Improving Gait Biometrics under Spoofing Attacks

Abdenour Hadid[1], Mohammad Ghahramani[1], John Bustard[2], and Mark Nixon[2]

[1] Center for Machine Vision Research
Dept. of Computer Science and Engineering, University of Oulu, Finland
{hadid,mghahram}@ee.oulu.fi
[2] School of Electronics and Computer Science
University of Southampton, United Kingdom
{jdb,msn}@ecs.soton.ac.uk

Abstract. Gait is a relatively new biometric modality which has a precious advantage over other modalities, such as iris and voice, in that it can be easily captured from a distance. While it has recently become a topic of great interest in biometric research, there has been little investigation into gait spoofing attacks where a person tries to imitate the clothing or walking style of someone else. We recently analysed for the first time the effects of spoofing attacks on silhouette based gait biometric systems and showed that it was indeed possible to spoof gait biometric systems by clothing impersonation and the deliberate selection of a target that has a similar build to the attacker. These findings are exploited in this current work for developing new solutions to cope with such possible spoofing attacks. We describe then in this paper an initial solution coping with gait spoofing attacks using part-based gait analysis. The proposed solution is thoroughly evaluated on the challenging USOU gait spoofing database collected within the EU Tabula Rasa project. The database consists of records of 22 subjects (14 male and 8 female), between 20-55 years old, walking through the Southampton tunnel in both their normal clothes and whilst wearing a common uniform. The obtained results are very promising and point out very interesting findings which can be used as a reference for developing more enhanced countermeasures by the research community.

Keywords: gait recognition, spoofing attacks, LBP features.

1 Introduction

Biometric gait recognition refers to the recognition of people from the way they walk. This has recently become a topic of great interest in biometrics research. Compared to some other biometric modalities, gait is potentially beneficial since it can be acquired from a distance and it does not require contact or client cooperation. This makes it an attractive option in video surveillance applications.

Current state-of-the-art systems show that it is possible to recognise people using gait recognition by using silhouette or model based approaches [8].

A. Petrosino (Ed.): ICIAP 2013, Part II, LNCS 8157, pp. 1–10, 2013.

Both approaches start by analysing video data to detect the walking subject. Silhouette-based approaches have enjoyed the most success. In particular, those which use the averaged silhouette have proved most popular [9]. Feature set selection has been deployed to identify which features of the silhouettes contribute most to recognition [13]. Early model-based approaches used pendular models to calculate the variation in thigh inclination, when walking [3]. This work has been extended to a unified approach which can model running or walking simultaneously [14]. More recently, these models have been employed in conjunction with vertex based location. This approach tracks and describes people by the motion of their joints. Such model based approaches have also been subject to feature set selection, which revealed that motion components can have greater discriminative ability than the structural components. A further area of research is the effect of the camera viewpoint relative to the subject's walking direction. By assuming that the human is a solid object, walking in a periodic fashion along a linear path (for two gait periods), recognition can be achieved which is invariant to the direction of path relative to the camera [2]. The covariate factors are of equal concern and there is interest in the degree that external factors impede recognition by gait. Analysis of covariate factors including clothing and footwear has shown that wearing a trench coat or the wearing of flip flops can significantly affect recognition performance [1]. This is not surprising in that the wearing of clothes that obscure the whole body will naturally obviate any gait biometric. In addition, the walking style consistent with flip flops is known to differ from that when wearing normal shoes, though no research has parameterized this effect. As such, the current state-of-art has been to investigate the nature of the within-class variation, and the between-class variation in gait as a biometric. It is interesting that the earliest approaches achieved recognition rates exceeding 90% and this is matched by the most recent approaches on databases extending to 300 subjects. Much of the earlier work was conducted on data acquired using controlled conditions whereas later recognition has used data acquired outdoors, which has resulted in slightly lower recognition performance. There are many databases for evaluating progress in gait recognition research such as HiD (NIST, US) [10], Soton (Southampton UK) [12], and CASIA (CAS, China) [15] 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 and variation in camera viewpoints and illumination.

While gait recognition has become a topic of great interest in biometric research, there has been 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. 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.

The only prior work on gait spoofing [4] 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 was no prior work on gait spoofing from visual data until our very recent work [5] which analysed for the first time the effects of spoofing attacks on silhouette based gait biometric systems and showed that it was possible to spoof gait biometric systems by clothing impersonation and the deliberate selection of a target that has a similar build to the attacker.

In this present paper, we exploit our recent findings in [5] revealing the vulnerability of gait recognition to spoofing attacks and introduce the first countermeasure in the literature to cope with such threats (i.e. gait spoofing attacks). We describe an initial solution using part-based gait analysis. Our solution is based on the observation that the overall human body has various types of information to be extracted and selected for gait recognition. Body shape (built), overall body movement and body limbs movement patterns could greatly contribute to gait recognition. In case of spoofing attacks, these types of information may be altered to attack the system. Our proposed solution is thoroughly evaluated on the challenging USOU gait spoofing database collected within the EU Tabula Rasa project. The database consists of records of 22 subjects (14 male and 8 female), between 20-55 years old, walking through the Southampton tunnel in both their normal clothes and whilst wearing a common uniform. The obtained results are very promising and point out very interesting findings which can be used as a reference for developing more enhanced countermeasures by the research community.

The rest of this paper is organized as follows. Section 2 extends the work in [5] and gives a thorough analysis and additional results on the vulnerabilities of gait biometrics to spoofing attacks. Section 3 describes our proposed countermeasure to cope with gait spoofing attacks. This proposed solution is then thoroughly evaluated in Section 4. Discussion and conclusions are drawn in Section 5.

2 Vulnerabilities of Gait Biometrics to Spoofing Attacks

To gain insight into the vulnerabilities of gait biometric systems when confronted to spoofing attacks, we considered in [5] a dynamic texture based gait recognition method which efficiently combines the shape and motion cues and preliminary evaluated its performance on the gait spoofing database recorded at the University of Southampton. The main focus was on analysing factors that may have a significant effect on silhouette based systems, in particular on how clothing can be used to spoof a target. Clothing spoofing was chosen as it is one of the most straightforward and inconspicuous factors that an attacker can use to alter their gait silhouette. Our analysis was focused on the simplest form of clothing-based spoofing attack, that of wearing the same clothes as the target. For secure environments where legitimate users have some degree of uniform, such as hospitals, scientific research establishments, banks etc. this attack is likely to be necessary to evade detection from human security monitoring such as CCTV.

2.1 OULU Baseline Gait Biometric System

The dynamic texture based gait recognition system [6] 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. The system works as follows. Firstly, a video sequence of a persons walking can be thought as spatiotemporal volume. The volume is partitioned into sub-volumes. Using the sub-volume representation, motion and shape are encoded on three different levels: pixel-level (single bins in the histogram), region-level (sub-volume histogram) and global-level (concatenated sub-volume histograms). Secondly, 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. The LBP-TOP features from each sub-volume are extracted and concatenated to encode motion and shape characteristics. Thirdly, to use the multi-resolution information, original uniform patterns are improved with ordering sampling points according to the sampling angle, by which they will also produce codes that satisfy the bit transition condition and any number of sampling points can be used on different LBP kernels. Fourthly, the length of the LBP-TOP histogram representation can be quite large depending on the number of sampling points and number of sub-volumes that are used. A better and more compact representation can be obtained by using feature selection methods. Gentle AdaBoost was used to perform feature selection and to build a strong classifier. Instead of building a classifier that gives the identity of the person from one sample, a two-class classifier was trained, which classifies whether two samples come from the same person or not.

2.2 Gait Spoofing Datasets

The Southampton gait database [11], one of the largest gait databases, is considered for experimental evaluation. The database contains multiple views and detailed camera calibration information. The database consists of recordings of subjects walking through the Southampton Gait Tunnel (see Figure 1) 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 system i.e. the performance when the system is 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. When producing impostor scores all the other clients are used, yielding in 8×112×113 impostor attacks.

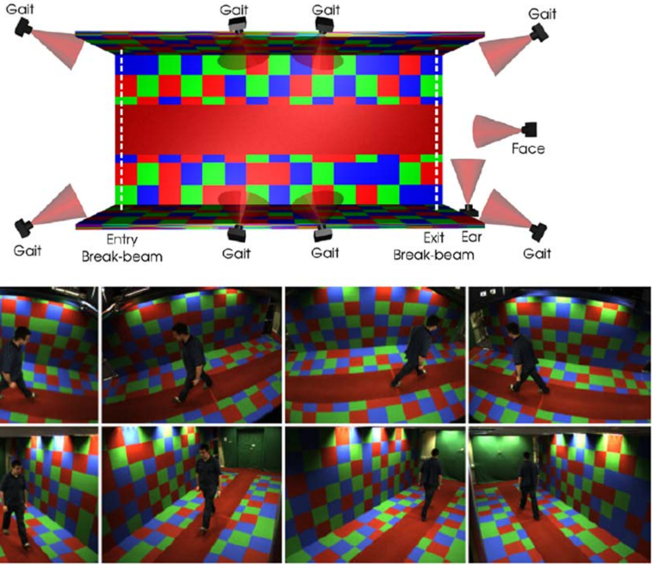

Fig. 1. Southampton Gait Tunnel

To analyse gait recognition performance under spoofing attacks, new data (referred to as USOU Gait Spoofing Database) has recently been recorded at the University of Southampton [7]. This consists of 22 subjects (14 male and 8 female), between 20-55 years old. The subjects were recorded walking through the Southampton Gait Tunnel in both their normal clothes and whilst wearing a common uniform (Figure 2). 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.

2.3 Resuls

For comprehensive analysis, we investigated different gait spoofing attacks scenarios including (**i**) clothing impersonation, (**ii**) deliberate selection of a target

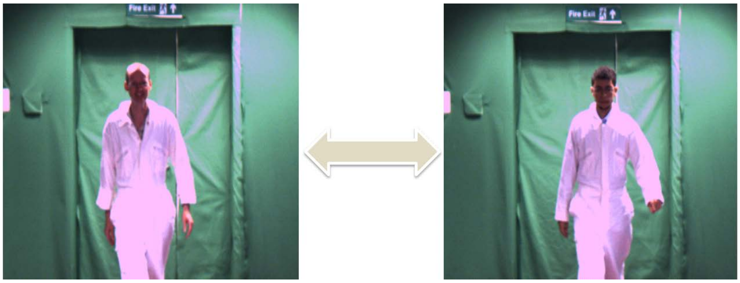

Fig. 2. Two subjects wearing the same clothes (common uniform) is used to investigate the degree to which one subject could impersonate another by mimicking their clothes

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 3 in terms of detection error trade-off (DET) profiles which illustrate the dynamic behaviour of the gait verification system 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 system when attacked. The lowest profile (curve labelled *baseline* in Figure 3) is that of the baseline performance when the system is not confronted to attacks. It is 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 the baseline performance.

The curve 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 4% to 28%. The curve labelled *targeted* shows how effective spoofing attempts are when an

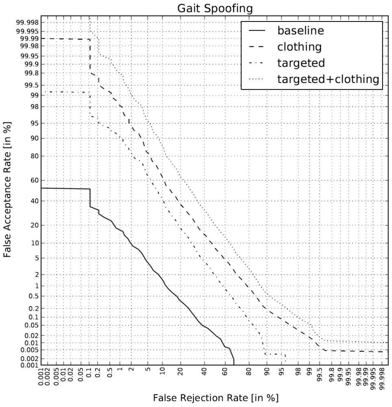

Fig. 3. Gait biometric performance under different kinds of spoofing attacks [5]

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 curve that combines target selection and clothing impersonation shows significant raise in the EERs compared to the baseline performance, thus indicating serious vulnerabilities to such combined attacks.

3 Proposed Countermeasure to Gait Spoofing

We analysed in the previous section the effects of spoofing attacks on silhouette based gait biometric system. Our thorough investigations showed that it is possible to spoof such gait systems especially when selecting the person with the most similar build and impersonating their clothing. We propose in this section a solution to cope with such threats. Our solution is an extension to the dynamic texture based gait recognition approach by exploiting the following two observations:

1. The overall human body has various types of information to be extracted and selected for gait recognition. Body shape (built), overall body movement and body limbs movement patterns could greatly contribute to gait recognition. In case of spoofing attacks, these types of information may be altered to attack the system. Hence, the baseline system is vulnerable to altered information as boosting did not learn from attacks and could potentially over-fit the training data.
2. The baseline system analyses the body in four divided regions. Based on the type of spoofing attacks (target or clothing), the information extracted from body portions could be altered. The overall histogram considers the overall portion and combines the altered information of body portions that are more

vulnerable to spoofing attacks to those carrying movement information than body built and shape information.

Our ideas to solve the shortcomings of the dynamic texture based gait recognition approach to better cope with spoofing attacks are:

- Prevent from over-training by employing histogram distance as the classifier.
- Divide the body into multiple horizontal portions, as shown in Figure 4.

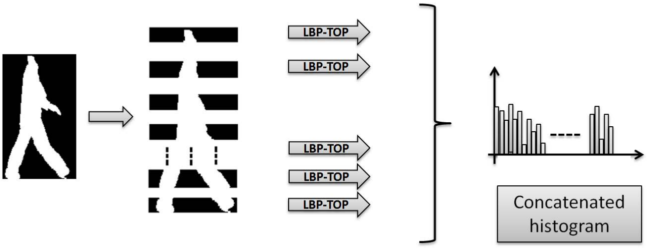

Fig. 4. Block diagram of our proposed initial gait anti-spoofing solution

The gait recognition database does not contain camera and viewpoint changes. Hence, we can divide the body into multiple regions to prevent altered information from body parts that are vulnerable to spoofing attacks to be combined with the overall information. We extract LBP-TOP features from each body part and concatenate the overall histogram to separate information extracted from body regions.

4 Experimental Analysis

To gain insight into the effectiveness of our solution, we focus our analysis on the clothing impersonation and combination of clothing and target selection. In the clothing impersonation scenario, the attacks are calculated by comparing each of the uniform recordings of each subject against the uniform recordings of all of the other subjects while the targeted clothing attacks are equivalent to each subject selecting the person with the most similar build and impersonating their clothing.

The results of the experiments are presented as DET curves in Figure 5. In all the experiments, the body is divided into 10 equal horizontal regions and LBP-TOP features are extracted and concatenated to obtain 10 sets of histograms as the resulting feature vector. In the "clothing attacks" scenario, the results in Figure 5 shows four plots comparing the baseline system "baseline", baseline system under attacks, anti-spoofing system performance using the baseline database and anti-spoofing system performance on the spoofing database. As expected, these results clearly show performance improvement against spoofing

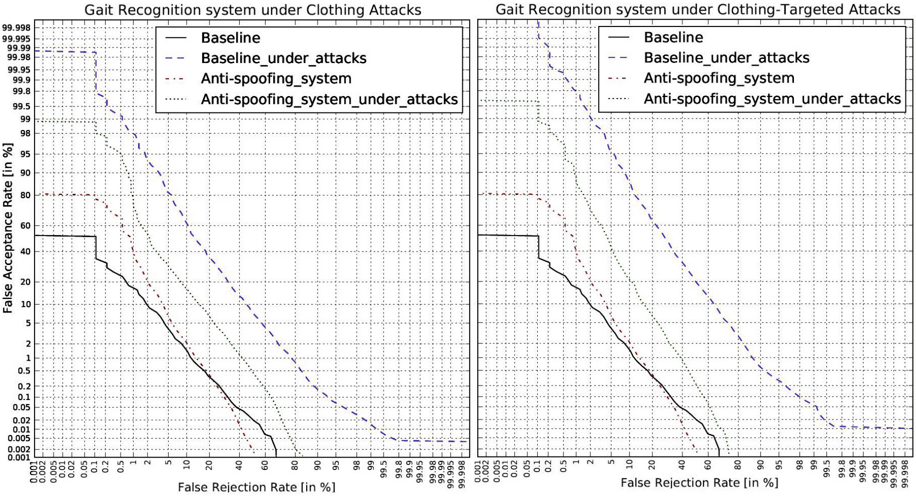

Fig. 5. The DET Curves of our proposed anti-spoofing solution and comparison with baseline results

attacks but at the cost of slight performance degradation on the baseline dataset. Similar conclusion can also be made on the results of the experiments for the "clothing targeted attacks" scenario. Due to more challenging spoofing attacks, the performance improvement is however less significant than in the "clothing attack" scenario.

5 Conclusion

Our investigations showed that it is possible to spoof silhouette based gait biometric systems especially when selecting the person with the most similar build and impersonating their clothing. Based on this finding, we described a solution to improve the performance of a gait baseline system against spoofing attacks. Our idea to solve the shortcomings of the baseline system consists of preventing from over-training by employing histogram distance as the classifier and dividing the body into multiple horizontal portions.

The experimental results showed that our anti-spoofing solution increases significantly the robustness of the baseline system to spoofing attacks. For example, the FAR of the baseline system drops from 80% to 20% at FRR of 10% under "clothing targeted attacks". Using our anti-spoofing solution under "clothing attacks" at FRR of 10%, the FAR performance gain was in the order of 45% (as the FAR of the baseline system which was 60% dropped till 15% using the proposed solution).

It is worth noting that while the countermeasure to gait anti-spoofing increases significantly the robustness of the system against spoofing attacks, some performance degradation on tests not including spoofing attacks can also be expected.

Acknowledgments. The financial support of the Academy of Finland is acknowledged. This work is done within the FP7 project TABULA RASA.

References

1. Bouchrika, I., Goffredo, M., Carter, J.N., Nixon, M.S.: Covariate analysis for viewpoint independent gait recognition. In: Tistarelli, M., Nixon, M.S. (eds.) ICB 2009. LNCS, vol. 5558, pp. 990–999. Springer, Heidelberg (2009)
2. Bouchrika, I., Goffredo, M., Nixon, M.S., Carter, J.N.: Viewpoint invariant gait recognition. IEEE Transactions on Systems, Man and Cybernetics (B) (2010)
3. Cunado, D., Nixon, M.S., Carter, J.N.: Automatic extraction and description of human gait models for recognition purposes. Computer Vision and Image Understanding 90(1), 1–41 (2003)
4. Gafurov, D., Snekkenes, E., Bours, P.: Spoof attacks on gait authentication system. IEEE Trans. on Information Forensice and Security 2(2007), 491–502 (2007)
5. Hadid, A., Ghahramani, M., Kellokumpu, V., Pietikäinen, M., Bustard, J., Nixon, M.: Can gait biometrics be spoofed? In: Proc. 21st International Conference on Pattern Recognition (ICPR 2012), Tsukuba, Japan, pp. 3280–3283 (2012)
6. Kellokumpu, V., Zhao, G., Li, S.Z., Pietikäinen, M.: Dynamic texture based gait recognition. In: Tistarelli, M., Nixon, M.S. (eds.) ICB 2009. LNCS, vol. 5558, pp. 1000–1009. Springer, Heidelberg (2009)
7. Matovski, D.S., Nixon, M.S., Mahmoodi, S., Carter, J.N.: The effect of time on gait recognition performance. IEEE TIFS 7(2), 543–552 (2012)
8. Nixon, M.S., Carter, J.N.: Automatic recognition by gait. Proc. of the IEEE 94(11), 2013–2024 (2006)
9. Nixon, M.S., Tan, T., Chellappa, R.: Human ID Based on Gait. Springer, New York (2006)
10. Sarkar, S., Phillips, P.J., Liu, Z., Vega, I.R., Grother, P., Bowyer, K.W.: The humanid gait challenge problem: Data sets, performance and analysis. IEEE TPAMI 27(2), 162–177 (2005)
11. Seely, R.D., Samangooei, S., Middleton, L., Carter, J., Nixon, M.: The university of southampton multi-biometric tunnel and introducing a novel 3d gait dataset. In: BTAS. IEEE (September 2008), http://eprints.ecs.soton.ac.uk/16970/
12. Shutler, J.D., Grant, M.G., Nixon, M.S., Carter, J.N.: On a large sequence-based human gait database. In: Conf. Recent Advances in Soft Computing, pp. 66–72 (2002)
13. Veres, G., Carter, J.N., Nixon, M.S.: What image information is important in silhouette-based gait recognition. In: CVPR, pp. 776–782 (2004)
14. Yam, C.Y., Nixon, M.S., Carter, J.N.: Automated person recognition by walking and running via model-based approaches. Pattern Recognition 37(5), 1057–1072 (2004)
15. Yu, S., Tan, T., Huang, K.: A study on gait-based gender classification. IEEE TIP 18(8), 1905–1910 (2009)