Development of Extracted Biometric Watermark Recognition using Chain Code and Support Vector Machine

Ms. Monika Patel[1],

Research Scholar
G. H. Patel Dept. of Computer Science and Technology
Sardar Patel University,
Vallabh Vidyanagar, Gujarat, India

Dr. Priti Srinivas Sajja[2]

Professor,
G. H. Patel Dept. of Computer Science and Technology
Sardar Patel University,
Vallabh Vidyanagar, Gujarat, India

ABSTRACT

In today's digital world, the major source of communication is digital media such as images, video, audio or text. Therefore imitate and copyright protection of digital content remains a vital problem across the globe. To deal with this problem, digital watermarking using biometric watermark has become valuable solution for providing ownership of digital content. After extracting the biometric watermark it becomes necessary to check whether it is matched with original one or not. In this paper we have developed a chain code based feature extraction method for developing fingerprint recognition system. We have implemented 8 neighborhood method allows generation of eight different codes for each fingerprint. These codes have been used as features of the fingerprint image, which have been later used for training and testing through Support Vector Machine (SVM) classifiers. This paper illustrates working of the proposed model and aforesaid algorithm for extracted watermark fingerprint recognition.

Keywords - Digital Watermarking, Biometric Watermark, Chain Code, Support Vector Machine, Watermark Fingerprint Recognition.

Introduction

Due to the proliferation of the World Wide Web and high speed internet, a huge amount of multimedia content such as text, graphics, images, video, and audio are easily accessible by the millions of the users. As a result, security, copyright protection and protecting ownership have become important problems in current research and applications. As a key, Digital watermarking is the most suitable technology to prove ownership on copyrighted material and detect the originality of illegally made copies and their usage over the network. In today's scenario biometric data like fingerprint, face and iris can be used as a watermark to present appropriate security to the digital data.

Digital watermarking is the method of embedding information into a digital data. The digital data may be audio, picture or video. The embedded information is known as a watermark that can be extracted or detected whenever it is required. In this paper biometric watermark fingerprint is inserted into a digital data. Fingerprints are "unique" to a person and no one can be easily distorted the digital media [16,17].

Biometric Watermark Recognition

In this method we have used fingerprint as a biometric watermark. So after extracting any watermark it becomes necessary to verify the matching ratio of original watermark and extracted watermark.

Biometrics is an automated technique which is used to recognize a person based on their physical and behavioral characteristics. Among all biometrics, like face, hand, iris, voice etc fingerprints is the most dominant biometric technology in commercial applications due to their distinctiveness, persistence, accuracy, throughput, size and cost of readers [5]. Nowadays fingerprint based recognition is popular for individual identification because it will not change by age. It is unique to individuals and with the new technologies it is easy and low cost to implement [5,7,28,30,31].

Architecture of Fingerprint Recognition System

Fingerprint recognition system can operate in either identification or verification mode. In verification mode system verifies the person's identity by comparing input fingerprint with individual's own template of fingerprints stored in database. In identification mode fingerprint of an individual is matched with all templates present in database. The general architecture of fingerprint recognition system is shown in below figure 1. Fingerprint recognition system basically follows four steps - Image Acquisition, Preprocessing, Feature extraction and Pattern Matching [10,12,15,18,27].

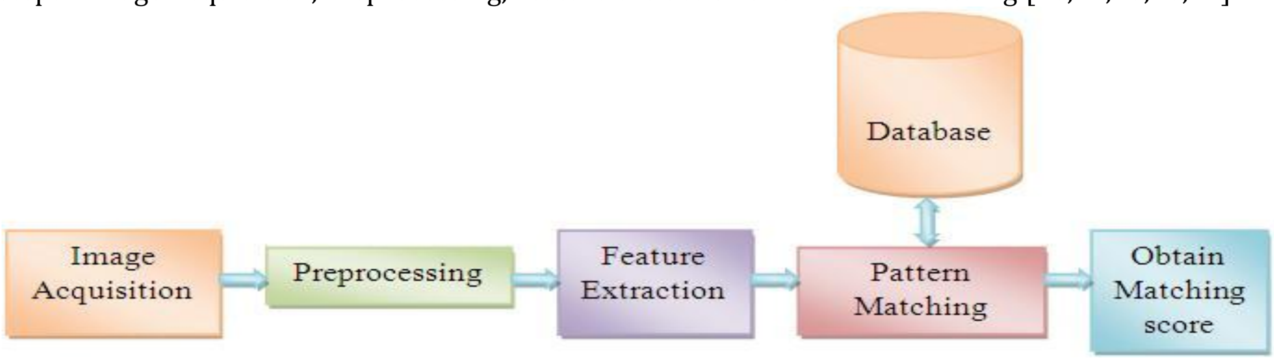


Figure 1: The general block diagram of Fingerprint recognition system [10,12,15,18,27]

1) *Image Acquisition*: user has to acquire the fingerprint of an individual to the system.
2) *Preprocessing:* After acquiring an image preprocessing is applied on image. Sometimes image may contain noise during acquisition process, so noise can be removed and image is converted into binary image.
3) *Feature extraction:* During this phase, the fingerprint is further processed to generate discriminative properties like ridges, valleys, minutiae, singular points etc. These features are helpful for identification or verification of individual.
4) *Pattern Matching:* Matching is totally dependent on whether the system performs identification or verification. If it performs identification i.e. one-to-many matching approach is used, where fingerprint of an individual matches with all available templates in database otherwise one-to one match is done for verification, where input image of a person is matched with only the template an individual claims to be.

Introduction to Chain Code

Chain code is one of the simplest ways to represent the images based on its boundary. Now a day, image representation through its boundary has been widely used as a topic of research. Because this representation influences the information for some process like in digital image processing, pattern recognition and machine vision system. Moreover chain code preserves information and allows considerable data reduction, provides a very compact region representation which is suitable for detecting such feature of a region as sharp corners, area, perimeter, moments, centers, eccentricity, projection and straight-line segments [4,21].

Basically chain code is working based on two different manners such as 4- neighborhood method or 8-neighborhood method. In order to obtain the chain code, from the first pixel of the image, we move downwards row by row and consider the first pixel of the body of image which exactly has got one neighbor, as the start point of the chain code. If a fingerprint has no initial point, we will consider its chain code as zero. Each pixel of image has received its eight neighbors; to each neighbor we assign one value between 0 and 7. After finding the start point of the chain code neighbors of a pixel and value is assigned to it in a given fingerprint image, we move to the next neighbor pixel which also be a part of image. Again in the cases of having two or more neighbor pixels with the above condition use the directional priority. While passing one pixel to its next pixel, we have inserted the number related to that next in the chain code of that image. After receiving the chain code for all segmented characters, we come to know that the chain code for different fingerprints has different size, and size of each chain code depends on the length of the desired fingerprints. In more ever, length of the chain codes is usually high; therefore one should convert it into it's normalize form. This chain code as its length will be fixed and limited [4,9,21].

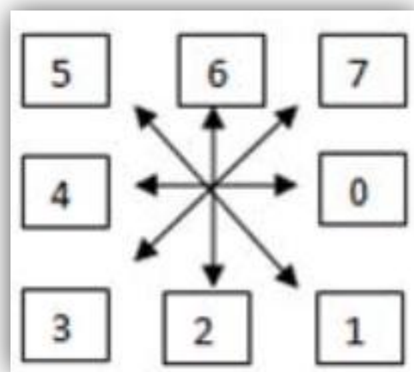
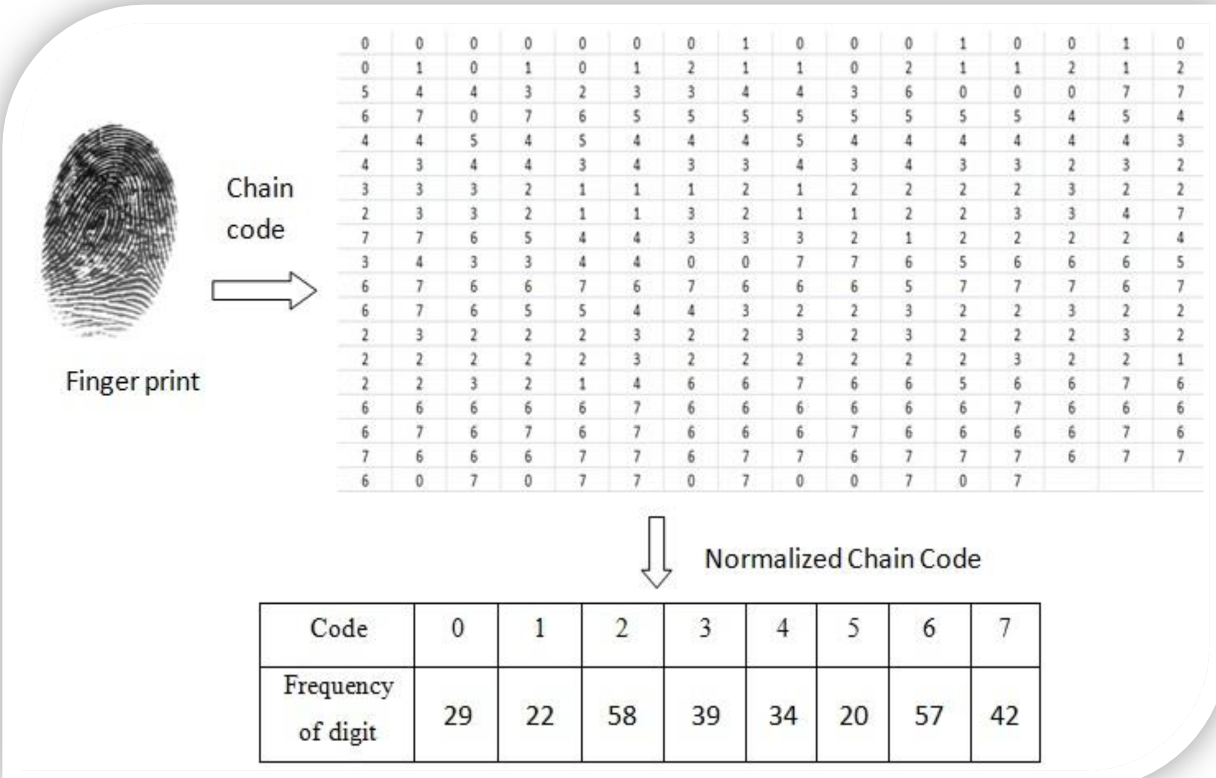


Figure 2: 8-neighborhood for chain code[4,9,21]

Algorithm for generating chain code considering 8neighborhood is as follows[4,9,21]:
Step1: Find out starting point which has nonzero values and store it in first
Step2: Initialize 0-7 total eight directions
Step3: Travels all 8 neighbors
Step4: Find first nonzero value
Step5: Add it in to chain code list
Step6: Move to next position
Step7: Check whether we reach to first point or not if not then go to step 3.

Chain Code Normalization

After applying chain code on segmented image, we can get the chain code of that image. So we can observe the length of obtained chain code which is too long. So in this case it becomes difficult to keep chain code of whole database of fingerprints. To overcome this problem we have to normalize the obtained chain code by transforming it into a two dimensional matrix. In this matrix, the first row contains the value of the chain code and the second row contains the frequency of occurrence of the each code (0 to 7). The following figure 3 demonstrates the example of chain code generation and normalization of fingerprint image [4,9,21].



0	0	0	0	0	0	0	1	0	0	0	1	0	0	1	0
0	1	0	1	0	1	2	1	1	0	2	1	1	2	1	2
5	4	4	3	2	3	3	4	4	3	6	0	0	0	7	7
6	7	0	7	6	5	5	5	5	5	5	5	5	4	5	4
4	4	5	4	5	4	4	4	5	4	4	4	4	4	4	3
4	3	4	4	3	4	3	3	4	3	4	3	3	2	3	2
3	3	3	2	1	1	1	2	1	2	2	2	2	3	2	2
2	3	3	2	1	1	3	2	1	1	2	2	3	3	4	7
7	7	6	5	4	4	3	3	3	2	1	2	2	2	2	4
3	4	3	3	4	4	0	0	7	7	6	5	6	6	6	5
6	7	6	6	7	6	7	6	6	6	5	7	7	7	6	7
6	7	6	5	5	4	4	3	2	2	3	2	2	3	2	2
2	3	2	2	2	3	2	2	3	2	3	2	2	2	3	2
2	2	2	2	2	3	2	2	2	2	2	2	3	2	2	1
2	2	3	2	1	4	6	6	7	6	6	5	6	6	7	6
6	6	6	6	6	7	6	6	6	6	6	6	7	6	6	6
6	7	6	7	6	7	6	6	6	7	6	6	6	6	7	6
7	6	6	6	7	7	6	7	7	6	7	7	7	6	7	7
6	0	7	0	7	7	0	7	0	0	7	0	7			

Code	0	1	2	3	4	5	6	7
Frequency of digit	29	22	58	39	34	20	57	42

Figure 3: Example of Feature Extraction using normalized chain code

Introduction to SVM

Support Vector Machine (SVM) is a well known feature classification technique. SVMs have been used in many pattern recognition and regression estimation problems and have been applied to the problems of dependency estimation, forecasting and constructing intelligent machines [6,25]. It provides a facility to split feature space into two major classes through optimal hyper plane such that the expected generalization error is minimized. An optimal hyper plane is represented by the largest margin of separation between the two classes. The training feature vectors have to lie outside the margin, a small subset of the feature vectors that lie exactly on the margin are the support vectors [6,24].

Suppose we have L training points, where each input x has D attributes (i.e. is of dimensionality D) and is in one of two classes y = -1 or + 1, our training data is of the form: [6,24]

$$\{x_i, y_i\} \ where \ i = 1 \dots L, y_i \in \{-1,1\}, x \in R^D \qquad \text{.......... (1)}$$

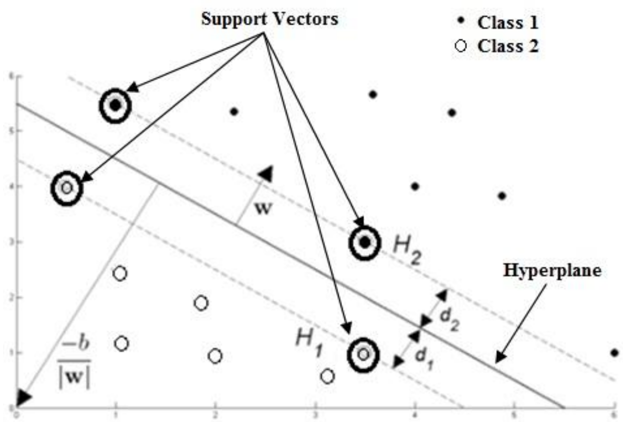


Figure 4: Hyperplane through two linearly separable classes.

Here we assume that the data is linearly separable, that means we can draw a line on a graph of x_1 vs x_2 separating the two classes when D = 2 and a hyperplane on graphs of $x_1, x_2 \dots x_D$ for when D > 2. This hyperplane can be described by $w \cdot x + b = 0$, $where$ w is normal to the hyperplane, $|b|/|w|$ is the perpendicular distance from the hyperplane to the origin [2]. |w| is the Euclidean norm of w. Let $d_+(d_-)$ be the shortest distance from the separating hyperplane to the closest positive (negative) example. Define the "margin" of a separating hyperplane to be $d_+ + d_-$.

For the linearly separable case, the support vector algorithm simply looks for the separating hyperplane with largest margin. This can be formulated as follows: suppose that all the training data satisfy the following constraints:[6,24]

$$\mathbf{x}_i \cdot \mathbf{w} + b \geq +1 \quad \text{for } y_i = +1 \qquad \text{............ (2)}$$

$$\mathbf{x}_i \cdot \mathbf{w} + b \leq -1 \quad \text{for } y_i = -1 \qquad \text{............. (3)}$$

This equations can be combined into following form:

$$y_i(\mathbf{x}_i \cdot \mathbf{w} + b) - 1 \geq 0 \quad \forall i \qquad \text{...........(4)}$$

Proposed System

The proposed system is developed for the recognition of extracted fingerprint which is used as a watermark. In this system we have performed digital watermark embedding and extracting process during the testing modules for the testing data set of fingerprints. After that testing data are converted into 0 and 1 form during the preprocessing. In our proposed system edge detection is applied on fingerprint watermark and the chain code is generated for the detected edges of the fingerprint. To save processing time and database space normalization is applied on chain code to generate normalized chain code and save it into the text file, which is supply to SVM classifier to test the data. Same way training of fingerprint data set is performed. The proposed model is shown in below figure 5.

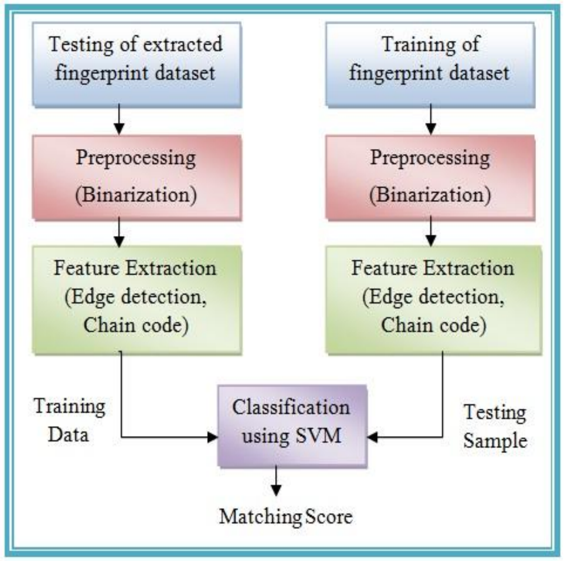


Figure 5: Proposed System

Algorithm for Testing Fingerprint Dataset

Step 1: Input cover image and fingerprint dataset
Step 2: Perform watermark embedding using DWT based alpha blending technique
Step 3: Watermarked images are generated having different fingerprints.
Step 4: Apply watermark extraction using DWT based alpha blending technique
Step 5: Perform binarization on each fingerprint image.
Step 6: Apply edge detection technique to extract the edges of image.
Step 7: Generate chain code for the extracted edges.
Step 8: Apply normalization on chain code and save it in ".txt" file.
Step 9: Test the text file using SVM tool.
Same way repeat steps 5 to 9 for training the fingerprint dataset.

Results

We have implemented this proposed system in MATLAB software. We have used 10 images of fingerprint for testing and training. Here we apply "Canny" edge detection technique to detect the edges of fingerprint image. In this proposed system classification is done using LibSVM tool. To implement the mentioned system we have used SVM package which contains some command for training and testing the data. SVM-Train command is used to train the dataset and SVM-Predict are used to test the dataset. We have taken one-class SVM and redial bias function as a kernel type. By implementing this proposed system we got approximately 100% accuracy which is shown in below figure 6.

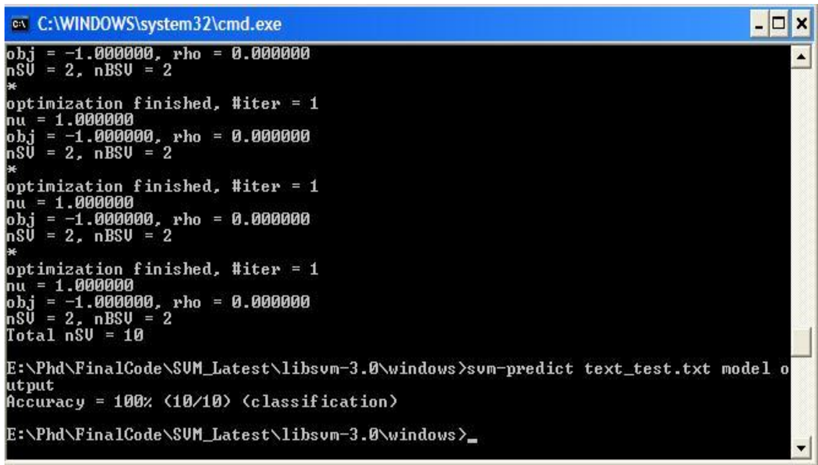


Figure 6: Result of SVM Classification

Conclusion

We have developed efficient fingerprint recognition system using chain code and support vector machine. Selection of feature extraction method is most important aspect for achieving high recognition ratio. In this work, we have implemented chain code based on 8-neighborhood feature extraction method. With the use of this obtained feature, we have trained the SVM classifier for fingerprint recognition. In the investigated work, the recognition rate is 100% for watermark fingerprint recognition. . In future we can implement PCA based pattern recognition technique using SVM. We can also use this technique for iris, face or any other biometric recognition.

References

[1] Al-Ani, M. S. (2013). A Novel Thinning Algorithm for Fingerprint Recognition. *International Journal of Engineering Sciences , 2* (2), 43-48.

[2] Alka Shrivastava, R. R. (2013). A SVM and K-means Clustering based Fast and Efficient Intrusion Detection System. *International Journal of Computer Applications , 72* (6), 25-29.

[3] Anil K. Jain, A. R. (2014). An Introduction to Biometric Recognition. *IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY , 14* (1), 4-20.

[4] Arora, S. (2011). Features Combined in a MLP-based System to Recognize Handwritten Devnagari Character. *Journal of Information Hiding and Multimedia Signal Processing , 2* (1).

[5] Bey, K. B. (2008). Agent based approach for distribution of fingerprint matching in a metacomputing environment. *8th international conference on New technologies in distributed system.* Lyon, Franc.

[6] BURGES, C. J. (1998). A Tutorial on Support Vector Machines for Pattern Recognition. *Data Mining and Knowledge Discovery , 2*, 121-167.

[7] Changlong J., K. H. (2009). Comparative assessment of fingerprint sample quality measures based on minutiae-based matching performance. *Electronic Commerce and Security, ISECS '09, Second International Symposium.*

[8] Dewi Nasien, H. H. The Heuristic Extraction Algorithms for Freeman Chain Code of Handwritten Character. *International Journal of Experimental Algorithms (IJEA) , 1* (1).

[9] H. Imran Khan, S. U. (2013). Isolated Kannada Character Recognition using Chain Code Features. *International Journal of Science and Research , 2* (8), 67-70.

[10] Hemlata Patel, P. A. (2012). Fingerprint Matching Using Two Methods . *International Journal of Engineering Research and Applications , 2* (3), 857-860.

[11] HYERAN BYUN, S.-W. L. (2003). A Survey of Pattern Recognision Applications of Support Vector Machines. *International Journal of Pattern Recognition and Artificial Intelligence , 7* (3), 459-486.

[12] Jyoti Rajharia, D. P. Fingerprint-Based Identification System:A Survey. *International Journal of Computer Technology and Electronics Engineering (IJCTEE) , 1* (3), 98-101.

[13] Kresimir Delac, M. G. (2004). A SURVEY OF BIOMETRIC RECOGNITION METHODS. *46th International Symposium Electronics in Marine, ELMAR-2004*, (pp. 184-193). Zadar, Croatia .

[14] Lin, C.-J. (n.d.). *A Library for Support Vector Machines*. Retrieved from http://www.csie.ntu.edu.tw/~cjlin/libsvm/

[15] Megha Kulshrestha, V. K. (2012). Finger Print Recognition: Survey of Minutiae and Gabor Filtering Approach. *International Journal of Computer Applications , 50* (4), 17-21.

[16] Monika Patel, D. P. (2016). A Novel DWT based Alpha Blending Watermarking Technique for Video Authentication. *Women in Science & Technology: Creating Sustainable Career* (pp. 183-189). V. V. Nagar: Indian Journal of Technical Education, Special Issue.

[17] Monika Patel, P. S. (2015). The Significant Impact of Biometric Watermark for Providing Image Security using DWT based Alpha Blending Watermarking Technique. *International Journal of Innovative Research in Computer and Communication Engineering , 3* (5), 3943-3952.

[18] Parth BPathak, P. A. (2013). A Survey on Different Fingerprint Recognition System. *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) , 2* (2), 519-523.

[19] Quratulain Shafi, J. K. (2010). Fingerprint Verification over the Network and its Application in Attendance Management. Taxila, Pakistan: Computer Engineering Department,University of Engineering and Technology.

[20] Ratiporn Chanklan, K. C. (2015). Fingerprint Recognition with Edge Detection and Dimensionality Reduction Techniques. *3rd International Conference on Industrial Application Engineering*, (pp. 569-574).

[21] Ravi Sheth, N. C. (2011). Handwritten Character Recognition System using Chain code and Correlation Coefficient. *International Conference on Recent Trends in Information Technology and Computer Science*, (pp. 31-36).

[22] Ravi Sheth, N. C. (2011). PCA Based Handwritten Character Recognition System Using Support Vector Machine & Neural Network. *AIJSTPME , 4* (4), 69-75.

[23] Ravi Subban, D. P. (2013). A Study of Biometric Approach Using Fingerprint Recognition . *Lecture Notes on Software Engineering , 1* (2), 209-213.

[24] S. Adebayo Daramola, T. S. (2013). Fingerprint Verification System Using Support Vector Machine. *International Journal on Computer Science and Engineering (IJCSE) , 5* (7), 678-683.

[25] Sami, E. (2012). Support Vector Machines for classification and locating faults on transmission lines. *Applied Soft Computing , 12*, 1650-1658.

[26] Sangame S.K, R. R. (2009). Recognition of isolated handwritten Kannada vowels. *Advances in Computational Research , 1* (2), 52-55.

[27] Sangram Bana, D. D. (2011). Fingerprint Recognition using Image Segmentation. *INTERNATIONAL JOURNAL OF ADVANCED ENGINEERING SCIENCES AND TECHNOLOGIES , 5* (1), 12-23.

[28] Wang Y., X. A. (2006). A fingerprint recognition algorithm based on principal component analysis. *IEEE Region 10 Conference.*

[29] Yuan Yao, P. F. (2001). Fingerprint Classification with Combinations of Support Vector Machines. *AVBPA 2001, LNCS 2091* (pp. 253-258). Springer-Verlag Berlin Heidelberg .

[30] Yulan Z., J. C. (2009). New algorithm of automation fingerprint recognition. *Information Engineering and Computer Science, ICIECS 2009.*

[31] *International Conference.*

[32] Zhi Y., W. J. (2009). Fingerprint image enhancement by super resolution with early stopping. *Intelligent Computing and Intelligent Systems, . ICIS 2009. IEEE International Conference.*