Can Gait Biometrics be Spoofed?*

A. Hadid, M. Ghahramani, V. Kellokumpu, M. Pietikäinen
Center for Machine Vision Research, University of Oulu, Finland

J. Bustard & M. Nixon
School of Electronics and Computer Science, University of Southampton, United Kingdom

Abstract

Gait recognition is a relatively new biometrics and no effort has yet been devoted to studying spoofing attacks against video-based gait recognition systems. Spoofing occurs when a person tries to imitate the clothing and/or walking style of someone else in order to gain illegitimate access and advantages. To gain insight into the performance of current gait biometric systems when confronted to spoofing attacks, we provide in this paper the **first investigation** *in the research literature on how clothing can be used to spoof a target and evaluate the performance of two state-of-the-art recognition methods on a novel gait spoofing database recorded at the University of Southampton. The experiments point out very interesting findings that can be used as a reference for future investigations by the research community.*

1. Introduction

Gait biometrics aims to recognise people from their way of walking. It is a relatively new biometric modality and has a precious advantage over other modalities, such as iris and voice, in that it can be easily captured from a distance. This makes it an attractive option in video surveillance applications. Gait also works in a non-contact and non-invasive manner. It has recently become a topic of great interest in biometric research. Furthermore, it is widely believed that gait is difficult to hide or replicate.

Using gait information, people can be recognized by silhouette or model based approaches [3]. There have been more approaches which use the human silhouette, and of these, approaches which use the averaged silhouette have proved most popular [4]. Much of the earlier work was conducted on data acquired using controlled conditions but more recent work reported recognition using data derived outdoors, though with slightly lower performance.

There are many databases for evaluating progress in gait recognition research such as HiD (NIST, US) [5], Soton (Southampton UK) [7], and CASIA (CAS, China) [9] databases. The earliest databases contained data from only tens of subjects, sometimes wearing specified clothing. More recent databases include many more people, outdoor as well as indoor data (thus with uncontrolled illumination) and variation in camera viewpoints.

There has been no or little investigation into gait spoofing attacks where a person tries to imitate the clothing or walking style of someone else e.g. in order to gain illegitimate access and advantages (see Figure 1 for an imitation illustration). The only prior work on gait spoofing [1] uses wearable sensors but not video-based analysis: the spoofing attacks were performed against an accelerometer based gait recognition system where users needed to have devices attached to their legs in order to obtain a gait signature. The main conclusion is that gait is potentially difficult to spoof as it is behavioural and encompasses the whole body. However, to the best of our knowledge, there is no prior work on gait spoofing from visual data. Perhaps, the most appealing approach to use computer vision techniques to analyse the spoofing attacks against gait biometric systems is to replicate the silhouette of the target e.g. by wearing clothing that makes an attacker's body shape appear the same as the target. This is probably the most straightforward and unobtrusive method for performing the attacks especially against silhouette based gait recognition systems which have been the focus of much of the existing research and on which the first commercial gait recognition system is currently being based.

To gain insight into the factors that may have a significant effect on spoofing silhouette based gait biometric systems, we provide in this paper the first investigation on how clothing can be used to spoof a tar-

*This work is done within the EU FP7 project TABULA RASA

Figure 1. How well one can mimic the clothing/walking styles of another person? For instance, thousands of Beatles' fans imitate the famous walking across Abbey Road, London, every year.

get and evaluate the performance of two state-of-the-art recognition methods on a novel gait spoofing database recorded at the University of Southampton. As this is the first clothing-based spoofing attack in the research literature, our investigation focuses on the simplest form of attack, which is to replicate the clothing of the target. This is an important potential vulnerability as such an attack is relatively straightforward. It is also likely that such an approach will already be used by an attacker to unobtrusively enter a secure area where uniforms or formalised styles of dress are common. This is a similar approach to that of wearing a 3D mask in order to spoof a facial recognition system. As with face recognition, gait recognition can also be performed in 2D or 3D. For comprehensiveness, we study both approaches as they may have different vulnerabilities to spoofing.

2. Baseline Gait Biometric Systems

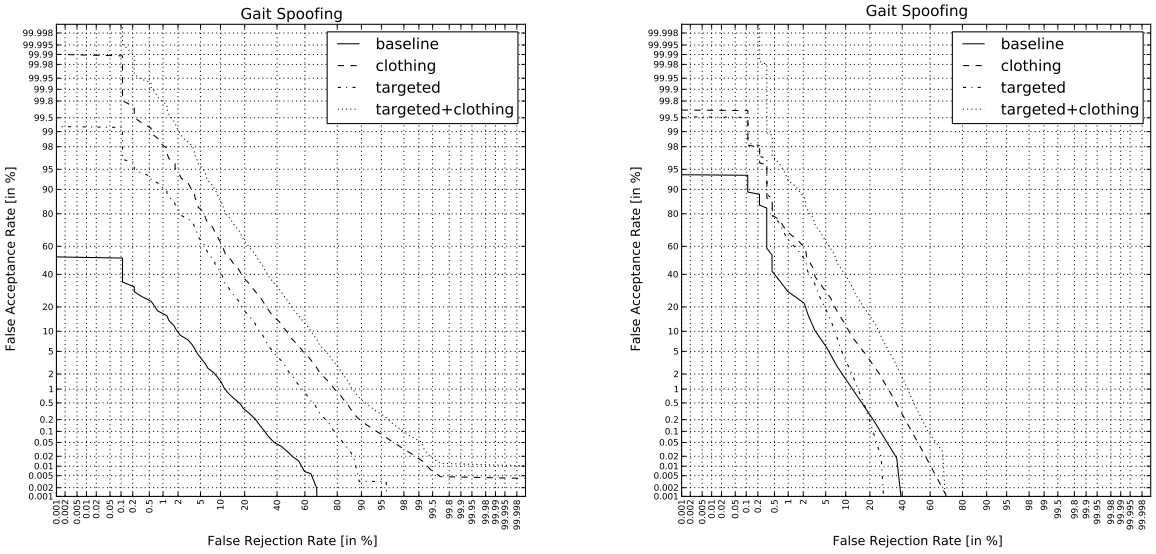
We considered two state-of-the-art systems developed at the universities of Southampton (USOU) and Oulu (UOULU). The USOU recognition system is a 3D gait approach and the UOULU system uses 2D data. 3D gait recognition systems have the advantage of using multiple synchronised and calibrated cameras, making video based replay attacks impractical. 3D approaches also address the difficulty of recognising subjects from different viewpoints therefore requiring that any spoofing strategy is effective when viewed from any direction. 2D approaches, using only one camera, are usually more practical as they are simpler to implement and to deploy in real-world applications. When efficiently combining the shape and motion cues, the performance of 2D approaches may easily reach that of 3D counterparts.

USOU Gait Recognition System: 3D volumetric data is used to synthesise silhouettes from a fixed viewpoint relative to the subject. The 3D volume is synthesised from eight synchronised camera views using shape from silhouette applied to the results of standard background subtraction approaches. The resulting silhouettes are then passed to a standard gait analysis technique using the average 3D silhouette [8]. The derived average silhouette is scale normalised so that it is 50 pixels high, whilst preserving the aspect ratio. The average silhouette is treated as the feature vector and used for verification via the Euclidean distance metric between samples.

UOULU Gait Recognition System: The dynamic texture based gait recognition system [2] of the University of Oulu (Finland) uses 2D dynamic texture descriptors, namely Local Binary Patterns from Three Orthogonal Planes (LBP-TOP), to describe human gait in a spatio-temporal way. A video sequence of a person's walking is thought as spatio-temporal volume. The LBP-TOP description is formed by calculating the LBP features from XY, XT and YT planes of volumes and concatenating the histograms to catch the transition information in spatio-temporal domain. Gentle AdaBoost is used to perform feature selection and to build a strong classifier.

3. Gait Spoofing Datasets

The Southampton gait database [6], one of the largest gait databases, is considered for the experimental evaluation. It contains multiple views and detailed camera calibration information. The database consists of recordings of subjects walking through the Southampton Gait Tunnel at least 9 times. Each recording consists of 8 synchronised video sequences of approximately 140 frames. 113 subjects were randomly selected for computing the baseline performance of the systems i.e. the performance when the systems are not confronted to spoofing attacks. Nine recordings of each of the 113 subjects were used, one for enrolment and eight for testing. This leads to one enrolment video for each user and 8×113 test client (positive sample) videos for each user.



(a) UOULU (b) USOU

Figure 2. Gait biometric performance under different kinds of spoofing attacks.

When producing impostor scores all the other clients are used, yielding in $8\times112\times113$ impostor attacks.

To analyze the performance under spoofing attacks, new data (referred to as USOU Gait Spoofing Database) has recently been recorded at the University of Southampton. This consists of 22 subjects (14 male and 8 female), between 20-55 years old. The subjects were recorded walking through the same tunnel in both their normal clothes and whilst wearing a common uniform. By having every subject wear the same clothes, the degree to which one subject could impersonate another by mimicking their clothes can be investigated. The uniform clothing appearance was achieved by having subjects wear white overalls over their normal clothes. Each recording of normal or uniform clothing was repeated between 10 and 35 times depending on subject availability.

4. Experimental Investigations

We investigated different spoofing scenarios including (**i**) clothing impersonation, (**ii**) deliberate selection of a target that has a similar build to the attacker and (**iii**) combination of clothing and target selection. This yielded in 4 protocols for studying gait under spoofing attacks:

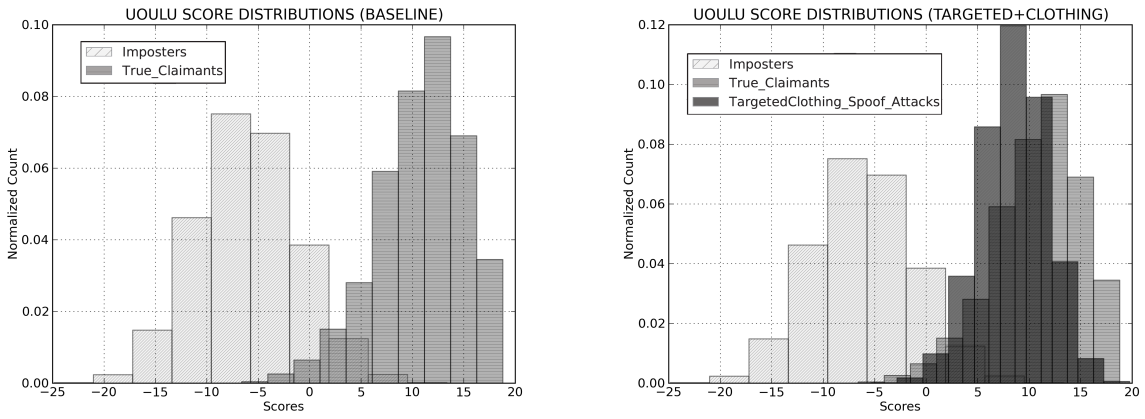
a) Baseline performance in which the original Southampton gait database without spoofing attacks was considered by computing only client and impostor scores. This provides the performance under normal settings.

b) Clothing attacks are calculated by comparing each of the uniform recordings of each subject against the uniform recordings of all of the other subjects. This provides insights into how clothing affects the performance.

c) Targeted attacks are measured by comparing each of the normal clothes recordings of each subject against each of the normal clothes recordings of the subject with most similar build. This provides insights into how selection of the target affects the performance.

d) Targeted clothing attacks are the same as targeted attacks except that instead of using the normal clothing recordings the uniform clothing recordings are used. This is equivalent to each subject selecting the person with the most similar build and impersonating their clothing.

The results of our experiments are shown in Figure 2 in terms of detection error trade-off (DET) profiles which illustrate the dynamic behaviour of the two gait verification systems (UOULU and USOU) as the decision thresholds are changed. The DET curves shows how the false acceptance rate varies according to the false rejection rate. The percentage of successful attacks is equivalent to the false accept rate of the systems when attacked. The lowest profiles (curves labelled *baseline* in Figure 2) are that of the baseline performance when the systems are not confronted to at-



(a) baseline

(b) targeted+clothing

Figure 3. Score distributions showing the overlap between the true claimants and the attacks.

tacks. They are important to gain insight into the effect of the spoofing as our focus is on the degradation in performance caused by spoofing attacks relative to these baselines.

The curves labelled *clothing* shows the average false accept rate when attackers replicate the clothing of their target but are unable to select which person they are attacking. This curve shows that clothing impersonation does convey a small advantage, increasing the Equal Error Rate (EER) from 6% to 12% for the USOU 3D gait system and from 4% to 28% for the UOULU 2D gait system.

The curves labelled *targeted* show how effective spoofing attempts are when an attacker selects a target that is most similar to them without also impersonating their clothing. In terms of equal error rate these kinds of attacks seem to be less effective than clothing impersonation. Finally, the curves that combine target selection and clothing impersonation show significant raise in the equal error rates compared to the baseline performance, thus indicating serious vulnerabilities to such combined attacks. This can also be seen in the score distributions in Figure 3 showing a clear overlap between the score distributions of the true claimants and the attacks on the 2D gait system.

5. Conclusion

We analysed for the first time the effects of spoofing attacks on silhouette based gait biometric systems. Our thorough investigations showed that it is indeed possible to spoof such systems especially when selecting the person with the most similar build and impersonating their clothing. The answer to the question in the title of this paper is then *gait biometrics may be spoofed* but perhaps not as easily as spoofing face biometrics which can easily be done using a simple photograph of the enrolled person's face whereas gait spoofing may require much more efforts e.g. to impersonate the clothing and walking style, and to select a target with a similar build to the attacker.

References

[1] D. Gafurov, E. Snekkenes, and P. Bours. Spoof attacks on gait authentication system. *IEEE Trans. on Information Forensice and Security*, 2(2007):491–502, 2007.

[2] V. Kellokumpu, G. Zhao, S. Z. Li, and M. Pietikäinen. Dynamic texture based gait recognition. In *IAPR/IEEE ICB 2009*, pages 1000–1009, 2009.

[3] M. S. Nixon and J. N. Carter. Automatic recognition by gait. *Proc. of the IEEE*, 94(11):2013–2024, 2006.

[4] M. S. Nixon, T. Tan, and R. Chellappa. *Human ID Based on Gait*. Springer-Verlag New York, 2006.

[5] S. Sarkar, P. J. Phillips, Z. Liu, I. R. Vega, P. Grother, and K. W. Bowyer. The humanid gait challenge problem: Data sets, performance and analysis. *IEEE TPAMI*, 27(2):162–177, 2005.

[6] R. D. Seely, S. Samangooei, L. Middleton, J. Carter, and M. Nixon. The university of southampton multi-biometric tunnel and introducing a novel 3d gait dataset. In *BTAS*. IEEE, September 2008.

[7] J. D. Shutler, M. G. Grant, M. S. Nixon, and J. N. Carter. On a large sequence-based human gait database. In *Conf. Recent Advances in Soft Computing*, pages 66–72, 2002.

[8] G. Veres, L. Gordon, J. Carter, and M. Nixon. What image information is important in silhouette-based gait recognition. In *CVPR*, 2004.

[9] S. Yu, T. Tan, and K. Huang. A study on gait-based gender classification. *IEEE TIP*, 18(8):1905–1910, 2009.