Integrating Facial Makeup Detection Into Multimodal Biometric User Verification System

Ekberjan Derman* CuteSafe Technology Inc. Gebze, Kocaeli, Turkey ekberjan.derman@cutesafe.com Chiara Galdi, Jean-Luc Dugelay Eurecom Digital Security Department 06410 Biot, France {chiara.galdi, jean-luc.dugelay}@eurecom.fr

Abstract-Multimodal biometric fusion is generally used for increasing the verification accuracy by combining two or more biometric traits. Fusion systems with predefined constant weight values for each biometry becomes much popular. Among biometrics, face modality is one of the most common traits that is used in such fusion system. However, face verification suffers from many challenging difficulties, one of which is facial makeup. Recently, it has been shown that the accuracy of face verification can be impacted by the presence of facial makeup. And as such, the verification result of a multimodal fusion system with constant weight value for each biometry can be degraded by facial cosmetics. In this work, we propose a method of integrating facial makeup detection into the fusion system to increase performance. In our investigated scenario, score level fusion of face, fingerprint and iris verification are performed, while the weight value of each trait changes dynamically according to the level of makeup classification of test facial image. So far, this is the first work taking into account the facial makeup within a multimodal biometric verification system. Experiments on 1600 different subjects reveal that our proposed method can help in increasing the overall performance of fusion system than without using the facial makeup information.

I. INTRODUCTION

A single trait based biometric verification system, such as using only fingerprint or face, usually has lower performance than systems combining two or more biometrics [1]. As such, multimodal biometric fusion obtained has obtained more and more interest, and face verification is one of the most common part of such a system [2]. Usually, a fusion system assigns a weight to each biometry, which indicates how much each trait should contribute to the final result. However, for a lowcost fusion system that uses a non-NIR(Near Infrared) camera for capturing face images, soft biometrics, especially facial makeup may impair the performance of face verification.

A significant challenge can be posed by the usage of makeup as a face alteration method, since it represents a non-permanent and cost effective, yet simple way of confounding the system [3]. Therefore, makeup detection in a face image can benefit face verification from the perspective of both accuracy and security. But a fusion system that includes face verification and has a predefined constant weight value for each biometric trait could be negatively affected by facial makeup. In this work, we especially concentrate on this situation, and propose a method

*: Corresponding author

to dynamically assign weight values for each biometric trait by classifying the test facial images into different makeup levels.

In our investigated scenario, the fusion system uses a total of three stand-alone biometrics, such as face, fingerprint, and iris, and the system performs score level fusion on them. In addition, the system carries out makeup detection on the captured facial image, and classifies it into four different groups, namely "no makeup", "light makeup", "medium makeup" and "heavy makeup". A predefined initial weight value is assigned for each of the three traits. Then, the weight of the face verifier would be adjusted according to the makeup classification result. If, for example, the face image is with heavy makeup, then it is reasonable that the face verifier would give incorrect matching result. Thus, even if the fingerprint and iris matchers give more accurate matching scores, the final fused result would be impaired. In such cases, by using our proposed method, the fusion system considers the result of face matcher as undependable, then chooses to abandon the face verifier and relies only on fingerprint and iris traits. Similarly, if the test face image is of medium or light makeup, the weight value of face matcher will also be adjusted accordingly, while with no makeup, the weight values of all traits would be the same as predefined.

This fusion mechanism is fundamentally different from previous multi-modal fusion systems, since we change the weight of each trait in the fusion system dynamically with the help of facial makeup detection. To the best of our knowledge, this is the first work that uses facial makeup detection in a biometric fusion system. We constructed a database with totally 1600 subjects, and tested our proposed algorithm accordingly.

The rest of this paper is organized as follows: Section II provides a brief overview of the related work, Section III introduces the proposed method, Section IV describes the approaches used for each component of the fusion system, Section V presents related experiments and results, while the last section concludes the paper.

II. RELATED WORK

In order to provide multiple evidences to improve the verification result, multimodal biometric systems have been studied thoroughly over the past decades. Data fusion from multiple biometric systems has been proven to be more efficient than single trait verification [1]. Fusion systems with two traits, such as using face and fingerprint [2][4][5], face and iris [6][7][8], or fingerprint and iris [9][10][11] are proposed by researchers. In [12], Aboshosha et al. proposed a decision level fusion system using face, fingerprint and iris. In all these works, researchers reported that multimodal fusion system outperforms their investigated single trait.

Soft biometrics, and in particular the impact of facial cosmetics to face verification, have raised attention in recent years. In [23], authors investigated the effects of facial makeup to automatic face recognition, indicated the need for a better understanding of face altering scheme with the help of facial cosmetics and the importance of designing algorithms to successfully overcome the obstacle generated by the application of facial makeup. In [3], authors proposed an algorithm for facial makeup detection by extracting the shape, texture and color characteristics of the input face, and presented an adaptive preprocessing scheme to exploit the knowledge of the presence or absence of facial makeup to improve facial matching accuracy. Authors in [16] built a facial makeup database, and investigated its effect on face recognition by treating the face as a whole as well as separately investigate the most significant makeup application areas such as skin, eyes, and mouth. Also, researchers in [17] proposed an algorithm for detecting facial makeup by shape and texture characteristics, and classify them using Support Vector Machines (SVM) and Alligator.

All these works have contributed significantly to multimodal biometric verification system, as well as facial makeup detection. However, no any previous work has been carried out for combining these two fields together, most probably due to the fact that facial makeup detection is a relatively new topic. In this work, we investigate a multimodal biometric fusion system by combining three different biometrics at score level, and integrate facial makeup detection into it, which presents an early attempt in this field. Instead of just giving information regarding whether the input image has makeup or not, we classify the facial input image into different levels of makeup and the classification result is sent to tune weight parameters of each single trait in our fusion system, which is a novel attempt.

III. THE PROPOSED FUSION SYSTEM

The overall flowchart of the proposed fusion system is described in Figure 1. There are three independent biometric verifiers in the system: face, fingerprint and iris. Since our main focus is on how to integrate the facial makeup detection into the fusion system, we do not provide any specific algorithm for face, fingerprint or iris verification. Instead, we propose how to utilize the facial makeup detection result to dynamically allocate weight values for different biometric traits. For that, we choose to concentrate on the scenario of performing score-level fusion on these three traits. The input of each trait is the captured relevant biometric image, while their output is a matching score respectively. Then these scores are fused together to obtain the final matching score, which can be used to decide whether the test subject is genuine or



Fig. 1. Overall flowchart of the proposed fusion system.

not. Traditionally, the final matching score can be obtained by the Sum Rule [14] as follows:

$$S = W_f S_f + W_{fp} S_{fp} + W_i S_i \tag{1}$$

where, S_f , S_{fp} and S_i represent matching scores obtained by the face, fingerprint and iris matchers, while W_f , W_{fp} and W_i correspond to these traits' relevant weight values respectively, and:

$$W_f + W_{fp} + W_i = 1.0 (2)$$

The weight values of each biometric trait in the fusion system represent what percentage of the final score should be from a given trait. In a conventional multimodal fusion system, these weight values are estimated beforehand and set as constant. In this work, we also estimate these values first, but further adjust them dynamically in accordance with the classification result of facial makeup detection. The input image of the face verifier is also used as input for the facial makeup detector for classifying it into four different makeup groups: no-makeup, light makeup, medium makeup, and heavy makeup. For each class, we assign corresponding confidence score (C_f). Then using this score, we decide how much we should rely on the face verifier, and change the weight value of each trait accordingly. For the four different makeup level, the confidence score C_f can be expressed as follows:

$$C_{f} = \begin{cases} 1.0 & no \ makeup \\ C_{1} & light \ makeup \\ C_{2} & medium \ makeup \\ C_{3} & heavy \ makeup \end{cases}$$
(3)

The values of C_1 , C_2 and C_3 can be determined experimentally. In this work, we chose these values as 0.8, 0.5 and 0.0 respectively, and carried out our test accordingly.

With this confidence score, we propose to change the final weight value of each trait and obtain the fused final score as follows:

$$S = C_f W_f S_f + W_{fp} S_{fp} + W_i S_i + \frac{1.0 - C_f}{2} W_f (S_{fp} + S_i)$$
(4)



Fig. 2. Reference image and makeup series images in their original form (figure adopted from [16]).

That is, if there is no facial makeup, the weight value of each trait would be the same as predefined, but if there is facial makeup, the system would choose whether to trust the face verifier or not, how much it should trust, and whether to rely more on the other two biometrics instead. The calculation of weight values W_f , W_{fp} and W_i , as well as the algorithm used to detect facial makeup is described more in detail in *Section IV*.

IV. METHODOLOGY

A. Biometric Verification

We use commercial software for obtaining matching scores for face and fingerprint verification. For the iris verification, we use the open source iris recognition system, OSIRIS [15], developed by *Telecom Sud Paris*.

B. Facial Makeup Detection

The facial makeup is detected using shape and texture descriptors [17]. The whole steps are illustrated in Figure 3.

We choose to first resize the input face image into 150x130 pixel and convert it into gray scale, on which we perform feature extraction. We use LGBP (Local Gabor Binary Pattern) [18] and HOG [19] techniques to extract texture and shape features. Considering the fact that LGBP is a texture and HOG is a shape descriptor, when used together, complementary information can be provided, and much better detection accuracies are obtained in facial makeup detection [17].

1) LGBP feature extraction: The gray scale face image is convolved with Gabor filter to obtain multiple Gabor Magnitude Pictures (GMPs) in frequency domain by applying multiscale and multi-orientation Gabor filters. The Gabor filter that we use is expressed as follows [18]:

$$\psi_{\mu,v}(z) = \frac{||k_{\mu,v}||^2}{\sigma^2} e^{-\frac{||k_{\mu,v}||^2||z||^2}{2\sigma^2}} \left[e^{ik_{\mu,v}z} - e^{-\frac{\sigma^2}{2}} \right]$$
(5)

in which, μ and v represent the orientation and scale of the Gabor filters, z = (x, y), ||.|| denotes the norm operator, and the wave vector $k_{\mu,v} = k_v e^{i\phi_{\mu}}$ where $k_v = k_{max}/\lambda^v$ and $\phi_{\mu} = \pi \mu/8\lambda$ is the spacing factor between filters in the frequency domain.

Gabor filters with totally five scales $v \in 0, ..., 4$ and eight orientations $\mu \in 0, ..., 7$ are used to obtain totaly 40 Gabor images. For each Gabor image, we use uniform binary-based LBP with eight sampling points within two pixel neighborhood [20]. Then, we represent the face region with 5 x 5 nonoverlapping regions, and compute the Local Binary Pattern (LBP) histogram independently within each of these regions. After that, we combine the resulting *m* histograms to yield the spatially enhanced histogram vector. Finally, we concatenate all these 40 histogram vectors together to generate one LGBP feature vector for the input face image. Since the LBP compresses the histograms from 256 to 59 elements, after LGBP feature extraction, we obtain a feature vector with length 59 x 5 x 5 x 40 = 59,000 for one single image.

2) HOG feature extraction: For extracting shape features, we calculate the histogram channels over rectangular cells (i.e. R-HOG) by computation of unsigned gradient [19]. Totally 9 rectangular cells and 9 bin histogram per cell is computed as suggested in [19]. Then these histograms and bins were concatenated to make a 81-dimensional feature vector. HOG technique is applied on a 5x5 non-overlapping regions. Thus, the total number of features extracted from one image is equal to 81 x 5 x 5 = 2025.

3) Feature level fusion: As since the HOG features lie into a range of [0, 1], we first apply normalization for LGBP features by using min-max normalization method [21]. After this normalization step, LBGP and HOG features are concatenated together to form a single feature vector for the input image, and sent to the classifier.

4) Classification: We employ Support Vector Machines (SVM) as our classifier [22]. Totally four classes are provided for the classifier: no-makeup, light makeup, medium makeup and heavy makeup. We use YouTube Makeup Database (YMU) [23] as our training dataset. We manually select and divide the YMU images into these four groups, provide totally 30 images per group, and use their relevant feature vector to train SVM. After successful training, the feature vector of the test image is sent to be classified. Then we obtain the value of C_f in Equation 3 using the classification result.

C. Biometric Fusion

For estimating the weight values of each biometric trait in the fusion system as described in *Section III*, we use the *Matcher Weighting* (MW) fusion method [21]. Weight values are assigned to each matcher based on their *Equal Error Rate* (EER), which describes the value when the matcher's *False Acceptance Rate* (FAR) and *False Rejection Rate* (FRR) are equal to each other. Let e_m denote the EER of a matcher *m*, where m = 1, 2, ..., M (here in our case, M = 3). Then the weight W_m associated with matcher *m* is calculated as:

.

$$W_m = \frac{\left(1/\sum_{m=1}^M \frac{1}{e_m}\right)}{e_m} \tag{6}$$

Using our test data, the EER of face, fingerprint and iris matchers are estimated using the above equation, and then sent to Equation 4 for obtaining final fused score.

V. EXPERIMENTS AND RESULTS

A. Test Data Construction

Lack of large scale test datasets for biometric verification is one of the biggest challenges. In order to evaluate the applicability of our proposed algorithm, test database of considerable size is mandatory. For experimental purpose, we constructed a database of totally 1600 different subjects, with each subject has face, fingerprint and iris images.

1) Face images: We used the FaceScrub [24] and FERET [25] image database. The FaceScrub database consists of totally 530 different subjects, while FERET database is with totally 994 different persons. Besides, we also collected our own database of 76 subjects with face images captured in different time period.

2) Fingerprint images: We used FVC2002 Db_a [26] and SDUMLA-HMT's URU4000B and ZY202-B [27] databases. The FVC2002 Db_a database contains images of totally 400 different fingers, with 8 impression for each finger. We select only five impressions for a single finger in our case. The SDUMLA-HTM database consists of totally 2x106x6=1272 different fingers. The first 1200 of them are used in our case.

3) Iris images: We used the CASIA-IrisV4 collected by the Chinese Academy of Sciences' Institute of Automation (CASIA) [28]. Totally 1600 subjects from the database are selected. We only selected iris images with no eyeglass, since our used iris matcher fails to detect pupil region when there is eyeglass and light reflection on it.

For an individual, assuming that face, fingerprint and iris biometrics are statistically independent, which is a widely accepted and reasonable practice in multimodal biometrics research [21], we create a virtual subject by associating an individual from the face database with an individual from the fingerprint and iris database. In this manner, we arrived at our database with 1600 subjects. Each of the first 606 subjects has five images for each biometry, while each of the rest has two, which is due to the lack of sufficient frontal face images from FERET database. This results in totally 606x5+2x994=5018 genuine images for our test.

We perform score normalization separately on the obtained scores from each of these three biometric traits by using minmax normalization [21]. Matching scores lie in the range of 0.0 and 1.0, where 0.0 means totally different, while 1.0 means exactly the same. For the score normalization process and determining fusion parameters, we used the entire database as suggested in [21].

B. Testing Protocol

Based on the *FVC2002* testing protocol [26], we carry out our experiments to:

• Calculate the FRR by matching each sample against the remaining samples of the same subject. If the matching *h* against *g* is performed, the symmetric one (i.e. *g* against



Fig. 3. Overall flowchart of the facial makeup detection process.



Fig. 4. Sample face (top), fingerprint (middle) and iris (bottom) images of one subject of our test database.

h) is not executed to avoid correlation. Thus in this case, the total number of *genuine* scores is: 606x10+994=7054.

• Compute the FAR by matching the first sample of each subject against the first sample of the remaining subjects. If the matching *h* against *g* is performed, the symmetric one (i.e. *g* against *h*) is not executed to avoid correlation. So we have a total number of impostor scores as: (1600x1599)/2=1,279,200.

C. Experimental Results

The obtained FRR with respect to 1.0% and 0.1% FAR, and EER of individual biometrics of face, fingerprint and iris matchers, as well as the fusion system without facial makeup detection and with facial makeup detection as proposed in this work, are shown in Table I. For comparison purpose, we also report performances of fusing only two biometrics with and without makeup detection as well. The calculated weight value, W_m , of each individual matcher in the fusion system obtained by Equation 6 is given in Table II. The result of facial makeup classification is illustrated in Table III. The Receiver Operating Characteristic (ROC) curves of individual matchers and fusion system combining face, fingerprint, iris and makeup detection are illustrated in Figure 5. The ROC curve is a two-dimensional measure of classification performance that describes the probability of classifying correctly the genuine test images against the rate of incorrectly classifying impostor examples.

From these results, we see that for single trait biometric verification, face matcher gives the lowest performance comparing to fingerprint and iris matchers. This is reasonable, since the face images collected in the database contains a vast variety of challenging conditions, such as illumination, head pose, facial



Fig. 5. ROC curve of each of the face (green), fingerprint (blue) and iris (purple) matchers, as well as fusion system that combines these three biometrics together with facial makeup detection (red).

TABLE I					
EXPERIMENTAL RESULTS OF THE PROPOSED FUSION SYSTEM					

Matcher	FRR		EER
	FAR = 1.0%	FAR = 0.1%	
Face	13.42 %	21.18%	5.70%
FP (Fingerprint)	3.11%	3.87%	2.75%
Iris	4.34%	8.02%	2.93%
Face + FP	2.78%	3.23%	1.97%
Face + FP + Makeup	2.63%	3.01%	1.79%
Face + Iris	3.84%	6.72%	2.45%
Face + Iris + Makeup	3.56%	6.48%	2.33%
FP + Iris	1.96%	2.85%	1.47%
Face + FP + Iris	1.19%	2.03%	1.08%
Face + FP + Iris + Makeup	0.98%	1.67%	0.99%

TABLE II Calculated Weight Values of Each Individual Biometric Matchers in the Fusion System

Matcher	Face	Fingerprint	Iris
Face Only	1.0	-	-
Fingerprint Only	-	1.0	_
Iris Only	-	-	1.0
Face + Fingerprint	0.325	0.675	_
Face + Iris	0.34	-	0.66
Fingerprint + Iris	-	0.516	0.484
Face + Fingerprint + Iris	0.191	0.417	0.392

TABLE III Facial Image Counts of Different Classes Obtained by Makeup Detection

No Makeup	Light Makeup	Medium Makeup	Heavy Makeup	Total
2216	1837	535	430	5018

t weight in any fusion l illustrated in Table II. always obtained higher odal biometric verificamodal ones. Besides, as ting the facial makeup ad dynamically tuning cording to the makeup reased performance for sion system than their p detection. The facial red in Table III reveals

expression, age difference, and facial cosmetic makeup, etc. All these contribute negatively to the verification process. As such, the face matcher has the lowest weight in any fusion system as obtained by Equation 6 and illustrated in Table II. Meanwhile, multimodal fusion system always obtained higher performance than single trait. Three-modal biometric verification has higher performance than two-modal ones. Besides, as we proposed in this work, by integrating the facial makeup detection into the fusion system, and dynamically tuning the weight value of each matcher according to the makeup classification result, we observed increased performance for both two-modal, and three-modal fusion system than their relevant modes without facial makeup detection. The facial makeup classification result that showed in Table III reveals without facial makeup detection, the fusion system consisting face, fingerprint and iris has an EER of 1.08%. With our tested 1,279,200 impostor scores, this means at least 13,815 scores would be falsely accepted. However, with our proposed method, we improved this EER to 0.99%, which reduces the falsely accepted score count to 12,664, that is, the fusion system is able to correctly reject 1151 impostor scores more. For the two-modal fusion system of face and fingerprint, which gained the biggest improvement of EER by the proposed method, there are at least 2302 more impostor scores can be correctly rejected. Thus, as the results reveal, our proposed method of taking into account the facial makeup detection while fusing the different biometric traits is shown as efficient and applicable to improve the performance of multimodal fusion.

VI. CONCLUSION

We proposed a method of integrating the facial makeup detection and classification result into a multimodal biometric system. Instead of assigning a predefined constant weight value for each single trait while fusing, we change these weight values dynamically according to the facial makeup classification result. This is the first work to investigate the possibilities of using facial makeup information into a multimodal fusion system. We constructed a database of totally 1600 different subjects, and experimental results by 7054 genuine and 1,279,200 impostor scores reveal that our proposed method can help to increase the verification result of the fusion system.

ACKNOWLEDGMENT

The authors would like to thank Prof. Bernadette Dorizzi and Prof. Mounim A. El Yacoubi from Telecom SudParis, France, as well as Mr. Ali Kuru from Proline, Turkey, for their constructional help and suggestions. This work is supported by European ITEA3 program (project name: 12028 IDEA4SWIFT) [29].

REFERENCES

- A. Ross and A. Jain, *Information Fusion in Biometrics*, Recognition Letters, vol. 24, pp. 2115-2125, September, 2003.
- [2] A. Rattani, D. R Kisku, and M. Bicego, *Feature Level Fusion of Face and Fingerprint Biometrics*, IEEE International Conference on Biometrics: Theory, Applications, and Systems (BTAS), 2007.
- [3] C. Chen, A. Dantcheva and A. Ross, Automatic Facial Makeup Detection with Application in Face Recognition, Proceedings of 6th IAPR International Conference on Biometrics (ICB), June, 2013.
- [4] N. Hassan, D. A. Ramli and S. A. Suandi, Fusion of Face and Fingerprint for Robust Personal Verification System, International Journal of Machine Learning and Computing, vol. 4, no. 4, August, 2014.
- [5] S. Karanwal, D. Kumar and R. Maurya, *Fusion of Fingerprint and Face by Using DWT and SIFT*, International Journal of Computer Applications, vol. 2, no. 5, pp. 0975-8887, June, 2010.
- [6] R. Connaughton, K. W. Bowyer and P. Flynn, Fusion of Face and Iris Biometrics, Handbook of Iris Recognition, pp. 219-237, Springer, London, 2013.
- [7] Y. Gon. Kim, K. Y. Shin, E. C. Lee and K. R. Park, *Multimodal Biometric System Based on the Recognition of Face and Both Irises*, International Journal of Advanced Robotic Systems, vol. 9, 2012, DOI: 10.5772/50869.

- [8] R. Connaughton, K. W. Bowyer and P. Flynn, Fusion of Face and Iris Biometrics from a Stand-Off Video Sensor, The 22nd Midwest Artificial Intelligence and Cognitive Science Conference (MAICS), Cincinnati, Ohio, USA, 2011.
- [9] M. Abdolahi, M. Majid and M. Jafari, *Multimodal Biometric System Fusion Using Fingerprint and Iris with Fuzzy Logic*, International Journal of Soft Computering and Engineering, vol. 2, no. 6, pp. 504-510, 2013.
- [10] P. U. Lahane, and S. R. Ganorkar, *Efficient Iris and Fingerprint Fusion for Person Identification*, International Journal of Computer Applications, vol. 50, no. 17, July, 2012.
- [11] V. Conti, C. Millitello, F. Sorbello and S. Vitabile, A Frequencybased Approach for Features Fusion in Fingerprint and Iris Multimodal Biometric Identification Systems, IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), vol. 40, issue. 4, pp. 384-395, April, 2010.
- [12] A. Aboshosha, K. A. E. Dahshan, E. A. Ebeid and E. K. Alsayed, *Fusion of Fingerprint, Iris and Face Biometrics at Decision Level*, International Journal of Advanced Research in Computer Science and Software Engineering, vol. 5, issue. 2, February, 2015.
- [13] L. Hong, Y. Wan and A. K. Jain, *Fingerprint Image Enhancement: Algorithm and Performance Evaluation*, IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 20, pp. 777-789, 1998.
- [14] A. Ross and A. Jain, *Information Fusion in Biometrics*, Pattern Recognition Letters, vol. 24, pp. 2115-2125, 2003.
- [15] N. Othman, B. Dorizzi and S. G. Salicetti, OSIRIS: An Open Source Iris Recognition Software, Pattern Recognition Letters, 2015 (document in press, published online 30 Sep. 2015).
- [16] M.-L. Eckert, N. Kose and J.-L. Dugelay, Facial Cosmetics Database and Impact Analysis on Automatic Face Recognition, IEEE International Workshop on Multimedia Signal Processing (MMSP), pp. 434-439, 2013.
- [17] N. Kose, L. Apvrille and J.-L. Dugelay, Facial Makeup Detection Technique Based on Texture and Shape Analysis, IEEE International Conference on Automatic Face and Gesture Recognition (FG2015), May 4-8, Slovenia.
- [18] W. Zhang and S. Shan, Local Gabor Binary Pattern Histogram Sequence (LGBPHS): A Novel Non-Statistical Model for Face Representation and Recognition, Proceedings of International Converence on Computer Vision (ICCV), pp. 786-791, 2005.
- [19] O. Ludwig and D. Delgado, *Trainable Classifier-Fusion Schemes: An Application to Pedestrian Detection*, IEEE International Conference on Intelligent Transportation Systems, pp. 432-437, 2009.
- [20] T. Ahonen, B. Hadid and M. Pietikainen, *Face Description with Local Binary Patterns: Application to Face Recognition*, IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 28, pp. 2037-2041, December, 2006.
- [21] R. Snelick, U. Uludag, A. Mink, M. Indovina and A. Jain, Large Scale Evaluation of Multimodal Biometric Authentication Using State-of-the-Art Systems, IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 27, no. 3, pp. 450-455, March, 2005.
- [22] C. C. Chang and C. J. Lin, LIBSVM: A Library for Support Vector Machines, ACM Transactions on Intelligent Systems, 2:27:1-27:27, 2011. Available at: http://www.csie.ntu.edu.tw/cjlin/papers/libsvm.pdf
- [23] A. Dantcheva, C. Chen and A. Ross, Can Facial Cosmetics Affect the Matching Accuracy of Face Recognition Systems?, IEEE International Conference on Biometrics: Theory, Applications and Systems (BTAS), 2012.
- [24] H. -W. Ng and S. Winkler, A Data-Driven Approach to Cleaning Large Face Datasets, IEEE International Conference on Image Processing (ICIP), Paris, France, October 27-30, 2014.
- [25] The Facial Recognition Technology (FERET) Database, http://www.itl.nist.gov/iad/humanid/feret/feret_master.html
- [26] D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman and A. K. Jain, FVC2002: Second Fingerprint Verification Competition, available at: http://bias.csr.unibo.it/fvc2002/
- [27] Y. Yin, L. Liu and X. Sun, SDUMLA-HMT: A Multimodal Biometric Database,
- [28] CASIA Iris Image Database, available at: http://biometrics.idealtest.org/
- [29] ITEA3 Project under the name: Identity, Doc, Exchange, Authentication 4 Systems Worldwide Interconnections of Frequent Travelers, description available at: https://itea3.org/project/idea4swift.html