Gait template protection using HMM-UBM

Tim Van hamme[1], Enrique Argones Rúa[2], Davy Preuveneers[1], Wouter Joosen[1]

Abstract: This paper presents a hidden Markov model-Universal background model gait authentication system, which is also incorporated into a template protection based on a fuzzy commitment scheme. We show that with limited enrollment data the HMM-UBM system achieves a very competitive equal error rate of $\approx 1\%$ using one sensor. The proposed template protection scheme benefits from eigenfeatures coming from multiple Universal background model systems fused with a novel technique that minimizes the bit error rate for genuine attempts. This allows the protected system to achieve a false rejection rate below 5% with an effective key length of 64 bits.

Keywords: Gait authentication, HMM-UBM, protected templates

1 Introduction

Gait, the steady state movement pattern during locomotion, has been considered as an authenticator in the last decade [AK16]. Gait can be observed a.o. with Inertial Measurement Unit (IMU) sensors incorporated in all kinds of personal and wearable devices. Furthermore, gait has proven to be difficult to duplicate [GSB07]. Although gait authentication is achieving remarkable authentication performances, there are only a few examples of attempts to reliably and securely protect gait templates in the literature [HCN15]. Template protection [Br09] is one of the most sensible approaches for integrating biometrics into secure and privacy friendly authentication solutions. In the case of biometric cryptosystems such as fuzzy extractors [DRS04], this also enables the integration of biometrics into cryptographic protocols.

In this work, we aim at designing a high performance gait template protection scheme based on a biometric cryptosystem. We adopt one of the best performing and established techniques for biometric authentication in different modalities [APA09, Fi07, RQD00],the well-established hidden Markov model universal background models (HMM-UBM), and apply it to IMU-based gait authentication. This technique adapts UBM parameters to the enrollment data, and it provides accurate results even when the enrollment data is scarce. This system will be used as a baseline, and also as a starting point for the protected system, based on fusing UBM-eigenfeatures [KBD05] from multiple UBMs in a fuzzy commitment scheme [JW99]. A novel continuous feature fusion technique will be used to obtain binary templates from their continuous counterparts.

We evaluate the unprotected and protected HMM-UBM systems on the largest publicly available gait dataset OU-ISIR [Ng14]. It contains gait data from IMU sensors located on three body positions around the waist from 495 subjects performing two level walk sequences, a sequence for up-slope walk, and a sequence for down-slope walk. It enables authentication on an open-world scenario with scarce training and authentication data. We

[1] imec–Distrinet, KU Leuven, Computer Science Dept., Celestijnenlaan 200A, B-3001 Heverlee, BELGIUM, FirstName.LastName@cs.kuleuven.be

[2] imec–COSIC, KU Leuven, Elektrotechniek Dept., Kasteelpark Arenberg 10, bus 2452, B-3001 Leuven-Heverlee, Belgium, Enrique.ArgonesRua@esat.kuleuven.be

show that in this scenario the proposed HMM-UBM approach using simple features derived from the provided IMU data obtains authentication performances close to 1% Equal Error Rate. Most important, the protected system using UBM-eigenfeatures from several HMM-UBM systems obtains also a remarkable performance of $\approx$ 0% False Acceptance Rate and False Rejection Rate below 5% for an effective key length of 64 bits, which is the best achieved compromise regarding security and usability for this modality.

2 Related work

Ngo et al. [Ng14] made the OU-ISIR dataset available to serve as a benchmark. They re-evaluate 4 previously proposed gait authenticators. These methods extract gait cycles to build a template gallery. However, this is the limiting factor, as robustly extracting gait cycles is hard. The best work achieved an equal error rate (EER) of 14.3%. Lu et al. [Lu14] steered away from extracting gait cycles by using a GMM-UBM verification method. They extract standard statistical features in both time and frequency domain from a 5 second window. They achieve an EER of 14.0%. San-Segundo et al. [Sa16] use the same verification framework, but drop the MAP adaptation approach in favor of i-vector adaptation. Features are based on perceptual lineal prediction (PLP) coefficients. An EER of 6.1% is reached. Zhong and Deng [ZD14] exploit i-vector adapted GMM-UBM models as well. They propose another feature extraction method, called gait dynamic images (GDI). It is a visual rotation invariant representation of gait. When evaluated on the benchmark OU-ISIR dataset an EER of 5.6% is attained. Zhao and Zhou [ZZ17] use GDI's to train a CNN. A binary classification model per user is trained for authentication purposes. Zhao and Zhou do not report on achieved EERs. Furthermore, this approach requires 15 minutes of enrollment data. On top of that, this work focuses on a small closed world scenario, where it is not possible to ensure the feasibility of the proposed approach for a more general large population open world scenario. Especially, since the advantage of UBMs w.r.t. classical ML and DL techniques is that they by definition make the 'open world assumption'. Gadaleta and Rossi [GR18] address this by first training a CNN, to obtain a gait representation. The representation serves as input for a one-class SVM. However, the work resorts back to extracting individual gait cycles. A 0.15% EER is achieved by querying the OSVM multiple times, with different gait cycles. The work has only been evaluated with 15 users. Long gait sequences are necessary for training the representation network, which is not available in the OU-ISIR database. Besides, in their results they suggest that 5 gait cycles is enough to provide accurate authentication in 80% of the cases, which is approximately the amount of available data per gait sequence in the OU-ISIR database. In terms of protection, Hoang et al. [HCN15] adopt a fuzzy commitment scheme. They built a template gallery by extracting gait cycles. The work was evaluated with only 38 subjects. The system requires 8 templates consisting of 4 gait cycles per subject. Which is around 4 times more training data than our system needs. They acquire a 139 bit effective key length at a less favorable 16.18% FRR and a 0% FAR. Their authentication system without error correcting codes performs worse than ours, with a 3.5% EER.

3 HMM-UBM Gait Recognition

In this section, we first explain the unprotected system for gait authentication based on UBM-HMMs, and then continue how to use this system as a starting point for designing a protected system based on the fuzzy commitment scheme.

3.1 Unprotected system

In the proposed unprotected system, we use HMMs as generative models of the gait sequences. We use continuous density HMMs, where each state output probability function is defined as a Gaussian Mixture Model (GMM). Gait acquisitions are defined as variable-length sequences of feature vectors, which are modeled as the output of the HMM.

Since we are dealing with scarce enrollment data, we adopted the UBM-HMM approach for authentication. In this approach an UBM is trained using gait sequences from multiple persons, representing the whole population. During the enrollment phase, the means of the UBM state output probability functions are adapted using Maximum-a-Posteriori adaptation [RQD00], obtaining an adapted model representing the enrolled user. During authentication, the loglikelihood of the provided gait sequence is computed for both the UBM and the adapted model, and the authentication is done by comparing the obtained loglikelihood ratio with a threshold. In our system, this threshold is a system parameter, i.e. we do not use user-specific thresholds or score normalization techniques. The relevance factor τ for the model adaptation was set to 14 as a result of a grid search.

3.2 Protected system

It is possible to use an UBM-HMM unprotected system as the underlying system of a fuzzy commitment scheme. Below we explain how to obtain low-dimensional representations of the users in a UBM-HMM system, and then how to use these representations under the restrictions imposed by a fuzzy commitment scheme for template protection.

UBM-eigenfeatures The protected system we propose for gait authentication is based on the use of HMM-UBM eigenfeatures. These eigenfeatures are a low-dimensional representation of the adapted models. The differences between the means of the adapted models and the UBM for a set of users representing the whole population are reduced in dimensionality using Probabilistic Principal Components Analysis. The obtained representation has several advantages for its use in a biometric fuzzy commitment cryptosystem, namely: they preserve most of the discriminability; and they have a fixed length. The procedure for obtaining these features was first introduced in [KBD05] for GMMs, and it is explained in detail in [Ar12] for the general case of HMMs.

Feature protection scheme The feature protection scheme is illustrated in Fig. 1, where $\mathsf{ECC}_{\mathsf{encode}}$ and $\mathsf{ECC}_{\mathsf{decode}}$ stand for the encoding and decoding procedures of an error correcting code (ECC), and $\mathrm{h}()$ is a cryptographically secure hash function. The binary representation $\mathbf{b}$ is not derived from the biometrics, but randomly generated. The authentication succeeds only when the Hamming distance between the binary representation obtained during authentication $\hat{\mathbf{b}}$ and the one generated during the enrollment is equal or less than the error correcting capability t of the employed ECC. This scheme is directly derived from a fuzzy commitment scheme [JW99], but adding a quantization metadata $\mathscr{Q}$, which is computed during enrollment. It relates the enrollment biometrics and the binary representation, and it is later on used during verification to assist the quantization of the probe template. This quantization metadata is designed in such a way that although it minimizes the Bit Error Rate (BER) for genuine attempts, it will not provide any information about the binary representation **b**, therefore it does not pose a risk for security, i.e., knowing the metadata does not provide any advantage to a security adversary trying to guess the secret string **m**. The composition of this metadata and its computation is thoroughly explained in the next section.

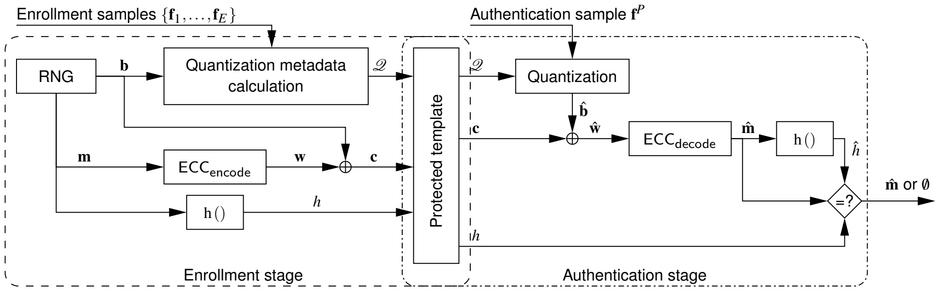

Fig. 1: Template protection approach incorporating quantization metadata to the Fuzzy Commitment

Quantization metadata Our protected system uses eigenfeatures coming from different UBMs, and many of them cannot provide a BER after quantization which is usable within a fuzzy commitment scheme, where the BER must be limited to the one that the employed error correcting code (ECC) can handle. Therefore, the proposed approach fuses different eigenfeatures to obtain each bit.

If we define n as the number of bits we need to extract–the length of the codeword **w** in Fig. 1–from our set of available features $\mathscr{F} = \{f_1,\ldots,f_F\}$, the algorithm that we propose computes a quantization metadata $\mathscr{Q}$ constituted by n disjoint sets of features $\mathscr{A}_i$, and a vector of weights $\mathbf{w} = [w_1,\ldots,w_F]^t$, i.e., $\mathscr{Q} = (\{\mathscr{A}_1,\ldots,\mathscr{A}_n\},\mathbf{w})$. The randomly chosen binary representation is denoted as $\mathbf{b} = [b_1,\ldots,b_n]$. During authentication, each bit b_i is estimated from the probe vector $\mathbf{f}^P = \left[f_1^P,\ldots,f_F^P\right]^t$ used for authentication as follows:

$$b_i = \frac{\operatorname{sign}\left(\sum_{f_j\in\mathscr{A}_i} w_j f_j^P\right)+1}{2} \tag{1}$$

The weights involved in this computation, as well as the disjoint sets defining which features contribute to each bit, are computed during the enrollment from a set of E enrollment vectors of features and the randomly chosen binary representation **b**.

Let us assume that the features in $\mathscr{F}$ are uncorrelated Gaussians $f_i \sim \mathscr{N}(\mu_i,\sigma_i)$. Let us also assume that σ_i is known, and we have an estimate $\hat{\mu}_i$ from E enrollment samples, and the feature mean is distributed population-wise as $\mu_i \sim \mathscr{N}(0,1)$. If the set of features contributing to bit i is defined as $\mathscr{A}_i = \left\{f_{i_1},\ldots,f_{i_{|\mathscr{A}_i|}}\right\}$ then the optimal BER for the genuine attempts is obtained when the weights are computed as:

$$w_{i_1} = (2b_i-1)\operatorname{sign}\hat{\rho}_{i_1} \tag{2}$$

$$w_{i_k} = \frac{\hat{\rho}_{i_k}\operatorname{sign}\left[(2b_i-1)\hat{\rho}_{i_k}\right]\sqrt{\sum_{j=1}^{k-1} w_{i_j}^2\sigma_{i_j}^2}}{\sigma_{i_k}\sqrt{\sum_{j=1}^{k-1}\hat{\rho}_{i_j}^2}}, \forall k>1 \tag{3}$$

In this case, the BER associated with the bit b_i for genuine attempts is as follows:

$$\mathrm{BER}_i\left(\hat{\rho}_i, E\right) = \sqrt{\frac{E}{2\pi}} \int_{\rho_i=-\infty}^{+\infty} \frac{1}{2} \left[1 - \operatorname{erf}\left(\frac{\hat{\rho}_i}{\sqrt{2}}\right) e^{-\frac{E(\rho_i-\hat{\rho}_i)^2}{2}}\right] \mathrm{d}\rho_i\,, \tag{4}$$

where the reliability of the binary feature $\hat{\rho}_i$ is defined as $\hat{\rho}_i = \sum_{j=1}^{|\mathscr{A}_i|} w_{i_j} \hat{\mu}_{i_j} / \sqrt{\sum_{j=1}^{|\mathscr{A}_i|} w_{i_j}^2 \sigma_{i_j}^2}$. Obtaining the sets $\mathscr{A}_1, \ldots, \mathscr{A}_n$ in such a way that the average BER is minimized is a number partitioning problem [Ko09]. We adopted a greedy approach for solving it, which provides a good approximation to the optimal solution. This approach basically iterates on the available features–those who have not yet been chosen–, choosing the most reliable one among them, i.e., the one with the maximum $|\hat{\rho}|$. The chosen feature is then incorporated into the least reliable set $\mathscr{A}_i$–the set with minimum $\hat{\rho}_i$. Weights are computed abiding Eqs. 2 and 3.

It can be easily checked that the quantization metadata does not provide any information about $\mathbf{b}$, since the features in $\mathscr{F}$ are uncorrelated and with median 0.

4 Feature extraction

In a gait system based on accelerometer and gyroscope sensory data, both linear acceleration including gravity $\mathbf{a}^g(n) = \left(a_x^g(n), a_y^g(n), a_z^g(n)\right)$ and gyroscopic velocity $\omega(n) = (\omega_x(n), \omega_y(n), \omega_z(n))$ signals are provided by the sensors at a given sample rate. In our case, sensors provide samples at 100 Hz rate. From these signals, we derived the following additional ones:

Gyroscopic dynamics $\alpha(n) = (\alpha_x(n), \alpha_y(n), \alpha_z(n))$, where each component $\alpha_d(n)$ is computed from its corresponding angular velocity component $\omega_d(n)$ as its first order differences, i.e. $\alpha_d(n) = \omega_d(n) - \omega_d(n-1)$. The magnitude of the angular dynamics were also derived: $\omega(n) = |\omega(n)|$ and $\alpha(n) = |\alpha(n)|$.

Roll and Pitch from Accelerometer The roll and pitch are estimated from the accelerometer signals without removing the gravity, as $r_a(n) = \operatorname{atan2}\left[a_z^g(n), a_y^g(n)\right]$ and $p_a(n) = \operatorname{atan2}\left[a_x^g(n), a_y^g(n)\right]$ respectively. Its associated roll and pitch velocities and accelerations $\dot{r}_a(n)$, $\dot{p}_a(n)$, $\ddot{r}_a(n)$, and $\ddot{p}_a(n)$ are obtained as the first and second order differences of $r_a(n)$ and $p_a(n)$ respectively.

Roll and Pitch from Accelerometer and Gyroscope If we define the pitch and roll estimated from the gyroscope signals as $p_g(n) = \sum_{k=0}^{n} \omega_x(n)$ and $r_g(n) = \sum_{k=0}^{n} \omega_z(n)$, we derive a joint estimate of the pitch and the roll signals as: $f(n) = 0.98\left[f(n-1) + f_g(n)\right] + 0.02 f_a(n)$, where f is either the pitch p or the roll r.

Vertical and Horizontal components The vertical and horizontal acceleration components are derived from the accelerometer data as $a_v(n) = a_y(n)$ and $a_h(n) = \left|a_x^2(n) + a_z^2(n)\right|$ respectively. Their corresponding velocities $v_v(n)$, $v_h(n)$ are computed by integration, and their corresponding jerks $j_v(n)$, $j_h(n)$ are computed by as the first order differences.

5 Experiments

In this paper we only used the gait sequences from the OU-ISIR database labeled as *level walk* captured with the Center sensor. Subjects usually have two level walk sequences observed by three IMU sensors located around the waist. The first walk sequence is used for enrollment, and the second one for test. Only the 483 users with two valid level walk sequences captured with the Left, Center, and Right sensors were considered, though only the sensor Center is used in the experiments. These users were divided into two experimental groups by lexicographic order of their pseudonyms, since no demographic data was available for a more sensible split. The first group is constituted by the first 242 users, labeled as $\mathrm{U}_0^1, \dots, \mathrm{U}_{241}^1$, and the second one by the remaining 241 users, labeled as $\mathrm{U}_0^2, \dots, \mathrm{U}_{240}^2$. Regarding impostor attempts, each user is impersonated by the 5 next users from his group. Only the second walks are used as impostor attempts, therefore group 1 has a total 242 genuine and 1210 impostor attempts, while group 2 has a total 241 genuine and 1205 impostor attempts.

Each group's UBM and eigenmatrix is trained using all the captures from the other group. Verification performance is reported for the unprotected system as the group-wise average Equal Error Rate (EER). For the protected system, where the working point is fixed by the employed ECC, FAR and FRR are reported for both groups.

S	M	EER%
1	128	1.45
2	64	1.60
4	32	1.46
8	16	1.42
16	8	1.49

Tab. 1: Performance in terms of average EER% using the Center sensor of HMM-UBM configurations with S states and M Gaussian mixtures per state for $C = S \cdot M = 128$.

We tested the unprotected system introduced in Section 3.1 using the Center sensor and the features introduced in Section 4. The average EER in the OU-ISIR dataset is shown in Tab. 1 for different number of states $S \in \{1, 2, 4, 8, 16\}$ and number of Gaussian mixtures in each state output distribution $M \in \{128, 64, 32, 16, 8\}$ for a constant model complexity $C = SM = 128$.

We also analyzed the authentication performance and EKL obtained by the protected system introduced in Section 3.2. For this experiment, the UBM-eigenfeatures are obtained from different unprotected systems, as shown in Tab. 2. Two different configurations of the protected system were tested: *System 1*, incorporating all the UBM-eigenfeatures from 16 unprotected systems, and *System 2*, incorporating all the UBM-eigenfeatures from 8 unprotected systems. In total, the number of UBM-eigenfeatures is $F = 3840$ for System 1, and $F = 1920$ for System 2.

The performance of this protected system is shown in Tab. 3 for different codes. The parameter k shown in this table coincides with the EKL of the protected scheme. This is the security parameter of the fuzzy commitment scheme. It can be seen that using 8 UBM-eigenfeatures sets it is possible to reach an EKL of 36, while when using 16 UBM-eigenfeatures sets it is possible to reach up to 64 bits with a low FRR.

System	S	M	D	N	System	S	M	D	N
1	1	128	240	4	2	1	128	240	2
	2	64	120	4		2	64	120	2
	4	32	60	4		4	32	60	2
	8	16	30	4		8	16	30	2

Tab. 2: Unprotected systems incorporated into the protected systems. D stands for the number of eigenfeatures computed for each state, and N is the number of unprotected systems with these parameters incorporated into the protected system.

	BCH Code							BCH Code					
System	n	k	t	Group	FAR	FRR	System	n	k	t	Group	FAR	FRR
1	127	64	10	1	0.08	4.96	2	127	29	21	1	0.00	8.68
				2	0.08	3.32					2	0.00	10.79
		57	11	1	0.08	3.72			22	23	1	0.08	5.37
				2	0.08	2.49					2	0.08	7.47
		50	13	1	0.25	2.07			15	27	1	0.25	2.89
				2	0.25	1.66					2	0.25	3.73
	63	57	1	1	0.41	2.07		63	36	5	1	0.08	4.96
				2	0.41	3.32					2	0.17	3.32
		51	2	1	0.74	1.24			30	6	1	0.25	3.31
				2	0.66	1.66					2	0.25	2.49
		45	3	1	1.32	0.83			24	7	1	0.33	2.07
				2	1.08	1.24					2	0.58	2.07

Tab. 3: Protected systems percentual performance figures for different code parameters.

6 Discussion and Conclusions

In this work we proposed HMM-UBM systems using simple and computationally inexpensive features for gait recognition, and analyzed their performance in an open world in a scarce enrollment and authentication data scenario, using the OU-ISIR dataset.

The authentication performance of the proposed HMM-UBM system reaches EERs around 1% using a single sensor. This level of performance is remarkable in comparison to the ones reported in the literature for this dataset. Although there are works reporting very low error rates, they are tested in closed set scenarios with a reduced number of users, which hinders a fair comparison with the one proposed here.

The quantization employed in the proposed protected method enables the fusion of multiple sets of features coming from multiple HMM-UBM systems. This fusion provides binary features with a BER that practical ECCs can handle for EKLs equivalent to the usual requirements for passwords [Gr17] and acceptable FRR.

These results demonstrate the feasibility of the proposed approaches in open-world scenarios even only with around 5 seconds of enrollment and authentication data.

References

[AK16] Alzubaidi, A.; Kalita, J.: Authentication of Smartphone Users Using Behavioral Biometrics. IEEE Communications Surveys Tutorials, 18(3):1998–2026, thirdquarter 2016.

[APA09] Argones Rúa, E.; Pérez-Piñar López, D.; Alba Castro, J.L.: Ergodic HMM-UBM System for On-Line Signature Verification. In: Biometric ID Management and Multimodal Communication. Springer Berlin Heidelberg, pp. 340–347, 2009.

[Ar12] Argones Rúa, E.; Maiorana, E.; Alba Castro, J. L.; Campisi, P.: Biometric Template Protection Using Universal Background Models: An Application to Online Signature. IEEE Trans. on Information Forensics and Security, 7(1):269–282, 2012.

[Br09] Breebaart, J.; Yang, B.; Buhan-Dulman, I.; Busch, C.: Biometric template protection. Datenschutz und Datensicherheit - DuD, 33(5):299–304, May 2009.

[DRS04] Dodis, Y.; Reyzin, L.; Smith, A.: Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data. In: Advances in Cryptology - EUROCRYPT 2004. Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 523–540, 2004.

[Fi07] Fierrez, Julian; Ortega-Garcia, Javier; Ramos, Daniel; Gonzalez-Rodriguez, Joaquin: HMM-based on-line signature verification: Feature extraction and signature modeling. Pattern Recognition Letters, 28(16):2325 – 2334, 2007.

[Gr17] Grassi, Paul A.; Fenton, James L.; Newton, Elaine M.; Perlner, Ray A.; Regenscheid, Andrew R.; andJustin P. Richer, William E. Burr: SP 800-63B–Digital Identity Guidelines–Authentication and Lifecycle Management. Technical report, 2017.

[GR18] Gadaleta, Matteo; Rossi, Michele: IDNet: Smartphone-based gait recognition with convolutional neural networks. Pattern Recognition, 74:25 – 37, 2018.

[GSB07] Gafurov, D.; Snekkenes, E.; Bours, P.: Spoof Attacks on Gait Authentication System. IEEE TIFS, 2(3):491–502, Sept 2007.

[HCN15] Hoang, Thang; Choi, Deokjai; Nguyen, Thuc: Gait authentication on mobile phone using biometric cryptosystem and fuzzy commitment scheme. International Journal of Information Security, 14(6):549–560, Nov 2015.

[JW99] Juels, Ari; Wattenberg, Martin: A Fuzzy Commitment Scheme. In: Proceedings of the 6th ACM Conference on Computer and Communications Security. CCS '99, ACM, New York, NY, USA, pp. 28–36, 1999.

[KBD05] Kenny, P.; Boulianne, G.; Dumouchel, P.: Eigenvoice Modeling With Sparse Training Data. IEEE Transactions on Speech and Audio Processing, 13(3), May 2005.

[Ko09] Korf, Robert E.: Multi-way number partitioning. In: Proceedings of the 21st International Jont Conference on Artifical Intelligence. Morgan Kaufmann Publishers Inc., San Francisco, CA, USA, pp. 538–543, 2009.

[Lu14] Lu, H.; Huang, J.; Saha, T.; Nachman, L.: Unobtrusive Gait Verification for Mobile Phones. In: Proceedings of the 2014 ACM International Symposium on Wearable Computers. ISWC '14, ACM, New York, NY, USA, pp. 91–98, 2014.

[Ng14] Ngo, T.T.; Makihara, Y.; Nagahara, H.; Mukaigawa, Y.; Yagi, Y.: The largest inertial sensor-based gait database and performance evaluation of gait-based personal authentication. Pattern Recognition, 47(1):228 – 237, 2014.

[RQD00] Reynolds, D.A.; Quatieri, T.F.; Dunn, R.B.: Speaker Verification Using Adapted Gaussian Mixture Models. Digital Signal Processing, 10:19–41, 2000.

[Sa16] San-Segundo, R.; Cordoba, R.; Ferreiros, J.; D'Haro-Enriquez, L.F.: Frequency features and GMM-UBM approach for gait-based person identification using smartphone inertial signals. Pattern Recognition Letters, 73:60 – 67, 2016.

[ZD14] Zhong, Y.; Deng, Y.: Sensor orientation invariant mobile gait biometrics. In: IEEE International Joint Conference on Biometrics. pp. 1–8, Sept 2014.

[ZZ17] Zhao, Y.; Zhou, S.: Wearable device-based gait recognition using angle embedded hait dynamic images and a convolutional neural network. Sensors, 17(3), 2017.