MobILive 2014 - Mobile Iris Liveness Detection Competition

Ana F. Sequeira[1,2], Hélder P. Oliveira[1], João C. Monteiro[1,2], João P. Monteiro[1] and Jaime S. Cardoso[1,2]
[1]INESC TEC, [2]Faculdade de Engenharia da Universidade do Porto
Rua Dr. Roberto Frias, n.378, 4200 - 465 Porto, Portugal
{afps,hfpo,jcsm,jpms,jsc}@inescporto.pt

Abstract

Biometric systems based on iris are vulnerable to several attacks, particularly direct attacks consisting on the presentation of a fake iris to the sensor. The development of iris liveness detection techniques is crucial for the deployment of iris biometric applications in daily life specially in the mobile biometric field. The 1st Mobile Iris Liveness Detection Competition (MobILive) was organized in the context of IJCB2014 in order to record recent advances in iris liveness detection. The goal for (MobILive) was to contribute to the state of the art of this particular subject. This competition covered the most common and simple spoofing attack in which printed images from an authorized user are presented to the sensor by a non-authorized user in order to obtain access. The benchmark dataset was the MobBIOfake database which is composed by a set of 800 *iris images and its corresponding fake copies (obtained from printed images of the original ones captured with the same handheld device and in similar conditions). In this paper we present a brief description of the methods and the results achieved by the six participants in the competition.*

1. Introduction

Biometric systems win over classical security methods as they rather identify an individual by what he is instead of based on something he knows or possesses. However, there are some disadvantages, including the lack of secrecy and the fact that a biometric trait cannot be replaced. Beyond these aspects, biometric systems are also vulnerable to external attacks which could decrease their level of security. Concerning these vulnerabilities we may find in the literature an analysis [8] of the eight different points of attack [7], illustrated in Fig. 1.

These attacks may be divided into two main groups: direct and indirect attacks. The *direct attacks* are related with the first vulnerability point in a biometric security system, which is the possibility to generate synthetic biometric samples in order to fraudulently access a system, and are performed at the sensor level. The *indirect attacks* includes all the remaining seven points of attack. In this case the intruder needs to have some information about the inner working of the recognition system and, in most cases, physical access to some of the application components is required. Iris has been traditionally regarded as one of the most reliable and accurate traits among the different biometric traits. Researchers were motivated to explore its vulnerabilities and to measure how spoofing attacks may compromise the security of iris based recognition systems (IRS). These systems may be vulnerable to attacks which consist on the presentation of a fake iris to the sensor pretending to be one of a legitimate user being the use of contact lenses or high quality iris printed images. The feasibility of some attacks on IRS have been reported by some researchers [6, 14] who showed that it is actually possible to spoof these systems with printed iris and well-made color iris lens. Several liveness detection methods have been presented through the past recent years. Anti-spoofing techniques were presented that use physiological properties to distinguish between real and fake biometric traits in order to improve the robustness of the system against direct attacks and to increase the security level offered to the final user. Iris liveness detection (ILD) approaches can broadly be divided into: i) software-based techniques, in which the fake irises are detected once the sample has been acquired with a standard sensor (i.e., features used to distinguish between real and fake eyes are extracted from the iris image, and not from the eye itself), and ii) hardware-based techniques, in which some specific device is added to the sensor in order to detect particular properties of a living iris such as the eye hippus or the pupil response to a sudden lighting event. In general, a combi-

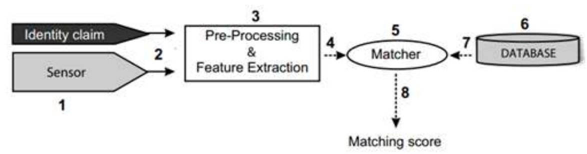
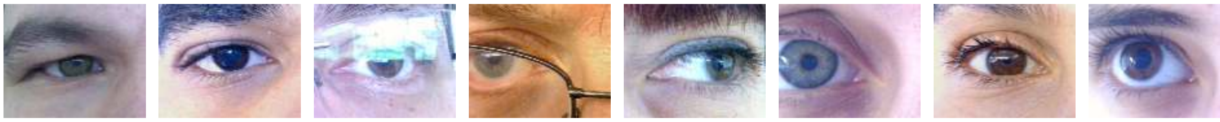


Figure 1. Architecture of an automated biometric verification system. Possible attack points are numbered from 1 to 8, from [8]



(a) (b) (c) (d) (e) (f) (g) (h)

Figure 2. Examples of iris images from MobBIO database: a) Heavily occluded; b) Heavily pigmented; c) Glasses reflection; d) Glasses occlusion; e) Off-angle; f) Partial eye; g) Reflection occlusion and h) Normal.

nation of both type of anti-spoofing schemes would be the most desirable approach to increase the security level of biometric systems [9]. In practice, it is necessary to balance the two following facts: hardware-based approaches usually present a higher detection rate and software-based techniques have the advantage of being less expensive (as no extra device is needed) and less intrusive for the user (which is a very important characteristic for a practical liveness detection solution). When developing a solution for a real-world application we stress the importance of the advantages of software-based techniques.

The MobILive2014 competition was motivated by the urge for liveness solutions in the mobile biometric field driven by the evolution in the use of mobile devices in our society. This competition covered the printed iris image attack using images captured with an handheld device.

2. The *MobILive* competition

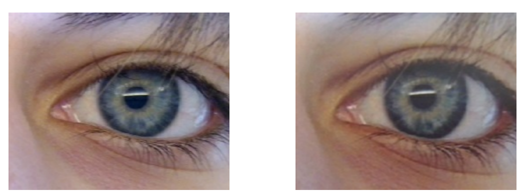
The 1^{st} Mobile Iris Liveness Detection Competition (*MobILive*[1]) was organized in the context of IJCB2014[2] in order to record recent advances in ILD and took place between December, 2013 and April, 2014. The main goal for the competition was to perform *iris liveness detection in mobile applications*. The problem of ILD is in fact a two-class classification problem in which is intended to distinguish between real iris images and fake iris images. This competition covered a specific kind of attack in which printed images from an authorized user are presented to the sensor by a non-authorized user in order to obtain access.

Our data was divided in train and test sets each one comprising data from 50 different individuals each. The train dataset was provided to the participants. The test set was used by the organizers to perform the evaluation of the methods. MobILive included an intermediate submissions period during which the participants submitted an executable file. The result of its evaluation (performed by the organizers) was published in a ranking. This ranking was updated after each new submission by evaluating the algorithms in the same randomly obtained subset of the test set composed by 200 images. The intermediate submissions were meant to stimulate interaction with the event, to give feedback to the participants about their performance compared with the other participants and to allow the refinement of the algorithms. The final results were obtained by the evaluation of the final submission (the last submission of each participant) on the entire test dataset.

3. The MobBIO*fake* dataset

The MobBIO*fake* [22] database was constructed upon the set of iris images from the MobBIO Multimodal Database [21] which also comprises samples of face and voice from 105 volunteers. The iris images, with a 250×200 pixels, were captured indoors with natural light and natural&artificial light, with variable eye orientations and occlusion levels, see [21] for more details. Some examples of iris images are depicted in Figure 2.

The MobBIO*fake* database is composed by 16 images (8 real and 8 fake) from 100 individuals, in a total of 1600 iris images. The fake samples were obtained from printed images of the original ones captured with the same handheld device and in similar conditions. An example is depicted in Figure 3. We tested different preprocessing methods and types of printing paper to choose the ones that minimized the noise introduced by the printing process.



(a) Real image (b) Fake image

Figure 3. Corresponding real and fake images of MobBIO*fake*.

4. Performance Evaluation

The metrics used to evaluate the results are *False Acceptance Rate (FAR)*, *False Rejection Rate (FRR)* and *Mean Error Rate (MER)* (which is the mean of FAR and FRR), where *Acceptance* stands for accepting an image as real and *Rejection* stands for rejecting an image as fake. The calculus of this error rates is done considering *False Real (FR)* as the number of fake images considered real; *True Fake (TF)* as the number of fake images considered fake; *False Fake*

[1]http://mobilive2014.inescporto.pt/
[2]http://ijcb2014.org/

(FF) as the number of real images considered fake; and *True Real (TR)* as the number of real images considered real, using the following formulas.

$$FAR = \frac{FR}{(FR + TF)} \quad (1)$$

$$FRR = \frac{FF}{(FF + TR)} \quad (2)$$

Under the standardization *ISO/IEC JTC1 SC37*, is currently being discussed a project named *ISO/IEC 30107 Presentation Attack Detection* [11]. This standard focus on techniques for the automated detection of presentation attacks undertaken by data capture subjects at the point of presentation and collection of the relevant biometric characteristics. Considering the scenario of MobILive2014, this document suggests the use of the two evaluation metrics: "Attack presentation classification error rate" (APCER) and "Normal presentation classification error rate" (NPCER). This values are, respectively, given by the proportion of attack/normal presentations incorrectly classified as normal/attack presentations and, in practice, correspond to the FAR and FRR error rates.

5. Methods and Participants

5.1. Participants

Ten participants registered in the competition from several countries, among these, six participants submitted their algorithms. In Table 1 we list the six teams in competition.

Table 1. Participating teams.

Team	Institution
Federico II	University Federico II of Naples, Italy
GUC	Gjϕvik University College, Norway
HH	Halmstad university, Sweden
IIT Indore	Indian Institute of Technology, India
IrisKent	University of Kent, UK
UNICAMP	Un. Campinas, F.U. Ouro Preto, Brazil

5.2. Briefs of the methods proposed[3]

5.2.1 Federico II

Submitted by D. Gragnaniello, C. Sansone and L. Verdoliva from DIETI, University Federico II of Naples, Italy. This approach is based on the use of local descriptors, which are powerful tools to describe the statistical behavior observed locally in small patches of the image. Among the best known we can count the Local Binary Pattern (LBP) [17], successfully used for different tasks, like texture and face recognition. These patterns are able to detect microstructures whose underlying distribution is estimated by histograms collected over the ensemble of all patches. In particular, LBP encodes the information between the target pixel and the neighboring pixel intensities: for each target pixel, x, it takes P neighbors sampled uniformly on a circle of radius R centered on x. These pixels are then compared with x, taking only the sign of the difference, and forming thus a vector of P values, which are then converted in a decimal number. In formulas:

$$LBP = \sum_{i=0}^{P-1} u(x_i - x)2^i \quad (3)$$

where x_i is the i-th neighbor of pixel x, $u(x) = 1$ when $x \geq 0$ and 0 otherwise. In order to increase the discriminative power of LBP, in [16] the authors propose to evaluate the histograms of the co-occurrence among these micro patterns. In this way, it is possible to better represent complex patterns and capture the spatial relations in the image. Hence in this work, the authors consider the features as proposed in [16], but the main difference is that they are evaluated on the prediction-error image (also called residual image). In fact, modeling the residuals rather than the pixel values is very sensible in these low-level methods (not based on image semantic), since the image content typically does not help detecting local alterations. This consideration is especially true for the problem of ILD, when printed iris are presented to the sensor, in order to detect seemingly invisible alterations of the natural characteristics of the biometric trait. In particular, the features are extracted from the prediction-error images evaluated as proposed in [25]. Finally, a Support Vector Machine (SVM) with linear kernel was used as classifier and a leave-one-out cross-validation to find the best value of its parameters. The proposed approach can be summarized in the following steps: 1) computation of the high-pass residuals; 2) feature extraction based on co-occurrence of adjacent LBP; 3) SVM classifier with linear kernel.

5.2.2 GUC

Submitted by R. Raghavendra, Kiran B. Raja and Christoph Busch from Gjϕvik University College, Norway. GUC's Presentation Attack Detection (PAD) (or spoof detection or counter measure) Algorithm for visible iris attack detection is based on both local and global statistical features. The pool of statistical features are based on various image quality measures that captures variation at pixel level and also at the block level to reflect the rich information to identify the presence of visible iris artefact. Further, the weighted multi-classifier fusion of these features are carried to make the final decision. The weights are optimized on the training dataset provided by the organizer.

[3]Presented as given by the authors.

5.2.3 HH

Submitted by Fernando Alonso-Fernandez and Josef Bigun from Halmstad University, Sweden. The fake iris detection system is based on Gray-Level Co-Occurrence textural features [10, 23, 4] extracted from the three color (RGB) channels of the image. This method looks for the best features by Sequential Forward Floating Selection (SFFS) [20], using SVM as classifier [24]. Given n features to combine, it employs as criterion value of the SFFS algorithm the HTER (*Half Total Error Rate*) of the corresponding classifier trained with the n features. This method also localize the eye center position, which is used as input of the Gray-Level Co-Occurrence Matrix (GLCM) feature extraction algorithm, so as to extract GLCM features in the desired region of the image only. For this purpose, the authors employ their eye detection algorithm based on symmetry filters [1].

5.2.4 IIT Indore

Submitted by Vivek Kanhangad, Pragalbh Garg and Pranjalya Singh from the Indian Institute of Technology Indore. The IIT Indore algorithm for ILD is based on the analysis of differences in texture patterns for discriminating between real and fake iris images. Specifically, the approach is based on feature level combination of the following three texture descriptors: Local Phase Quantization [18]; Binary Gabor Pattern [27]; Local Binary Pattern [17]. The combined feature set resulting from the feature level fusion of the above descriptors is then used to train a support vector machine (SVM) classifier with linear kernel.

5.2.5 IrisKent

Submitted by Yang Hu, Konstantinos Sirlantzis and Gareth Howells, from University of Kent, UK. This method exploits the combination of multiple features for ILD in mobile applications. Firstly, some base level features are extracted. The base level features are then fed to a score level combiner and a feature level combiner. The final decision is made based on the output of the two combiners. In score level combiner, each base level feature is fed to a classifier. The response of each classifier is used as scores and combined to produce an output. In feature level combiner, different selected features are combined to form a new feature vector. This feature vector is fed to a classifier whose score is used as output. The base level features are extracted using a spatial pyramid structure [26, 13]. The spatial pyramid structure partitions image into increasing finer sub-regions. Local features within each sub-region are pooled together, and the pooled features of each sub-region are concatenated to form base level features. The spatial pyramid structure captures the local and global distributions of the features. It gives us information of the iris region as well as the distributions around the iris. In the algorithm, 9 local features are extracted to form 9 base level features: sparse coding on sift features [26, 15], sparse coding on hog features, local binary patterns, red channel histogram, red channel correlogram, color histogram, intra-color correlogram, inter-color correlogram and multi-color correlogram [3]. Sparse coding on sift features encodes the sift descriptor by sparse coding as a local feature. The sift descriptor is a gradient histogram characterizing the local appearance of image. Similarly, sparse coding on hog feature encodes hog features by sparse coding. Hog is a gradient orientation based histogram and it is widely used in object detection. The local binary patterns provide local contrast information around each pixel. Additionally, histogram and correlogram are computed on all RGB color channels. Correlogram is a pairwise intensity distribution. It reveals color and texture distribution of image. Intra-colour correlogram concatenates the correlogram at each color channel. Inter-color correlogram concatenates the correlogram between each two color channels. It reveals the color and texture distribution across the color channels. Multi-color correlogram is the combination of intra-color correlogram and inter-color correlogram. We perform feature selection for score level combiner. A feature is selected if it can either improve the accuracy of ILD or preserve the accuracy and enlarge the gap between real and fake images. In feature level combiner, considering computational cost, we simply select the features with top performance. In the experiments, LBP and intra-color correlogram are selected for the score level combiner, while LBP and multi-color correlogram are selected for the feature level combiner.

5.2.6 LIV-IC-UNICAMP

Submitted by D. Menotti[1,2], G. Chiachia[1] and A. X. Falcão[1] from (1) University of Campinas and (2) Federal University of Ouro Preto. A key characteristic of the UNICAMP system is the use of a special type of convolutional neural networks (CNNs) for feature extraction. These networks are inspired in recent work on biologically-inspired computer vision [19] and have two important properties: (i) *optimal* architecture and (ii) *random* filter weights. The first property has shown to be of crucial importance for CNNs [19, 2] and the second one allows for the construction of robust, highly nonlinear feature extractors even from datasets with few training samples, while also performing surprisingly well [12, 5]. In the attempt to discover optimal CNN architectures, the number of layers and the operations considered by the authors are the same as in [19], as well as the optimization procedure, which consists of randomly sampling and evaluating thousands of candidate CNNs to choosing the best one. In order to evaluate these CNNs, the authors further divided the images made available into training and test sets such that they were disjoint in terms of person identity. In fact, the UNICAMP method can be viewed as the combination of three subsystems, each one containing one CNN for feature extraction and one linear SVM (operating on top of these features) to predict whether iris images are fake or real. The difference among these subsystems is their corresponding CNN, which were found to perform best when allowed to output feature vectors of size in the intervals $[200, 5000]$, $[5000, 10000]$ and $[10000, 20000]$. While each of these subsystems perform quite well by their own, the authors found that combining them by majority voting led to superior performance. In addition, six (out 800) samples that were most frequently mistaken by the subsystems (*i.e.*, supposedly outliers) were removed while training the linear SVMs for the final submission.

6. Discussion and Results

In Table 2 is shown the updated rankings for the three intermediate submissions.

Table 2. Ranking of the algorithms' performance in $1^{st}, 2^{nd}, 3^{rd}$ intermediate submissions.

Rank	1^{st}	2^{nd}	3^{rd}
1	FedericoII	FedericoII	UNICAMP / IITIndore
2	GUC	GUC	GUC / Federico II
3	IITIndore	IrisKent	IrisKent
4	IrisKent	UNICAMP	HH
5		IITIndore	

We remark that the intermediate submissions and the publication of the ranking motivated the healthy competition among the participants. Through the publication of updated rankings the participants could assess the performance of their methods relatively to the others and we believed that the competition benefited form this synergy between the participants. The final results were obtained in the test dataset composed by 800 images. The final version of the algorithms was the last one received till 17^{th} of March, 2014. In Table 3 the final results are presented for the six teams in competition.

Table 3. Final results presenting the FAR, FRR and MER (in %). "No." refers to the number of submissions.

Rank	Team	No.	FAR	FRR	MER
1	IIT Indore	2	0.00	0.50	0.25
2	GUC	2	0.75	0.00	0.38
3	Federico II	1	1.25	0.00	0.63
4	UNICAMP	3	0.50	2.00	1.25
5	IrisKent	4	0.25	3.75	2.00
6	HH	2	29.25	7.00	18.13

The best result was obtained by the *IIT Indore* team with a MER of 0.25%, closely followed by the *GUC* and *FedericoII* teams. In general, the results obtained were very good and improved the published results for this database.

7. Further analysis of results

The results obtained, by most of the participants, were far better than what was the state-of-the-art with this database, around 12% of MER [22]. Considering these results, four of them below 2%, we decided to analyze the characteristics of our images and test the robustness of the methods to a more ''clever" manipulation of images. Some intuitive research was performed and one of the attempts made was to convert the images to the $CIELab$ color space and analyze the variation of the values of the three channels. Particularly, the values of the L and the b channels allowed to determine a strong separation between the two classes of images being possible to define a threshold that would separate the real and fake images quite well. Putting ourselves in the role of a malignant agent, in order to be well succeeded in the spoofing attack, we would try to make our fake images resemble the most to the real ones. Therefore, we manipulated some fake images (approximately 100 images, i.e., 12.5% of the total of fake images) so that the values of these two channels were distributed similarly to the ones of the real images. In Table 4 we present the results obtained by evaluating the algorithms in this dataset. We must state that this results may be considered invidious since the algorithms were not trained for these type of images.

Table 4. Results of the evaluation in the manipulated test set (in %). "No." refers to the number of submissions.

Rank	Team	No.	FAR	FRR	MER
1	IIT Indore	2	0.00	0.50	0.25
2	GUC	2	0.75	0.00	0.38
3	UNICAMP	3	0.50	2.01	1.26
4	IrisKent	4	5.75	3.75	4.75
5	Federico II	1	16.25	0.00	8.13
6	HH	2	29.25	7.00	18.13

There are some methods clearly more robust to these changes than others. The methods of *FedericoII* and *IrisKent* teams appear to be more sensible to this changes. The four remaining methods are not affected by the changes in the images.

Other similar changes could be performed which would increase the feasibility of the spoofing, however this kind of manipulation requires from the intruder to possess privileged knowledge and ease of access to the database storage.

8. Conclusions

We believe that the deployment of iris biometric applications in daily life, particularly in the mobile biometric field, has created a necessity for ILD solutions. The 1^{st}

MobILive Competition was organized having as main goals the possibility to record recent advances in ILD and stimulate new ones. In our view, the objectives were accomplished, considering that excellent results were achieved, exceeding the state-of-the-art results, by participants from all over the globe. However, the results obtained also encourage us to go further. One very important aspect in this field of research is the necessity of more public available datasets with more variety of acquiring scenarios. We made our contribution and we expect to have motivated the appearance of new, more challenging, databases for ILD.

ACKNOWLEDGEMENTS

The authors would like to thank Fundação para a Ciência e Tecnologia (FCT) - Portugal the financial support for the PhD grants with references SFRH/BD/74263/2010 and SFRH/BD/87392/2012.

References

[1] F. Alonso-Fernandez and J. Bigun. Eye detection by complex filtering for periocular recognition. In *Proc. IWBF*, 2014.

[2] J. Bergstra, D. Yamins, and D. D. Cox. Making a Science of Model Search: Hyperparameter Optimization in Hundreds of Dimensions for Vision Architectures. In *Intl. Conf. on Machine Learning*, pages 115 – 123, 2013.

[3] P. Chiranjeevi and S. Sengupta. Detection of moving objects using multi-channel kernel fuzzy correlogram based background subtraction. In *IEEE Trans. on Cyber. (to appear)*.

[4] D. A. Clausi. An analysis of co-occurrence texture statistics as a function of grey level quantization. In *Can J Remote Sensing*, volume 28, no. 1, pages 45 – 62, 2002.

[5] A. Coates and A. Ng. The Importance of Encoding Versus Training with Sparse Coding and Vector Quantization. In *Intl. Conf. on Machine Learning*, pages 921 – 928, 2011.

[6] J. Daugman. Iris recognition and anti-spoofing countermeasures. In *7-th International Biometrics conference*, 2004.

[7] M. Faundez-Zanuy. On the vulnerability of biometric security systems. *IEEE Aerospace and Electronic Systems Magazine*, pages 3 – 8.

[8] J. Galbally, J. Fierrez, and J. Ortega-Garcia. Vulnerabilities in biometric systems: attacks and recent advances in liveness detection. *DATABASE*, 1(3):4, 2007.

[9] J. Galbally, J. Ortiz-Lopez, J. Fierrez, and J. Ortega-Garcia. Iris liveness detection based on quality related features. In *5th IAPR Int. Conf. on Biometrics*, pages 271 – 276, 2012.

[10] R. Haralick, K. Shanmugam, and I. Dinstein. Textural features for image classification. In *IEEE TSMC*, volume SMC-3, no. 6, pages 610 – 621, 1973.

[11] I. International Organization for Standardization. ISO/IEC CD 30107 - Presentation attack detection (working draft), 2011. http://www.iso.org/iso/home.

[12] K. Jarrett, K. Kavukcuoglu, M. Ranzato, and Y. LeCun. What is the Best Multi-Stage Architecture for Object Recognition? In *IEEE Intl. Conf. on Computer Vision*, pages 2146 – 2153, 2009.

[13] S. Lazebnik, C. Schmid, and J. Ponce. Beyond bags of features: Spatial pyramid matching for recognizing natural scene categories. In *IEEE Conference on Computer Vision and Pattern Recognition*, pages 2169 – 2178, 2006.

[14] E. Lee, K. Park, and J. Kim. Fake iris detection by using purkinje image. In *Advances in Biometrics*, volume 3832 of *Lecture Notes in Computer Science*, pages 397–403. 2005.

[15] D. Lowe. Object recognition from local scale-invariant features. In *Proceedings of the International Conference on Computer Vision*, volume 2, pages 1150 – 1157, 1999.

[16] R. Nosaka, Y. Ohkawa, and K. Fukui. Feature extraction based on co-occurrence of adjacent local binary patterns. In *Advances in image & video technology*, pages 82 – 91, 2012.

[17] T. Ojala, M. Pietikainen, and T. Maenpaa. Multiresolution gray-scale and rotation invariant texture classification with local binary patterns. In *IEEE Trans. Pattern Anal. Mach. Intell*, volume 24, pages 971 – 987, 2002.

[18] V. Ojansivu and J. Heikkil. Blur insensitive texture classification using local phase quantization. In *Image and Signal Processing, Lecture Notes in Computer Science*, volume 5099, pages 236 – 243, 2008.

[19] N. Pinto and D. D. Cox. Beyond simple features: A large-scale feature search approach to unconstrained face recognition. In *IEEE International Conference on Automatic Face and Gesture Recognition*, pages 8 – 15, 2011.

[20] P. Pudil, J. Novovicova, and J.Kittler. Flotating search methods in feature selection. In *Pattern Recognition Letters*, volume 15, pages 1119 – 1125, 1994.

[21] A. F. Sequeira, J. C. Monteiro, A. Rebelo, and H. P. Oliveira. MobBIO a multimodal database captured with an handheld device. In *Proceedings of Int. Conf. on Computer Vision Theory and Applications*, pages 133 – 139, 2014.

[22] A. F. Sequeira, J. Murari, and J. S. Cardoso. Iris liveness detection methods in mobile applications. In *Proceedings of International Conference on Computer Vision Theory and Applications*, pages 22 – 33, 2014.

[23] L. Soh and C. Tsatsoulis. Texture analysis of sar sea ice imagery using gray level co-occurrence matrices. In *IEEE TGRS*, volume 37, pages 780 – 795, 1999.

[24] V. Vapnik. In *The Nature of Statistical Learning Theory*, 1995.

[25] M. J. Weinberger, G. Seroussi, and G. Sapiro. Loco-i: a low complexity, context-based, lossless image compression algorithm. In *Data Compression Conf.*, pages 140 – 149, 1996.

[26] J. Yang, K. Yu, Y. Gong, and T. Huang. Linear spatial pyramid matching using sparse coding for image classification. In *IEEE Conference on Computer Vision and Pattern Recognition*, pages 1794 – 1801, 2009.

[27] L. Zhang, Z. Zhou, and H. Li. Binary gabor pattern: an efficient and robust descriptor for texture classification. In *Proc. 19th Int. Conf. on Image Proc.*, pages 81 – 84, 2012.