Template Protection for Biometric Gait Data

Claudia Nickel[1], Xuebing Zhou[2], Christoph Busch[1]

[1] Hochschule Darmstadt - CASED, [2] Fraunhofer IGD
c.nickel@fbi.h-da.de, xuebing.zhou@igd.fraunhofer.de, christoph.busch@h-da.de

Abstract: Biometric gait recognition is a well suited method for authentication on mobile devices as it is unobtrusive and concurrent. Hence, in contrast to PIN authentication it is no extra-effort for the user. The characteristic gait of a subject can be recorded using accelerometers which are nowadays already contained in many mobile devices. From this data biometric feature vectors can be extracted and stored as reference data on the device. Only if the user is not recognized by his walk an active authentication via PIN is necessary.
As the number of attacks on mobile devices increases it cannot be assumed that the data stored on the device is under constant control of the subject. Therefore, template protection techniques should be applied to secure biometric data. As biometric gait recognition is a new field of research no specific template protection methods have been developed so far. This paper describes a new method for securing biometric gait features based on histograms and using the earth mover's distance for comparison. The method is tested with gait data of 48 subjects recorded using a mobile phone and the results are compared to the ones obtained without template protection.

1 Introduction

A survey by Furnell and Clarke [CF05] shows that data in mobile devices is often insufficiently protected. When turning on the phone, entering a PIN is only necessary in 66% of the cases and after a stand-by phase this is only required at 18% of the devices (either because the phone does not offer this setting or because the owner did not select it). This implies that in most cases everybody who has physical access to the device can directly access all stored information. As the proportion of sensitive information (contacts, emails, ...) saved in mobile devices grows, this is becoming critical. 30% of the respondents of the survey consider PIN authentication to be inconvenient. But most mobile devices do not offer a suitable alternative. Accelerometer-based gait recognition is such an alternative. In contrast to PIN authentication no active input of the user is necessary. Most smartphones do contain accelerometers for games or changing the orientation of the display. These accelerometers can directly be used to record the specific gait of a subject. This means that no special hardware is needed to collect the gait data which is a great advantage to other biometric modalities like fingerprint. When a subject is walking with his phone he is directly authenticated based on his gait. Recently, Gafurov et al. [GS09, GHS06] and Ailisto et al. [ALM$^+$05] have suggested methods for extracting feature vectors from accelerometer data. Using data collected with dedicated accelerometers (i.e. not accelerometers contained in mobile devices) they report equal error rates up to 6.4%.

While biometric identification and authentication provides considerable convenience and also some security benefits over token- or password-based methods, other security and privacy concerns unique to biometrics must be taken into account. These include identity theft, cross-matching, and the exposure, often irrevocable, of sensitive private information, as well as traceability of individuals.

This has stimulated research on the protection of stored biometric data in recent years, primarily focusing on preventing information leakage. Template protection techniques, also referred to as biometric encryption, untraceable biometrics, cancelable or revocable biometrics, have been developed. These convert biometric data elements into multiple (ideally) uncorrelated references, from which it is infeasible to retrieve the original information and in some cases have already been integrated into existing systems [gen, pri]. [ZWBK09] gives an overview and security analysis of existing template protection techniques, which have been already developed for different modalities like finger [UJ04, RCCB07], face [VKjS$^+$06, Zho07], iris [WHNB08] and vision based gait recognition [ATIS09]. Template protection is a generalized and efficient method to preserve privacy and to enhance security of biometric data by limiting the exposure of template data which cannot be revoked. They exhibit the following key properties:

One-Way and Robustness A secure reference can be computed efficiently from a biometric datum (template) while it is either computationally hard or impossible to deduce the template from such a reference. The derivative references can be compared to a biometric datum under similarity metrics for the underlying biometric template. This allows the successful comparison of measurements exhibiting small variations or measurement errors to a derivative reference.

Diversity and Randomness Template protection can create numerous secure references from one biometric feature with the references independent on each other, i.e. knowledge of one reference does not yield information on other references derived from the same template. This eliminates the problem of cross-matching and tracebility.

The resulting various references are also called pseudo identifiers [BBGK08]. Different methods to protect the biometric data exist, which can be classified into four categories: cancelable biometrics, biometric salting, fuzzy encryption and biometric hardening passwords.

Although the research on accelerometer based biometric gait recognition shows that it offers a promising way to provide a more convenient method for authentication on mobile devices, no research has been done so far in the area of template protection for biometric gait data collected using accelerometers. One reason for this might be, that biometric data stored on the mobile device seems to be under control of the subject (similar to systems using on-card biometric comparison, see [iso]). Nevertheless several attacks on mobile devices have been reported [HJO08, Win] which make clear that data stored on the mobile devices should be protected.

The paper is structured as follows. The next section gives an overview over the collected gait data and the extracted feature vectors. Section 3 describes the developed template protection method and section 4 explains the test and states the obtained results. A summary and conclusions are given in section 5.

2 Biometric Gait Data

As our focus on the application of the proposed technique is the protection of biometric gait data collected with and stored on mobile devices, a database containing suitable test data had to be created. Our database consists of data of 48 subjects collected using a standard mobile device (T-Mobile G1) which contains accelerometers for measuring acceleration in three directions as indicated in figure 1. The phone was carried in a bag which was attached to the belt of the walking subject at the right hip (see figure 1). All subjects had to walk about 37 meters down the hall, wait for a short time, turn around, wait again and walk back. Subjects were told to walk at a normal speed, which results in different walking speeds for different subjects depending on what is assumed to be normal. An example of the accelerometer data recorded during one of these sessions is given in figure 2.

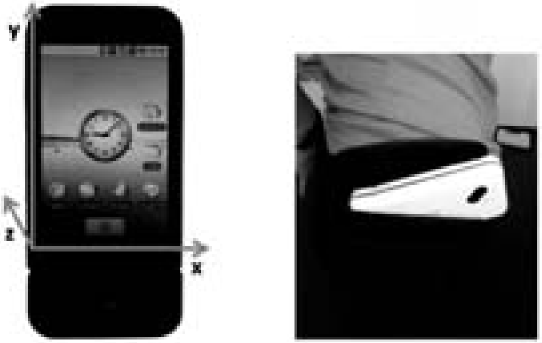

Figure 1: Phone attached to subject and the three axes in which acceleration is measured.

From this data, the parts where the subject is walking (called *walk* and indicated by the dashed lines in figure 2) have been extracted. As two sets of data have been collected from each subject at two different days, four walks of each subject are available for tests. The first walk is used to compute the reference data, the further three walks provide the probes. The movements of a subject approximately repeat every two steps (see figure 3), which suggests the extraction of these *cycles* and determination of a cycle which is typical for a specific subject and hence can be used as feature vector. As most of the gait recognition methods proposed in literature are based on a cycle extraction method (e.g. [GS09, GHS06, ALM$^+$05]), our proposed template protection method should be applicable to these features (cycles). Therefore, to get appropriate test data, cycles have been manually extracted from the collected data. The most suitable cycles of each subject have been selected by determining the reference cycle (from the first walk) and one probe cycle of each of the other walks in such a way that sum of the distance from the reference to the probes is minimal. The data is interpolated to a fixed sampling rate (100 Hz) and

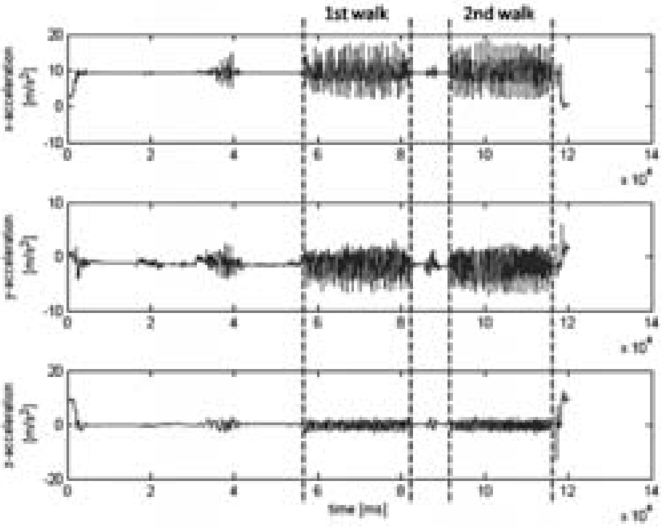

Figure 2: Recorded accelerometer data.

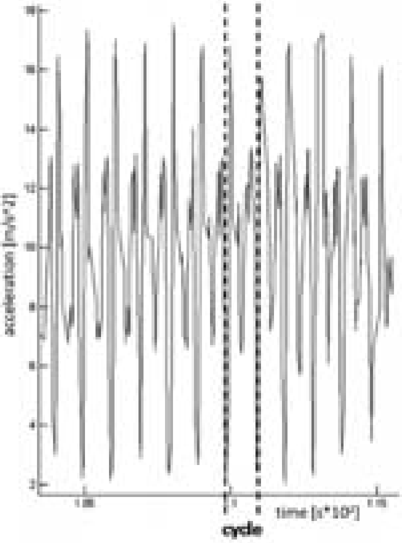

Figure 3: Example of gait data. The cyclic repetition can be clearly seen.

centered around zero. After these preprocessing steps our data base consisted of 192 cycles (feature vectors) of length between 62 and 138 samples.

3 Horizontal Projection

Biometric template protection techniques are used to create pseudo identifiers from the biometric template. This pseudo identifier should only reveal limited information about the original biometric characteristic and in addition the generation of different pseudo identifiers from the same biometric template should be possible. To transform the template in a way such that no private information can be obtained, one-way functions can be used. We propose using a horizontal projection of the values in the feature vector to the y-axis as one-way function which is the same as calculating the histogram of the accelerometer data. Figures 4 and 5 show examplary four cycles of two different subjects and the obtained histograms. Crosses on the cycles show the accelerometer values contained in the feature vector. Only these values contribute to the histogram. The direction of projection is indicated at the upper left cycle.

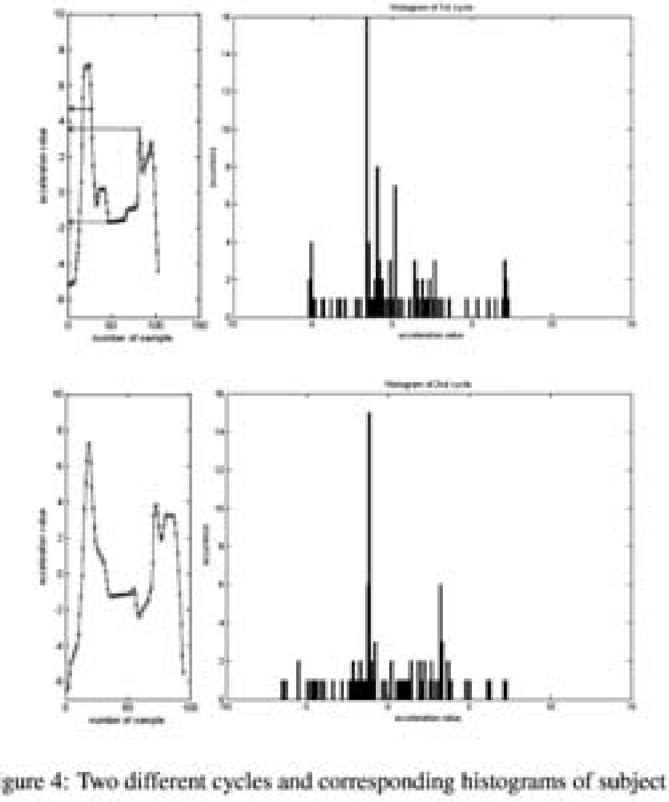

Figure 4: Two different cycles and corresponding histograms of subject 1.

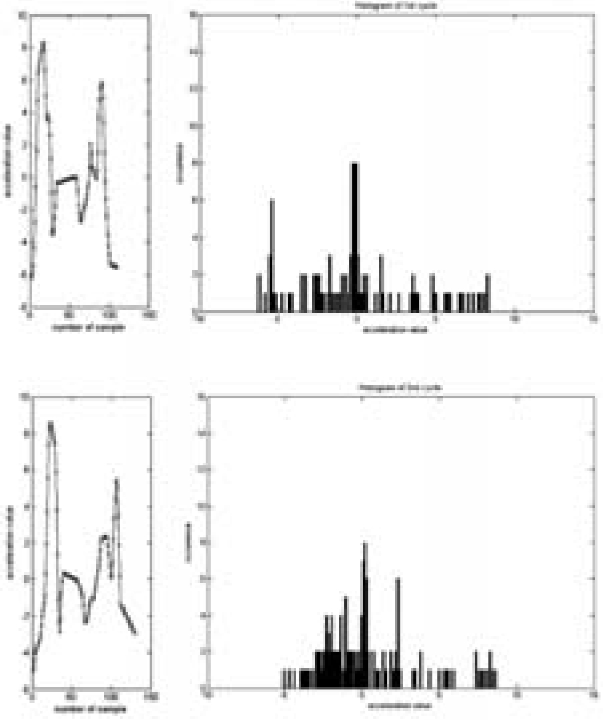

Figure 5: Two different cycles and corresponding histograms of subject 2.

The figures already indicate that the histograms obtained from cycles of the same subject are more similar than histograms of different subjects. This assumption has been tested using the data described in section 2. Test and results are given in the following section. The histogram generation removes private information (e.g. about health conditions) from the template and makes it impossible to reconstruct the original gait cycle. The histogram reveals information about the minimal and maximal value of the gait cycle (corresponding to the first and last non-zero bin), but furthermore no relevant information about the shape of the cycle can be obtained. To give the possibility of creating different protected templates from one biometric feature, it is possible to permutate the bins of the histogram. This permutation can be chosen differently for different applications to prevent cross matching but it has to be considered when calculating the distance between the histograms.

4 Tests and Results

Cycles obtained as described in section 2 are used to test the proposed method. From each cycle a histogram was created. Positions of the used bins have been the same for all cycles.

200 bins were used as this resulted in best recognition rates, but varying the number of bins did not have significant influence. This resulted in protected templates of length 200.
For comparision of the templates the earth mover's distance (EMD) [RTG98] returned the best results, which is a well known distance for comparing histograms. To illustrate this metric, bins of one of the histograms are assumed to be piles of soil and the bins of the second histogram are assumed to correspond to holes in which the soil should be filled. EMD measures the minimum cost needed to fill the holes with the soil, where the cost is the amount of soil transported times the distance by which it is moved. In our basic case the distance between bins at the same position will be zero, neighboured bins have distance one and so on. When the bins have been permuted, the distance matrix has to reflect this permutation.
The obtained results are given as Detection Error Trade-off curve (DET curve) by the dotted line in figure 6. The result is compared with the one obtained without template protection indicated by the continuous line in figure 6. The distance used for comparison in that case is dynamic time warping (DTW) [MÖ7]. Without using template protection the equal error rate (EER) is 12.85%. By using the proposed template protection method this increases to 29.47%. The reason for this will be the loss of information introduced by the histogram calculation, due to which no temporal information remains.

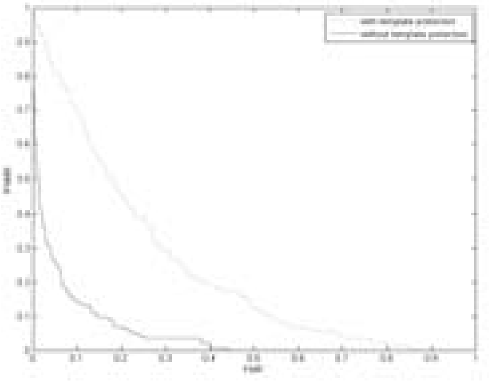

Figure 6: DET-curves obtained with and without template protection.

5 Summary and Conclusion

Having in mind the increasing amount of sensitive information stored on mobile devices and the increasing number of attacks on those devices, the need for secure, user-friendly authentication methods becomes clear. Accelerometer based gait recognition is such a method as it is able to authenticate a subject unobtrusively whithout his intervention. Up to now, no publications about template protection for accelerometer based gait recognition exist. This paper proposes a template protection method for cycle-based gait recognition

techniques, as this is the mainly chosen approach applied in existing feature extraction methods.
The feature vectors are converted into protected templates via histogram generation. Diversibility is obtained by applying different permutations to the template for different applications. The resulting templates are compared using the earth mover's distance. This technique does increase the EER significantly from 12.85% to 29.47% which indicates that the temporal distribution of acceleration values, which gets lost by histogram computation, does contain major information. Future work will focus on developing template protection methods which keep this information to guarantee a lower EER.

6 Acknowledgement

This work was supported by CASED (www.cased.de).

References

[ALM$^+$05] Heikki J. Ailisto, Mikko Lindholm, Jani Mäntyjärvi, Elena Vildjiounaite, and Satu-Marja Mäkelä. Identifying people from gait pattern with accelerometers. *Biometric Technology for Human Identification II*, 5779(1):7–14, 2005. VTT Electronics, Finland.

[ATIS09] Savvas Argyropoulos, Dimitrios Tzovaras, Dimosthenis Ioannidis, and Michael G. Strintzis. A channel coding approach for human authentication from gait sequences. *Transactions on Information Forensics and Security*, 4(3):428–440, 2009.

[BBGK08] Jeroen Breebaart, Christoph Busch, Justine Grave, and Els Kindt. A reference architecture for biometric template protection based on pseudo identities. In *BIOSIG 2008: Biometrics and Electronic Signatures*, 2008.

[CF05] N.L. Clarke and S.M. Furnell. Authentication of users on mobile telephones - A survey of attitudes and practices. *Computers & Security*, 24(7):519 – 527, 2005.

[gen] http://genkeycorp.com/.

[GHS06] Davrondzhon Gafurov, Kirsi Helkala, and Torkjel Søndrol. Biometric Gait Authentication Using Accelerometer Sensor. *Journal of Computers*, 1(7), 2006.

[GS09] Davrondzhon Gafurov and Einar Snekkenes. Gait recognition using wearable motion recording sensors. *EURASIP J. Adv. Signal Process*, 2009:1–16, 2009.

[HJO08] S.M. Habib, C. Jacob, and T. Olovsson. A practical analysis of the robustness and stability of the network stack in smartphones. In *Computer and Information Technology, 2008. ICCIT 2008. 11th International Conference on*, pages 393 –398, 24-27 2008.

[iso] ISO/IEC FCD 24787: Information technology – Identification cards – On-card biometric comparison.

[MÖ7] Meinard Müller. *Information Retrieval for Music and Motion*, chapter 4 - Dynamic Time Warping. Springer-Verlag New York, Inc., Secaucus, NJ, USA, 2007.

[pri] http://www.priv-id.com/.

[RCCB07] Nalini K. Ratha, Sharat Chikkerur, Jonathan H. Connell, and Ruud M. Bolle. Generating Cancelable Fingerprint Templates. In *IEEE Transactions on Pattern Analysis and Machine Intelligence*, volume 29, April 2007.

[RTG98] Y. Rubner, C. Tomasi, and L.J. Guibas. A metric for distributions with applications to image databases. In *Computer Vision, 1998. Sixth International Conference on*, pages 59 –66, 4-7 1998.

[UJ04] U. Uludag and A. Jain. Fuzzy fingerprint vault. In *Workshop: Biometrics: Challenges Arising from Theory to Practice*, August 2004.

[VKjS+06] Michiel Van Der Veen, Tom Kevenaar, Geert jan Schrijen, Ton H. Akkermans, Fei Zuo, and Prof Holstlaan. Face Biometrics with Renewable Templates. In Ping Wah Wong Edward J. Delp III, editor, *Proceedings of SPIE: Security, Steganography, and Watermarking of Multimedia Contents VIII*, volume 6072, 2006.

[WHNB08] Zhifang Wang, Qi Han, Xiamu Niu, and Christoph Busch. A Novel Template Protection Algorithm for Iris Recognition. *Intelligent Systems Design and Applications, International Conference on*, 2:340–345, 2008.

[Win] WinCE/Infojack. Windows Mobile trojan sends unauthorized information and leaves device vulnerable. online, last visited May 2010. http://www.avertlabs.com/research/blog/index.php/2008/02/26/windows-mobile-trojan-sends-unauthorized-information-and-leaves-devicevulnerable/.

[Zho07] Xuebing Zhou. Template Protection and its Implementation in 3D Face Recognition Systems. In *in Proceedings of SPIE Conference on Biometric Technology for Human Identification*, pages 214–225, 2007.

[ZWBK09] Xuebing Zhou, Stephen Wolthusen, Christoph Busch, and Arjan Kuijper. A Security Analysis of Biometric Template Protection Schemes. In *International Conference on Image Analysis and Recognition (ICIAR09)*, pages 429–438, 2009.