Performance Evaluation of Fingerprint Recognition and Authentication Using the Neural Network Command Line

Mukesh Kumar   **Arun Jain**
Student of CSE Department, HCTM   C.S.E. Department, HCTM
Haryana, India   Haryana, India

Abstract- Fingerprint authentication/identification is a good of biometric technique for identity recognition. It is good and very important technique used in forensic research for investigation purpose. Here in my proposed work I have implemented an algorithm for personal authentication of a person by his/her fingerprints using Neural Network and compare it with SVM technique on the basis of CCR. Here I have considered the fingerprint of a person as an image and after the fingerprints of many persons we have created a database for all the images. Whenever we have two check the authenticity of a person then he/she has to scan his/her finger by a scanner. Then this input fingerprints will be matched with the databases for matching for recognition. Because, now a fingerprint is an image, that's why nprtool has been used. The experiment result of this research work will achieve a good performance on these databases. After completed all the required steps, the result shows improvements in MSE and PSNR and also perform cumulative cost results over the SVM technique.

Keywords- Fingerprint, NN, SVM, MSE, PSNR, CCR.

I.   INTRODUCTION

A biometrics system can be used for authentication and recognize identity of a person. For recognition and authentication identity, we can use the features of the physics or behavior (how a person behave) of a person. Voice and Signature can be choose for this purpose which is the part of behavioral biometric technique or we can go for physiological features such as iris, palmprints, face and fingerprints as shown in figure 1. Biometrics is a Greek word and the meaning is measure the life. Bios means life and metricos means measure. All the biometric techniques provide good way of security for authentication or identification. A person can be identified/recognize or authenticate by:

- An ID card with a photograph.
- A code number or a password.
- A person's biological makeup of behavior, such as a fingerprint, a facial image, iris, palmprints or a signature.
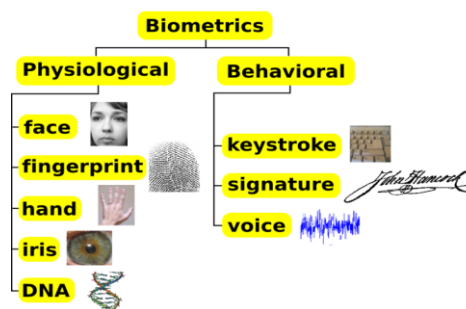

Figure 1 : Factors of a Biometric Authentication System [1]

II.   LITERATURE REVIEW

[2] The author worked on fingerprint and he proposes a feature extraction algorithm based on minutiae which is more accurate and much faster than our earlier fingerprint recognition algorithm. [3] The researcher has worked on sticky finger also called gummy finger, and reports that gummy finger, namely artificial fingers that are easily made available and were accepted by extremely high rates. [4] They propose various fusion techniques for face and fingerprint authentication which is considered as multimodal biometric system. [5] This research presents an advance approach for identification, which uses finger surface feature as a biometric identifier and dense range data images of the hand, we calculate the curvature-based surface representation, shape index for all the fingers. [6] They propose a fingerprint authentication scheme and are protected by a construct called a Fuzzy Extractor. They use Pin Sketch and apply to the minutiae for quantizing and digitally for the minutiae measurements so that a construct called can be applied to the minutiae. [7] In this paper, the authors have developed a prototype model for automatic identity-authentication system which uses fingerprints for authentication. [8] This study describes a biometric fingerprint identification system and later it is implementation to establish the identity of a person. The approach based on matching the fingerprint on two parameter minutia and furrows.

III. METHODOLOGY

Biometric technique fingerprint authentication is base on matching the extracted features of input fingerprint with the database stored templates, to do this; the algorithm finds a central point in the fingerprint image and centers on that. In a pattern-based algorithm, the template contains the type, size, and orientation of patterns within the aligned fingerprint image. The candidate fingerprint image is graphically compared with the template to determine the degree to which they match. Here we are implementing our proposed algorithm which will use Neural Network Pattern recognition tool for matching input image with the database image and we have also compare it with SVM technique. When the input image is matched then it will display the results. The whole proposed process and the results of the research work are explain in the experimental and results section.

IV. EXPERIMENTAL RESULTS

When the proposed algorithm is applied and checked to a scanned input fingerprint image for recognition of identity. We found that the results are good and also more secure good SVM algorithms and also gives us better CCR(%) values. The MSE and PSNR values are also improved.

As per our proposed algorithm, the whole process of recognize and identification of fingerprint is divided in five steps parts. Let us see the phase wise experimental result using NN technique.

A. loading a scanned fingerprint image for recognition
[path,filename]=uigetfile('.jpg', 'Select an Image');*

Figure 2: Scanned input loaded fingerprint image

B. Edges detection and Binarization of scanned fingerprint image
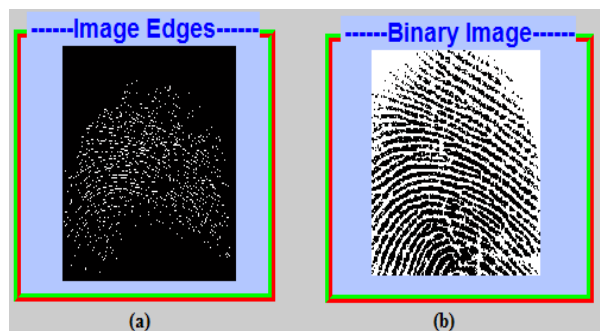*img1=edge(img1);   Img1=im2bw(img1);*

Figure 3: (a) edges of loaded fingerprint image (b) Binarization of fingerprint Image.

C. Extract the features of binary image using SURF method.
Points1=detectSURFFeatures(k1);
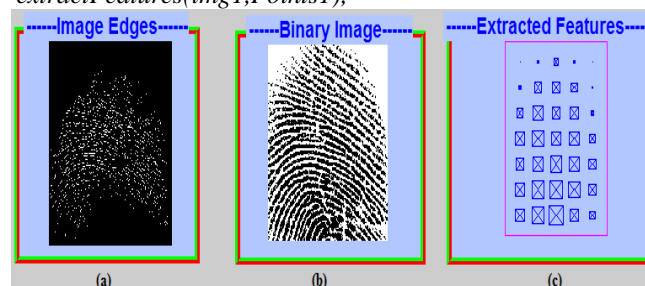*[features1, valid_Points1]=extractFeatures(img1,Points1);*

Figure 4: (a) detected edges (b) binary Image (c) Extracted features for matching

D. **In this phase code for fingerprint matching using NN Pattern Recognition Tool (nprtool) will work for the matching of input and database template images with the help of extracted features by "Surf Feature Extraction" and recognition using NN.**

nnstart;

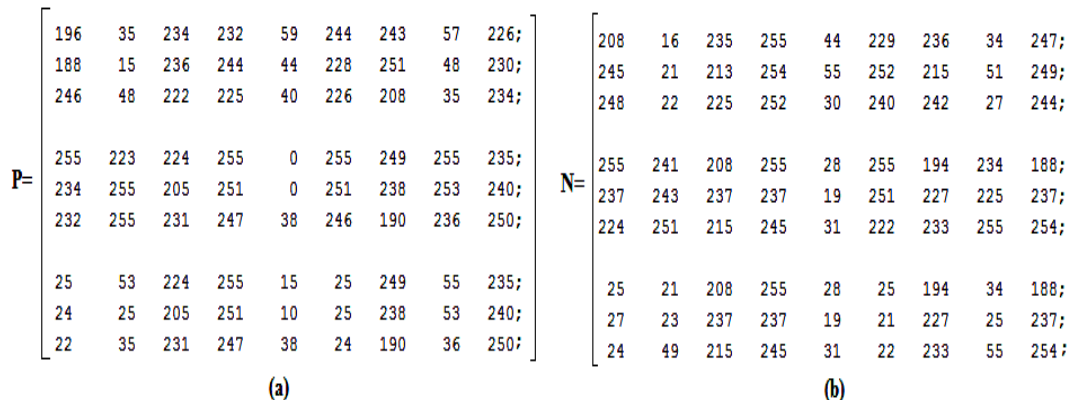*index_Pairs=matchFeatures(features1,features2)*

[a_d b]=size(index_Pairs)

$$P=\begin{bmatrix} 196 & 35 & 234 & 232 & 59 & 244 & 243 & 57 & 226; \\ 188 & 15 & 236 & 244 & 44 & 228 & 251 & 48 & 230; \\ 246 & 48 & 222 & 225 & 40 & 226 & 208 & 35 & 234; \\ \\ 255 & 223 & 224 & 255 & 0 & 255 & 249 & 255 & 235; \\ 234 & 255 & 205 & 251 & 0 & 251 & 238 & 253 & 240; \\ 232 & 255 & 231 & 247 & 38 & 246 & 190 & 236 & 250; \\ \\ 25 & 53 & 224 & 255 & 15 & 25 & 249 & 55 & 235; \\ 24 & 25 & 205 & 251 & 10 & 25 & 238 & 53 & 240; \\ 22 & 35 & 231 & 247 & 38 & 24 & 190 & 36 & 250; \end{bmatrix}$$

$$N=\begin{bmatrix} 208 & 16 & 235 & 255 & 44 & 229 & 236 & 34 & 247; \\ 245 & 21 & 213 & 254 & 55 & 252 & 215 & 51 & 249; \\ 248 & 22 & 225 & 252 & 30 & 240 & 242 & 27 & 244; \\ \\ 255 & 241 & 208 & 255 & 28 & 255 & 194 & 234 & 188; \\ 237 & 243 & 237 & 237 & 19 & 251 & 227 & 225 & 237; \\ 224 & 251 & 215 & 245 & 31 & 222 & 233 & 255 & 254; \\ \\ 25 & 21 & 208 & 255 & 28 & 25 & 194 & 34 & 188; \\ 27 & 23 & 237 & 237 & 19 & 21 & 227 & 25 & 237; \\ 24 & 49 & 215 & 245 & 31 & 22 & 233 & 55 & 254; \end{bmatrix}$$

(a)   (b)

Figure 5: (a) training image matrix for NN (b) Testing Image matrix for NN

$$T=\begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}$$
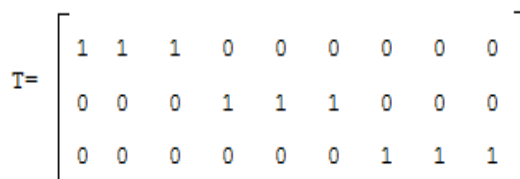
Figure 6: Target image matrix for NN

Now the next step in NN process is to apply the weights between input, output and hidden Neurons. I have used 5000 time iteration for better resuts and better MSE and PSNR values.

a=0.3; b=-0.3 ;

*W1=a + (b-a) *rand(S1,R);*

*W2=a + (b-a) *rand(S2,S1);*

*n1=W1*P;*

A1=logsig(n1);

*n2=W2*A1;*

A2=logsig(n2);

e=A2-T;

```
Command Window
Iteration : 1010      mse :    0.000509
Iteration : 1041      mse :    0.000508
Iteration : 1042      mse :    0.000507
Iteration : 1043      mse :    0.000507
Iteration : 1044      mse :    0.000506
Iteration : 1045      mse :    0.000506
Iteration : 1046      mse :    0.000505
Iteration : 1047      mse :    0.000504
Iteration : 1048      mse :    0.000504
Iteration : 1049      mse :    0.000503
Iteration : 1050      mse :    0.000502
Iteration : 1051      mse :    0.000502
Iteration : 1052      mse :    0.000501
Iteration : 1053      mse :    0.000501
Iteration : 1054      mse :    0.000500
Iteration : 1055      mse :    0.000499
Iteration : 1056      mse :    0.000499
Iteration : 1057      mse :    0.000498
Iteration : 1058      mse :    0.000498
Iteration : 1059      mse :    0.000497
Iteration : 1060      mse :    0.000496
Iteration : 1061      mse :    0.000496
Iteration : 1062      mse :    0.000495
>>
```

```
Command Window
Columns 1 through 8

   0    0    0    0    0    0    0    0

Columns 9 through 16

   0    0    0    0    0    0    0    0

Columns 17 through 24

   0    0    0    0    0    0    0    0

Columns 25 through 26

   0   13

i =   6

PERSON  RECOGNISED
>>
```
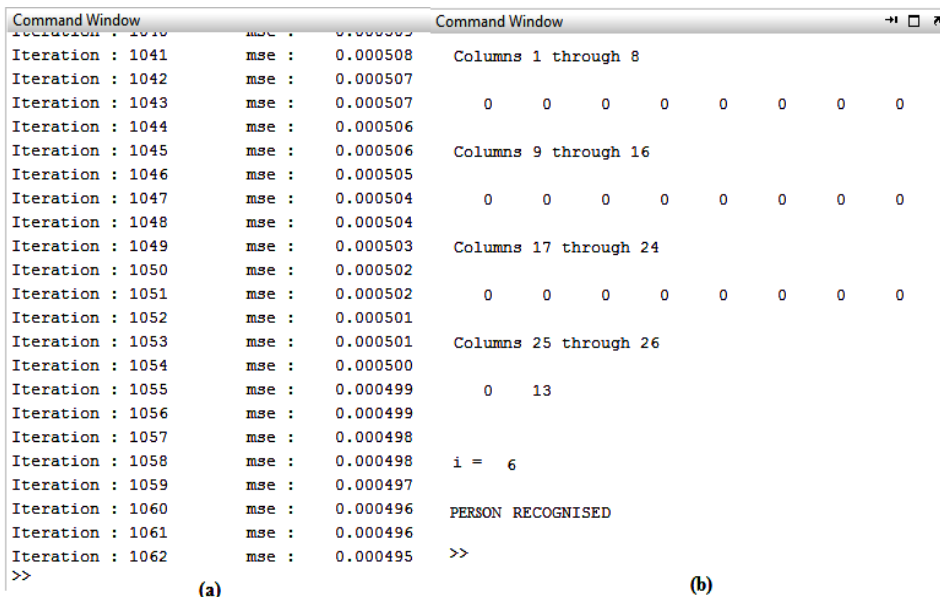
(a)   (b)

Figure 7: (a) NN Process (b) Matching result

E.   Finally Results will be displayed as the picture of the identified user and are analyzed between input fingerprint and recognized fingerprint images using MSE and PSNR and CCR.
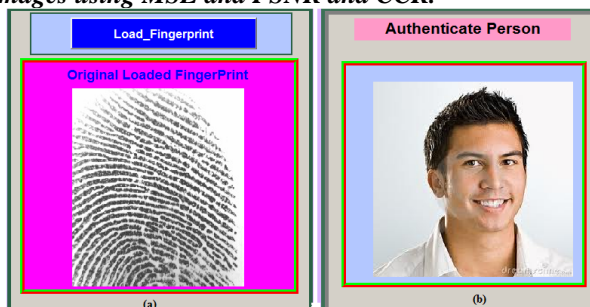
Figure 8: (a) Loaded fingerprint (b) Matches with (Authenticate Person).
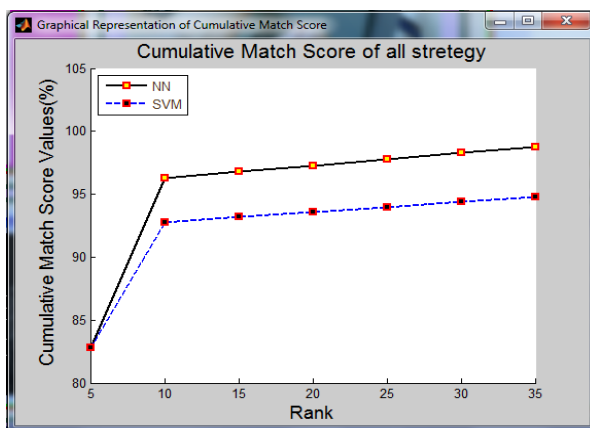
Figure 9: Cumulative match score and compare with prior techniques.

	CCR%
NeuralNetwork	98.7801
SupportVectorMachine	94.7801

(a)

	MSE	PSNR
Proposed	2.3300e-05	6.4260e+10

(b)

Figure 10: (a) Comparison on the basis of CCR (b) MSE and PSNR Values.

V.   CONCLUSION

Biometric fingerprint technique provides good security for recognizing the identity of a person. Biometric data is sensitive and we may need to protect it. It is certain that biometrics based identification will have a profound influence on the way we conduct our daily business. It is also certain that, as the most mature and well understood biometric, fingerprints will remain an integral part of the preferred biometric-based identification solutions in the years to come. At the last we found that our technique is good and providing better results in comparison with the SVM technique. In future we can propose a new algorithm on fingerprint authentication by combining both NN and SVM together to improve the result in terms of CCR values. The same work using NN and compare it with SVM can be implemented with fusion techniques (multi-biometric system/multi-model system). We can use different fusion technique and can apply any one technique on fingerprint with the face of a person for better security reasons.

ACKNOWLEDGMENT

REFERENCES
[1]   http://google/800px-Biometrics_traits_classification.jpg.
[2]   Ravikanth, C., Kumar, A.: Biometric authentication using finger-back surface. In: Proc. CVPR, pp. 1–6 (2007).
[3]   Anil Jain and Ling Hong "Identity authentication using Fingerprints" 2002.
[4]   T. sutomu Matsumoto" Impact of Artificial "Gummy" Fingers on Fingerprint Systems Proceedings of SPIE Vol. 4677 (2002).
[5]   R. Snelick, M. Indovina, J. Yen, and A. Mink. Multimodal Biometrics: Issues in Design and Testing. In Proceedings of Fifth International Conference on Multimodal Interfaces, pages 68–72, Vancouver, Canada, November 2003.
[6]   Woodard, D.L., Flynn, P.J.: Finger surface as a biometric identifier. Computer Vision and Image Understanding 100(3), 357–384 (2005).

[7]   A. Arakala, J. Jeffers, and K. J. Horadam. Fuzzy Extractors for Minutiae-Based Fingerprint Authentication. In Proceedings of Second International Conference on Biometrics, pages 760-769, Seoul, South Korea, August 2007.

[8]   Mr. Ratnakar anandrao kharade, Mr. M.S. Kumbhar / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 2, Issue 6, November- December 2012.

[9]   Ravi Bhusan tiwari and Sanjay Sharma, "Biometric authentication using fingerprint " in Youth Education and Research Trust (YERT), Vol. 1(8) January 2013.