REAL TIME FACE SPOOF DETECTION

[1]FARISA K A, [2]MABLE JOSE T
[1]M.Sc STUDENT, [2]ASSISTANT PROFESSOR
DEPARTMENT OF COMPUTER SCIENCE
ST.JOSEPH'S COLLEGE, IRINJALAKKUDA

Abstract— Automatic face recognition is now widely used in applications ranging from deduplication of identity to authentication of mobile payment. This popularity of face recognition has raised concerns about face spoof attacks (also known as biometric sensor presentation attacks), where a photo or video of an authorized person's face could be used to gain access to facilities or services. While a number of face spoof detection techniques have been proposed, their generalization ability has not been adequately addressed. We propose an efficient and rather robust face spoof detection algorithm based on image distortion analysis (IDA). Four different features (specular reflection, blurriness, chromatic moment, and color diversity) are extracted to form the IDA feature vector. An ensemble classifier, consisting of multiple SVM classifiers trained for different face spoof attacks (e.g., printed photo and replayed video), is used to distinguish between genuine (live) and spoof faces. The proposed approach is extended to multiframe face spoof detection in videos using a voting-based scheme. We also collect a face spoof database, MSU mobile face spoofing database (MSU MFSD), using two mobile devices (Google Nexus 5 and MacBook Air) with three types of spoof attacks (printed photo, replayed video with iPhone 5S, and replayed video with iPad Air). Experimental results on two public-domain face spoof databases (Idiap REPLAY-ATTACK and CASIA FASD), and the MSU MFSD database show that the proposed approach outperforms the state-of-the-art methods in spoof detection. Our results also highlight the difficulty in separating genuine and spoof faces, especially in cross-database and cross-device scenarios.

Index Terms—face recognition,spoof detection,image distrotion analysis,ensemble classifier,cross-databse,cross-device.

I. INTRODUCTION

AS A convenient user authentication technique, automatic face recognition has attracted increasing attention in various access control applications, especially for mobile phone unlocking. With the release of face unlocking functionality in the Android mobile operating system, face recognition becomes another biometric authentication technique for mobile phones,similar to fingerprintauthentication(Touch ID) in the iOS system. Unlike fingerprint authentication, face recognition does not require any additional sensor since all smart phones come equipped with a front facing camera. However, similar to other biometric modalities, we need to address concerns about face spoof attacks on face recognition systems, particularly in unconstrained sensing and uncooperative subject scenarios. It is relatively easier to acquire a person's face image or video (e.g., with a digital camera or from social media) than it is to acquire other biometric traits such as fingerprint, palm print, and iris. Further, the cost of launching a face spoof attack, such as a printed photo, displayed photo, or replayed video is relatively low . State of the art Commercial Off-The-Shelf (COTS) face recognition systems are not well designed to differentiate spoof faces from genuine live faces. Figure 2 shows the face identification performance of a COTS face recognition system (COTS11) when spoof faces as probe are matched to genuine faces in the gallery. In this experiment,more than 70% of probe videos (spoof faces) were successfully matched to the gallery mates by COTS1 at rank-1, indicating that COTS1 cannot effectively distinguish between genuine and spoof faces. In this paper we do not address 3D face mask attacks, which are more expensive to launch.2 Instead, we focus on printed photo and replayed video attacks. The fragility of face recognition systems to face spoof attacks has motivated a number of studies on face spoof detection . However, published studies are limited in their scope because the training and testing images (videos) used were captured under the same imaging conditions. It is essential to develop robust and efficient face spoof detection (or anti-spoofing) algorithms that generalize well to new imaging conditions and environments. In this paper, we study the cross-database face spoof detection problem and propose a face spoof detection approach based on Image Distortion Analysis (IDA). The contributions of this paper can be summarized as follows:

- **i)** A face spoof detection algorithm based on IDA, which is effective in grasping the intrinsic distortions of spoof face images with respect to the genuine face images.
- **ii)** We construct a face spoof database, named the MSU Mobile Face Spoof Database (MSU MFSD), using the cameras of a laptop (MacBook Air3) and a mobile phone (Google Nexus 54) and three types of attack medium (iPad, iPhone, and printed photo). The MSU MFSD database allows us to evaluate the generalization ability of face spoof detection algorithms across different cameras and illumination conditions with mobile devices. For a subset of the MSU MFSD database (35 subjects), we have the subjects' permission to make their data publicly available.
- **iii)** We present results for both intra-database and cross-database scenarios using two public-domain face spoof databases (Idiap REPLAY-ATTACK and CASIA FASD), and our own database (MSU MFSD).

II. LITERATURE SURVEY

The contributions of Chingovask [4] paper can be summarized as follows. Firstly, it introduces REPLAY-ATTACK, a novel spoofing attack database containing three types of possible attacks using three different media and two different recording conditions. Secondly, it proposes simple and easily reproducible LBP based face spoofing counter-measure and explores its efficiency against a variety of attacks. Variants of LBP were also investigated, but the regular LBPu2 3×3 shows the best performance/complexity tradeoff. .[1] In the face spoof detection techniques, the technique is been applied which will detect the fake images which are given as input to take access of the data of the biometric system. In the paper, various techniques of spoof detection is been reviewed in terms of description and outcome.

.

III. PROPOSED SYSTEM

To evaluate the effectiveness and generalization ability of the proposed face spoof detection methods, we use both intra-database and cross-database protocols. For intra-database testing, we follow the conventional definition of training, developing (if available), and testing

sets in the Idiap and CASIA databases. We also define a cross-database protocol to evaluate the generalization ability of spoof detection methods.

A. Intra-Database Testing Protocol

For the Idiap spoof database, we follow the protocols specified in by using all frames in the training and developingsets for training and parameter tuning, respectively. The optimized classifiers are then tested on all frames in the testing set to evaluate the intra-database performance on the Idiap database. For the CASIA spoof database, the low quality subset (L) and normal quality subset (N) contain only long distance spoof attack samples; only the High quality subset (H) contains short distance spoof attack samples. Therefore, we only test our method under the H protocol specified in for the given training and testing sets. For the MSU spoof database, there are a total of 55 subjects. We use 35 subjects for the training set and the other 20 for the testing set. The publicly available MSU database (35 subjects) will contain the same testing set (20 subjects) defined here but only a subset of the training set (15 subjects). In this paper, we report the spoof detection performance using both the publicly available MSU database and the complete MSU database. Since there is no developing set in the CASIA and MSU databases, parameter tuning was conducted by crossvalidation on the training set. The intra-database performance of the proposed approach on the Idiap and CASIA databases can be directly compared with the state-of-the-art methods.

B. Cross-Database Testing Protocol

The cross-data base performance is evaluated by training the spoof detector on database A (e.g., Idiap) and testing it on a different database B (e.g., MSU), and vice versa. In each cross-database experiment, multi-fold validation is conducted to enumerate different subsets of databases A and B for training and testing, respectively. For example, when using database A for training and database B for testing, we have four possibilities: training on the training set of A and testing on the training/testing set of B; training on the testing set of A and testing on the training/testing set of B. The average performance of this 4-fold evaluation is reported along with variance. Under the above protocol, a good cross-database performance will provide strong evidence that: i) features are generally invariant to different scenarios (i.e., camera and illuminations), ii) a spoof classifier trained on one scenario is generalizable to the other scenario, and iii) data captured in one scenario can be useful for developing spoof detectors working in the other scenario.

C. Baseline Methods

Most of the published methods have been evaluated on the two public-domain face spoof databases (e.g., Idiap and CASIA) following an intra-database testing protocol. Very few publications have reported the crossdatabase face spoof detection performance . We have implemented two state of the art methods based on the LBP features .12 These two baseline methods use the same front-end processing described in Section III for face detection and normalization. For each normalized face image, the first method extracts uniform LBP features, including LBPu2 8,1, LBPu2 8,2, LBPu2 8,3, LBPu2 8,4 and LBPu2 16,2 channels, constituting a 479-dimensional feature vector.13 For the second method , the 479-dimensional LBP feature vector is extracted after the normalized face image is convolved by a Differences of Gaussian (DoG) filter. This DoG filter was proposed to improve the robustness of LBP features, with $\sigma 1 = 0.5$ and $\sigma 2 = 2$. The resultant LBP features are then fed to train SVM classifiers. These two baseline methods are referred to as LBP+SVM and DoG-LBP+SVM in the experimental results.

NUMBER OF GENUINE AND SPOOF FACES USED IN OUR EXPERIMENT

Database	Training		Developing		Testing	
	Genuine	Spoof	Genuine	Spoof	Genuine	Spoof
Idiap	22,497	69,686	22,498	70,246	29,791	93,686
CASIA (H)	4,579	11,858	–	–	5,603	16,958
MSU	11,567	33,050	–	–	11,178	33,102

COMPARISON OF INTRA-DATABASE PERFORMANCE ON THE IDIAP, CASIA AND MSU DATABASES

Method	Intra-DB testing on Idiap			Intra-DB testing on CASIA (H protocol)			Intra-DB testing on MSU		
	HTER(%)	TPR@ FAR=0.1	TPR@ FAR=0.01	EER(%)	TPR@ FAR=0.1	TPR@ FAR=0.01	EER(%)	TPR@ FAR=0.1	TPR@ FAR=0.01
LBP-TOP u2 [17]	8.51	≈94.5	≈74.5	13 (75 frms)	≈82	**≈81**	N/A	N/A	N/A
LBP-TOP [16]	7.60	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
CASIA DoG baseline [9]	N/A	N/A	N/A	26 (30 frms)	≈45	≈14	N/A	N/A	N/A
LBP+SVM baseline	16.1	94.5	57.3	7.5 (30 frms)	**93.3**	29.7	14.7†	69.9†	21.1†
				6.7 (75 frms)	**93.3**	49.0	10.9‡	87.0‡	31.5‡
DoG-LBP+SVM baseline	11.1	92.1	67.0	14.2 (30 frms)	66.7	53.3	23.1†	62.8†	16.4†
				12.7 (75 frms)	84.4	49.7	14.0‡	77.3‡	21.4‡
IDA+SVM (proposed)	7.41	92.2	**87.9**	13.3 (30 frms)	86.7	50	**8.58**†	**92.8**†	**64.0**†
				12.9 (75 frms)	86.7	59.7	**5.82**‡	**94.7**‡	**82.9**‡

†Using the 35 publicly available subjects in the MSU database, 15 for training and 20 for testing.
‡Using all the 55 subjects in the MSU database, 35 for training and 20 for testing.

IV. ANALYSIS

We evaluated three different types of spoof detection feature vectors: LBP features (as used in), DoG-LBP features (as used in), and IDA features defined here. The Idiap REPLAY-ATTACK, CASIA FASD (H protocol), and MSU MFSD databases are used for experiments. The same classification configuration is adopted for comparing the IDA and other features. When training on a data set with multiple types of spoof attack, the ensemble classifier scheme is used. While training on a data set with only one type of attack, a single classifier scheme is used. Again, for both intra-database and cross-database experiments related to the MSU database, we report the performance on two sets of the MSU MFSD database: the entire dataset with 55 subjects, and a subset with 35 subjects which are publicly available.

Method	Trained on Idiap and tested on MSU				Trained on MSU and tested on Idiap			
	TPR@↑ FAR=0.1	TPR@↑ FAR=0.01	TPR@↓ FAR=0.1	TPR@↓ FAR=0.01	TPR@↑ FAR=0.1	TPR@↑ FAR=0.01	TPR@↓ FAR=0.1	TPR@↓ FAR=0.01
LBP+SVM	34.6±9.8	4.7±2.7	35.7±10.8	4.0±2.5	35.7±8.9	10.4±3.3	42.9±14.2	9.0±2.8
DoG-LBP+SVM	69.0±11.4	30.7±18.9	73.9±16.4	38.3±26.9	54.2±7.8	17.4±7.1	45.1±8.1	10.7±3.8
IDA+SVM (proposed)	**99.6±0.7**	**90.5±5.7**	**99.9±0.1**	**90.4±8.4**	**82.2±8.9**	**47.2±21.2**	**74.9±16.3**	**46.5±20.8**

(a)

Method	Trained on Idiap and tested on MSU				Trained on MSU and tested on Idiap			
	TPR@↑ FAR=0.1	TPR@↑ FAR=0.01	TPR@↓ FAR=0.1	TPR@↓ FAR=0.01	TPR@↑ FAR=0.1	TPR@↑ FAR=0.01	TPR@↓ FAR=0.1	TPR@↓ FAR=0.01
LBP+SVM	23.4±11.4	9.0±9.7	24.7±10.6	11.5±12.4	12.1±8.6	4.7±4.6	23.8±3.4	8.1±3.3
DoG-LBP+SVM	16.7±1.3	6.6±1.6	15.1±1.7	5.6±1.4	39.2±13.2	20.0±8.9	48.8±21.7	25.8±15.9
IDA+SVM (proposed)	**64.4±1.7**	**31.2±3.7**	**61.1±4.5**	**26.0±2.4**	**72.5±5.3**	**29.4±17.0**	**69.1±2.2**	**38.5±12.8**

(b)

Method	Trained on CASIA and tested on MSU				Trained on MSU and tested on CASIA			
	TPR@↑ FAR=0.1	TPR@↑ FAR=0.01	TPR@↓ FAR=0.1	TPR@↓ FAR=0.01	TPR@↑ FAR=0.1	TPR@↑ FAR=0.01	TPR@↓ FAR=0.1	TPR@↓ FAR=0.01
LBP+SVM	7.8±3.6	0.2±0.2	6.1±3.6	0	0.8±1.1	0	0.5±0.8	0.1±0.1
DoG-LBP+SVM	14.2±3.8	4.8±5.0	14.7±3.6	6.2±5.5	4.6±0.7	0.2±0.1	5.9±3.6	0.2±0.1
IDA+SVM (proposed)	**67.2±31.8**	**33.8±29.8**	**67.9±31.9**	**43.0±39.8**	**26.9±4.4**	**10.8±3.2**	**28.3±5.8**	**11.9±7.1**

(c)

Method	Trained on CASIA and tested on MSU				Trained on MSU and tested on CASIA			
	TPR@↑ FAR=0.1	TPR@↑ FAR=0.01	TPR@↓ FAR=0.1	TPR@↓ FAR=0.01	TPR@↑ FAR=0.1	TPR@↑ FAR=0.01	TPR@↓ FAR=0.1	TPR@↓ FAR=0.01
LBP+SVM	2.3±0.5	0	3.0±0.6	1.2±1.4	**6.0±1.0**	**0.5±0.5**	6.9±1.4	0.8±0.5
DoG-LBP+SVM	6.0±1.7	0.4±0.5	10.6±5.2	1.8±2.9	4.1±1.3	0	4.1±1.7	0.1±0.1
IDA+SVM (proposed)	**21.9±4.2**	**1.4±1.1**	**26.9±6.4**	**1.6±1.0**	2.1±0.5	0	**9.1±7.2**	**1.1±1.3**

(d)

TABLE:COMPARISONOF CROSS-DATABASE PERFORMANCEOF DIFFERENTMETHODS.
(a) CROSS-DATABASE PERFORMANCE(%) ON REPLAY ATTACK SAMPLESBETWEEN THE IDIAP AND MSU DATABASES.(b)CROSS-DATABASE PERFORMANCE(%) ON PRINTEDATTACK SAMPLES BETWEEN THE IDIAP AND MSUDATABASES.(c)CROSS-DATABASE PERFORMANCE(%) ON REPLAY ATTACK SAMPLES BETWEEN THE CASIA AND MSUDATABASES.(d)CROSS-DATABASE PERFORMANCE(%) ON PRINTED ATTACK SAMPLESBETWEEN THE CASIA AND MSU DATABASES.

V. CONCLUSION

In this paper, we address the problem of face spoof detection, particularly in a cross-database scenario. While most of the published methods use motion or texture based features, we propose to perform face spoof detection based on Image Distortion Analysis (IDA). Four types of IDA features (specular reflection, blurriness, color moments, and color diversity) have been designed to capture the image distortion in the spoof face images. The four different features are concatenated together, resulting in a 121-dimensional IDA feature vector. An ensemble classifier consisting of two constituent SVM classifiers trained for different spoof attacks is used for the classification of genuine and spoof faces. We have also collected a face spoof database, called MSU MFSD, using two mobile devices (Android Nexus 5, and MacBook Air 13. To our knowledge, this is the first mobile spoof face database. A subset of this database, consisting of 35 subjects, will be made publicly available

Evaluations on three face spoof databases (Idiap REPLAY-ATTACK, CASIA FASD, and MSU MFSD) show that the proposed approach performs better than the state-of-the-art methods in intra-database testing scenario and significantly outperforms the baseline methods in cross-database scenario.

REFERENCES

[1] Ramandeep kaur, P.S Mann, “Techniques of Face spoof Detection:review,”.

[2] Z. Wu, N. Evans, T. Kinnunen, J. Yamagishi, F. Alegre, and H. Li, “Spoofing and countermeasures for speaker verification: A survey,” Speech Commun., vol. 66, pp. 130–153, Feb. 2015.

[3] L. Best-Rowden, H. Han, C. Otto, B. F. Klare, and A. K. Jain, “Unconstrained face recognition: Identifying a person of interest from a media collection,” IEEE Trans. Inf. Forensics Security, vol. 9, no. 12, pp. 2144–2157, Dec. 2014.

[4] I. Chingovska, A. Anjos, and S. Marcel, “On the effectiveness of local binary patterns in face anti-spoofing,” in Proc. IEEE BIOSIG, Sep. 2012, pp. 1–7.

[5] N. Erdogmus and S. Marcel, “Spoofing in 2D face recognition with 3D masks and anti-spoofing with Kinect,” in Proc. IEEE BTAS, Sep./Oct. 2013, pp. 1–6.Y.

[6] Z. Zhang, D. Yi, Z. Lei, and S. Z. Li, “Face liveness detection by learning multispectral reflectance distributions,” in Proc.FG, Mar. 2011, pp. 436–441.

[7] A. Anjos and S. Marcel, “Counter-measures to photo attacks in face recognition: A public database and a baseline,” in Proc. IJCB, Oct. 2011, pp. 1–7.

[8] X. Tan, Y. Li, J. Liu, and L. Jiang, “Face liveness detection from a single image with sparse low rank bilinear discriminative model,” in Proc. ECCV, Sep. 2010, pp. 504–517.

[9] Z. Zhang, J. Yan, S. Liu, Z. Lei, D. Yi, and S. Z. Li, “A face antispoofing database with diverse attacks,” in Proc. ICB, Mar./Apr. 2012, pp. 26–31.

[10] L. Sun, G. Pan, Z. Wu, and S. Lao, “Blinking-based live face detection using conditional random fields,” in Proc.AIB,2007, pp. 252–260.

[11] W. Bao, H. Li, N. Li, and W. Jiang, “A liveness detection method for face recognition based on optical flow field,” in Proc. IASP, Apr. 2009, pp. 233–236.

[12] S. Bharadwaj, T. I. Dhamecha, M. Vatsa, and R. Singh, “Computationally efficient face spoofing detection with motion magnification,” in Proc. IEEE Conf. Comput. Vis. Pattern Recognit. Workshops (CVPRW), Jun. 2013, pp. 105–110.