New Shielding Functions to Enhance Privacy and Prevent Misuse of Biometric Templates

Jean-Paul Linnartz and Pim Tuyls

WY7, Nat.Lab., Philips Research, 5656 AA Eindhoven, The Netherlands
j.p.linnartz@philips.com pim.tuyls@philips.com

In biometrics, a human being needs to be identified based on some characteristic physiological parameters. Often this recognition is part of some security system. Secure storage of reference data (i.e., user templates) of individuals is a key concern. It is undesirable that a dishonest verifier can misuse parameters that he obtains before or during a recognition process. We propose a method that allows a verifier to check the authenticity of the prover in a way that the verifier does not learn any information about the biometrics of the prover, unless the prover willingly releases these parameters. To this end, we introduce the concept of a delta-contracting and epsilon-revealing function which executes preprocessing in the biometric authentication scheme. It is believed that this concept can become a building block of a public infrastructure for biometric authentication that nonetheless preserves privacy of the participants.

Introduction

Measurement of distinguishing features of physical objects and living beings can be used to identify these and distinguish them from others. In some cases, there is a desire to add cryptographic properties to this identification process. In biometrics, a human being is identified by measuring a set of parameters of the body. Biometric data are said to identify a person based on "who he is", rather than on "what he has" (such as a smartcard) or "what he knows" (such as a password). An unresolved issue, however, is that when deployed at large scale, a citizen looses privacy as he must reveal his identifying biometric data to his bank, to the government, to his employer, the car rental company, to the owner of a discotheque or nightclub, etc. Each of them will obtain the same measured data, and unless special precautions are taken there is no guarantee that none of these parties will ever misuse the biometric data to impersonate the citizen.

This paper proposes, reviews and analyzes a novel technique to enhance the privacy and security of authentication and key establishment in biometric applications. In particular, we prevent misuse of templates. Following the tradition in cryptography to name our role players, we will say that prover Peggy allows verifier Victor to measure her object [1] or physiological parameters [2] called "Prop." We are

not only interested in security breaches due to a dishonest Peggy, but also in those resulting from an unreliable Victor.

Often the distinction is made between **identification** and **verification**. Identification estimates which object is presented by searching for a match in a data base of reference data for many objects. Victor a priori does not know whether he sees Prop1 (belonging to Peggy) or Prop2 (belonging to Petra). On the other hand, verification attempts to establish whether the object presented truly is the object Prop that a known prover Peggy claims it to be. Peggy provides not only Prop but also a message in which she claims to be Peggy and can be linked to Prop, in some direct or implicit way. Here, we address primarily the setting of verification, that is, Victor is assumed to have some a priori knowledge about Prop in the form of certified reference data, but at the start of the protocol he is not yet sure whether Prop or a fake replacement is present.

To further develop the insight in the security aspects of verification, we distinguish (possibly against common practice in biometric literature) between verification and **authentication**. In a typical verification situation, the reference data itself allows a malicious Victor to artificially construct measurement data that will pass the verification test, even if Prop itself has never been available. In authentication, the reference data gives insufficient information to allow Victor to (effectively) construct valid measurement data.

While such protection is not yet mature for biometric authentication, it is common practice with computer passwords. When a computer verifies a password, it does not compare the password p typed by the user with a stored reference copy. In stead the password is processed by a cryptographic one-way function F and the outcome is compared against a locally stored reference string $F(p)$ [3]. This prevents that the system can be attacked from the inside such that the unencrypted or decryptable password of its users can be stolen.

The main difference with biometrics is that during measurements it is unavoidable that noise or other aberrations occur. Noisy measurement data will be quantized into discrete values before these can be processed by any cryptographic function. Due to external noise, the outcome of the quantization may differ from experiment to experiment. In particular if Peggy's physiological parameter takes on a value close to a quantization threshold, minor amounts of noise can change the outcome. Minor changes at the input of a cryptographic function will be amplified and the outcome will bear no resemblance to the expected outcome. This effect, identified as 'confusion' and 'diffusion' [3], makes it less trivial to use biometric data as input to a cryptographic function. Particularly the comparison of measured data with reference data can not be executed in the encrypted domain.

It is an essential part of this paper to discuss whether the measurement must be stored itself or it suffices to store and exchange only a (one-way) cryptographic derivative. Storage of reference data (user templates) and protecting their privacy is well recognized as a key concern with biometric authentication [4,15]. Preferably the derivative should not allow an attacker to construct fake data. It was previously known that enrollment data can be encrypted. However, a security weakness appears when during authentication the data needs to be decrypted. This problem was also addressed in [6, 7, 9, 10]. In the current paper we further develop and generalize the mathematical formulation, including an information theoretic evaluation of

concealing properties and we analyze a new solution.Before an authentication can take place, Prop must have gone through an **enrollment** phase. During this phase, Peggy and Prop visit a Certification Authority. Prop's parameters are measured. These measurements are processed and stored for later use. In an on-line application, such reference data can be stored in a central (possibly even publicly accessible) data base or these data can be certified with a digital signature of the Certification Authority, and given to Peggy. In the latter case, it is Peggy' responsibility to securely give this certified reference data to Victor.

Key establishment: In addition to authentication, the system can use Prop's (biometric) parameters to generate a secret key [11, 12]. An important property is that Victor should not be able to calculate this key on his own, by misusing reference data that is offered to him. Victor must measure Prop, otherwise he should not be able to find the key.

We illustrate this by the example of access to a data base of highly confidential encrypted documents to which only a (set of) specific users is allowed access. The computer retrieval system authenticates humans and retrieves an\ decryption key from their biometric parameters. This system must be protected against a dishonest software programmer Mallory who has access to the biometric reference data from all users. If Mallory downloads the complete reference data file, all encrypted documents, and possibly reads all the software code of the system, she should not be able to decrypt any document.

We distinguish between to attacks

1. Misuse of templates: a dishonest Victor can attempt to calculate the parameters of Prop or to establish the key without having access to the object. This corresponds to a system operator who attempts to retrieve user passwords from the reference database of data strings $F(p)$.
2. Misuse of measurement data: After having had an opportunity to measure Prop, a dishonest Victor misuses its measurement data. This corresponds to grabbing all keystrokes including the plain passwords typed by a user.

This text primarily addresses attack 1. Attack 2 typically is prevented by mutual cryptographic authentication of Victor and Peggy in addition to the biometric exchange of data from Prop [14].

Model

In order to study countermeasures against misuse of templates, we consider the system depicted in Figure 1. This authentication system consists of a mechanism to extract a measurement Y of the object, some signal processing function $G(W,Y)$ and a cryptographic function F. F is one-way in the sense that it is "easy" to calculate the output given the input signal but it is computationally "infeasible" to find a valid input given an output value [4]. An important aim is to propose and study appropriate choices for G to enhance the reliability and reproducibility of the detection and to shield the information (or 'entropy') in the authentication secret Z from the reference data. The reference data consists of two parts: the cryptographic key value V against

which the processed measurement data U is compared, and the data W which assists in achieving reliable detection.

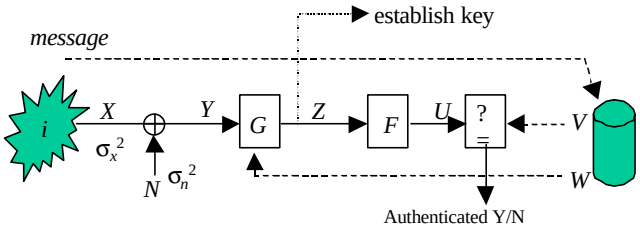

Figure 1: Model of authentication of Prop *i* and generation of a seed for key establishment. Noise *N* occurs during measurement *Y* of parameter *X*. The delta-contracting function *G* and the hash *F* are invoked to create U, which then is verified against reference template (W,V).

Peggy authenticates herself with Prop as follows:

- When she claims to be Peggy, she sends her identifier message to Victor, and makes Prop available for measurement.
- Victor retrieves the authentication challenge W from an on-line trusted database. Alternatively, in an off-line application Peggy could provide Victor with reference data (V,W) together with a certificate that this data is correct.
- Peggy allows Victor to take a (possibly noisy) measurement $Y = X + N$ of the physiological properties X of Prop
- Victor calculates $Z = G(W,Y)$.
- Optional for key establishment: Victor can extract further cryptographic keys from Z, for instance to generate an access key.
- Victor calculates the cryptographic hash function $F(Z)$.
- The output $U = F(Z)$ is compared with reference authentication response V. If $U = V$, the authentication is successful.[1] [2]

Here, X, N, and Y are real (or complex) valued vectors of length n_1, $X \in \mathrm{R}^{n1}$. Vector W contains n_2 values, typically real, complex or high resolution digital numbers, that control the function $G(W,X)$. Further, Z, U and V are discrete-valued (typically binary) vectors of length n_3, n_4, and n_4, resp. During authentication, Z is the estimate of the authentication secret S that was chosen during enrollment, which we will describe next.

[1] In a networked system, the creation of U is typically executed locally at the verifier, whereas V is stored in a central database. Either Victor sends U to the data base and the verification is done at the data base, or the database send V to Victor and Victor himself compares U with V.

[2] Note that here we make an exact match. Checking for imperfect matches would not make sense because of the cryptographic operation F. Measurement imperfections (noise) are eliminated by the use of W and the δ-contracting property of G.

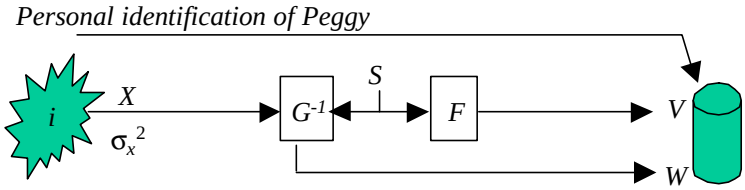

Figure 2: Enrollment of Prop *i*, involving the estimation of *X*, the choice of *S*, and the calculation of *V* and *W*. Here G^{-1} is the inverse of the delta-contracting function and F a hash function.

During enrollment, some secret S ($S \in \{0,1\}^{n3}$) is chosen, and the corresponding $V = F(S)$ is calculated V ($V \in \{0,1\}^{n4}$). Further, X is measured. The enrollment can be performed under more ideal circumstances, or can be repeated to reduce the variance of the noise. Thus we assume that $N \approx 0$ during enrollment and that X is available. Thirdly, a value for W is calculated such that not only $G(W,X) = S$ but also during authentication $G(W,Y) = S$ for $Y \approx X$. We call this property δ-contracting.

Definition 1: Let $G(W,Y)$: $R^{n1+n2} \rightarrow \{0,1\}^{n3}$ be a function and $\delta \geq 0$ be a non-negative real number. The function G is called "δ-contracting" if and only if for all $X \in R^{n1}$ there exist (an efficient algorithm to find) at least one vector $W \in R^{n2}$ and one binary string $S \in \{0,1\}^{n3}$ such that $G(W,Y)$ is constant on a ball with radius δ around X, i.e., $G(W, X) = G(W, Y) = S$ for all $Y \in R^{n1}$ such that $\| X - Y \| \leq \delta$.

Any function is 0-contracting. The δ-contracting property ensures that despite the noise, for a specific Prop all likely measurements Y will be mapped to the same value of Z.

Definition 2: Let $G(W,X)$: $R^{n1+n2} \rightarrow \{0,1\}^{n3}$ be a function. The function G called "versatile " if and only if for all $S \in \{0,1\}^{n3}$ and all $X \in R^{n1}$, there exists (an efficient algorithm to find) at least one vector $W \in R^{n2}$ such that $G(W,Y) = S$.

A trivial ∞-contracting function is $G(W,X) = Constant$. However this function is not versatile. The property of versatility is relevant particularly for key establishment. A trivial versatile and ∞-contracting function is $G(W,X) = C(W)$. However, in this solution W reveals the secret S, or at least, the conditional entropy $H(S|W) = 0$

Theorem: If W is a constant, i.e., if $G(W,Y) = C(Y)$ then either the largest contracting range of G is $\delta = 0$ or $G(W,Y)$ is a constant independent of Y.

Proof: Assume G is δ-contracting, with $\delta > 0$. Choose two points Y_1 and Y_2 such that $G(W,Y_1) = Z_1$ and $G(W,Y_2) = Z_2$. Define a vector $r = \lambda(Y_2 - Y_1)$ such that $0 < \|r\| < \delta$. Then, $Z_1 = G(W,Y_1) = G(W,Y_1 + r) = G(W,Y_1 + 2r) = \ ... = Z_2$ Thus $G(W,Y_1) = G(W,Y_2)$ is constant.

Corrolary: The desirable property that biometric data can be verified in the encrypted domain cannot be achieved unless Prop-specific data W is used. Biometric authentication that attempts to process Y without such "helper" data is doomed to store decryptable user templates.

Definition 3: Let $G(W,Y)$: $R^{n1+n2} \rightarrow \{0,1\}^{n3}$ be a δ-contracting function with $\delta \geq 0$ and $\varepsilon \geq 0$ be a non-negative real number. The function G is called "ε-revealing" if

and only if for all $X \in R^{n1}$ there exists (an efficient algorithm to find) a contracting vector $W \in R^{n2}$ such that the mutual information $I(W;S) < \varepsilon$.

Hence W conceals S: it reveals only a well-defined, small amount of information about S. Similarly, we require that V conceals S. However we do not interpret this in the information theoretic sense but in the complexity theoretic sense, i.e., the computational effort to obtain a reasonable estimate of (X or) S from V is prohibitively large, even though in the information theoretic sense V may (uniquely) define S.

Proposed System

We have developed several constructions of δ-contracting and ε-revealing biometric authentication systems. We will describe one here. For a more elaborate discussion, we refer to a forthcoming paper [8]. For simplicity we adopt a model of X and N being zero mean i.i.d. jointly Gaussian random vectors with variance σ_x^2 and σ_n^2, resp. For the i-th dimension (1, 2, .. i , ... ,n_1, $n_1 = n_2$) of Y, W and Z, the δ-contracting function is

$$z_i = \begin{cases} 1 & \text{if } 2nq \le y_i + w_i < (2n+1)q, \quad \text{for any } n = ..,-1,0,1,.. \\ 0 & \text{if } (2n-1)q \le y_i + w_i < nq,, \quad \text{for any } n = ..,-1,0,1,.. \end{cases}$$

with q a quantization step size. During enrollment, x_i is measured and the C.A. will find a w_i such that the value of $x_i + w_i$ is pushed to the nearest lattice point where $x_i + w_i + \delta$ will be quantized to the same z_i for any small δ. This can be interpreted as a watermark of Quantization Index Modulation [5]. For the i-th dimension of S, the value of w_i will be

$$w_i = \begin{cases} (2n+\frac{1}{2})q - x_i & \text{if } s_i = 1 \\ (2n-\frac{1}{2})q - x_i & \text{if } s_i = 0 \end{cases}$$

where n= .., -1, 0, 1, 2, ... is chosen such that $-q < w_i < q$. The value of n is discarded, but the values of w are released as helper data.

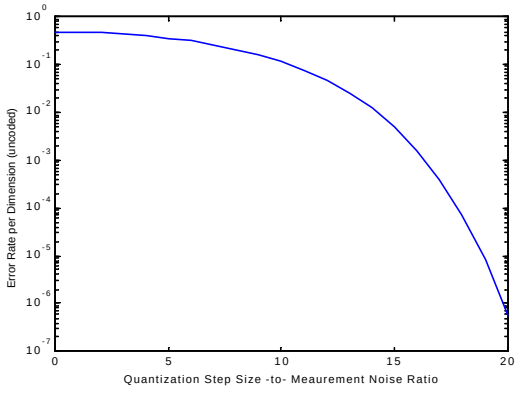

Figure 3. Uncoded error probability per dimension as a function of q/σ_n

We analyse the case of a single specific dimension, where a secret message s = {-1,+1} is verified. The contraction range δ equals $q/2$. The probability that an honest couple Peggy-Victor makes an error in one dimension equals

$$P_e = 2Q\left(\frac{q}{2s_n}\right) - 2Q\left(\frac{3q}{2s_n}\right) + 2Q\left(\frac{5q}{2s_n}\right) - \ldots$$

where Q(x) is the integral over the Guassian pdf with unity variance. In a practical situation, if one can apply error correction decoding to further reduce the error rate, compared to Figure 3.

The next analysis will quantify ε by calculating the leakage of information for our assumptions of the statistical behavior of the input signals X and W, where the statistics of W are determined by those of X and S. The signals in all dimensions are calculated in an identical manner, so we omit the index i. We observe that for $s_i = 1$ $w = (2n+1/2)q - x$, so

$$f_W(w|s_1=1) = \begin{cases} 0 & \text{for } |w| > q \\ \sum_{n=-\infty}^{\infty} \frac{1}{\sqrt{2p}\, s_x} \exp\left(-\frac{((2n+1/2)q-w)^2}{2s_x^2}\right) & \text{for } |w| < q \end{cases}$$

Figure 4 plots $q * f(w/q)$ as a function of w/q. The solid lines depict $f_W(w|s=0)$ and the crosses depict $f_W(w|s=1)$. Information leaks whenever $f_W(w|s=1) \neq f_W(w|s=1)$. The symmetry properties $f_W(w|s) = f_W(q- w|s)$ and $f_W(w|s=1) = f_W(-w|s=0)$ apply. $f_W(w|s=1)$ has a maximum for $w = q/2$, which corresponds to highly likely values of x near $x = 0$. The unconditional probability density of W follows from $f_W(w) = f_W(w|s=1)\ P(s=1) + f_W(w|s=0)\ P(s=0)+$. Despite the suggestion by Figure 4, it is neither true that that $f_W(w|s=1) = 1 - f_W(-w|s=1)$ nor that $f_W(w)$ is constant.

Using Bayes rule, the a posteriori probability p_{w1} on $s = 1$ can be expressed as

$$p_{w1} = P(s=1|W=w) = \frac{f_W(w|s=1)}{f(w)} P(s=1)$$

Similarly, we define p_{w0}. Then, the mutual information $I(W;S)$ follows from:

$$I(W;S) = H(S) - \int_{-q}^{q} H(S|W=w)\, f_W(w) dw$$

Here $H(S)$ stands for the information theoretic entropy of a discrete random variable S, defined as $H(S) = -\Sigma_i P(S=i) \log_2 P(S=i)$. Since S takes the value 0 or 1 with probability 0.5, $H(S) = 1$ bit. Thus,

$$I(W;S) = H(S) + \int_{-q}^{q} \{p_{w1} \log p_{w1} + p_{w0} \log(1-p_{w0})\} f_W(w) dw$$

$$I(W;S) = 1 + \frac{1}{2}\int_{-q}^{q} f_W(w|s=1) \log \frac{f_W(w|s=1)}{2 f_W(w)} dw + \frac{1}{2}\int_{-q}^{q} \{f_W(w|s=0)\} \log \left\{\frac{f_W(w|s=0)}{2 f_W(w)}\right\} dw$$

Expanding the logarithm into separate terms, i.e., applying the rule log(a/b) = log a - log b), we get

$$I(W;S) = 1 + \frac{1}{2}\int_{-q}^{q} f_W(w \mid s=1) \log\, f_W(w \mid s=1) dw + \frac{1}{2}\int_{-q}^{q} \{f_W(w \mid s=0)\} \log\{f_W(w \mid s=0)\} dw$$
$$- \int_{-q}^{q} f_W(w) \log 2\, f_W(w) dw$$

Or simply,

$$I(W;S) = \int_{-q}^{q} f_W(w \mid s=1) \log\, f_W(w \mid s=1) dw - \int_{-q}^{q} f_W(w) \log\, f_W(w) dw$$

Figure 5 shows that quantization values as crude as $q / \sigma_n = 1$ are sufficient to ensure small leakage ($\varepsilon << 10^{-5}$). Crude quantization steps are favorable as these allow reliable detection (i.e., a large contracting range δ).

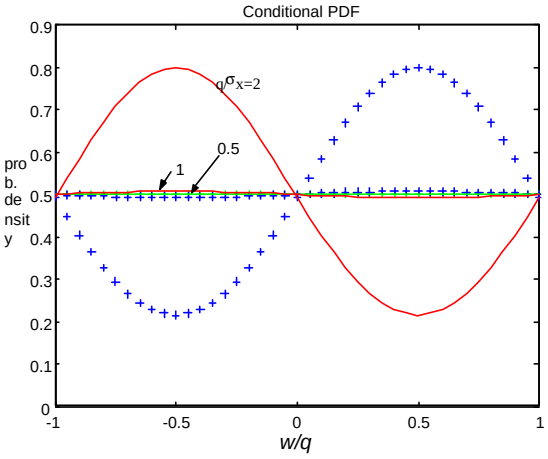

Figure 4: Probability density of *W*, for various *q*: q/σ_x = 0.5, 1 and 2.

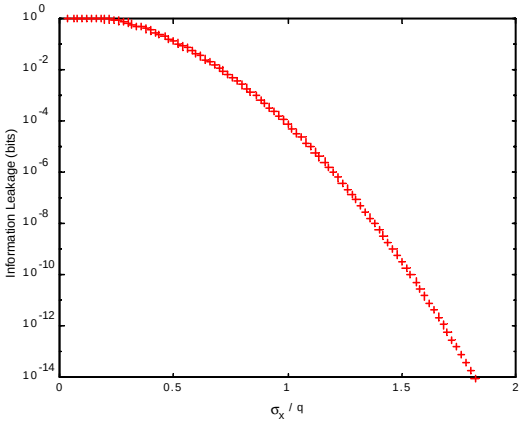

Figure 5: Mutual Information I(*W*;*S*) as a function of signal-to-noise ratio σ_x^2/σ_n^2 for various values of q/σ_n

Conclusion

This paper introduced the concepts of a *versatile* secure biometric authentication and key establishment, and δ-*contracting* and ε-*revealing* function to preprocess measurement data. These shielding properties can be an essential step towards a design of a public biometric authentication and key establishment infrastructure. That is, the authentication 'challenge' and 'reference response' can be released by a public data base for public use, without the risk of revealing what the actual biometric parameters of a particular citizen are.

The δ-*contracting* and ε-*revealing* function prevents a number of attacks, in particular threats from misuse of reference data (user templates) by dishonest verifiers.

References

1. R. Papu, B. Recht, J. Taylor and N. Gerhenfeld, "Physical one-way functions", Science, Vol. 297, 20 Sept. 2002, pp. 2026-2030.
2. S. Pankanti, R.M. Bolle and A. Jain, Biometrics - The future of Identification, IEEE Computer, Volume 33, No. 2, pp. 46-49, February 2002.
3. D. Polemi, "Review and evaluation of Biometric Techniques for Identification and Authentication - Final Report", 1997, http://www.cordis.lu/infosec/src/stud5fr.htm
4. Bruce Schneier, Applied Cryptography, J. Wiley, New York, 1993.
5. B. Chen and G.W. Wornell, “Digital Watermarking and Information embedding using dither modulation”, IEEE Workshop on Multimedia Signal Processing, Redondo Beach, CA, 1998. (extended in a paper for IEEE Tr. on Inf. Theory, 2001, Vol. 47(4), pp. 1423-1443)
6. A. Juels and M. Wattenberg. A Fuzzy Commitment Scheme. In G. Tsudik, ed., Sixth ACM Conference on Computer and Communications Security, pages 28-36, ACM Press, 1999.
7. Ari Juels en Madhu Sudan, "A fuzzy Vault scheme", ICIT Proceedings Int. Symp. on Inf. Theory, p. 408, 30 Juni-5 July 2002, Lausanne.
8. D. Denteneer, J.P. Linnartz, P. Tuyls, E. Verbitskiy,”Reliable (robust) biometric Authentication with privacy protection”, acc. for The IEEE Benelux Symp. on Inf. Theory, Veldhoven, The Netherlands, 2003.
9. G.I. Davida, Y. Frankel, and B.J. Matt. On enabling secure applications through off-line biometric identification. In IEEE Symposium on Privacy and Security, 1998.
10. G. I. Davida, Y. Frankel, and B.J. Matt. On the relation of error-correction and cryptography to an offline biometric based identification scheme. In proceedings WCC99, Workshop on Coding and Cryptography, 1999.
11 C. Soutar: Biometric Encryption for secure key generation, January 1998. Presentation at the 1998 RSA Data Security Conference
12. C. Soutar and G.J. Tomko: Secure private key generation using a fingerprint. In CardTech/SecurTech Conference Proceedings, Vol 1, pages 245-252, May 1996.
13. R. Chandrasekaran. Brave new World: ID systems using the human body are here, but privacy issues persist. Washington Post, 30 March 1997, p. HO-1
14 UK patent application No. GB 2348 584 A, 4 Oct. 2000
15 A.J. Menezes, P.C. van Oorschot and S.A. Vanstone, “Handbook of Applied Cryptopgraphy”, CRC Press, New York, 96.