Cryptographic Protection of Biometric Templates: Chance, Challenges and Applications

U. Korte, R. Plaga

Federal Office for Information Security (BSI)
Godesberger Allee 185-189
D-53175 Bonn
ulrike.korte@bsi.bund.de
rainer.plaga@bsi.bund.de

Abstract: In this contribution a survey is presented about the possibilities and difficulties of a cryptographic protection of biometric information for the purpose of authentication. The crucial role of sufficient information content of biometric templates will be presented. It will be shown how to use this approach of a cryptographic protection of biometric templates in connection with biometric databases. Finally, a proposal is given, how to combine it with centralised PIN verification procedures in online banking scenarios as a new application scenario.

1. Requirements for the protection of biometric information.

Traditional biometric authentication systems store biometric templates together with the data identifying an individual in a database for later comparison. In order to authenticate an individual the biometric data presented is looked up in the database. If a record is found with biometric data that is sufficiently close to that presented, the person is identified. However, the storage of biometric data leads to considerable risks for the authentication system and raises serious concerns regarding data protection. This way of storing biometric data is often criticised as a mass storage of privacy sensitive personal data that is potentially threatened by internal or external attacks on the database.

The following risks concerning security and privacy are to be prevented:

- **Identity theft**

Storage of the templates in many databases and locations increases the probability of theft and abuse. A human being has only a limited number of biometric features (for example 1 face, 10 fingers, 2 irises). Due to this limitation a compromised template is compromised forever. In contrary to a password or PIN, no revocation and renewal is possible.

- **Cross matching attack**

As soon as identical templates are stored in multiple databases or datasets, it is possible to perform cross matching between them. In this case the privacy of the human being is not guaranteed.

- **Disclosure of sensitive information**

Biometric information, in contrast to passwords or access tokens, in principle allows to draw conclusions about the properties of the enrolee's body.

In some publications it is even reported that biometric templates may reveal sensitive medical information. In an epidemiological study performed at the "Centre for Disease Control" (CDC) Kahn et al. [19] found that there is a correlation between the ridge count difference between the right fourth and fifth fingertip and the "upper body tissue distribution", a property that indicates the risk for diabetes.

Therefore it would be of very great value to protect the biometric information by cryptographic means against external but also internal attacks.

2. A chance: Protecting templates by applying error-correcting and cryptographic methods.

2.1. General Description

There is a voluminous body of literature that proposes procedures with slightly different methods how to protect biometric templates with error-correcting and cryptographic methods. Most of these methods also provide for key derivation. Examples for such schemes are e.g. [17], [11], another one is discussed by Kevenaar & Zhou at this workshop BIOSIG 2007. Still another procedure [18] is described in the next subsection.

In the rest of this subsection we give a qualitative overview of these methods. The main simplification in this description is the omission of detailed technical procedures employing some kind of "helper data" (as for example a "secret key s", as described in subsection 2.2.).

An approach based on these publications, that are pursued at the BSI, is not to store the biometric template together with identity information gathered during enrolment itself, but a *public data record* as reference data. This data record allows both identification and verification of an individual if, and only if, the requestor proves his knowledge of the original template. Without proof no information can be derived from the public record and thus it cannot be used for fraudulent authorisation. In particular, the data stored for identification or verification do not allow the recovery of the corresponding biometric data. This property minimises the risk of unauthorised access to biometric data and can thus help to soothe common resentments against biometric authentication.

This approach is conceptually very similar to password authentication systems that store only the hash values of the passwords from which it is computationally hard to draw conclusions about the original password. The hash value does not allow the recovery of the corresponding password without exhaustive search but still provides means to verify the correctness of the password presented during authentication. However, the transfer of this approach to biometric authentication is not straightforward because biometric measurements are inherently prone to errors, which are not tolerated by cryptographic hash functions. Therefore, the biometric authentication systems must be based on an error-tolerant authentication scheme.

The error-correcting methods remove noise in the template. It is fundamentally impossible to avoid noise during biometric data acquisition, because “life means change“. For example, faces age and iris patterns are not perfectly invariant to a contraction of a pupil. More noise is introduced by changes in the environmental conditions, which is again an unavoidable circumstance. Finally noise often finds its way into the sensor, during transmission or in the data processing process (“algorithmic noise“). The latter noise sources can be reduced or even removed by improved engineering.

The error corrected template is a *”bit identical“ unique data set that can be derived repeatedly from the different noisy biometric templates of a user*. It is often designated as a “biometric key“[12].

One way to obtain the cryptographically protected ”public data record“, mentioned above, would be to hash this biometric key[1].

The error correction is indispensable in order to use cryptographic algorithms for the protection of information, however it comes with a price tag attached: Because a large number of ”noisy“ templates must be assigned unambiguously to one ”noise free“ error-corrected template, the latter has a much shorter, decreased informational content. This factor is security relevant, because it can make the protection scheme vulnerable to ”brute-force“ attacks.

[1] In some schemes the error correcting code is used in connection with some helper data instead of the biometric template.

2.2. Example of one special cryptographic and error correcting scheme

A prototype system for the protection of biometric DNA templates was developed in a project of the BSI [20]. This system is based on a scheme published by Juels and Wattenberg [18] and uses the biometric data presented for authentication to extract a secret key which can be used for further cryptographic applications (e.g. for the encryption of the user's name).

Juels and Wattenberg [18] proposed a very simple scheme based on any binary (not necessarily linear) $[n, k, 2t+1]$ error correcting code $C \subset GF(q)^n$ for the Hamming distance with generator matrix G, where $GF(q)^n$ denotes the finite field with q elements. The encoding function transforms messages consisting of k symbols into n symbol code words (n>k), that can be retransformed into the original messages even if up to t symbols of the received codeword are corrupted due to error.

During enrolment, a random codeword, i.e. $c = G(s)$ for a random $s \in GF(q)^k$, is bitwise added (XOR) to the biometric template f and the result is stored in the database as:

$$y = c \oplus f \qquad (1).$$

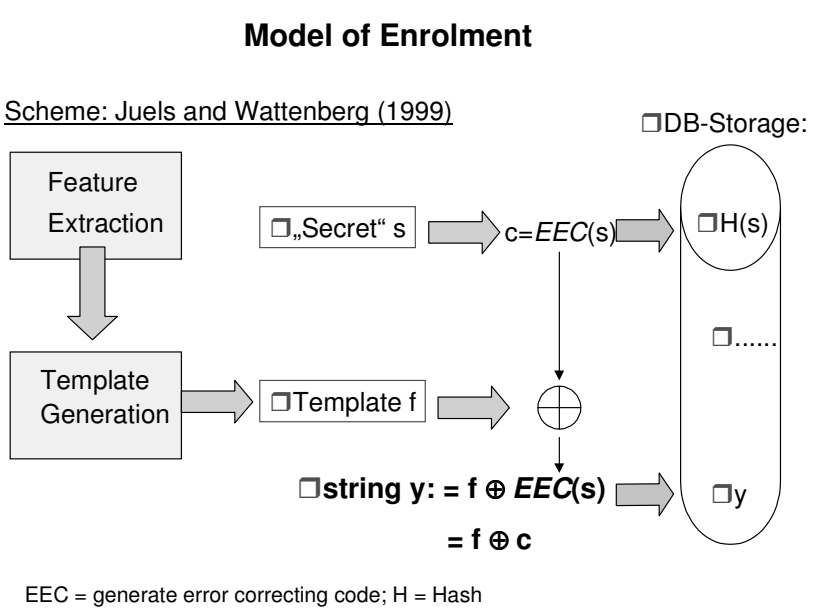

Figure 1: Model of Enrolment

Furthermore, the secret s is hashed with a cryptographic hash function H and H(s) is stored in the database. This scheme is sketched in symbolical form in figure 1.

For authentication, the template f^*, presented by the user, is added to the value y stored in the database. The result is $f^* \oplus y = f^* \oplus c \oplus f$. If the hamming distance between f^* and f is at most t, $c = G(s)$ and hence s can be recovered. If the hash value of the recovered s matches the one stored in the database, the user is authenticated.

This approach extracts a secret key from the biometric template presented and the corresponding public string. No information about this key shall be extractable from the public string without the corresponding biometric template.

3. A security challenge and requirements to meet it.

3.1. "Brute force" attacks against cryptographically protected templates and the information content of biometric templates.

The security of cryptographic protocols for the protection of templates, as discussed in the previous section, has not been systematically evaluated, yet. This is perhaps the most important reason why these schemes have hardly been introduced in production processes up to now. "Brute force" attacks, in which all bit combinations that are combinatorically possible, are tried to reverse a one-way function.

By analogy to the case of passwords the length "k" of the biometric key should not be shorter than the minimal entropy "n" of a secure password. We choose $k \geq 50$ bits as a guide line because commercial online password-crack services [23] offer to decrypt shorter password hashes at modest costs.

Brute-force attacks against biometric templates are not quite as straightforward as in the case of passwords. A typical brute-force attack would have to be staged with trial biometric features rather than mere bit permutations in the case of passwords. However, there are publicly available tools to "create" e.g. artificial fingerprints from random numbers [10].

The number of artificial templates necessary for a successful match of any given template is limited and large databases with such features ("biometric dictionaries") could be efficient attack tools. The templates are usually much longer than passwords, so that just trying all bit combinations is often infeasible.

However, templates contain strong correlations, i.e. their bits are not independent from each other and the true information content is much smaller than the template length. The attacker can, therefore, create a large number of "artificial" templates on a computer which can then be used to create a "dictionary" of suitably correlated templates. Error-correcting methods are then employed to create an even much smaller "dictionary" of "error-corrected" templates. If this dictionary has less than about 2^{50} entries, trying all combinations of a cryptographically protected template becomes computationally feasible even with modest financial resources.

Therefore, to rely on the inability of an attacker to understand the correlations in templates of the various biometric features in use and to exploit such a knowledge to write an efficient attack code would mean to rely on ”security by obscurity”. A sophisticated method to create suitably correlated templates via modifying biometric images was developed by Adler [2]. He describes successful ”hill-climbing” attacks on the biometric encryption system by Soutar et al. [22]. It seems likely that similar methods will be developed for any biometric key (at the latest after its widely spread introduction). Therefore, the length of the final error-corrected template (the ”biometric key's length”) must be at least about 50 bits.

What is the value of this maximal ”biometric key's length k“ for a given biometric system? A mathematical theory to derive this value was developed at the BSI [21]. There it is shown that under certain idealised conditions the following inequality holds:

$$k \leq -\log_2(FAR) \qquad (2)$$

Here “k” is the maximal length of the biometric key and FAR is the false acceptance rate i.e. the ratio of ”successful verifications“ to the ”number of impostor verification attempts“ of the biometric system.

The maximal length of biometric keys can then be inferred from the FAR determined in the BioP2 study performed on behalf of BSI and BKA [7]. Using the result inferred for ”experienced users“ of the biometric systems and accepting a false-rejection rate of not more than 5%, the maximally extractable key length derived on the basis of equation (2) for one finger or one iris are 17 bits, and the one for one face are 14 bits. Strictly speaking the application of equation (2) is not warranted in the cases of the fingerprint- and face-based biometric systems because they do not conform to some assumptions necessary for an application of the ”idealised” biometric model laid out in reference [21]. However, the methods employed are optimised for achieving an optimal FAR and not a maximal biometric-key length. Therefore, it seems likely that the biometric-key length estimated for finger and face based systems using equation (2) remains valid as an upper limit.

We conclude that with the ”state-of-art-systems“ employed under practical conditions at an international airport, the maximally extractable key length from one biometric feature is not sufficient for a cryptographic protection of the templates against brute-force attacks.

3.2. Requirements for cryptographic keys

The secret key extracted by the identification function shall be suited for cryptographic applications with at least strength of functions-medium. In particular, the following requirements must be met:

- The length and the entropy of the key should be at least 50 bit, preferably more than 80 bits.

- There should be no exploitable dependency between the keys of distinct individuals, i.e. the knowledge of the keys of one or several individuals should not give any advantage in determining the keys of a different individual.

4. Biometric keys with sufficient length for secure applications: future possibilities.

A prerequisite for a secure use of biometric keys is that at least one of the following alternative future technical developments allows the extraction of long enough biometric keys:

1. The technical performance of biometric systems is substantially improved.

2. ”Multi-modal” biometrics are employed, i.e. the biometric key is extracted from more than one biometric feature, e.g. several fingerprints.

3. New biometric features, which allow to extract more information, are employed.

Biometrics is still a relatively young and immature technology.

Option 1, substantial improvements of the template quality, can be expected in the future.

Option 2, the extraction of biometric keys from more than one feature, seems promising especially in the case of finger prints. It raises some yet unsolved questions which are in the focus of the present workshop BIOSIG 2007 (contributions by Veldhuis and the expert panel).

Option 3 could e.g. be realised as a DNA based biometric system. The human genome contains about 2.5 Mbytes of stable discriminatory information [9]. Extracting just a tiny fraction of this information in real time would be sufficient for its use as a biometric key. In the prototype system for the protection of biometric templates, as described in section 2.2., biometric keys with a length of 70 bits at a false rejection rate below 1 % were extracted from true genetic fingerprints [20]. The principle feasibility of the cryptographic protection was thus demonstrated.

5. Application scenarios

5.1. Biometric databases

The emergence of the deployment of biometric technologies is actually creating new application fields where biometric templates are stored e.g. in centralised or decentralised databases.

There exist already forensic databases or biometric material databases for medical research for example.

The method described in chapter 2.2, to protect biometric templates by error correcting codes and cryptography, is an effective countermeasure to the threats concerning the privacy and security of the biometric template, also mentioned in chapter 2.

5.2. Biometric Authentication in the context of automated teller machines

In the banking industry the use of biometric templates in connection with automated teller machines or point of sale systems is still in its infancy. There were some experimental testing scenarios in connection with automated teller machines at the end of the 20th century (e.g. Dresdner Bank, Bank United of Texas).

In recent years the banking organisations all over the world have implemented new "Chip card and PIN authentication schemes" in automated teller machines in order to reduce card fraud costs. Since then new attacks on these schemes have been published (see e.g. [1], [6]).

Because of these security threats about 40 Japanese banks have introduced biometric palm vein authentication technologies in about 19.000 automated teller machines. The vein is an externally invisible biometric feature and, therefore, difficult to copy. There are also projects in Brazil and in Austria (see [5]).

In Europe, the banking transaction of an automated teller machine is sent to the computer centre of the card issuing bank and there the customer authentication is performed centrally.

Therefore, in this case, it is recommendable, to prevent the storage of the unprotected biometric templates in a central database ([5]). Especially, the method of protecting biometric templates by error-correcting and cryptographic methods could be practised, as described in the following text.

The values of the false acceptance rate for vein based biometric solutions, published by vendors, are 0,00008% in ([5]) and 0,0001% in ([16]). According to the schemes described in chapter 2 and to the formula (2) in chapter 3, the upper bound of the derived "biometric key's length" lies below 21 bits. Therefore, even for vein based biometrics the problem discussed in chapter 3 is not solved, yet.

It is advisable to combine the biometric method with the traditional PIN and chip schemes, as done in Japan. "This mechanism ensures a three stage security solution; ensuring users provide something they 'own' (the card), something they 'know' (the pin) and something they 'are' (the biometric identifier) before the transaction is processed" (see [16]).

One major challenge for the future will be to create new international standards for personal identification schemes including biometric authentication technologies in order to guarantee interoperability between different banking organisations and countries.

One approach is the generalisation of the existing international banking standards ([3], [4], [14] and [15]) and combining them with the biometric template protection approach in chapter 2.

The banking industry actually supports many different PIN generation and verifying procedures and formats.

For the VISA PVV PIN Algorithm [15], which supports a non-secret PIN Verification Value (PVV), we suggest a generalisation of the PIN procedure in the following way, introducing biometric technologies. The major aim for this generalisation is to allow the introduction of biometric technology with minimal changes in the actual standards and hardware implementations.

According to the scheme of Juels and Wattenberg (see chapter 2.2. and [18]), in a banking card personalisation centre, a random codeword, i.e. $c = G(s)$ for a random $s \in GF(q)^k$, is bitwise added (XOR) to the biometric template f of the cardholder during enrolment and the result is stored on the banking card as $y = c \oplus f$.

Then the secret value s is hashed with a cryptographic hash function to obtain H(s). After generating a secret PIN, the hash value H(s) is used as a new input parameter to produce the non-secret PIN verification value PVV in a generalised way, combining conventional PIN procedures and biometric technologies, as shown in picture 2.

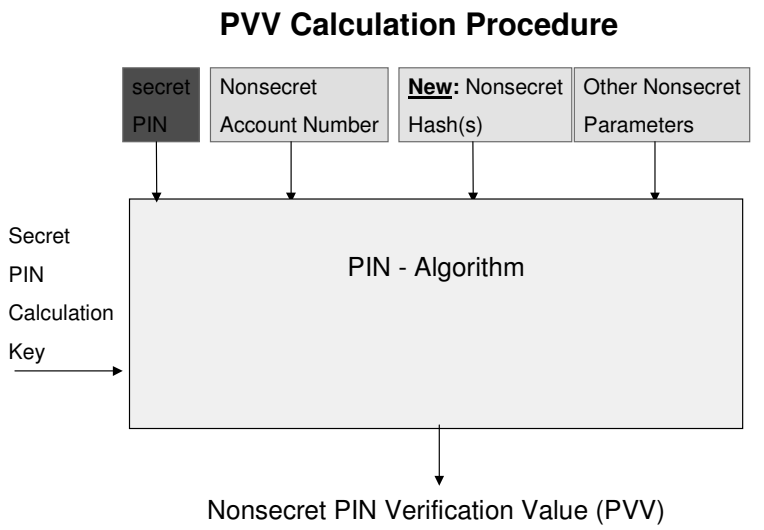

Figure 2: PVV calculation procedure in the banking card personalisation centre

The biometric data is introduced as one non-secret parameter. For example in the IBM-implementation [13], the parameter "data_array-Reserved-2" and "data_array-Reserved-3" of the API "Clear PIN Generate Alternative" could be used for this purpose.

If a customer uses an automated teller machine, he enters his secret PIN. Further more, a biometric feature is extracted and a biometric template is generated. In the banking card this biometric template f^*, presented by the user, is added to the value y stored in the banking card. The result is $f^* \oplus y = f^* \oplus c \oplus f$. Since we are working with an error correcting code, the corresponding decode function produces a value s^*. If the hamming distance between f^* and f is at most t, then $s^* = s$, otherwise not. After hashing the received value s^*, $H(s^*)$ is integrated into the banking transaction together with the encrypted PIN.

The banking transaction is encrypted and sent to the banking authorisation centre. In the banking authorisation centre the transaction is decrypted.

The encrypted PIN and the hash value H(s^*) are extracted together with other parameters, e.g. the PVV, the account number, and are used as input parameters for the PIN verification procedure, as shown in picture 3. The generalised PIN verification procedure generates a new PVV-value PVV*, corresponding to the supplied PIN, account information, hash value H(s^*) and other parameters and compares it with the input-PVV. If the PVV* = PVV, the user is authenticated. If an authorisation fails, the retry counter can be limited by a small value in order to prevent brute force attacks.

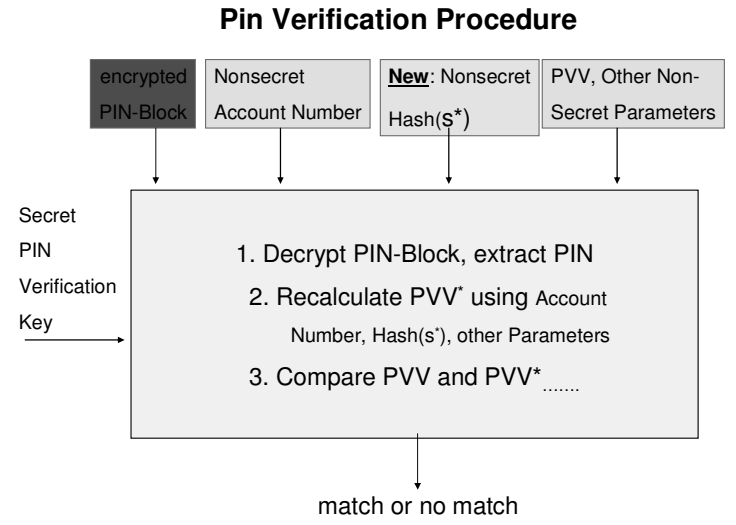

Figure 3: PIN verification procedure

6. Conclusion

In this paper methods are surveyed to protect biometric templates in general and for special application scenarios with authentication schemes, e.g. in connection with biometric databases and automated teller machines. We conclude that there exist suitable algorithms and protocols for this task. We suggest a suitable integration in existing protocols. However, there is still one fundamental obstacle to construct secure systems: a *lack of entropy in most single biometric features*. Strategies to overcome this problem are proposed. The challenge for the near future is to implement a secure system for practical use.

References

[1] B. Adida, M. Bond, J. Clulow, A. Lin, S. Murdoch, R. Anderson, and R. Rivest. Phish and Chips (Traditional and New Recipes for Attacking EMV). Security Protocols, 14th International Workshop, Cambridge, England, March 27–29, (2006).

[2] A. Adler. Vulnerabilities in biometric encryption systems. In: Proceedings Audio- and Video-based Biometric Person Authentication – AVBPA 2005, Tarrytown New York. LNCS vol. 3546, pp.1100-1109, Springer, Berlin Heidelberg New York, (2005).

[3] American National Standard. X9.8-1982. American National Standard for Personal Identification Number (PIN) Management and Security, American Bankers Association, Washington, (1982).

[4] American National Standard. X9.9-1986, American National Standard for Financial Institution Message Authentication (Wholesale), American Bankers Association, Washington, (1986).

[5] T. Bengs, W. Grudzien. Biometrie in der Kreditwirtschaft. In: Datenschutz und Datensicherheit (DUD) 2007, volume 3/207, pp. 157-159, (2007).

[6] O. Berkman, O. M. Ostrovsky. The unbearable lightness of PIN cracking, Tel Aviv University, School of Computer Science, http://www.arx.com/documents/The_Unbearable_Lightness_of_PIN_Cracking.pdf, as of 29.05.2007.

[7] BSI, BKA, Secunet. Untersuchung der Leistungsfähigkeit von biometrischen Verifikationssystemen – BioP2, available at: http://www.bsi.bund.de/fachthem/biometrie/projekte/index.htm, (2005).

[8] Bundesamt für Sicherheit in der Informationstechnik. Biometrie, http://intranet/internet/literat/faltbl/F23Biometrie.htm, as of 11.01.2007.

[9] J. M. Butler. Forensic DNA Typing. Elsevier, Amsterdam, (2005).

[10] R. Cappelli, A. Erol, D. Maio, D. Maltoni. Synthetic Fingerprint-image Generation. In: Proceedings International Conference on Pattern Recognition (ICPR2000).Vol.3, pp. 475-478. (2000). "Sfinge" tool is available for download at: http://bias.csr.unibo.it/research/biolab/sfinge.html.

[11] Y. Dodis, L. Reyzin and A. Smith. Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data. In Advances in Cryptology—EUROCRYPT 2004, volume 3027 of Lecture Notes in Computer Science, Springer-Verlag, 523-540, (2004).

[12] F. Hao, R. Anderson, J. Daugman. Combining crypto with biometric effectively, IEEE Trans. Comp. 55, 1081-1088, (2006).

[13] IBM, CCA Basic Services Reference and Guide, Release 2.53, IBM xSeries and pSeries PCICC Feature, twelfth edition (2004).

[14] International Organisation for Standardization. ISO 9564-1, Banking - Personal Identification Number (PIN) management and security – Part 1: Basic principles and requirements for online PIN handling in ATM and POS systems, (2002).

[15] D.B. Johnson et al.. Common Cryptographic Architecture – Cryptographic Application Programming Interface, IBM Systems Journal, vol. 30, No. 2, 1991, 130-150, (1991).

[16] P. Jones. Banking on vein at the ATM, Biometric Technology Today, May 2006, 8-9, (2006).

[17] A. Juels and M. Sudan. A Fuzzy Vault Scheme. In IEEE International Symposium on Information Theory, 2002, 408-413, (2002).

[18] A. Juels and M. Wattenberg. A Fuzzy Commitment Scheme. In Proc. ACM Conf. Computer and Communications Security, 1999, 28-36 (1999).

[19] H. S. Kahn, R. Ravindranath, R. Valdez & K. M. Venkat Narayan. Fingerprint Ridge-Count Difference between Adjacent Fingertips (dR45) Predicts Upper-Body Tissue Distribution: Evidence for Early Gestational Programming, Am.J.of Epidemiology 153, 338- 344 (2001).

[20] U. Korte, M. Krawczak, U. Martini, J. Merkle, R. Plaga, M. Niesing, C. Tiemann, H. Vinck. Abschlußbericht Projekt BioKeyS, BSI, (2006).

[21] R. Plaga. Report: Biometric keys: suitable use-case and achievable information content, (2007).

[22] C. Soutar, D. Roberge, A. Stoianov, R. Gilroy, B. V. K. Vijaya Kumar. Biometric Encryption™ using image processing. Proc. SPIE vol. 3314, pp.178-188; (1998), see also Website of Bioscrypt Inc., http://www.bioscrypt.com.

[23] e.g. http://www.rainbowcrack-online.com.