LivDet 2015 Fingerprint Liveness Detection Competition 2015

Valerio Mura, Luca Ghiani, Gian Luca Marcialis, Fabio Roli
University of Cagliari (Italy)
Department of Electrical and Electronic Engineering
{valerio.mura, luca.ghiani, marcialis, roli}@diee.unica.it

David A. Yambay, Stephanie A. Schuckers
Clarkson University (USA)
Department of Electrical and Computer Engineering
{yambayda, sschucke}@clarkson.edu

Abstract

A spoof or fake is a counterfeit biometric that is used in an attempt to circumvent a biometric sensor. Liveness detection distinguishes between live and fake biometric traits. Liveness detection is based on the principle that additional information can be garnered above and beyond the data procured by a standard authentication system, and this additional data can be used to determine if a biometric measure is authentic.

The Fingerprint Liveness Detection Competition (LivDet) goal is to compare both software-based and hardware-based fingerprint liveness detection methodologies. The competition is open to all academic and industrial institutions. The number of competitors grows at every LivDet edition demonstrating a growing interest in the area.

In this edition eleven institutions have registered with twelve submissions for the software-based part and one for the hardware-based part.

1. Introduction

Biometrics has been an expanding industry in recent years and provides security through identifying a person based on physiological or behavior characteristics. However, it has been shown that biometric systems are vulnerable to spoof attacks by artificial fingerprint casts made of materials such as PlayDoh, silicone, or latex. This is a subset of Presentation Attack which focus on vulnerabilities at the presentation of a biometric to a biometric recognition system.

There have been numerous methods proposed to solve the susceptibility of fingerprint devices to attacks by spoof fingers. One primary countermeasure to spoofing attacks is called liveness detection. Liveness detection, or presentation attack detection, is based on the principle that additional information can be garnered above and beyond the data procured by a standard authentication system, and this additional data can be used to determine if an image is authentic.

Liveness detection uses either a hardware-based or software-based modules as part of an authentication system in order to provide additional security. Hardware-based approaches use additional sensors to gain measurements outside of the fingerprint image itself. Software-based approaches use image processing algorithms to gather information directly from the collected fingerprint. These systems classify images as either live or fake.

A standard assessment of fingerprint liveness detection methods has been lacking in the industry by which methods of different organizations can be compared. The First International Fingerprint Liveness Detection Competition LivDet 2009 [3], provided an initial assessment of software systems based on the fingerprint image only, but did not address integrated systems. The second and third editions of Liveness Detection Competition (LivDet 2011 [8], LivDet 2013 [1]) included integrated system testing. Similar to the two previous competitions, LivDet 2015 contained two parts: evaluation of software-based systems in Part 1: *Algorithms*, and evaluation of integrated systems in Part 2: *Systems*.

The number of participants increases with each edition and demonstrates the growing interest in this area.

In this paper, we describe the LivDet 2015 competition characteristics and we summarize the results achieved from the participants. Section 2 give a brief overview of fingerprint spoofing techniques and liveness detection countermeasures. In section 3 the evaluation protocols of the algorithms and the systems portion of the competiotion are

examined in depth. Section 4 presents the competition results and Section 5 concludes the paper.

2. Fingerprint Liveness Detection

The concept of spoofing has existed for some time now. Research into spoofing can be seen beginning in 1998 from research conducted by D. Willis and M. Lee where six different biometric fingerprint devices were tested against fake fingers and it was found that four of the six were susceptible to spoofing attacks [7]. This research was approached again in 2000-2002 by multiple institutions including; Putte and Kuening as well as Matsumoto *et al*. [6, 4]. The research presented by these researchers looked at the vulnerability of spoofing. In 2001, Kallo *et al*. looked at a hardware solution to liveness detection; while in 2002, Schuckers delved into using software approaches for liveness detection [2, 5].

There are two approaches to create artificial fingers, the cooperative method and non-cooperative method. In the cooperative method the subject pushes the finger into a plasticine-like material creating a negative impression of the fingerprint as a mold. The mold is then filled with a material, such as gelatin, PlayDoh or silicone that will reproduce the fingerprint characteristics. In the non-cooperative method a latent fingerprint left on a surface is enhanced, digitized through the use of a photograph, and, finally, the negative image is printed on a transparency sheet. This printed image can then be made into a mold, for example, by etching the image onto a printed circuit board which can be used to create the spoof cast.

The challenge to fingerprint recognition systems is the ability to detect if a presented fingerprint is from a live person or an artificial finger. Systems are being upgraded to incorporate liveness detection solutions that will be able to detect if the submitted probe is a spoof or live finger. Liveness detection can be incorporated into a system through the addition of hardware components to the capture device that can search for traits in the fingerprint through the use of blood pressure, electrocardiogram, temperature or other methods. Liveness detection can also be implemented through the use of algorithms that are added to the system. This method looks to see if there are features within the fingerprint image to determine liveness. There are many solutions that have been proposed to mitigate the vulnerability of spoofing and the LivDet competitions create a benchmark for measuring liveness detection solutions.

3. Experimental Protocol and Evaluation

The competition features two distinct parts; Part 1: Algorithms and Part 2: Systems, with separate protocols designed for each part. Each part contains their own constraints necessary to eliminate the variability that may be present across algorithms or systems. The design of the experiment will be discussed in detail in this section and will also outline the constraints placed on entrants for each part.

Participants	**Algorithm names**
Instituto de Biociencias, Letras e Ciencias Exatas	COPILHA
Institute for Infocomm Research (I2R)	CSI
Institute for Infocomm Research (I2R)	CSI_MM
Dermalog	hbirkholz
Universidade Federal de Pernambuco	hectorn
Anonymous participant	anonym
Hangzhou Jinglianwen Technology Co., Ltd	jinglian
Universidade Federal Rural de Pernambuco	UFPE I
Universidade Federal Rural de Pernambuco	UFPE II
New York University	nogueira
Zhejiang University of Technology	titanz

Table 1: Name of the participants and the submitted algorithms.

3.1. Participants

The competition is open to all academic and industrial institutions. Upon registration, each participant is required to sign a database release agreement detailing the proper usage of data made available through the competition. Participants are then given a database access letter with a username and password to access the server to download the training data. In Table 1 the participants names and the correspondent algorithms names are presented as they are used in this paper. Only one out of ten preferred to remain anonymous and two institutes, Universidade Federal Rural de Pernambuco and Institute for Infocomm Research(I2R), submitted two different algorithms for Part 1.

One system was submitted to LivDet 2015 Part 2: Systems as Anonymous.

3.2. Part 1: Algorithm Data Set

The dataset for *Part 1: Algorithms* consists of images from four different optical devices; Green Bit, Biometrika, Digital Persona and Crossmatch. The detailed characteristics of the sensors are shown in Table 2.

For each of these devices there are more than 4000 images. Live images came from multiple acquisitions of all fingers of different subjects. Each finger was acquired in a variety of ways in order to mimic real scenarios. Acquisitions include normal mode, with wet and dry fingers

Scanner	Model	Resolution [dpi]	Image Size [px]	Format
Green Bit	DactyScan26	500	500x500	PNG
Biometrika	HiScan-PRO	1000	1000x1000	BMP
Digital Persona	U.are.U 5160	500	252x324	PNG
Crossmatch	L Scan Guardian	500	640x480	BMP

Table 2: Device characteristics for Part 1 datasets.

Dataset	Live Image	Ecoflex	Gelatine	Latex	WoodGlue	Liquid Ecoflex	RTV
Green Bit	1000	250	250	250	250	250	250
Biometrika	1000	250	250	250	250	250	250
Digital Persona	1000	250	250	250	250	250	250
	Live Image	**Body Double**	**Ecoflex**	**Playdoh**	**OOMOO**	**Gelatin**	**-**
Crossmatch	1500	300	270	281	297	300	-

Table 3: Number of images for each testing sets. Training sets were a similar size but did not include the unknown materials (liquid Ecoflex, RTV, OOMOO and Gelatin).

and with high and low pressure. The spoof images of the LivDet 2015 datasets were collected using the cooperative method that was earlier described. The spoof materials used for this experiment are Ecoflex, gelatine, latex, woodglue, a liquid Ecoflex and RTV (a two-component silicone rubber) for the Green Bit, the Biometrika and the Digital Persona datasets, and Playdoh, Body Double, Ecoflex, OOMOO (a silicone rubber) and a novel form of Gelatin for Crossmatch dataset. The entire datasets were divided into two parts by using images from different subjects: a training set, for the configuration of algorithms, and a testing set to evaluate the performance. The testing sets included spoof images of unknown materials, *i.e*. materials which were not included in the training set. The unknown materials are liquid Ecoflex and RTV for Green Bit, Biometrika and Digital Persona datasets, and OOMOO and Gelatin for Crossmatch dataset. This practice has been adopted to assess the reliability of algorithms under attack by unknown materials.

3.3. Algorithm Submission

The algorithm submission for LivDet 2015 uses the same structure as previous editions. As stated for the other LivDet editions each submitted algorithm must be a Win32 console application with the following list of parameters:

LIVENESS_XYZ.exe [ndataset] [inputfile] [outputfile]

The parameters are used to configure the correct dataset, charge the image list to process and receive the output file scores. For each image the algorithm returns a score from 0 to 100, where 0 means that the image are classified as fake and 100 means that the image from a live finger. The classification threshold for tests is set to 50.

3.4. Part 2: Systems Submission

Part 2: Systems component of LivDet is characterized by participants shipping a complete fingerprint system with the ability to capture a fingerprint image as well as to produce a liveness detection score. Participants are supplied with three spoof recipes upon registration. These recipes were given for training purposes. Once the system is provided to the competition organizers, the system is tested using the three known recipes. Two unknown spoof recipes are also tested to examine the flexibility of the sensor toward novel spoof methods. The known recipes for LivDet 2015 are Playdoh, Body Double, and Ecoflex. The two unknown spoof recipes used were OOMOO (a silicone rubber) and a novel form of Gelatin. Participants for LivDet 2015 were required to provide their system to run on either a Windows 32-Bit or 64-Bit system run through either USB or firewire connection with the main file being an .exe or similar executable file. The submitted system needs to be able to output a file with the collected image as well as a liveness score on the range of 0 to 100 with 100 being the maximum degree of liveness and 50 being the threshold value to determine if an image is live or spoof. If the system is not able to process a live subject it is counted as a failure to enroll and counted against the performance of the system (as part of Ferrlive). However, if the system is unable to process a spoof finger it is considered as a fake non-response and counted as a positive in terms of system effectiveness for spoof detection (as part of *Ferrspoof*).

Laboratory staff systematically tested submitted fingerprint systems by collecting live data from human subjects

and attempting to spoof the system through the use of spoofs made from casts. 2011 attempts were completed with 1010 live attempts from 51 subjects (2 images each of all 10 fingers) and 1001 spoof attempts across the five different materials giving approximately 200 images per spoof type. 500 spoofs were created from each of 5 fingers of 20 subjects for each of the five spoof materials. Two attempts were performed with each spoof.

3.5. Performance Evaluation

The parameters adopted for the performance evaluation are the following:

- *Evaluation per sensor/system:*
  - *Frej_n*: Rate of failure to enroll for the sub-set *n*.
  - *Frej_n*: Rate of failure to enroll for the sub-set *n*.
  - *Fcorrlive_n*: Rate of correctly classified live fingerprints for sub-set *n*.
  - *Fcorrfake_n*: Rate of correctly classified fake fingerprints for sub-set *n*.
  - *Ferrlive_n*: Rate of misclassified live fingerprints for sub-set *n*.
  - *Ferrfake_n*: Rate of misclassified fake fingerprints for sub-set *n*.
  - *FakeNonResponse*: Rate of failure to acquire for fake fingerprints for system.
- *Overall evaluation:*
  - *Frej_n*: Rate of failure to enroll.
  - *Fcorrlive_n*: Rate of correctly classified live fingerprints.
  - *Fcorrfake_n*: Rate of correctly classified fake fingerprints.
  - *Ferrlive_n*: Rate of misclassified live fingerprints.
  - *Ferrfake_n*: Rate of misclassified fake fingerprints.

4. Results and Discussion

4.1. Part 1: Algorithms

Table 4 summarizes the results of each algorithm on all datasets used for testing. The accuracy, the rate of samples correctly classified, is a fundamental parameter of a classification system. Six of the twelve algorithms submitted to the competition achieved over 90% average classification rate, separating live and fake fingerprints.

More details on performance of all algorithms on all datasets are provided in the Table 6. This table shows the results on the parameters of performance defined in the previous section. In particular, note that the column **Fcorrfake** counts the percentage of fakes classified as such for all fake images (known and unknown). Columns **Fcorrfake known** and **Fcorrfake unknown** are the percentage correctly classified spoof image from known material, and unknown materials, respectively. A comparison between these two columns show that the various systems have a small decrease in classification accuracy when fakes are created with unknown materials to training systems. Another important consideration to make comparing the performance of the various datasets is that the higher resolution for Biometrika sensor did not necessarily achieve the best classification performance, while the small size of the images for the Digital Persona device generally degrades the accuracy of all algorithms.

Algorithm	**1**	**2**	**3**	**4**	**Overall**
nogueira	95.40	94.36	93.72	98.10	95.51
unina	95.80	95.20	85.44	96.00	93.23
jinglian	94.44	94.08	88.16	94.34	92.82
anonym	92.24	92.92	87.56	96.57	92.51
titanz	91.76	92.36	89.04	91.62	91.21
hbirkholz	91.36	93.40	88.00	89.93	90.64
hectorn	90.00	88.20	84.20	86.94	87.32
CSI_MM	86.56	87.84	75.56	89.99	85.20
CSI	82.12	83.20	76.20	88.33	82.71
COPILHA	72.76	75.64	79.96	69.00	74.11
UFPE II	87.68	71.24	75.44	61.16	73.33
UFPE I	82.56	64.32	78.36	59.97	70.82

Table 4: Accuracy of the algorithms on the testing datasets [%]. **1** = Green Bit, **2** = Biometrika, **3** = Digital Persona, **4** = Crossmatch.

4.2. Part 2: Systems

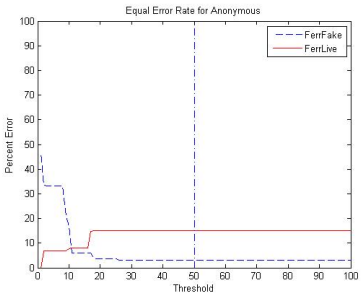
The FerrFake and FerrLive of the submitted systems is given in Table 5 and the equal error curve of the system is shown in Figure 1a. Anonymous scored a FerrLive of 14.95% and a FerrFake of 6.29% at the (given) threshold

Submitted System	FerrLive	FerrFake
Anonymous	14.95%	6.29%
Submitted System	FerrFake Known	FerrFake Unknown
Anonymous	11.09%	1.00%

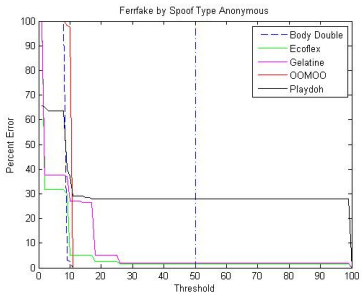
Table 5: FerrLive and FerrFake for submitted system.

	Algorithm	Frej [%]	Fcorrlive [%]	Fcorrfake [%]	Fcorrfake known [%]	Fcorrfake unknown [%]	Accuracy [%]
Green Bit	COPILHA	0.20	63.30	79.07	80.80	75.60	72.76
	CSI	0.00	83.40	81.27	83.90	76.00	82.12
	CSI_MM	0.00	89.10	84.87	86.20	82.20	86.56
	hbirkholz	0.20	96.40	88.00	91.20	81.60	91.36
	hectorn	0.20	88.80	90.80	92.60	87.20	90.00
	anonym	0.20	90.90	93.13	96.50	86.40	92.24
	jinglian	0.20	92.50	95.73	97.50	92.20	94.44
	UFPE I	0.20	81.10	83.53	93.80	63.00	82.56
	UFPE II	0.20	79.20	93.33	98.20	83.60	87.68
	nogueira	0.20	96.50	94.67	95.70	92.60	95.40
	titanzhang	0.20	91.40	92.00	94.20	87.60	91.76
	unina	0.20	93.50	97.33	98.00	96.00	95.80
Biometrika	COPILHA	0.00	77.50	74.40	83.00	57.20	75.64
	CSI	0.00	85.00	82.00	82.60	80.80	83.20
	CSI_MM	0.00	89.00	87.07	86.30	88.60	87.84
	hbirkholz	0.00	92.00	94.33	94.60	93.80	93.40
	hectorn	0.00	86.90	89.07	92.00	83.20	88.20
	anonym	0.00	93.10	92.80	96.50	85.40	92.92
	jinglian	0.00	96.20	92.67	92.40	93.20	94.08
	UFPE I	0.00	58.20	68.40	73.30	58.60	64.32
	UFPE II	0.00	62.70	76.93	79.40	72.00	71.24
	nogueira	0.00	91.50	96.27	97.30	94.20	94.36
	titanz	0.00	89.80	94.07	93.60	95.00	92.36
	unina	0.00	89.10	99.27	99.60	98.60	95.20
Digital Persona	COPILHA	0.00	82.30	78.40	82.90	69.40	79.96
	CSI	0.00	71.80	79.13	80.80	75.80	76.20
	CSI_MM	0.00	74.10	76.53	78.20	73.20	75.56
	hbirkholz	0.00	87.40	88.40	90.00	85.20	88.00
	hectorn	0.00	90.70	79.87	84.40	70.80	84.20
	anonym	0.00	92.30	84.40	91.20	70.80	87.56
	jinglian	0.00	89.30	87.40	90.80	80.60	88.16
	UFPE I	0.00	67.20	85.80	86.00	85.40	78.36
	UFPE II	0.00	78.20	73.60	74.20	72.40	75.44
	nogueira	0.00	91.90	94.93	95.40	94.00	93.72
	titanz	0.00	90.40	88.13	90.00	84.40	89.04
	unina	0.00	64.30	99.53	99.60	99.40	85.44
Crossmatch	COPILHA	0.00	40.00	99.03	99.53	98.32	69.00
	CSI	0.00	96.87	79.49	86.37	69.68	88.33
	CSI_MM	0.00	97.53	82.18	90.60	70.18	89.99
	hbirkholz	0.00	93.67	86.05	89.31	81.41	89.93
	hectorn	0.00	93.07	80.59	83.43	76.55	86.94
	anonym	0.00	97.40	95.72	95.53	95.98	96.57
	jinglian	0.00	98.07	90.47	91.89	88.44	94.34
	UFPE I	0.00	70.80	48.76	46.18	52.43	59.97
	UFPE II	0.00	77.40	44.34	43.24	45.90	61.16
	nogueira	0.00	99.07	97.10	97.88	95.98	98.10
	titanz	0.00	96.40	86.67	90.83	80.74	91.62
	unina	0.00	98.93	92.96	97.77	86.10	96.00

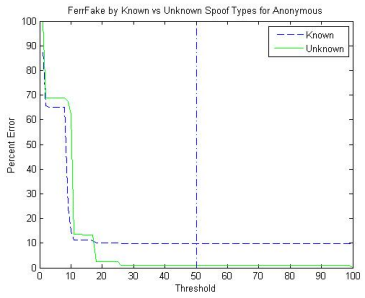
Table 6: Performance of all algorithms on all datasets.



(a) Equal Error Curve.



(b) FerrFake by Spoof Type.



(c) FerrFake by Known/Unknown Spoof Types.

Figure 1: Performance on *System Part* for Anonymous.

of 50. There is an 11.09% FerrFake for known recipes and 1% for unknown recipes. This result is opposite what has been seen in previous LivDet competitions where known spoof types typically have a better performance than unknown spoof types. This result is primarily due to the Playdoh spoof type and is described in the next paragraph. The error rates for each spoof type can be seen in Figure 1b and the known vs unknown are shown in Figure 1c.

The error rate for spoof materials was primarily due to impact on color differences error for the playdoh. Testing across 6 different colors of playdoh found that certain colors behaved in different ways. For yellow and white playdoh, the system detected spoofs as fake with high accuracy. For brown and black playdoh, the system would not collect an image. Therefore, it was recorded as a fake non-response and not an error in detection of spoofs. For pink and lime green playdoh, the system incorrectly accepted spoofs as live for almost 100% of images collected. The fact that almost all pink and lime green playdoh images were accepted as live images resulted in a 28% total error rate for playdoh. The system had a 6.9% Fake Non-Response Rate primarily due to brown and black playdoh.

The results from Part 2: Systems show improvement over the general results seen in LivDet2011, however the anonymous system did not perform as well as what was seen in LivDet 2013.

5. Conclusions

LivDet 2015 is the fourth international public competition for software-based fingerprint liveness detection and the third public assessment of system-based fingerprint liveness detection, proved to be an important competition. This edition highlighted the improvements in system spoofing detection for both algorithm and system parts. The number of participants, from both academic and industrial institutions, is growing with respect to previous editions. Since effective liveness detection solutions is a key component to minimize the vulnerability of fingerprint systems to spoof attacks, we hope that this competition success continues to increase such that further improvement in performance is encouraged.

6. Acknowledgement

This work has been partly supported by the project "Computational quantum structures at the service of pattern recognition: modeling uncertainty" [CRP-59872] funded by Regione Autonoma della Sardegna, L.R. 7/2007, Bando 2012.

References

[1] L. Ghiani, V. Mura, S. Tocco, G. L. Marcialis, F. Roli, D. Yambay, and S. Schuckers. Livdet 2013 fingerprint liveness detection competition 2013. *6th IAPR/IEEE Int. Conf. on Biometrics (ICB 2013), Madrid (Spain), 2013.*

[2] P. Kallo, I. Kiss, A. Podmaniczky, J. Talosi, and Negykanizsa. Detector for recognizing the living character of a finger in a fingerprint recognizing apparatus. *Patent US 6,175641, Jan. 16, 2001.*

[3] G. L. Marcialis, A. Lewicke, B. Tan, P. Coli, F. Roli, S. Schuckers, D. Grimberg, A. Congiu, and A. Tidu. First international fingerprint liveness detection competition livdet 2009. *14th Int. Conf. on Image Analysis and Processing (ICIAP 2009), Springer LNCS 5716.*, pages 12–23, 2009.

[4] T. Matsumoto, H. Matsumoto, K. Yamada, and S. Hoshino. Impact of artificial gummy fingers on fingerprint systems. *In Proceedings of SPIE, 4677, Optical Security and Counterfeit Deterence Techniques IV, Yokohama, Japan.*

[5] S. Schuckers. Spoofing and anti-spoofing measures. *Information Security Technical Report*, 7(4):56–62, 2002.

[6] T. van der Putte and J. Keuning. Dont get your fingers burned, smart card reserch and advanced applications, ifip tc8/wg8.8. *Fourth Working Conference on Smart Card Research and Advanced Applications*, pages 289–303, 2001.

[7] D. Willis and M. Lee. Six biometric devices point the finger at security. *Biometrics Under Our Thumb, Network Computing, June 1998.*

[8] D. Yambay, L. Ghiani, P. Denti, G. L. Marcialis, F. Roli, and S. Schuckers. Livdet 2011 fingerprint liveness detection competition 2011. *5th IAPR/IEEE Int. Conf. on Biometrics (ICB 2012), New Delhi (India), March, 29th, April, 1st, 2012.*