Правительство Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
Высшего профессионального образования
Санкт-Петербургский государственный университет

Математическое обеспечение и администрирование информационных систем
Информационно-аналитические системы

Шайхетдинова Алиса

Аутентификация по рисунку вен руки в мультимодальных биометрических системах

Выпускная квалификационная работа

Научный руководитель:
Доцент, к.ф.-м.н. Михайлова Елена Георгиевна

Рецензент:
RNDr. Игорь Чермак, CSc

Санкт-Петербург

2017

Saint-Petersburg State University

Software and Administration of Information Systems
Analytical Information Systems

Shaykhetdinova Alisa

Finger-based Multimodal Biometric Recognition

Graduation project

Scientific supervisor:
Assoc. Prof. Mikhailova Elena Georgievna

Reviewer:
RNDr. Igor Čermák, CSc

Saint-Petersburg

2017

Contents

Abstract — Most biometric systems from real world applications use a single source of biometric modality which is known as unimodal biometrics. Multimodal biometric recognition requires several biometric features for recognition of a person to eliminate some drawbacks of unimodal biometrics and, thereby, raise the level of security. The physiological biometrics such as fingerprint (which is now the most popular trait for recognition) and the pattern of blood veins of human's body (which cannot be easily faked or cracked) in conjunction can produce high performance biometric system. In this paper a novel approach for biometric authentication is suggested which employs these two traits: fingerprint and finger vein. Proposed method uses both the Minutiae Extraction to extract features from the images of fingerprints and the Scale-Invariant Feature Transform for images of finger vein. The extracted features in the form of coefficients are stored in the databases. Then the matching is done between the coefficients of the input test images and the features stored in the databases using distance measure and finally the fusion is carried out. This approach was tested on standard databases of fingerprint and finger vein images. The proposed method provides a maximum accuracy of 97%, with a reduction in false rejection rate.

Keywords: fingerprint; finger vein; fusion; scale-invariant feature transform; minutiae extraction; multimodal biometric recognition

I. Introduction

A reliable identity system is a critical component in applications that grant services to only enrolled users. Sharing networked computer resources, providing access to private facilities, boarding a flight or performing remote financial transactions are examples of such applications. Biometrics offers a solution for this problem by employing fully- or semi- automated schemes for recognition. Biometrics enables to establish an identity based on who you are, rather than by what you possess, such as an ID card, or what you remember, such as a password. Nowadays,

biometric recognition is a familiar and secure way to authenticate the identity of a person utilizing human characteristics or behavior. Since many various characteristics are unique to an individual, biometrics provides a more reliable system of authentication than ID cards (which can be stolen) or passwords (which can be forgotten).

II. Operation of a biometric system

A biometric system is a recognition system that acquires biometric data from an individual, extracts key features from the data, compares this feature vector with the set of features stored in the main database, and executes an action based on the result of the comparison. A conventional biometric system has three main parts: a sensor level; a quality assessment and feature extraction level and a matching level. Each of these levels is briefly described below.

1. **Sensor level:**

   A corresponding biometric reader or scanner is needed to acquire the raw biometric data of a person. The sensor module is pivotal to the efficiency of entire biometric system, because it defines the human machine interface. A badly designed interface can cause low user acceptability, due to a high failure-to-acquire rate. The quality of the raw data is also impacted by the characteristics of the camera technology which is used for biometric modalities that are acquired as images. (In case of this work sensor level was not considered. Biometric data was loaded as high quality images from opened databases.)

2. **Quality assessment and feature extraction level:**

   The assessment of image's quality is a next step after acquiring the raw data. System determines suitability of data for further processing. If data is suitable then the set of salient distinctive features is extracted to represent

the modality. During enrollment, this feature sets are stored in the database as templates for further matching phase.

It is possible to generate template from a single biometric sample, or by processing several samples. It is more efficient to store multiple templates in order to avoid intra-class variations.

3. **Matching and decision-making level:**

   The extracted features are compared against the stored templates to generate match scores. The matcher module also includes a decision making module. There the match scores are used to either validate a claimed identity (verification) or provide a ranking of the enrolled users in order to identify an individual (identification).

III. Performance of a biometric system

Unlike recognition systems, based on passwords, where it is necessary to have a perfect match between two strings in order to claim the identity, a biometric system rarely has two same feature sets extracted from one user's trait. The reasons of that variation are imperfect sensing conditions (e.g., noisy fingerprint due to sensor failure), changes in ambient conditions (e.g., level of illumination) and difference in the user's interaction with the sensor (e.g., partial fingerprints). Thus, the distance between two feature vectors generated from the same biometric trait of a user is usually not zero. The variability in the biometric feature set of an individual is referred to as intra-class variation, and the variability between feature sets originating from two different individuals is known as inter-class variation. An applicable feature set has small intra-class and large inter-class variations.

Detailed description of the evaluation metrics employed in this work can be found in Section XII (Experimental results).

IV. Multibiometric system

Multibiometrics reduces drawbacks and alleviates some of the unibiometric systems' limitations by uniting the evidence presented by multiple modalities. Multibiometric systems offer several advantages over traditional unibiometric systems. Some of these advantages are listed below.

1. Multibiometric systems can significantly improve the matching accuracy of a biometric system depending upon the information being united and the fusion methodology adopted.

2. The problem of fake biometric attack is also exists. It is possible to address this trait by appending hardware and software mechanisms for vitality detection into the biometric recognition system (fingerprint devices can incorporate vitality detection by measuring, for example, thermal properties of the human skin or other biomedical characteristics.)
   Another solution is multimodal-biometric system. It becomes increasingly difficult (almost impossible) for an impostor to spoof multiple biometric traits of a legitimately enrolled user.

3. Multibiometrics also addresses the problem of noise in acquired data. If the biometric data from one trait is noisy, the availability of other (less noisy) traits may assist to determine the identity.

Thus, a properly designed multibiometric system can improve matching accuracy, increase population coverage and deter spoofing activities.

V. Issues in designing multibiometric system

Some of the factors that impact the design and structure of multibiometric system considered in this paper are described below:

1. **Determining sources of biometric information:**

   The multimodal biometric system considered in this work is implemented combining the evidence presented by fingerprint and finger vein.

   A *fingerprint* is consist of ridges and valleys on the surface of a fingertip. Humans have used fingerprints for personal identification for many years. The matching accuracy for this modality has been shown to be very high, cost – very low.

   The field of *vein pattern* technology uses the subcutaneous vascular network of the finger to verify the identity. This feature is a highly distinctive and does not depend on the skin condition.

   We can make sure that combination of chosen traits is good by comparing (Table 5.1) performance of considered techniques using following seven categories:

   - Universality – how commonly people have this biometric characteristic.
   - Uniqueness – how well this biometric characteristic distinguishes one person from another.
   - Permanence – how well this biometric characteristic resists aging.
   - Collectability – how easy it is to acquire this biometric characteristic.
   - Performance – how accurate, fast, and robust the system which utilize this biometric characteristic
   - Acceptability – how public approves it in everyday life.
   - Circumvention – how easy it is to fool the system.

Biometric Trait	Fingerprint	Finger vein	Fingerprint + Finger Vein
Universality	M	H	H
Distinctiveness	H	M	H
Permanence	H	M	H
Collectability	M	H	H
Performance	H	H	H
Acceptability	M	H	H
Circumvention	L	L	L

Table 5.1 – Comparison of performance of different techniques (H - high, M - medium, L - low)

2. **Cost benefits:**

   The modalities used in the proposed approach are selected for increasing accuracy without extra costs for several sensors and the raise of time to acquire the biometric data: fetching both biometrics theoretically can be made by *one sensor* simultaneously.

3. **Acquisition and processing sequence:**

   Usually the evidence is gathered sequentially (Figure 5.1), but in case of chosen modalities it would be possible and convenient to *gather it simultaneously* (Figure 5.2) using the same unit (fingerprint sensor combined with infrared camera for vein-based trait).

   The information acquired can be *processed in parallel mode* too. This approach cause higher accuracy and lower error rates, due to utilizing more evidence about the user.

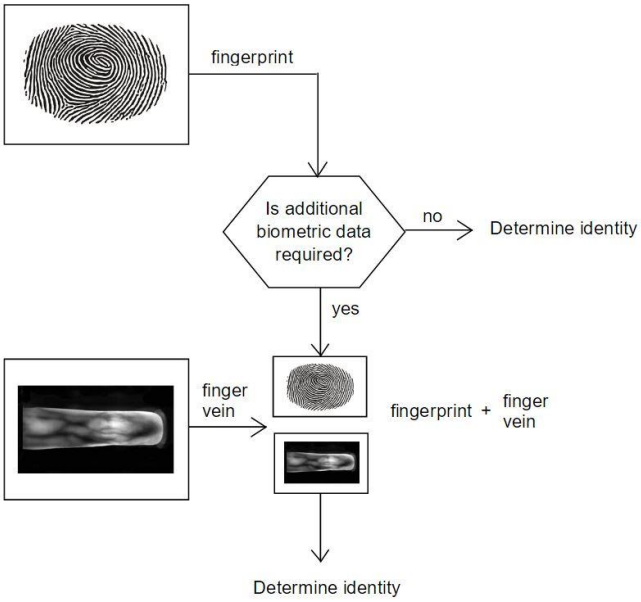


Figure 5.1 - Sequential recognition. It is more convinient for user because a decision can be made without acquiring all the biometric traits and, thus, it reduces the average processing time.

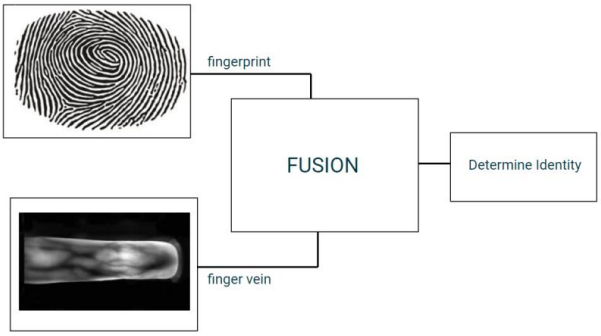


Figure 5.2 - Parallel mode of operation.

4. Type of information:

In the context of a biometric system the various levels of fusion are possible: sensor level, feature level, match score level, decision level. In the proposed method *fusion* is implemented *at the match score level*. It is relatively easy to access and combine the scores generated by the different matchers. Information fusion at the match score level is the most commonly used approach in multibiometric systems.

5. **Fusion methodology:**

Score level fusion techniques can be divided into three categories: transformation-based, classifier-based and density-based. It this paper *transformation-based score level fusion* is implemented.

Scores of the individual matchers must be comparable. Hence, it is necessary to transform the match scores into a common domain by applying normalization.

There are several *normalization techniques* (*min-max, z-score, MAD*), which are implemented and compared. Then the sum, max and min classifier combination rules applied to get the fused match scores from the normalized match scores.

The full block diagram of the proposed technique is represented on Figure 5.3.

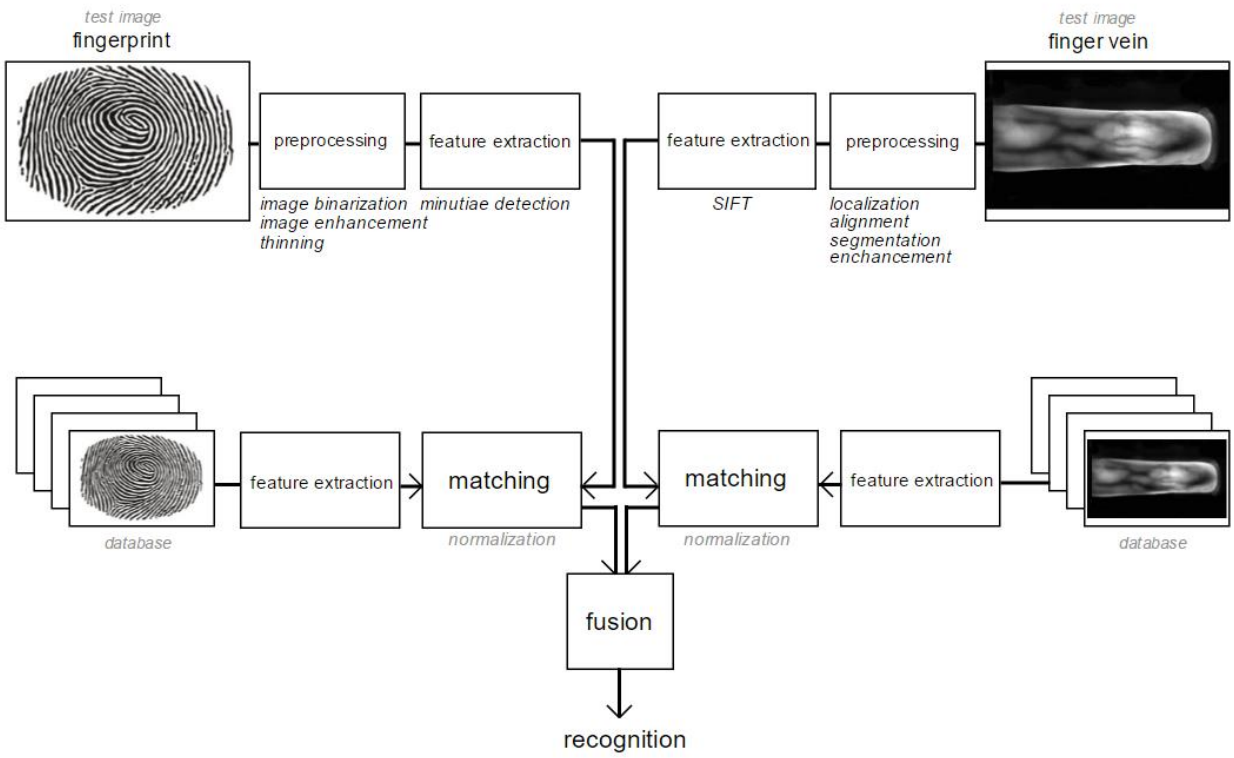


Figure 5.3 - Flow of information in a match score level fusion scheme

VI. Related Works.

The concept of fusion has been studied under several different terminologies including: stacked generalizations [11], classifier ensembles [12], hybrid methods [13], cooperative agents [14], dynamic classifier selection [15] and opinion pool [16]. Feature level fusion of multi-biometrics was presented in [17]. Weighted Summation Fusion method is used there to combine unimodal features, extracted using LBP, PCA and PNN. [18] presents a decision level fusion scheme for palmprint and hand vein biometrics using an evolutionary technique such as Ant Colony Optimization (ACO) to compute the fusion parameters by selecting them dynamically. Hybrid fusion for biometrics was discussed in [19]. It adaptively tunes itself between the two levels of fusion (score level and decision level), and improves the final performance over the original two levels. Another hybrid fusion is presented in [20]. This strategy combines three classifiers based on feature and score level fusion using a decision level fusion rule.

The detailed survey of uni- and multi- modal biometric systems was done in [5] and the drawbacks of using only one modality in the recognition system was presented. The positive impact of the fusion such biometrics as fingerprint and face was discussed in [6].

A multimodal biometric recognition based on hand images was discussed in [3] **.** The Shearlet transform and Scale-invariant feature transform were used for extraction features from finger vein and palm vein images. Finally, fusion on the matching results from those biometrics was performed on the score level. In [4], a multimodal biometric system utilized iris and facial images was considered. Contourlet transform and two dimensional principal component analyses were used there to extract the iris features and the facial features respectively, and a new fusion feature vector was formed by the combination of the iris and facial features.

Recently, biometric recognition based on veins has achieved more attention from researches. A review on vein biometric recognition using geometric pattern matching techniques was presented in [7]. A well defined classification has also been provided for vein pattern extraction strategies. Palm vein recognition has been deliberated in [8], based on the implementation of Local Derivative Pattern (LDP) as feature extraction algorithm and Histogram Intersection matching algorithm in a palm vein-based biometric identification system. In [9], Palm-dorsal vein recognition method, based on histogram of local Gabor phase XOR Pattern (HLGPXP) has been suggested.

From these examples, it is clear that the biometrics based on veins ensures improved security and it cannot be easily spoofed or falsified. Hence, in our proposed system, we have used finger vein biometrics in addition to traditional fingerprint biometric.

VII. Main part

Used programs and databases

Experiments have been conducted on following different databases:

- Finger Vein Database
- Multi-Sensor Fingerprint Database

from a public-domain database (SDUMLA-HMT), which has several pictures for each finger. These image sets have been used in several studies of multimodal biometrics, such as [10]. In order to produce the system, considered in this paper, fingerprint scores of one person and finger vein scores of another person were merged as final score vector for «virtual user».

To simulate work of the system:

1. Fingerprint and finger vein images (except one sample, which is used for test-phase) for every «virtual user» were preprocessed and features were extracted.
2. The templates were loaded in the databases (for fingerprints and vein pattern separately) - Enrollment.
3. Chosen test images were preprocessed, features were extracted (for both modalities) and compared to templates in the databases. Then two vectors of matching scores for each template were created, normalized and fused. Scores of fused vector higher then threshold indicated enrolled users, which looked like the test sample the most. Using this action FAR and FRR rates were evaluated.

MATLAB code is utilized here for the biometric system simulation, excluding acquisition and quality assessment phases, including feature extraction, template matching and decision phases.

Overview of the algorithms deployed in the proposed method.

Preprocessing.

The captured finger image may contain various noises, thus cause poor matching result. The preprocessing should have place.

For fingerprint:

- Enhancement

  The performance of applied algorithm relies on the quality of the input fingerprint images. In our case, the quality of the image is good, and we do not need to enhance our image.
- Binarization

  Convert the gray scale image in binary image. After this filter, ridges in the fingerprint are colored with black, furrows with white.

- Thining

  Eliminate the redundant pixels of ridges till they are just one pixel wide.

For finger vein pattern:

- Enhancement
- Histogram equalization (Figure 7.1)

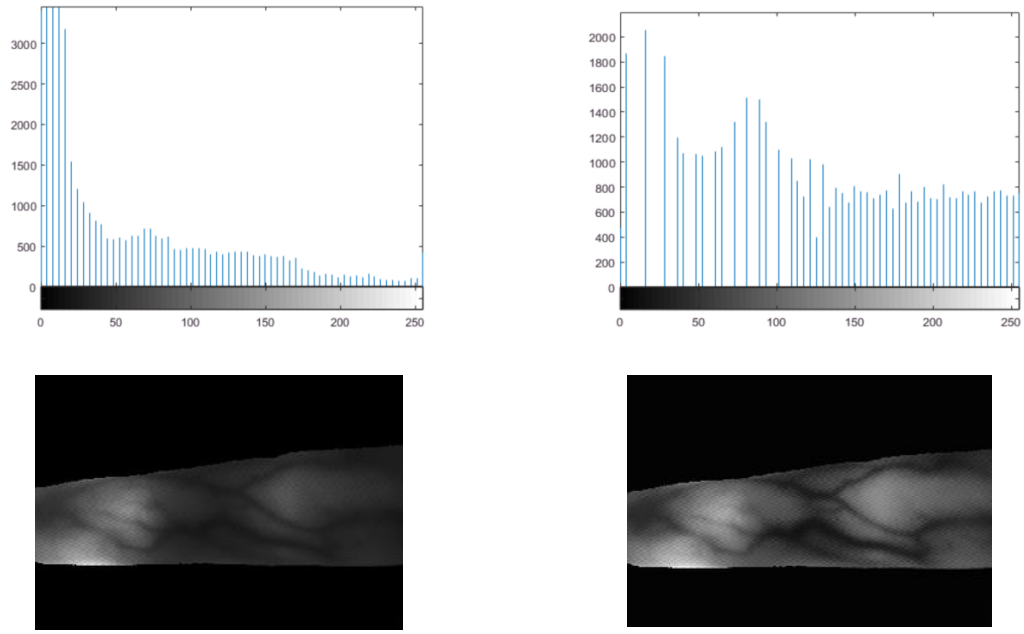


Figure 7.1 – Initial picture (left) and picture after histogram equalization (right)

- ROI localization

  Captured image contains not only the finger vein region but also some uninformative parts. ROI extraction is used in order to localize the finger region and to isolate the shade. Special masks are used to isolate the boundary and localize the effective finger region (Figure 7.2 (d)). ROI localization is usually consists of finger region segmentation, image orientation correction, and ROI detection.

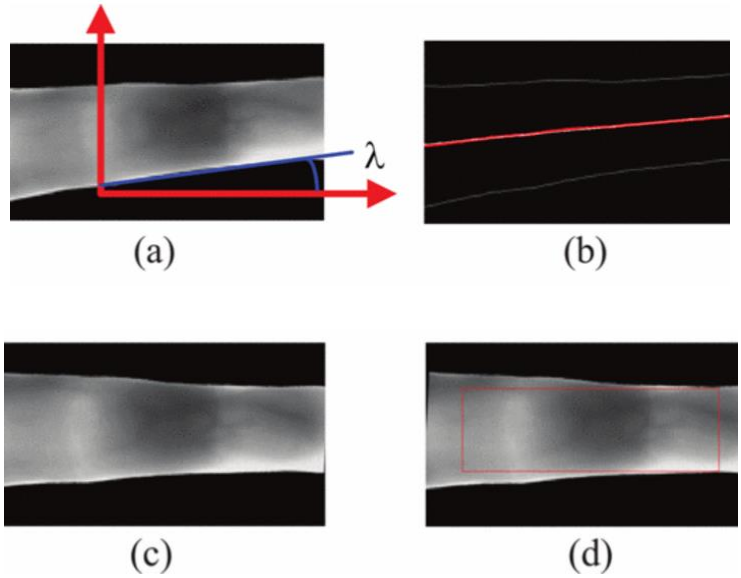
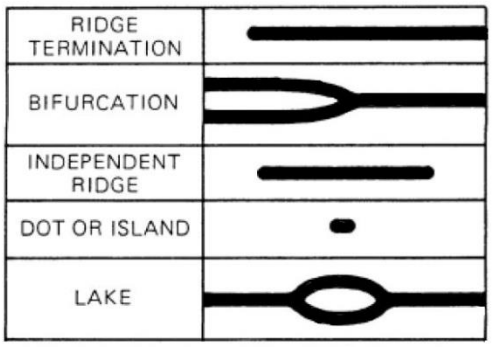


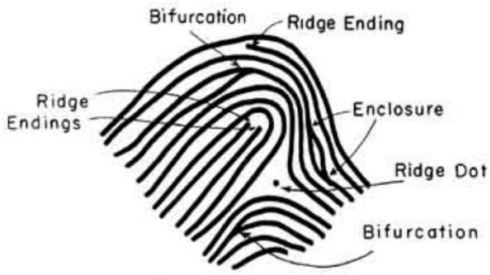
Figure 7.2 – ROI localization

Feature extraction.

For fingerprint: Minutiae extraction.

The set of minutiae points is considered to be the most distinctive feature for fingerprint representation and is widely used in fingerprint matching.





Typically, a ridge pixel is given a value of «1», while a background (furrow) pixel is - «0». From the binary thinned image the minutiae are detected by using 3x3 pattern masks. In Matlab we use filter "minutie". "Minutie" computes the number of one-value of each 3x3 window:

- if the central pixel is 1 and has only 1 one-value neighbor, then it is a termination.
- if the central pixel is 1 and has 3 one-value neighbor, then it is a bifurcation. (see Figure 7.3)

0	1	0
0	1	0
1	0	1

0	0	0
0	1	0
0	0	1

Figure 7.3 – bifurcation (left image) and termination (right image)

- if the central pixel is 1 and has 2 one-value neighbor, then it is a usual pixel.

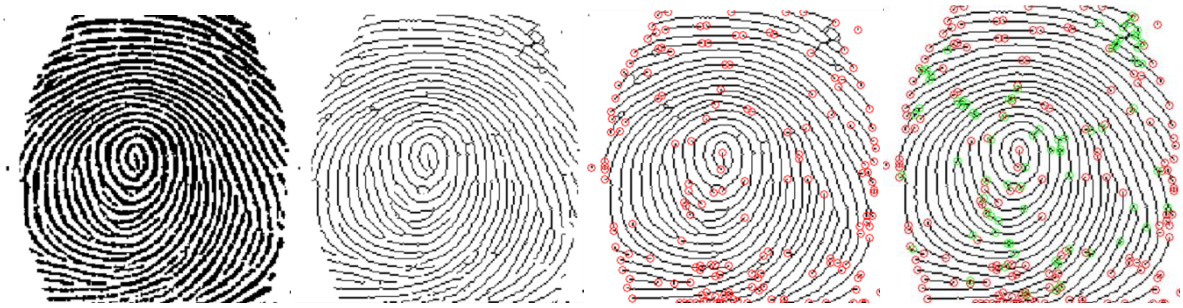


Figure 7.4 – Termination (red) and bifurcation (green) minutiae in a sample preprocessed fingerprint image

For finger vein pattern:

Scale-invariant feature transform (SIFT) algorithm [4] shows its tolerance to scale, rotation, and view-point variations in the image processing.

Detector
1. Find Scale-Space Extrema
2. Key point localization and filtering - Improve key points and throw out bad ones

Descriptor
3. Orientation Assignment - Remove effects of rotation and scale
4. Create descriptor - Using histograms of orientations

Fusion.

X – input pattern;

x_j – feature vector (derived from the input pattern X) provided by j classifier;

$\{w_1, w_2, \dots, w_M\}$ – M possible classes (enrolled users)

According to the Bayesian decision theory:

Assign $X \rightarrow w_r$ if $P(w_r|x_1,x_2) \geq P(w_k|x_1,x_2)$, where k = 1, …, M.

Transform this formula into other representations:

1. Sum Rule: if $P(w_r|x_1) + P(w_r|x_2) \geq P(w_k|x_1) + P(w_k|x_2)$, k = 1.. M.
2. Max Rule: if $\max(P(w_r|x_1),P(w_r|x_2)) \geq \max(P(w_k|x_1),P(w_k|x_2))$, k = 1.. M.
3. Min Rule: if $\min(P(w_r|x_1),P(w_r|x_2)) \geq \min(P(w_k|x_1),P(w_k|x_2))$, k = 1.. M.

Normalization.

Let X denote the set of raw matching scores from a specific matcher, and let $x \in X$. The normalized score of x is then denoted by x'.

Scaling:

1. Min-Max: $x' = \frac{x - \min(X)}{\max(X) - \min(X)}$
2. Z-score: $x' = \frac{x - \mathrm{mean}(X)}{\mathrm{std}(X)}$, mean(X) - arithmetic mean of X, std(X) - the standard deviation of X
3. Median: $x' = \frac{x - \mathrm{med}(X)}{\mathrm{MAD}(X)}$, med(X) - median of X, MAD(X) = med $|x - \mathrm{med}(X)|$

VIII. Experimental results

The evaluation metrics employed here are FAR (False Acceptance Rate) and FRR (False Rejection Rate).

FAR (FMR) is the likelihood that a biometric system will incorrectly accept an access attempt by an unauthorized user. Typically FAR is stated as the ratio - number of false acceptances divided by the number of all attempts (the fraction of impostor scores exceeding the threshold η).

FRR (FNMR) is the likelihood that the biometric system will incorrectly reject an access attempt by an authorized user. FRR typically is stated as the ratio of the number of false rejections divided by the number of all identification attempts (the fraction of genuine scores falling below the threshold η).

Regulating the value of η changes the FRR and the FAR values, but for a given biometric system, it is not possible to decrease both these errors simultaneously. The FAR and FRR are not independent in the same system and the sensitivity of the importance of FAR respectively FRR is also not the same. It is dependent on security requirements – sometimes the goal is to have FAR as low, as is possible (and the FRR is relatively high), sometimes some «compromise» is set up – the claim, that is necessary to decrease both parameters in the same system could be a task, but in real it does not work.

The performance of the proposed technique is evaluated using metrics of FAR and FRR. The values are taken for both modalities (finger vein, fingerprint) and for the fusion system.

Genuine Accept Rate – percentage of genuine users accepted by the system (the fraction of genuine scores exceeding the threshold. η): GAR = 1 – FRR.

The goal of considered system is to have higher GAR when FAR value is fixed and low enough.

Table 8.1 shows the performance (accuracy) of the considered multimodal system which employs combined normalization and fusion techniques described above.

Normalization Technique	Fusion Technique		
	Sum Rule	Max Rule	Min Rule
Min-Max	97.8	92.0	94.9
Z-score	95.4	94.2	93.1
Median	91.5	92.5	90.8

Table 8.1 - Genuine Accept Rate (GAR) (%) of different normalization and fusion techniques at the 0.1% False Accept Rate (FAR) for the final Multimodal database

We observe that the best accuracy is reached when a multimodal system employs the fusion with Sum Rule and Min-Max normalization technique.

At a FAR of 0.1%, the GAR

- of the fingerprint module is about 90.7%,
- of the finger vein is about 91.5%,

while that of the multimodal system is 97.8% if Min-Max normalization is used. (Figure 8.2.)

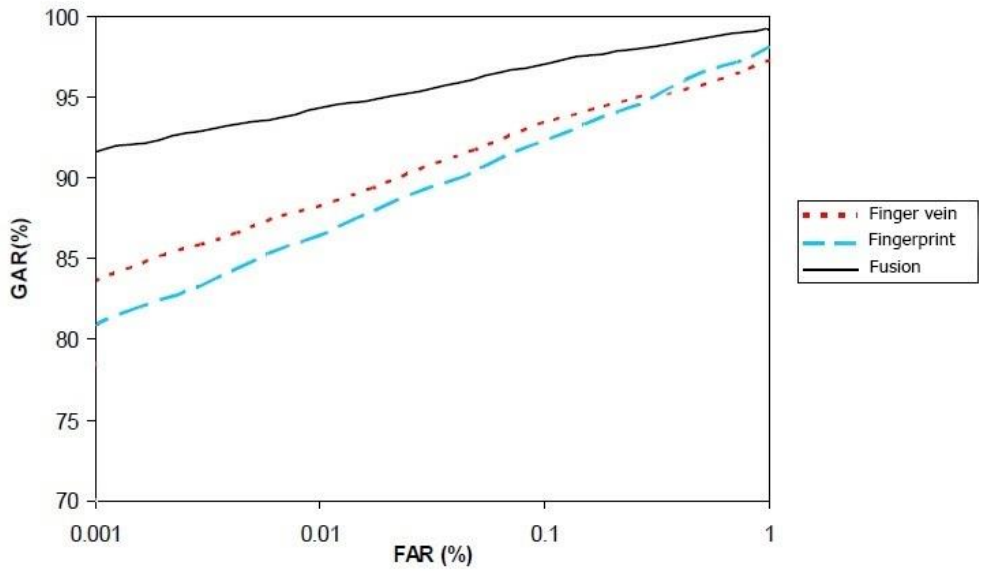


Figure 8.2 - Performance gain obtained by Sum Rule based fusion with applying Min-Max normalization

IX. Conclusion

In this paper the novel approach for personal recognition is presented.
This multimodal biometric system:

- uses fingerprint and finger vein images from «virtual» users
- utilizes the Minutiae Extraction for fingerprints and the Scale-Invariant Feature Transform for images of finger vein.
- provides better performance than any of the unimodal systems which use only one of the considered modalities.
- achieves the best accuracy while employing Min-Max normalization and Sum Rule for fusion.

The traits which are taken in proposed method are convenient for acquisition from one sensor. So it is possible to avoid extra costs for several sensors and raise of the time taken to acquire the biometric data.

It becomes increasingly difficult for an impostor to spoof multiple biometric traits. Thus, fusion of fingerprint and finger vein with suggested feature extraction and fusion techniques can be widely used in real personal authentication applications.

References

[1] Handbook of Biometrics, A.K. Jain, P. Flynn, A.A. Ross

[2] Handbook of Multibiometrics, A.A. Ross, K. Nandakumar, A.K. Jain

[3] Hand Vein-based Multimodal Biometric Recognition, S. Bharathi, R. Sudhakar, Valentina E Balas

[4] Joint Iris and Facial Recognition Based on Feature Fusion and Biomimetic Pattern Recognitio, Ying Xu, FeiLuo, Yi-Kui Zhai and Jun-Ying Gan // Proceedings of the 2013 International Conference on Wavelet Analysis and Pattern Recognition, pages 202-208

[5] Unimodal and Multimodal Biometric Sensing Systems: A Review, M.O. Oloyede, G.P. Hancke, IEEE Access, volume 4, 2016

[6] Multi-biometric cohort analysis for biometric fusion, G. Aggarwal, N.K. Ratha, R.M. Bolle, IEEE 2008

[7] A review on vein biometric recognition using geometric pattern matching techniques, A. Agarwal, S. Maheshwari, G. Yadav, IEEE 2014

[8] Palm vein biometric identification system using local derivative pattern, A.F. Akbar, T.A.B. Wirayudha, IEEE 2016

[9] Palm-Dorsal Vein Recognition Method Based on Histogram of Local Gabor Phase XOR, Z. Meng, X. Gu, Journal of Signal Processing Systems 73(1) October 2013

[10] Multimodal Biometric Authentication Using Fingerprint and Iris Recognition in Identity Management, K. Vishi, S.Y. Yayiligan, 2013 Ninth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, pages 334-341

[11] Stacked generalization, Wolpert, D. H., Technical Report LA-UR-90-3460, Los Alamos National Laboratory, 1990

[12] Boosting and Other Ensemble Methods, Drucker, H., Cortes, C, Jackel, L. D., LeCun, Y., and Vapnik, V., Neural Computation, 6(6) 1994: 1289-1301

[13] Hybrid Methods in Pattern Recognition, Bunke, H. and Kandel, A., volume 47 of Machine Perception and Artificial Intelligence, World Scientific, 2014

[14] Multi-Agent Reinforcement Learning: Independent vs. Cooperative Learning. Tan, M., Singh, M. P., Readings in Agents, pages 487-494, San Francisco, USA, 1997

[15] Combination of Multiple Classifiers Using Local Accuracy Estimates, Woods K., Bowyer K., Kegelmeyer W P, IEEE 1997, Transactions on Pattern Analysis and Machine Intelligence, 19(4):405-410.

[16] Consensus Theoretic Classification Methods, Benediktisson, J. A., Swain, P. H. , IEEE Transactions on Systems 1997, Man and Cybernetics, 22(4):688-704.

[17] Person Identification System using Feature Level Fusion of Multi-Biometrics, Ch.Venkata RamiReddy, Dr. K.V.Krishna Kishore, IEEE ICCIC 2016

[18] Decision level biometric fusion using Ant Colony Optimization, Amioy Kumar, Madasu Hanmandlu, Harsh Sanghvi, H. M. Gupta. IEEE 17th International Conference on Image Processing, 2010

[19] Hybrid fusion for biometrics: Combining score-level and decision-level fusion, Qian Tao, Raymond Veldhuis, IEEE 2008

[20] Face and Iris biometrics person identification using hybrid fusion at feature and score-level, Valentine Azom, Aderemi Adewumi, Jules-Raymond Tapamo, PRASA-RobMech, 2015