Large Crowdcollected Facial Anti-Spoofing Dataset

1st Denis Timoshenko
ID R&D Inc.
New York, USA
timoshenko@idrnd.net

2nd Konstantin Simonchik
ID R&D Inc.
New York, USA
simonchik@idrnd.net

3rd Vitaly Shutov
ID R&D Inc.
New York, USA
shutov@idrnd.net

4th Polina Zhelezneva
ID R&D Inc.
New York, USA
zhelezneva@idrnd.net

5th Valery Grishkin
dept. Computer Modelling and Multiprocessor Systems
Saint Petersburg State University
Saint Petersburg, Russia
valery-grishkin@yandex.ru

***Abstract*—The study about the vulnerabilities of biometric systems against spoofing has been a very active field of research in recent years. In this particular research we are focusing on one of the most difficult types of attack — video replay. We have noticed that currently most of face replay anti-spoofing databases focus on data with little variations of the devices used for replay and record. This fact may limit the generalization performance of trained models since potential attacks in the real world are probably more complex. In this review we present a face anti-spoofing database, which covers a huge range of different devices used for recording and for the video playback. The database contains 1942 genuine images, and 16885 fake faces are made from high quality records of the genuine faces. The database was collected using Amazon Mechanical Turk and Yandex Toloka services. The database was manually checked and the test protocol was provided. Some methods are also provided to be used as a baseline for future research. We hope that database as such can serve as an evaluation platform for the future studies in the literature.**

***Index Terms*—computer science, biometrics, datasets.**

I. Introduction

The facial recognition system has been widely implemented in daily life [1]. The facial recognition technology is usually used in the system because it simplifies the process of secure login or increases its accuracy as a second factor authentication [2]. However, the facial recognition system has some drawbacks such as spoofing [3]. Facial spoofing is an attack that deceives the facial recognition system using imprinted images or videos played on the screen. Spoofing attack occurs when someone tries to impersonate a registered user by forging the face and taking advantage of such illegal access. There are some possible types of attacks: printed photo, photo on the screen, video played on the screen, 3D face rendering, mask [4] or 3D mask [5]. Most of the work on the facial spoofing detection focuses on the outline structure of facial expressions such as: eye blinking, lip or head movement. We hope that a detailed description of the features can be extracted to detect the spoofed sample and the valid sample. However, the system, which asks the users to turn their head or blink or make some other type of mimic movements, is not comfortable for the users. This fact leads the study of the totally frictionless facial spoofing recognition technology that doesnt require any specific actions from the users. In this project, we are concentrating on the creation of such a database, which will be used to train the anti-spoofing system that meets the following requirements: the system doesn't require the users to do any mimics, putting the focus on the professional database collection process — high risk spoofing attacks, there shouldn't be any visible frames on the image, maximizing versatility of the devices used for spoofing as well as for the image recording.

Compared with previous databases, our database has much wider coverage of data variation as shown in Section III. We further developed a baseline algorithm to get a preliminary study. In Section II, we provide a comparative analysis of the presented database and the existing ones, as well as the analysis of the amount of identities and the devices used for spoofing. It is worth mentioning that most of the existing spoofing datasets consist of attacks using a printed photo mainly, while the presented database contains images reproduced from the screens of different quality. The second distinguishing feature is the amount of different devices used for spoofing attacks. At the end of the section there is a detailed description of the test protocols, as well as recommended metrics to be estimated. In Section III we give a description of the baseline system for detecting spoofing attacks. The result of the experiment shows that utilization of presented here dataset paves the way for creation of really accurate, fast and convenient algorithm that can detect replay spoofing attack even using a single image.

II. LCC FASD description

A. Comparison with Previous Databases

As we were focused on collecting the data for the antispoofing database to train and evaluate the algorithm that should allow the implementation of truly frictionless, secure and fast antispoofing technology, the database was formed according to the following basic principles:

- There are no requirements for the face mimicking for the user.
- No frames/borders must be visible at the image.
- Wide range of displaying and capturing devices available on the market should be used.

- Short videos or single images should be collected.

In Tab. I we provided a statistical comparison with previous NUAA and Idiap databases, which are the only existing databases available to the anti-spoofing researchers. NUAA database uses photos of different sizes as attacks like it is shown in Tab. I. In Idiap only A4-sized photos are used to maximize the preservation of the facial textures. In contrast, our database used wide range of quality photos presented from the screen, the photos were captured by a large variety of devices (smartphones mostly).

TABLE I
STATISTICAL COMPARISON WITH PREVIOUS DATABASES

Database	Identities	Devices	Volume
CASIA FASD [6]	50	n/a	600
OULU NPU [7]	55	4	4950
Idiap Replay-Attack [8]	50	3	400
Replay-Mobile [9]	40	2	1190
NUAA [10]	15	n/a	12641
Spoof in the Wild [11]	165	4	4478
LCC FASD (ours)	243	83	18827

The dataset consists of the images captured from the short videos with the face of the user being cropped. The cropping parameters were made so that the face was in the center of the image with the additional gap between the face and borders. The image was un-resizable so that original properties of the image couldn't be tampered with. Thereby absolute size of the images varies between 150 and 1350 pixels.

The examples of the genuine and the spoofed images are shown in Fig. 1 and Fig. 2.

Fig. 1. Example of the genuine images.

B. Database Statistics

LCC FASD is consisted of 3 subsets: training, development and evaluation. Totally there are 1942 genuine images and 16885 spoofing images collected from Youtube, Amazon Mechanical Turk (https://www.mturk.com/) and Yandex Toloka

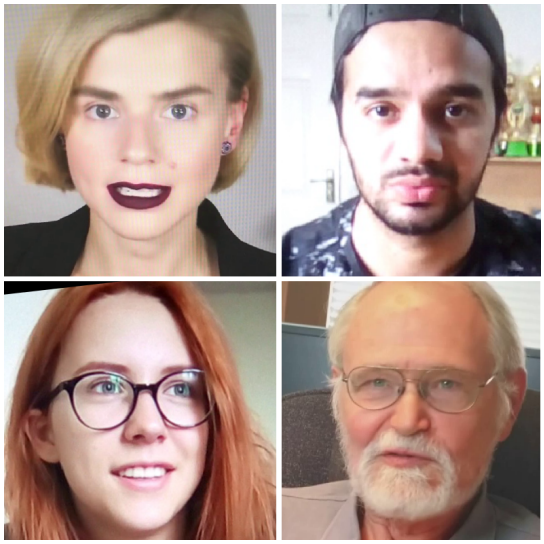

Fig. 2. Example of the spoofed images.

(https://toloka.yandex.com/) web services. The subject and image statistics are presented in Tab. II.

TABLE II
STATISTIC OF SUBJECTS AND IMAGES FOR LCC FASD

Part	Identities	Genuine images	Spoofing images
training	118	1223	7076
development	25	405	2543
evaluation	100	314	7266
TOTAL	243	1942	16885

The advantage of the database is the wide range of spoofing and recording devices. Since the specified web services were used this allowed us to get an insight on the devices typically used by the people who participated in the collection process. Thereby the presentation of the devices should be almost the same as the presentation existed on the market.

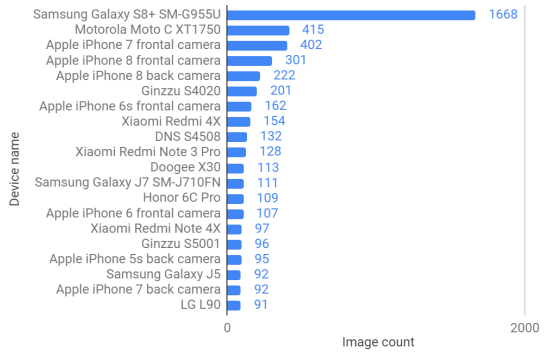

Fig. 3. Top-20 recording devices.

Fig. 3 shows the top-20 used cameras for image capturing. Totally 83 devices were used for capturing. Fig. 4 shows the top-20 used devices for image displaying. Totally 82 devices were used for displaying. The

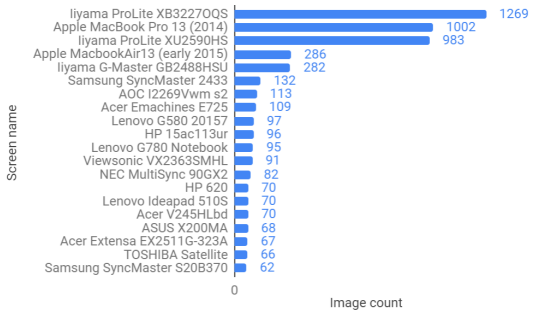

Fig. 4. Top-20 displaying devices.

whole database can be downloaded through the link: https://drive.google.com/open?id=1NeyTFAwdJSjxA9ZtdviwdUjdptEVjM_i.

C. Training and Evaluation Protocol

The whole database has been split into the training, development and evaluation sets. This separation allows the use of the dataset for scientific research purposes and also for the challenge. Researchers are free to use development set both for training and calibration of the system. Evaluation set is not made for training or for calibration.

The evaluation of the antispoofing algorithm implies that a set of performance characteristics should be estimated using the evaluation set only: Detection-Error Trade-off (DET). From DET curves, the point where FAR equals FRR is located, and the corresponding value, which is called the Equal Error Rate (EER), should also be reported. For any evaluating algorithm, a DET curve and EER result should be reported. Example can be seen in the following section for the baseline algorithm.

Researchers are free to use any additional metrics to report their algorithm performance. Error cost function, which is the weight sum of FAR and FRR can be used. Considering security typical system operates with low FAR values the cost function usually operates with FAR weight significantly more compared to the FRR one. Thus, FAR in the optimum of the cost function is much smaller than FRR and should be estimated with a much lower error. For that situation the amount of spoofing images prevails to the genuine subset.

III. Antispoofing methods

In this section, we introduce two different spoofing attack detection methods to evaluate the dataset. First method is based on classical Local Binary Patterns (LBP) and Gradient Boosting Machine (GBM) approach, the second one is based on Deep Neural Network. Finally we compare the experimental results and analyze them.

A. LBP-GBM method

a) Color spaces: RGB is one of the most popular models for sensing and displaying. But because of the high correlation between the channels it is better to use other color spaces: HSV and YCrCb. Both of them are based on color separation of the luminance and chrominance information. So we can make an assumption that spoof and real images can be separated much simpler in this channel.

b) Features: Frequency features are extracted from face using log-scale magnitude of 2-D discrete Fourier transform. After transformation is applied, we're shifting zero-frequency component to the center of the spectrum.

Radius of the rings was selected by the image larger side divided by 32. Totally 32 rings are extracted from the image. Then mean and deviation magnitude values are pulled and concatenated from all the rings into the single 64 dimensional vector. This vector is normalized using L2 norm.

Texture characteristics are extracted from the face using uniform LBP. From each of HSV and YCrCb channels we're extracting LBP vector with radius 2 and 18 of neighbors and concatenate them together. Also we're extracting LBP vector from channels with applied Gaussian blur filter with 3×3 kernel and $\sigma = 1/2$.

Keypoint features extracted using ORB [12] feature descriptor. ORB descriptor matrix extracted from face then from each column of matrix mean and std computed. Before concatenating vectors we're normalizing them using L2 norm. In the end result we have 64 dimensional vector from keypoint features.

As a result of all extractions, we got a 418 dimensional vector, which is passed to the classifier.

c) Classifier: Due to the nonlinear nature of the input the simple Support Vector Machines (SVM) with linear kernel performed with the high classification error. Then we tested SVM with RBF kernel, but its performance was too slow and it produced a high classification error also. So we decided to apply a GBM as a feature classifier. GBM is based on oblivious trees, which are well balanced, less prone to overfitting, and they are speeding up execution of testing time significantly [13]. In this work, we use GBM implementation from Yandex CatBoost project [14]. The model was trained with a maximum number of trees of 104, tree depth of 6 and L2 regularization of 10, using log loss function.

B. DNN-based methods

To evaluate DNN-based antispoofing method on the collected dataset we selected the state-of-the-art SeNet architecture presented in the work [15].

The SeNet-154 was originally trained with ImageNet and then a transfer learning strategy is applied to fine-tune the network to the representation attack domain, using binary cross-entropy loss function and Adam optimizer with learning rate of 10-4. Input data was randomly cropped by 224×224 window and randomly flipped. We didn't apply resizing because this operation could disrupt some important frequency bands of the image. A similar experiment has been conducted for ResNext-50 architecture with SE-layers with learning rate of 103 and Xception [16] with learning rate of 104 and 299×299 image cropping window.

All the pretrained models were uploaded from https://github.com/Cadene/pretrained-models.pytorch.

ResNext-50 has been trained with cutting of 2 top layers, adding a new classification layer and freezing the entire pretrained part. SeNet-154 and Xception pretrained layers haven't been frozen and only the top layer has been modified. Fine-tuning is done for at most 30 epochs.

IV. Experimental results

The test results of various anti-spoofing methods on the proposed dataset are shown in Fig. 5. As the experimental results show, the top results obtained using the Neural Network approaches: EER 4.1% for Xception, EER 6% for ResNext-50 and EER 3.8% for SeNet-154 architecture. However, classical LBP-GBM method shows EER equal to 14.6%.

The best EER is small, though it exceeds the known results on printed attacks OULU dataset, where it is under 1% [7]. It can be contingent on either algorithm quality or complexity of the dataset itself.

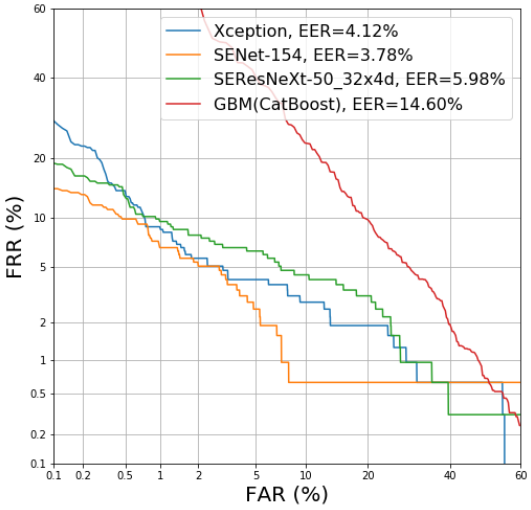

Fig. 5. DET Curve.

We came to the final but important conclusion. Despite the fact that replay spoofing attacks are of high risk, no artifacts seen by naked eye are present on the image, by training the above algorithm on the dataset we can obtain a system, which will detect these types of attacks with sufficiently high reliability. This important result stresses that even with one image, presented on a quality screen, it is possible to detect a spoofing attack. Utilization of the dataset shown in our research paves the way for creation of a quite accurate, fast and convenient antispoofing algorithm.

V. Conclusion

In this project, we are releasing a face anti-spoofing database with replay attacks to serve as an evaluation platform in the literature. The database contains 1942 genuine images, and 16885 fake faces are produced from the high quality records of the genuine faces. The database is split into 3 subsets to provide training, calibration and evaluation for development of the antispoofing algorithm. We are demonstrating the full statistics for the provided dataset. Further development of the baseline algorithm allows us to demonstrate the possibility of detection in such types of attacks even while using a single image. Taking into consideration the number of the devices used to record the dataset and the number of the individual faces we can conclude that this is the most representative database from the said point of view.

References

[1] W. Zhao, R. Chellappa, J. Phillips, A. Rosenfeld, "Face recognition: A literature survey," ACM Comput. Surv., pp. 399–458, 2003.

[2] C. Rathgeb, A. Uhl, "Two-factor authentication or how to potentially counterfeit experimental results in biometric systems," Proc. of the Int. Conf. on Image Analysis and Recognition (ICIAR'10), part II, vol. 6112, pp. 296–305, 2010.

[3] J. Galbally, S. Marcel, J. Firrez, "Biometric antispoofing methods: A survey in face recognition," IEEE Access, vol. 2, pp. 1530–1552, 2014.

[4] N. Kose, J.-L. Dugelay, "Mask spoofing in face recognition and countermeasures," Image Vision Comput., vol. 32, pp. 779–789, 2014.

[5] N. Erdogmus, S. Marcel, "Spoofing 2D face recognition systems with 3D masks," BIOSIG, pp. 1–8, 2013.

[6] Z. Zhang, J. Yan, S. Liu, Z. Lei, D. Yi, S. Z. Li, "A face antispoofing database with diverse attacks," Proc. — 2012 5th IAPR Int. Conf. on Biometrics (ICB), New Delhi, 2012, pp. 26–31.

[7] Z. Boulkenafet, J. Komulainen, L. Li, X. Feng, A. Hadid, "OULU-NPU: A mobile face presentation attack database with real-world variations," 2017 12th IEEE Int. Conf. on Automatic Face & Gesture Recognition (FG 2017), Washington, DC, 2017, pp. 612–618.

[8] I. Chingovska, A. Anjos, S. Marcel, "On the effectiveness of local binary patterns in face anti-spoofing," BIOSIG, pp. 1–7, 2012.

[9] A. Costa-Pazo, S. Bhattacharjee, E. Vazquez-Fernandez, S. Marcel, "The replay-mobile face presentation-attack database," BIOSIG, pp. 1–7, 2016.

[10] X. Tan, Y. Li, J. Liu, L. Jiang, "Face liveness detection from a single image with sparse low rank bilinear discriminative model," ECCV 2010: Comput. Vision ECCV 2010, pp. 504–517.

[11] Y. Liu, A. Jourabloo, X. Liu, "Learning deep models for face anti-spoofing: Binary or auxiliary supervision," Proc. IEEE Comput. Vision and Pattern Recognition, pp. 389–398, 2018.

[12] E. Rublee, V. Rabaud, K. Konolige, G. Bradski, "ORB: an efficient alternative to SIFT or SURF," Proc. IEEE Int. Conf. on Comput. Vision, pp. 2564–2571, 2011.

[13] J. H. Friedman, "Greedy function approximation: A gradient boosting machine," Annals of Statistics, pp. 1189–1232, 2000.

[14] A. V. Dorogush, V. Ershov, A. Gulin, "Catboost: gradient boosting with categorical features support," arXiv preprint arXiv:1706.09516, 2017.

[15] J. Hu, L. Shen, S. Albanie, G. Sun, E. Wu, "Squeeze-and-excitation networks," IEEE Transactions on Pattern Analysis and Machine Intelligence, pp. 7132–7141, 2017.

[16] F. Chollet, "Xception: Deep learning with depthwise separable convolutions," IEEE Conf. on Comput. Vision and Pattern Recognition, pp. 1800–1807, 2017.