International Journal of Latest Trends in Engineering and Technology Vol.(8)Issue(3), pp.240-247 DOI: http://dx.doi.org/10.21172/1.83.036 e-ISSN:2278-621X

#### NOVEL MULTI-MODEL BIOMETRIC FUSION Δ **APPROACH USING PALM-PRINT & FACE BIOMETRIC**

Navdeep<sup>1</sup>, Surinder<sup>2</sup>

Abstract - As we know that fingerprint authentication for individual identification is a popular method of biometric system, similarly palm-print can be good technique for authenticating a person's identity, but for good results, if we combine two or more biometric techniques then the security can be increased. Here we have used a multi-biometric model for authentication and recognition of an individual using neural network and Support Vector Machine. To overcome the security issues, my proposed approach is to combine the face recognition method and the Palm-print method of biometric system. Firstly the face from the first object will be detected then the second palm-print object will be loaded. Secondly both the detected face and the palm-print object image will be merged using fusion techniques and then further processing will extract their features for matching process. The last step is to classify and recognize using combined NN and SVM techniques to increase the accuracy, security and to enhance the performance over previous technique (Individually NN and SVM) will be increased compared to previous work results.

Keywords- Multi- Model Biometric, Face, Palm-print, MSE, PSNR, CCR

#### **INTRODUCTION** Т

In biometrics system is recognition and the identification of an individual on the basis of physiological or behavioral characteristics [8-16] of a person such as iris, palmprints, face, voice and palm-prints as shown in figure 1. Biometrics word arrived from the Greek words bios (Life) and metricos (Measure). It is basically a pattern-recognition system that is used to identify a user and relies on something that is a part of a person's biological makeup of behavior, such as a face, signature or a palm-print.



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

The problem of resolving the identity of a person can be categorized into two fundamentally distinct types of problems with different inherent complexities. Verification (authentication) refers to the problem of confirming or denying a person's claimed identity (Am I who I claim I am?). Identification (Who am I?) refers to the problem of establishing a subject's identity - either from a set of already known identities (closed identification problem) or otherwise (open identification problem).

#### П. FACIAL RECOGNITION

Department of Computer Science & Engineering Singhania University, Jhunjhunu, Rajasthan, INDIA <sup>2</sup> Dept. of Computer Science & Engineering, HCTM Technical Campus, Kaithal (Haryana)

Facial recognition is one of the most common biometric methods of identification. Here face is detected from a person image and then features are extracted from the face image. In addition, the method of acquiring face images is non-intrusive. Two primary approaches to the identification based on face recognition are the following: (i) Transform approach [2, 3]: the universe of face image domain is represented with a set of orthonormal basis vectors. Nowadays, eigenfaces is the most popular basis vector.

# III. PALM-PRINT

Palm-print refers to an image acquired of the palm region of the hand. It can be either an online image (i.e. taken by a scanner or CCD) or offline image where the image is taken with ink and paper [4], [5]. Palm-print recognition is also a kind of "image acquisition". If someone wants to check someone else identity, then he/she has to scan the fingers using a scanner for the palm-prints. Multiple images of the same palm have been captured. Now the retrieve palm-prints will be an image of the palm-print and will used in the identification purpose. In this process the main concentration is to capture the centre point of the palm-print, which contains many of the unique features. After capturing all images of the palm-print, the next step is to binary conversion the images (Figure 2, Figure 3).



Figure 2: Different samples of palm-prints [5].



Figure 3: Lower palm prints of different human being.

# IV. LITERATURE REVIEW

The purposes of biometric fusion are to enhance system security, efficiency, applicability, and robustness. Some types of fusion have been used successfully for years in large scale fingerprint identification systems. [7] Combined two biometric techniques verification system fingerprint and voice. The fusion decrease privacy concerns. The Accuracy is increased in comparison of the previous results for voice verification over the same speaker database. [8] Proposes a method of authentication and identification using face and palm-print techniques. By amalgamate the palm-print and face features increases accuracy, robustness of the biometric authentication. In this paper three fusion techniques (PCA, DCT & DWT) are analyzed and DWT will be established as a most suited fusion technique for multi model biometric system of iris, palm print, face and signature [17]. The fused image is then extracted by using Inverse Discrete Wavelet transform [9].

# V. PROPOSED ARCHITECTURE

As in fingerprint matching technique matching algorithms compare the previously stored image templates against a candidate fingerprints for authenticity. My proposed work is same but with multi-biometric system model using NN\_SVM [11]. In this proposed algorithm my concentration is on physiological fingerprint and face recognition methods. I have considered both objects as images, fused and stored those images in a database as templates.

MULTI-MODEL BIOMETRIC	FUSION ARCHITECTURE (USING F	ALM-PRINT AND FACE)
LOAD MODULE	FUSION MODULE	MATCHING MODULE
FIRST OBJECT FACE LOAD FIRST IMAGE FACE DETECTION (vision.CascadeObjectDetector) FACE EXTRACTION (method imcrop) SECOND_OBJ_PALM-PRINT LOAD PALM-PRINT	OUTPUT_OBJ_1 (Grayscale Extracted Face ) OUTPUT_OBJ_2 (Grayscale Palm-Print) FUSION (Wavelet Decomposition at level 5 using db2 by Mean method)	PRE-PROCESSING (Binarization of image) EXTRACT FEATURES (DetectSURFFeatures) RECOGNITION (Using NN_SVM;MatchFeatures)

Figure 4: Multi-biometric Proposed Architecture

Whenever we have to check the authenticity of a person we will scan his fingerprint and photo using a scanner/digital camera. These new objects will be fused and compared with our created database using NN and SVM. The complete process of this proposed work is divided into three main modules load module, Fusion module and the Matching module as shown in figure 4 and the flow chart of the proposed work is shown in figure 5.



Figure 5: Flowchart of proposed work

# VI. EXPERIMENTAL RESULTS

Here I have used MATLAB 12.0 GUI for my experiment and results. When I tried to check the authenticity of a person using my multi-biometric system model then I found, that it always provides good (CCR%) results in comparison to NN and SVM individually and we also find improvements in MSE and PSNR values. Let us see the working of all the modules and the results of this research work;

# A. Load module

This module is divided into two segments (First Object Face and Second Object Finger). (Figure 6)

# i) First Segment (First\_Object\_Face)

- 1. The first step of this segment is to load the image of a person as an input image.
- 2. Now the face will be detected from the loaded image.
- 3. After detect the face from the input image next step is to extract the detected face from the image.



Figure 6: (a) loaded image (b) Detected face (c) Extracted face

### ii) Second Segment (Second\_Object\_Fingerprint)

1. Here the Fingerprint of the same person, whose image is loaded in the first segment phase, is loaded figure 7 showing the loaded fingerprint..



Figure 7: Loaded Fingerprint of the same person.

# B. Fusion Module

For fusion we need at least two images, here we will take first gray scale image of extracted face from loaded face image and second gray scale image of loaded fingerprint image as shown in figure 8.



Figure 8: (a) first image (Extracted face) (b) second image ( Loaded Fingerprint).

The next step is to apply our fusion method. Here I have used wavelet decomposition at level 5 by db2 using 'mean' method. After fusion of two images the new image figure will be saved into the database for further matching process. (Figure 9)

```
wfusimg(bgImg,fgImg,'db2',5,'mean','mean');
bgImg=Background Image fgImg=Front Image
```



Figure 9: (a) Extracted Face (b) Fingerprint (c) Fused Image

### C. Matching Module

- 1. First we well convert our fused image into binary (b/w, 0/1) image. As shown in figure 10(a).
- 2. After binary conversion the main features will be extracted for matching purpose using Surf feature and Extract feature methods figure 10(b).



Figure 10: (a) Binary Image (b) Extracted Features

```
points1=detectSURFFeatures(Image);
[feature,valid_points1]=extractFeatures(Image,points1);
```

Match extracted features with database template and recognize using proposed technique (NN\_SVM method) as shown in the figure 11, NN iteration and MSE Values in 12 and final result in figure 13.

nnstart;

```
df1=dlogsig(n1,A1(:,i));
                                   p=10*log(10);
df2=dlogsig(n2,A2(:,i));
                                   psnr(i)=p*(((255).^2)/mse);
s2 = -2*diag(df2) * e(:,i);
s1 = diag(df1) * W2'* s2;
                                   trainset=[(1:20);(51:70);(101:120)];
W2 = W2-0.1*s2*A1(:,i)';
                                   testset=[(21:50);(71:100);(121:150)];
b2 = b2 - 0.1 + s2;
W1 = W1-0.1*s1*P(:,i)';
b1 = b1-0.1*s1;
A1(:,i)=logsig(W1*P(:,i),b1);
A2(:,i)=logsig(W2*A1(:,i),b2);
error =0.5*mean(mean(e.*e));
mse=error;
                                                      (b)
              (a)
```



test sets.

Iteration	-	1236	mse	-	0.024675
Iteration	=	1237	mse	=	0.024626
Iteration	=	1238	mse	=	0.024577
Iteration	=	1239	mse	=	0.024528
Iteration	=	1240	mse	=	0.024479
Iteration	=	1241	mse	=	0.024431
Iteration	=	1242	mse	=	0.024382
Iteration	=	1243	mse	=	0.024334
Iteration	=	1244	mse	=	0.024285
Iteration	=	1245	mse	=	0.024237
Iteration	=	1246	mse	=	0.024189
Iteration	=	1247	mse	=	0.024141
Iteration	=	1248	mse	=	0.024093
Iteration	=	1249	mse	=	0.024045
Iteration	=	1250	mse	=	0.023997
Iteration	=	1251	mse	=	0.023949
Iteration	=	1252	mse	=	0.023902
Iteration	=	1253	mse	=	0.023854
Iteration	=	1254	mse	=	0.023807
Iteration	=	1255	mse	=	0.023760
Iteration	=	1256	mse	=	0.023713
Iteration	=	1257	mse	=	0.023666
Iteration	=	1258	mse	=	0.023619
Iteration	=	1259	mse	=	0.023572
Iteration	=	1260	mse	=	0.023525

Figure 12: NN iteration and MSE values.

index\_pairs=matchFeatures(feature1,feature2);
[a\_d b]=size(index\_pairs)

3. Display the outcome and analyze on the basis of MSE, PSNR and CCR values.



Figure 13: Final Result identity exists.

Calculating Mean Squared Error (MSE) and Peak Signal to Noise Ratio (PSNR) Values in table 1 and cumulative match score of all strategy which is proposed, NN and SVM in Table 2. Graphically representation of the table 2 is shown in figure 14 as a final result and analysis.

$$MSE = \frac{\sum_{M,N} [I_1(m,n) - I_2(m,n)]^2}{M*N}$$
....(i)  

$$PSNR = 10 \log_{10} \left(\frac{R^2}{MSE}\right)$$
....(ii)

I1= first input Image I2=Second Input Image M= Rows, N= Columns

R= 255

Table 1: showing the MSE and PSNR Values

	MSE	PSNR
Proposed	0.0414	7.2286e+07

Table 2: Cumulative	Match	Score	of all	Strategy
---------------------	-------	-------	--------	----------

Proposed 101.04	
NINI 00.04	14
1111 33.04	14
SVM 97.04	14



Figure 14: Cumulative Match Score of all strategy.

### VII. CONCLUSION

Biometric technology provides a strong method of linking persons to identify records. But we know that if we combine to biometric techniques then it will definitely give us good results, even better than single biometric. That's why I have planned for this multi-biometric system model and for this research work I have taken face and Palm-prints of a person then fused the images into one and stored the fused features into the database. Compared with other existing systems, the proposed method (NN\_SVM) of personal authentication has merits of high accuracy, high performance in-terms of CCR (%) small size and cost-effective.

#### REFERENCES

- [1] http://google/biometric-chart-imgae.jpg.
- [2] 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.
- [3] Ravi Bhusan tiwari and Sanjay Sharma, "Biometric authentication using fingerprint " in Youth Education and Research Trust (YERT), Vol. 1(8) January 2013.
- [4] Zhang, D. (2004). Palmprint Authentication, Kluwer Academic Publishers.
- [5] Fisher, Barry A.J. Techniques of Crime Scene Investigation. Boca Raton, CRC Press. 2004. ISBN 0-8493-1691-X.
- [6] Austin Hicklin, Brad Ulery and Craig Watson "A Brief Introduction to Biometric Fusion" in National Institute of Standards and Technology 16 June 2006.
- [7] Jan Flusser, Filip 'Sroubek, and Barbara Zitov'a "Image Fusion:Principles, Methods, and Applications" A tutorial, Institute of Information Theory and Automation, 2007.
- [8] A. Selwal, S.K Gupta and S. Jangra, "A Hybrid Template Security Scheme for Multimodal Biometric System based on Fingerprint and Hand Geometry", Int'l J. of Control Theory and Applications, Vol. 10 (2017), Issue No. 15, Pg. 143-152, ISSN: 0974-5572.
- [9] Shant Kaushik and Surender Jangra, "Finger Vein Biometric Authentication Scheme using Repeated Line Tracking and DWPT based Scheme", Int'l J. of Control Theory and Applications, Vol. 10 (2017), Issue No. 18, Pg. 289-294, ISSN: 0974-5572.
- [10] A. Selwal, S.K Gupta and Surender, "Low Overhead Octet Indexed Template Security Scheme for Multimodal Biometrics System", Journal of Intelligent & Fuzzy System 32 (2017), pp. 3325-3337, DOI:10.3233/JIFS-169274, IOS Press.
- [11] T. Kumar, S. Jangra and S. Bhushan, "Face Recognition with Decision Tree using SVM and SURF", Published in, "Int'l J. of Control Theory and Applications", Vol. 10 (2017), Issue No. 15, Pg. 173-180, ISSN: 0974-5572.
- [12] A. Selwal, S.K. Gupta and S. Kumar, "A Scheme for Template Security at Feature Fusion Level in Multimodal Biometric System", Advances in Science and Technology Research Journal, Vol. 10, No. 31, Sept. 2016, Pg. 23-30.
- [13] S. Jangra, S. Goel and A. Selwal, "Hyper Spectral Image Restoration Approach using LRMR and LDA", IEEE Xplorer, Pg. 415-418, 2015, e-ISBN: 978-1-5090-0148-4.

- [14] A. Selwal, S.K. Gupta and Surender, "Fuzzy Analytic Hierarchy Process based Template Data Analysis of Multimodal Biometric Conceptual", Procedia Computer Science (Elsevier), 85 (2016), Pg. 899-905.
- [15] A. Selwal, S.K. Gupta and Surender, "Template Security Analysis of Multimodal Biometric Frameworks based on Fingerprint and Hand Geometry", Perspectives in Science (Elsevier), (2016) 8, Pg.705-708, ISSN: 2212-0209.
- [16] A. Selwal, S. K. Gupta, Surender and Anubhuti, "Performance analysis of template data security and protection in Biometric Systems, IEEE Xplore, 2015, pp. 1-6. e-ISBN : 978-1-4673-8253-3.
- [17] Y. S. Sangwan, S. Jangra and K. Kuhar, "Facial Skin Segmentation using BFO and PSO", Int'l J. of Control Theory and Applications, Vol. 10 (2017), Issue No. 18, Pg. 31-39, **ISSN:** 0974-5572.