Proc. 3^{rd} IEEE Benelux Signal Processing Symposium (SPS-2002), Leuven, Belgium, March 21–22, 2002

SENSING PRESSURE FOR AUTHENTICATION

Neil Henderson, Neil White

University of Southampton, Department of Electronics and Computer Science
Highfield, Southampton, SO17 1BJ, UK
n.henderson@ecs.soton.ac.uk

Raymond Veldhuis, Pieter Hartel, Kees Slump

University of Twente
P.O. Box 217, 7500AE Enschede, The Netherlands
r.n.j.veldhuis@el.utwente.nl

ABSTRACT

The use of signals resulting from tapping a rhythm on a pressure sensor is explored for authentication. The features used for authentication can be divided into rhythm and waveform features. This paper studies the use of waveform features. A verification scheme based on prototype waveforms is presented. The scheme is tested on experimental data. Based on waveform-only information, an Equal Error Rate of 7.7% is achieved with an indication of further room for improvement. Suggestions for data collection and training are presented.

1. INTRODUCTION

Who is knocking on your door? You can often tell by just listening. In the early days of telegraphy, operators would identify each other by recognizing the way in which they tapped out messages [1]. This simple idea is worked out in [3, 4] where it is described how newly developed polymer thick-film pressure sensors can be used for authentication based on a tapped rhythm or provide feedback on the way an object is held.

The Piezo-electric and Piezo-resistive sensors are screen printed on a thin layer of Mylar, which is then bonded onto an object. The sensors are robust, thin (70 microns) and inexpensive (a few euro cents in mass production). The sensors can easily be integrated into objects of various shapes, including smart cards [3] and hand-held devices such as PDAs and tools.

In order to demonstrate the potential of polymer thick-film pressure sensors for authentication purposes, a small verification experiment is described in [3]. In this experiment sequences of pressure pulses were generated by 34 subjects tapping on a piezo-electric sensor bonded on a smart card. The features (pulse height and duration and the duration of the first inter-pulse interval) and the verification scheme used in the experiment are similar to those used for verification based on key-stroke dynamics [5]. These features are simple to derive from the pulse waveform, which is an advantage for the intended application in a smart card processor. The experiment described in [3] showed that, even with this small feature set, the Equal Error Rate for a verifier can be as low as 2.3%. It is expected that these results can be improved when a larger feature set, based on sensor-signal characteristics, is used.

In this paper we study the possibilities of a such more advanced and larger feature set for verification. Our study is based on the same experimental data that were used in [3]. We concentrate on the waveform properties of the pulses which result from tapping the sensor. The use of rhythm features will be the topic of a later paper. The shape of the pulses seem to be characteristic for the person tapping the sensor. Therefore, we want the waveform features to represent the details of the pulse shapes. In Section 2 we present more considerations on the feature set. The verification scheme is presented in Section 3. It is based on the similarity to one or more prototype waveforms. Deviations to the prototype waveforms are modelled statistically. Section 4 describes how the verification scheme was evaluated. For this purpose, the data set was divided into a training and a test set. The training set was used to determine the parameters of the verification scheme. The evaluation was done on the test set. The results are presented as Receiver Operating Curves and plots of the false rejection and acceptance rates. We discuss the results of the evaluation in Section 5 and give some recommendations for the further development of the verifier. Finally, Section 6 gives conclusions.

2. CONSIDERATIONS ON THE FEATURE SET

As has been mentioned earlier, we want the waveform features to represent the details of the pulse shapes, because these details seem to be characteristic for the person tapping the sensor. The importance of shape details can be illustrated as follows. The data used in [3] consist of sequences obtained from 34 subjects who were asked to repeat the same rhythm a number of times. The signals were sampled at a rate of 2 kHz. Four typical examples are shown in Figure 1. The left panels show the first (top) and last (bottom) sequence of Subject 1. The right panels show the first (top) and last bottom) sequence of Subject 15. From this figure one can observe that both subjects produce different waveforms. Intra-subject variations can also be observed: Subject 1 does not seem to vary the waveform of the pulses within one sequence, but the pulses of the last sequence differ from those of the first. Subject 2 seems to vary the pulse shape systematically within one sequence. We assume that this subject produces a different pulse for accented taps.

Shape details can be captured by comparing pulses with prototypes. A pulse sufficiently close to a prototype would then lead to authentication. It is still to be determined what is meant by 'sufficiently close'. Because subjects seem to vary their pulse shapes in time and within a sequence, the use of 1 prototype per user may lead to problems. Therefore, we allow 2 prototypes per user. It is shown in Section 4 that this indeed increases performance.

3. VERIFICATION SCHEME

Each pulse may vary slightly around its prototype. This variation is modelled as a zero-mean multivariate Gaussian random process, with a user-specific covariance matrix $\mathbf{C}$. Let us denote a tapping

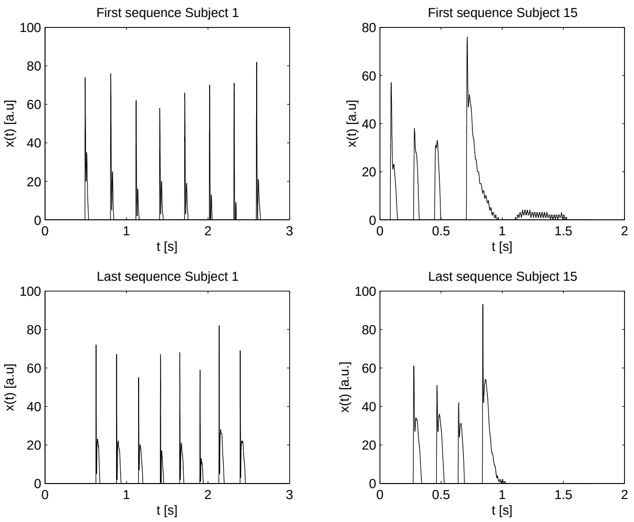

Figure 1: *Typical waveforms. Left panels: First and last sequence of Subject 1. Right panels: First and last sequence of Subject 15*

sequence, arranged in a column vector of length m, by $\mathbf{x}$ and the corresponding prototype vector by $\mathbf{p}$. The probability density of $\mathbf{x}$ is then given by

$$P(\mathbf{x}) = \frac{1}{\sqrt[m]{2\pi|\mathbf{C}|}}\,\mathrm{e}^{-\frac{1}{2}(\mathbf{x}-\mathbf{p})^{\mathrm{T}}\mathbf{C}^{-1}(\mathbf{x}-\mathbf{p})}. \tag{1}$$

The superscript $^{\mathrm{T}}$ denotes matrix or vector transposition. It can be shown, under the assumption that the pulses of imposters have a uniform probability on the outcome space, that the optimal verifier will accept a pulse $\mathbf{y}$ when

$$P(\mathbf{y}) > P_{\mathrm{T}}, \tag{2}$$

in which the threshold probability P_{T} still needs to be specified. The covariance matrix $\mathbf{C}$ is needed to determine this region. In fact, it has to be estimated from the data. For each subject we have available 16 sequences, containing about 5 pulses on average. This means that we have on average about 80 pulses per subject to estimate $\mathbf{p}$ and $\mathbf{C}$. The maximum pulse duration is about 0.25 s, corresponding to 500 samples. This means that $\mathbf{C}$ would be a 500×500 matrix, which cannot be estimated reliably from 80 pulses on average and which would, anyhow, require too much storage in a practical system.

Fortunately, we can reduce the dimension of $\mathbf{x}-\mathbf{p}$ to a more practical proportion, and at the same time obtain a very simple covariance matrix. It so happens that the available realizations of $\mathbf{x}-\mathbf{p}$ are practically in a low-dimensional subspace of $\mathbb{R}^m$. This can be seen as follows. First, we arrange all (say n, $n < m$) sequences $\mathbf{x}-\mathbf{p}$ from one subject as columns in an $m \times n$ data matrix $\mathbf{X}$. We apply singular value decomposition [2] to $\mathbf{X}$. I.e. we write

$$\mathbf{X} = \mathbf{U}\mathbf{S}\mathbf{V}^{\mathrm{T}}. \tag{3}$$

The $m \times m$ matrix $\mathbf{U}$ is orthonormal and spans up the column space of $\mathbf{X}$. The $n \times n$ matrix $\mathbf{V}$ is orthonormal and spans up the row space of $\mathbf{X}$. For the $m \times n$ matrix $\mathbf{S}$ we have

$$S_{ij} = \begin{cases} \sigma_i, & 1 \le i = j \le n \\ 0, & \text{otherwise}, \end{cases} \tag{4}$$

with $\sigma_1 \ge \sigma_2 \ge \ldots \ge \sigma_n \ge 0$ the so-called singular values of $\mathbf{X}$. We can approximate $\mathbf{X}$ by a matrix of rank n_{dim} given by

$$\tilde{\mathbf{X}} = \mathbf{U}\tilde{\mathbf{S}}\mathbf{V}^{\mathrm{T}}, \tag{5}$$

with

$$\tilde{\sigma}_i = \begin{cases} \sigma_i, & 1 \le i \le n_{\mathrm{dim}} \\ 0, & n_{\mathrm{dim}}+1 \le i \le n. \end{cases} \tag{6}$$

The square approximation error is then given by

$$\|\tilde{\mathbf{X}}-\mathbf{X}\|_{\mathrm{F}}^2 = \sum_{i=1}^{m}\sum_{j=1}^{n}(\tilde{X}_{ij}-X_{ij})^2 = \sum_{i=n_{\mathrm{dim}}+1}^{n}\sigma_i^2. \tag{7}$$

With $n_{\mathrm{dim}} = 5$ we have a relative square approximation error of no more than 1–2% for the available data. This means that with a relative square error of 1–2%, all $\mathbf{x}-\mathbf{p}$ are in a 5-dimensional subspace of $\mathbb{R}^m$, spanned up by the first $n_{\mathrm{dim}} = 5$ columns of $\mathbf{U}$, which are also called the first n_{dim} principal components of $\mathbf{X}$. Instead of computing the covariance matrix of $\mathbf{x}-\mathbf{p}$ we consider the projection of $\mathbf{x}-\mathbf{p}$ on the subspace of $\mathbb{R}^m$, spanned up by the first n_{dim} columns of $\mathbf{U}$. Let the matrix consisting of the first n_{dim} column of $\mathbf{U}$ be denoted by $\mathbf{U}_{\mathrm{r}}$. The coefficients of the projection on the subspace are then given by $\mathbf{U}_{\mathrm{r}}^{\mathrm{T}}(\mathbf{x}-\mathbf{p})$. It can be shown that the coefficients of the vector

$$\mathbf{x}' = \begin{pmatrix} \frac{\sigma_1}{\sqrt{n-1}} & & \\ & \ddots & \\ & & \frac{\sigma_{n_{\mathrm{dim}}}}{\sqrt{n-1}} \end{pmatrix}^{-1} \mathbf{U}_{\mathrm{r}}^{\mathrm{T}}(\mathbf{x}-\mathbf{p}) \tag{8}$$

$$\stackrel{\mathrm{def}}{=} \mathbf{W}(\mathbf{x}-\mathbf{p}) \tag{9}$$

are statistically independent and have a zero-mean, unit-variance Gaussian distribution. The $n_{\mathrm{dim}} \times m$ matrix $\mathbf{W}$ in (9) is called the projection matrix.

If we want to verify whether a sequence $\mathbf{y}$ has been tapped by a person with pulse-prototype vector $\mathbf{p}$ and projection matrix $\mathbf{W}$, we have to check if the probability of

$$\mathbf{y}' = \mathbf{W}(\mathbf{y}-\mathbf{p}) \tag{10}$$

is above a certain threshold. This is a similar condition as the one for $\mathbf{y}$ in (2). It can be rephrased as follows. Let us define the distance from a pulse to a prototype by

$$D(\mathbf{y},\mathbf{p}) \stackrel{\mathrm{def}}{=} \|\mathbf{y}'\|_2^2 = \sum_{i=1}^{n_{\mathrm{dim}}} |y_i'|^2. \tag{11}$$

Under the assumption that the $\mathbf{y}'$ of imposters have a uniform probability on the outcome space, the optimal verifier will accept a pulse when

$$D(\mathbf{y},\mathbf{p}) \le T \tag{12}$$

and otherwise it will reject it. The choice of the threshold T in (12) depends on the required false-acceptance probability or the imposter-detection probability.

So far, have derived a verifier for single pulses. We will now extend this verifier to sequences of pulses and 2 prototypes. Let us denote the 2 prototype vectors and corresponding projection matrices by $\mathbf{p}^{\mathrm{I}}$ and $\mathbf{p}^{\mathrm{II}}$, and $\mathbf{W}^{\mathrm{I}}$ and $\mathbf{W}^{\mathrm{II}}$, respectively. Let the sequence contain q pulses $\mathbf{y}_1, \ldots, \mathbf{y}_q$. The extended verifier will accept this sequence when

$$D_s(\{\mathbf{y}_1, \ldots, \mathbf{y}_q\}, \{\mathbf{p}^{\mathrm{I}}, \mathbf{p}^{\mathrm{II}}\}) \stackrel{\text{def}}{=} \frac{1}{q}\sum_{i=1}^{q} \min(D(\mathbf{y}, \mathbf{p}^{\mathrm{I}}), D(\mathbf{y}, \mathbf{p}^{\mathrm{II}}) \leq T, \tag{13}$$

with the distance $D(\mathbf{y}, \mathbf{p})$ defined in (11), and otherwise it will reject it. It can be shown that choosing the minimum distance to a prototype is optimal when the probability of occurrence of the prototypes is unknown. Using the mean distance to the best-matching prototypes makes the threshold independent of q. The choice for the mean is optimal when the pulses in the sequence are statistically independent.

4. EXPERIMENTAL EVALUATION

For the evaluation we have used the data of 33 subjects that were also used in [3]. For each subject there are 16 recordings of the same self-chosen rhythmic sequence of pulses. All sequences of one subject were recorded in the same session, which lasted about 5 minutes. The length of a sequence is typically 3 to 4 seconds. A sequence may contain 2 to 8 pulses. Eight sequences of each subject were put in a training set. The remaining sequences were taken as the test set.

The dimension of the subspaces n_{dim} was set to 5. For each subject initially 2 prototypes $\mathbf{p}^{\mathrm{I}}$ and $\mathbf{p}^{\mathrm{II}}$ and 2 projection matrices $\mathbf{W}^{\mathrm{I}}$ and $\mathbf{W}^{\mathrm{II}}$ were derived from the test set. The prototypes were selected by a K-means (or LBG) algorithm [6] from the subject's data matrix $\mathbf{X}$. The initial prototypes were chosen as the columns of $\mathbf{X}$ with maximum Euclidian distance. The data matrix was split into 2 matrices $\mathbf{X}^{\mathrm{I}}$ and $\mathbf{X}^{\mathrm{II}}$, containing the pulse vectors that closest $\mathbf{p}^{\mathrm{I}}$ and $\mathbf{p}^{\mathrm{II}}$, respectively. If, for a subject, less than $3n_{\text{dim}}$ pulses were assigned to a prototype, the number of prototypes was reduced to 1, which was taken as the average pulse vector. This was done in order to avoid overtraining with a limited set of training data. In this case, the acceptance criterion (13) becomes

$$D_s(\{\mathbf{y}_1, \ldots, \mathbf{y}_q\}, \mathbf{p}) \stackrel{\text{def}}{=} \frac{1}{q}\sum_{i=1}^{q} D(\mathbf{y}, \mathbf{p}) \leq T. \tag{14}$$

For 11 of the 33 subjects, the number of prototypes was reduced to 1. This happened mostly when the number of pulses in a sequence was 4 or less.

For each of the sequences in the training set, the distances D_s (13) or (14) to all (sets of) prototype vectors of all 33 subjects were computed. The threshold T was increased in small steps from 0 to a maximum of 100. For all the values of T, the false-rejection probabilities α (the fraction of sequences that were falsely rejected) and the detection probabilities p_{d} (the fraction of 'imposter' sequences that were rejected) were estimated. This was done for 2 variants of the verifier: a verifier (A) that was based on either 2 or 1 prototype waveform, such as described in Section 3, and a verifier (B) that only uses 1 waveform prototype. In addition, in order to compare our results with the approach of [3] we have computed α and p_{d} for a verifier (C) based on pulse duration and height. The first inter-pulse interval that was also used in [3] is a rhythm feature and therefore not included. The distance used for verifier (C) was the Mahalanobis distance, which is very similar to the distance used in this paper. In [3] only the first pulse of a sequence is used for verification. We have tried both the average of all pulses as well as the first pulse of a sequence for this verifier. The results were very similar and we decided to present only the results based on the average of all pulses of a sequence. The verifier (A) was also tested on a subset of the test data, containing only sequences of subjects that were assigned 2 prototypes. This was done on order to get an indication of the performance when the number of prototype is always 2.

Figure 2 shows the estimated receiver operating curves (p_{d} as function of α) of all tested verifiers. Figure 3 shows the estimated false-rejection probability α and the estimated false-acceptance probability $1 - p_{\text{d}}$ as functions of the threshold T.

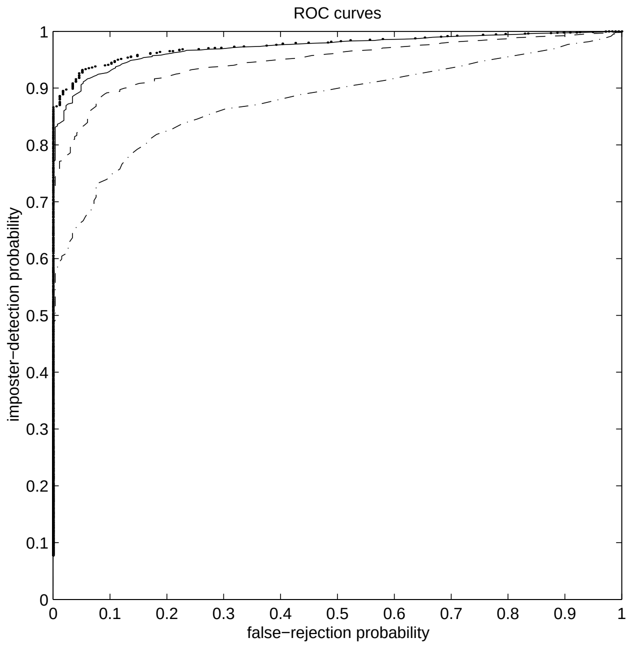

Figure 2: *Estimated receiver operating curves for: a verifier (A) based on 2 or 1 waveform prototypes (solid line), a verifier (B) based on 1 waveform prototype (dashed line), a verifier (C) based on duration and height of the pulses (dash-dot line), and verifier (A) operating on the test data of the subjects that were assigned 2 prototypes (dots).*

The Equal Error Rate (the value of α and $1 - p_{\text{d}}$ at which $\alpha = 1 - p_{\text{d}}$) is often taken as a measure of performance. For the verifier based on 2 waveform prototypes we found an Equal Error Rate of 7.7%. When applied to the subset of the test data, containing only sequences of subjects that were assigned 2 prototypes the Equal Error Rate decreased to 6.5%. For the verifier based on 1 waveform prototype we found an Equal Error Rate of 10.7%. Finally, for the verifier based on pulse duration and height we found an Equal Error Rate of 18.2%.

5. DISCUSSION

Both Figures 2 and 3 show that a more advanced, but clearly more complex, verifier based on pulse shape details is superior to a verifier only based on pulse duration and height. The figures also show that allowing 2 waveform prototypes per subject instead of 1 gives an additional improvement.

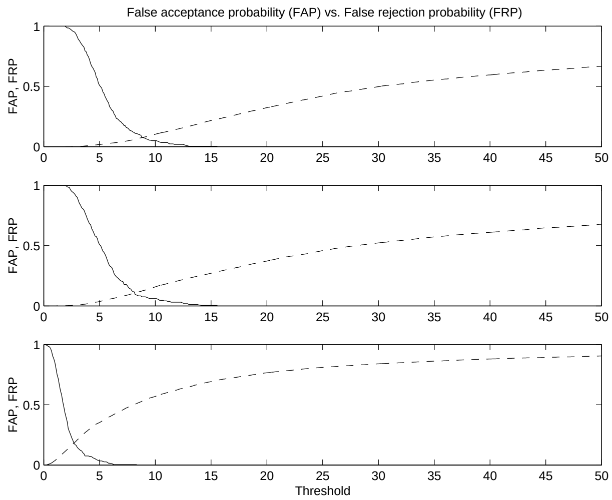

Figure 3: *Estimated false rejection (solid lines) and false acceptance probabilities (dashed lines). Top panel: Verifier based on 2 or 1 waveform prototypes. Middle panel: Verifier based on 1 waveform prototype. Bottom panel: Verifier based on pulse duration and height.*

The estimated performance increased further when the test set was restricted to the sequences from subjects that were assigned 2 prototypes. Those subjects usually produced 5 or more pulses per sequence. This indicates that it is worth while to have a minimum total number of pulses in the training set large enough to reliably estimate 2 (or more) prototypes. Now, only 1 prototype vector was assigned to 11 of the 33 subjects, including Subject 15 whose sequences were shown in Figure 1. This subject's systematic use of two clearly distinct waveforms indicates that 2 prototypes would have improved his verification results.

In [3] the verifier based on pulse duration and height was evaluated with one additional rhythm feature: the duration of the first inter-pulse interval. With the the same Mahalanobis distance as was used in this paper, the Equal Error Rate improves substantially to 3.4%. This implies that we can also expect additional improvements when rhythm features are incorporated. How much this improvement will be is still unclear.

One must be careful in generalizing the results to a practical verification situation. One problem, for example, is that all sequences have been recorded in one session. It was found that even in the course of this single short session subjects changed their pulse shape. It may very well be that pulse shapes measured after a few days differ even more.

Another problem is that the number of subjects and the number of pulses that were recorded is on the small side. More subjects are needed to get a better indication of the probability of imposter sequences in a practical application. It has already been mentioned that more pulses per sequence are needed in order to be able to always use 2 prototype waveforms (or more) per subject. More pulses per sequence are also needed in order to be able to use more rhythm features than only the first inter-pulse interval.

6. CONCLUSION

An authentication method based on tapping sequences has been presented and evaluated. A tapping sequence can have waveform and rhythm features. Only waveform features have been taken into account. The method is based on the distance of pulses to 1 or 2 prototype waveforms. It achieves an Equal Error Rate of 7.7%. It has a better performance than a simpler method, only based on pulse duration and height, but at the price of a higher computational complexity. There is further room for improvement, if the minimum number of pulses per sequence is such that always 2 prototype waveforms can be used. Further experiments with training and test data that are recorded under more realistic conditions are needed. For example, it has to be investigated whether and to what extent the performance drops when training and test data are recorded on different days. The expected positive effects on the performance of adding rhythm features will be studied in a later paper.

7. REFERENCES

[1] W. L. Bryan and N. Harter. Studies in the physiology and the psychology of the telegraphic operator. *Psychological review*, 4:27–53, 1897.

[2] G.H. Golub and C.F. van Loan. *Matrix Computations*. North Oxford Academic Publishing, Oxford, 1983.

[3] N. J. Henderson and P. H. Hartel. Pressure sequence - a novel method of protecting smart cards. *Smart Card Research and Advanced Applications* pages 241–256, Bristol, UK, Sep 2000. Kluwer Academic Publishers, Boston/Dordrecht/London. ISBN 0-7923-7953-5.

[4] N. J. Henderson, N. White, and P. H. Hartel. iButton enrolment and verification times for the pressure sequence smartcard biometric. In I. Attali and Th. Jensen, editors, *2nd Conf. Smart card research (eSmart)*, page to appear, Cannes, France, Sep 2001.

[5] Joyce and Gupta. Identity autentication based on keystrokes dynamics. *Communications of the ACM*, 33(3):168–176, 1990.

[6] Y. Linde and A. Buzo and R.M. Gray. An Algorithm for Vector Quantizer Design. *IEEE Transactions on Commnication*, 28(1):84–95, 1980.