

# A novel encryption and recognition algorithm for signature & palm print using fuzzy features

<sup>1</sup>Rafeeq Ahmed K, <sup>2</sup>Dr. Farrukh Sayeed, <sup>3</sup>Dr. Swati Sharma

<sup>1</sup>Research Scholar, <sup>2</sup>Principal, <sup>3</sup>Associate Professor

<sup>1,2</sup>Department of Electronics and Communication Engineering,

<sup>3</sup>Department of Electrical Engineering,

<sup>1,3</sup>Jodhpur National University, Jodhpur, India

<sup>2</sup>ACE College of Engineering, Trivandrum, India

**Abstract :** Palm print as a biometric modality has marked its place as a secure authentication method for the application of data access. Signatures are still used as a valid personal identification method. Proper recognition algorithms with high recognition accuracy are in need. Also with the development of technology, any database is vulnerable to counterfeit and theft, thus arise the security concerns. Therefore, for enabling a high level of recognition accuracy and a high level of security we propose a novel recognition and encryption algorithm based on fuzzy logic. The features from the palm print and signature images are extracted using the Empirical Wavelet Transform on the images and then applying the concept of fuzzy logic/fuzzy entropy. The features are named as fuzzy features and fuzzy entropy features respectively. The features are then tested for recognition using SVM as a classifier.

**Index Terms -** Biometric, Signature, Palm Print, Empirical Wavelet transform, Averaging, Fuzzy Feature, Fuzzy Logic, Fuzzy Entropy, SVM.

## I. INTRODUCTION

Biometric systems are mainly employed in two scenarios: verification and identification. The handwritten signature is a particularly important type of biometric trait, mainly due to its ubiquitous use to verify person's identity in legal, financial and administrative areas. One of the reasons for its widespread use is that the process to collect handwritten signatures is non-invasive, and people are familiar with the use of signatures in their daily life [1].

Being a behavioural biometric trait which can be imitated, the robust system needs to be designed to counter intrapersonal and interpersonal variations. H. Baltzakis and N. Papamarkos used the global, grid and texture features and two stage neural network classifier for offline signature verification [2]. Shashi Kumar D R et al [3] introduced Off-line Signature Verification Based on Fusion of Grid and Global Features Using Neural Networks. L.Basavaraj and R.D Sudhaker Samuel [4] used dynamic features for offline signature verification based on four speed stroke angle. Mohammed A. Abdala & Noor Ayad Yousif [5] proposed a verification system using global, texture and grid features on two neural networks classifier.

Recent studies approach the problem from a representation learning perspective [6] [7] [8] [9]. These methods depend on the learning feature representations directly from the signature images instead of using the feature extraction methods for doing the task. In our paper a novel approach to extract the features based on the fuzzy logic concept has been developed using the signature image.

In palm print Local statistical approaches transform images into another domain and then divide the transformed images into several small regions [10, 11, 12, 13, 14, 15, 16, 17]. Local statistics such as means and variances of each small region are calculated and regarded as features. Gabor, wavelets and Fourier transforms have been applied.

Line-based approaches either develop edge detectors or use existing edge detection methods to extract palm lines [18, 19, 20, 21, 22, 23-25, 26, 27]. These lines are either matched directly or represented in other formats for matching. Subspace-based approaches also called appearance-based approach in the literature of face recognition. They use principal component analysis (PCA), linear discriminant analysis (LDA) and independent component analysis (ICA) [28, 29, 30, 31, 32, 33, 34, 35, 36, 37]. The subspace coefficients are regarded as features. Various distance measures and classifiers are used to compare the features.

In our case, the fuzzy features are extracted from the transformed image of the palm print using the EWT transform.

### A. Palm print

Palm print recognition is a biometric authentication method based on the unique patterns of various characteristics in the palms of people's hands. The palm print consists of principal lines, wrinkles (secondary lines), and epidermal ridges which differ from person to person. The three main categories of palm matching techniques are minutiae-based matching, correlation-based matching, and ridge-based matching. Minutiae-based matching, the most widely used technique, relies on the minutiae points, specifically the location, direction, and orientation of each point. Correlation-based matching involves simply lining up the palm images and subtracting them to determine if the ridges in the two palm images correspond. Ridge-based matching uses ridge pattern landmark features such as sweat pores, spatial attributes, and geometric characteristics of the ridges, and/or local texture analysis, all of which are alternates to minutiae characteristic extraction. This method is a faster method of matching and overcomes some of the difficulties associated with extracting minutiae from poor quality images.

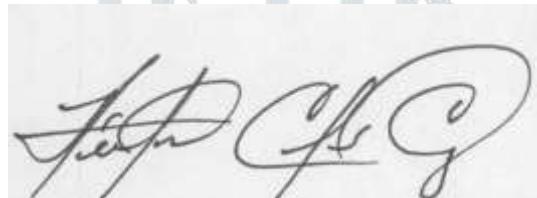


**Fig 1.1 Palmpprint and close-up showing two types of minutiae and other characteristics**

Palm print recognition systems use a scanning device or a camera-based application, along with associated software that processes image data from a photograph of an individual's palm and compares it to a stored record for that person. Palm prints are used for criminal, forensic, or security applications.

#### B. Signature

People are used to signatures as a means of transaction related identity verification, and most would see nothing unusual in extending this to encompass biometrics. Signature verification is a technique used by banks, intelligence agencies and high-profile institutions to validate the identity of an individual. Signature verification is often used to compare signatures in bank offices and other branch capture. In the signature verification process, the way a person signs her name is analyzed.



**Fig 1.2 Signature Specimen**

These are some of the features of signatures used in verification.

- Width and Height of the signature.
- Area of signature pixels.
- Normalized area.
- Signature height-to-width ratio (Aspect ratio).
- Slant Angle.
- Signature shape.
- Signing pressure
- Signing speed

Signature verification enjoys a synergy with existing processes that other biometrics do not. People are used to signatures as a means of identity verification and are still in use in various fields.

## II. PROPOSED METHOD OF FEATURE EXTRACTION

In this paper, we discuss signature and palm print feature extraction using fuzzy and fuzzy entropy algorithm. Before applying the fuzzy logic/fuzzy entropy, EWT and averaging step is done to reduce the size of image and thus increasing the computational speed without significant loss in information. Fuzzy logic and fuzzy entropy algorithm is applied on this averaged palm print or signature input individually and output is obtained. This output is stored in the database as fuzzy output/fuzzy entropy output, not as the original image. Thus, the fear of counterfeit and stealing biometric is averted.

### 2.1 EWT & Averaging

The fundamental idea of wavelet transforms is that the transformation should allow only changes in time extension, but not shape. In mathematics, a wavelet series is a representation of a square-integrable (real or complex-valued) function by a certain orthonormal series generated by a wavelet. The Empirical Wavelet Transform (EWT) aims to decompose a signal or an image on wavelet tight frames that are built adaptively.

In 1D, the procedure consists in detecting the supports of some "modes" in the Fourier spectrum and then using these supports to build Littlewood-Paley type wavelets. The empirical wavelet transform (EWT) consists of two major steps: detect the Fourier supports and build the corresponding wavelet accordingly to those supports; filter the input signal with the obtained filter bank to get the different components. [38]

The basic idea to build a 2D-EWT is to use a tensor product, which means process the rows and then the columns of the input image by using the 1D-EWT. A simple way is to consider a mean spectrum for the rows, then perform the detection of the Fourier supports based on this mean spectrum and finally use the same filters for all columns. The complete algorithm corresponds to perform the following steps (the input image is denoted as f):

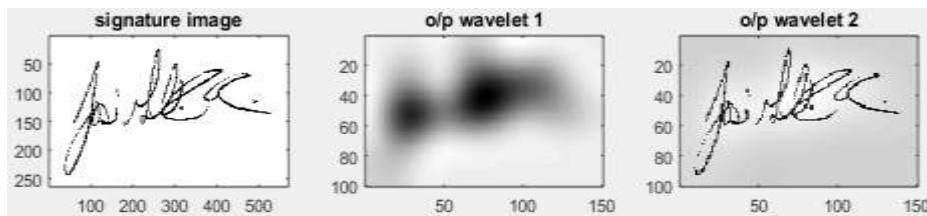
1. Take the 1D FFT of each rows i of f and compute the mean row spectrum magnitude:

$$F_{row} = \frac{1}{N_{row}} \sum_{i=0}^{N_{row}} f(i, \omega) \quad (1)$$

2. Take the 1D FFT of each columns j of f and compute the mean row spectrum magnitude:

$$F_{column} = \frac{1}{N_{column}} \sum_{j=0}^{N_{column}} f(\omega, j) \quad (2)$$

3. Perform the boundaries detection on  $F_{row}$  and build the corresponding filter bank
4. Perform the boundaries detection on  $F_{column}$  and build the corresponding filter bank
5. Filter f along the rows provides  $N_R + 1$  output images.
6. Filter each previous output image along the columns provides at the end  $(N_R+1)(N_C + 1)$  sub band images.



**Fig 2.1 Empirical wavelet transform of a signature image**

Steps involved in EWT averaging are shown below

- EWT is done on the input image. The number of modes for EWT is set as two wavelets. Almost all the features are retained in two modes of empirical wavelet transform of the biometric image.
- In this step, the output of the EWT is averaged. The average of corresponding pixels of the two modes of EWT is calculated. Thus, an average image is formed from the two modes of EWT.

Each pixel of the average image is calculated by

$$x_{ave}(i, j) = (x_{mode1}(i, j) + x_{mode2}(i, j))/2 \quad (3)$$

- In this step, the image is divided into patches. Then the average of pixels of each patch is calculated.

Let the number of patches be n and dimensions of each patch be (a, b). The average value of  $n^{\text{th}}$  patch is given by

$$X_{ave}(n) = (\sum x(a, b))/(a * b) \quad (4)$$

A new image is formed by the average values  $X_{ave}(n)$  of each patch representing the corresponding patch. Thus, the averaging algorithm reduces the output image size.

This increases the computational speed of the algorithm. The choice of the number of patches and the number of pixels included in each patch determines the amount of features retained without loss in the averaging algorithm. As the number of pixels in each patch reduces so reduces the amount of information lost. So the number of patches and the number of pixels included in each patch is chosen carefully so as not to lose any significant data.

The reduced size averaged image is used for both fuzzy logic and fuzzy entropy methods. Computational complexity is reduced very much. At the same time, results show features are all retained if we carefully select the number of patches and pixels per patch.

## 2.2 Fuzzy feature

Fuzzy logic starts with builds on a set of user-supplied human language rules that the fuzzy system convert into their mathematical equivalents. Fuzzy logic models, called fuzzy inference systems, consist of a number of conditional if-then rules. For the designer who understands the system, these rules are easy to write, and as many rules as necessary can be supplied to describe the system adequately.

Steps in designing a fuzzy logic based system are

- Understand and characterize the system behavior by using our knowledge and experience.
- Directly design the control algorithm using fuzzy rules, which describe the principles of the controller's regulation in terms of the relationship between inputs and outputs.
- Simulate and debug the design. If the performance is not satisfactory, we only need to modify some fuzzy rules and retry.

Fuzzy feature logic reduces the design development cycle time. With fuzzy feature design methodology, some time consuming steps are eliminated. Moreover, during the debugging and tuning cycle, system can be modified easily and debugged by simply modifying rules, instead of redesigning the controller.

Fuzzy inference systems rely on membership functions to explain to the computer how to calculate the correct value between 0 and 1. The degree to which any fuzzy statement is true is denoted by a value between 0 and 1.

If  $X$  is a collection of objects denoted generically by  $x$ , then a fuzzy set  $A$  in  $X$  is defined as a set of ordered pairs

$$A = \{(x, \mu_A(x)) : x \in X\} \quad (5)$$

Where  $\mu_A$  is called the Membership Function (MF) for the fuzzy set  $A$ . The MF maps each element of  $X$  to a membership grade (or membership value) between 0 and 1.

The input of fuzzy feature is the EWT averaged output of the signature/palm print image.

Steps involved in fuzzy feature algorithm are

- 1) The input image is divided into patches, say  $n$  patches
- 2) For each patch, calculate the  $I_{ij}$ , which is the intensity value of the patch and  $I_{average}$  ( $I_{ave}$ ), which is the average intensity value of the patch.
- 3)  $Q$  function ( $q_{func}$ ) is calculated from the error function:

$$q_{func} = 1 - erf_{func} \quad (6)$$

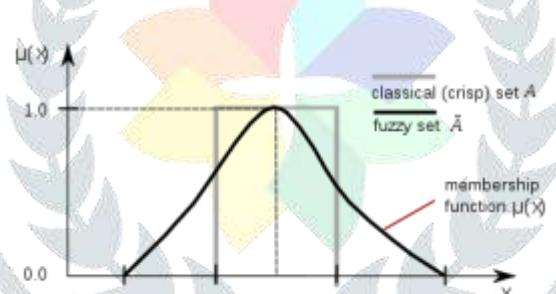
where error function is defined as:

$$erf(x) = 1.128 \int_0^x e^{-t^2} dt \quad (7)$$

The value of  $x$  here is the deviation of the pixel value from the average pixel value in that patch.

- 4) Using the intensity value, average intensity value and the degree of scatter  $\Delta x$ , calculate the membership value ( $\mu_{ij}$ ) using the equation

$$\mu_{ij} = 0.5 \left\{ q_{func} \frac{|I_{ij} - I_{ave}|}{|\Delta x \sqrt{2}|} \right\} \quad (8)$$



**Fig 2.2 Membership function**

- 5) Fuzzy feature value is calculated from intensity value ( $I_{ij}$ ) and the membership value ( $\mu_{ij}$ )

$$F_n = \frac{\sum_{i=1}^n \sum_{j=1}^m \mu_{ij} I_{ij}}{\sum_{i=1}^n \sum_{j=1}^m I_{ij}} \quad (9)$$

In this work, fuzzy feature is applied on the palm print and signature. The output values are stored in the database for recognition and verification purposes.

### 2.3 Fuzzy entropy

Fuzzy logic is based on fuzzy sets. In the fuzzy approach, each element has a degree of membership to the set. A fuzzy set expresses the degree to which an element belongs to a set. Hence, the characteristic function of a fuzzy set is allowed to have values between 0 and 1, which denotes the degree of membership of an element in a given set.

Fuzzy entropy is used to express the mathematical values of the fuzziness of fuzzy sets. Entropy is the measure of the uncertainty of a system. Entropy increases as the level of irregularity increases. According to information theory, the entropy of a system is a measure of the amount of information of the system. If all information in the system is at the same level and has the same probability, the entropy of the system is maximum.

The fuzzy entropy method is used in various areas of research and its yielding better. With the application of entropy in fuzzy sets, successful results are obtained in neural networks, machine learning, image processing and many other engineering areas. The input of fuzzy feature is the EWT averaged output of the signature/palm print image.

Steps in calculation of fuzzy entropy of an image are

1.  $x_{ij}$  represents the average value of pixels in one patch of the image and  $x_{ave}$  is the average value of the pixels of the whole image.  $x_{ave}$ , the average value of the whole image is calculated
2. Distance vector of an image is calculated;  $d_{ij}$  is the distance vector defined as

$$d_{ij} = |x_{ij} - x_{ave}| \quad (10)$$

3. Gradient vector is represented as  $n_{i,j}$ . The gradient vector  $n_{i,j}$  for the pixel  $x_{i,j}$  of the image is calculated as given where i and j represents the row and column address respectively.

$$n_{i,j} = [(x_{i+1,j+1} - x_{i,j})^2 + (x_{i+1,j} - x_{i,j+1})^2]^{\frac{1}{2}} \quad (11)$$

4. The average border distance of the central pixel is given by r which depends on the image size.

5. Fuzzy entropy is calculated as defined by:

$$\text{FuzzyEn}(X) = -\sum_{i=1}^n (\mu_{ij} d_{ij}) \ln(\mu_{ij} d_{ij}) \quad (12)$$

where  $\mu_{ij} = e^{-\ln(d_{ij}/r)^{n_{ij}}}$

6.  $\mu_{ij}$  is defined as the membership function of one patch.

7. Fuzzy entropy algorithm is applied to the signature and palm print images and a final output is obtained.

The output is stored in the database and is used as an input to the classifier.

	$x_{i,j}$	$x_{i,j+1}$		
	$x_{i+1,j}$	$x_{i+1,j+1}$		

**Fig 1.3 Pixels of image**

## 2.4 SVM classifier

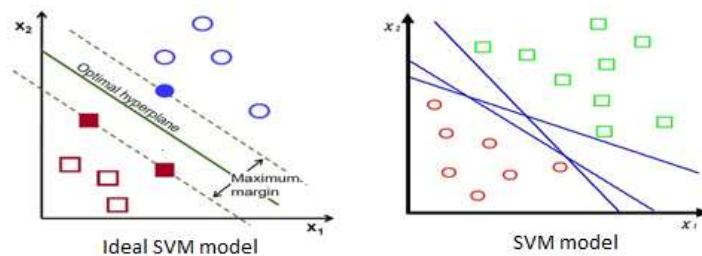
A Support Vector Machine (SVM) is a discriminative classifier formally defined by a separating hyperplane. In other words, given labeled training data (supervised learning), the algorithm outputs an optimal hyperplane which categorizes new examples. In two-dimensional space this hyperplane is a line dividing a plane in two parts where in each class lay in either side.

Given a set of training examples, each marked as belonging to one or the other of two categories, an SVM training algorithm builds a model that assigns new examples to one category or the other, making it a non-probabilistic binary linear classifier. An SVM model is a representation of the input as points in space, mapped so that the examples of the separate categories are divided by a clear gap that is as wide as possible. New inputs are then mapped into that same space and predicted to belong to a category based on which side of the gap they fall.

A support vector machine constructs a hyperplane or set of hyperplanes in a high or infinite-dimensional space, which can be used for classification, regression, or other tasks. Kernel machine, whereas the original problem may be stated in a finite dimensional space, it often happens that the sets to discriminate are not linearly separable in that space. For this reason, it was proposed that the original finite-dimensional space be mapped into a much higher-dimensional space, presumably making the separation easier in that space. To keep the computational load reasonable, the mappings used by SVM schemes are designed to ensure that dot products may be computed easily in terms of the variables in the original space, by defining them in terms of a kernel function  $k(x,y)$ . Also  $k(x,y)$  is selected to suit the problem.[39]

The hyperplanes in the higher-dimensional space are defined as the set of points whose dot product with a vector in that space is constant. The vectors defining the hyperplanes can be chosen to be linear combinations with parameters of images of feature vectors that occur in the database.

The points  $x$  in the feature space that are mapped into the hyperplane are defined with this choice of a hyperplane. Note that if  $k(x,y)$  becomes small as  $y$  grows further away from  $x$ , each term in the sum measures the degree of closeness of the test point  $x$  to the corresponding data base point  $x_i$ . In this way, the sum of kernels above can be used to measure the relative nearness of each test point to the data points originating in one or the other of the sets to be discriminated.

**Fig 2.4 Ideal vs general SVM Model**

The outputs of fuzzy feature and fuzzy entropy are tested using SVM classifier individually.

### III. RESULTS AND DISCUSSIONS

We used three different polynomials named as Poly1, Poly2 & Poly3. These three polynomials are the three different degrees of order 1, order 2 and order 3 of Lagrange multiplier. These gave almost similar results. The recognition results are tabulated for both signature and palm print images using SVM. For the signatures the CEDAR[40] database is used and for the palm print the CASIA[41] database is used for extracting the features. 70% of images of each person are used for training and 30% images are used for testing in both the cases.

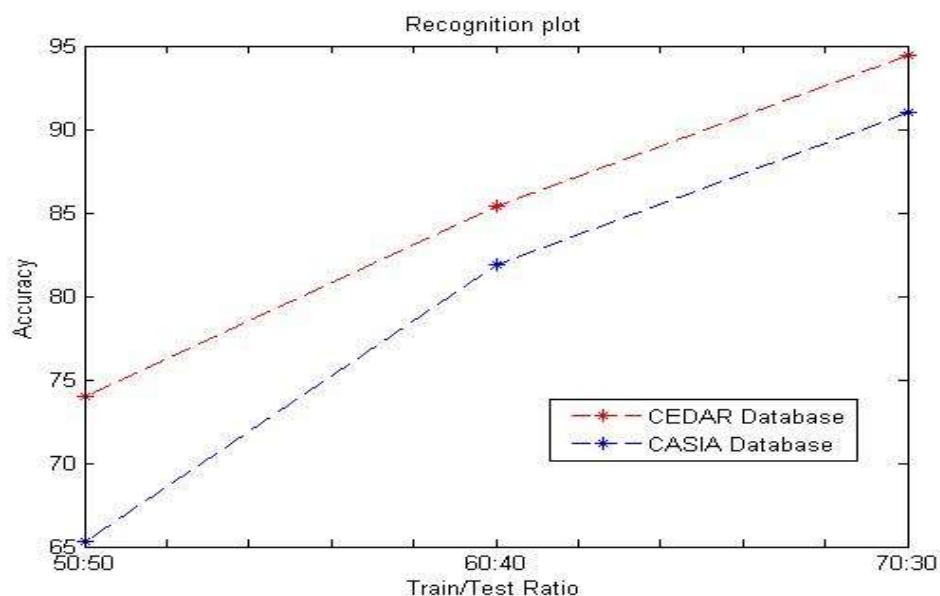
**Table 3.1 Recognition results for signature**

SVM recognition for Signature (%)			
	Poly 1	Poly 2	Poly 3
Fuzzy features	94.44	94.07	94.07
Fuzzy Entropy features	97	96	96

**Table 3.2 Recognition results for palm print**

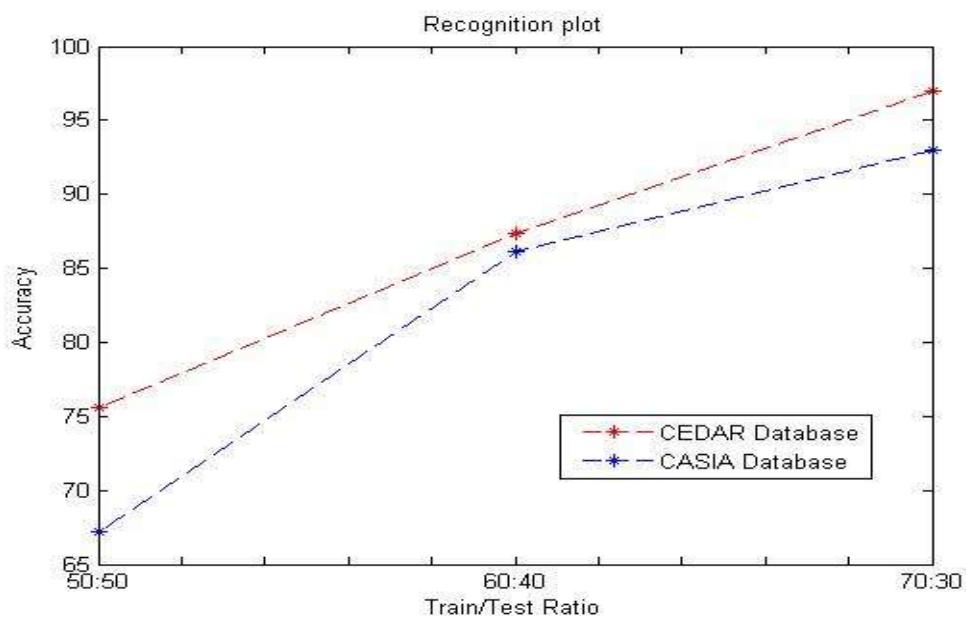
SVM recognition for Palm print (%)			
	Poly 1	Poly 2	Poly 3
Fuzzy features	91	91	91
Fuzzy Entropy features	93	92	92

The recognition rate for the signature is 97% using Fuzzy Entropy features and 94.44% using fuzzy features. In case of palm print the maximum recognition rate of 93% is achieved by using Fuzzy Entropy features. Both the fuzzy features are giving slightly better results in case of signatures.



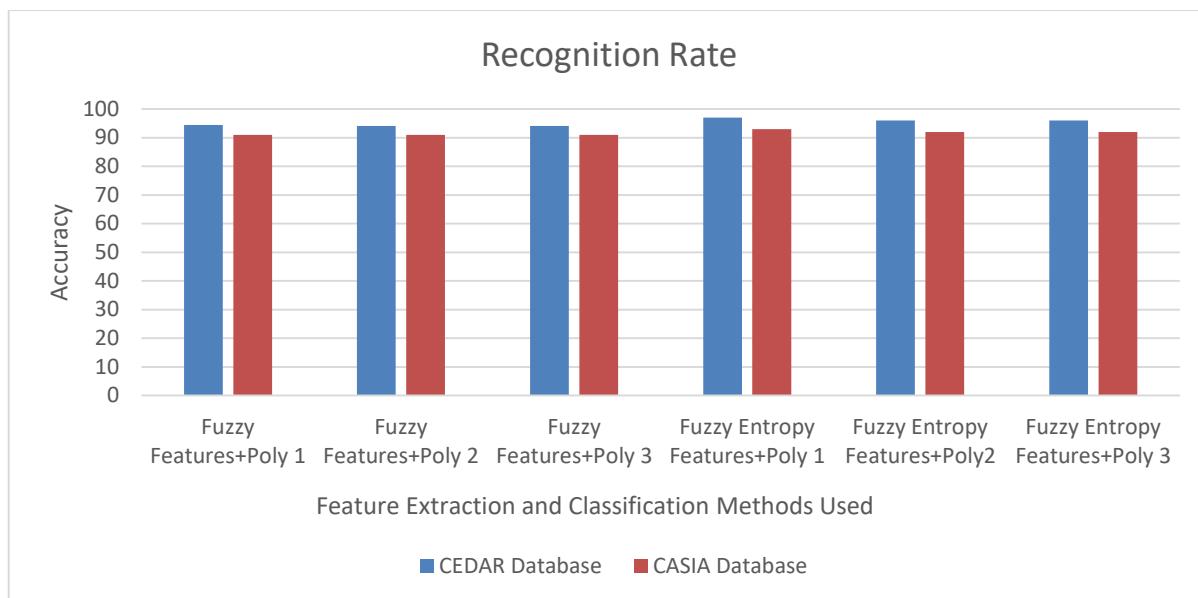
**Fig 3.1 Recognition rate for Fuzzy features combined with SVM( Poly1) for maximum accuracy**

The recognition rate for fuzzy features and fuzzy entropy features when combined with SVM (Poly 1) for attaining maximum accuracy is shown with the help of Fig 3.1 and Fig 3.2 respectively and Table 3.3 shows the recognition plot for combinations of all the feature extraction and classification methods.



**Fig 3.2 Recognition rate for Fuzzy entropy features combined with SVM (Poly 1) for maximum accuracy**

**Table 3.3: Recognition plot for combinations of all feature extraction and classification methods**



#### IV. CONCLUSION

A new type of image recognition algorithm is developed for the palm print and signature. The training data once entered into the biometric scanner is saved in the biometric database in an encrypted form as an output of fuzzy logic/fuzzy entropy applied on the EWT averaged Images of both signature and palm print. The encrypted database cannot be decrypted without the fuzzy logic or fuzzy entropy algorithm developed here, thus making it secure. Results show that accuracy is higher for both fuzzy features and fuzzy entropy features thus making both the algorithms suitable for biometric applications. The maximum recognition rate of 97% is achieved for the signatures and 93% for the palm print using the fuzzy Entropy features using SVM as the classifier.

#### REFERENCES

- [1] Rejean Plamondon and Sargur N. Srihari. Online and off-line handwriting recognition: a comprehensive survey. *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, 22(1):63–84, 2000.
- [2] H. Baltzakis, N. Papamarkos, A new signature verification technique based on a two-stage neural network classifier, *Engineering Applications of Artificial Intelligence* 14 (2001) 95-103.
- [3] Shashi Kumar D R, K B Raja, R. K Chhotaray, SabyasachiPattanaik, Off-line Signature Verification Based on Fusion of Gridand Global Features Using Neural Networks , *International Journal of Engineering Science and Technology Vol. 2(12)*, 2010, 7035-7044.
- [4] L.Basavaraj and R.D Sudhaker Samuel, Offline-line Signature Verification and Recognition: An Approach Based on Four Speed Stroke Angle *International Journal of Recent Trends in Engineering*, Vol 2, No. 3, November 2009.
- [5] Mohammed A. Abdala & Noor Ayad Yousif, Offline Signature Recognition and Verification Based on Artificial Neural Network,*Eng & Tech. Journal*, Vol.27, No.7,2009.
- [6] Luiz G. Hafemann, Robert Sabourin, and Luiz S. Oliveira. Writer independent feature learning for Offline Signature Verification using Deep Convolutional Neural Networks. In *International Joint Conference on Neural Networks*, pages 2576–2583, July 2016.
- [7] Luiz G. Hafemann, Robert Sabourin, and Luiz S. Oliveira. Learning features for offline handwritten signature verification using deep convolutionalneural networks. *Pattern Recognition*, 70:163–176, October2017.
- [8] H. Rantzs, H. Yang, and C. Meinel. Signature embedding: Writer independent offline signature verification with deep metric learning. In *Advances in Visual Computing*. Springer, 2016.
- [9] Z. Zhang, X. Liu, and Y. Cui. Multi-phase offline signature verification system using deep convolutiona generative adversarial networks. In *2016 9th International Symposium on Computational Intelligence and Design (ISCID)*, volume 02, pages 103–107,2016.
- [10] C.C. Han, H.L. Cheng, C.L. Lin, K.C. Fan, Personal authentication using palm-print features, *Pattern Recognition* 36 (2) (2003) 371–381.
- [11] J. You, W.K. Kong, D. Zhang, K.H. Cheung, On hierarchical palm print coding with multiple features for personal identification in large databases, *IEEE Transactions on Circuits and Systems for Video Technology* 14 (2) (2004) 234–243.
- [12] G. Lu, K. Wang, D. Zhang, Wavelet based feature extraction for palm print identification, in: *Proceeding of Second International Conference on Image and Graphics*, 2002, pp. 780–784.
- [13] X. Wu, K. Wang. D. Zhang, Palm print recognition using directional energy feature, in: *Proceedings of International Conference on Pattern Recognition*, vol. 4, 2004, pp. 475–478.
- [14] A. Kumar, D.C.M. Wong, H.C. Shen, A.K. Jain, Personal verification using palm print and hand geometry biometric, in: *Lecture Notes in Computer Science*, Springer, 2003, pp. 668–678.
- [15] X. Wu, K. Wang, D. Zhang, Wavelet based palm print recognition, in: *Proceedings of the First International Conference on Machine Learning and Cybernetics*, vol. 3, 2002, pp. 1253–1257.

- [16] A. Kumar, D. Zhang, Palm print authentication using multiple classifiers, in: Proceedings of SPIE Symposium on Defense and Security-biometric Technology for Human Identification, 2004, pp. 20–29.
- [17] A. Kumar, H.C. Shen, Palm print identification using Palm Codes, in: Proceedings of 3rd International Conference on Image and Graphics, 2004, pp. 258–261.
- [18] F. Li, M.K.H. Leung, X. Yu, Palm print identification using Hausdorff distance, in: Proceedings of International Workshop on Biomedical Circuits and Systems, 2004, pp. S3/3–S5-8.
- [19] X. Wu, K. Wang, D. Zhang, Line feature extraction and matching in palm print, in: Proceeding of the Second International Conference on Image and Graphics, 2002, pp. 583–590.
- [20] X. Wu, K. Wang, D. Zhang, Fuzzy direction element energy feature (FDEEF) based palm print identification, in: Proceedings of International Conference on Pattern Recognition, vol. 1, 2002, pp. 95–98.
- [21] W.W. Boles, S.Y.T. Chu, Personal identification using images of the human palms, in: Proceedings of IEEE Region 10 Annual Conference, Speech and Image Technologies for Computing and Telecommunications, vol. 1, 1997, pp. 295–298.
- [22] M. Rafael Diaz, C.M. Travieso, J.B. Alonso, M.A. Ferrer, Biometric system based in the feature of hand palm, in: Proceedings of 38th Annual International Carnahan Conference on Security Technology, 2004, pp. 136–139.
- [23] S.Y. Kung, S.H. Lin, M. Fang, A neural network approach to face/palm recognition, in: Proceedings of IEEE Workshop Neural Networks for Signal Processing, 1995, pp. 323–332.
- [24] P.A. Recobos Rodrigues, J.D. Landa Silva, Biometric identification by dermatoglyphics, in: Proceedings of International Conference on Image Processing, vol. 1, 1996, pp. 319–322.
- [25] X. Wu, K. Wang, D. Zhang, A novel approach of palm-line extraction, in: Proceeding of the Third International Conference on Image and Graphics, 2004, pp. 230–233.
- [26] D.S. Huang, W. Jia, D. Zhang, Palm print verification based on principal lines, *Pattern Recognition* 41 (4) (2008) 1316–1328.
- [27] M.K.H. Leung, A.C.M. Fong, H.S. Cheung, Palm print verification for controlling access to shared computing resources, *IEEE Pervasive Computing* 6 (4) (2007) 40–47.
- [28] T. Connie, A.T.B. Jin, M.G.K. Ong, D.N.C. Ling, An automated palm print recognition system, *Image and Vision Computing* 23 (5) (2005) 501–515.
- [29] X. Wu, D. Zhang, K. Wang, Fisher palms based palm print recognition, *Pattern Recognition Letters* 24 (15) (2003) 2829–2838.
- [30] G. Lu, D. Zhang, K. Wang, Palm print recognition using Eigen palms features, *Pattern Recognition Letters* 24 (9) (2003) 1463–1467.
- [31] X.Y. Jing, D. Zhang, A face and palm print recognition approach based on discriminant DCT feature extraction, *IEEE Transactions on Systems, Man, and Cybernetics—Part B: Cybernetics* 34 (6) (2004) 2405–2415.
- [32] G.M. Lu, K.Q. Wang, D. Zhang, Wavelet based independent component analysis for palm print identification, in: Proceedings of International Conference on Machine Learning and Cybernetics, vol. 6, 2004, pp. 3547–3550.
- [33] A. Kumar, D. Zhang, Palm print authentication using multiple classifiers, in: Proceedings of SPIE Symposium on Defense and Security-Biometric Technology for Human Identification, 2004, pp. 20–29.
- [34] G. Feng, K. Dong, D. Hu, D. Zhang, when face are combined with palm prints: a novel biometric fusion strategy, in: *Lecture Notes in Computer Science*, Springer, vol. 3072, 2004, pp. 701 -707.
- [35] L. Shang, D.S. Huang, J.X. Du, C.H. Zheng, Palm print recognition using FastICA algorithm and radial basis probabilistic neural network, *Neurocomputing* 69 (13–15) (2006) 1782–1786.
- [36] L. Shang, D.S. Huang, J.X. Du, Z.K. Huang, Palm print recognition using ICA based on winner-take-all network and radial basis probabilistic Neural network, in: *Lecture Notes in Computer Science*, vol. 3972, 2006, pp. 216–221.
- [37] “Online Signature Verification using the Entropy Function”, Madasu Hanmandlu , Farrukh Sayeed, Shantaram Vasikarla, 2015 IEEE Applied Imagery Pattern Recognition Workshop (AIPR) ,Washington D.C, USA ,13-15<sup>th</sup> October,2015.
- [38] “Facial Emotion Recognition for Human-Machine Interaction using Hybrid DWT-SFET Feature Extraction Technique”, Dr. Farrukh Sayeed et al, 2016 Second International Conference on Cognitive Computing and Information Processing (CCIP),Mysuru,12-13 Aug,2016.
- [39] “Off-line signature verification based on a new symbolic representation and dynamic time warping”, Xinxin Yao, Hua-Liang Wei, 2016 22nd International Conference on Automation and Computing (ICAC)
- [40] CEDAR database for signatures ((<http://www.cedar.buffalo.edu/NIJ/publications.html/>)
- [41] CASIA Palm Print database (biometrics.idealtest.org)