is indicated by the dashed line in Fig. 5. For a broad range of operating points, the FNMR for a given FMR is approximately five times lower than the FNMR for the single-attempt system, indicating a strong benefit from allowing two attempts rather than only one. Moreover, the maximum key size at a fixed FMR is slightly larger for multiple attempts (dashed line) than for a single attempt (solid line).

The probably most realistic configuration for a biometric-enabled payment system is represented by the dash-dotted curve of Fig. 5. This curve represents the configuration in which two attempts are allowed, *and* in which the “goats” were removed from the data set by the procedure described in Section 3.3, assuming these subjects will revert to PIN after a few unsuccessful attempts to use biometric authentication. For this condition, the FNMR at a constant FMR is substantially lower than for the previous ones (e.g. a FNMR of 0.2% at a FMR of 0.1%). The maximum key size is not changed after removal of goats from the data set, however.

3.5. Discussion

3.5.1. Biometric performance

The baseline condition in which no template protection technique was employed achieved a FNMR of about 1.5% at a FMR of 0.1% and an EER of 0.8%. If these performance figures are compared to other studies performed on the same fingerprint database we can conclude that our feature extraction and comparison algorithms perform slightly worse than those used by others. For example, Breebaart et al. (2009) reported a FNMR of 0.75% at a FMR of 0.1% based on minutiae comparison, which is two times lower than our results. Simon-Zorita et al. (2003) reported EERs below 1% using 3 enrollment images. Xu and Veldhuis (2009) report EERs between 0.1 and 0.3% on a subset of the MCVT database. Other studies report similar performance numbers using different database subsets (Xu et al., 2009a,b).

When the results for the real-valued baseline condition are compared to the PIE/PIR approach, we observed a virtually identical performance curve. This indicates that for the employed feature extraction and quantization scheme, classification by means of binary comparison does not result in a significant degradation of the verification performance. This result is in line with other studies based on fingerprint data (Chen et al., 2007), 2D face biometrics (Chen et al., 2008) and

3D face biometrics (Busch et al., 2008) that also indicated minor effects of the incorporation of quantization and key binding principles. In another study, a performance decrease of a factor of about 3 was nevertheless reported when comparing real-valued and binary fingerprint templates (Tuyls et al., 2005).

In the described approach no advanced bit-extraction methods such as multi-bit extraction and reliable component selection were used (e.g. Tuyls et al., 2005; Chen et al., 2007, 2009; Kelkboom et al., 2009b); the incorporation of such methods may even result in small performance improvements compared to the current results.

The simulations indicate significant benefits of having two biometric verification attempts rather than one. When the number of attempts for verification is increased from one to two, the FNMR at a constant FMR improves by about a factor of five, which is more than the factor of about two reported in Breebaart et al. (2009). Because both FNMR and FMR typically decrease with an increase in the number of attempts, the system threshold should be set more restrictively to reach the same FMR. As a result, the maximum size of the key that can be used to bind with the biometric data increases. As indicated in Fig. 5, the gain in maximum key size amounts to about 3 bits.

3.5.2. Biometric benefits and hurdles revisited

The obtained results have implications for the employment of fingerprint biometrics in a payment system. We have shown that it is technically feasible to use biometric key binding and key release methods to bridge the gap between biometric and PIN authentication. The results indicate that biometric performance (expressed as FMR and FNMR) is not significantly influenced by the deployment of such key binding and key release mechanisms. Hence, compared to a conventional biometric system (e.g. not employing key release mechanisms), the proposed approach has several advantages. Firstly, the renewability of the biometric reference data is more secure; data can be revoked and renewed in case of a security breach. Secondly, the irreversibility property improves the data privacy, making it harder to use the stored data for other purposes than payment authentication. Thirdly, the employed keys can be used as “biometric PIN”, facilitating a simple integration in a PIN-based infrastructure. In conclusion the proposed method alleviates several of the identified deployment hurdles for biometrics in a payment system *when compared to the integration of a conventional biometric approach*.

To evaluate the potential benefits, the appropriate reference is the existing system based on PIN. We argued that biometric and PIN need to co-exist to allow for a cost effective upgrade of terminals, and to provide authentication means for clients for whom biometric authentication fails. This co-existence is also

supported by the simulations presented in Section 3. Under the assumption that a biometric payment system requires a FMR of 0.1% or below (which is equal to the probability of correctly guessing a 4-digit PIN in one attempt), the associated FNMR of 1.5% is most likely of considerable concern for payment system operators. Even when the “goats” are excluded from the biometric database, an FNMR of 0.1% or higher is still substantial. When millions of transactions are processed daily, banks, retailers and customers will most likely demand that a more fail-safe fallback (e.g. PIN) is available at any time.

Obviously, the cost of extending (new) terminals with biometric sensors reflects only a small portion of the total cost to integrate biometrics in a PIN payment system. All involved parties will have to reach consensus on a broad range of system aspects, such as biometric modalities that are supported, data exchange formats, security reviews, and alike, which can be lengthy and costly processes. Furthermore, bank cards need to be upgraded, enrollment facilities need to be constructed, personnel requires proper training, and so on. Despite the fact that it will be very difficult to estimate the cost associated with the complete upgrade process, it seems logical that biometrics will only be considered if its introduction is supported by solid and indisputable evidence that the associated benefits will indeed materialize *compared to PIN*. When cost benefits are considered, the simulations do unfortunately not indicate that shorter transaction times can indeed be achieved. In the publications that report transaction time reductions (Boyle, 2006; Banking automation bulletin, 2009; van Hooren, 2009), these results seem mostly attributable to the fact that no payment card had to be swiped to identify the customer. Both identification and transaction authentication are performed based on a fingerprint scan. With a non-zero biometric FNMR, such approach is only feasible on small-scale trials. On large scale systems, with millions of customers, two-factor authentication becomes a necessity, and hence it is doubtful whether biometric authentication will be faster than PIN in that case. Our results indicate that a single biometric authentication attempt will not always suffice, resulting in an increase in the average number of attempts for each transaction. Moreover, in the case of two subsequent false rejects, the customer will still have to revert to PIN. Depending on how often this will occur in practice, transaction times may not be shorter, and may even become longer than for PIN alone.

We did not find any evidence that biometrics can save cost of service calls resulting from forgotten PINs. PIN authentication will still be required in the case of a biometric false non-match, or at terminals that do not support biometrics at all. In fact, when customers use their PIN less frequently due to biometrics, the probability that they forget their PIN may actually increase,

which could even result in higher expenses associated with PIN resets.

A second claimed benefit for biometrics is supposedly better security. Obviously, when PIN and biometrics are *both* required for authentication, one expects that fraudulent transactions will become more challenging for an adversary than with PIN or biometrics alone. However such multi-factor authentication defeats the original purposes of cost saving and improved customer convenience and hence this is a very unlikely scenario for payment systems. When considering the maximum key entropy for the key-binding approach, the maximum key size at a FMR of 0.1% amounts to about 10 to 12 bits (depending on the configuration of the system and the target group). The key size can be increased up to 20 or 30 bits at the expense of a higher FNMR, assuming banks are willing to accept FNMRs in the order of 1% or beyond. Irrespective of the exact operating point for this security versus convenience trade-off, the number of bits remains small in a cryptographic context. This implies that similar to PIN, appropriate procedural mechanisms should be in place to prevent guessing attacks and to limit the number of erroneous attempts. Interestingly, we have also observed that the biometric security can be increased by allowing for 2 authentication attempts rather than one, resulting in a lower FMR and higher key entropy. This obviously has the drawback that the probability of success during the first attempt will decrease, and hence the authentication process will take more time due to an increase in the average number of authentication attempts.

The third benefit often associated with the use of biometrics for authentication is the improved customer convenience. Our simulations did not indicate that customer convenience is strongly improved. Firstly, customers will have to remember their PIN just in case biometrics do not work properly or are not supported by the payment terminal. Secondly, false non-matches may result in the necessity of multiple biometric authentication attempts which may not be regarded as being convenient at all. Thirdly, in former biometric payment trials, customers seem to especially value the employed single-factor authentication (e.g. biometrics only). For example, van Hooren (2009) quotes “When asked what they liked about the system, again the majority, some 80%, said that the payment method was very convenient as they could authorize payments with nothing more than their fingertip.” Again, this benefit is valid on small-scale trials, but is difficult to realize on large-scale systems given a non-zero FNMR biometric.

The difficulty to demonstrate clear benefits for payment authentication using fingerprints compared to PIN may in part explain why large-scale payment systems in Europe and the USA have not yet embraced biometrics. Most of the trials and systems that have

been used in these areas have predominantly been focussing on fingerprints. It may well be the case that similar conclusions were drawn from these trials. On the other hand, Japan has a large biometric infrastructure for ATM withdrawals. Their choice for finger and palm vein biometrics instead of fingerprints may have been critical to achieve a positive balance between investments and resulting benefits. The claimed FNMR and FMR reported by some vendors are substantially lower than for fingerprints (Ogata, 2009), while potential issues with hygiene and latent biometrics can be solved with contactless sensors.

3.5.3. Limitations and unresolved issues for the proposed approach

The simulation results suggest that fingerprints do not provide a sufficiently high biometric authentication performance to support the claimed benefits of cost reduction, customer convenience and security when compared to PIN. These results were obtained with one fingerprint database and one specific feature extraction algorithm only. A large-scale test involving more data sources and processing algorithms would be required to validate whether the reported results show consistency under different conditions. Furthermore, it is not clear what the performance will be if different age groups are involved, if weather conditions are taken into account, and what happens if biometric sensors are left unattended as would be the case in ATMs. Furthermore, in the simulations involving multiple attempts, we assumed that each captured biometric sample is evaluated independently, i.e., at least one of them should give a positive result. Potentially more clever combinations of two captures biometric samples (e.g., multi-sample fusion, see Kelkboom et al., 2009a) may provide better performance.

A second potential issue relates to the modality dependence of biometric systems. To allow an interoperable system in which a subject with a card from issuing bank A can biometrically authenticate a transaction at a terminal from acquiring bank B, both banks will need an agreement on which biometric modalities they support, which sensors are being integrated in the terminal, and what feature extraction and PIR algorithms are supported. Such choices require support and consensus by many involved parties which may be very difficult to achieve in practice. Similar arguments hold for the storage of AD data. Consensus is required in what format this should be done, where it is stored (on a bank card, or on a central server). Although the pseudonymous identifier is modality independent and can be generated for virtually all biometric modalities, it remains to be seen if performances and key sizes are indeed comparable and interchangeable in such systems.

A third limitation relates to the key entropy that is reported throughout this study. This performance in-

indicator is based on the assumption of independent bit values in the extracted binary string. In practice, bit values and bit errors can be correlated and hence the actual key entropy may be lower than reported here. Moreover, it may not be trivial to design an error correction scheme that actually achieves the presented upper bound. Hence the reported key entropy values are most probably too optimistic.

A fourth limitation related to template protection techniques is that at this point in time, methods to evaluate and benchmark privacy and security are still under development. It is therefore difficult to objectively assess the actual level of privacy and security that is being provided by a certain method, or to compare different approaches among each other.

A final limitation is the fact that we did not consider comparison-on-card biometric systems. In principle, off-line biometric authentication can be performed by a smart card with an integrated biometric comparison algorithm. This approach also alleviates privacy risks because biometric references are stored on a smart card carried by the customer, at the expense of a more costly smart card. Online authentication is difficult to realize with this approach, however. Moreover, the difficulty to materialize benefits compared to PIN is probably equally challenging for a comparison-on-card approach as for the key release approach described in this paper.

4. Conclusions

Recent developments in the area of the protection of biometric data have provided means to transform inherently noisy biometric references into constant and renewable binary strings. Although these transforms have mainly been developed with security and privacy benefits in mind, we have shown that the ability to bind cryptographic keys with biometric data, and the release thereof during verification allows to seamlessly integrate biometrics in existing payment infrastructures with minimal changes to the authentication processing infrastructure. The keys embedded in biometric data (or the hash thereof) can readily be used as replacement of a PIN (or a PVV) eliminating the need for the transmission of biometric data between banks for online verification.

By means of simulation, the influence of the proposed approach onto claimed benefits and existing employment hurdles for the deployment of biometrics was investigated. The results suggested that it is unlikely that fingerprint biometrics can *replace* PIN and instead, both authentication means should co-exist. This co-existence allows for a smooth upgrade path for payment terminals, lets customers choose their preferred authentication means, and serves as fallback when biometric authentication fails.

For such a co-existence scenario, our fingerprint-based simulations did not provide an indication that claimed benefits of biometric technology, such as an improved security, an improved customer convenience, and cost reduction will actually materialize. Instead, it seems that these properties are virtually on par when comparing biometrics and PIN, which may be an important reason for the absence of large-scale fingerprint payment systems today. Future research involving different biometric modalities, or combinations thereof (such as finger vein and fingerprint data captured by one combined sensor) may result in a more positive balance between investment effort and the resulting benefits.

5. Acknowledgments

The authors would like to thank the associate editor and the anonymous reviewers for their very thoughtful and helpful comments to improve this paper.

References

- ARTICLE 29 - Data Protection Working Party. Working Document on Biometrics. Retrieved May 24, 2008 from <http://ec.europa.eu/justice-home/fsj/privacy/docs/wpdocs/2003/wp80-en.pdf>, 2003.
- Banking automation bulletin. Equens perspective - Biometrics answers call for fast, simple checkout. Retrieved from <http://www.equens.com/Images/Article/%20biometrics.pdf>, October 2009.
- BBC news. Plastic card fraud goes back up. Retrieved May 2, 2011 from <http://news.bbc.co.uk/2/hi/business/7289856.stm>, March 2008.
- O. Berkman and O. M. Ostrovsky. The unbearable lightness of pin cracking. In *Proceedings of the 11th International Conference on Financial cryptography and 1st International conference on Usable Security, FC'07/USEC'07*, pages 224–238, Berlin, Heidelberg, 2007. Springer-Verlag. ISBN 3-540-77365-7, 978-3-540-77365-8. URL <http://portal.acm.org/citation.cfm?id=1785594.1785622>.
- T. P. Bhatla, V. Prabhu, and A. Dua. Understanding credit card frauds. Retrieved August 17, 2009 from http://www.popcenter.org/problems/credit_card_fraud/PDFs/Bhatla.pdf, June 2003.
- R. M. Bolle, S. Pankanti, and N. K. Ratha. Evaluation techniques for biometrics-based authentication systems (FRR). *Pattern Recognition, International Conference on*, 2:2831, 2000. doi: <http://doi.ieeecomputersociety.org/10.1109/ICPR.2000.906204>.
- M. Boyle. Let your fingers do the paying. Retrieved January 15, 2010 from <http://money.cnn.com/2006/01/24/magazines/fortune/pluggedinfortunebiometrics/?cnn=yes>, January 2006.
- J. Breebaart, C. Busch, J. Grave, and E. Kindt. A reference architecture for biometric template protection based on pseudo identities. In *Proc. BIOSIG*, pages 25–38, Darmstadt, Germany, 2008.
- J. Breebaart, T. Akkermans, and E. Kelkboom. Intersubject differences in false nonmatch rates for a fingerprint-based authentication system. *EURASIP J. on Advances in Signal Processing*, 2009 (Article ID 896383):1–9, 2009.
- C. Busch, A. Nouak, X. Zhou, J.-M. Suchier, E. J. C. Kelkboom, and T. Kevenaer. 3D Face recognition for unattended border control. In *Proc. Net-ID 2008 Conference*, pages 126–136, 2008.
- R. Cappelli, D. Maio, D. Maltoni, J. L. Wayman, and A. K. Jain. Performance evaluation of fingerprint verification systems. *IEEE*

- transactions on pattern analysis and machine intelligence*, 28(1): 3–18, Jan 2006.
- C. Chen, R. N. J. Veldhuis, T. A. M. Kevenaer, and A. H. M. Akkermans. Multi-bits biometric string generation based on the likelihood ratio. In K. W. Bowyer, P. J. Flynn, V. Govindaraju, and N. Ratha, editors, *IEEE conference on Biometrics: Theory, Applications and Systems, Washington DC*, pages 1–6. University of Notre Dame, September 2007.
- C. Chen, R. Veldhuis, T. Kevenaer, and A. Akkermans. Biometric binary string generation with detection rate optimized bit allocation. In *IEEE Computer Society Conference on Computer Vision and Pattern Recognition. Workshop on Biometrics*, pages 1–7, Anchorage, Alaska, USA, June 2008.
- C. Chen, R. N. J. Veldhuis, T. A. M. Kevenaer, and A. H. M. Akkermans. Biometric quantization through detection rate optimized bit allocation. *EURASIP Journal on advances in signal processing*, 2009(Article ID 784834):1–16, 2009. doi:10.1155/2009/784834.
- L. Coventry, A. De Angeli, and G. Johnson. Usability and biometric verification at the ATM interface. In *CHI*, pages 153–160, Ft. Lauderdale, Florida, USA, April 5–10 2003.
- G. Doddington, W. Liggett, A. Martin, M. Przybocki, and D. Reynolds. Sheep, goats, lambs and wolves a statistical analysis of speaker performance in the nist 1998 speaker recognition evaluation. In *Int. conf. on spoken language processing*, 1998.
- Y. Dodis, L. Reyzin, and A. Smith. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. In C. Cachin and J. Camenisch, editors, *Advances in Cryptology - EUROCRYPT 2004*, volume 3027 of *Lecture Notes in Computer Science*, pages 523–540. Springer Berlin, Heidelberg, 2004. URL http://dx.doi.org/10.1007/978-3-540-24676-3_31.
- Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. *SIAM Journal on Computing*, 38(1):97–139, 2008.
- R. O. Duda and P. E. Hart. *Pattern classification and scene analysis*. Wiley-interscience, New York, USA, 1973.
- EDPS. Opinion of the European Data Protection Supervisor on a research project funded by the European Union under the Seventh Framework Programme (FP7) for Research and Technology Development - Turbine (TrUsted Revocable Biometric IdeNitiEs). Retrieved May 7, 2011 from http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/11-02-01_FP7_EN.pdf, February 2011.
- ENISA. ATM crime: Overview of the european situation and golden rules on how to avoid it. Technical report, European network and information security agency (ENISA), August 2009.
- Europay, Mastercard, VISA (EMVCo). Emv 4.2. Retrieved May 2, 2011 from <http://www.emvco.com/specifications.aspx>, June 2008.
- European Central Bank. Report on payment statistics. Retrieved February 8, 2010 from <http://sdw.ecb.eu>, Feb 2010.
- European Parliament and European Council. Directive 1995/46/EC of the european parliament and of the council of 24 october 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995.
- Federal trade commission. Consumer sentinel network data book for january - december 2008. Technical report, Federal trade commission, February 2009.
- L. Gong, M. A. Lomas, R. M. Needham, and J. H. Saltzer. Protecting poorly chosen secrets from guessing attacks. *IEEE J. on Selected Areas in Communications*, 11(5):648–656, 1993.
- Identity theft resource center. Identity theft: The aftermath 2008. Retrieved August 17, 2009 from http://www.idtheftcenter.org/artman2/uploads/1/Aftermath_2008_20090520.pdf, June 2008.
- Identity theft website. Retrieved May 24, 2008 from <http://www.idtheft.com>, 2008.
- International Biometric Group. Financial success for biometrics? *Biometric Technology Today*, 13(4):9 – 11, 2005. ISSN 0969-4765. doi: DOI:10.1016/S0969-4765(05)70289-7. URL <http://www.sciencedirect.com/science/article/B6W70-4G4KV14-M/2/a23e51fde09e25b5d1528abde1f3f097>.
- ISO/IEC. 7813:2006 - Information technology - Identification cards - Financial transaction cards, 2006.
- ISO/IEC JTC1 SC27. FDIS 24745 - Information technology - security techniques - biometric information protection, 2010.
- A. K. Jain, K. Nandakumar, and A. Nagar. Biometric template security. *EURASIP J. Adv. Signal Process*, 2008:113:1–113:17, January 2008. ISSN 1110-8657. doi: <http://dx.doi.org/10.1155/2008/579416>. URL <http://dx.doi.org/10.1155/2008/579416>.
- P. Jones. Banking on vein at the ATM. *Biometric Technology Today*, 14(5):8 – 9, 2006. ISSN 0969-4765. doi: DOI:10.1016/S0969-4765(06)70532-X. URL <http://www.sciencedirect.com/science/article/B6W70-4K30V54-K/2/5fef00017aec15afaf8ddd792a76a4b>.
- P. Jones. Banking on biometrics. *Biometric Technology Today*, 15(4):7 – 8, 2007. ISSN 0969-4765. doi: DOI:10.1016/S0969-4765(07)70100-5. URL <http://www.sciencedirect.com/science/article/B6W70-4NJXNSY-H/2/b6f7c18bfe52f3e4752f9f678ccea8a55>.
- A. Juels and M. Sudan. A fuzzy vault scheme. *Designs, Codes and Cryptography*, 38:237–257, 2006. ISSN 0925-1022. URL <http://dx.doi.org/10.1007/s10623-005-6343-z>. 10.1007/s10623-005-6343-z.
- A. Juels and M. Wattenberg. A fuzzy commitment scheme. In *Proceedings of the 6th ACM conference on Computer and communications security, CCS '99*, pages 28–36, New York, NY, USA, 1999. ACM. ISBN 1-58113-148-8. doi: <http://doi.acm.org/10.1145/319709.319714>. URL <http://doi.acm.org/10.1145/319709.319714>.
- E. Kelkboom, J. Breebaart, R. Veldhuis, X. Zhou, and C. Busch. Multi-sample fusion with template protection. In A. Brömme, C. Busch, and D. Hühnlein, editors, *BIO SIG 2009: Proceedings of the Special Interest Group on Biometrics and Electronic Signatures*, pages 55–67, Bonn, Germany, September 17–18 2009a. Gesellschaft für Informatik.
- E. J. C. Kelkboom, B. Gökberk, T. A. M. Kevenaer, A. H. M. Akkermans, and M. van der Veen. "3D Face": Biometric template protection for 3d face recognition. In *Proc. ICB*, pages 566–573, Seoul, Korea, 2007.
- E. J. C. Kelkboom, K. T. J. de Groot, C. Chen, J. Breebaart, and R. N. J. Veldhuis. Pitfall of the detection rate optimized bit allocation within template protection and a remedy. In *IEEE 3rd international conference on biometrics: theory, applications and systems (BTAS)*, pages 1–8, Washington, DC, USA, 2009b.
- E. J. C. Kelkboom, J. Breebaart, I. Buhan, and R. N. J. Veldhuis. Analytical template protection performance and maximum key size given a gaussian modeled biometric source. In *Proc. SPIE Defense, security and sensing*, Orlando, Florida, USA, April 2010.
- J.-P. Linnartz and P. Tuyls. New shielding functions to enhance privacy and prevent misuse of biometric templates. In J. Kittler and M. Nixon, editors, *Audio- and video-based biometric person authentication*, volume 2688 of *Lecture Notes in Computer Science*, pages 1059–1059. Springer Berlin, Heidelberg, 2003. URL http://dx.doi.org/10.1007/3-540-44887-X_47.
- Logica CMG. e-identity - European attitudes towards biometrics. Whitepaper, Logica CMG, 2006.
- D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman, and A. K. Jain. IBG comparative biometric testing - round 6. Technical report, International biometric group, Middlesex, United Kingdom, 2006.
- T. Mansfield, G. Kelly, D. Chandler, and J. Kane. Biometric product testing - final report. Technical report, Centre for mathematics and scientific computing, national physics laboratory, Middlesex, United Kingdom, 2001.
- D. B. McIntosch. Biometrics - a fad or the future? *Biometric Technology Today*, 17(5):9 – 11, 2009. ISSN 0969-4765. doi: DOI:10.1016/S0969-4765(09)

- 70077-3. URL <http://www.sciencedirect.com/science/article/B6W70-4WCWF7P-H/2/79389aba73ac82da5368e8cbb022ee23>.
- S. K. Modi and S. J. Elliott. Impact of image quality on performance: Comparison of young and elderly fingerprints. In K. Sirlantzis, editor, *Proceedings of the 6th international conference on recent advances in soft computing (RASC)*, pages 449–454, 2006.
- D. Moss. Collar the lot of us! The biometric delusion. Retrieved January 7, 2011 from http://www.theregister.co.uk/2009/08/14/biometric_id_delusion/, August 2009.
- S. J. Murdoch, S. Drimer, R. Anderson, and M. Bond. Chip and PIN is broken. In *IEEE Symposium on security and privacy*, Oakland, CA, USA, May 2010.
- K. Nandakumar, A. K. Jain, and S. Pankanti. Fingerprint-based fuzzy vault: Implementation and performance. In *IEEE transactions on information forensics and security*, pages 744–757, 2007.
- H. Ogata. Interoperability of biometric transactions in Japanese bank systems. In *1st ASEAN-FBI meeting*, Bangkok, Thailand, June 2009.
- ORC. Public attitudes toward the uses of biometric identification technologies by government and the private sector. Retrieved January 7, 2010 from <http://www.search.org/files/pdf/Biometricsurveyfindings.pdf>, 2001.
- J. Ortega-Garcia, J. Fierrez-Aguilar, D. Simon, M. F. J. Gonzalez, V. Espinosa, A. Satue, I. Hernaez, J. J. Igarza, C. Vivaracho, D. Escudero, and Q. I. Moro. Mcyt baseline corpus: A bimodal biometric database. *IEEE Proceedings Vision, Image and Signal Processing, Special Issue on Biometrics on the Internet*, 150(6): 395–401, December 2003.
- P. J. Phillips, P. J. Flynn, T. Scruggs, K. W. Bowyer, J. Chang, K. Hoffman, J. Marques, J. Min, and W. Worek. Overview of the face recognition grand challenge. In *IEEE conference on computer vision and pattern recognition*, pages 947–954, 2005.
- P. J. Phillips, W. T. Scruggs, A. J. O’Toole, P. J. Flynn, K. W. Bowyer, C. L. Schott, and M. Sharpe. FRVT 2006 and ICE 2006: Large-scale results. Technical report IR 7408, NIST National Institute of Standards and Technology, 2007.
- D. Simon-Zorita, J. Ortega-Garcia, M. Sanchez-Asenjo, and J. Gonzales Rodriguez. Minutiae-based enhanced fingerprint verification assessment on image quality factors. *Proc. 2003 international conference on image processing (ICIP)*, 2:891–894, September 2003.
- L. Tan. Fingerprint scan favored in Malaysia, Singapore. Retrieved January 15, 2010 from <http://www.zdnetasia.com/news/security/0,39044215,62011592,00.htm>, May 2007.
- L. Tan. Citibank Singapore launches biometric payment service. Retrieved January 15, 2010 from <http://www.zdnetasia.com/news/security/0,39044215,61965886,00.htm>, November 2009.
- The UK payments association. 2008 fraud figures announced by APACS. Retrieved May 2, 2011 from http://www.ukpayments.org.uk/media_centre/press_releases/-/page/685/, March 2009.
- TNS/TRUSTe. Consumer attitudes about biometrics in ID documents. Retrieved May 2, 2011 from http://www.truste.com/pdf/Biometrics_Study.pdf, August 2005.
- B. Toth and T. Mansfield. Latest biometric test results - performance, quality and interoperability. Technical report, Deloitte, 2006.
- P. Tuyls, A. H. M. Akkermans, T. A. M. Kevenaar, G. J. Schrijen, A. M. Bazen, and R. N. J. Veldhuis. Practical biometric authentication with template protection. In *Audio and video-based biometric person authentication*, pages 436–446. Springer, Berlin, Germany, 2005.
- University of Bologna. FVC2006: The fourth international fingerprint verification competition. Retrieved May 2, 2011 from <http://bias.csr.unibo.it/fvc2006/>, 2006.
- M. van Hooren. The market needs future proof payment solutions. Retrieved January 15, 2010 from <http://www.equens.com/Images/Futureofpayments.pdf>, March 2009.
- G. A. von Graevenitz. Biometric authentication in relation to payment systems and ATMs. *Datenschutz und Datensicherheit*, 31(9):681–683, 2007.
- L. Williams. How ‘visionary’ raised - and lost - a fortune. Retrieved May 2, 2011 from http://articles.sfgate.com/2008-12-07/news/17134023_1_unpaid-bills-venture-capital-touch, 2008.
- M. Wittman, P. Davis, and P. Flynn. Empirical studies of the existence of the biometric menagerie in the FRGC 2.0 color image corpus. *Computer Vision and Pattern Recognition Workshop*, 0:33, 2006. doi: <http://doi.ieeecomputersociety.org/10.1109/CVPRW.2006.71>.
- H. Xu and R. N. J. Veldhuis. Spectral representations of fingerprint minutiae subsets. In *Proceedings of the 2009 2nd International Congress on Image and Signal Processing*. IEEE Computer Society Press, October 2009. URL <http://doc.utwente.nl/68291/>.
- H. Xu, R. N. J. Veldhuis, A. M. Bazen, T. A. M. Kevenaar, T. A. H. M. Akkermans, and B. Gokberk. Fingerprint verification using spectral minutiae representations. *Trans. Info. For. Sec.*, 4(3):397–409, 2009a. ISSN 1556-6013. doi: <http://dx.doi.org/10.1109/TIFS.2009.2021692>.
- H. Xu, R. N. J. Veldhuis, T. A. M. Kevenaar, and T. A. H. M. Akkermans. A fast minutiae-based fingerprint recognition system. *IEEE Systems journal*, 3(4):418–427, 2009b.
- N. Yager and T. Dunstone. Worms, chameleons, phantoms and doves: New additions to the biometric menagerie. In *IEEE workshop on automatic identification advanced technologies*, pages 1–6, Alghero, Italy, 2007.