Multimodal Biometric Authentication using Fingerprint and Iris Recognition in Identity Management

Kamer Vishi¹, Şule Yildirim Yayilgan¹
¹Faculty of Computer Science and Media Technology, Dept. of Information Security
Gjøvik University College
Gjøvik, Norway
kamer.vishi@hig.no, sule.yayilgan@hig.no

Abstract—The majority of deployed biometric systems today use information from a single biometric technology for verification or identification. Large-scale biometric systems have to address additional demands such as larger population coverage and demographic diversity, varied deployment environment, and more demanding performance requirements. Today’s single modality biometric systems are finding it difficult to meet these demands, and a solution is to integrate additional sources of information to strengthen the decision process. A multimodal biometric system combines information from multiple biometric traits, algorithms, sensors, and other components to make a recognition decision. Besides improving the accuracy, the fusion of biometrics has several advantages such as increasing population coverage, deterring spoofing activities and reducing enrolment failure. The last 5 years have seen an exponential growth in research and commercialization activities in this area, and this trend is likely to continue. Therefore, here we propose a novel multimodal biometric authentication approach fusing iris and fingerprint traits at score-level. We principally explore the fusion of iris and fingerprint biometrics and their potential application as biometric identifiers. The individual comparison scores obtained from the iris and fingerprints are combined at score-level using a three score normalization techniques (Min-Max, Z-Score, Hyperbolic Tangent) and four score fusion approaches (Minimum Score, Maximum Score Simple Sum and User Weighting). The fused-score is utilized to classify an unknown user into the genuine or impostor.

Keywords—Biometrics; Authentication; Fingerprint Recognition; Iris Recognition; Identity Management; Image Quality; Score Normalization; Score-level Fusion.

I. INTRODUCTION

In this newly complicated world of terrorism, identity theft, and rampant consumer fraud, biometrics has been heralded as a key technology for identity management, and hence security. As never before has identity management been so important. Governments and enterprises of all sizes have become much more vigilant regarding security. There is always a need to re-examine and potentially improve security, and biometrics is attracting growing interest as fraud increases and the conventional authentication methods PINs, passwords, and identity cards prove inadequate to counter the growing threats [7].

Biometric tools have become prominent differentiators for multiple applications in a variety of markets. The use of biometrics offers no panacea to completely remedy society’s threats, and it provides no guarantee against terrorist activities. However, biometric technologies remain a critically important component of the total solution. The biometric authentication market has emerged and is expanding at an increasing rate. Biometric systems are proliferating. The diversity of the various modalities and the many false claims of their promoters and detractors alike have somewhat clouded the market with at best some misinformation and at worst a public concern that this new technology is somehow menacing and will restrict freedoms. Unfortunately, many of the key benefits of biometrics have become obfuscated due to unfortunate sensationalism and myths that have surrounded biometric solutions [8].

Biometric technologies vary in capability, performance, and reliability. The success of a given biometric modality depends not only on the effectiveness of the technology and its implementation, but also on the total security solution for which any biometric system comprises only a part. The next several years will be exciting for the biometric market. We can expect increased user acceptance and demand as biometrics continue to become more user friendly and more reliable. Improved technology and biometric need are converging. There should be significant growth in each of the various biometric modalities, as well as in multimodal biometrics [9].

Because of their security, speed, efficiency, and convenience, biometric authentication systems have the potential to become the new standard for access control. Biometrics replaces or supplements knowledge and possession authentication with a person’s physical or behavioural characteristics. Biometrics can be used in any situation where identity badges, PINs/passwords, or keys are needed. Biometrics offers some clear advantages over traditional identity methods:

- Biometric traits cannot be lost, stolen, or borrowed.
- Generally, physical human characteristics are much more difficult to forge than security codes, passwords, badges, or even some encryption keys.
- Biometrics guard against user denial - the principle of nonrepudiation - by providing definitive recognition of an individual.
- Biometrics cannot be delegated or shared. Its use proves that the individual in question was present for a given transaction.
- Identity verification can eliminate the need to carry a token or remember a password, although all three can be used.
- Biometrics is the only technique available today that can determine if a person is who he denies he is or if he has pre-enrolled.

Moreover, with the greater demand on biometrics in everyday life, governments are expected to enact statutes that help administer biometric solutions while maintaining privacy and legal support. Indeed, it has been the use of biometric solutions by government agencies and by mainstream industries such as banking and health care that has increased public awareness and acceptance of the technology.

A. Components of Biometric Systems

Components of biometric systems may vary from system to system, however, a generalized biometric system is a functional combination of five main following components or subsystems as shown in Figure 1: (1) sensor/data capture (acquisition), (2) signal processing, (3) data storage (also called template storage), (4) comparison (matching) algorithm, (5) decision making.

![Figure 1. Components of Biometric System and Process Flow Diagram.](Image)

1) Data Acquisition: This subsystem is responsible to capture the sample of biometric characteristic (e.g. image or signal) from individual. This biometric sample is an uncompressed data and it is called raw biometric data and is captured by so called sensor [5]. This component is the only point where interaction between user and biometric system takes place and this process is also referred as biometric presentation [15].

2) Signal Processing: This subsystem is responsible to extract the features from biometric sample in order to generate digital representation called biometric template or reference which represent the uniqueness of the sample as well as be somewhat invariant related to multiple samples created from the same individual over the time [22, 23]. The signal processing process includes sample enhancement, quality assessment (segmentation), and feature extraction. The output of quality control checks (segmentation and feature extraction) is a quality score, reflecting the quality of the sample by how successful was the feature extraction algorithm [5].

3) Data Storage: This subsystem stores the biometric template, this template that is housed for future processes is also called reference in the biometrics domain [17]. Those templates are generated and stored during the enrolment process into enrolment database.

4) Comparison (Matching) Algorithm: On this subsystem depending on the application, each new created sample template is then compared with one or more reference templates by comparison algorithm. The result of the comparison algorithm is a comparison score or similarity (dissimilarity) score, indicating how similar the templates are [5]. The comparison score is then transferred to a decision making module.

5) Decision Policy: This subsystem uses score as input from the comparison component to compare with verification or identification attempts threshold. The threshold is a predefined value, normally chosen by biometric system administrator. If the score resulting from comparator (template comparison) exceeds the threshold the compared templates are match, if the score falls below the threshold value the compared templates are not-match [15]. According to [16] the threshold plays an important role in security of systems: "Systems can be either highly secure or not secure at all, depending on their threshold settings."

B. Fingerprint and Iris Recognition

In this paper, we use two biometric traits namely fingerprint and iris. To the best of our knowledge, there is no published research on this field that fused fingerprint and iris recognition at score-level, particularly normalization by minmax, z-score and hyperbolic tangent, and fusion of scores by combination approaches such as minimum score, maximum score, simple sum and user weighting. There are many researches that have fused fingerprint and iris at feature-extraction (template) level, in particular application of multimodal biometrics in cryptography [10] [11] [12] [13].

The main motivation behind this choice of fingerprint and iris characteristics for a multi-biometric authentication system is that fingerprint is the oldest and most widely adopted biometric technology and, as a result, is the most mature of all biometric technologies [1], iris recognition is proved that it is most accurate and hygienic biometric technology among others, this is reported in Biometric Product Testing Final Report [14].

As the core of our work revolves around examining whether the performance of a biometric-based authentication system can be improved through integrating complementary biometric features which comes primarily from two different
and independent modalities. Therefore, the main aim of this paper will be to investigate the effectiveness of the suggested fusion techniques for multimodal biometrics, with the following specific objectives:

- Explore existing multimodal approaches
- Evaluate fingerprint-based authentication performance.
- Evaluate iris-based authentication performance.
- Evaluate multimodal score-level fusion approach.
- Study the effectiveness of fusion of fingerprint and iris biometrics into the various comparison score fusion approaches in both unimodal and multimodal biometrics thorough experimental investigation.

We propose a new multi-modal biometric authentication approach using iris and fingerprint images as biometric traits. We fuse these two modalities at score-level by fusing different comparison scores from fingerprint and iris traits into a single score by combination approach. Since comparison scores that are generated from these uncorrelated and independent modalities are not homogeneous, score normalization step is essential to transform comparison scores into a common scale before fusing them. The individual comparison scores obtained from the iris and fingerprints are combined at score-level using three normalization methods (Min-Max, Z-Score, Hyperbolic Tangent) and four fusion approaches (Minimum Score, Maximum Score Simple Sum and User Weighting). The fused-score is utilized to classify an unknown user into the genuine or impostor. We demonstrate that fusion based at score-level achieves high performance on different multimodal biometric databases involving fingerprint and iris modalities. In addition, we have analyzed the properties (performance, robustness and efficiency) of score normalization and fusion methods. Furthermore, we have analyzed the quality of fingerprint and iris databases. Finally, we show that fusion of uncorrelated modalities such as fingerprint and iris achieves better accuracy and security compared to unimodal biometric systems.

II. FUSION OF MULTIMODAL BIOMETRICS

To the best of our knowledge, fusion of fingerprint and iris at score level is not treated or better saying less studied. Fusion of these two modalities is studied at feature-extraction level in earlier work.

A. Score Level Fusion of Fingerprint and Iris: Normalization and Fusion Methods

In biometric systems there are several types of fusion levels such as: sensor (sample) level, feature (template) level, score level or decision level. Many researches and industrial statistics have shown that comparison score level fusion is more accurate and effective than others [9]. The score level fusion has two main steps. The first step of fusion at this level is called "score normalization", which means that calculated comparison scores by certain comparator (algorithm) $S_i$ are mapped onto a new score scale or domain $S'_i$. For instance, if comparator X produces scores on a domain of [1; 100] and comparator Y generates scores on a domain of [1; 2500], in these cases score normalization is required to map them to a common domain.

The Score Normalization process is research area onto itself [18], even though in this section are described fundamental points [9] [2]. This process is performed to change the comparator’s parameters and data types to map comparison scores to a common scale (domain). Commonly, score normalization techniques are evaluated on the bases of robustness and efficiency. The most used score normalization techniques that are employed in this work are: Min-Max (MM), Z-Score (ZS), and Hyperbolic Tangent (TanH).

The second step of fusion at score level is fusion itself. In general, score fusion techniques fall into two categories: classification and combination approaches. Classification approaches formulates the problem as dividing the decision space into two classes: genuine and impostor. The reliability and effectiveness of this method is dependent on the large amount and quality of input data that are available to train the classifier and this is one of the disadvantages of this approach. Although, comparison scores need not to be homogeneous and hence normalization step here is not required. Some of the classification methods that have been researched are: neural network, nearest neighbourhood algorithms and tree-based classifiers.

Combination approach is most common and effective method for comparison score fusion. This method combines comparison scores from multiple comparators and generates single comparison score. It is obvious that this technique requires score normalization in advance to fuse the comparison scores. The most used score level combination fusion techniques that are used in this work are: minimum score, maximum score, simple sum and user weighting.

III. EXPERIMENTS

A. Databases

Fingerprint and Iris experiments in this work are made over four different databases (DB) collected from two different institutions.

1) Fingerprint databases and an iris database are collected by Machine Learning and Applications (MLA) Group
at Shandong University in China (SDUMLA-HMT) [3].

2) Another iris database is collected by Institute of Automation, Chinese Academy of Sciences (CASIA-Iris-Lamp) [4].

The fingerprint images on SDUMLA-HMT database [3] are collected with five different sensors (multi-sensor database). Fingerprint images in SDUMLA-HMT database are acquired from six fingers such as: thumb finger, index finger and middle finger, of both hands. It is worth mentioning that MLA Group has requested from participants eight impressions (attempts) for each of six fingers to five previous mentioned sensors. Some of fingerprint images are shown in Figure 3. Fingerprint database (DB) consist of: (fingers)x5(sensors)x8(attempts)x106(subjects) = 25,440 fingerprint images.

We consider all images from each sensor as a database (DB) and we have checked the quality of images from five different sensors (for each of these databases). We have selected the best quality and the worst quality databases among these which are DB2 from FPR620 sensor and DB3 from FT-2BU sensor.

![Fingerprint images](image)

Figure 3. Fingerprint image samples from a) DB2 (best db) and b) DB3 (worst db).

It is to be noted that we have reduced the number of participants, fingers and impressions as following: 2 fingers, in particular index fingers of both hands from 100 participants out of 106, and from 8 impressions we have used only first 5 impressions for finger in order to correlate fusion with 2 irides and 5 iris attempts (1000 iris images). After this modification we do have: 2(fingers)x100(subjects)x5(attempts) = 1000 images per database in total 2000 fingerprint images from two databases (DB2 and DB3) out of 25,440 fingerprint images.

In our fingerprint experiment we have assigned DB2 as FP-DB1 (for best quality database) and DB3 as FP-DB2 (for worst quality database). MLA Group did not follow finger coding from ISO 19794-2 [6]. We have converted the existing finger codes according to ISO 19794-2 (Figure 4) for two fingerprint databases, namely DB2 and DB3.

![Finger position codes](image)

Figure 4. Finger position codes (names) according to ISO 19794-2 [6].

An illustration of finger position codes (names): to the right side MLA Group and to the left side ISO 19794-2.

In our fingerprint experiment we have assigned DB2 as FP-DB1 (for best quality database) and DB3 as FP-DB2 (for worst quality database). MLA Group did not follow finger coding from ISO 19794-2 [6]. We have converted the existing finger codes according to ISO 19794-2 (Figure 4) for two fingerprint databases, namely DB2 and DB3.

An illustration of finger position codes (names) from MLA Group and ISO is given in figure 5 respectively.

Iris experiments in this work are conducted on two different databases (DB) collected from different institutions.

1) First iris database (named as Iris-DB1) is collected by Institute of Automation, Chinese Academy of Sciences (CASIA-Iris-Lamp) [4].

2) Second iris database (named as Iris-DB2) collected by Machine Learning and Applications (MLA) Group at Shandong University in China (SDUMLA-HMT Iris) [3].

In our iris experiments we have reduce the number of participants (images) in order to perform fusion with fingerprint databases.

- From SDUMLA-HMT iris database we have chosen only 100 subjects out of 106 in total 1000 iris images: 2(irises)x5(irisimages)x100(subjects) = 1000 iris images
- From CASIA-Iris-Lamp we have used also only 100 subjects out of 411 and it is to be noted that we have reduced the number of attempts from 20 to 5, in order to comply with 1000 images in total: 2(irises)x5(irisimages)x100(subjects) = 1000 iris images

**B. Fusion Experiments**

Fusion is performed over four previously mentioned databases. Based on quality assessment results that we have conducted over databases, the best databases are named with suffix 1, while the worst databases are named with suffix 2 such as:

1) **Fingerprint Databases:**

   - Fingerprint best quality database SDUMLA-HMT DB2 is named as FP-DB1,
• Fingerprint worst quality database SDUMLA-HMT DB3 is named as FP-DB2.

2) Iris Databases:
• Iris best quality database CASIA-Iris-Lamp is named as Iris-DB1,
• Iris worst quality database SDUMLA-HMT iris database is named as Iris-DB2.

We have defined four fusion scenarios, fusion with the best and the worst databases as following:
1) Fusion of FP-DB1 and Iris-DB1
2) Fusion of FP-DB1 and Iris-DB2
3) Fusion of FP-DB2 and Iris-DB1
4) Fusion of FP-DB2 and Iris-DB2

As we have mentioned earlier, fusion in this work is performed at score level. First we have normalized all scores by three normalization techniques such as MinMax, Z-Score and Tangent Hyperbolic. After normalization, fusion stage is performed by four most used fusion techniques such as Minimum score, Maximum Score, Simple sum and User weighted sum.

3) Real vs. Virtual Users: For fusion scenarios 1 and 3 we have used heterogeneous databases for fingerprint and iris, thus we have created so called "virtual users", while for fusion scenarios 2 and 4 we have used modalities (fingerprint and iris) from homogeneous databases or "real users" [19], methodology of real and virtual users is illustrated in figure 6. A "real user" denoted as A subject has provided both required modalities to the database, iris and fingerprint, this case is for SDUMLA-HMT database (same subjects for both iris and fingerprint). While a participant B, donated with only one biometric modality, either iris data (BI) or fingerprint data (BF), therefore these modalities are combined from different users in order to create another user [19]. In this case we have combined iris modality from CASIA-Iris-Lamp and fingerprint modality from SDUMLA-HMT fingerprint database, and thus we have created so called a "virtual user".

IV. EXPERIMENTAL RESULTS
A. Comparison of Fingerprint Databases

At first we will be looking at the results when comparing two fingerprint databases collected by two different sensors. Figure 7 illustrates that the fingerprint SDUMLA-HMT database (FP-DB1) is performing best and the other fingerprint SDUMLA-HMT database (FP-DB2) worst. This is due to bad quality of images that are in (FP-DB2). EER is the Equal Error Rate.

B. Comparison of Iris Databases

Secondly, we will be looking at the results when comparing two iris databases collected by two different sensors. Figure 8 illustrates that the CASIA-Iris-Lamp iris database (Iris-DB1) is performing best and SDUMLA-HMT iris database (Iris-DB2) worst. This is due to bad quality of images that are in (Iris-DB2).

C. Fingerprint and Iris Fusion Results

In Figure 9 is given a summary of comparison between fingerprint and iris databases. In this case another DET (Decision Error Trade-off)-curve (orange color) is for SDUMLA-HMT iris database (Iris-DB2) that we have carried out some image enhancement, we have enhanced the contrast of iris images to 30 % and we have received EER=3.30 % lower than before (EEE=7.35 %), to prove that quality of images is the key factor in biometric systems.

In the previous sections we saw the results from the fingerprint and iris in a separate manner. We retrieved both low and high EERs and in such cases when having unimodal biometric, then it is often affected by several practical problems like noisy sensor data, unacceptable error rates, spoof attacks etc. Multi-modal biometrics overcomes some of these problems.
Biometric fusion can be performed in different levels:

1) Sensor level
2) Feature extraction level
3) Score level
4) Decision level

As we have mentioned in previous section, in this paper we conduct fusion at the score-level because it is the most popular and suitable way. Score-level fusion requires normalization of the fingerprint and iris scores as an initial step. We have applied several normalization techniques such as Min-Max, Z-score, and Tanh. Afterwards, we used four fusion methods which are Simple Sum, Maximum score, Minimum score and User Weighted sum. All these normalization and fusion techniques are very known in multi-modal biometrics [20] [21].

D. Comparison of Uni-modal and Multi-modal Biometrics

In Figures [10] [11] [12] and [13] respectively, we are going to show only one graph for normalization and fusion method per fusion scenario, instead of 3 (normalization methods) x 4 (fusion methods) x 4 (scenarios) = 48 DET graphs in total for fusion scenarios.

1) [1st scenario:] Fusion of FP_DB1 and Iris_DB1:
Figure 10 shows fusion performance of iris database Iris_DB1 and fingerprint database FP_DB1 using Hyperbolic Tangent estimators (TanH) normalization and Simple Sum rule fusion. As can been seen from the figure, EER of fingerprint, iris and fingerprint + iris are 0.86 %, 0.71 % and 0.00010 %, respectively.

2) [2nd scenario:] Fusion of FP_DB1 and Iris_DB2:
Figure 11 shows fusion performance of fingerprint database FP_DB1 and iris database Iris_DB2 using Hyperbolic Tangent estimators (TanH) normalization and Maximum Score rule fusion. As can been seen from the figure, EER of fingerprint, iris and fingerprint + iris are 0.86 %, 0.71 % and 0.0320 %, respectively.

3) [3rd scenario:] Fusion of FP_DB2 and Iris_DB1:
Figure 12 shows fusion performance of fingerprint database FP_DB2 and iris database Iris_DB1 using MinMax normalization and Maximum Score rule fusion. As can been seen from the figure, EER of fingerprint, iris and fingerprint + iris are 1.01 %, 0.71 % and 0.00015 %, respectively.

4) [4th scenario:] Fusion of FP_DB2 and Iris_DB2:
Figure 13 shows fusion performance of fingerprint database FP_DB2 and iris database Iris_DB2 using Hyperbolic Tangent estimators (TanH) normalization and Maximum Score rule fusion. As can been seen from the figure, EER of fingerprint, iris and fingerprint + iris are 1.01 %, 7.35 % and 0.0038 %, respectively.
Figure 11. Scenario 2: Multi-modal Performance of Iris and Fingerprint using TanH Score Normalization + Maximum Score rule Fusion. $EER_{FP_{DB1}} = 0.86\%$, $EER_{Iris_{DB2}} = 7.35\%$, $EER_{Finger+Iris} = 0.0320\%$.

Figure 13. Scenario 4: Multi-modal Performance of Iris and Fingerprint using TanH Score Normalization + Simple Sum Score Fusion. $EER_{FP_{DB2}} = 1.01\%$, $EER_{Iris_{DB2}} = 7.35\%$, $EER_{Finger+Iris} = 0.0038\%$.

V. CONCLUSION

Fingerprint-based recognition resulted in different performances of using two different databases (FP-DB1 and FP-DB2) collected by two different sensors: FPR620 optical fingerprint sensor and FT-2BU capacitive fingerprint sensor both developed by ZhongZheng Inc., respectively. The general performance for best quality of fingerprint images (FP-DB1) resulted in EER = 0.86 %, while the general performance for worst quality of fingerprint images (FP-DB2) resulted in EER = 1.01 %, the difference of performance of these two fingerprint databases in percentage of 0.15 % is due to quality of captured images. Therefore, we conclude that FT-2BU capacitive fingerprint sensor generates worse images than FPR620 optical fingerprint sensor.

Iris-based recognition resulted in different performances of using two different databases (Iris-DB1 and Iris-DB2) collected by two different sensors: OKI sensor and SDUMLA-HMT sensor, respectively. From the best quality of iris database (CASIA-Iris-Lamp or Iris-DB1) we have achieved the performance of EER = 0.71 %, whereas the performance of the worst quality iris database (SDUMLA-HMT iris database) resulted in an EER = 7.35 %, the difference of performance of these two iris databases in percentage of 6.64 % is due to quality of captured iris image and failure of VeriEye software to correctly segment the iris.

After we completed the iris experiment and achieved such distinction performances we have conducted iris image processing on SDUMLA-HMT iris database, particularly we have enhanced the contrast of iris images about 30 %. We have repeated again the iris comparison process for SDUMLA-HMT iris database (Iris-DB2) and we achieved higher results than in first case and the EER = 3.30 % while without image processing EER was 7.35 %. As one can see we only by contrast enhancement we have increased the biometric performance about 55 % than before.

Furthermore, experimental results show that in most cases fused performance (fingerprint + iris) was significantly improved compared to unimodal biometric performances fingerprint and iris, respectively. It is to be noted that the best fusion performance is fusion by hyperbolic tangent estimators score normalization technique and simple sum rule fusion: $EER_{Finger+Iris} = 0.00010\%$.

REFERENCES


