Mj. Int. J. Sci. Tech. **2008**, *2*(03), 498-501

Maejo International

Journal of Science and Technology

ISSN 1905-7873

Available online at www.mijst.mju.ac.th

Full Paper

Image-based fingerprint verification system using LabVIEW

Ajat S. Arora [1] and Sunil K. Singla [2,]*

[1] Department of Electrical and Instrumentation Engineering, Sant Longowal Institute of Engineering and Technology, Longowal, Punjab, India

[2] Department of Electrical and Instrumentation Engineering, Thapar University, Patiala, Punjab, India

*Corresponding author, e-mail: sunilksingla2001@yahoo.com

Received: 4 April 2008 / Accepted: 1 September 2008 / Published: 5 September 2008

Abstract: Biometric-based identification/verification systems provide a solution to the security concerns in the modern world where machine is replacing human in every aspect of life. Fingerprints, because of their uniqueness, are the most widely used and highly accepted biometrics. Fingerprint biometric systems are either minutiae-based or pattern learning (image) based. The minutiae-based algorithm depends upon the local discontinuities in the ridge flow pattern and are used when template size is important while image-based matching algorithm uses both the micro and macro feature of a fingerprint and is used if fast response is required. In the present paper an image-based fingerprint verification system is discussed. The proposed method uses a learning phase, which is not present in conventional image-based systems. The learning phase uses pseudo random sub-sampling, which reduces the number of comparisons needed in the matching stage. This system has been developed using LabVIEW (Laboratory Virtual Instrument Engineering Workbench) toolbox version 6i. The availability of datalog files in LabVIEW makes it one of the most promising candidates for its usage as a database. Datalog files can access and manipulate data and complex data structures quickly and easily. It makes writing and reading much faster. After extensive experimentation involving a large number of samples and different learning sizes, high accuracy with learning image size of 100×100 and a threshold value of 700 (1000 being the perfect match) has been achieved.

Keywords: biometrics, fingerprint, LabVIEW, datalog files, segmentation, pseudo random sub-sampling

Introduction

Biometric-based personal authentication (verification/identification) systems use physiological (e.g. fingerprint, face, hand geometry, etc.) or behavioural (e.g. speech, handwriting) traits of a person. Biometric systems are becoming increasingly popular, compared to traditional systems because of their ability to provide more security. In practice there are three different methods to check the identity of a person [1,2]; these are:

- Ownership: something you have (key, smart card, etc.)
- Knowledge: something you know (PIN, password, etc.)
- Biometrics: something you are or something you do (fingerprints, face, voice, etc.)

The conventional methods (ownership and knowledge) of checking someone's identity actually suffers from two common problems [2,3]:

- Their inability to differentiate between an authorised person and an imposter who fraudulently acquires the access privilege of the authorised person
- Their being lost, stolen, copied (ownership) or forgotten, guessed (knowledge)

Only the third method, i.e. biometrics, can identify you as you and is much more secured than the conventional methods.

Fingerprint is one of the most promising methods among all the biometric techniques and has been used for personal authentication for a long time. A fingerprint consists of raised friction ridges separated by recessed valleys of skin [4,5]. The locations and angular orientation of the ridge endings and ridge bifurcations within the fingerprint uniquely characterise the fingerprint. Presently, it is used for commercial applications as well as by law enforcement agencies. In practice fingerprint systems are of two types [1,2], viz. fingerprint identification and fingerprint verification.

Fingerprint Identification: This kind of system compares the biometric information of a person to all entities on a database. A person does not assert his/her identity to that system; instead the person just gives the biometric information. The system then tries to match this data to all the entities in the database and drives whether a match can be made. This type of system is known as identification system. This system gives the information: "Who the person is."

Fingerprint Verification: A verification system authenticates a person's identity by comparing the captured fingerprint information to one specific entry on a database that corresponds to that person. By comparing one-to-one the system decides whether the identity claimed by the individual is true or not. A verification system is also known as a one-to-one system.

The fingerprint has gained widespread public acceptance due to its convenience and reliability. It takes little time and effort to acquire one's fingerprint so its recognition is considered among the least intrusive of all biometric verification techniques. Fingerprint verification algorithms are of minutiae-based and image-based [6]. For minutiae-based fingerprint algorithm, only a small part of the finger image is required for verification. Normally, ridge ending and ridge bifurcation are taken into consideration. According to the empirical study, two individuals will not have eight or more common minutiae [7,8]. It would be ideal to use this algorithm where space restrictions impacted the use and deployment of biometrics, but this type of system requires a high-quality fingerprint image. Also, minutiae-based approach requires extensive preprocessing operation and it is also required to reduce the number of false minutiae erroneously detected in noisy fingerprint images [9]. Image-based matching algorithm uses both the micro and macro features of a fingerprint. The size of the image required for authentication must be larger as compared to minutiae-based algorithm, so the memory requirement is more. However, this algorithm is computationally more efficient because it can be directly applied to the gray-scale fingerprint image without or with very little preprocessing. Moreover, unlike the minutiae-based system, the image-based fingerprint verification system is capable of dealing with bad-quality images from which the minutiae cannot be extracted reliably, and also with fingerprints that suffer from non-uniform shape distortion [10]. Instead of using only the minutiae locations the image-based system uses the gray-level information which provides much richer and more discriminatory information than only the minutiae locations.

Present Work

In the present work an image-based algorithm for fingerprint verification is discussed as it is faster than the minutiae-based algorithm. The proposed algorithm has been developed using LabVIEW (Laboratory Virtual Instrument Engineering Workbench) 6i software. The proposed verification algorithm consists of two steps: enrollment of the user and authentication of the user.

In the enrollment process new users are enrolled in the system. Each user has to enter his/her name and password along with biometric information, i.e. the fingerprint. The flow chart of enrollment type module is shown in Figure 1. For the enrollment of the user a data record is to be maintained in the database containing the name and the password of the user. If simple text files are used the name and password get stored together as a single string. Using LabVIEW datalog files [11] (which are exclusively available in LabVIEW to maintain database of records) the information regarding the user is stored in the form of clusters. Datalog files make writing and reading much faster. They also simplify data retrieval because the original blocks of data can be read as a record without having to read all records that precede it in the file. Random access is fast and easy with datalog files because all it needs is to access the record as a record number. This module is designed in such a way that no two users should be of the same name although a user can have any password. If the same name is entered that already exists in the database the algorithm will demand a new name to be entered. The next step is to store the reference biometric information of the person concerned. The reference/query image may contain the information which is not required. In order to eliminate such undesirable information, a preprocessing step, i.e. segmentation, is performed. Segmentation is the process of separating the foreground region in the image from the background one. The foreground region corresponds to the clear fingerprint area containing the ridges and valleys, which is the area of interest. The background corresponds to the region outside the border of the fingerprint area which does not contain any valid fingerprint information. The segmentation is performed by calculating the variance. A foreground region has a high variance value while a background region has a low one. The image is divided into an 8 × 8 window and its variance calculated. If the variance is below a particular value then that is a background**.** If it is above a particular value then it contains the biometric information. The variance k of the window of size $W \times W$ is given by:

$$\sigma^2(k) = \frac{1}{W^2}\sum_{i=0}^{W-1}\sum_{j=0}^{W-1}\left(I(i,j) - M(k)\right)^2$$

where $M(k)$ = mean of block k

$I(i, j)$ = value at pixel (i, j)

σ = standard deviation

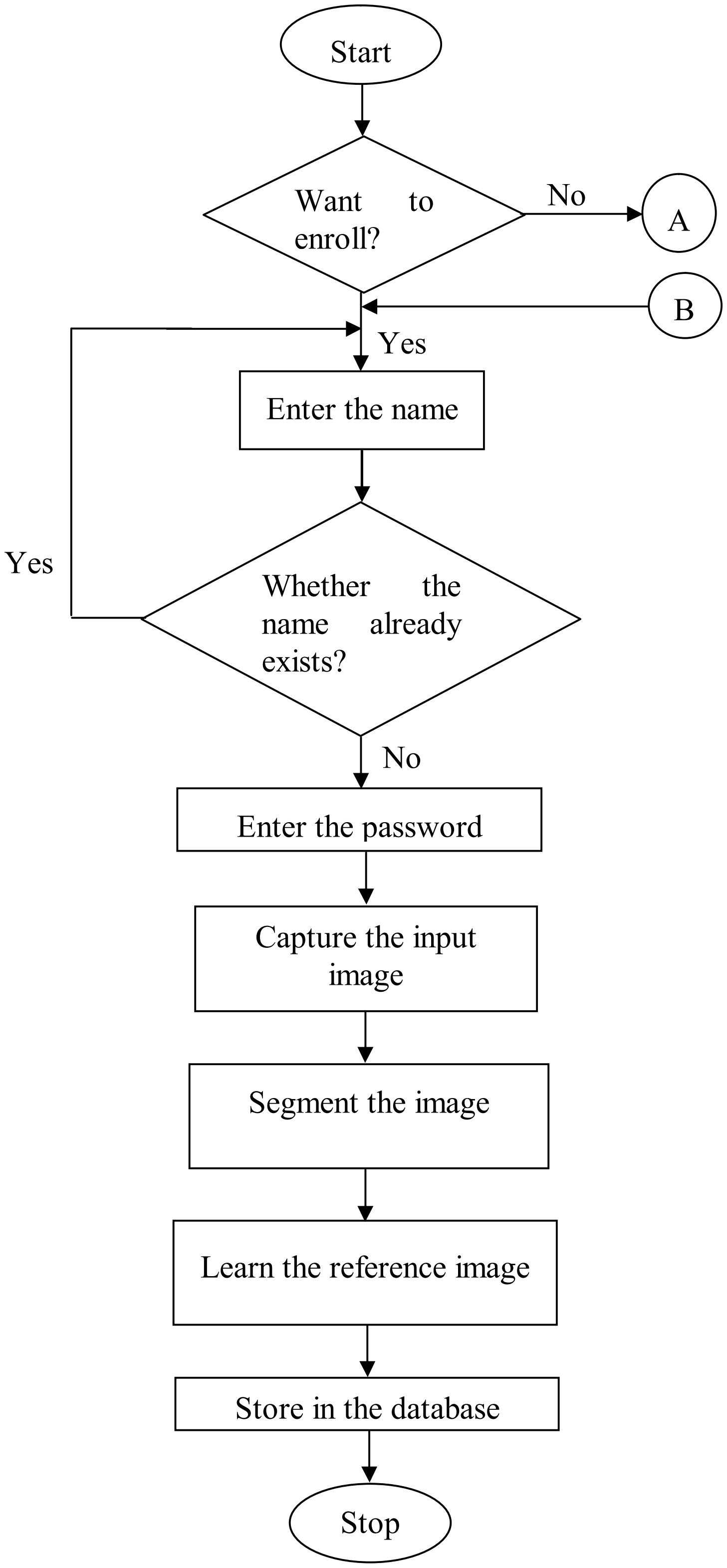


Figure 1. Flowchart of enrollment process

From the segmented image a template is extracted. The size of the extracted template is very critical for the accuracy of the system. Too small template may not provide enough distinction; on the other hand if the entire fingerprint is taken as a template then the elastic deformation of the query image may cause serious errors. Experiments have been conducted by considering the template sizes of 50×50, 100×100 and 200×200 pixels extracted from the centre of the image. The extracted template is fed to the image acquisition (IMAQ) learn pattern virtual instrument (VI). This VI creates a description of the template of the reference image that is to be compared with the data of the query image during the matching stage. In the learning phase a pseudo random sub-sampling is performed in which pixels are analysed by checking their surrounding neighborhood for uniformity and each pixel is classified according to how large the uniformity of its surrounding neighborhood is (e.g. 3×3, 5×5 and so on)[12]. This step will reduce the amount of calculations in the matching stage. The features of the reference image are extracted using the edge detection operation and the information is stored in a file along with the circular intensity profile of the reference image used in finding the rotated version of the image in the search/query image.

In the verification step (Figure 2), the name and password of the user is first checked. If they are incorrect the system gives a message: "You are not an enrolled user", and stops. If this stage is passed then the system demands for the fingerprint image in question and, after the preprocessing step, compares the two images (one in the reference pallet and the other the preprocessed image in question) with the help of the image acquisition (IMAQ) match pattern virtual instrument (VI), which matches the two images and calculates the threshold value. If the threshold value lies within the accepted limit the system will accept the identity of the user; otherwise, it will reject it.

Database

In the present work the fingerprint images from FVC2002/Db1_a database has been used to obtain the results. The database has been created by:

- Translating the fingerprint images by 1 pixel in both X and Y direction
- Rotating the fingerprint images by 1 degree
- Both translating and rotating the images by 1 pixel and 1 degree

The images are translated and rotated up to ±15 pixels and ±15 degrees. Figure 3 shows the original image (1_1 of FVC2002/Db1_a), its translated, rotated and translated plus rotated versions. In this way for every selected image of FVC2002/Db1_a, 90 images (30 translated, 30 rotated and 30 translated plus rotated) are obtained.

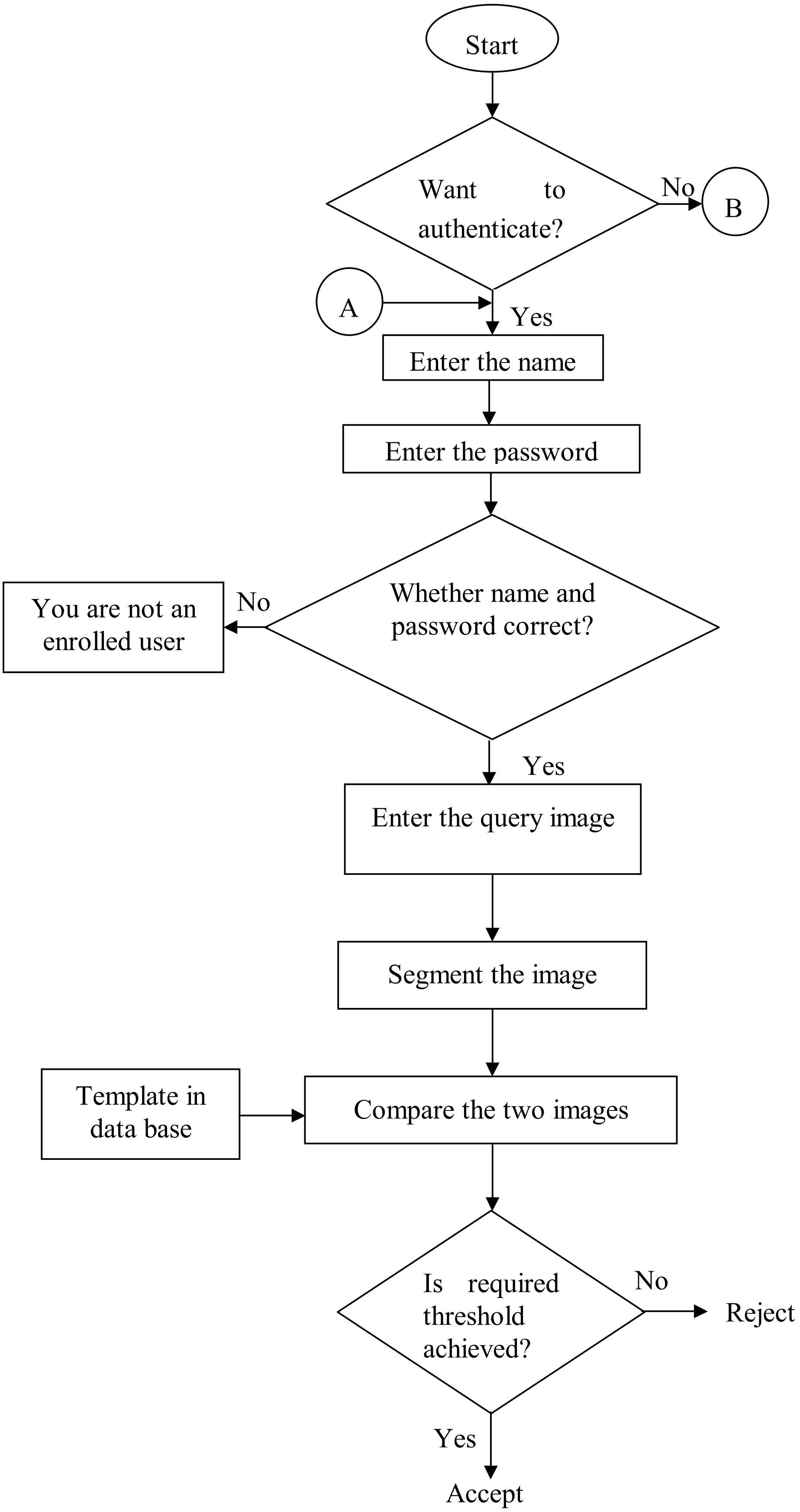
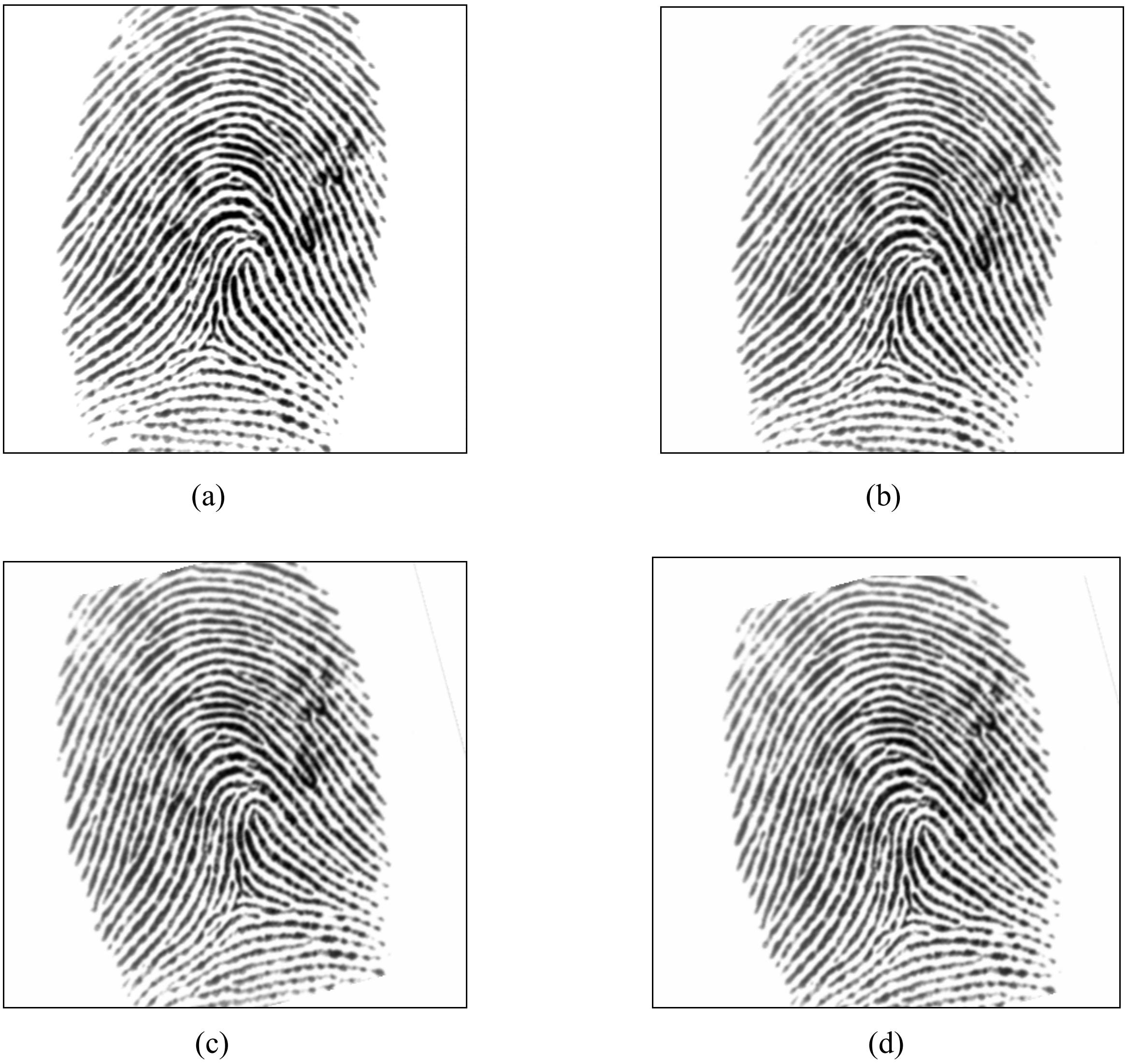


Figure 2. Flow chart of verification process

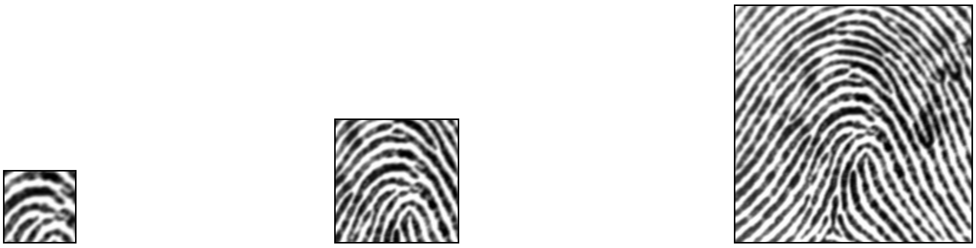


(a) (b) (c) (d)

Figure 3. (a) Original image; (b) translated image in X and Y direction; (c) rotated image; (d) rotated plus translated image

Results and Discussion

Two performance measures, namely false rejection rate (FRR) and false acceptance rate (FAR) were calculated for different images for comparison of results with different thresholds and window sizes. Experiments were performed by considering template size of 50×50, 100×100 and 200×200 pixels extracted from the centre of the image. Figure 4 shows the extracted images of template size 50×50, 100×100 and 200×200 pixels respectively, extracted from the centre of the image 1_1 of FVC2002/Db1_a database.



(a) (b) (c)

Figure 4. Template size of (a) 50×50 pixels, (b) 100×100 pixels, and (c) 200×200 pixels extracted from the centre of image 1_1

False rejection rate (FRR)

For the images which were only translated from the original image, no false rejection was found for any reference template size at any threshold value. However, when the images were rotated or translated plus rotated, the following results were obtained for different template learning images (Tables 1-6, and Figures 5-10). Tables 1-3 show % false rejection for different learning image sizes when only rotation was applied to the images, while Tables 4-6 represent the same when both rotation and translation were applied to the images. Figures 5-10 are the graphical representation of the different results obtained for the various learning image sizes.

Table 1. FRR for rotation-only learning images, size 200×200 pixels

Threshold	Image No.													
	1_1	2_1	3_1	4_1	5_1	6_1	7_1	10_1	11_1	12_1	13_1	14_1	15_1	16_1
700	0%	13%	37%	13%	0%	13%	0%	13%	13%	0%	7%	0%	7%	0%
750	3%	13%	37%	13%	0%	13%	0%	13%	17%	7%	7%	3%	7%	3%
800	3%	13%	40%	17%	0%	13%	0%	13%	30%	20%	7%	3%	7%	13%
850	3%	13%	50%	47%	0%	23%	0%	13%	37%	37%	17%	7%	20%	20%
900	10%	23%	73%	73%	7%	37%	7%	27%	43%	63%	60%	37%	37%	27%

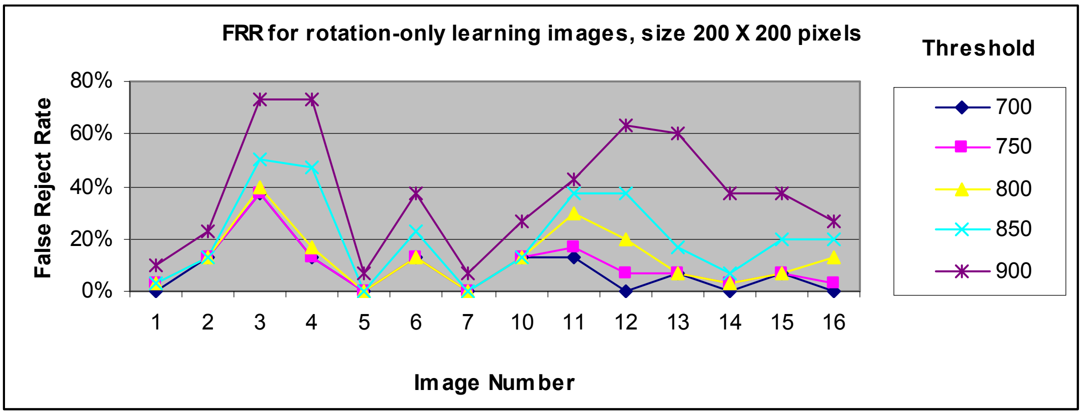


Figure 5. FRR for rotation-only learning images, size 200×200 pixels, at various thresholds

Table 2. FRR for rotation-only learning images, size 100 × 100 pixels

Threshold	Image No.													
	1_1	**2_1**	**3_1**	**4_1**	**5_1**	**6_1**	**7_1**	**10_1**	**11_1**	**12_1**	**13_1**	**14_1**	**15_1**	**16_1**
700	0%	0%	3%	0%	0%	0%	3%	13%	0%	0%	0%	0%	0%	0%
750	0%	0%	3%	0%	0%	7%	7%	13%	0%	0%	0%	0%	0%	0%
800	0%	3%	13%	0%	0%	13%	20%	13%	0%	0%	0%	0%	3%	0%
850	0%	3%	27%	3%	0%	17%	43%	13%	10%	0%	0%	0%	17%	17%
900	7%	20%	37%	3%	33%	37%	87%	17%	30%	10%	3%	7%	53%	57%

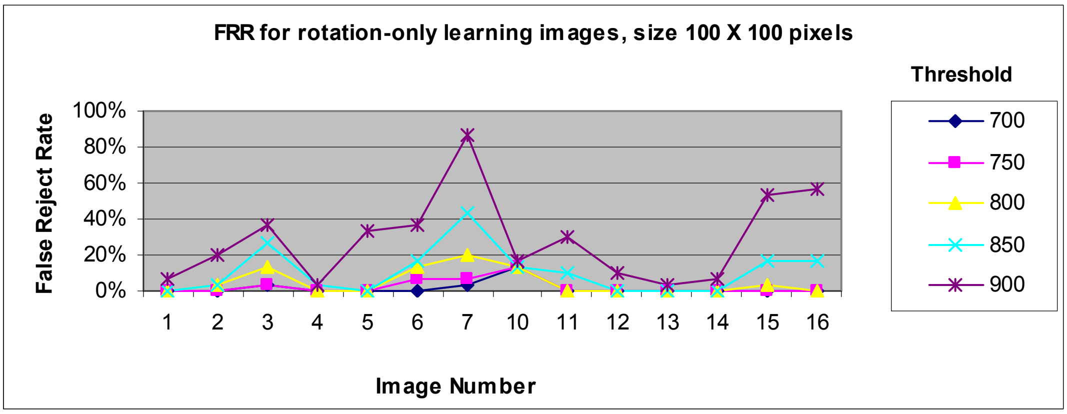


Figure 6. FRR for rotation-only learning images, size 100 × 100 pixels, at various thresholds

Table 3. FRR for rotation-only learning images, size 50 × 50 pixels

Threshold	Image No.													
	1_1	**2_1**	**3_1**	**4_1**	**5_1**	**6_1**	**7_1**	**10_1**	**11_1**	**12_1**	**13_1**	**14_1**	**15_1**	**16_1**
700	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
750	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
800	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
850	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	10%	3%
900	0%	17%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	33%	10%

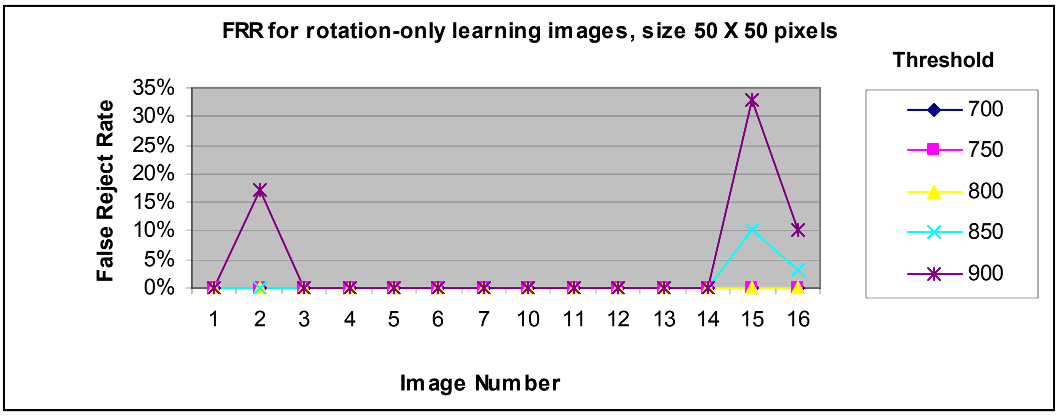


Figure 7. FRR for rotation-only learning images, size 50 × 50 pixels, at various thresholds

Table 4. FRR for rotation-and-translation learning images, size 200 × 200 pixels

Threshold	**Image No.**													
	1_1	**2_1**	**3_1**	**4_1**	**5_1**	**6_1**	**7_1**	**10_1**	**11_1**	**12_1**	**13_1**	**14_1**	**15_1**	**16_1**
700	0%	13%	27%	13%	0%	13%	0%	13%	13%	0%	7%	0%	7%	0%
750	3%	13%	27%	13%	0%	13%	0%	13%	17%	7%	7%	3%	7%	3%
800	3%	13%	30%	17%	0%	13%	0%	13%	30%	20%	7%	3%	10%	13%
850	3%	13%	40%	47%	0%	23%	0%	13%	37%	40%	17%	7%	20%	20%
900	10%	23%	67%	73%	7%	33%	7%	23%	50%	53%	60%	33%	37%	27%

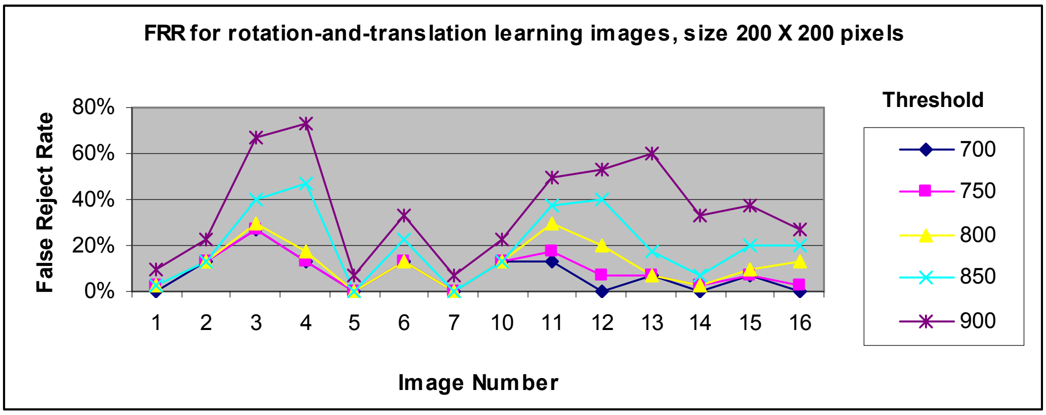


Figure 8. FRR for rotation-and-translation learning images, size 200 × 200 pixels, at various thresholds

Table 5. FRR for rotation-and-translation learning images, size 100 × 100 pixels

Threshold	**Image No.**													
	1_1	**2_1**	**3_1**	**4_1**	**5_1**	**6_1**	**7_1**	**10_1**	**11_1**	**12_1**	**13_1**	**14_1**	**15_1**	**16_1**
700	0%	0%	0%	0%	0%	0%	3%	13%	0%	0%	0%	0%	0%	0%
750	0%	3%	0%	0%	0%	7%	3%	13%	0%	0%	0%	0%	0%	0%
800	0%	7%	10%	0%	0%	10%	17%	13%	0%	0%	0%	0%	3%	0%
850	3%	7%	20%	3%	0%	13%	43%	13%	10%	0%	0%	0%	20%	17%
900	10%	23%	27%	3%	33%	30%	83%	17%	30%	10%	7%	10%	53%	57%

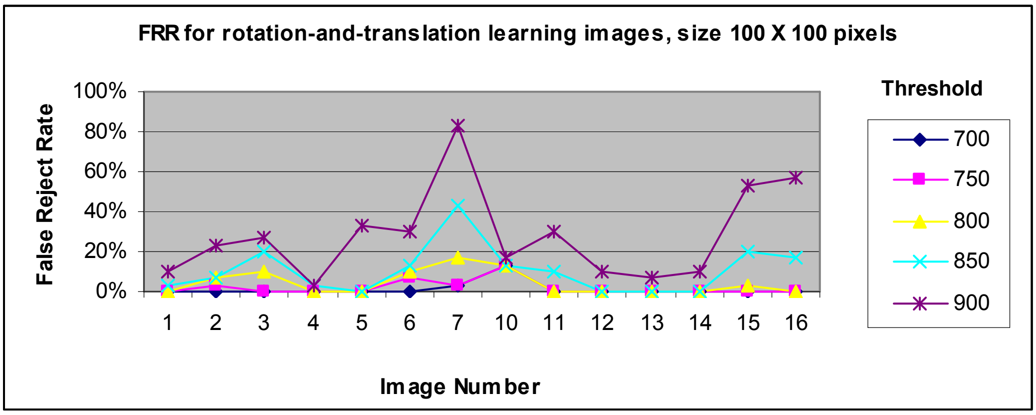


Figure 9. FRR for rotation-and-translation learning images, size 100 × 100 pixels, at various thresholds

Table 6. FRR for rotation-and-translation learning images, size 50 × 50 pixels

Threshold	**Image No.**													
	1_1	**2_1**	**3_1**	**4_1**	**5_1**	**6_1**	**7_1**	**10_1**	**11_1**	**12_1**	**13_1**	**14_1**	**15_1**	**16_1**
700	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
750	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
800	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	3%	0%
850	0%	0%	0%	0%	0%	0%	3%	3%	0%	0%	0%	0%	17%	3%
900	0%	20%	3%	0%	0%	0%	3%	7%	0%	0%	3%	0%	37%	10%

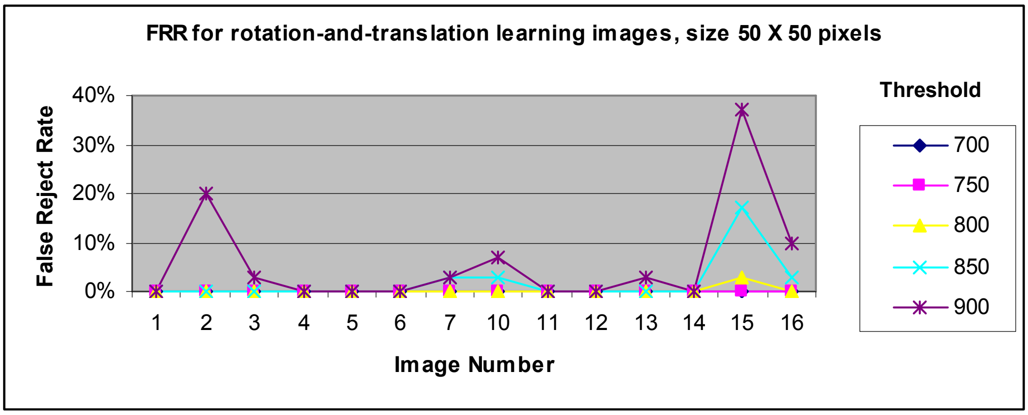


Figure 10. FRR for rotation-and-translation learning images, size 50 × 50 pixels, at various thresholds

False acceptance rate (FAR)

No false acceptance was found for the learning image sizes of 100 × 100 and 200 × 200 pixels up to threshold of 700. However, for the learning image size of 50 × 50 pixels the following results were observed (Table 7 and Figure 11). Table 7 represents % false acceptance at various thresholds for the learning image size of 50 × 50 pixels while Figure 11 is the graphical representation of the results from Table 7.

Table 7. FAR for learning images, size 50 × 50 pixels

Threshold	**Image No.**													
	1_1	**2_1**	**3_1**	**4_1**	**5_1**	**6_1**	**7_1**	**10_1**	**11_1**	**12_1**	**13_1**	**14_1**	**15_1**	**16_1**
700	0%	25%	90%	50%	3%	68%	70%	75%	88%	100%	13%	5%	23%	0%
750	0%	10%	75%	30%	0%	40%	60%	68%	53%	90%	8%	0%	3%	0%
800	0%	5%	53%	5%	0%	13%	30%	33%	35%	80%	8%	0%	0%	0%
850	0%	0%	28%	3%	0%	8%	15%	10%	13%	60%	0%	0%	0%	0%
900	0%	0%	3%	0%	0%	0%	5%	0%	0%	25%	0%	0%	0%	0%

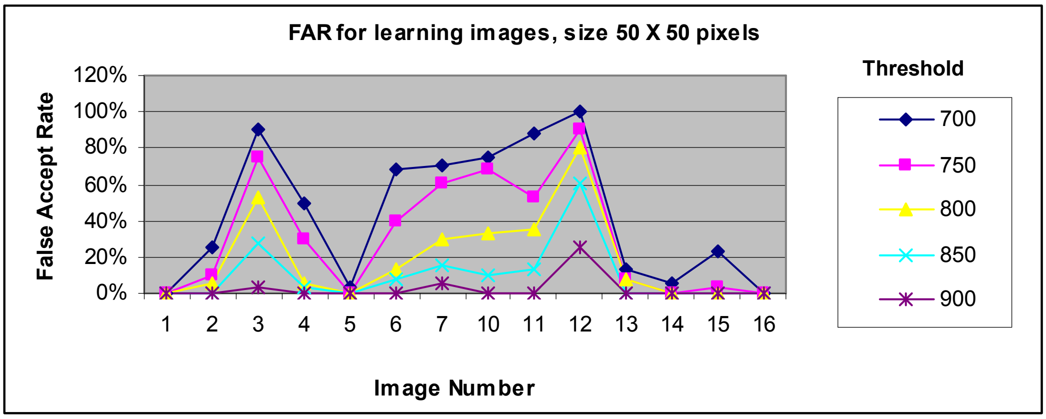


Figure 11. FAR for learning images, size 50 × 50 pixels, at various thresholds

From the above results for FFR and FAR, it is observed that as the threshold value increases, so does the % false rejection, although for the smaller learning images (50 × 50 pixels) the % false rejection is less in comparison to that for the larger learning images (100 × 100 and 200 × 200 pixels). However, no false acceptance was observed (down to threshold of 700) for the learning image sizes of 100 × 100 and 200 × 200 pixels, although for the 50 × 50 pixel learning images a considerable number of false acceptance was observed. The above results are expected as smaller images contain less information in comparison to larger images, and thus the probability of more than one image having the same little information is greater.

Conclusions

An image-based fingerprint verification system has been developed and checked for validity by employing images from FVC2002/Db1_a database. The success rate of the verification system is highly dependent on the threshold value and size of the template used for the learning stage. Smaller- sized learning images have lower false rejection rate and higher false acceptance rate, while larger-sized learning images have higher false rejection rate and lower false acceptance rate. Moreover, the higher the value of the threshold is, the higher the false rejection and the lower the false acceptance become. So, a compromise has to be made between false acceptance and false rejection. The experimental results for different fingerprints and various learning image sizes reveal that a 100 × 100 learning image size and a threshold value of 700 (1000 being the perfect match) is a good compromise for the false acceptance and false rejection rate.

References

1. G. Hribernig, D. Tukulj, and M. Luetic, "Biometric- easy access to networked word", International Conference and Workshop on Telecommunication and Mobile Computing, Graz University of Technology, Austria, **2001**.
2. A. K. Jain, L. Hong, S. Pankanti, and R. Bole, "An identity–authentication system using fingerprints", Proceedings of the IEEE, **1997,** *85*, 1365-1388.

3. A. K. Jain, U. Uludag, and R. L. Hsu, "Hiding a face in a fingerprint image", Proceedings of IEEE International Conference on Pattern Recognition, **2002**, *3*, 756-759.
4. A. K. Jain, A. Ross, and S. Pankanti, "Biometrics: a tool for information security", *IEEE Transact. Information Forensics and Security*, **2006**, *1*, 125-142.
5. J. Feng, "Combining minutiae descriptor for fingerprint matching", *J. Pattern Recognition Soc.*, **2008**, *41*, 342-352.
6. P. Reid, "Biometric for Network Security",1st Indian Reprint, Pearson Education, New Delhi, **2004.**
7. E. Spinella, "Biometrics Scanning Technologies: Finger, Facial and Retinal Scanning", SANS Technology Institute, San Francisco, **2002**.
8. D. Maio and D. Maltoni, "Direct gray scale minutiae detection in fingerprints", *IEEE Transact. Pattern Analysis and Machine Intelligence*, **1997**, *19*, 27-40.
9. B. C. Seow, S. K. Yeoh, S. L. Lal, and N. A. Abu, "Image based fingerprint verification", Proceedings of IEEE Conference on Research and Development, Malaysia, **2002,** 58-61.
10. A. M. Bazen, G. T. B. Verwaaijen, S. H. Gerez, L. P. J. Veelenturf, and B. Zwaag, "Correlation-based fingerprint verification system", Proceedings of Conference on Research on Integrated Systems and Circuits, Netherlands, **2000**, 205–213.
11. J. Travis, "LabVIEW for Everyone", 2nd Edn., Prentice Hall, NJ, **2002**.
12. "IMAQ Vision Concepts Manual", National Instruments Corporation, Austin, **2000**.