algorithms

MDPI

Article

Design and Implementation of a Multi-Modal Biometric System for Company Access Control †

Elisabetta Stefani and Carlo Ferrari *

Department of Information Engineering, The University of Padova, Via Gradenigo 6a, 35131 Padova PD, Italy; elisabetta.stefani@studenti.unipd.it

* Correspondence: carlo.ferrari@unipd.it; Tel.: +39-049-827-7729

† This paper is an extended version of our paper published in the 2nd International Conference on Data Compression, Communication, Processing and Security (CCPS 2016).

Academic Editors: Francesco Bergadano and Bruno Carpentieri
Received: 1 February 2017; Accepted: 23 May 2017; Published: 27 May 2017

Abstract: This paper is about the design, implementation, and deployment of a multi-modal biometric system to grant access to a company structure and to internal zones in the company itself. Face and iris have been chosen as biometric traits. Face is feasible for non-intrusive checking with a minimum cooperation from the subject, while iris supports very accurate recognition procedure at a higher grade of invasivity. The recognition of the face trait is based on the Local Binary Patterns histograms, and the Daughman's method is implemented for the analysis of the iris data. The recognition process may require either the acquisition of the user's face only or the serial acquisition of both the user's face and iris, depending on the confidence level of the decision with respect to the set of security levels and requirements, stated in a formal way in the Service Level Agreement at a negotiation phase. The quality of the decision depends on the setting of proper different thresholds in the decision modules for the two biometric traits. Any time the quality of the decision is not good enough, the system activates proper rules, which ask for new acquisitions (and decisions), possibly with different threshold values, resulting in a system not with a fixed and predefined behaviour, but one which complies with the actual acquisition context. Rules are formalized as deduction rules and grouped together to represent "response behaviors" according to the previous analysis. Therefore, there are different possible working flows, since the actual response of the recognition process depends on the output of the decision making modules that compose the system. Finally, the deployment phase is described, together with the results from the testing, based on the AT&T Face Database and the UBIRIS database.

Keywords: data security; adaptive multi-modal biometric system; biometric identifiers; face recognition; iris recognition

1. Introduction

Access control is a fundamental issue of any security system, and it is mainly devoted to checking the truthfulness of users' claimed identity, in order to both verify personal access rights and support tracing and logging services. Access control implies authorization, and it strongly relies on identity analysis and authentication. Within a company structure, the requirements and rules that preside over the access control may differ with respect to different locations, expected actions, and functions of principals. Moreover, they can vary over time. The main focus of this paper is authentication (i.e., the process of confirming the identity of an entity), and its deployment in a real context within a company security system where it should be responsible for regulating the main access and the transit to the different zones inside the company itself.

Authentication involves the verification of the validity of at least one form of identification (e.g., documents, digital certificate, biometric identifiers, etc.). The most interesting approach for

identity assessment falls into the category "checking something that the user is or does" as the factors of authentication, known as inherence factors. Examples of inherence factors are static or dynamic biometric parameters like face, fingerprint, iris, retinal pattern, signature, voice, etc. These biometric identifiers are distinctive and measurable characteristics which can be used to label and describe individuals in an almost unique way [1]. There are several advantages in using biometrics: they cannot be lost or forgotten, and they require the person under recognition to be present at the check point. Additionally, it is difficult to forge them.

Each biometric has its strengths and weaknesses, and the choice depends on the application. No single biometric is expected to effectively meet the security requirements of all the applications, thus each biometric technique is admissible and there is no "optimal" biometric characteristic [2]. The match between a specific biometric and an application is determined depending upon the operational mode of the application and the properties of the chosen biometric itself.

Biometrics can be either singularly or simultaneously used for identification. In [3], a system that couples One-Time-Password technique with face recognition has been proposed. As there is no proof of correlation among the different biometric parameters of an individual, the combination of independent sources of information is very promising for the improvement of the quality of the recognition process. Multi-biometric systems are biometric systems that consolidate multiple sources of biometric evidence; the integration of evidence is known as fusion, and there are various levels of fusion, which can be divided into two broad categories: pre-classification (fusion before matching) and post-classification (fusion after matching) [4,5]. Depending on the nature of the sources, multi-biometric systems can also be classified into different categories; multi-sensor systems, multi-algorithm systems, multi-instance systems, multi-sample systems, multi-modal systems, and hybrid systems [6].

Multi-modal biometric systems are more reliable than uni-modal systems due to the presence of multiple and independent pieces of evidence [7]. They address the problem of non-universality, since multiple traits ensure sufficient population coverage and provide anti-spoofing measures by making it difficult for an intruder to simultaneously spoof different biometric traits of a legitimate user. A system can operate either in selection or checking mode. The former is an identification process: a person's traits are acquired to establish the identity of the individual; it is a one-to-many search process in which the biometric characteristics set against all the database entries that represent enrolled users, in order to find those biometric references with a specific degree of similarity. The latter is about verification: a person's traits are acquired in order to verify the claimed identity (e.g., a user name) of the unknown individual; it is a one-to-one comparison in which the submitted biometric characteristics set against a specified stored biometric reference and returns both the comparison score and the decision.

Both of these operational modes require an enrolment process where a subject presents her/his biometric characteristics to the sensors, in a controlled way, along with the non-biometric information, to form the user template. This subject information could be name, social security number, driver license's number, etc. Therefore, biometric features from the captured sample and the non-biometric information are stored in the database of the "user templates". It is clear that determining the "true" identity of an individual is beyond the scope of any biometric technology. Rather, biometric technology can only link a person to a biometric pattern and any identity data (e.g., name) and personal attributes (e.g., age, gender, profession, etc.) that were presented at the time of enrolment in the system [8].

A challenge–response type of authentication can be strengthened using multi-modal biometric systems, ensuring that "live" users are indeed present at the point of data acquisition, since these systems ask them to present a particular and predefined subset of biometric traits [9].

The problem of studying the best theoretical method to obtain an effective and efficient system for individuals' authentication has been widely addressed: there is a huge number of possible solutions, each employing different required credentials, algorithms, and practical deployments [2,10]. Nevertheless, the goal of all these systems is to minimize (and possibly set to zero) the number of users who are impostors but manage to be authenticated, or who are enrolled users but are rejected.

One of the main difficulties that all these attempts share, is at the level of the decision fusion, which is generally built into the actual code of the decision module. In this work, we aim to make explicit the knowledge and strategies about data fusion in the form of behavior, to be selectively activated according to the actual acquisition status, results, and available biometric traits. As we are considering an indoor application environment where all computing facilities are inside, and where there is quite a small number of enrolled users at a time, we are not concerned with the issues of confidentiality, integrity, and availability that can arise in more general situations [11]. The setting of the decision thresholds in biometric algorithms usually pursues the balance between the false acceptance rate (FAR) and the false rejection rate (FRR). At the level of the system deployment, the balance between FAR and FRR can differ with respect to the various areas which the access control refers to, and it finally depends on the security requirements (usually stated in the Service Level Agreement at the design level). Hence, the system deployment can benefit from the customization of a kind of general template methodology according to the given security constraints [12,13].

2. Materials and Methods

As stated in the previous section, the goal of this project is the design of an adaptive biometric system for indoor access control and presence monitoring. This system should operate within the scope of a medium/large-sized company which needs to keep some areas restricted to particular employees, depending on their roles or responsibilities. Therefore, proper sensors are supposed to be placed at any check point and in every room or structure in which only authorized users are allowed.

The system is intended to handle several different situations:

- different types of restricted areas have to be accessed by different types of user, depending on their role;
- company employees should be given an easy way to access, since they have to get in and out at least twice a day (they are enrolled in a special database);
- partners, suppliers, or auditors, provided with their own company device (thus known by the company) are submitted to an indirect authentication (e.g., having their template stored on their device and sending it to the company for the matching);
- since the company is open to the public, clients are supposed to access only the reception area;
- some employee is allowed to bring someone else in with them (the system is supposed to know who and where);
- the system works autonomously, but proper human intervention is always possible.

The system is intended to operate both in verification and in identification mode. Furthermore, the system is required to guarantee the requirements of the Service Level Agreement (SLA) that affect the expected FAR and FRR values, depending on the different areas or rooms within the company.

In a multi-modal biometric system it is worth coupling non-invasive easy-to-use biometrics at lower accuracy together with more robust but expensive parameters, which can intervene whenever a higher degree of confidence is required. Face and iris recognitions have been chosen for the proposed system.

The face identifier has been chosen because face recognition is a non-intrusive method of authentication and also requires minimum cooperation from the subject. Moreover, face matching is typically fast, even if it may be not very accurate. One popular approach to face recognition is based on the location, dimensions, and proportions of facial attributes such as eyes, eyebrows, nose, lips, and chin and their spatial relationships. The dimensions, proportions, and physical attributes of a person's face tend to univocally distinguish a single person with good enough confidence. Another approach that is widely used is based on the overall analysis of the face image that represents the face as a weighted combination of a number of canonical faces [14]. Face recognition involves two major tasks: face location and face recognition. Face location is the determination of the location of the face in the input image. Recognizing the located face means that the face is recognized from a general viewpoint (i.e., from any pose). It is worth mentioning that face recognition can be in a static controlled environment where the used is asked for some degree of cooperation, or in a dynamic uncontrolled

environment where the user can be completely unaware of being under analysis [15]. The visual texture of the iris is formed during fetal development, and stabilizes during the first two years of life. The complex iris texture carries very distinctive information that is useful for personal recognition of high accuracy. Besides, it is extremely difficult to surgically tamper with the texture of the iris and it is rather easy to detect artificial irises (e.g., designer contact lenses) [5,16]. Iris recognition is more accurate, but also more invasive because the user has to be very cooperative and the overall acquisition time (pose time plus true acquisition time) can be quite high.

An interesting approach which can be used for face recognition is the Pyramid Match Kernel [17], whici is based on a fast kernel function which maps unordered feature sets to multi-resolution histograms and computes a weighted histogram intersection in this space. Other methods for implementing face recognition are: the eigenface method using principal component analysis (PCA), which is based on the idea that a high-dimensional dataset is often described by correlated variables and therefore only a few meaningful dimensions account for most of the information; the PCA method finds the directions with the greatest variance in the data, called principal components. The Fisherfaces method uses linear discriminant analysis (LDA), which performs a class-specific dimensionality reduction; in order to find the combination of features that separates best between classes, it maximizes the ratio of between-classes to within-classes scatter [18]. The chosen methodology is the Local Binary Patterns (LBP). It is based on the extraction of local features from images; the basic idea is to summarize the local structure in an image by comparing each pixel with its neighbourhood. Then, the LBP image is divided into local regions and a histogram is extracted from each one. Finally, the spatially-enhanced feature vector (called Local Binary Patterns Histograms (LBPH) [18]) is obtained by concatenating all the local histograms. The application of facial recognition is expected to happen in a dynamic but somehow controlled environment in which a person who wants to be authenticated has to walk along a hallway following an ordered queue so that the sensor can easily detect whether a face is present in the acquired image and locate it.

Daughman's method has been chosen for iris recognition. It consists of several phases: segmentation (i.e., the location of the iris in the eye image), normalization with the Daugman's Rubber Sheet Model, encoding with the Log-Gabor wavelet and matching using the Hamming Distance [19].

A previous work involving face and iris for identity verification is described in [20]. These two biometric traits are combined using two different fusion strategies: the former is based on the computation of either an unweighted or weighted sum and the comparison of the result to a threshold, the latter considers the matching distances of face and iris classifiers as a two-dimensional feature vector and it uses a classifier, such as Fisher's discriminant analysis and a neural network with radial basis function (RBFNN), to classify the vector as being genuine or an impostor.

A convenient mode in which a multi-modal system can operate is the serial mode: it means that the two biometric characteristics do not have to be acquired simultaneously and that a decision could be arrived at without acquiring all the traits. This last aspect is very important, especially for those applications where there are time constraints, because it leads to a reduction of the overall recognition time.

The proposed multi-modal biometric system relies on two different modules: the module for face identification and the module for iris verification. The fusion methodology adopted at the decision level is a post-classification method, and it follows the OR rule; i.e., it is sufficient that only a biometric trait is recognized as genuine to lead to a positive final decision. This serial matching approach gives the possibility of not acquiring all the traits; for example, only face recognition is considered if the information collected at the first module is believed to be enough to determine if a user is genuine or an impostor.

The system consists of several different submodules, each of them providing its own functionality. There are two *sensor modules* for face and iris acquisition, which capture the raw biometric data. In the *feature extraction modules*, the acquired data is processed to extract a set of salient and discriminatory features. In the *matcher modules*, the extracted features are compared against the stored templates,

providing a matching score. These last modules encapsulate the *decision making modules*, which can operate either in verification or identification mode. Moreover, there is the *system database module*, which stores the biometric templates of the enrolled users.

The system is intended to be adaptive; this means that it does not have a fixed and predefined behaviour, but its working flow depends on the response of the actual recognition process. Such a response depends on the values of evidence from the single decision modules, the number of previous attempts that did not result in a clear decision, and the evaluation of the quality of the acquisition set-up (lighting, focus, occlusions, and so on).

From a numeric value (generally normalized between 0 and 1) that represents the confidence of the matching, each decision module is given three possible different outputs {*YES*, *NO*, *MAYBE (?)*}, depending on the comparison of that value with some predefined thresholds that divide the interval [0,1] in different sub-intervals (see Figure 1). A decision module outputs the *YES* value if the obtained score is within the interval [0, t_1] and the user is recognized as one of the enrolled users (in identification mode) or their claimed identity has been confirmed (in verification mode). The output value *NO* is produced if the obtained score is within the interval [t_2, 1] and the user is rejected as if they were impostors. The output value *MAYBE (?)* results any time the obtained score is within the interval (t_1, t_2) and the decision module is not able to make a final decision with a sufficient degree of confidence.

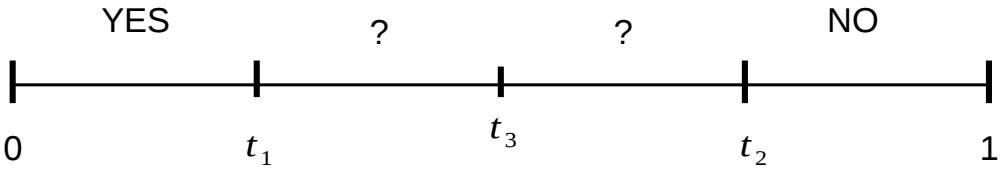

Figure 1. Face identification thresholds.

The *MAYBE (?)* value calls for further processing. From a general point of view, there are two main general choices, which involve either the repetition of the identification with a new acquisition of the same biometric, or passing to the analysis of a different biometric. Within the serial paradigm underlining the proposed system, an unsolvable uncontrolled face identification can reasonably be followed by a controlled face identification any time the degree of uncertainty is not very high. This means that if a user obtains an output score that is similar to a genuine user's score (but not similar enough), she/he is asked to try the face identification again, augmenting her/his cooperation during data acquisition, because face processing is always faster and less invasive than iris verification. Conversely, if the obtained score is nearer to the *NO* interval, the user is asked to submit to iris verification in order to keep a high degree of accuracy in the overall recognition performance.

If the unsolvable matching comes from a controlled face identification, it is worth repeating the same process instead of immediately proceeding to iris verification. The number of repetitions can depend on the quality of the resulting matching. Figure 2 represents the general template of the system flow: the choices are ruled by a special threshold: t_3, usually set in the middle of the *MAYBE* interval, as shown in Figure 1. Therefore, there are several different ways of working. For example, a user can be immediately identified and authenticated using their face as they approach the entrance; or they can be asked to repeat the face acquisition in a more controlled way; they can be asked to get closer and the authentication mode can be switched to the verification mode using the iris; again, this last phase can be repeated.

Formally, the system works according to some deductive rules which the decision making modules are based on and which represent response behaviors, according to the set-up and status of the acquisition point, the consequent quality of the acquired data, and the actual level of cooperation of the subjects. The effect of those rules strongly depends on the chosen values of the thresholds t_1, t_2, and t_3 that must always comply with the constraints shown in Figure 1.

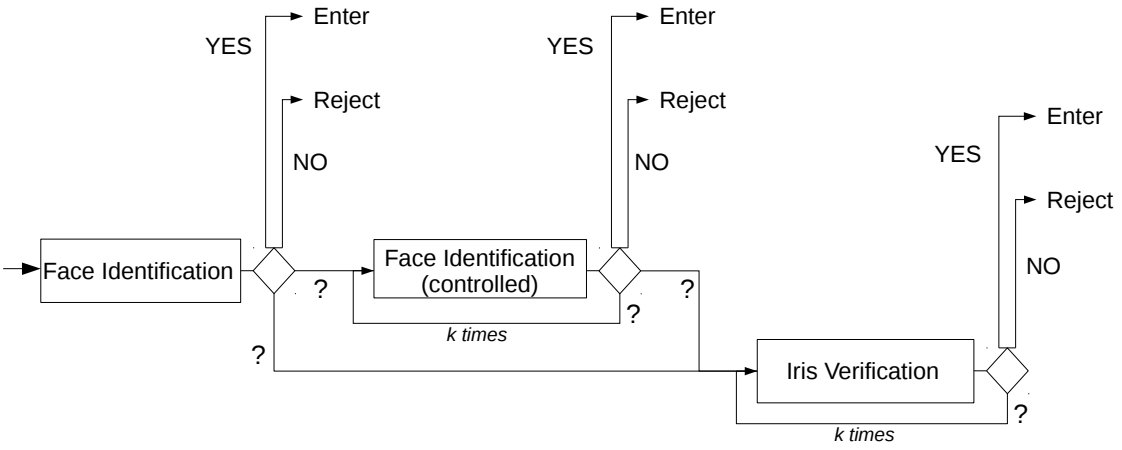

Figure 2. Possible system flows.

The following list shows those rules and their effect on the system working flow:

- require a controlled face identification if MAYBE is the result of the uncontrolled face identification and the obtained score is in the interval $[t_1, t_3]$;
- require a controlled face identification if MAYBE is the result of the (previous) controlled face identification and the obtained score is in the interval $[t_1, t_3]$ and the limit of max k repetition has not been reached;
- require iris verification if MAYBE is the result of the uncontrolled face identification and the obtained score is in the interval $[t_3, t_2]$;
- require iris verification if MAYBE is the result of the (previous) controlled face identifications and the obtained score is in the interval $[t_3, t_2]$;
- require iris verification if MAYBE is the result of the (previous) iris verifications and the limit of max k repetition has not been reached;
- ask for human intervention if NO is the result;
- ask for human intervention if the limit of k repetitions has been reached.

The number of repetitions k can be arbitrarily set by the programmer, and human supervision is always permitted.

3. Results

The sequence of face recognition and iris recognition is the core activity of the proposed system for access control. The soundness of the overall approach can be checked offline using proper data sets that are artificially combined to emulate the data acquisition processes. Moreover, the tests against the face identification and the iris verification procedures have been conducted separately, since no proof of correlation exists between the face and the iris parameter of a person, and the test sets and the outcomes are completely independent in this sense. The two databases that have been exploited in the system test are the AT&T Face Database from the AT&T Laboratories of Cambridge [21] and the UBIRIS database of irises [22]. The AT&T Face Database contains 10 different images (samples) of each of 40 distinct subjects, while UBIRIS maintains information about around 240 subjects. In order to form a coherent test set, 40 subjects have been randomly selected from the 240 subjects already in UBIRIS, each having five different iris images.

3.1. Face Identification

To test the face identification phase, the AT&T Face Database was divided into a training set and a test set. The best three face images for each of the 40 users were selected by hand in order to train the LBPH model. The remaining seven images of each user (summing up to a total of 280 images)

formed the test set. Those samples were intended to be as the acquired data from the camera sensors in an actual system. Because face recognition can be iterated requiring new (and better) data, the test set has been further divided in two different subsets—namely, $T1$ and $T2$. The former contains the four worst images for every user in terms of confidence result: it consists of 160 images that are intended to be dedicated to the first face identification attempt. $T1$ is used to support the simulation of that identification process which occurs while a user is walking towards the entrance and they are not paying much attention on being recognized. The latter test subset $T2$ is made up with the remaining 120 images (the remaining three images of each user) of higher quality, and it is used for the controlled face identification (possibly more than once, up to k times). $T2$ is then used to support that identification process, which occurs while a user is aware that their first attempt is failed and they are trying to be authenticated again in a more collaborative way (like standing still and keeping their head straight).

At first, all the images related to the genuine users (all the images in $T1$) were presented to the system, activating the face identification procedure. The frequency of the occurrence for the three possible outcomes is presented in the first row of Table 1. The samples of accepted users obtained a score in the interval $[0, t_1)]$, and they represent slightly more than the half of the entire data set: from a qualitative point of view, this percentage shows the system as a quite conservative one, allowing people to go on if there is a high evidence about the truthfulness of their claimed identity. The percentage of wrongly rejected genuine users (3.13%) represents the FRR of the face recognition process under unstructured acquisition, and it becomes a lower bound estimation of the FRR of the overall system. Around 43% of the presented data got a score in the interval $[t_1, t_3]$, which is associated to unsolved checks, pushing back for further acquisitions. A similar analysis is reported in the second row of Table 1, using all the images in $T2$, which are related to further and controlled acquisition of the genuine users. Despite a small growth of the overall FRR by a 1.6%, 81.7% of the data of those subjects that were forwarded to a structured face acquisition phase were correctly classified as genuine, leaving a reasonable fraction to the subsequent iris verification.

Table 1. Face recognition acceptance rates for genuine subjects.

Input Set	Accepted Genuine Users	Rejected Genuine Users	Unsolved
$T1$, (160 images)	86 (53.75%)	5 (3.13%)	89 (43.12%)
$T2$, (120 images)	98 (81.7%)	2 (1.6%)	20 (16.7%)

Table 2 reports—for both $T1$ and $T2$—the percentage of samples which resulted in the MAYBE output value, i.e., the percentage of users that were either sent back to the face analysis (over new acquired data) or moved forward to the iris analysis. With respect $T1$, only one third of the data—which gave an unsolved check (with a score in $[t_3, t_2]$—were directly sent to the iris verification phase, while the remaining part (with a score in $[t_1, t_3]$) was solved using a more controlled face recognition procedure. Moreover, it is worth noting that data in the $T2$ set never asked for more controlled acquisitions after the first one.

A more complete assessment of the goodness of the face identification process requires further analysis of its robustness against not-enrolled subjects that try to overcome the security barriers. Picking 160 face images of male and female subjects of various racial origins from another face database (faces94 [23]), we formed a test set of potential intruders.

Table 3 reports the results of the test: as there were no accepted impostors, we can say that this first phase does not contribute to the FAR of the overall system. At the same time, there was a heavier role of the iris data because around 30% of the samples required further controls that activated the iris verification procedure, as shown in Table 4.

Table 2. Solving rates for genuine subjects, in unsolvable state.

Input Set	Forwarded to Structured Face Acquisition	Forwarded to Iris Verification
*T*1, (160 images)	46 (28.75%)	23 (14.37%)
*T*2, (120 images)	0%	20 (16.7%)

Table 3. Face recognition acceptance rates for impostor subjects.

Input Set	Accepted Impostors	Rejected Impostors	Unsolved
face94, (160 images)	0 (0%)	112 (70%)	48 (30%)

Table 4. Solving rates for impostors, in unsolvable state.

Input Set	Forwarded to Structured Face Acquisition	Forwarded to Iris Verification
face94, (160 images)	1 (0.625%)	47 (29.375%)

3.2. Iris Verification

The assessment of the iris verification procedure started from the exhaustive analysis of the impostors: over the 40 sets of five samples from UBIRIS, each set being associated to a single subject. For the iris verification phase, only two thresholds are sufficient, because the only countermeasure when the score of a comparison is in the interval $[t_1, t_2]$ asks for the repetition of the acquisition of the iris (Figure 3). The thresholds t_1 and t_2 were set to 0.35 and 0.4, respectively. Using a brute force approach, all the combinations of couples (trials) of samples from different subjects were presented to the iris verification procedure. For all the tests, the score was always above the t_2 threshold, resulting in the correct identification of an impostor. Because it appears that there is no chance of errors with in this kind of comparison, its FAR is zero (i.e., all the impostors are blocked).

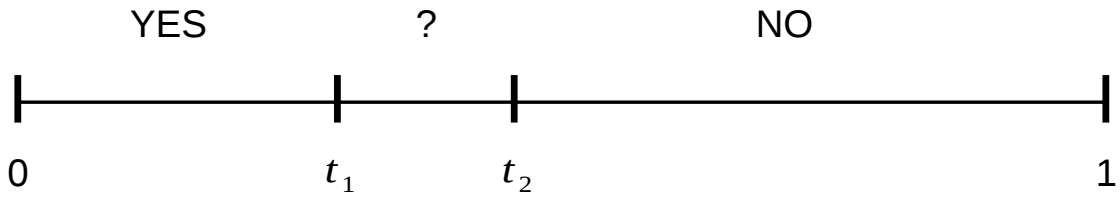

Figure 3. Iris verification thresholds.

The second step in the assessment involved the testing of all the intra-user couples of samples. Because there are 40 different users and five images for each user, there are 400 intra-user couples of samples, 10 couples for each subject. As shown in Table 5, almost three-quarters of the comparisons succeeded in finding a genuine user (the obtained score was below t_1). Moreover, only a few comparisons raised an Undecided output, mainly because the distance between t_2 and t_1 is small. In this case, the verification needs to be repeated. The 22.5% genuine user rejection rate looks quite high, but a deeper analysis of the actual iris images under test led us to the discovery that almost half of the samples showed a very bad quality, mainly because they were out of focus.

Table 5. Iris recognition acceptance rates for genuine subjects.

Input Set	Accepted Genuine Users	Rejected Genuine Users	Undecided
UBIRIS, (400 images)	290 (72.5%)	90 (22.5%)	20 (5%)

4. Discussion

This paper shows the design of an adaptive multi-modal biometric system that consolidates face identification and iris verification in a serial mode. Testing conducted so far on publicly available databases confirms the advantages of using two different kinds of biometric parameters that differ in invasivity and accuracy. In the iris verification testing, a very high percentage (about 23%) of comparisons had to be conducted again because the utilized images were not good. The code for iris verification is not capable of extracting useful information from very noisy images, as they cannot be properly segmented or encoded. A pre-processing step can be added to filter those samples that are not good enough for processing. This addition is useful in order to save time while testing, but also in the real specified context: any time a user submits to iris verification is immediately advised if their acquired image is not good enough to be segmented or encoded, so that they can repeat the process right away. To achieve an even better degree of security, the system has been provided with the possibility of modifying the iris verification phase so that a user's acquired image is set against more than one user's template images (e.g., two or three images), and the resulting decision is a combination of the single comparisons.

Future development can usefully exploit the use of more than two biometrics. Moreover, all those issues from a deployment that involves mobile devices as well as energy-aware resources need to be investigated. As a key point of the proposed system is to form a general prototypical system to be tailored in the most different contexts, further investigation is also needed in order to design proper strategies that will cope with partially conflicting behaviors, taking into account some (sub)optimal performance figures to be computed in real-time. If a loosely coupled human supervision is permitted, a scheme for the online modification of the threshold values in order to maintain the desired security levels could be coupled to the general system.

Acknowledgments: This work has been partially supported by the University of Padova Research Project CPDA157799 "Fostering Independent Living in the Aging Population through Proactive Paging and Cognitive Support".

Author Contributions: Both the two authors have equally contributed in all phases of the research that is reported in this article.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Kisku, D.R.; Gupta, P.; Sing, J.K. *Advances in Biometrics for Secure Human Authentication and Recognition*; CRC Press: Boca Raton, FL, USA, 2016.
2. Anil, K.; Ross, J.A.; Prabhakar, S. An introduction to biometric recognition. *IEEE Trans. Circuits Syst. Video Technol.* **2014**, *14*, 4–20.
3. Carpentieri, B. Implementing a secure authentication system. *Int. J. Comput.* **2017**, *2*, 47–52.
4. Dhamala, P. Multibiometric Systems. Master's Thesis, Department of Telematics, Norwegian University of Science and Technology, Trondheim, Norway, 2012.
5. Li, C.; Hu, J.; Pieprzyk, J. A new biocryptosystem-oriented security analysis framework and implementation of multibiometric cryptosystems based on decision level fusion. *IEEE Trans. Inf. Forensics Secur.* **2015**, *10*, 1193–1206, doi:10.1109/TIFS.2015.2402593.
6. Somnath, D.; Debasis, S. *Unimodal and Multimodal Biometric Data Indexing*; De Gruyter: Boston, MA, USA, 2014.
7. Crouse, D.; Han, H.; Chandra, D.; Barbello, B.; Jain, A. Continuous authentication of mobile user: Fusion of face image and inertial Measurement Unit data. In Proceedingns of the International Conference on Biometrics (ICB 2015), Phuket, Thailand, 19–22 May 2015; pp. 135–142, doi:10.1109/ICB.2015.7139043.
8. Wayman, J.; Jain, A.; Maltoni, D.; Maio, D. An introduction to biometric authentication systems. In *Biometric Systems: Technology, Design and Performance Evaluation*; Springer: London, UK, 2005; pp. 1–20.
9. AlMahafzah, H.; AlRwashdeh, M.Z. A Survey of Multibiometric Systems. *Int. J. Comput. Appl.* **2012**, *43*, 36–43.

10. Mhashe, V.D.; Patankar, A.J. Multimodal biometrics by integrating fingerpirnt and Palmprint for security. In Proceedings of the IEEE International Conference on Computational Intelligence and Computing Research, Enathi, Tamilnadu, India, 26–28 Decembre 2013; doi:10.1109/ICCIC.2013.6724125.
11. Hu, P.; Ning, H.; Qiu, T.; Song, H.; Wang, Y.; Yao, X. Security and privacy preservation scheme of face identification and resolution framework using fog computing in internet of things. *IEEE Internet Things J.* **2017**, doi:10.1109/JIOT.2017.2659783.
12. Imran, M.; Rao, A.; Kumar, H.G. A new hybrid approach for information fusion on multibiometric systems. In Proceedings of the 2011 IEEE Third National Conference in Computer Vision, Pattern Recognition, Image Processing and Graphics, Hubli, Karnataka, India, 15–17 December 2011; doi:10.1109/NCVPRIPG.2011.57.
13. Giot, R.; El-Abed, M.; Rosenberger, C. Fast computation of the performance evaluation of biometric systems: Application to multibiometrics. *Future Gener. Comput. Syst.* **2013**, *29*, 788–799, doi:10.1016/j.future.2012.02.003.
14. Donida Labati, R.; Genovese, A.; Ballester, E.M.; Piuri, V.; Scotti, F.; Sforza, G. Biometric Recognition in automated border control: A survey. *ACM Comput. Surv.* **2016**, *49*, 1–39, doi:10.1145/2933241.
15. Alling, A.; Powers, N.R.; Soyata, T. Face recognition: A tutorial on computational aspects. In *Emerging Research Surrounding Power Consumption and Performance Issues in Utility Computing*; Deka, G.C., Siddesh, G.M., Srinivasa K.G., Patnaik L.M., Eds.; IGI Global: Hershey, PA, USA, 2016.
16. Wildes, R.P. Iris Regognition, an emerging biometric technology. *Proc. IEEE* **1997**, *85*, 1348–1363.
17. Grauman, K.; Darrell, T. The pyramid match kernel: Discriminative classification with sets of image features. In Proceedings of the Tenth IEEE International Conference on Computer Vision (ICCV'05) , Beijing, China, 15–21 October 2005; Volume 2, pp. 1458–1465.
18. OpenCV Tutorials. Available online: http://docs.opencv.org/2.4/doc/tutorials/tutorials.html (accessed on 1 April 2016).
19. Verma, P.; Dubey, M.; Verma, P.; Basu, S. Daughman's algorithm method for iris recognition—A biometric approach. *Int. J. Emerg. Technol. Adv. Eng.* **2012**, *2*, 177–185.
20. Wang, Y.; Tan, T.; Jain, A.K. Combining face and iris biometrics for identity verification. In Proceedings of the 4th International Conference on Audio- and Video-based Biometric Person Authentication, Guildford, UK, 9–11 June 2003; pp. 805–813.
21. The Database of Faces. Available online: http://www.cl.cam.ac.uk/research/dtg/attarchive/base.html (accessed on 15 July 2016).
22. Hugo, P.; Alexandre, L.A. UBIRIS: A noisy iris image database. In Proceedings of the 13th International Conference on Image Analysis and Processing–ICIAP 2005, Cagliari, Italy, 6–8 September 2005; pp. 970–977.
23. Collection of Facial Images. Available online: http://cswww.essex.ac.uk/mv/allfaces/index.html (accessed on 15 July 2016).