Gaithashing: a two-factor authentication scheme based on gait features

Christoforos Ntantogian, Stefanos Malliaros, Christos Xenakis
Department of Digital Systems, University of Piraeus, Piraeus, Greece
{dadoyan, stefmal, xenakis}@unipi.gr

Abstract

Recently, gait recognition has attracted much attention as a biometric feature for real-time person authentication. The main advantage of gait is that it can be observed at a distance in an unobtrusive manner. However, the security of an authentication system, based only on gait features, can be easily broken. A malicious actor can observe the gait of an unsuspicious person and extract the related biometric template in a trivial manner and without being noticed. Another major issue of gait as an identifier has to do with their high intra-variance, since human silhouettes can be significantly modified, when for example the user holds a bag or wears a coat. This paper proposes gaithashing, a two-factor authentication that interpolates between the security features of biohash and the recognition capabilities of gait features to provide a high accuracy and secure authentication system. A novel characteristic of gaithashing is that it enrolls three different human silhouettes types. During authentication, the new extracted gait features and the enrollment ones are fused using weighted sums. By selecting appropriate weight values, the proposed scheme eliminates the noise and distortions caused by different silhouette types and achieves to authenticate a user independently of his/her silhouette. Apart from high accuracy, the proposed scheme provides revocability in case of a biometric template compromise. The performance of the proposed scheme is evaluated by carrying out a comprehensive set of experiments. Numerical results show that gaithashing outperforms existing solutions in terms of authentication performance, while at the same time achieves to secure the gait features.

Keywords: gait, biohash, biometrics, fusion, authentication.

1 Introduction

Currently, users authentication and access control is mainly carried out based on the usage of passwords or tokens. However, these mechanisms present fundamental limitations in terms of both security and usability. More specifically, short length passwords are usually of low entropy, which means that an attacker may guess them, while lengthy passwords are difficult to remember. It is also hard for users to remember a lengthy, secure password for each employed service. This results in the usage of the same or similar passwords to each service, which increases significantly the risk of a password to be broken and the associated services to be compromised. Moreover, tokens can be easily misplaced or stolen.

To overcome these limitations, biometric technology has emerged, which is defined as: *"automated recognition of individuals based on their behavioral and biological characteristics"* [8]. The authentication systems that employ biometrics include two fundamental procedures: a) enrollment and b) authentication. During enrollment, distinctive biometric features are extracted from an underlying user of the system to form its biometric template, which is stored in a database or token. In the authentication procedure, the system extracts the considered biometric features of a tentative user and creates its biometric template, which is

compared against the initial (i.e., the template created and stored during enrollment) for user's acceptance or rejection.

A major challenge in biometrics is the protection of the extracted templates, in order to prevent malicious actors to perform impersonation attacks. Due to the fact that biometric characteristics are immutable, a security breach of the biometric templates renders the subjects' biometrics useless. For this reason, prior to their storage to a physical medium (e.g., hard disk, USB token), a protection scheme should be applied to secure them. In general, the protection schemes for biometric templates should be designed to fulfill the following requirements:

- **Irreversibility:** It should be computationally hard to reconstruct the original biometric features from a secure biometric template.

- **Revocability:** Different versions of secure biometric templates can be generated, based on the same biometric data. Thus, if a biometric template is compromised, then it can be replaced with a new one.

- **Unlinkability:** Secure biometric templates of the same subject, which are used in different authentication systems, should not allow cross-matching.

Apart from security, another important issue that need to be addressed is the intrinsic intra-variance that biometrics present. That is, the biometric features of the same subject cannot be extracted exactly the same, twice. As a result, the authentication of a valid user may fail, in case the extracted gait features differ significantly from the enrollment ones. As a matter of fact, the application of protection schemes may increase even more the intra-variance of biometrics, resulting in poor recognition results. Thus, the considered biometric template protection schemes seek to achieve an optimal balance between security and performance.

A prominent template protection scheme is biohash [10], which transforms a biometric feature to a non-invertible bitstream, using tokenized random data. Biohash involves two authentication factors to verify a user:

1. **Proof by possession:** The user is authenticated by proving the possession of a token, which is unique for each user of the system.
2. **Proof by property:** The user is authenticated by his/her biometric feature.

The biohash scheme has been successfully applied to various biometric features, including face [21], fingerprint [10] and palmprints [2]. In all these studies, biohash exhibits very good authentication performance, protecting, at the same time, the employed biometric features.

Recently, gait recognition has attracted much attention as a biometric feature, for real-time person authentication. The main advantage of gait is that it can be observed at a distance, in an unobtrusive manner. For this reason, it is very suitable for surveillance applications or in environments where the application of other biometric traits (such as fingerprints or iris) is constrained. However, the security of an authentication system that employs, only, gait features can be easily broken. That is, a malicious

actor may observe and record the gait of an unsuspicious person, and then, try to extract the related biometric template in a trivial manner, without being noticed. This compromised template can be used for authenticating a malicious in controlled environments gaining unauthorized access. Another major issue of gait features has to do with their high intra-variance. This is attributed to the fact that gait features are extracted from human silhouettes, which can be significantly modified, when, for example, the user holds a bag or wears a coat. The introduced noise, due to changes in human silhouettes, distorts the gait features, resulting in poor authentication performance.

This paper proposes gaithashing, a two-factor authentication scheme that secures gait features and addresses their intra-variance, using fusion methods. The proposed scheme interpolates between the security features of biohash and the recognition capabilities of gait features to provide a high accuracy and secure authentication system. A novel characteristic of gaithashing is that it enrolls three different human silhouettes types. That is: a) straight (i.e., the user wears trousers, blouse and shoes), b) coat (similar to straight silhouette, but the user also wears a coat), and, c) bag (similar to straight silhouette, but the user carries also a briefcase). During authentication, the new extracted gait features are fused with each one of the enrollment templates, using weighted sums. By selecting appropriate weight values, gaithashing performs comparison between gait features of the same silhouette type, eliminating in this way the noise and distortions caused by different silhouette types. Apart from high accuracy, the proposed scheme provides revocability in case of a biometric template compromise. The gaithashing scheme is evaluated by carrying out a comprehensive set of experiments. Numerical results show that gaithashing outperforms existing solutions in terms of authentication performance, while at the same time achieves to secure the gait features. Moreover, a comparative analysis of the performance of gaithashing with other state-of-the-art protection schemes is carried out, in order to highlight the advantageous characteristics of gaithashing. Overall, the contributions of this paper are twofold:

- We propose a two-factor authentication scheme that extracts gait features and converts them to non-invertible bitstreams, without affecting the authentication accuracy.
- We implement gaithashing and conduct comprehensive sets of experiments to evaluate and fine-tune the proposed scheme.

The rest of the article is organized as follows. Section 2 provides the background for biometric template security and performance, as well as analyzes the related work. Section 3 presents the gait feature extraction and protection procedure. Section 4 describes and evaluates two different enrollment and authentication schemes, while section 5 analyzes the proposed scheme named gaithashing. Section 6 evaluates gaithashing by elaborating on its authentication performance and comparing it to other state-of-the-art schemes. Finally, section 7 includes the conclusions.

2 Background

2.1 Biometric template security and performance

Protection schemes for biometric templates can be categorized as follows: a) biometric cryptosystems, and b) cancelable biometrics. Biometric cryptosystems are designed to securely bind a key to a biometric feature or generate a key from a biometric feature. On the other hand, cancelable biometrics consists of intentional, repeatable distortions of biometric features, based on one-way transforms, where the comparison of biometric templates takes place in the transformed domain. A comprehensive overview of biometric template protection schemes is presented in [17]. One of the most widely used cancellable biometrics algorithm is biohash and its variations [10], [13]. The one-way transformation of biohash is based on random projections [20]. The mathematical properties of random projections ensure the security of the protected template, while at the same time the authentication performance is not deteriorated. For this reason, the proposed scheme of this paper adopts a simple variation of biohash to secure the extracted gait features (see section 3.2).

As mentioned previously, biometric systems include two procedures: a) enrollment and b) authentication. During enrollment, biometric features are extracted from a user of the system to form its biometric template, which is stored in a database or token. During authentication, the system extracts the considered biometric features of a user and creates a new biometric template, which is compared against the enrolled one for user's acceptance or rejection. Due to the intrinsic noise of biometric features, the authentication and enrollment template cannot perfectly match. For this reason, biometrics systems compare the distance ((i.e., Euclidean, Hamming, or any other metric) between the enrolled and authentication template of a user against a predetermined threshold. If the distance is lower than the threshold value, then the user is successfully authenticated; otherwise he/she is rejected.

The performance of a biometric system can be estimated and quantified using the following two metrics: i) false acceptance rate (FAR) and ii) false rejection rate (FRR). FAR represents the probability that an authentication system will incorrectly accept an authentication attempt by an impostor (i.e., a non-valid user that does not have an enrolled biometric template in the system); whereas FRR represents the probability that the system will incorrectly reject an authentication attempt by a genuine user (i.e., a valid and registered user of the system with an enrolled biometric template). As we analyze below, the exact value of FAR and FRR depend on the predetermined threshold value of the system. Another important metric that can be used to evaluate the authentication performance of a biometric system, is the Equal Error Rate (EER). The latter is the rate at which both acceptance and rejection errors are equal (i.e., EER=FAR=FRR). It is evident that the lower the value of EER is, the higher the accuracy of the biometric system.

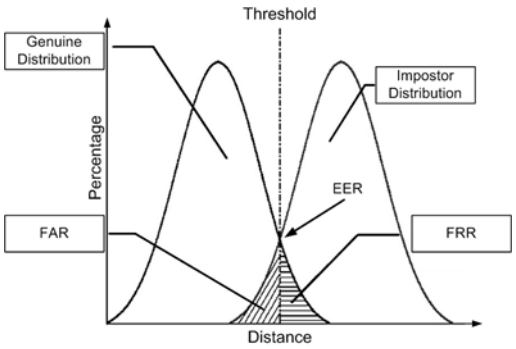

Figure 1: Genuine and impostor distributions as a function of distance between enrollment and authentication templates

To gain better understanding of the FAR, FRR and EER metrics, figure 1 plots genuine and impostor distributions of a generic biometric system as a function of the distance between the enrolled and authentication templates. As expected, genuine users have small distances, while impostors have high distances. We can also observe that the two distribution curves have an overlapping area. This means that in this overlapping area the system cannot distinguish genuine users from impostors. Moreover, as shown in figure 1, the threshold value is set at the intersection point of the two curves. The threshold value divides the overlapping area into two sub-areas. The left sub-area represent the FAR, while the right sub-area represents the FRR. The intersection point of the two curves defines the EER value (see figure 1), since at this point the FAR and FRR are equal (i.e., EER=FAR=FRR). Moreover, it is evident that a biometric system presents optimum results (i.e., FAR and FRR equal to 0) when the genuine and impostor curves do not overall at all. On the other hand, as the overlapping area between the genuine and impostor curves increases, then the authentication performance is deteriorated.

2.2 Related work

Over the last years, several studies have been performed to consider gait signatures, by using shape analysis and extracting features from the silhouette of the human body. Here, we provide a brief overview of the most recent works in this area. In [22], the authors pinpoint that temporal information is critical to the performance of gait recognition. To address this, they propose a novel temporal template, named chrono-gait image (CGI) in order to retain temporal information in a gait sequence. Moreover, the authors of [5] argue that the change of viewing angle of the sensor causes significant distortion to the extracted features. Based on this observation, they formulate a new patch distribution feature (PDF) to address this issue. The same viewing angle problem is addressed in [12]. The authors propose a transformation framework of the walking silhouettes to normalize gaits from arbitrary views. In [15], the proposed method is based on the idea that the problem of human gait recognition can be transformed from the spatiotemporal into the spatial domain, specifically, the 2D image domain. This is achieved by representing a sample of a human gait as a still image.

Towards this direction, [11] argues that variations of walking speed may lead to significant changes of human walking patterns. Based on this observation, a differential composition model (DCM) is proposed that differentiates the effects caused by walking speed changes on various human body parts; while at the same time it balances the different discriminabilities of each body part on the overall gait similarity measurements. In [19], the concept of the gait energy image (GEI) is extended from 2D to 3D images, creating gait energy volume (GEV). The obtained numerical results show that the GEV performance is improved, compared to the GEI baseline and fused multi-view GEI approaches. Next, in [18] the authors instead of using human silhouette images from moving picture, they apply 3D point clouds data of human body obtained from stereo camera, which has the scale-invariant property. In this way, they achieve significant performance improvement in terms of gait recognition. In [6], the authors propose a multi-view, multi-stance gait identification method, using unified multi-view population hidden Markov models, in which all the models share the same transition probabilities. Hence, the gait dynamics in each view can be normalized into fixed-length stances by Viterbi decoding. [14] provides an extensive overview of the methods used for accelerometer-based gait analysis, using mobile devices. In [7], the extraction of distinguishable gait features is proposed using the radial integration transform (RIT), the circular integration transform (CIT), and the weighted Krawtchouk moments. In our proposed scheme, we use the CIT and RIT transformations for gait feature extraction, due to their excellent recognition capabilities (see section 3.1 for analysis).

On the other hand, the related work in protection schemes for gait features is rather limited. In [4], the authors propose an authentication system that protects gait features using biometric cryptosystems. Gait features are extracted using an accelerometer attached to the user's body. Experimental results show that the proposed scheme achieves small EER values, only, for small key sizes. Thus, high accuracy is achieved without providing an adequate level of security. Finally, in [1], the authors propose a template protection scheme for gait features, based on channel coding (i.e., LDPC codes). Their approach, achieves EER=6% for straight silhouette types, but 20% and 30% for bag and coat types respectively.

A common limitation of the majority of previous works is that they focus, only, on the extraction and not on the protection of the gait features. On the contrary, in this paper we propose and integrate feature extraction and protection into one system, providing a complete solution for biometric authentication based on gait features. Moreover, the previous works [1] and [4] that attempt to secure gait features, fail to achieve an optimum tradeoff between security and performance (see section 6.2). On the hand, in this paper, by interpolating between the security of biohash and the recognition capabilities of gait features, we achieve to outperform existing solutions, without undermining the provided security. Finally, it is important to mention that biohash has been successfully applied to various biometric features including fingerprints [10] [16], face [21] [9], singatures [13], palmprints and palm veins [2] [3], but to the best of our

knowledge it has not been applied to gait features.

3 Gait feature extraction and protection

The key functionality of the proposed biometric system is the caption and extraction of gait features from a human silhouette as well as the protection of the extracted gait features. As we analyze below, the extraction of the gait features is based on the CIT and RIT transformations which converts the human walking to gait vectors. Next, the extracted gait vectors are converted to bitstreams with the help of the user's token based on the biohash algorithm.

3.1 CIT and RIT transformations

For the extraction of gait features, this paper considers three different types of human silhouettes: 1) straight (i.e., the user wears trousers, blouse and shoes), 2) coat (similar to straight silhouette, but the user also wears a coat), and, 3) bag (similar to straight silhouette, but the user carries also a briefcase). It is worth noting that although the current work considers only the above three types of silhouettes, the proposed authentication system can be easily extended to take into account other types of silhouettes (e.g., the user wears a hat) or various combinations (e.g., a user wearing a coat and a hat).

The extraction of gait features is based on two feature-based algorithms: the RIT and CIT transformations. These algorithms are selected due to their capability to represent important shape characteristics [2]. That is, during human movement, there is a considerably large diversity in the angles of lower parts of the body (e.g. arms, legs), which vary among individuals. Both RIT and CIT transformations ensure that the important dynamics of human shape are captured, thus enabling the correct classification of individuals. Moreover, these algorithms are less sensitive to the presence of noise on the silhouette image, compared to other schemes [2].

At this point, we provide a brief presentation of these transformations, where additional details can be found in [7]. The first step in gait analysis is the extraction of the walking subject's silhouette from the input image sequence. The normalized silhouettes are defined as $\tilde{S}_G(x, y)$ where transformations are applied. More specifically, the RIT transform of a function $f(.,.)$ is defined as the integral of $f(.,.)$ along a line starting from the center of the silhouette(x_0, y_0), which forms angle θ with the horizontal axis. The discrete form of RIT, which computes the transform in steps of $\Delta\theta$ is given by:

$$RIT(t\Delta\theta) = \frac{1}{J}\sum_{j=1}^{J}(\tilde{S}_G(x_0 + j\Delta u * \cos(t\Delta\theta), y_0 + j\Delta u * \sin(t\Delta\theta))),$$

where $\tau = 1, \dots, T, \Delta u$ and $\Delta\theta$ are constant step sizes of distance u and angle θ, J is the number of silhouette pixels that coincides with the line that has orientation θ and are positioned between the center of the silhouette and the end of the silhouette in that direction, and

$T = 360^{\circ}/\Delta\theta$.

In a similar manner, CIT is defined as the integral of a function $f(.,.)$ along a circle curve $h(\rho)$ with center (x_0, y_0) and radius ρ. The discrete form of the CIT transform is given by:

$$CIT(k\Delta\rho) = \frac{1}{T}\sum_{t=1}^{T}(\tilde{S}_G(x_0 + k\Delta\rho * \cos(t\Delta\theta), y_0 + k\Delta\rho * \sin(t\Delta\theta))),$$

where $k = 1, \dots K, \Delta\rho$ and $\Delta\theta$ are the constant step sizes of the radius and angle variables, $k\Delta\rho$ is the radius of the smallest circle that encloses the binary silhouette image $\tilde{S}_G$, and $T = 360^{\circ}/\Delta\theta$. The output of the CIT and RIT transformations are the fixed-length vectors Γ_{CIT} and Γ_{RIT} of size $n_1 = 80$ and $n_2 = 120$ respectively.

3.2 Biohash

After the extraction of the gait features (using the CIT and RIT transformations), the biohash algorithm is applied to secure them. The biohash algorithm *is a two factor authentication scheme* that identifies a user based on what he/she is (i.e., biometrics) and what he/she has under his/her possession (i.e., token). In the context of our proposed scheme, the biohash algorithm converts the gait feature vectors Γ_{CIT} and Γ_{RIT} (see section 3.1) to non-invertible bitstreams, using a token that the user possess. Since the application of biohash is similar to both CIT and RIT vectors, here we present the biohash algorithm in a generic way. More specifically, we present the application of biohash to a vector Γ of size n, which is converted to a bitstream B. Biohash includes the following phases [20]:

1. The token of the user generates a set of orthonormal pseudorandom vectors
$$\{r_i \in R^n | i = 1, \dots, n\},$$
2. A vector Z of size n with elements z_i is computed such as:
$$z_i = \langle \Gamma | r_i \rangle \in R, i = \{1, \dots, n\},$$
where $\langle . | . \rangle$ indicates the inner product operation. This procedure is also known as random projection.
3. The mean value μ and standard deviation σ of z_i are computed.
4. The final step is the binarization of z_i. As shown in table 1, first it divides the real-space of z_i into 8 segments. Next, each segment is mapped to a three bit digit value $b_i \in \{0,1\}^3$, so that two successive segments have only one bit difference between them (see table 1). In this way, it transforms the elements of vector Z into a bitstream $B = \{b_1 b_2 \dots b_n\}$ of $3n$ bits length.

Table 1: Conversion of z_i to b_i

Segment	z_i	b_i
1	$-\infty \leq z_i < \mu - 3\sigma$	000
2	$\mu - 3\sigma \leq z_i < \mu - 2\sigma$	001
3	$\mu - 2\sigma \leq z_i < \mu - \sigma$	011
4	$\mu - \sigma \leq z_i < \mu$	010
5	$\mu \leq z_i < \mu + \sigma$	110
6	$\mu + \sigma \leq z_i < \mu + 2\sigma$	111
7	$\mu + 2\sigma \leq z_i < \mu + 3\sigma$	101
8	$\mu + 3\sigma \leq z_i < +\infty$	100

4 Initial experiments and observations

In this section we propose and evaluate experimentally two initial enrollment and authentication schemes. As we analyze below, despite the fact that these two schemes proved inadequate, due to their poor authentication performance, they provided useful observations and insights that allowed us to fine-tune and design and optimal enrollment and authentication scheme that is presented in section 5.

As we mentioned in section 3.1, in this work we consider three types of gait features that are extracted from three types of human silhouettes: i) straight $G_{straight}$, ii) coat G_{coat}, and, iii) bag G_{bag}. Thus, an important question that arises here is: *Which one of the three considered gait features the authentication system should enroll?* To answer this question, we consider the following two enrollment and authentication schemes each of which encompasses a different technical approach:

1st scheme: Enrollment of one of the three considered gait feature vectors. The selection of the specific silhouette type that will be used for enrollment is arbitrary.

2nd scheme: First, a feature-level fusion of all three gait feature vectors is performed. Next, we enroll the single vector generated from the fusion.

In the sections below, we present and evaluate through experiments the two above mentioned enrollment and authentication schemes.

4.1 1st scheme

In the first scheme, we enroll gait features that are extracted only from one of the three considered types of human silhouettes. The specific gait feature that will be used for enrollment is selected arbitrary. In this analysis, we consider gait features from a straight human silhouette to be used for enrollment (note that the same procedure is followed, if another type of human silhouette is selected for enrollment). In this case, the CIT and RIT transformations are applied to extract the gait features from a straight silhouette $G_{straight}$. That is,

$$GaitVector_{(cit,straight)} = CIT\_Transformation(G_{straight}),$$
$$GaitVector_{(rit,straight)} = RIT\_Transformation(G_{straight}).$$

Next, the biohash algorithm is applied to the two feature vectors (i.e., one

for CIT and one for RIT), in order to generate two different enrollment bitstreams, denoted $Ebits_{(cit,\ straight)}$ and $Ebits_{(rit,\ straight)}$, respectively, which are stored in the enrollment database. That is:

$$Ebits_{(cit,straight)} = Biohash\left(GaitVector_{(cit,straight)}, Token\right),$$
$$Ebits_{(rit,straight)} = Biohash\left(GaitVector_{(rit,straight)}, Token\right).$$

In the authentication procedure, the silhouette G of the user can be one of the three types (i.e., straight, coat, bag). First, the CIT and RIT transformation are applied to extract two gait feature vectors (i.e., one from CIT and one from RIT) as follows:

$$GaitVector_{(cit)} = CIT\_Transformation(G),$$

$$GaitVector_{(rit)} = RIT\_Transformation(G).$$

Next, using the user's token and the extracted feature vectors, biohash is applied to generate two different authentication bitstreams $Abits_{(cit)}$ and $Abits_{(rit)}$. That is:

$$Abits_{(cit)} = Biohash\left(GaitVector_{(cit)}, Token\right),$$

$$Abits_{(rit)} = Biohash\left(GaitVector_{(rit)}, Token\right).$$

At this point, the hamming distance between the authentication and the enrollment bitstreams is computed, separately for each transformation. Finally, the sum of the two hamming distances is computed as follows:

$$FinalResult = HDistance\left(Ebits_{(cit,straight)}, Abits_{(cit)}\right) + HDistance\left(Ebits_{(rit,straight)}, Abits_{(rit)}\right)$$

Finally, a user is accepted if FinalResult is less than a predetermined threshold, otherwise he/she is rejected.

4.2 2nd scheme

In the second scheme, we apply feature-level fusion [23], in order to enroll gait features from all the three considered human silhouettes. In particular, the CIT and RIT transformations are applied to extract the gait features from the three considered human silhouettes: i) straight, ii) coat, and, iii) bag. Next, we fuse the extracted feature vectors to create two mean feature vectors $GaitVector_{(cit,fused)}$ and $GaitVector_{(rit,fused)}$ as follows:

$$GaitVector_{(cit,fused)} = \frac{GaitVector_{(cit,straight)} + GaitVector_{(cit,bag)} + GaitVector_{(cit,coat)}}{3},$$

$$GaitVector_{(rit,fused)} = \frac{GaitVector_{(rit,straight)} + GaitVector_{(rit,bag)} + GaitVector_{(rit,coat)}}{3}.$$

Subsequently, biohash is applied to the two mean feature vectors, in order to generate two different enrollment bitstreams denoted $Ebits_{(cit,\ fusion)}$ and $Ebits_{(rit,\ fusion)}$, respectively, which are stored in the enrollment database. The computation of the enrollment bitstreams is performed as follows:

$$Ebits_{(cit,fusion)} = BioHash(GaitVector_{(cit,fused)}),$$

$$Ebits_{(rit,fusion)} = BioHash\left(GaitVector_{(rit,fused)}\right).$$

Similarly to the first scheme, in the authentication procedure, the silhouette G of the user can be one of the three types that were captured in the enrollment procedure (i.e., straight, coat, bag). First, the CIT and RIT transformations are applied to extract two gait feature vectors (i.e., one from CIT and one from RIT). As previously, using the user's token and the gait features vectors, biohash is applied to generate two different authentication bitstreams $Abits_{(cit)}$ and $Abits_{(rit)}$. Next, the hamming distance between the authentication and the enrollment bitstreams is computed, separately, for each transformation. After that, the final score named FinalResult is computed, which is the sum of the two previsouly computed hamming distances. That is:

$$FinalResult = HDistance\left(Ebits_{(cit,fusion)},\ Abits_{(cit)}\right) + HDistance\left(Ebits_{(rit,fusion)},\ Abits_{(rit)}\right)$$

4.3 Experiments and numerical results

In this section, we evaluate the authentication performance of the two enrollment and authentication schemes. To this end, we have implemented in C++ programming language the following software modules: i) the CIT and RIT transformation algorithms, ii) the biohash algorithm, and iii) the above two enrollment and authentication schemes. In the carried out experiments, we captured silhouettes of 75 subjects (i.e., users). Three different human silhouette categories were considered: a) straight, b) coat, and, c) bag. The relative position of the camera and the subject was vertical. Thus, the angle of the direction of the camera and the face of the subject was 90 degrees.

The evaluation of the two schemes is performed by computing the genuine and impostor distributions. More specifically, to investigate the authentication performance of the proposed scheme, we classify the users as: a) genuine and b) impostors. Let user A be a genuine user with a token denoted as TRN_A, while his/her biometric data is denoted as $GAIT_A$. Assume now that an impostor has his/her own biometric data $GAIT_{impostor}$ and his/her own token $TRN_{impostor}$. The goal of the impostor is to be authenticated as user A. We identify three different attack scenarios for the impostor: i) a type 1 impostor uses his own biometric data $GAIT_{impostor}$ and his own $TRN_{impostor}$; ii) a type 2 impostor has stolen and uses user's A token TRN_A but uses his/her own biometric data $GAIT_{impostor}$; and iii) a type 3 impostor has stolen and uses the biometric data of user A $GAIT_A$ and uses his/her own $TRN_{impostor}$. Impostors of type 1 are weaker (in terms of probability of successful authentication as genuine users) than impostors of type 2 and 3, since they do not possess any authentication credential (token or gait features). It is evident that in case that an impostor possesses both gait features and the token of a valid user, then he/she can be successfully authenticated as a genuine user.

Figure 2 shows the genuine and impostor distributions for the first scheme (recall that the straight silhouette has been selected to enroll gait

features). Note that since the genuine bag and coat distributions had exactly the same curves they are presented as one curve named genuine bag/coat. The same applies also for type 1 and 3 impostors distributions and, therefore, their curves are represented by a single one named type 1/3. Figure 2 shows that the type 1/3 impostors are clearly separated (i.e., no overlap) from the genuine distributions, which means that the 1st scheme achieves EER=FAR=FFR=0%. We also observe that the genuine straight distributions have a very small overlap with type 2 impostors. We have estimated that the EER value for type 2 impostors and genuine straight is equal to 9%. However, it can be deduced from figure 2 that genuine bag/coat distributions overlap greatly with type 2 impostor distribution, which means that the system cannot distinguish them. As a matter of fact, we have derived the EER value equal to 34% for type 2 impostors and genuine bag/coat, which is considerably high and unacceptable.

It is worth noting that we repeated the experiments using this time gait features extracted from a bag silhouette as enrollment. Again, the same distribution behavior was observed with the difference that this time genuine bag distributions had a small overlap with type 2 impostors, while straight/coat curves overlapped greatly with type 2 impostors. In this case, the Type 2 EER value was derived equal to 33%. Note that similar results we observed using a coat silhouette as enrollment. From the above analysis, we deduce the following observation:

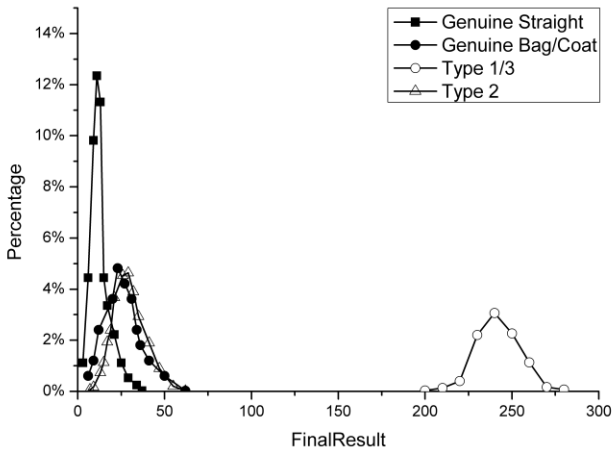

Figure 2. Distributions of the FinalResult values of the first scheme for genuine users and impostors.

Observation 1: *Gait features that are extracted from the same user are similar only when they are extracted from the same silhouette type. On the contrary, gait features that are extracted from different silhouette types of the same user have great differences.*

The above observation indicates that if, for example, we use enrollment templates generated from a straight silhouette type, then a valid user may be rejected if his/her authentication templates are generated from bag or coat types. Similarly, if we use gait features extracted from bag silhouette as enrollment template, then a valid user may be rejected, if the silhouette type for authentication is straight or coat. This happens because when the enrollment and authentication templates (i.e., gait features) are generated from different silhouette types, the extracted gait vectors differ significantly, due to distortions that are caused by the different captured silhouette type. The above leads to the more generic observation:

Observation 2: *If we use enrollment templates only from one silhouette type, then the authentication performance is significantly deteriorated.*

Figure 3 shows the genuine and impostor distributions for the second enrollment and authentication scheme. First, we observed that all three genuine silhouette types had exactly the same distribution curve. For this reason, figure 3 shows one genuine distribution curve that represents all silhouette types. It is observed again that the type 1/3 and genuine distributions are clearly separated and thus EER=FAR=FFR=0% is achieved for these types of impostors. On the other hand, the type 2 impostor distribution overlaps almost entirely with the genuine one, resulting in a very high EER value equal to 45% for type 2 impostors. This means that if we use feature fusion at the enrollment phase, the authentication performance is worse than the first scheme for all silhouette types.

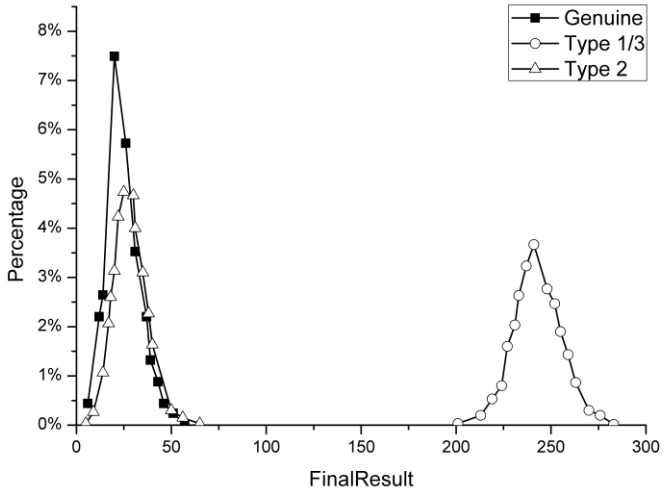

Figure 3. Distributions of the FinalResult values of the second scheme for genuine users and impostors.

From the above analysis, we deduce the following observation:

Observation 3: *Feature-level fusion has adverse impact on the authentication performance.*

5 Gaithashing

In this section, we describe the final enrollment and authentication scheme called *gaithashing* that yields the best numerical results. Unlike the previous two schemes that enroll only one feature gait vector (i.e., from a specific type of silhouette or fused), gaithashing enrolls separately gait feature vectors from all the three considered human silhouette types. Moreover, in the authentication process of gaithashing, the new extracted gait features are fused with each one of the enrollment templates, using weighted sums. By selecting appropriate weight values, gaithashing performs comparison between gait features of the same silhouette type, in order to increase the authentication performance and avoid the pitfalls of the previously mentioned schemes.

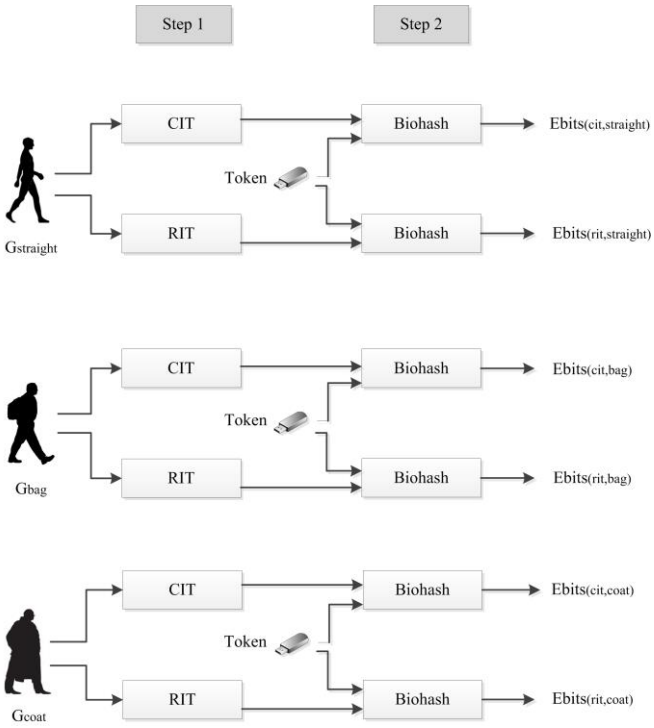

Figure 4: Gaithashing enrollment procedure

Algorithm 1: Enrollment Algorithm

Input: Three gait silhouettes ($G_{straight}$, G_{bag}, G_{coat}), Token

Output: Six enrollment Bitstreams ($Ebits_{(cit,straight)}$, $Ebits_{(cit,bag)}$, $Ebits_{(cit,coat)}$, $Ebits_{(rit,straight)}$, $Ebits_{(rit,bag)}$, $Ebits_{(rit,coat)}$)

1: $Categories = \{straight, bag, coat\}$
2: **for** i *in* $Categories$ **do**
3: $GaitVector_{(cit,i)} = CIT\_Transformation(G_{(i)})$;
4: $GaitVector_{(rit,i)} = RIT\_Transformation(G_{(i)})$;
5: $Ebits_{(cit,i)} = Biohash(GaitVector_{(cit,i)}, Token)$;
6: $Ebits_{(rit,i)} = Biohash(GaitVector_{(rit,i)}, Token)$;
7: **end**

Figure 5: Gaithashing enrollment algorithm

More specifically, as shown in Figure 4, the first step of the enrollment procedure in gaithashing is to capture the aforementioned three distinct silhouettes of the user: a) straight $G_{straight}$, b) coat G_{coat}, and, iii) bag G_{bag}. Next, the CIT and RIT transformations are applied, separately, to each one of the three silhouettes of the user to extract the gait features. In this way, in total, six different gait features are extracted: three from the CIT transformation and three from RIT. In the second step, biohash is applied to each one of the six gait features using the token of the user, generating six different enrollment bitstreams. That is, three enrollment bitstreams for the CIT transformation $Ebits_{(cit,straight)}$, $Ebits_{(cit,bag)}$, $Ebits_{(cit,coat)}$, and three enrollment bitstreams for RIT $Ebits_{(rit,straight)}$, $Ebits_{(rit,bag)}$, $Ebits_{(rit,coat)}$, which are stored in the enrollment database. The algorithm of the enrollment procedure is presented in figure 5.

The authentication procedure includes four distinct steps. Note that in the authentication procedure, the silhouette G of the user can *be one of the three types that were captured in the enrollment procedure (i.e., straight, coat, bag)*. In the first step, the CIT and RIT transformation are applied to extract two different gait features (i.e., one from CIT and one from RIT). In the second step, using the user's token and the extracted features, biohash is applied to generate two different authentication bitstreams $Abits_{(cit)}$ and $Abits_{(rit)}$. During the third step, the authentication and the enrollment bitstreams are compared and fused, separately, for each transformation to produce the intermediate scores CitSum and RitSum (i.e., first-level fusion as shown in figure 6). Finally, in the fourth step, the CitSum and RitSum are fused (i.e., second-level fusion as shown in figure 6) to generate the final score named as FinalResult. At this point, the user is accepted if FinalResult is less than a predetermined threshold; otherwise he/she is rejected. As mentioned below, the first and second level fusions are based on weighted sums. The exact values of the employed weights as well as the predetermined threshold are derived experimentally (see section 6.1), maximizing the authentication performance.

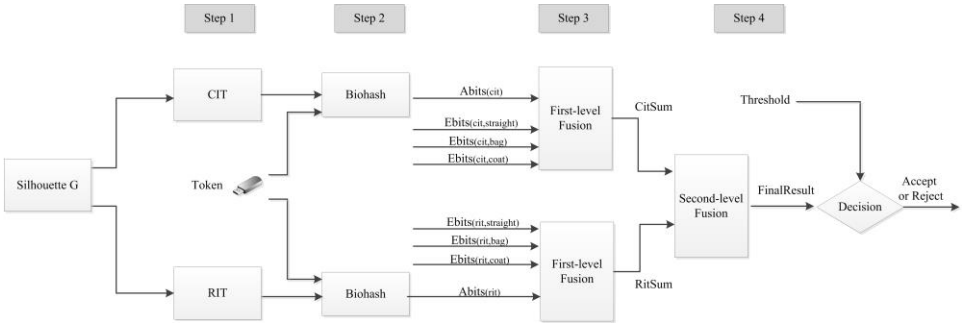

Figure 6: Gaithashing authentication procedure

5.1 First-level fusion

The first-level fusion module is invoked in the authentication procedure, right after the generation of the authentication bitstreams. This module, calculates the hamming distances between each authentication and enrollment bitstream of the user. Note that the hamming distance

represents the number of different bits between two bitstreams. In total, three hamming distances are computed for each transformation (CIT and RIT) as follows:

$$Score_{(cit,straight)} = HDistance\left(Ebits_{(cit,straight)}, Abits_{(cit)}\right),$$
$$Score_{(cit,bag)} = HDistance\left(Ebits_{(cit,bag)}, Abits_{(cit)}\right),$$
$$Score_{(cit,coat)} = HDistance\left(Ebits_{(cit,coat)}, Abits_{(cit)}\right).$$

and

$$Score_{(rit,straight)} = HDistance\left(Ebits_{(rit,straight)}, Abits_{(rit)}\right),$$
$$Score_{(rit,bag)} = HDistance\left(Ebits_{(rit,bag)}, Abits_{(rit)}\right),$$
$$Score_{(rit,coat)} = HDistance(Ebits_{(rit,coat)}, Abits_{(rit)}).$$

A small hamming distance value between the authentication and enrollment bitstreams means that the compared bitstreams are similar. On the contrary, a high hamming distance value means that the compared bitstreams are different and they do not share similarities.

Since the user's silhouette type should match with one of the three enrollment types, it is evident that one of the previously generated scores from the RIT transformation and one from CIT have small hamming distance values (see observation 1), while the remaining scores have high hamming distance. Let X_1 be the minimum between the three scores of CIT, that is,

$$X_1 = Min(Score_{(cit,straight)}, Score_{(cit,bag)}, Score_{(cit,coat)}),$$

and X_2, X_3 the remaining two scores. Similarly, we assign Y_1 the minimum between the three scores of RIT:

$$Y_1 = Min\left(Score_{(rit,straight)}, Score_{(rit,bag)}, Score_{(rit,coat)}\right),$$

and Y_2, Y_3 the remaining two scores. In essence, X_1 and Y_1 represent the hamming distance between authentication and enrollment bitstreams of the same silhouette type, while X_2, X_3 and Y_2,Y_3 represent the hamming distance between authentication and enrollment bitstreams of different silhouette types. In other words, the values of X_2, X_3 and Y_2,Y_3 are considered to be noise. At this point, the first-level fusion module fuses the hamming distances of each transformation using weighted sums and generates two intermediate scores, CitSum and RitSum such as:

$$CitSum = \alpha_1 * X_1 + \alpha_2 * X_2 + \alpha_3 * X_3,$$
$$RitSum = b_1 * Y_1 + b_2 * Y_2 + b_3 * Y_3,$$

where $\alpha_1, \alpha_2, \alpha_3$ and b_1, b_2, b_3 are weight values such as $\alpha_1 > \alpha_2, \alpha_3$ and $b_1 > b_2, b_3$,while it is $\alpha_1 + \alpha_2 + \alpha_3 = 1$ and $b_1 + b_2 + b_3 = 1$. Note that the impact of X_1 and Y_1 on the value of CitSum and RitSum respectively is greater than the other scores. This happens because their corresponding weight values (i.e., α_1 and b_1) are greater than the other weight values. In this way, the noise introduced by X_2, X_3 and Y_2,Y_3 do not affect, significantly, the value of CitSum and RitSum.

5.2 Second-level fusion and decision

In this step, first a final score (denoted as FinalResult) is computed by fusing the CitSum and RitSum values, using weighted sums such as:

$$FinalResult = w_1 * CitSum + w_2 * RitSum,$$

where w_1 and w_2 are weights such as $w_1 + w_2 = 1$. Finally, the user is accepted or rejected based on the following simple rule: If FinalResult is less than a predetermined threshold, then the user is authenticated successfully; otherwise the user is rejected. The algorithm of the authentication procedure is presented in figure 7.

Algorithm 2: Authentication Algorithm

Input: An authentication gait silhouette (G), Six Enrollment Bitstreams, Token, Threshold.
Output: Acceptance or rejection of the user.

$Categories = \{straight, bag, coat\}$
$GaitVector_{(cit)} = CIT\_Transformation(G)$;
$GaitVector_{(rit)} = RIT\_Transformation(G)$;
$Abits_{(cit)} = Biohash(GaitVector_{(cit)}, Token)$;
$Abits_{(rit)} = Biohash(GaitVector_{(rit)}, Token)$;
for i *in Categories* **do**
  $Score_{(cit,i)} = HDistance(Ebits_{(cit,i)}, Abits_{(cit)})$;
  $Score_{(rit,i)} = HDistance(Ebits_{(rit,i)}, Abits_{(rit)})$;
end
$X_1 = Min(Score_{(cit,straight)}, Score_{(cit,bag)}, Score_{(cit,coat)})$ and X_2, X3 the remaining two scores;
$Y_1 = Min(Score_{(rit,straight)}, Score_{(rit,bag)}, Score_{(rit,coat)})$ and Y_2, Y3 the remaining two scores;
$CitSum = \alpha_1 * X_1 + \alpha_2 * X_2 + \alpha_3 * X_3$;
$RitSum = b_1 * Y_1 + b_2 * Y_2 + b_3 * Y_3$;
$FinalResult = w_1 * CitSum + w_2 * RitSum$;
if $FinalResult < Threshold$ **then**
  User is accepted;
else
  User is rejected;
end

Figure 7: Gaithashing authentication algorithm

6 Evaluation of the proposed scheme

6.1 Authentication performance

To evaluate the authentication performance of the proposed scheme, we have implemented the two-level fusion and decision algorithm of gaithashing. The parameters of the carried out experiments are the same as in section 4.3. That is, three different human silhouette categories were considered: a) straight, b) coat, and, c) bag. Moreover, we classify the users as: a) genuine and b) impostors. We identify three different attack scenarios for the impostor: i) a type 1 impostor uses his own biometric data and his/her own token; ii) a type 2 impostor has stolen and uses a valid token of a genuine user but uses his/her own biometric data; and iii)

a type 3 impostor has stolen and uses the biometric data of a genuine user but uses his/her own token.

We have conducted two set of experiments. The aim of the first set is to derive the distributions of the FinalResult values for both genuine users and impostors (all three types). The FinalResult is the most important parameter in the proposed scheme, since the authentication of a user is based on its value. By investigating the distribution of FinalResult values, we gain insights for the behavior of the gaithashing scheme and whether it can distinguish impostors from genuine users. In the second set of experiments, the goal is to estimate the FAR, FRR and EER values. As mentioned previously (see section 2.1), FAR represents the probability that the authentication system will incorrectly accept an authentication attempt by an impostor, whereas FRR represents the probability that the authentication system will incorrectly reject an authentication attempt by a genuine user. This experiment allows us to estimate an appropriate threshold value that can minimize both FAR and FRR, at the same time.

In the carried out experiments, the values of weights were set as follows: $\alpha_1 = b_1 = 0.5, \alpha_2 = b_2 = 0.25, \alpha_3 = b_3 = 0.25$ (first-level fusion) and $w_1 = 0.4$, $w_2 = 0.6$ (second-level fusion). As we analyze below, these values were selected after trying various combinations and experiments, in order to achieve the best authentication performance (i.e., minimize the EER value).

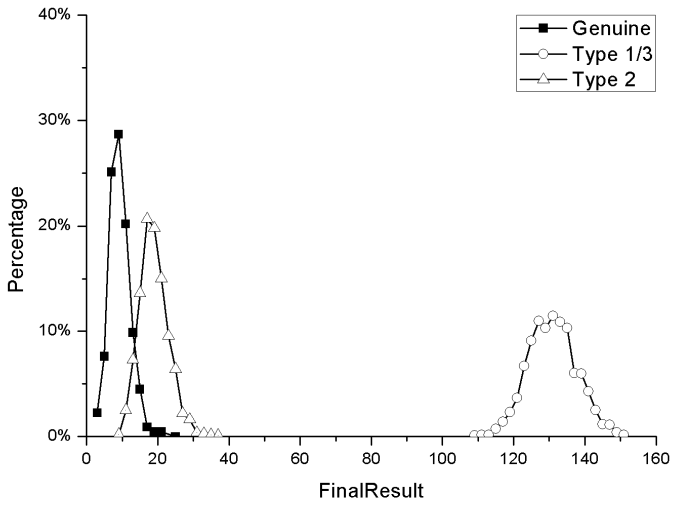

Figure 8: Distributions of the FinalResult values of gaithashing for genuine users and three impostor types

Figure 8 shows the distribution of the FinalResult values for both impostors 1, 2, 3 and genuine users. Note that the distributions of impostors type 1 and 3 were identical and are presented in one curve. It is observed that the FinalResult values of type 1 and type 3 impostors is considerably higher than the genuine. In fact, the highest value of FinalResult for genuine users is 25, while the values of FinalResult for impostors type 1/3 begins at 110. As a result, the distribution curves of the genuine users and type 1/3 impostors do not overlap at all. This means

that gaithashing can always distinguish between impostors type 1/3 and genuine users. In other words, an impostor of type 1 and 3 cannot be authenticated as genuine user. For example, if we set the threshold value equal to 60, then the FinalResult value for all genuine users is less than the threshold value, while all impostors of type 1 and 3 have FinalResult value higher than the threshold, which means that they will be rejected. On the other hand, we observe that the type 2 impostor distribution marginally overlaps with the genuine one. The intersection area of the two curves (i.e., genuine and impostor type 2 distribution) begins for FinalResult equal to 10 and ends for FinalResult equal to 25. In this area, gaithashing cannot distinguish between genuine users and type 2 impostors, since they share the same FinalResult values. The above results indicate that depending on the value of the selected threshold, an impostor type 2 may be authenticated, successfully, as a genuine user or a genuine user may be rejected, incorrectly. For example, if we set threshold equal to 10, then as shown in figure 8, no impostor of type 2 will be accepted. However, a small percentage of genuine users will be rejected, because their FinalResult value is greater than the threshold.

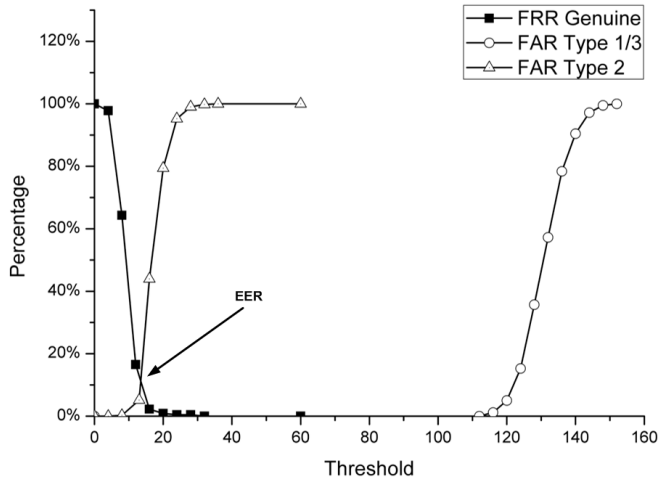

Figure 9: Gaithashing FRR-FAR values as functions of the threshold value

To quantify and investigate further the authentication performance of gaithashing, we have estimated the FAR and FRR values, as a function of threshold values (see figure 9). As expected, the value of FRR decreases, as the threshold increases. On the other hand, the values of FAR for the three impostors types increases as the threshold increases. Thus, the value of the threshold regulates a tradeoff between FAR and FRR. A small threshold value may minimize FAR, but the FRR may be very high. On the contrary, a high threshold value may minimize FRR, but the value of FAR can be very high. For this reason, we have to estimate the EER value (see section 2.1), where the FAR and FRR are equal (i.e., EER=FAR=FRR). Evidently, the value of EER should be as low as possible, since a low value of EER entails a low value of FAR and FRR. This value can be easily estimated, since it is the intersection point of the FAR and FRR curves. Thus, as shown in figure 9, for impostors of type 2, the EER equals to 10.8% which is obtained for threshold value equal to

14. This means that if we set the threshold equal to 14, then for 100 authentication attempts, the proposed scheme presents in total 10 false rejections of a genuine user or false acceptance of a type 2 impostor. Moreover, the EER for impostors of type 1/3 is equal to 0%, since the FRR and FAR curves do not intersect. This means that gaithashing is able to always detect type 1/3 impostors. Thus, we can deduce that the proposed scheme attains very high performance for all impostor scenarios, while false alarms are kept to minimal.

It is important to mention that the employed weight values for the first and second level fusion play a key role in the performance of gaithashing. These were derived after a fine tuning procedure in which we performed several trials in order to minimize the EER value. More specifically, table 2 shows various weight values that we tested and the corresponding EER value for impostors of type 2 (note that the EER value for impostors type 1/3 was equal to 0% independently of weight values). Recall that $\alpha_1 > \alpha_2, \alpha_3$ and $b_1 > b_2, b_3$, while it is $\alpha_1 + \alpha_2 + \alpha_3 = 1$, $b_1 + b_2 + b_3 = 1$ and $w_1 + w_2 = 1$. First, we randomly selected weights values for the first-level fusion, while the weights for the second level fusion were constant and equal to $w_1 = w_2 = 0.5$. Initially, we tested the following weight values: $\alpha_1 = 0.5$, $\alpha_2 = \alpha_3 = 0.25$ and $b_1 = 0.5$, $b_2 = b_3 = 0.25$, (1^{st} trial). Numerical results showed that gaithashing achieved EER=11.4%. Next, in the 2^{nd} trial we increased the values of α_1 (i.e., $\alpha_1 = 0.6$) and b_1 (i.e., $b_1 = 0.6$) and we observed that the EER value increased (i.e., EER=13.2%), which was not acceptable. In the third trial we increased only the value of α_1 (i.e., $\alpha_1 = 0.6$), while b_1 was equal to its initial value (i.e., $b_1 = 0.5$). Again, we observed that the value of EER was higher compared to the first trial (i.e., EER=12.5%). In the fourth trial, we reduced α_1 (i.e., $\alpha_1 = 0.4$) and b_1 (i.e., $b_1 = 0.4$). We observed that the value of EER did not modified, significantly, but it was higher than the first trial (i.e., EER=13.2%).

Table 2: Gaithashing tested weight values and corresponding EER of type 2 impostors

Trials	α_1	α_2, α_3	b_1	b_2, b_3	w_1	w_2	**EER**
1	0.5	0.25	0.5	0.25	0.5	0.5	11.4%
2	0.6	0.2	0.6	0.2	0.5	0.5	13.2%
3	0.6	0.2	0.5	0.25	0.5	0.5	12.5%
4	0.4	0.3	0.4	0.3	0.5	0.5	13.2%
5	0.5	0.25	0.5	0.25	0.6	0.4	11.6%
6	0.5	0.25	0.5	0.25	0.4	0.6	10.8%

Next, we modified the weight values of the second level fusion w_1 and w_2, while the weight values of the first-level fusion are constant and equal to the first trial. As shown in table 2, in the 5^{th} trial we assigned $w_1 = 0.6$ and $w_2 = 0.4$ and observed that the value of EER was not significantly modified, compared to the first trial (i.e., EER=11.6%). In the 6^{th} trial, we selected $w_1 = 0.4$ and $w_2 = 0.6$. This time we observed that the value of EER was decreased, compared to the first trial and it was equal to 10.8%. Although we performed several other trials, the value of EER was not reduced further. Thus, we concluded that the weight values of the sixth trial should be selected in order to achieve the minimum EER value (i.e., EER=10.8%).

Apart from the aforementioned experiments, it is important to mention that we tried to further improve the EER value of gaithashing for type 2 impostors, using decision based fusion. In particular, we have implemented a scheme that performs two-level fusion. The first-level fusion is identical with gaithashing. That is, the hamming distances between each authentication and enrollment bitstreams of the subject are calculated and the CitSum and RitSum are derived using weights. In the second-level fusion, the CitSum and RitSum values are compared to two pre-defined thresholds (i.e., $\text{Threshold}_{\text{cit}}$ and $\text{Threshold}_{\text{rit}}$ respectively) to derive a binary decision (i.e., TRUE or FALSE). That is:

$$CitAuth = \begin{cases} TRUE, if\ CitSum < Threshold_{cit} \\ FALSE, if\ CitSum \geq Threhold_{cit} \end{cases}$$

$$RitAuth = \begin{cases} TRUE, if\ RitSum < Threshold_{rit} \\ FALSE, if\ RitSum \geq Threhold_{rit} \end{cases}$$

The final result denoted as FinalAuth is calculated by performing a decision-level fusion using the AND or OR logical rules. In particular, using the OR logical rule, a user is successfully authenticated if either the CitAuth or RitAuth value is TRUE, whereas using the AND rule, both CitAuth and RitAuth values should be TRUE. To obtain numerical results (i.e., EER), we tested various values for the $\text{Threshold}_{\text{cit}}$ and $\text{Threshold}_{\text{rit}}$. The lowest EER values that we achieved for type 2 impostors were equal to 48% and 19% for the OR and AND rules respectively. On the other hand, as we mentioned previously gaitashing achieved EER =10.8%. Thus, it is evident that the decision based fusion approach does not improve the EER of gaithashing and as a matter of fact, it deteriorates the authentication performance [41].

To summarize, the EER values of the three proposed schemes are shown in Table 3. We conclude that all schemes achieve 0% EER for both Type 1 and 3 impostors. However, for type 2 impostors, we obtained EER = 34% for straight silhouette enrollment, as well as 27% and 32% for coat and bag enrollment respectively. Moreover, in the second scheme the EER was equal to 45%. However, the third scheme achieves EER = 10.8%, which is a significant improvement over the previous two schemes. This result means that for every 100 authentication attempts, the third scheme has in average 10 false acceptances of type 2 impostors and 10 false rejections of genuine users.

Table 3: EER values of the three proposed schemes

Impostors type	**1st scheme**	**2nd scheme**	**3rd scheme (Gaithashing)**
Type 1	0%	0%	0%
Type 2	34% straight enrollment 27% coat enrollment 32% bag enrollment	45%	10.8%
Type 3	0%	0%	0%

Apart from the fusion techniques, there are some other methods that could

possibly improve the authentication performance of the system. In particular:

a) Use of multiple feature extraction algorithms: Apart from CIT and RIT transformation algorithms, we can extract gait features using other feature extraction algorithms proposed in the literature (such as the ones presented in [11] and [15]). As a matter of fact, we can use multiple extraction algorithms to extract multiple gait features for the same user. Since different algorithms capture different characteristics of a human silhouette, we can enroll all extracted features and perform a feature-level fusion, in order to improve the authentication performance. The negative side effect of this approach is that it increases the overall complexity as well as the processing and storage overhead, due to the extraction and enrollment of several gait features for each user.

b) Use of multi-modal biometrics: The ISO/IEC standards propose the use of multiple biometric features (i.e., also named as multi-modal biometrics), in order to overcome the limitations imposed by uni-modal biometric systems [42]. In general, multi-modal biometric systems are considered to be more reliable and robust to attacks [43], since an impostor should compromise two or more biometric features of a genuine user. In the proposed gaithashing system, gait features can be combined with face or iris or any other biometric modality to create a feature vector for the user. The downside of this approach is that the proposed system will inherit the usability issues of the other biometric modalities. That is, gait is the only biometric modality that provides unconstructive access control and authentication at-a-distance. All other biometric modalities (including fingerprints, iris, face) have several usability issues (see section 6.2). Therefore, on the one, hand multimodal biometrics may improve the EER results, but on the other hand it will reduce the usability of the system.

c) Use of multiple sensors: Another improvement in the authentication performance may be achieved by using multiple sensors. That is, we can use different cameras to capture the human silhouette of a user and obtain multiple gait features (each one derived from a different camera) that can be used for enrollment. However, we have to notice that the use of multiple cameras may cause deployment issues and increase the overall cost.

6.2 Comparison of gaithashing to previous works

In this section, we compare the authentication performance of gaithashing to state-of-the-art template protection schemes. Recall that the proposed gaithashing is a cancellable biometric scheme (see section 2.1), based on the biohash algorithm to secure gait features. To this end, we compare gaithashing to: i) schemes that secure gait features, based on other algorithms than biohash; ii) schemes that secure biometric features other than gait, based on the biohash algorithm, and, iii) schemes that secure other biometric features (not gait), based on other two-factor authentications (i.e., not biohash). Note that to perform this comparative analysis, we present only the numerical results (i.e., EER values) of the

previous schemes. The detailed analysis of the exact algorithms employed in the previous schemes is omitted, since it is out of the scope of the paper.

Table 4: EER values of gaithashing and previous schemes that secure gait features

Authors	EER
T. Hoang and D. Choi [4]	7.84% for key size 50 bits 16.9% for key size 55 bits
S. Argyropoulos et al. [1]	6% for straight 20% for bag 30% for coat
Gaithashing	10.8% for type 2 impostors 0% for type 1/3 impostors

Table 4 compares the EER values between the proposed scheme and previous schemes that secure gait features. Note that since these schemes are single-factor authentication (and not two-factor authentication like gaithashing), they estimate EER values considering one impostor type (i.e., a user that tries to be authenticated using his/her biometrics). The scheme presented in [4] applies fuzzy commitment to secure gait features using a cryptographic key. The authors have estimated the EER values of their scheme as a function of the cryptographic key size. On the other hand, gaithashing does not rely on cryptographic keys to secure gait features. As mentioned in [4], for a key size 50 bits, the scheme achieves EER equal to 7.84%. It is evident, that although EER is lower than gaithashing, it cannot provide adequate security, due to very small key size. Even worse, as the key size increases, then EER also increases. That is, for key size of 55 bits the EER value becomes 16.9%, which is significantly higher than 10.8% of our proposed scheme. Moreover, the work in [1] uses channel coding approach to secure gait features, achieving a very low value for EER, only, in the case of straight silhouette (i.e., 6%). On other hand, the EER values are unacceptably high for bag and coat silhouette types (i.e., 20% and 30% respectively). On the contrary, the performance of gaithashing and the EER value are independent of the silhouette type. This can be attributed to the fact that gaithashing uses all possible silhouette types for enrollment, while in the authentication procedure the proposed scheme performs score-level fusion, using weighted sums to compare gait features between the same silhouette type. In this way, gaithashing ensures that genuine users are authenticated successfully, independently of their sillouette type. Another reason that gaithashing yields these remarkable results is related to the fact that the proposed scheme inherits the recognition capabilities of the biohash algorithm. That is, by mixing the random numbers generated by the user's token with gait features [18], gaithashing is capable of preserving the biometric intra-class variations (i.e., variation in the gait features between the same user), while at the same time enhances the biometric inter-class variations (i.e., variations in the gait features of different users).

Moreover, compared to the previous schemes [1] and [4] of table 4, gaithashing protects the enrollment bitstreams in the sense that an attacker, even if he/she is able to access the database, it cannot revert the bitstreams back to gait features. This happens because the generated

bitstreams are non-invertible, due to mathematics properties of the biohash algorithm [18]. Moreover, gaithashing provides unlinkability, meaning that an attacker cannot cross-match enrollment bitstreams of the same user, which are used in different authentication systems (assuming that the user is using a different token between authentication systems). Last but not least, in case of a database compromise, gaithashing provides a simple yet effective way to revoke the enrollment bitstreams. That is, the users should replace their tokens with new ones, in order to generate new enrollment bitstreams.

Table 5: EER values of gaithashing and previous schemes that apply biohash to secure other biometric modalities (not gait).

Authors	**Biometric Modality**	**EER- Type 1 Impostor**	**EER - Type 2 Impostor**	**EER - Type 3 Impostor**
A. Teoh et al. [20]	Face	0%	1.77%	0%
A. Jin et al. [26]	Face	0%	Not considered	Not considered
D. Ling et al. [25]	Face	0%	Not considered	Not considered
T. Connie et al. [2]	Palmprint	0%	Not considered	Not considered
L. Hengjian et al. [24]	Palmprint	0%	Not considered	Not considered
A. T. B. Jin et al. [10]	Fingerprint	0%	Not considered	Not considered
A. Teoh et al. [27]	Fingerprint	0%	2.39%	0.23%
A. Lumini and L. Nanni [13]	Face Fingerprint	0% 0%	2.4% 6.8%	0% 0%
Gaithashing	Gait	0%	10.80%	0%

Table 5 compares the EER values of gaithashing with a representative set of previous biometric template protection schemes that apply the biohash algorithm (or some modified version of biohash) to: i) face, ii) palmprints, and, iii) fingerprints. To the best of our knowledge, there is no previous work that applies biohash to gait features. As we notice in table 5, the majority of previous works (i.e., [26], [25], [2], [24], [10]) consider only type 1 impostors and overlooks to take into account type 2 and 3 impostors. Thus, the presented EER results of these schemes may be very low for type 1 impostors (in fact they achieve EER=0%), but they do not provide complete and realistic views of the overall authentication performance, since numerical results of EER for type 2 and 3 impostors are missing. On the other hand, the proposed solutions in [20], [27] and [13] have considered type 2 and 3 impostors in their numerical results. As a matter of fact, their EER are lower than gaithashing. This is attributed to the fact that the previous works (i.e., [20], [27] and [13]) have significantly enhanced the initial biohash algorithm (as described in [10]) by using advanced binarization techniques that may improve the authentication performance, but at the same time increase the overall complexity of the system. Moreover, some of these previous works (e.g., [13]) do not analyze possible security implications of their binarization techniques. On the other hand, the aim of the proposed gaithashing is to achieve a relatively low EER value in a simple but effective manner by focusing on fusion techniques. However, we mention that gaithashing can

be easily modified to adopt advanced binarization techniques to further reduce the EER values.

Table 6: EER values of gaithashing and other protection schemes that are based on two-factor authentication (not biohash) to secure other biometric modalities (not gait)

Authors	Biometric Modality	EER - Type 1 Impostor	EER - Type 2 Impostor	EER - Type 3 Impostor
P. Färberböck et al. [33]	Iris	2.6%	Not considered	Not considered
C. Rathgeb and A. Uhl [34]	Iris	0.25%	Not considered	Not considered
O. Ouda et al. [35]	Iris	2.3%	Not considered	Not considered
E. Anzaku, et al. [36]	Fingerprint	0.31%	Not considered	Not considered
C. Karabat and H. Erdogan [37]	Face	0,145%	11.85%	Not considered
J. Zhe et al. [38]	Fingerprint	0.20%	10%	Not considered
W. Song and H. Jiankun [39]	Fingerprint	0%	Variable (3.5% - 7.5%)	Not considered
J. Zhe et al. [40]	Fingerprint	0%	Variable (1.33% - 24.71%)	0%
Gaithashing	Gait	0%	10.8%	0%

Finally, we compare gaithashing to other protection schemes that are based on two-factor authentication (not biohash) to secure other biometric features (not gait) (see table 6). Note that the EER results of schemes [39] and [40] are variable, because they have used multiple datasets to evaluate their performance and derive results. From table 6 we observe again that the majority of the previous schemes (i.e., [33], [34], [35], [36]) erroneously do not take into account type 2 and 3 impostors and estimate EER values, only, for impostors of type 1. We observe also that even for type 1 impostors, these schemes have higher EER values compared to gaithashing. For instance, in the work of [33] the EER value for type 1 impostors is equal to 2.6%. Moreover, we observe that the schemes of [37] and [38], which take into account impostors of type 2 (but not type 3), present almost the same or higher EER values (11.85% and 10% respectively). Finally, the schemes of [39] and [40] have variable EER values for type 2 impostors and their minimum EER is lower than our proposed gaithashing (i.e., 3.5%, and 1.33% respectively). On the other hand, the maximum EER value of [40] is considerably higher than gaithashing (i.e., 24.71%), while in [39] the maximum EER value is equal to 7.5%, which is little lower than our proposed gaithashing.

Unlike the previous schemes of Table 5 and 6 that secure biometric features such as fingerprints, face and palmprints, the proposed gaithashing specifically focus on securing gait features, which offer significant advantages compared to the other biometric features. Generally speaking, gait features have some unique characteristics that make them suitable for various applications, such as non-invasive physical access control, covert security, and visual surveillance. In particular, gait is the

only biometric modality that provides *unobtrusive identification at a distance*, so that unauthorized or suspicious persons can be remotely recognized when they enter a surveillance area. Moreover, most biometrics features including iris, face, and fingerprint require specialized and expensive scanners, in order to extract high-resolution images to achieve an acceptable recognition performance [29]. On the other hand, gait features can be captured using off-the-shelf camcorders [31]. As a matter of fact, gait features extraction can be performed even with mobile devices using their accelerometer and gyroscope sensors [28]. In [32] an Android application is developed that captures gait features, using accelerometer sensors, which are commonly found in the majority of today's smartphones and tablets. On the other hand, the extraction of other biometric features using mobile devices faces some challenging issues. For instance, fingerprint scanner technology in mobile devices (e.g., Apple touch ID [30]) should use large sensors, in order to acquire high quality images and increase accuracy. However, the incorporation of large sensors in mobile devices increases their total cost as well as their thickness [29], which is not desirable by consumers.

Moreover, unlike other biometrics like fingerprint or iris, which require careful and close contact with the scanner, the extraction of gait features does not require much cooperation from the users. It is also worth noting that fingerprints and palmprint scanners tend to be fragile and susceptible to performance degradation over time caused by dust, moisture, and electrostatic discharge. Finally, the performance of fingerprint and palmprint recognition is significantly deteriorated when hands are too moist or oily. On the other hand, gait recognition is in general more robust and it is not affected by environmental or other external factors.

7 Conclusions

This paper proposed gaithashing, a two-factor authentication scheme that secures gait features in an efficient manner. The proposed scheme combines the security features of biohash and the recognition capabilities of gait features to provide a high accuracy authentication system. In gaithashing, a user is authenticated only if he/she possesses a valid token and a valid gait feature. The performance of the gaithashing scheme is evaluated by carrying out two sets of experiments. The obtained numerical results and the carried out evaluation allow us to derive the following generic observations:

- Gaithashing achieves EER=0% for type 1 and 3 impostors (i.e., type 1 impostor uses his/her own gait features and his/her own token, while type 3 impostors use compromised gait features and they own token for authentication). This means that the proposed scheme always detects type 1 and 3 impostors.
- It achieves very high accuracy (EER=10.8%) for type 2 impostors (i.e., an impostor that uses a compromised token and his/her own gait features for authentication).
- Gaithashing addresses the distortions caused when the subject

wears a coat or holds a bag, by enrolling three different types of human silhouettes (i.e., straight, coat, bag). The proposed scheme can be easily extended to take into account other types of human silhouettes (e.g., a user wearing a hat).

- The proposed scheme secures gait features by converting them to non-invertible bitstreams using the biohash algorithm and a user's token.
- Gaithashing provides unlinkability and easy revocability of the gait templates, simply by replacing the user's token with a new one.

8 Acknowledgments

This work was sponsored in part by the project "BIOTAFTOTITA: "Secure and Revocable Biometric Identification for use in Disparate Intelligence Environments", (GSRT 09SYN-72-597) and by the project "SPAGOS: Secure and Privacy-Aware eGovernment Services", (GSRT 11SYN-9-2059), both funded by the Hellenic General Secretariat for Research and Technology (GSRT).

9 References

[1] S. Argyropoulos, D. Tzovaras, D. Ioannidis, and M. Strintzis., "A channel coding approach for human authentication from gait sequences", IEEE Transactions on Information Forensics and Security, Vol. 4, No 3, pp:428-440, Sept. 2009.

[2] T. Connie, A. Teoh, M. Goh, and D. Ngo. "Palmhashing: a novel approach for dual-factor authentication", Pattern Analysis and Applications, Springer, Vol. 7, No. 3, pp:255-268, Sept. 2004.

[3] R. Fuksis, A. Kadikis, and M. Greitans., "Biohashing and fusion of palmprint and palm vein biometric data", IEEE International Conference on Hand-Based Biometrics (ICHB), Hong Kong, Nov. 2011.

[4] T. Hoang and D. Choi., "Secure and privacy enhanced gait authentication on smart phone", Hindawi, The Scientific World Journal, May 2014.

[5] H. Hu. "Multi-view gait recognition based on patch distribution feature and uncorrelated multilinear sparse local discriminant canonical correlation analysis", IEEE Transactions on Circuits and Systems for Video Technology, Vol 24, No 4, pp. 617-630, April 2014.

[6] M. Hu, Y. Wang, Z. Zhang, and Z. Zhang. "Multi-view multi-stance gait identification", 18th IEEE International Conference on Image Processing (ICIP), Brussels, Sept. 2011.

[7] D. Ioannidis, D. Tzovaras, I. G. Damousis, S. Argyropoulos, and K. Moustakas., "Gait recognition using compact feature extraction transforms and depth information", IEEE Transactions on Information Forensics and Security, Vol. 2, No. 3, pp:623-630, Sept. 2007.

[8] ISO/IEC JTC 1/SC 37 - Biometrics.

[9] A. T. B. Jin and T. Connie., "Remarks on biohashing based cancelable biometrics in verification system", Neurocomputing, Eslevier, Vol. 69, No. 16-18, pp:2461- 2464, Oct. 2006.

[10] A. T. B. Jin, D. N. C. Ling, and A. Goh., "Biohashing: two factor authentication featuring fingerprint data and tokenised random number", Pattern Recognition, Elsevier, Vol. 37, No. 11, pp:2245-2255, Nov. 2004.

[11] W. Kusakunniran, Q. Wu, J. Zhang, and H. Li., "Gait recognition across various walking speeds using higher order shape configuration based on a differential composition model", IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics, Vol. 42, No. 6, pp:1654-1668, Nov. 2012.

[12] W. Kusakunniran, Q. Wu, J. Zhang, Y. Ma, and H. Li., "A new view-invariant feature for cross-view gait recognition", IEEE Transactions on Information Forensics and Security, Vol. 8, No. 10, pp:1642-1653, Oct. 2013.

[13] A. Lumini and L. Nanni., "An improved biohashing for human authentication", Pattern Recognition, Elsevier Science, Vol. 40, No. 3, pp:1057-1065, March 2007.

[14] M. McGuire. "An overview of gait analysis and step detection in mobile computing devices", IEEE 4th International Conference on Intelligent Networking and Collaborative Systems (INCoS), Bucharest, Sept 2012.

[15] M. Milovanovic, M. Minovic, and D. Starcevic. "Walking in colors: Human gait recognition using kinect and cbir", IEEE MultiMedia, Vol. 20, No. 4, pp:28-36, Oct./ Dec. 2013.

[16] N. Radha and S. Karthikeyan. "An evaluation of fingerprint security using non-invertible bio-hash", International Journal of Network Security & Its Applications, Vol. 3, No. 4, pp:118-128, July 2011.

[17] C. Rathgeb and A. Uhl. "A survey on biometric cryptosystems and cancelable biometrics", EURASIP Journal on Information Security, pp:1-25, Sept. 2011.

[18] J. Ryu and S. Kamata., "Front view gait recognition using spherical space model with human point clouds", 18th IEEE International Conference on Image Processing (ICIP), Brussels, Sept. 2011.

[19] S. Sivapalan, D. Chen, S. Denman, S. Sridharan, and C. Fookes., "Gait energy volumes and frontal gait recognition using depth images", IEEE International Joint Conference on Biometrics (IJCB), Washington DC, USA, Oct. 2011.

[20] A. B. J. Teoh, Y. W. Kuan, and S. Lee., "Cancellable biometrics and annotations on biohash", Pattern Recognition, Elsevier Science, Vol. 41, No. 6, pp:2034-2044, June 2008.

[21] A. B. J. Teoh and D. C. L. Ngo., "Cancellable biometrics featuring with tokenised random number", Pattern Recognition Letters, Elsevier Science, Vol. 26, No. 10, pp:1454-1460, July 2005.

[22] C. Wang, J. Zhang, L. Wang, J. Pu, and X. Yuan. "Human identification using temporal information preserving gait template", IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 34, No. 11, pp:2164- 2176, Nov. 2012.

[23] R. Arun, G. Rohin, "Feature Level Fusion Using Hand and Face Biometrics", Proceedings of SPIE conference on Biometric Technology for Human Identification II, Vol. 5779, pp:196-204, March 2005.
[24] L. Hengjian, W. Lianhai, "Chaos-Based Cancelable Palmprint Authentication System", International Workshop on Information and Electronics Engineering, China, March 2012.
[25] D. Ngo C. Ling, A. T. B. Jin, A. Goh, "Eigenspace-Based Face Hashing", First International Conference on Biometric Authentication (ICBA 2004), Hong Kong, China, July 2004.
[26] A. T. B. Jin., D. N. C. Ling, and A. Goh, "Personalised cryptographic key generation based on FaceHashing", Computers and Security, Elsever Science, Vol. 23, No. 7, pp: 606-614, Oct. 2004.
[27] A. J. B. Teoh, W. K. Yip, K-A Toh, "Cancellable biometrics and user-dependent multi-state discretization in BioHash", Pattern Analysis and Applications, Springer, Vol. 13, Issue 3, pp: 301-307, Aug. 2010.
[28] H. M. Thang, V. Q. Viet, N. D. Thuc, D. Choi, "Gait identification using accelerometer on mobile phone", International Conference on Control, Automation and Information Sciences (ICCAIS), Vietnam, Nov. 2012.
[29] Wired, "The Trouble With Apple's Touch ID Fingerprint Reader" http://www.wired.com/2013/12/touch-id-issues-and-fixes/
[30] Apple touch ID, http://support.apple.com/kb/HT5883
[31] H. Ng, H.-L Tong, W.-H. Tan, T. T-V. Yap, P-F Chong, J. Abdullah, "Human Identification Based on Extracted Gait Features", International Journal on New Computer Architectures and Their Applications (IJNCAA) Vol. 1, No. 2, pp: 358-370, 2011.
[32] StepRecorder, https://play.google.com/store/apps/details?id=owen.free.steprecorder
[33] P. Färberböck, J. Hämmerle-Uhl, D. Kaaser, E. Pschernig, A. Uhl, "Transforming Rectangular and Polar Iris Images to Enable Cancelable Biometrics", In Proceedings of the 7th international conference on Image Analysis and Recognition, pp: 276-286, June 2010.
[34] C. Rathgeb, A. Uhl, "Two-Factor authentication or how to potentially counterfeit experimental results in biometric systems", In Proceedings of the 7th international conference on Image Analysis and Recognition, pp:296-305, June 2010.
[35] O. Ouda, N. Tsumura, T. Nakaguchi, "Tokenless Cancelable Biometrics Scheme for Protecting Iris Codes", 20th International Conference on Pattern Recognition (ICPR), pp:882,885, Aug. 2010.
[36] E. T Anzaku, S. Hosik, R. Yong-Man, "Multi-Factor Authentication Using Fingerprints and User-Specific Random Projection", 12th International Asia-Pacific Web Conference (APWEB), pp:415-418, Apr. 2010.
[37] C. Karabat, H. Erdogan, "A Cancelable Biometric Hashing for Secure Biometric Verification System," Fifth International

Conference on Intelligent Information Hiding and Multimedia Signal Processing, pp:1082-1085, Sept. 2009

[38] J. Zhe, A. T. B. Jin, S. O Thian., T. Connie, "Secure Minutiae-Based Fingerprint Templates Using Random Triangle Hashing", First International Visual Informatics Conference, (IVIC 2009), Kuala Lumpur, Malaysia, Nov. 2009.

[39] W. Song, H. Jiankun, "Alignment-free cancelable fingerprint template design: A densely infinite-to-one mapping (DITOM) approach", Pattern Recognition, Vol. 45, Issue 12, pp: 4129-4137, Dec. 2012

[40] J. Zhe, L. Meng-Hui, A. T. B. Jin, G. Bok-Min, "A non-invertible Randomized Graph-based Hamming Embedding for generating cancelable fingerprint template", Pattern Recognition Letters, Vol. 42, pp: 137-147, Jun. 2014.

[41] Q. Tao, R. Veldhuis, "Hybrid fusion for biometrics: Combining score-level and decision-level fusion", Computer Visioin and Pattern Recognition Workshops, IEEE Computer Society Conference, pp. 1-6, Jun. 2008

[42] ISO/IEC TR:24722:2007 Information technology – Biometrics – Multimodal and other multibiometric fusion.

[43] Z. Huang, Y. Liu, C. Li, M. Yang, L. Chen, "A robust face and ear based multimodal biometric system using sparse representation", Pattern Recognition, vol. 46,issue 8, pp. 2156-2168, Aug. 2013.