[Pattern Recognition 50 (2016) 17–25](http://dx.doi.org/10.1016/j.patcog.2015.08.007)

Contents lists available at [ScienceDirect](http://www.sciencedirect.com/science/journal/00313203)

Pattern Recognition

journal homepage: [www.elsevier.com/locate/pr](http://www.elsevier.com/locate/pr)

Robust multimodal face and ﬁngerprint fusion in the presence of spooﬁng attacks



Peter Wild [n](#_bookmark0), Petru Radu, Lulu Chen, James Ferryman

*University of Reading, School of Systems Engineering, Whiteknights, Reading RG6 6AY, United Kingdom*

## a r t i c l e i n f o

*Article history:*

Received 28 February 2015 Received in revised form 15 June 2015

Accepted 7 August 2015

Available online 19 August 2015

*Keywords:* Multibiometrics Anti-spooﬁng

1-Median

## a b s t r a c t

Anti-spooﬁng is attracting growing interest in biometrics, considering the variety of fake materials and new means to attack biometric recognition systems. New unseen materials continuously challenge state- of-the-art spooﬁng detectors, suggesting for additional systematic approaches to target anti-spooﬁng. By incorporating liveness scores into the biometric fusion process, recognition accuracy can be enhanced, but traditional sum-rule based fusion algorithms are known to be highly sensitive to single spoofed instances. This paper investigates 1-median ﬁltering as a spooﬁng-resistant generalised alternative to the sum-rule targeting the problem of partial multibiometric spooﬁng where *m* out of *n* biometric sources to be combined are attacked. Augmenting previous work, this paper investigates the dynamic detection and rejection of liveness-recognition pair outliers for spoofed samples in true multi-modal conﬁguration with its inherent challenge of normalisation. As a further contribution, bootstrap aggregating (bagging) classiﬁers for ﬁngerprint spoof-detection algorithm is presented. Experiments on the latest face video databases (Idiap Replay-Attack Database and CASIA Face Anti-Spooﬁng Database) and ﬁngerprint spooﬁng database (Fingerprint Liveness Detection Competition 2013) illustrate the efﬁciency of proposed techniques.

& 2015 The Authors. Published by Elsevier Ltd. This is an open access article under the CC BY license

([http://creativecommons.org/licenses/by/4.0/).](http://creativecommons.org/licenses/by/4.0/))

1. Introduction

Fingerprint and face biometrics as most widely adopted traits are being exposed to an increasing threat of presentation attacks. Conse- quently, there are numerous studies [[1,2]](#_bookmark22) and open challenges [[3,4]](#_bookmark25) on anti-spooﬁng techniques assessing the spooﬁng detector's ability to distinguish between genuine and fake attempts for especially these two traits. Recently, the integration of anti-spooﬁng scores with recognition scores has received considerable attention [[5–7]](#_bookmark31). The standard approach, as outlined in [[5]](#_bookmark27), has been to reject spoofed samples before comparing them against the gallery template. However, recognition scores can be helpful in the probe-attack spooﬁng detec- tion problem and liveness scores can impact on the recognition task. Considering imposters with access to fake ﬁngers or face photographs reveals an impact on overall accuracy (shifted imposter score distribu- tion for non-zero-effort attempts [[7]](#_bookmark31)) and assuming a correlation between successful spoofs achieving a higher score and their corre- sponding liveness score is likely (and shown) to help in the ﬁnal judgment of the decision task, especially in an ensemble of classiﬁers

n Corresponding author. Tel.: þ 44 118 378 7633; fax: þ44 118 975 1994.

*E-mail addresses:* [p.wild@reading.ac.uk](mailto:p.wild@reading.ac.uk) (P. Wild), [p.radu@reading.ac.uk](mailto:p.radu@reading.ac.uk) (P. Radu), [l.chen@reading.ac.uk](mailto:l.chen@reading.ac.uk) (L. Chen), [j.m.ferryman@reading.ac.uk](mailto:j.m.ferryman@reading.ac.uk) (J. Ferryman).

where this paper looks for outliers. It is therefore useful to investigate the beneﬁts of dealing with a holistic (liveness and veriﬁcation) multi- class problem rather than two separate classiﬁcation problems (live vs. fake and genuine vs. impostor). If a system involves multiple modalities there is an even larger variety of different ways to treat the problem of combining liveness and recognition scores. Multibiometrics using face and ﬁngerprint biometrics comes with many beneﬁts including expected increased accuracy, higher universality (absence of single characteristics), efﬁciency (fast indexing), but its robustness to spooﬁng attempts has been shown to be compromised [[8,9]](#_bookmark37). Furthermore, with the inclusion of multiple modalities the attacker has an even more extended choice to select the easiest modality to be attacked. It is therefore desirable to ﬁnd new techniques coping with spooﬁng attacks, which are subject to investigation in this paper. The paper focuses on three objectives: (1) investigation of spooﬁng robustness in multibiometrics; (2) development of novel methods towards anomaly detection for increased systematic anti-spooﬁng; and (3) proposition of a novel bootstrap aggregating (bagging) of classiﬁers method combin- ing features in ﬁngerprint counter-spooﬁng.

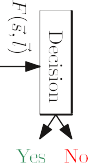
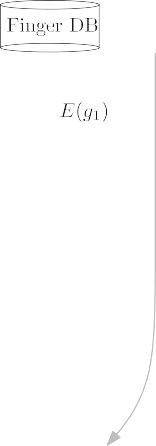
With regard to the ﬁrst topic on spooﬁng robustness in multi-

biometrics, the paper tests degradation in accuracy for the “partial multibiometric spooﬁng” scenario, where *m* out of *n* samples are spoofed, highlighting the tradeoff between accuracy and security for different fusion methods. [Fig. 1](#_bookmark1) illustrates this concept. The

<http://dx.doi.org/10.1016/j.patcog.2015.08.007>

0031-3203/& 2015 The Authors. Published by Elsevier Ltd. This is an open access article under the CC BY license ([http://creativecommons.org/licenses/by/4.0/).](http://creativecommons.org/licenses/by/4.0/))

are outlined in [Section 3](#_bookmark3). [Section 4](#_bookmark7) highlights experimental results with regard to the proposed and investigated techniques. This includes a discussion of methods towards anomaly detection in multibiometrics, highlighting parameter choice and optimisation for the proposed 1-median ﬁltering. [Section 5](#_bookmark17) concludes this paper with an outlook on future work.



1. Related work

Fig. 1. Partial multibiometric spooﬁng of observations *oi* given templates *gi* fusing scores *si* and liveness values *li*.

sensitivity of a recognition and liveness fusion method with regard to spooﬁng is especially interesting in multimodal conﬁguration, where scores originate from different underlying distributions and multiple traits facilitate a selection of the modality to be attacked. The paper analyses the impact of the number of spoofed ﬁngers or spoofed face on accuracy using the latest biometric datasets. The relative robustness of several score-level fusion rules can be used to choose the most robust fusion rule [[9]](#_bookmark37).

As a second outlined contribution, this paper presents a novel

multibiometric spooﬁng-aware fusion method following the idea of

There are several anti-spooﬁng or liveness detection algorithms extracting features (usually trained for modality, sensor, material, etc.), in order to determine whether a biometric sample is either *live* or *fake*. For evaluation purposes, *ferrlive* (rate of misclassiﬁed live samples) and *ferrfake* (rate of misclassiﬁed fake samples) are employed. Whereas for individual modalities the anti-spooﬁng pro- blem is well deﬁned and evaluated separately from biometric system performance, research on fusion between match scores and liveness factors is still in its infancy [[13]](#_bookmark45). Recently, [[14]](#_bookmark47) suggested a framework for veriﬁcation systems under spooﬁng attacks. Within the frame- work [[8]](#_bookmark34) adopted in this paper, liveness and recognition scores are combined considering the scenario of probe-spooﬁng only (i.e. no gallery-spooﬁng, enforced by e.g., attended enrolment). Formally, given a vector of biometric observation (units, e.g. ﬁngers, eyes)

!*o* ¼ ð*o*1; …*on*Þ from one or more modalities, and corresponding

claimed identity template !*g* ¼ ð*g*1; …; *gn*Þ, the task of the fusion

*F* ﬁ

module is to compute a uni ed decision score, using comparison scores !*s* ¼ ð*s*1; …; *sn*Þ and (probe) liveness values !*l* ¼ ð*l*1; …; *ln*Þ, so

ﬁ *V*

that the veri cation task (authentication based on threshold *η*) can

be formulated as follows:

8< accept if *F* !*s* !*l η*;

:

*V* ð!*o* ; !*g* Þ≔

ð

;

ÞZ

ð1Þ

anomaly detection and extending research in [[10]](#_bookmark38) to multiple mod- alities. This paper investigates 1-median-based fusion using outlier detection applied in a multibiometric setup. Note that the extension to multiple modalities raises further questions with regard to normal- isation. For different modalities, scores generally follow different distributions. Therefore, counter-spooﬁng is much more challenging than for single-modality approaches, including multi-instance or multi-algorithm approaches. Further, this work presents further the- oretical considerations and discusses parameter choice in detail. Recognition scores and liveness scores are likely to be dependent, as spooﬁng tries to achieve a high recognition score in order to success- fully claim the alien (spoofed) identity. In partial multibiometric spooﬁng this information can be used to further discriminate between genuines and impostors. Despite spooﬁng sensitivity of traditional fusion techniques, it is a reasonable assumption to claim a higher difﬁculty for attackers to spoof multiple modalities at the same time or even to obtain the necessary samples to produce a fake ﬁngerprint or face mask. On the other hand, special spooﬁng-robust fusion schemes might exhibit a reduced level of accuracy. This trade-off between cost and security to limit drawbacks [[5,11]](#_bookmark40) is investigated.

Third and last, as a by-product of evaluations the paper further

presents a novel spooﬁng detector again employing a fusion principle: bootstrap aggregating (bagging) of classiﬁers. This technique is employed in combining the decision outcome of multiple different classiﬁers. Using also multiple features to be more robust vs. changes in materials (see [[12]](#_bookmark43)), the paper aims at investigating this technique in the employed system as an anti-ﬁngerprint spooﬁng technique towards integral fusion concepts in robust anti-spooﬁng. Bagging is shown to outperform state-of-the-art detectors on the most challen- ging LivDet 2013 Crossmatch subset database.

The remainder of this paper is organised as follows: [Section 2](#_bookmark2) introduces the problems of anti-spooﬁng and spooﬁng-aware fusion in biometrics. The proposed methods of bagging for spoof-detection and 1-median ﬁltering for spooﬁng-resistant multibiometric fusion

reject else:

Let *i* be the current index and *E*ð*oi*Þ; *E*ð*gi* Þ refer to extracted (modality-speciﬁc) features of samples, then *si* ¼ *C*ð*E*ð*oi*Þ; *E*ð*gi* ÞÞA

½0; 1] is used to denote the normalised comparison result of *oi*; *gi*

and *li* ¼ *L*ð*oi*ÞA½0; 1] denote the likeliness of a genuine (live) sample.

ﬁ *F*

Clearly, it is desirable to nd a method unaffected in performance if *m* out of the *n* elements of !*o* are spoofed. This testing setup is

referred to as “partial multibiometric spooﬁng”, introduced in [[10]](#_bookmark38) and extended in this work towards multiple modalities. Note that this notion of live or spoofed probes vs. always-live enrolled gallery samples (assuming attended enrollment) leads to a simpler model- ling (2 classes distinguishing live probe from spoof or live, but different sources) than in the general asymmetric case (8 classes based on live/spoof probe, live/spoof gallery sample, and same/ different source) or symmetric case (6 classes) [[7]](#_bookmark31), fully concentrat- ing on a dichotomous authentication task, which can be evaluated in the traditional way using receiver operating characteristics.

*2.1. On combining anti-spooﬁng and recognition*

Marasco et al. [[5]](#_bookmark27) are among the ﬁrst considering fusion of liveness with recognition scores separately for each modality, using simple rejection of spoofed samples. If a spooﬁng attempt is indicated, the current modality matching score is ignored. This initial study is extended in [[15]](#_bookmark48) evaluating sequential fusion, classiﬁer fusion, and Bayesian Belief Networks for combining match scores and liveness measures, high- lighting the superiority of the latter method for the LivDet2009 dataset but also that accuracy is decreased when taking liveness detection into account. Chingovska et al. [[6]](#_bookmark29) evaluate binary decision rules and Logistic Regression (LR) as decision and score-level fusion techniques combining face recognition and liveness scores addressing the integration (but neglecting the partial spooﬁng problem) of liveness. They report higher resistance to spooﬁng attacks (91.54% vs. 10%) but are outperformed by

LR approaches achieving both, high veriﬁcation accuracy and good spooﬁng detection. Recently, Poh et al. [[7]](#_bookmark31) have targeted the problem of integrating spooﬁng and matching scores in a probe and gallery- spooﬁng scenario, investigating Gaussian Copula-based Bayesian classi- ﬁers and a mixture of linear classiﬁers for this task. While their method outperforms classical Support Vector Machine (SVM) based techniques, the approach needs training with regards to the full range of attacks.

The assessment of traditional fusion rules (this work is using Kittler et al.'s classical framework [[16]](#_bookmark49)) in the presence of spooﬁng attacks is a further relevant sub-problem and addressed in this work. Rodrigues et al. [[8,17]](#_bookmark50) ﬁrst addressed this security issue of spooﬁng attacks against a multimodal biometric system. They presented two methods, one using likelihood ratio and another employing fuzzy logic, both exceeding the accuracy of traditional fusion rules. Also Akhtar et al. [[18]](#_bookmark51) studied the impact of spooﬁng on parallel and serial fusion rules for face and ﬁngerprint reporting that score-level fusion methods from the literature are not robust to spooﬁng attacks and that serial fusion gave better results for an overall assessment of performance, veriﬁcation time, user acceptabil- ity and robustness.

*2.2. Anti-spooﬁng in ﬁngerprint and face recognition*

* 1. *Score and liveness fusion using 1-median ﬁltering*

Aiming to overcome the limitations of traditional sum-rule based techniques, which are known to be very susceptive towards outliers and thus easy to be attacked in multibiometric conﬁgura- tion, where an attacker can target the weakest link in the chain of combined biometric units to be attacked (e.g. using a particular available latent ﬁngerprint), 1-median ﬁltering [[10]](#_bookmark38) is investigated as a method for joint face and ﬁngerprint score-and-liveness fusion. The motivations in the deﬁnition of 1-median ﬁltering are (1) an extension towards a hybrid between sum rule and median rule as in Kittler et al.'s classical fusion methods [[16]](#_bookmark49) to ﬁnd an optimal compromise between (0-spoof) accuracy and (*m*-

spoof) robustness performance; and (2) an incorporation of high- dimensional information to be combined (score !*s* and liveness !*l*

pairs as introduced in [Section 2](#_bookmark2)).

Based on the median rule's property to be less affected by outliers (which is very beneﬁcial for spooﬁng resistance), this fusion method can be formulated as follows:

*Fmf* ð!*s* Þ≔P X *M*ð!*s* ; *si*Þ*si*: ð2Þ

*n*

*i* ¼ 1

*M*ð!*s* ; *si*Þ *i*

1

*n*

¼

1

8< 1 if .*s n* . o *ϕ*

. — .

:

In ﬁngerprint recognition, there are two general ways to

*M*ð!*s* ; *si*Þ≔

*i med sj j* ¼ 1

;

ð3Þ

address the spooﬁng problem: either by actively assessing the liveness (e.g. by measuring pulse, perspiration patterns, or blood pressure), or by passively analysing patterns of spoofed

materials (e.g. lack of detail, pattern differences). The latter

0 else:

Note that parameter *ϕ* limiting the zone of inﬂuence allows for an arbitrary tradeoff between the sum rule (*ϕ* ¼1 results in

*Fmf* ð!*s* Þ¼ 1 P*n si*, the classical sum rule) and the median rule

type, which is the subject of interest in this paper, reveals high

*n*

*i* ¼ 1

risk of material and sensor-dependence [[12]](#_bookmark43). An excellent

(for *ϕ* sufﬁciently small, the deﬁnition becomes *Fmf* ð!*s* Þ¼

recent survey of spooﬁng methods in ﬁngerprint recognition

can be found in [[2]](#_bookmark22). Among the most common techniques for

*medn*

*j* ¼ 1

*sj*, the median rule). One of the important tasks is to ﬁnd

static (extracted from single image) texture-based anti-spoof- ing methods are statistical features [[19]](#_bookmark52), Power Spectrum Four- ier analysis [[20]](#_bookmark53), Ridge Frequency Analysis [[19]](#_bookmark52), Local Binary Patterns (LBP) [[21]](#_bookmark54) and Local Phase Quantisation [[22]](#_bookmark18). However, recent developments towards material-independent static anti- spooﬁng suggest to combine multiple features and probably even detectors. Fumera et al. [[13]](#_bookmark45) give a good introduction into the problem of combining multiple liveness detectors for a single modality, fusion of liveness detector and matcher for a single modality, and anti-spooﬁng capabilities of ad hoc fusion rules combining multiple comparison scores.

Face spooﬁng counter-measures can broadly be classiﬁed into

a suitable (trained) parameter *ϕ*, which can be either ﬁxed or a function of the scores. The choice of *ϕ* is not straightforward and should rely on the underlying distribution's properties. Parameter selection is discussed in [Section 4.7](#_bookmark16).

As a motivation for the selection of the median, consider the following theoretical considerations: as observed in [[6]](#_bookmark29) unimodal non-zero-effort imposter score distributions (comparing a spoofed sample with a genuine reference) are shifted towards the genuine distribution (comparing two live genuine samples) compared to zero-effort imposters (comparing two live samples from different identities). In an equally weighted mixture-model for random

variables *Xi*, we have *E*ð1 P*n Xi*Þ¼ 1 P*n E*ð*Xi*Þ¼ *μ* assuming

*n*

*i* ¼ 1

*n*

*i* ¼ 1

2

texture-based and motion-based counter-measures. A good over-

view on face counter-spooﬁng may be found in [[23]](#_bookmark19). The ﬁrst

category assessing textural properties is the more widespread

independent, normalised (same mean *μ* and variance *σ* ) distribu-

tions. However, for the variance, we get *Var*ð1 P*n Xi*Þ¼

*n*

*i* ¼ 1

*i* ¼ 1

*n*2

*i*

*n*

1 *Var*ðP*n X* Þ¼ 1*σ*2. While this illustrates the positive effect of

group with approaches like LBP [[24]](#_bookmark20), or statistical features [[25]](#_bookmark21) exploiting the observation that images/videos with spoofed faces (printed or replayed) do not exhibit the same noise-level like genuine samples. The second type of motion-based approaches targets the reproduction of (ﬂat) printed photographs or re-display of faces on tablets exploiting the difference in 3D appearance of spoofed approaches. For fusion purposes this paper focuses on the ﬁrst type and employs an existing anti-spooﬁng system [[26]](#_bookmark23).

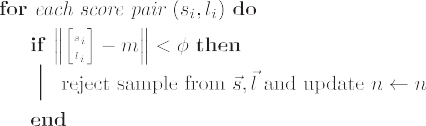
1. Proposed methods

In order to solve the problem of robust face and ﬁngerprint fusion in the presence of spooﬁng attacks, this work proposes 1- median ﬁltering for enhanced tolerance with regards to a number of attack-outliers in the ensemble of score-liveness tuples, and bagging of classiﬁers for enhanced (fused) spooﬁng resistance. Both methods are described in detail in the next subsections.

fusion on imposter scores (narrowing the variance), it also clearly

illustrates that if one of the random variables follows a degraded spoof-imposter distribution with lower mean, this is likely leading to a bimodal distribution (especially if *n* is large). Assuming the distributions can be modelled by Gaussians, a mixture of two normal distributions with highly unequal means has a positive kurtosis, as the smaller distribution lengthens the tail of the more dominant one. While there are exceptions to the rule [[27]](#_bookmark24), as a rule of thumb, it is generally suggested, that in skewed distributions, the mean is farther out the longer tail than the median [[28]](#_bookmark26), therefore a better representative in the ﬁltering process (which is likely to succeed as can be seen from theoretical considerations if the number of spoofed modalities is low compared to *n*). However, note that the crucial pre-assumption is a proper normalisation, which ideally should leave genuine score distribution almost unaffected. Further, note that median ﬁltering is not to be mixed up with image- or kernel-based combination and works on score (and liveness-) values to be combined.

Algorithm 1. Median ﬁltering.







The outlined technique can easily be extended to 2D for combin- ing points ð*si*; *li*Þ of recognition and liveness scores, using the geometric-median (1-median). This is the point minimising the sum of distances to the sample points using score *si* and liveness *li* as coordinate values.

two (genuine and impostor) joint score- and liveness-distributions. Training of *Ψ* is discussed in [Section 4.5](#_bookmark11).

* 1. *Bagging-based ﬁngerprint liveness detection*

For ﬁngerprint anti-spooﬁng relatively poor performance com- pared to other test sets is reported for the Crossmatch subset of LivDet 2013 ﬁngerprint database [[4]](#_bookmark25). In order to improve those results, this paper proposes the following novel spoof detection algorithm. The employed setup follows a three-stage architecture with preprocessing, feature extraction, and classiﬁer fusion. [Fig. 3](#_bookmark5) illustrates the processing chain. In the preprocessing stage, the ﬁngerprint image is segmented and aligned. The background of the image is removed using Otsu's thresholding [[29]](#_bookmark25) and the region of interest is automatically cropped at a dimension of 248 by 256 pixels. Feature extraction extracts global properties and local texture details using three methods selected as representa- tive methods (wavelet-based, statistical and frequency-based) to make maximal use of the fusion technique:

1. *2D Gabor ﬁlters* [[30]](#_bookmark28): These ﬁlters as a product of a Gaussian and a sinusoid capturing local details are parameterised by Gaussian

: ð4Þ

2 ! !

*Fmf* ð *s* ; *l* Þ≔

1 X

# 

¨

!*s*

*s*

" !*s* # " *si* #!" *si* #

*M*

!*l*

;

*li*

*li*

space constants *δx* and *δy*, frequency *f* of the modulating sinusoid

and orientation *θ*

P*n M* " !#; " *i* #! *i* ¼ 1

*i* ¼ 1

*l*

*li*

1

02

2

02

2

*n*

*G*ð*x*; *y*; *f* Þ¼ 2

*πδxδy*

*e* — 1=2ð*x* =*δx* þ *y* =*δy* Þ cos ð2*πfx*0 Þ

" !*s* # " *s* #!

*M*

;

*i*

# 

!

*l*

8>< 1 if ¨" *si* #

*i*

*n* " *sj* #¨o *ϕ*

*j*

*x*0 ¼ *x* sin *θ* þ *y* cos *θ y*0 ¼ *x* cos *θ* — *y* sin *θ* ð7Þ

# 

—

*l*

;

ð5Þ

Similar to [[31]](#_bookmark30) *θ* is set to 01; 451; 901 and 1351 at frequency *f* ¼ 0.1,

*l i* 0 else:

≔

¨

*l*

*med*

*j* ¼ 1

[Fig. 2](#_bookmark6) illustrates how median ﬁltering uses the median as a seed point to select all points in a local neighbourhood, computing the centroid of the set of ﬁltered points as an even better local rep- resentative. As the median is less affected by outliers (left example) it is beneﬁcial in the presence of outliers, whereas in case samples are less scattered (right example), no samples are rejected. [Algorithm 1](#_bookmark4) illustrates all the steps. Note that the additional processing time needed for the comparison should have a negligible impact, as *n* is traditionally rather small.

Note that the 1-median is not necessarily an input point and for performance reasons an approximation (e.g., coordinate-wise med- ian) might be sufﬁcient. As the task of the fusion module is to come to a ﬁnal single decision score, a further mapping to a single scalar

is necessary. For this task, LR or SVMs can be employed to ﬁnd the hyperplane *Ψ* : !*w* !*x* !*b* 0 optimally separating the sets of

· — ¼

genuine and zero-/*m*-spoof impostors, where *m* is the number of spoofed samples in the joint fusion scheme

*Fmf* ð!*s* ; !*l* Þ≔*dist*ð*F*2 ð!*s* ; !*l* Þ; *Ψ* Þ: ð6Þ

*mf*

Separability becomes more difﬁcult for larger values of *m* (spoofed samples), the presented implementation uses *m* ⌊*n*=2 . Threshold variation is equal to moving the hyperplane separating the

¼ c

corresponding to 10 pixels (typical inter ridge distance). The

ﬁltered region of interest is divided in blocks of 20 20 pixels. For each block, mean and standard deviation are computed leading to a total of 880 features.

~

1. *Gray level co-occurrence matrix* (*GLCM*): 6 features each were extracted from 20 by 20 sized pixel-blocks (leading to a total feature vector size of 1100 components) computing local characteristics following [[31]](#_bookmark30): maximum probability, entropy, contrast, energy, homogeneity and inverse difference moment of order *k*.
2. *Fourier Transform* (*FT*) *based features*: As global features on the Fourier-transformed image, the sum of absolute differences between pairs of concentric circles (at distance 1–3 pixels, evaluated at 25 locations) are computed, similar to [[32]](#_bookmark32), yielding 180 components.



Fig. 2. 1-Median ﬁltering vs. sum-rule in 2D with outliers (left) and without (right). Fig. 3. Proposed ﬁngerprint counter-spooﬁng based on bagging classiﬁers.



The ﬁnal feature of 2160 components is obtained by concatenat- ing the 3 individual feature vectors described above and Principal Component Analysis (PCA) is applied as a feature selection procedure retaining 99% of the variance of the data with 80 PCA components. Besides a fusion of features, the suggested anti-spooﬁng algorithm employs a multiple classiﬁer framework, which distinguishes itself from a standard multiple classiﬁer system by applying a bagging [[33]](#_bookmark33) technique for its component (base) classiﬁers.

The Bootstrap AGGregatING (bagging) method [[33]](#_bookmark33) is used to add base classiﬁers to the base ensemble using bootstrap replicates on the training set. The bootstrap method facilitates determining the probability distribution of the data without using the Central Limit Theorem [[34]](#_bookmark35). The idea behind bootstrap sampling is to create an artiﬁcial random list of the labelled training set by picking some labels more than once. One classiﬁer is trained on this random list

and is added to the base ensemble. In the operational phase, the

multi-biometric databases exist with multiple traits collected from the same person, this does not extend to spooﬁng datasets. Further, spooﬁng datasets are created for liveness detection purposes and therefore usually do not have to come with a large number of genuine samples, which are needed for the intended recognition- based assessment. In contrast to spooﬁng evaluations assessing *ferrfake* and *ferrlive* (see [Section 2](#_bookmark2)) measures, this evaluation refers

to Receiver Operating Characteristics (ROC). Note that for *m* 40

spoofed samples these refer to pairs of Spoof False Acceptance Rate (SFAR) and Genuine Acceptance Rate (GAR, the percentage of genuine users being accepted), rather than False Acceptance Rate (FAR) and GAR pairs, see [[36]](#_bookmark39). For comparing recognition perfor- mance (S)EER is employed as the (Spoof) Equal Error Rate where GAR (S)FAR and decidability index (*d*-Prime) as

¼

*d*0 ¼ .*μ* — *μ* .=qðﬃﬃ*σ*ﬃﬃﬃ2ﬃﬃþﬃﬃﬃﬃﬃ*σ*ﬃﬃ2ﬃﬃÞﬃﬃ=ﬃﬃ2ﬃﬃﬃ measuring the separation of distribu-

1

2

1

2

base classiﬁers are applied to the input feature and their outputs are combined at the decision level by using majority vote. To beneﬁt from the variations of the training set, it is better if the base classiﬁers are unstable (e.g. neural networks and tree classiﬁers). In the present work, three base classiﬁers are employed: (1) regu- larised LR; (2) single layer perceptron, and; (3) SVM. The three base classiﬁers are trained *n* 100 times on different bootstrap replicates of the training data. In the operational phase, the 300 classiﬁers decisions are recorded as 0 or 1, where 1 indicates that the classiﬁer believes that the image is spoofed. The ﬁnal spooﬁng score *sf* for one test ﬁngerprint image is given as

¼

tions with mean *μi* and standard deviation *σi*.

Paired data originate from the following datasets ([Table 1](#_bookmark8)):

*LivDet 2013 CrossMatch* [[4]](#_bookmark25): The 4500 images of 99 users support up to 3 genuine samples per ﬁnger and a varying number of spoofed samples made from BodyDouble, Latex, Playdoh and WoodGlue.

●

●

*Idiap ReplayAttack* [[37]](#_bookmark41): The counter-spooﬁng video database of 1300 clips of 50 clients with 320 240 pixels resolution provides 8 genuine and 40 attack samples per user offering a *controlled* (homogeneous background) and challenging *adverse* recording setup. There are 4 mobile attacks using iPhones, 4

~

*sf* ¼

*m*

*i* ¼ 1

P

*n i*

*j* ¼ 1 *j*

P

*D*

ð8Þ

high-resolution iPad replays, and 2 hard-copy prints.

# ●

~

*mn*

where *m* is the number of base classiﬁers types, *n* is the number of bootstrap replicates and *Di* is the decision of base classiﬁer of type *I* trained on the bootstrap replicate number *j*. In the proposed implementation, *m* ¼ 3; *n* ¼ 100. The value of *sf* is in the range

*j*

½0; 1]. By setting and adjusting a threshold *t* A½0; 1], different

ﬁ ﬁ

operating points of the anti-spoo ng approach are con gurable.

1. Experiments and discussion

In order to evaluate the suggested 1-median ﬁltering and bagging approaches, a modularised setup is employed, using state-of-the-art feature extraction, recognition and spooﬁng algorithms described in the following sections. After an introduction into database, metrics and employed reference setup, this section concentrates on questions related to baseline performance of spooﬁng detectors evaluating the bagging classiﬁer approach and inter-relation of recognition and anti- spooﬁng. Then, partial multibiometric spooﬁng in multibiometric face and ﬁngerprint context is assessed, considering recognition-only and joint recognition and liveness fusion techniques.

* 1. *Setup: database and metrics*

As in many other approaches assessing face and ﬁngerprint fusion [[18,35]](#_bookmark36), also this work builds on a chimeric dataset pairing face and ﬁngerprints originally originating from different people. This approach is justiﬁable, since ﬁngerprints and faces as biometric modalities can be assumed to be independent. While also true

Table 1

Employed test databases.

Mod. Database/set Images Users Training Testing

FP LivDet2013 Crossmatch 4500 99 Left hand Right hand

Face ReplayAttack 1300 50 *train* set *devel, enroll, test*

Face AntispooﬁngFace 600 50 – *train, test*

*CASIA AntispooﬁngFace* [[38]](#_bookmark42): This database of 600 clips of 50 clients with 640 480 pixels resolution comes with 3 genuine and 9 fake samples per user, offering low, medium and high quality setups and 3 fake attacks.

A chimeric dataset is compiled, combining faces and ﬁngers from the databases above, forming a new set of 85 classes. Note the number of classes, 85, is due to the restriction of LivDet to right-hands only and guaranteeing a minimum number of genuine and spoof ﬁngers to simulate the selection of *n* out of *m* spoofed samples of different ﬁngers in a random way. Testing uses right hands only to allow for a training of the employed counter- spooﬁng detector and learning-based parameters of median ﬁlter- ing. Spooﬁng attempts are simulated by randomly replacing *m* out of *n* samples (4 ﬁngers and 1 face) with spoofs.

* 1. *Setup: baseline system*

For experiments, the following baseline system is employed:

*NIST Biometric Image Software* [[39]](#_bookmark44): For ﬁngerprint feature extraction (using minutiae detection *mindtct*) and comparison (using *bozorth3* in 1:1 verify mode). While the ﬁnal score is not normalised, (capped) min–max normalisation is used to map scores to the unit interval 0; 1 .

●

●

½ ]

*Neurotechnology VeriLook 5.5* [[40]](#_bookmark46): For processing video/still image face samples. The off-the-shelf software extracts a 4– 35 kB template via facial reference points and is able to account for off-axis registration (using 15 degrees roll, pitch and yaw parameters). Note that quality assurance (ISO/IEC 19794- 5:2005) was deactivated to account for low-quality samples in the dataset. The setup employed in this work used the *low matching speed* setting with switched-off threshold (such that ﬁnal scores could be obtained).

●

*LBP-TOP Face-Liveness* [[24]](#_bookmark20): Using the open-source implementa- tion in [[26]](#_bookmark23) for face liveness-detection. The LBP-TOP operator calculates LBP features at three orthogonal planes that intersect



Fig. 4. LBP-TOP process [[24]](#_bookmark20): for each of three planes intersecting at one pixel, LBP histograms are computed and concatenated.

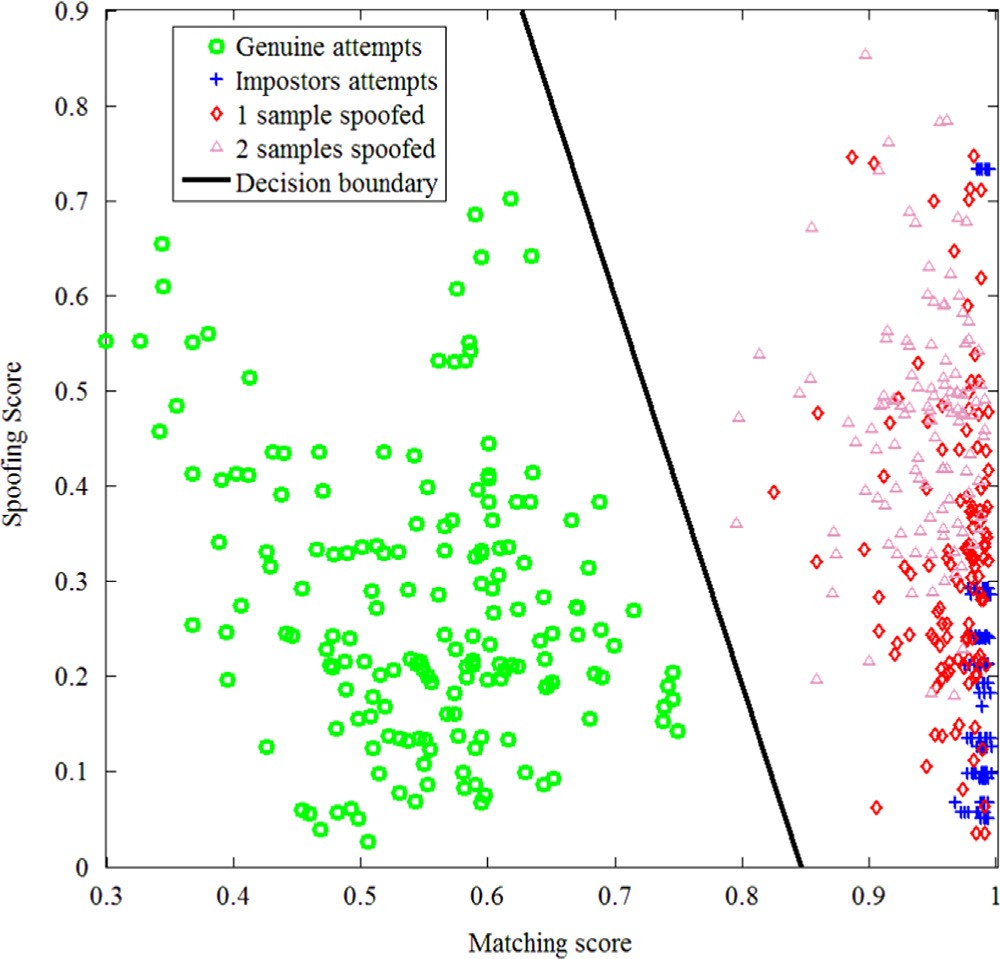


Fig. 5. Fused liveness-comparison scores with trained decision boundary for genuine, impostor, 1-spoof and 2-spoof pairs for ﬁnger-and-face fusion.

in the centre pixel. The features are extracted from each separate plane and then concatenated together. A multi-resolution description is then generated such that the histograms along the time domains (*XT* and *YT*) are concatenated for different values of time *t*. [Fig. 4](#_bookmark9) illustrates the process. Compared with traditional 2D LBP features, LBP-TOP can capture spatio- temporal features combining information from both image and time domains. SVMs are then applied for classiﬁcation.

* *Bagging Fingerprint-Liveness*: As introduced in [Section 3](#_bookmark3).
  1. *Baseline performance of spooﬁng detectors*

In a ﬁrst experiment, the detection performance of employed spooﬁng detectors is investigated. For anti-spooﬁng performance assessment, *ferrfake* and *ferrlive* rates are computed, using the underlying LivDet 2013 Crossmatch dataset for the ﬁngerprint modality, and the ReplayAttack database for face. The implemen- tation of the face spooﬁng-detection algorithm based on the open source package provided from the original work [[26]](#_bookmark23) yielded an accuracy of 85% on ReplayAttack. A similar accuracy is obtained for the presented ﬁngerprint detection scheme, however the rate is much more remarkable given the high quality of the underlying spooﬁng dataset. Counter-spooﬁng using bagging classiﬁers yielded an accuracy of 84% on the Crossmatch set (the method is trained using a distinct subset of the test database using ﬁngers from left hands), a value which signiﬁcantly outperforms the best accuracy reported (68.8%) in the results of the LivDet liveness

detection competition [[4]](#_bookmark25) for this subset. Given that integrated feature-level and classiﬁer fusion in spooﬁng detectors is not a common practice, recognition rates are very promising and sug- gest to explore this topic even further in the future.

* 1. *On the mutual impact of liveness and recognition*

Spooﬁng systems are usually evaluated on their own without taking recognition into consideration [[6]](#_bookmark29). However, the joint operation of liveness and recognition systems in practice raises a series of questions, most notably how to combine recognition and liveness information. This section highlights that not only liveness values are useful in justifying the authenticity of an identiﬁcation claim, but also vice versa: the recognition score of a template is actually helpful to judge the presence of a spooﬁng attack. In LivDet, counter-spooﬁng performance is measured in terms of *ferrfake* and *ferrlive* rates referring to ﬁnger images as inputs, not comparisons. If recognition scores are to be considered in the evaluation of spooﬁng detection, it is important not to assume speciﬁc properties of the comparison. In real- world applications, however, a fake ﬁngerprint will be employed to fake the originating identity causing its corresponding score to be distributed according to the spoof-imposter score distribution, whereas a live ﬁngerprint is to originate from either genuine or zero-impostor distributions. The impostor score distribution is likely to shift towards the genuine score distribution in evaluations considering non-zero-effort impostors [[6]](#_bookmark29), whereas the genuine score distribution remains unaffected. Since spoofs are unlikely to be perfect, scores are typically degraded, which can be used to judge the presence of a fake sample using, e.g. fuzzy logic as employed in [[8]](#_bookmark34). Simple fuzzy-rule based (inverting the recognition score contribution after threshold *t* 0.6) product fusion of recognition and liveness scores using randomly determined identity claims in experiments increased the spooﬁng detection capability from 18.36% *ferrfake ferrlive* to 13.86% for the LivDet CrossMatch set. The integration of spooﬁng scores into recognition accuracy can further increase recognition accuracy when considering 1-spoof impostors in evaluations, e.g. by simply rejecting the sample [[15]](#_bookmark48). Therefore, the real challenge is to ﬁnd a suitable tradeoff between recognition accuracy and spooﬁng robustness, sub- ject to investigation in the next sections.

¼

¼

* 1. *Combining liveness and recognition scores with logistic regression*

With the positive impact of recognition on spooﬁng detection and vice versa, it is reasonable to proceed towards a holistic framework integrating both evidence as discussed in [Sections 2 and 3](#_bookmark3) and illustrated in [Fig. 1](#_bookmark1). When combining both sets of scores individually using sum rule, logistic regression can be used to learn a more robust boundary. This boundary is trained (and then outliers eliminated using the presented 1-median ﬁltering approach) in already com- bined (fused) space, which is able to clearly distinguish between different zero-effort and spoof detection. The 1-spoof and 2-spoof examples are used to account for the median tolerating a number of

# Image of Fig. Image of Fig.

Fig. 6. ROC for partial multibiometric spooﬁng using sum rule.

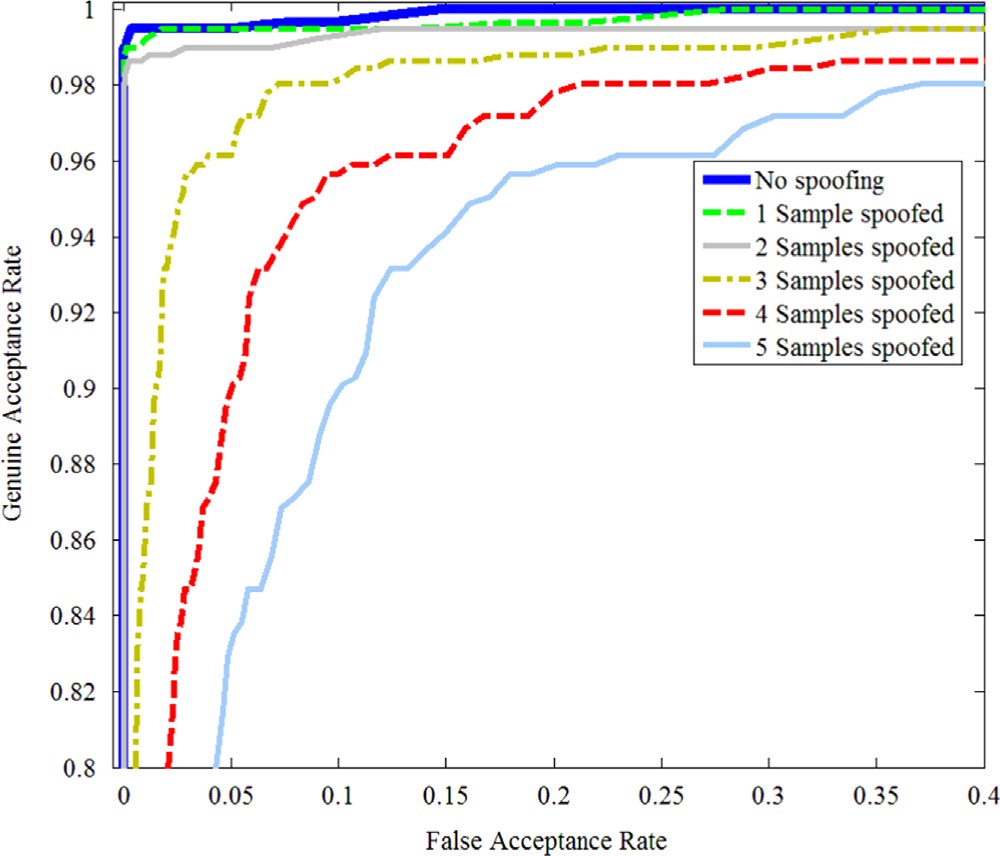


Fig. 7. ROC for partial multibiometric spooﬁng using median rule.

outliers up to half of the samples. The trained decision hyperplane in [Fig. 5](#_bookmark10) has the following form:

*Ψ* : *y* ¼ — 13:52*x* þ12:4257: ð9Þ

The experiment also clearly illustrates how *m*-spoof distributions are shifted towards the genuine distribution with increased *m*.

* 1. *Classical fusion in partial multibiometric spooﬁng*

In partial multibiometric spooﬁng, *m* out of *n* biometrics samples of an identity are spoofed (*n* 5 with 4 ﬁngerprints and 1 face in experiments, using equal probabilities). That is, an attacker is assumed to have access to *m* 0; 1; …; *n* latent ﬁngerprints or face masks/print-outs for the attempt to spoof the system, referred to as

¼

¼

an *m*-*spoof* attack. Recognition rates for the common fusion rules sum, product and median are evaluated in this scenario and results listed in [Table 3](#_bookmark15). Conﬁrming assumed behaviour, experiments in this work show that spooﬁng clearly impacts on recognition. For simple sum rule fusion it is evident that recognition is affected if even a single sample is spoofed, EER is degraded from 0% to 2.32% (*d*-Prime from 2.91 to 2.62). While perfect separation in the ﬁrst

Fig. 8. ROC for partial multibiometric spooﬁng using 1-median ﬁltering þ LR.

Table 2

Average mean vs. median of *m*-spoof imposter distribution.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Unit | 0-spoof | 1-spoof | 2-spoof | 3-spoof | 4-spoof | 5-spoof |
| Median | 0.991 | 0.989 | 0.984 | 0.965 | 0.935 | 0.921 |
| Mean | 0.989 | 0.964 | 0.940 | 0.914 | 0.889 | 0.873 |

case is certainly also attributable to the size of the dataset, the degradation is clearly visible, taking also the large number of 5 combinations of 2 modalities in a single authentication attempt in our particular setup into account. Further *m*-spooﬁng of faces and ﬁngerprints suggest an increase of abs. 2–3% using sum rule for every additional spoofed sample (EERs of 2.32–12.24% for 1–5 spoofs), which is even more pronounced compared to previous ﬁngerprint-only experiments [[10]](#_bookmark38) and spooﬁng of all samples did not always lead to acceptance (due to degraded accuracy of spoofed samples). The ROCs in [Figs. 6 and 7](#_bookmark12) illustrate the degradation for sum and median rules, respectively.

In contrast to previous experiments on ﬁngerprints only, median rule has shown to be even more successful in combining results. There is little difference between 0-spoof, 1-spoof, and 2- spoof samples (EERs of 0.42%, 0.87%, and 1.20%), suggesting better tolerance vs. spooﬁng attempts clearly outperforming the sum- rule. However, this comes at a price of clearly degraded initial performance. Further, results indicated that the underlying dis- tributions have a huge impact on the performance of the median rule (reported results refer to min–max-normalised scores). It is therefore important to consider learning distributions beforehand and employ a proper normalisation method. If median rule is extended to median ﬁltering, the low 0% EER of 0-spoofs can be retained and still a better spooﬁng resistance than sum rule is observed. The product rule performed slightly worse than sum rule with 1–5 spoof EERs of 3.35–15.72%.

As an interesting side-aspect of the evaluation conducted in this

paper, the effect of face-only vs. ﬁngerprint-only spooﬁng is inves- tigated. If always a speciﬁc modality is spoofed, a clear discrepancy of spooﬁng success can be observed: for 1-spoof spooﬁng restricted to spooﬁng the face image only (without spooﬁng detection) 7.33% EER is obtained (using sum rule), whereas ﬁngerprint-only spooﬁng results in 1.19% EER. This underlines the difﬁculty of ﬁnding suitable counter-spooﬁng fusion methods being able to tackle these different shifts in distributions. Note that however the quality of the employed

Table 3

EER/SEER (in %) and *d*-Prime results of face-and-ﬁnger fusion on the test set varying the number *m* of spoofed samples.

Method (S)EER d-Prime

*m* ¼ 0 *m* ¼ 1 *m* ¼ 2 *m* ¼ 3 *m* ¼ 4 *m* ¼ 5 *m* ¼ 0 *m* ¼ 1 *m* ¼ 2 *m* ¼ 3 *m* ¼ 4 *m* ¼ 5 Sum rule 0 2.32 5.71 7.52 10.38 12.24 2.91 2.62 2.27 2.11 1.89 1.67

Product rule 0 3.35 7.61 9.48 12.64 15.72 6.44 3.40 2.31 2.03 1.69 1.42

Median rule 0.42 0.87 1.20 3.91 6.74 10.03 2.38 2.37 2.31 2.14 1.89 1.68

Median ﬁltering (*ϕ* ¼ 1*σ*) 0 1.71 3.65 5.22 8.02 10.60 2.66 2.45 2.19 2.06 1.87 1.69

Median ﬁltering (*ϕ* ¼ 0:5*σ*) 0 1.03 2.04 3.50 6.23 9.53 2.29 2.17 2.01 1.90 1.75 1.69

1-Median ﬁlter 0.47 0.81 1.16 1.39 1.71 1.81 3.18 3.16 3.12 3.11 3.10 3.08

face database was also very challenging and thus impacting on this result. Experiments continue with the setup using random selection of spooﬁng samples (i.e. 20% probability to spoof face and 4 20% probability to spoof ﬁngerprint).

~

* 1. *Median ﬁltering*

In order to evaluate the suggested 1-median ﬁltering an experiment using LR on the joint liveness-and-score pairs is conducted, incorporat- ing liveness information into decision. Obtained EER for the method show much more stable results and also ROC curves are much ﬂatter, see [Fig. 8](#_bookmark13) plotted using log-scale. Median-ﬁltering on probabilities of already combined scores and liveness measures is able to retain EERs below 2% over all spooﬁng attempts, within a narrow band (0.81– 1.81%), and at the same time retains a very high 0-spoof accuracy (0.47%). Results refer to using a ﬁlter radius of *ϕ* 3*σ*, i.e. relative to the standard deviation of fused samples. Also corresponding *d*-Prime clearly illustrate the much better separation of genuine and *m*-impostor distribution. However, the tradeoff is a slightly degraded initial 0- spoof performance of 0.47% (which however, is much better than previously published results in [[10]](#_bookmark38) due to better spooﬁng detection).

¼

In a further experiment we veriﬁed the superiority of the median

compared to the mean when looking at simple recognition-score *m*- spoof imposter distributions. From [Table 2](#_bookmark14) we can see that (1) mean recognition scores decrease with the number of spoofed samples indicating an effect of the spooﬁng effort; and (2) median conse- quently delivered better performance suppressing the negative impact of spoofed samples (note the small changes especially for up to 2-spoof in contrast to the mean) conﬁrming theoretical considerations. Finally, we also tested the effect on variance and found that variance is increasing for a larger number of spoofed samples in multibiometric conﬁguration (e.g., *σ*2 0:00012 for 0-spoof, 0.0222 for 3-spoofed and 0.0293 for the 5-spoof case).

¼

Finally, a critical task in setting up parameters for the median ﬁltering is a suitable choice for the ﬁlter radius *ϕ*. The introduction of ﬁlter parameter *ϕ* results in a tradeoff permitting for better choices between the median rule (*ϕ* 0), which is better for suppression of spooﬁng attempts, and the sum rule (*ϕ* ), which delivers the best zero-spoof performance. While one method is to employ static values of *ϕ*, in order to avoid over-ﬁtting with regards to the training set, dynamic selection methods of *ϕ* are investigated, based on the scattering of input scores (e.g., as a factor of *σ* being the standard deviation of the *n* scores/tuples to be combined). As can be seen from ﬁlter evaluations on score-only combinations in [Table 3](#_bookmark15), small values of *ϕ* (0.5) deliver a closer performance to median ﬁltering, whereas larger values of *ϕ* are closer to the performance of the sum rule. This way an arbitrary compromise between classical accuracy using the sum rule and potentially slightly degraded 0-spoof performance but higher spooﬁng resistance, as for the median rule, can be obtained. While the paper does not aim to provide an assessment of computational cost, note that the overhead introduced by median ﬁltering is minimal, as the number *n* of employed features is typically a ﬁxed and low number.

¼ 1

≈

* 1. *Rejection of spooﬁng samples*

Finally, the classical alternative in many implementations imple- menting counter-spooﬁng functionality is to reject samples during quality assurance, if they appear to originate from a spoofed source. Unfortunately spooﬁng detector errors in multibiometric conﬁguration add up and cause a high number of falsely rejected genuine attempts. In order to virtually compare this method with the presented integrated approach, the ﬁnal score is set to 1, if and only if one or

more of the spooﬁng scores were greater than a threshold (*t*¼ 0.44 is

used). The resulting (virtual, as normally this would result in a Failure to Acquire error) EER of approx. 22% clearly illustrates the superiority of integrated recognition-and-spooﬁng fusion. Further, especially for commercial applications falsely rejected users are considered critical, whereas any threshold is typically set at a very conservative level which limits the use of employed techniques. Compared to techniques integrating liveness results, an advantage is that no information is lost and the overall scores can be taken into account.

1. Conclusion

Experiments in this paper show that 1-spooﬁng in face and ﬁngerprint fusion can successfully be targeted by employing med- ian instead of sum rule for combinations using its property to be less affected by a certain number of outliers. However, this comes at the cost of a reduced 0-spoof performance. Its extension to 1- median ﬁltering is able to ﬁnd arbitrary trade-off points between sum and median rule, allowing for better ﬂexibility in choosing the right tradeoff between accuracy and security. The paper investi- gated how spooﬁng detection and recognition can mutually beneﬁt from each other and evaluated 1-median ﬁltering as a novel multibiometric fusion method integrating liveness and recognition scores. Results yielded more stable results for this method in partial multibiometric spooﬁng conﬁguration, where *m* out of *n* samples of an identity are spoofed (EERs 0.47–1.81% vs. 0–12.24% for the sum rule). The paper presented an analysis of the ﬁlter radius in median ﬁltering and investigated the impact of face vs. ﬁngerprint spooﬁng. Finally, bootstrap aggregating (bagging) classiﬁers were proposed for anti-spooﬁng and shown to deliver highly accurate results (84% accuracy) on the challenging LivDet2013 crossmatch dataset. We believe the following remaining questions should be further inves- tigated in future work: a closer investigation of score normalisation issues for median ﬁltering; an extension towards user-adaptive anti-spooﬁng and recognition fusion, and; integration of extrinsic factors (e.g. acquisition conditions) and/or quality-related measure- ments into the fusion scheme.

Conﬂict of interest

None declared.

Acknowledgements

This work was supported by the EU FASTPASS project under Grant agreement 312583.

References

1. [A. Anjos, J. Komulainen, S. Marcel, A. Hadid, M. Pietikainen, Face anti-spooﬁng:](http://refhub.elsevier.com/S0031-3203(15)00295-2/sbref1) [visual approach, in: S. Marcel, et al., (Eds.), Handbook of Biometric Anti-](http://refhub.elsevier.com/S0031-3203(15)00295-2/sbref1) [Spooﬁng, Springer, London, 2014, pp. 65–82.](http://refhub.elsevier.com/S0031-3203(15)00295-2/sbref1)
2. [E. Marasco, A. Ross, A survey on antispooﬁng schemes for ﬁngerprint](http://refhub.elsevier.com/S0031-3203(15)00295-2/sbref2) [recognition systems, ACM Comput. Surv. 47 (2) (2014) 28:1–28:36.](http://refhub.elsevier.com/S0031-3203(15)00295-2/sbref2)
3. M. Chakka, et al., Competition on counter measures to 2-d facial spooﬁng attacks, in: Proceedings of the International Joint Conference on Biometrics, 2011, <http://dx.doi.org/10.1109/IJCB.2011.6117509>.
4. L. Ghiani, et al., Livdet 2013 ﬁngerprint liveness detection competition, in: Proceedings of the International Conference on Biometrics, 2013, [http://dx.doi.](http://dx.doi.org/10.1109/ICB.2013.6613027) [org/10.1109/ICB.2013.6613027](http://dx.doi.org/10.1109/ICB.2013.6613027).
5. E. Marasco, P. Johnson, C. Sansone, S. Schuckers, Increase the security of multi- biometric systems by incorporating a spooﬁng detection algorithm in the fusion mechanism, in: C. Sansone, et al. (Eds.), Proceedings of the International Work- shop on MCS, Lecture Notes in Computer Science, vol. 6713, Springer, Berlin, 2011, pp. 309–318, <http://dx.doi.org/10.1007/978-3-642-21557-5_33>.
6. I. Chingovska, A. Anjos, S. Marcel, Anti-spooﬁng in action: Joint operation with a veriﬁcation system, in: Proceedings of the International Conference on Computer Vision and Pattern Recognition, Workshop, 2013, pp. 98–104, [http://](http://dx.doi.org/10.1109/CVPRW.2013.22) [dx.doi.org/10.1109/CVPRW.2013.22](http://dx.doi.org/10.1109/CVPRW.2013.22).
7. N. Poh, R. Wong, G.-L. Marcialis, Toward an attack-sensitive tamper-resistant biometric recognition with a symmetric matcher: a ﬁngerprint case study, in: Proceedings of the Symposium on Computational Intelligence in Biometrics and Identity Management, 2014, pp. 1–6.
8. [R.N. Rodrigues, L.L. Ling, V. Govindaraju, Robustness of multimodal biometric](http://refhub.elsevier.com/S0031-3203(15)00295-2/sbref8) [fusion methods against spoof attacks, J. Vis. Lang. Comput. 20 (3) (2009) 169–179.](http://refhub.elsevier.com/S0031-3203(15)00295-2/sbref8)
9. Z. Akhtar, G. Fumera, G. Marcialis, F. Roli, Evaluation of multimodal biometric score fusion rules under spoof attacks, in: Proceedings of the International Conference on Biometrics, 2012, pp. 402–407, [http://dx.doi.org/10.1109/ICB.](http://dx.doi.org/10.1109/ICB.2012.6199784) [2012.6199784](http://dx.doi.org/10.1109/ICB.2012.6199784).
10. P. Wild, P. Radu, L. Chen, J. Ferryman, Towards anomaly detection for increased security in multibiometric systems: spooﬁng-resistant 1-median fusion elim- inating outliers, in: Proceedings of the International Joint Conference on Biometrics, 2014, <http://dx.doi.org/10.1109/BTAS.2014.6996293>.
11. A. Rattani, N. Poh, A. Ross, A Bayesian approach for modeling sensor inﬂuence on quality, liveness and match score values in ﬁngerprint veriﬁcation, in: Proceedings of the International Workshop on Information Forensics and Security, 2013, pp. 37–42, <http://dx.doi.org/10.1109/WIFS.2013.6707791>.
12. A. Rattani, A. Ross, Automatic adaptation of ﬁngerprint liveness detector to new spoof materials, in: Proceedings of the International Joint Conference on Biometrics, 2014, <http://dx.doi.org/10.1109/BTAS.2014.6996254>.
13. [G. Fumera, G. Marcialis, B. Biggio, F. Roli, S. Schuckers, Multimodal anti-](http://refhub.elsevier.com/S0031-3203(15)00295-2/sbref13) [spooﬁng in biometric recognition systems, in: S. Marcel, et al., (Eds.), Hand-](http://refhub.elsevier.com/S0031-3203(15)00295-2/sbref13) [book of Biometric Anti-Spoo](http://refhub.elsevier.com/S0031-3203(15)00295-2/sbref13)ﬁ[ng, Springer, London, 2014, pp. 165–184.](http://refhub.elsevier.com/S0031-3203(15)00295-2/sbref13)
14. I. Chingovska, A. Rabello dos Anjos, S. Marcel, Biometrics evaluation under spooﬁng attacks, IEEE Trans. Inf. Forensics Secur. 9 (12) (2014) 2264–2276. <http://dx.doi.org/10.1109/TIFS.2014.2349158>.
15. E. Marasco, Y. Ding, A. Ross, Combining match scores with liveness values in a ﬁngerprint veriﬁcation system, in: Proceedings of the International Confer- ence on Biometrics: Theory, Applications and Systems, 2012, pp. 418–425, <http://dx.doi.org/10.1109/BTAS.2012.6374609>.
16. J. Kittler, M. Hatef, R.P. Duin, J. Matas, On combining classiﬁers, IEEE Trans. Pattern Anal. Mach. Int. 20 (3) (1998) 226–239. [http://dx.doi.org/10.1109/](http://dx.doi.org/10.1109/34.667881) [34.667881](http://dx.doi.org/10.1109/34.667881).
17. R. Rodrigues, N. Kamat, V. Govindaraju, Evaluation of biometric spooﬁng in a multimodal system, in: Proceedings of the International Conference on Biometrics: Theory, Applications and Systems (BTAS), 2010, pp. 1–5, [http://](http://dx.doi.org/10.1109/BTAS.2010.5634531) [dx.doi.org/10.1109/BTAS.2010.5634531](http://dx.doi.org/10.1109/BTAS.2010.5634531).
18. Z. Akhtar, G. Fumera, G. Marcialis, F. Roli, Evaluation of serial and parallel multibiometric systems under spooﬁng attacks, in: Proceedings of the Inter- national Conference on Biometrics: Theory, Applications and Systems, 2012, pp. 283–288, <http://dx.doi.org/10.1109/BTAS.2012.6374590>.
19. A. Abhyankar, S. Schuckers, Fingerprint liveness detection using local ridge frequencies and multiresolution texture analysis techniques, in: Proceedings of the International Conference on Image Processing, 2006, pp. 321–324, <http://dx.doi.org/10.1109/ICIP.2006.313158>.
20. P. Coli, G. Marcialis, F. Roli, Power spectrum-based ﬁngerprint vitality detec- tion, in: Proceedings of the Workshop on Automatic Identiﬁcation Advanced Technologies, 2007, pp. 169–173. [http://dx.doi.org/10.1109/AUTOID.2007.](http://dx.doi.org/10.1109/AUTOID.2007.380614) [380614](http://dx.doi.org/10.1109/AUTOID.2007.380614).
21. S. Nikam, S. Agarwal, Fingerprint liveness detection using curvelet energy and co-occurrence signatures, in: Proceedings of the International Conference on Computer Graphics, Imaging and Visualisation, 2008, pp. 217–222, [http://dx.](http://dx.doi.org/10.1109/CGIV.2008.9) [doi.org/10.1109/CGIV.2008.9](http://dx.doi.org/10.1109/CGIV.2008.9).
22. L. Ghiani, G. Marcialis, F. Roli, Fingerprint liveness detection by local phase quantization, in: Proceedings of the International Conference on Pattern Recognition, 2012, pp. 537–540.
23. [A. Anjos, M.M. Chakka, S. Marcel, Motion-based counter-measures to photo](http://refhub.elsevier.com/S0031-3203(15)00295-2/sbref23) [attacks in face recognition, IET Biometrics 3 (3) (2013) 147–158.](http://refhub.elsevier.com/S0031-3203(15)00295-2/sbref23)
24. G. Zhao, M. Pietikainen, Dynamic texture recognition using local binary patterns with an application to facial expressions, IEEE Trans. Pattern Anal. Mach. Int. 29 (6) (2007) 915–928. <http://dx.doi.org/10.1109/TPAMI.2007.1110>.
25. X. Tan, Y. Li, J. Liu, L. Jiang, Face liveness detection from a single image with sparse low rank bilinear discriminative model, in: K. Daniilidis, et al. (Eds.), ECCV 2010, Lecture Notes in Computer Science, vol. 6316, 2010, pp. 504–517.
26. T. de Freitas Pereira, A. Anjos, J.M. de Martino, S. Marcel, LBP-TOP based countermeasure against face spooﬁng attacks, in: Proceedings of the Work- shop on Computer Vision, Springer, 2013, pp. 121–132, [http://dx.doi.org/10.](http://dx.doi.org/10.1007/978-3-642-37410-4_11) [1007/978-3-642-37410-4\_11](http://dx.doi.org/10.1007/978-3-642-37410-4_11).
27. [P.T. von Hippel, Mean, median, and skew: correcting a textbook rule, J. Stat.](http://refhub.elsevier.com/S0031-3203(15)00295-2/sbref27) [Educ. 13 (2) (2005) 1–13.](http://refhub.elsevier.com/S0031-3203(15)00295-2/sbref27)
28. [D. Moore, G. McCabe, Introduction to the Practice of Statistics, Freeman, New](http://refhub.elsevier.com/S0031-3203(15)00295-2/sbref28) [York, 2003.](http://refhub.elsevier.com/S0031-3203(15)00295-2/sbref28)
29. [N. Otsu, A threshold selection method from gray-level histograms, IEEE Trans.](http://refhub.elsevier.com/S0031-3203(15)00295-2/sbref29) [Syst. Man Cybern. 9 (1) (1979) 62–66.](http://refhub.elsevier.com/S0031-3203(15)00295-2/sbref29)
30. J. Daugman, Complete discrete 2-d Gabor transforms by neural networks for image analysis and compression, IEEE Trans. Acoust. Speech Signal Process. 36 (7) (1988) 1169–1179. <http://dx.doi.org/10.1109/29.1644>.
31. S.B. Nikam, S. Agarwal, Gabor ﬁlter-based ﬁngerprint anti-spooﬁng, in: J. Blanc-Talon, et al. (Eds.), Proceedings of the International Conference on ACIVS, Lecture Notes in Computer Science, vol. 5259, Springer, Berlin, 2008, pp. 1103–1114, <http://dx.doi.org/10.1007/978-3-540-88458-3_100>.
32. H. Choi, R. Kang, K. Choi, A. Jin, J. Kim, Fake-ﬁngerprint detection using multiple static features, Opt. Eng. 48 (2009) 047202–047202–13.
33. L. Breiman, Bagging predictors, Mach. Learn. 24 (2) (1996) 123–140. [http://dx.](http://dx/) doi.org/10.1023/A:1018054314350.
34. [B. Efron, R.J. Tibshirani, An Introduction to the Bootstrap, Chapman](http://refhub.elsevier.com/S0031-3203(15)00295-2/sbref34) & [Hall,](http://refhub.elsevier.com/S0031-3203(15)00295-2/sbref34) [New York, 1994.](http://refhub.elsevier.com/S0031-3203(15)00295-2/sbref34)
35. N. Poh, A. Merati, J. Kittler, Heterogeneous information fusion: a novel fusion paradigm for biometric systems, in: Proceedings of the International Joint Conference on Biometrics, 2011, pp. 1–8, [http://dx.doi.org/10.1109/IJCB.2011.](http://dx.doi.org/10.1109/IJCB.2011.6117494) [6117494](http://dx.doi.org/10.1109/IJCB.2011.6117494).
36. P. Johnson, B. Tan, S. Schuckers, Multimodal fusion vulnerability to non-zero effort (spoof) imposters, in: Proceedings of the International Workshop on Information Forensics and Security, 2010, pp. 1–5, [http://dx.doi.org/10.1109/](http://dx.doi.org/10.1109/WIFS.2010.5711469) [WIFS.2010.5711469](http://dx.doi.org/10.1109/WIFS.2010.5711469).
37. I. Chingovska, A. Anjos, S. Marcel, On the effectiveness of local binary patterns in face anti-spooﬁng, in: Proceedings of the International Conference of the Biometrics Special Interest Group (BIOSIG), 2012, pp. 1–7.
38. Z. Zhang, J. Yan, S. Liu, Z. Lei, D. Yi, S. Li, A face antispooﬁng database with diverse attacks, in: Proceedings of the International Conference on Biometrics, 2012, pp. 26–31, <http://dx.doi.org/10.1109/ICB.2012.6199754>.
39. NIST, Biometric Image Software V4.2, 2013, 〈[http://www.nist.gov/itl/iad/ig/](http://www.nist.gov/itl/iad/ig/nbis.cfm) [nbis.cfm](http://www.nist.gov/itl/iad/ig/nbis.cfm)〉.
40. Neurotechnology Inc, VeriLook SDK, 2014, 〈[http://www.neurotechnology.com/](http://www.neurotechnology.com/verilook.html) [verilook.html](http://www.neurotechnology.com/verilook.html)〉.

Peter Wild received his Ph.D. degree in computer science with “sub-auspiciis- praesidentis” honours (2013) from the University of Salzburg, where he held positions as Research Assistant (2007–2012) and Postdoc (2013). Currently, he is Postdoc in computer vision at the University of Reading. His research was awarded the European Biometrics Industry Award 2013.

Petru Radu is a Research Associate at the University of Reading, UK. In 2013, he obtained his Ph.D. in iris recognition at the University of Kent, where he continued as a Postdoc in Image Processing and Document Analysis. Petrus research interests include statistical pattern recognition, image processing and multiple classiﬁer systems.

Lulu Chen received her Ph.D. degree in computer science from the University of Reading in 2013, and currently works as a Postdoc in the University of Reading. Her research interests include computer vision, image processing, biometric recogni- tion for automated border control, biometric counter-spooﬁng and human action recognition with sensor fusion.

James M. Ferryman (M96) received his Ph.D. degree in computational vision in 2000 from the University of Reading and became a Full Professor in 2014. Prof. Ferryman leads the Computational Vision Group. His current research interests include biometrics for border control, multi-sensor surveillance, behavioral analy- sis, cognitive systems, and performance evaluation.