ISSN (Print) : 0974-6846
**Indian Journal of Science and Technology,** *Vol 9(42), DOI: 10.17485/ijst/2016/v9i42/93805, November 2016* ISSN (Online) : 0974-5645

# An Efficient Integrator based on Template Matching Technique for Person Authentication using Different Biometrics

**Sumana Kundu*** **and Goutam Sarker**

CSE Department, National Institute of Technology, Durgapur, West Bengal - 713209, India;
sumana.kundu@yahoo.co.in, sarkergoutam@yahoo.co.in

## Abstract

**Objectives:** A boosting based multiple classifier system has been developed using different biometric features like finger-print, palm-print, wrist-vein and handwriting for person authentication. **Methods/Statistical Analysis:** The multi-classifier is comprised of template matching based four different classifiers. These individual classifiers identify fingerprints, palm-prints, wrist-veins and handwritings separately and the super-classifier performs combination of four conclusions to set up the final decision based on programming based boosting method for person authentication. **Findings:** A new concept of Programming Based Boosting has been introduced in the super-classifier of this system to ultimately perform accurate person authentication with a variety of biometrics. This achieves better decision or conclusion regarding person identification/authentication than that with conventional single classifier with one or two biometrics or multimodal classifiers with conventional bagging or boosting. The method of utilizing multiple classifiers with four different biometric features in a single system is productive and viable as it would be difficult for an impostor to spoof all four different biometrics of a genuine user simultaneously. Also the accuracy, precision, recall and F-score of the classifiers are substantially moderate and the training and testing time of all the biometrics are quite low and affordable. **Application/Improvements:** This system will extremely helpful in such applications where accurate but rapid human identification is required like at the time of ATM transactions, VIP office entrance, access to computers or emails or e-bank account etc.

**Keywords:** Biometrics, Person Authentication, Programming based Boosting, Super-classifier, Template Matching

## 1. Introduction

Biometric traits can give a trustworthy, positive distinguishing proof of a person that increases security and makes access control more easily implemented. Biometric mechanism uses an assortment of various estimations of attributes and characteristics to recognize people. Biometric identifiers are generally classified as physiological and behavioral characteristics. Physiological attributes are related to the shape of the body. Example incorporate, however are not restricted to fingerprint, palm veins, face identification, DNA, palm print, hand geometry, iris identification, retina and odour/scent. Behavioral attributes are related to the pattern of behavior of a person, including however not restricted to typing rhythm, gait, and voice. Single biometric systems have limitations like uniqueness, high error rate, non-universality and noise. Multimodal systems also prevent spoofing since it would be difficult for an impostor to spoof multiple biometric traits of a genuine user concurrently. Another benefit of utilizing multimodality is that it tackles the issue of data distortion. In such case where the quality of one of the biometric features is unacceptable, the other can compensate for it. As for example, if a fingerprint has been scarred and the scanner rejects the distorted sample, having another modality like handwriting can prevent over this. Consequently, multimodal biometric frameworks overcome some of these issues by strengthening the proof acquired from several sources. Biometric features are acquired

* *Author for correspondence*

from different sources to identify a person. Different characteristics can be examined by a single system or separate systems that functions on its own and their decisions can be merged together.

In this paper, we introduce a multi-classifier for person recognition where every classifier functions on different biometric features. There are four individual classifiers for Fingerprint, Palm-print, Wrist-vein and Handwriting identification. These four individual classifiers are based on different Template matching techniques. Ultimately a Super-classifier provides the proper recognition of person based on programming based boosting logic considering the results of four individual classifiers.

## 2. Related Research

Biometrics is highly effective for person authentication as well as in the field of cryptography. In[1], the biometric signal is encrypted using Arnold transform algorithm and hided into the cover image with Qualified Significant Wavelet Tree (QSWT). The cover image is the image of the person. The Compressed cover image becomes transmitted over wireless channel for remote authentication. The Inverse Wavelet Transform is utilized to isolate encrypted signal and the cover image. The biometric signal becomes decrypted by inverse Arnold transformation algorithm. Iris is utilized here as an input for improving accuracy and to reduce fraud access. A technique[2] was presented to combine fragments of fingerprint of the sender and the receiver to create a random sequence, which was utilized as a public-key for Encryption and Decryption. The key thus generated was different as it was watermarked with sender's biometric signature. The encrypted message was then sent to the receiver along with the key. The receiver utilized this key to decrypt the message to plain text.

Various unimodal and multimodal biometric systems have already been developed. In a fingerprint recognition algorithm using EBFNN[3], fingerprint features are extracted by six-layer WT decomposition on binary images. Then, the extracted features are fed as input to the designed EBFNN for training and perform fingerprint identification. A PCA of symmetric sub-space model of neural network algorithm (SSA)[4] was approached for fingerprint recognition. A feature extraction algorithm for palm-print identification was proposed based on statistical features 2D-DCT[5], which exploited the local spatial variations in a palm-print image. A system was proposed using ridge features for palm print recognition[6], which extracted the features such as orientation field and region mask and minutiae extraction and cascade filtering was applied for matching. A hand-vein verification system[7] was approached using a BGM algorithm. A maximum curvature algorithm was used to extract the vein. Another hand-vein identification system[8] was proposed based on near-infrared imaging of dorsal hand veins and matching of the key points that were extracted from the dorsal hand-vein images by the scale-invariant feature transform. An automatic handwriting identification[9] was presented using scanned images of handwriting with feed forward neural network. A writer identification system[10] was presented that utilize RBF in the Off-line mode.

A fingerprint and iris feature-level fusion based identification technique[11] was proposed using conventional RBFNN. Here iris and fingerprint features were extracted by block sum method and Haar wavelet method respectively. A multimodal biometric identification system[12] was proposed based on palm-print and fingerprint. In this multimodal biometric system each and every biometric feature processes its information individually and then the processed information was combined using a fusion technique. Euclidean-distance matching algorithm was used to compare the database template and the input data. A multimodal identification system[13] was approached, where palm print and palm vein features were analyzed using Contourlet transform. Local minutiae and a global feature were captured by the algorithm from a palm print and palm vein images and stored them as a compact code. After ROI extraction from the source images, the iterated directional filter bank structure was used to divide the (2-D) image spectrum into fine sub-components. Euclidean Distance algorithm was used to perform the feature matching technique. Hierarchical minutiae matching algorithm was proposed for fingerprint and palmprint identification systems[14]. The hierarchical strategy which was utilized in the matching stage can reject many finger prints quickly to save time which did not belong to the same finger as the input fingerprint. An ensemble systems[15] was presented which is the analysis of some well-established recognition techniques, used as a tool to enhance the performance of cancellable multi-biometric processing where two optimization techniques were studied in order to increase the efficiency of the ensemble systems.

Different multi-classification systems based on

appearance based method using different hybrid artificial neural networks[16,17] have been proposed and developed in[18–20]. In these systems different biometrics such as face, iris, fingerprint and handwriting were utilized for person authentication. All these systems consist of three different classifiers which were operated on three different biometric features.

The majority of the multimodal systems depends on fusion technique and utilizes two biometric traits for person identification. Two biometric features may not be sufficient to avoid forging. The training times of some multimodal systems for different biometrics were moderately high and for some systems the accuracy was moderately low. To overcome such kind of problems a multi modal system which considers four different biometric features is approached in this paper. This system did not follow the traditional fusion technique, rather than a new programming based boosting method is used to combine four different classifiers conclusion considering four different biometric features to get the final identification of the person.

## 3. Work Flow of the Present System

This multi-classification system contains four different classifiers based on template matching technique for fingerprint, palm-print, wrist-vein and handwriting identification separately. Then super-classifier concludes the final identification of the person based on programming based boosting considering the result of these four individual classifiers.

### 3.1 Preprocessing of Different Biometrics

Four different biometric traits such as fingerprint, palm-print, wrist-vein and handwriting are used in four different classifiers individually. All the different biometric patterns of training and test databases have to be preprocessed before make templates and also before recognition. Different steps for preprocessing of different biometrics are described below.

#### *3.1.1 Preprocessing of Fingerprint Patterns*

- *RGB to Gray scale image conversion:* In the first step all the RGB fingerprint images were converted into gray scale patterns.
- *Background Removal:* Backgrounds of the fingerprint patterns have been removed in this step.
- *Patten Normalization:* In this step, all the fingerprint patterns were normalized into equal and lower dimensions.
- *Gray scale to Binary conversion:* All the gray scale fingerprints were converted into binary patterns before make the fingerprint templates.

#### *3.1.2 Preprocessing of Palm-print Patterns*

- *Found ROI from palm-print image:* In the first step, Region of Interest (ROI)[21] containing principal lines have been identified from the entire palm-print pattern.
- *Principal Line Detection:* Huang's method[21,22], which is based on the Radon transform[17] was used for principal line extraction and then a series of postprocessing operations were used to enhance the line extraction results. These patterns have been used to make palm-print templates.

#### *3.1.3 Preprocessing of Wrist-vein Patterns*

- *RGB to Gray scale conversion of the patterns:* In this step all the RGB wrist-vein patterns were converted into gray scale patterns.
- *Get more prominent vein structure:* To get more prominent vein structure, Contrast-Limited Adaptive Histogram Equalization (CLAHE) was used.
- *Pattern crop:* In this step, a particular region was cropped from the entire wrist-vein pattern to get the exact vein region.
- *Patten Normalization:* In this step, all the patterns were normalized into equal and lower dimensions.
- *Gray scale to Binary pattern conversion:* All the gray scale patterns were converted into its corresponding binary patterns. These binary patterns were used to make wrist-vein templates.

#### *3.1.4 Preprocessing of Handwriting Patterns*

- *RGB to Gray scale conversion of the patterns:* In this step all the RGB handwriting patterns were converted into gray scale patterns.
- *Background Removal:* In this step, backgrounds of all the handwriting patterns have been removed.
- *Pattern Normalization:* All the handwriting patterns were normalized into same and lower dimension before make the handwriting templates.

## 3.2 Training and Test databases

There are four different training databases for four different biometric features i.e., fingerprint palm-print, wrist-vein and handwriting. Each database contains different biometric patterns of different persons. In fingerprint database for each person's finger print, three different qualities of finger prints and for each person, three different angular ($0^{\circ}, 90^{\circ}$ and $180^{\circ}$ ) finger prints are also included. The palm-print database consists of four different qualities of palm-prints for right and left hands respectively for each person. The wrist-vein database contains four different qualities of wrist-vein patterns for right and left hands respectively for each person. Finally, the handwriting database contains six different qualities of handwritings (name and surname separately) for each person (Figure 1).

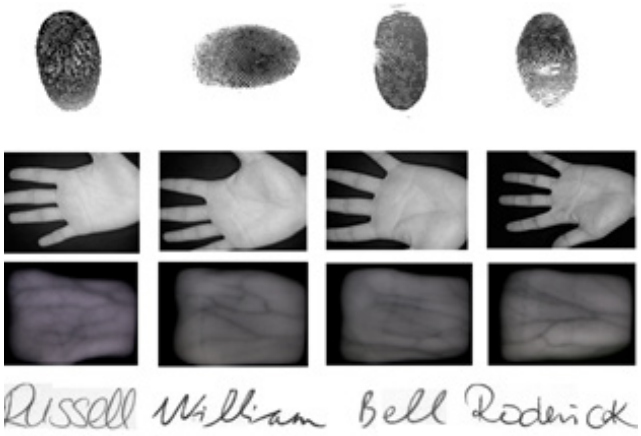

**Figure 1.** Samples of few training patterns of different biometric features for single classifiers.

The test sets for testing to estimate the performance of individual classifiers with *Holdout method* contains different people's (same as training data set) patterns (fingerprints, palm-print, wrist-vein and handwriting) of various qualities/instances. These patterns are completely different from training set. The test sets for testing to estimate the performance of the super-classifier contain pattern sets of different people (same as training data set). Each pattern test set of super-classifier contains one fingerprint, palm-print, wrist-vein and handwriting pattern of a particular person. The patterns of each pattern set are also of various qualities which are also completely different from training set. The test sets for individual four classifiers and super-classifier also contain some unknown patterns of various qualities which were not included to make the templates for different biometrics (Figure 2. and Figure 3).

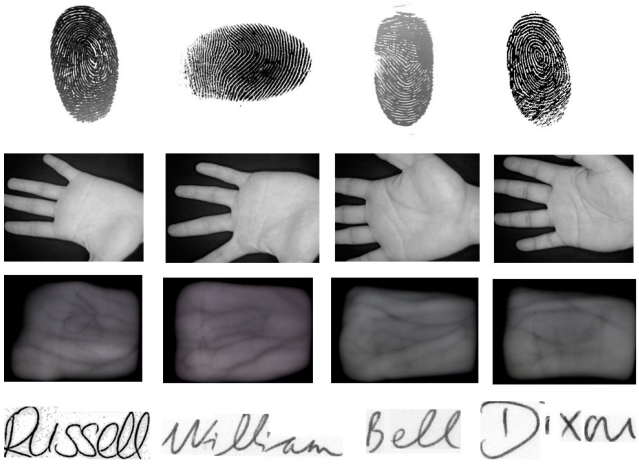

**Figure 2.** Samples of few test patterns of different biometric features for single classifiers.

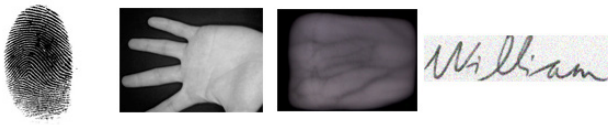

**Figure 3.** A sample of test pattern set (person 2) of super-classifier for person identification.

## 3.3 Templates Generation from Different Biometric Patterns

Different preprocessed biometric patterns were used to make templates. In the 1st classifier, fingerprint templates have been made from different qualities of fingerprints of each person and angle ($0^{\circ}, 90^{\circ}$ and $180^{\circ}$ ). So, different qualities of respective preprocessed training fingerprints were added to make final templates for any particular person respective to angles. In the 2nd classifier, palm-print templates have been made from different qualities of palm-prints of each person and of both left and right hands. So, different qualities of respective preprocessed training palm-prints were added to make final templates for any particular person respective to left and right hands. In the 3rd classifier, wrist-vein templates have been made from different qualities of wrist-vein patterns of each person and of both left and right hands. So, different qualities of respective preprocessed training wrist-vein patterns were added to make final templates for any particular person respective to left and right hands. In the 4th classifier, handwriting templates have been made

from different qualities of handwritings of each person and of name and surname. Hence, different qualities of respective preprocessed training handwriting patterns were added to make final templates for any particular person respective to name and surname (Figure 4).


**Figure 4.** Samples of few templates of different biometrics (fingerprint, palm-print, wrist-vein and handwriting).

## 3.4 Programming based Boosting

The system uses programming based boosting in super-classifier that is super-classifier concludes the final identification of the person based on programming based boosting method considering the decisions of four individual classifiers. In case of programming, the weight of the vote of each classifier is pre assigned or 'programmed' beforehand. The weights of the different links from the individual classifiers into the integrator are programmed. These weights are the performances in terms of normalized *accuracy* of the individual classifiers.

## 3.5 Identification Testing

At the time of testing, after preprocessing, each given biometric pattern was compared with all the templates of corresponding biometric. Depending on the correlation coefficients between the test images and templates, a threshold has been set to differentiate between known and unknown pattern. The corresponding correlation coefficient above threshold is considered as corresponding known biometric pattern. The values of the correlation coefficient of each and every output unit represent the probability of belongingness of the input test pattern into the different classes. Finally, the super-classifier concludes the final identification of the person based on programming based boosting method considering the decisions of four individual classifiers. Similarly, finally we calculate the probability of belongingness of the input test pattern for that corresponding class concluded by super-classifier by taking the minimum value of probability among four different classifiers.

If the output of three or more classifiers are contradictory in nature, then the conclusion obtain by the classifier with higher weighted link has to be accepted with minimum probability. So, the ensemble algorithm for super-classifier works well in such contradictory situations (Figure 5 and the Algorithm 1).

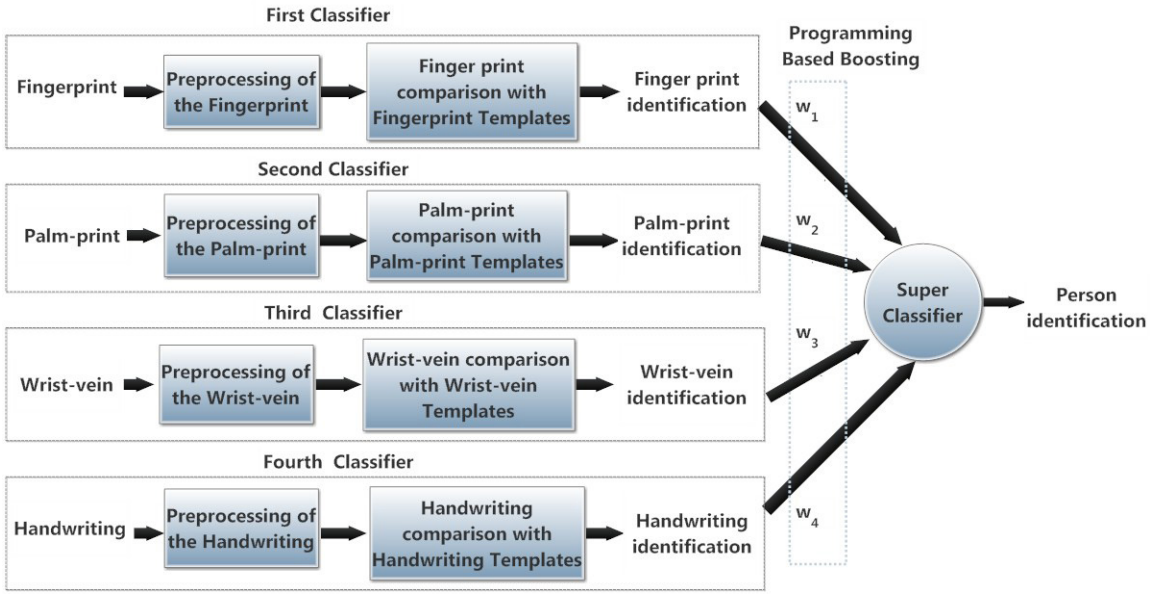


**Figure 5.** Block diagram of the proposed system for identification testing.

**Algorithm 1: Algorithm for Person Identification using Super-classifier**

***Input:*** *Test folder comprising pattern sets including known and unknown patterns.*
***Output:*** *Identification of the given test pattern set.*

Steps:

1. *Get a pattern set (one fingerprint, one palm-print, one wrist-vein and one handwriting of a particular person) to test.*
2. *Preprocess every single pattern of the given pattern set with the preprocessors of 4 individual classifiers.*
3. *Compare these preprocessed patterns with the templates of respective classifiers individually for corresponding patterns recognition.*
4. *For each biometric pattern, if the $n^{th}$ value of correlation coefficients is above thresholdthen conclude the respective pattern to be of the $n^{th}$ person, otherwise conclude 'unidentifiable person'.*
5. *Calculate the probabilities of belongingness of the patterns for particular classes from the respective values of correlation coefficients.*
6. *Get the results of 4 individual classifiers.*
7. *Input these results to super-classifier.*
8. *Now the weights of the links of four individual classifiers become, $wt_1$, $wt_2$, $wt_3$ and $wt_4$ where, $wt_1 = \frac{w_1}{w_1 + w_2 + w_3 + w_4}$, $wt_2 = \frac{w_2}{w_1 + w_2 + w_3 + w_4}$, $wt_3 = \frac{w_3}{w_1 + w_2 + w_3 + w_4}$ and $wt_4 = \frac{w_4}{w_1 + w_2 + w_3 + w_4}$ respectively. Here, $w_1$, $w_2$, $w_3$ and $w_4$ are the respective accuracies of4 individual classifiers.*
9. *If all classifiers outputs the patterns as $n^{th}$ person, then super-classifier calculate the maximum weight among the weights of 4 links and concludes that patterns as $n^{th}$ person, otherwise conclude 'unidentifiable person'.*
10. *The probability of belongingness of the pattern set into this $n^{th}$ class is, $p=min(p_1, p_2, p_3, p_4)$, where $p_1$, $p_2$, $p_3$ , $p_4$ are the probabilities of belongingness into the classes for four individual classifiers.*
11. *If any 3 classifiers outputs the patterns as $n^{th}$ person (say, for patterns of person 2, $1^{st}$,$3^{rd}$and $4^{th}$ classifier give outputs as person 2) and one classifier output as different (say, for pattern of person 2, $2^{nd}$ classifier give output as person 1), then super-classifier first sums up the weights (say, $wt=wt_1+wt_3+wt_4$) of the links of the classifiers which give same outputs, then compare this result with the fourth one (say, $wt_2$).Get the maximum weight,(say, $mwt=max(wt,wt_2)$) and concludes the identification of the person as per the output corresponding to maximum weight.*
12. *The probability of belongingness of the pattern set into the particular class depends on the previous step. If super-classifier conclude the decision over the majority of the classifiers, then probability of belongingness of the pattern set into the particular class is, $p=min(p_i, p_j, p_k)$, where $i=j=k=1$ or 2 or 3 or 4. Otherwise, $p=p_l$ , where $i=j=k \neq l$.*
13. *If any 2 classifiers outputs the patterns as $n^{th}$ person and other 2 classifiers outputs the patterns as $m^{th}$ person (say, for patterns of person 2, $1^{st}$ and $3^{rd}$ classifier give outputs as person 2 but $2^{nd}$ and $4^{th}$ classifier give outputs as person 4), then super-classifier first sums up the weights of 2 corresponding links separately which give same outputs (say, $wt1=wt_1+wt_3$ and $wt2=wt_2+wt_4$), then compare this two values to get the maximum weight (say, $mwt=max(wt1,wt2)$) and concludes the identification of the person as per the output corresponding to maximum weight.*
14. *The probability of belongingness of the pattern set into the particular class depends on the previous step. The minimum probability among 2 probabilities corresponding to 2 winning links is taken as the final probability of this pattern set.*
15. *If any 2 classifiers outputs the patterns as $n^{th}$ person and other 2 classifiers give 2 different decisions or outputs individually (say, for patterns of person 2, $1^{st}$ and $4^{th}$ classifier give outputs as person 2 but $2^{nd}$ classifier give output as person 1 and $3^{rd}$ classifier give output as person 4), then super-classifier first sums up the weights (say, $wt=wt_1+wt_4$) of the links of the classifiers which give same outputs, then compare this result with the weights of another 2 links to get the maximum weight (say, $mwt=max(wt, wt_2, wt_3)$) and concludes the identification of the person as per the output corresponding to maximum weight.*
16. *The probability of belongingness of the pattern set into the particular class depends on the previous step. If super-classifier conclude the decision over the majority of the classifiers, then probability of belongingness of the pattern set into the particular class is, $p=min(p_i, p_j)$, where $i=j=1$ or 2 or 3 or 4. Otherwise, $p=p_k$ or $p_l$, where $i=j \neq k \neq l$. i.e. the probability of the corresponding winning link.*
17. *If all four classifier outputs as different, then the super-classifier calculate the maximum weight among 4 links and concludes the identification of the person as of that corresponding link otherwise as, 'unidentifiable person'.*
18. *The probability of belongingness of the pattern set into the particular class is, $p=min(p_1, p_2, p_3, p_4)$, where $p_1$, $p_2$, $p_3$ , $p_4$ are the probabilities of belongingness into the classes for four individual classifiers.*
19. *If any more testing is required, go to step 1.*
20. *Stop.*

# 4. Result and Performance Analysis

We have taken the patterns of four different biometric features from four different standard databases for training and test databases. We were unable to gather all the different biometric patterns from one standard database. That is why it was assumed that, different biometric patterns of different standard databases were of same particular people without losing any generality to evaluate the present system's performance.

We have used training and test database for Fingerprint samples from FVC 2004 databases (http://www.advancedsourcecode.com/fingerprintdatabase.asp), Palm-print samples from CASIA Palm print Image Database(http://biometrics.idealtest.org/dbDetailForUser.do?id=5), Wrist vein samples from CIE Biometrics (http://biometrics.put.poznan.pl/vein-dataset/) Handwriting samples from IAM handwriting database (http://www.iam.unibe.ch/fki/databases/iam-handwriting-database/download-the-iam-handwriting-database).

## 4.1 Performance Evaluation Metrics of the Classifiers

Holdout method[23] was used to estimate the performance of the classifier.

| | | Actual Class | |
|---|---|---|---|
| | | X | Y |
| Predicted Class | X | a | b |
| | Y | c | d |

**Figure 6.** Confusion matrix (2 class).

From the confusion matrix (Figure 6), if there are only two classes (say X and Y), then the *accuracy, precision, recall* and *F-score* are defined as follows:

$$Accuracy = \frac{a+d}{a+b+c+d} \times 100 \quad (1)$$

$$Precision = \frac{a}{a+b} \quad (2)$$

$$Recall = \frac{a}{a+c} \quad (3)$$

$$F-score = \frac{2 * recall * precision}{recall + precision} \quad (4)$$

For the performance assessment of the classifier, when we applied holdout technique we could test such patterns which were excluded in training dataset. In assessment of a classifier with accuracy metric the overall performance of the classifier is reflected regardless of the individual performance evaluation for each and every class or category. This is more suitable for assessing the system performance through a specific numeric value. Precision, recall and F-score metrics were utilized to explain the performance of every class.

## 4.2 Experimental Results

The proposed system was made to learn on a computer with Intel Core 2 Duo E8400, 3.00 GHz processor with 4 GB RAM and Windows 7 32-bit Operating System.

Some salient portion of experimental result which handles contradictory situation (each classifier is identifying separate person) is given below:

```
Given Fingerprint is of person :1  with probability
:0.57403
Given Palm print is of person :2  with probability
:0.45707
Given Wrist_vein print is unknown
Given Handwriting is of person :3  with probability
:0.80382

Superclassifier conclude...
Given Biometrics are of person :3  with probability
:0.45707
```

Now if we use simple majority voting logic then super-classifier conclude the given pattern set as of 'unidentifiable person' because 4 different classifiers give 4 different result of recognition. But when programming based boosting technique is used, the super-classifier concludes the given pattern set as of person 3 with probability 0.45707. Here, the weights of the links corresponding to four different classifiers are 0.2460, 0.1903, 0.2782 and 0.2855 respectively. The weight of the link corresponding to fourth classifier is highest and the minimum graded probability of biometrics is obtained from second classifier. Thus the maximum weighted result with minimum probability (the probability which is safest to accept) is concluded.

**Table 1.** Accuracy of the classifiers (Holdout method)

| Classifiers | Accuracy |
|---|---|
| First classifier (Fingerprints) | 86.67 % |
| Second classifier (Palm-prints) | 78.33 % |
| Third classifier (Wrist-veins) | 75.00 % |
| Fourth classifier (Handwritings) | 95.00 % |
| Super-classifier | 96.67 % |

**Table 2.** Performance measurement of the classifiers with holdout method

| Performance evaluation metrics person wise | | 1st classifier (Finger prints) | 2nd classifier (Palm-prints) | 3rd Classifier (Wrist-veins) | 4th classifier (Hand writings) | Super-classifier |
|---|---|---|---|---|---|---|
| Precision | person1 | 0.80000 | 1.00000 | 1.00000 | 1.00000 | 1.00000 |
| | person2 | 0.90000 | 0.66667 | 1.00000 | 1.00000 | 1.00000 |
| | person3 | 1.00000 | 1.00000 | 0.90909 | 1.00000 | 1.00000 |
| | person4 | 0.78571 | 0.75000 | 1.00000 | 1.00000 | 0.85714 |
| | Unknown Person | 0.90000 | 0.66667 | 0.44000 | 0.80000 | 1.00000 |
| Recall | person1 | 1.00000 | 0.83333 | 0.83333 | 0.83333 | 1.00000 |
| | person2 | 0.75000 | 0.66667 | 0.66667 | 0.91667 | 1.00000 |
| | person3 | 0.91667 | 0.58333 | 0.83333 | 1.00000 | 0.83333 |
| | person4 | 0.91667 | 1.00000 | 0.50000 | 1.00000 | 1.00000 |
| | Unknown Person | 0.75000 | 0.83333 | 0.91667 | 1.00000 | 1.00000 |
| F-score | person1 | 0.88889 | 0.90909 | 0.90909 | 0.90909 | 1.00000 |
| | person2 | 0.81818 | 0.66667 | 0.80000 | 0.95652 | 1.00000 |
| | person3 | 0.95652 | 0.73684 | 0.86957 | 1.00000 | 0.90909 |
| | person4 | 0.84615 | 0.85714 | 0.66667 | 1.00000 | 0.92308 |
| | Unknown Person | 0.81818 | 0.74074 | 0.59459 | 0.88889 | 1.00000 |

**Table 3.** Learning time of the biometric features (in seconds)

| Classifiers | Training Time for 60 number of training samples for each biometrics | Testing Time (single test sample) | Total Time |
|---|---|---|---|
| First Classifier (Fingerprints) | 2.0817 | 0.0252 | 2.1069 |
| Second Classifier (Palm-prints) | 3.3052 | 0.0131 | 3.3183 |
| Third Classifier (Wrist-vein) | 5.3772 | 0.0737 | 5.4509 |
| Fourth Classifier (Handwriting) | 0.9153 | 0.0122 | 0.9275 |
| Super-Classifier | 11.6794 | 0.1242 | 11.8036 |

**Table 4.** Comparative study with the accuracy of the systems

| Multimodal Systems | Accuracy (%) |
|---|---|
| Fingerprint – Iris[11] | 92 % |
| Palm print – Fingerprint[12] | 87 % |
| Present System | 96.67 % |

From Table 1 it can be seen that the accuracies of four different classifiers for four different biometric features (fingerprint, palm-print, wrist-vein and handwriting) are 86.67%, 78.33%, 75.00%, 95.00% and the accuracy of the super-classifier is 96.67%. Along these measurements, it is proven that the super-classifier is effective for person recognition than considering single classifiers utilizing single biometric traits exclusively. In Table 2, precision, recall and F-score metrics explain the performance of each class with holdout method. In Table 3, the multi-classification system indicates overall low training time as well as testing time (< 1 second) for different biometric patterns. Table 4 display a comparative study of the proposed system in terms of accuracy with other systems[11,12] mentioned in Section 2. Hence, the proposed approach displays improvement in terms of accuracy with low learning time as compared to systems mentioned in the Section 2.

## 5. Conclusion

In this template matching based multi-classifier framework, rather than utilizing a single classifier with a single biometric feature for person identification, an effort has been made to utilize multiple template matching based classifiers acting on the various biometric features. It is worthwhile from the point of view that we need not have to depend on a single classifier based on a specific biometric and rather, the decision coming out of the different types of classifiers using different biometric features are suitably integrated based on weighted voting logic. In this way, the different conclusions from individual classifiers are fused together to find out the most dependable conclusion.

The performance assessment with accuracy, precision, recall, F-score with Holdout method for individual three classifiers along with super-classifier is moderately high for different biometric traits. Additionally the training and testing time is quiet low for different biometrics. The present multi-classifier based on different biometrics is simple, efficient and faster than other conventional unimodal identification systems.

## 6. References


1. Punidha R, Vincy SA, Judith M, Ramya D. Remote service access using biometrics. Indian Journal of Science and Technology. 2016 Jan; 9(1):1–6.
2. Ankit K, Rekha J. Biometrics as a cryptographic method for network security. Indian Journal of Science and Technology. 2016 Jun; 9(22):1–6.
3. Luo J, Lin S, Ni J, Lei M. An improved fingerprint recognition algorithm using EBFNN. 2nd International Conference on Genetic and Evolutionary Computing; Tianjin. 2008. p. 504–7.
4. Yu C, Jian Z, Bo Y, Deyun C. A novel principal component analysis neural network algorithm for fingerprint recognition in online examination system. Asia-Pacific Conference on Information Processing; China. 2009. p. 182–6.
5. Imtiaz H, Aich S, Fattah S A. Palm-print Recognition based on DCT domain statistical features extracted from enhanced image. International Conference on Electrical Engineering and Information and Communication Technology; Bangladesh. 2014. p. 1–4.
6. George A, Karthick G, Harikumar R. An efficient system for palm print recognition using ridges. International Conference on Intelligent Computing Applications; India. 2014. p. 249–53.
7. Lajevardi M, Arakala A, Davis S, Horadam KJ. Hand vein authentication using biometric graph matching. IET Biometrics. 2014; 3(4):302–13.
8. Wang Y, Zhang K, Shark Lik-K. Personal identification based on multiple keypoint sets of dorsal hand vein images. IET Biometrics. 2014; 3(4):234–45.
9. Anton C, Ştirbu C, Badea R, Vasile V. Identify handwriting individually using feed forward neural networks. International Journal of Intelligent Computing Research. 2010; 1(4):183–8.
10. Ashok J, Rajan EG. Off-line hand written character recognition using radial basis function. Int J Advanced Networking and Applications. 2011; 2(4):792–5.
11. Gawande U, Zaveri M, Kapur A. Fingerprint and iris fusion based recognition using RBF neural network. Journal of Signal and Image Processing. 2013; 4(1):142–8.
12. Dhameliya MD, Chaudhari JP. A multimodal biometric recognition system based on fusion of palmprint and fingerprint. IJETT. 2013; 4(5):1908–11.
13. Gaikwad DP, Narote SP. Multi-modal biometric system using palm print and palm vein features. Annual IEEE India Conference (INDICON); India. 2013. p. 1–5.
14. Chen F, Huang X, Zhou J. Hierarchical minutiae matching for fingerprint and palmprint identification. IEEE Transactions on Image Processing. 2013; 22(12):4964–71.
15. Canuto AMDP, Fairhurst MC, Pintro F. Ensemble systems and cancellable transformations for multibiometric-based identification. IET Biometrics. 2014; 3(1):29–40.
16. Naseera S, Rajini GK, Prabha NA, Abhishek G. A comparative study on CPU load predictions in a computational grid using artificial neural network algorithms. Indian Journal of Science and Technology. 2015 Dec; 8(35):1–5.
17. Gharehchopogh FS, Khaze SR, Maleki I. A new approach in bloggers classification with hybrid of k-nearest neighbor and artificial neural network algorithms. Indian Journal of Science and Technology. 2015 Feb; 8(3):237–46.
18. Kundu S, Sarker G. An efficient multiple classifier based on fast RBFN for biometric identification. 2nd International Conference on Advanced Computing, Networking, and Informatics - Smart Innovation, Systems and Technologies; India. 2014. p. 473–82.
19. Kundu S, Sarker G. A super classifier with programming based boosting using biometrics for person authentication. Advances in Intelligent Systems and Computing 509: Proceedings of International Conference on Computational Intelligence; 2015.
20. Kundu S, Sarker G. A person identification system with biometrics using modified RBFN based multiple classifiers. Advances in Intelligent Systems and Computing: Proceedings of International Conference on Intelligent Computing and Communication; 2016.
21. Li W, Zhang B, Zhang L, Yan J. Principal line-based alignment refinement for palmprint recognition. IEEE Transactions on Systems, Man, and Cybernetics- Part C: Applications and Reviews. 2012; 42(6):1491–9.
22. Huang DS, Jia W, Zhang D. Palmprint verification based on principal lines. Pattern Recognition. 2008; 41(4):1316–28.
23. Pudi V, Krishna PR. Data Mining. India: Oxford University Press; 2009.