ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 2, Issue 8, August 2013

A Study on Handwritten Signature Verification Approaches

Surabhi Garhawal, **Neeraj Shukla**

***Abstract*— People are comfortable with pen and papers for authentication and authorization in legal transactions. Due to increasing the amount of handwritten signatures it is very essential that a person offline hand written signature to be identified uniquely. A signature is a behavioural biometric characterized by behavioural trait that a writer learns and acquires over a period of time and becomes his unique identity This paper explains the significance of offline systems and presents the survey of various approaches being followed in different areas. This being a nascent area under research, the survey covers some of the examples of the ways.**

Index Terms* — Signature verification, feature extraction, FAR *(*False Acceptance Rate*),* FRR *(*False Rejection Rate*).

I. INTRODUCTION

Handwritten signatures are widely accepted as a means of personal authentication and verification. So legality most documents like bank cheques, visa application and academic certificates, attendance register monitoring need to have authorized offline handwritten signatures. Today's society where forgery is rampant, there is the need for an automatic Handwritten signature verification (HSV) system to complement visual verification. Biometrics is the technological means that enables the identification or true verification of an individual from its physical or behavioral characteristics depending on their nature. It is classified into two categories namely behavioral and physiological. Where physiological biometrics measure some physical features of the subject like fingerprints, iris, hand and finger geometry which are stable over time. With the use of edge direction histogram derived from the edge map of the picture, only a small number of most possible intra prediction modes are chosen. Therefore the fast mode decision algorithm helps to speed up intra coding significantly. Usually, two acquisition modes are used for capturing the signature, which are off-line mode and on-line mode, respectively. The off-line mode allows generating a handwriting static image from a scanning document and used for analysis. In contrast, the on-line mode allows generating from pen tablets or digitizers and analysis is based on dynamic information such as force, speed and rushing HSV systems are suited for forgery detection as they
are cheap and nonintrusive and provide a direct link between the writer's identity and the transaction.
The objective of signature verification systems is to differentiate between original and forged signature, which is related to intra-personal and inter-personal variability. Intra-personal variation is variation among the signatures of the same person and inter-personal is the variation between the originals and the forgeries. There will always be slight variations in a human's handwritten signature, the consistency generated by natural motion and practice over time generates a recognizable pattern that makes the handwritten signature suitable for biometric identification. This technology has certain advantages as well as disadvantages associated with it. Some of the advantages being [14]:

1) The signature is the usually established of all the ways in which we look for confirm our identity.
2) Use of signature verification will reduce the disruption to received practices with respect to transactions where Personal verification has to be authenticated.
3) Measurement of signature image individuality is noninvasive and having no negative or undesirable health connotations.

Disadvantages:

1) There are some inconsistencies to a person's signature [2].
2) Great unevenness can be observed in signatures depending upon age, country, time, habits, psychological or mental state, physical and practical conditions.

II. SIGNATURE VERIFICATION CONCEPT

A signature is any written specimen in a person's own handwriting meant to be used for identification. A signature verification (SV) system authenticates the identity of any person, based on an analysis of his/her Signature through a set of processes which differentiates a genuine signature from a forgery signature. The precision of signature verification systems can be expressed by two types of error: the percentage of genuine signatures rejected as forgery which is

Manuscript received Aug, 2013.
***Surabhi Garhawal*, Gyan Ganga college of Technology, Jabalpur (M.P)**
***Neeraj Shukla**, Dept. of computer science* **Gyan Ganga college of Technology, Jabalpur (M.P)**

called False Rejection Rate (FRR); and the percentage of forgery signatures accepted as genuine which is called False Acceptance Rate (FAR).While dealing with any signature verification system, we take FRR and FAR as its performance estimate parameters.

III. TYPES OF FORGERIES

A signature forgery means an attempt to copy someone else's signature and use them against him to steal his identity there can be basically three types of forgeries [1]: Both offline and online systems are used to detect various types of forgeries.

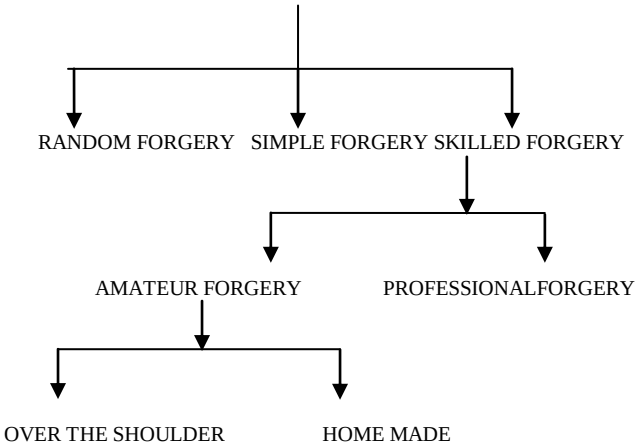

Figure 1.1 Classification of forgeries

Signature forgeries are classified as follows [7], [4], [8], [14]:

1) **Random/simple or zero effort**. The forger doesn't have the shape of the writer signature but comes up with a draw of his own. He may derive this from the writer's name. This forgery accounts for majority of forgery cases though it's easy to detect with naked eyes.
2) **Simple /casual forgery**. The forger knows the writers signature shape and tries to imitate it without much practice.
3) **Skilled forgeries**. This is where the forger has unrestricted access to genuine signature model and comes up with a forged sample.

The skilled forgery category has been classified further into amateur and professional forgery. A professional forgery is done by a person with professional expertise in handwriting analysis and is able to come up with high quality forgery. The amateur forgeries are again categorized in the context of online verification into home improved and over the shoulder forgeries. In home improved the forger has a paper copy of the signature and has ample time to practice at home. The reproduction is based on static features of the image. And over the shoulder forgeries are produced when immediately the forger has witnessed the writer make a genuine signature; the forger in this case has dynamic properties of signature and spatial image [8], [14].

Figure 1.2 Genuine and Forgery signature

VI. DEFINITION OF TERMS

Definition of some terms that are used as follows:

Pattern Matching is the description or classification of measurements based on underlying model [10].
False Rejection (FR) is when a genuine signature is rejected as a forged signature [10].Suppose that it is known for a fact that a given signature has been signed by a particular person, which is genuine. But, if the system refutes this clam and rejects this signature as not that particular person, such cases of rejection are termed as false rejection.
False Acceptance (FA) is when a forged signature is accepted as a genuine signature [10].Suppose that it is known for a fact that a given signature does not belong to a person A. however, on comparing with feature vector of person A, if the system accepts the signature as belonging to the person A, then such cases of acceptance are termed as false acceptance.
False Rejection Rate (FRR) is ratio of the number of genuine signatures rejected to the total number of genuine signatures submitted [8].
False Acceptance Rate (FAR) is ratio of the number of forged signatures accepted to the total number of forged signatures submitted [8].
Average Error Rate (AER) is the average of FAR and FRR [8].
Equal Error Rate (EER) is a point where FAR and FRR are equal [8], [14].

IV. BASIC PROCEDURE OF HSV

Offline handwritten signature verification is a pattern recognition problem and a typical pattern recognition system has the following steps:

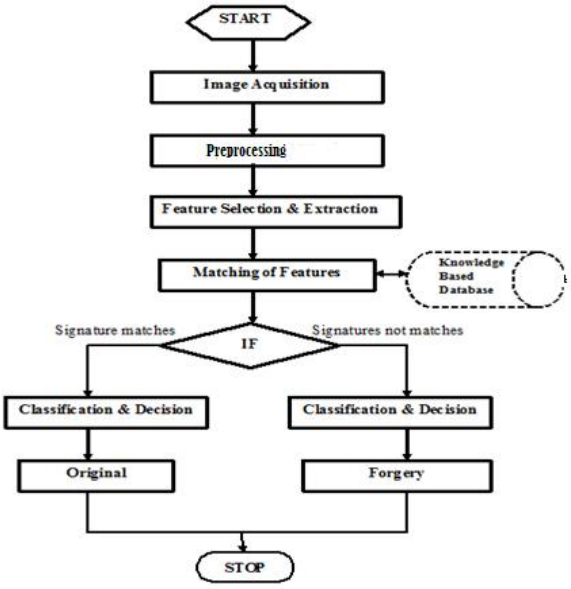

Figure 1.3 Workflow of signature verification system

1. Image Acquisition

For offline signature verification system, images of the signatures are scanned using a digital scanner. Scanned images are stored digitally for offline processing.

2. Preprocessing

The purpose of pre-processing phase is to make signatures standard and ready for feature extraction. The pre-processing stage primarily involves some of the following steps:

1) **Noise reduction**: A noise filter is a normalization that applied to remove the noise caused during scanning and improves the quality of document.
2) **Resizing**: The image is cropped. Then zoom in or zoom out, to the bounding rectangle of the signature
3) **Binarization**: it is the process of transformation from color to grayscale and then converts to binary image.
4) **Thinning**: The goal of thinning is to eliminate the thickness differences of pen by making the image one pixel thick. The aim of this is to reduce the character features to help in feature extraction and classification.
5) **Clutter Removal**: Any unconnected black dots are removed before processing and this is done by masking.
6) **Skeletonization**: Skeletonization is used to remove selected foreground pixels from the binary image. So the outcome is a representation of a signature pattern by a collection of thin arcs and curves.

3. Feature Extraction

Features extracted for off-line handwritten signature verification can be broadly divided into three main categories:

1) **Global features**– The signature is viewed as a whole and features are extracted from all the pixels confining the signature image. Based on the style of the signature, different types of Global features are extracted. Signature area (Signature Occupancy Ratio), Signature height-to-width ratio, Maximum horizontal histogram and maximum vertical histogram, Image area, Edge point numbers of the signature, Signature height, Horizontal and vertical center of the signature Image area, Pure width, Pure height, Vertical projection peaks, Horizontal projection peaks Number of closed loops Local slant angle Number of edge points Number of cross points Global slant angle Baseline shift.
2) **Local features** – Local features are extracted from a portion or a limited area of the signature image. It applied to the cells of a grid virtually super imposed on a signature image or to particular elements obtained after signature segmentation. These features are calculated to describe the geometrical and topological characteristics of local segments. These features are generally derived from the distribution of pixels of a signature, like local pixel density or slant.
3) **Geometric features**– These features describe the characteristic geometry and topology of a signature and preserve their global as well as local properties. Geometrical features have the ability to tolerate with distortion, style variations, rotation variations and certain degree of translation.

Classification:

The classification stage is the decision making part of the recognition system. The performance of a classifier relies on the quality of the features. There are many existing Classical and soft computing techniques for handwriting identification. They are given as:

1) **Classical Techniques:**
- Template matching
- Statistical techniques
- Structural techniques

2) **Soft Computing Techniques:**
- Neural networks (NNs)
- Fuzzy- logic technique
- Evolutionary computing techniques

V. Approaches to Signature Verification

Template Matching- Fang et al. [3] proposed two methods for the detection of skilled forgeries using template matching. One method is related to the optimizing matching of the one-dimensional projection profiles of the signature patterns and the other is based on the elastic matching of the strokes in the two-dimensional signature patterns. Given a test signature to be verified, the positional variations are compared with the statistics of the training set and a decision based on a distance measure and both binary and grey-level signature images are tested. The average verification error rate of 18.1% was achieved when the local peaks of the

vertical projection profiles of grey-level signature images were used for matching and for full estimated covariance matrix incorporated [5]. True verification performance is affect by the variation of signature stroke widths and a registered signature image selected from a collection of samples in off-line signature verification using a pattern matching scheme.
Katsuhiko Ueda in [6] proposed the modified pattern matching method, in which independent of signature stroke width and collection of a registered signature image for Japanese signature verification. Experimental results showed that the proposed methods improve the identification.

Neural Networks- The proposed system [12] using structure features from modified direction feature and other features as surface area, length skew and centroid feature where signature is divided into two halves and for each half a position of the centre of gravity is calculating with reference to the horizontal axis. For classification two approaches are compared the Resilient Backpropagation (RBP) neural network and Radial Basic Function(RBF) using a database of 2106 signatures containing 936 genuine and 1170 forgeries. These two classifiers register 91.21% and 88 % true verification respectively.
The works of Alan McCabe [17] Several Network topologies are tested and their accuracy is compared. The most successful version of the NN based HSV system uses a single MLP with one hidden layer to model each user's signature. It is trained using five genuine signatures and one hundred zero-effort forgeries. Using this approach, a 3:3% OER is reported for the best case.
In [21] signature is captured and presented to the user in an image format. Then Signatures are verified cbn using parameters extracted from the signature based on various image processing techniques. It helps in detecting the exact person and it provides more accuracy of verifying signatures as compared to prior works. For verification of signatures some novel features needs to be extracted. For implementation of above this paper uses Feed Forward Neural Network (FFNN) for recognition and verification of signatures of individuals.

Hidden Markov Model- The approach of Justino et al [9] uses the graphometric features, that is static features like the density of pixels and the pseudo dynamic features represented by axial slant. They employ grid segmentation and divide the signature image into four zones each with column containing cells with horizontal and vertical projections. Each column is changed to a characteristic vector assigned a numeric value. HMM is used for the learning and verification process.
In [13], a system is introduced that uses only global features. A discrete radon transform which is a sinograph is measure for each signature binary image at range of $0 - 360$ _, which is a function of total pixel in the image and the intensity per given pixel calculated using non overlapping beams per angle for X number of angles. Because of this periodicity, it is shift, rotation and scale invariant. HMM is used to model each writer signature. The method achieves an AER of 18.4% for a set of 440 genuine signatures from 32 writers with 132 skilled forgeries.
The inference taken form [19], the signature to be trained or recognized is vertically divided into segments at the centre of gravity using the space reference positions of the pixels. Number of segmented signature blocks is equal to the number of states in the HMM for each user notwithstanding the length of the signatures. That shows successful signatures a recognition rate of 99.2% is possible.

Fuzzy Logic Based Approaches-In [16], global features of the signature like the skeleton of the pen trace and the structure of upper and lower envelope are used as shape descriptors. These are obtained by sampling upper and external points from the binary image of the signature. High pressure regions where the writer made more pressure or emphasis to be generated to a linear function that is be used for maximizing the correlation between the vertical and horizontal projections of the skeleton. For each of the above shape descriptors a multi- layer perception is assigned and the network is trained with a modified back propagation algorithm and the output of each individual network is combined through a fuzzy integral voter. Using a test set of 1000 signatures the approach obtained 90% true verification.
The authors in [15] propose the system that extracts angle features that are modeled in to a fuzzy model based on Takagi-Sugeno model. The model is extended to include structural parameters that account for variation in writer's styles and changes in mood and the inputs are optimized to derive multiple rules. This approach obtained over 70% true verification.
In [20] find points as control points on the boundary of the signature. These points are locations of the boundary; show the structural characteristics of a signature. Four different types of local features are extracted from control points on set of training signatures and these features fuzzified for training of FIS. According to that output of FIS, after that make decision that test signature is forgery or genuine. Effectiveness of the algorithm depend on variations between training signatures so if the training signatures of the specific person are not enough similar to each other, the algorithm cannot have good performance and FAR (False Acceptance Rate) will grow.

Statistical approach- Using statistical information, the relation, variation, etc between two or more data items can easily be determined. Strictly speaking, to find out the relation between some collected data items we generally follow the rule of Correlation Coefficients. Statistical based on departure of two variables from independence. To verify an entered signature with the help of an average signature, which is obtained from the set of, previously collected signatures, follows the concept of correlation to find out the amount of divergence in between them.
A Bayesian model is used for off-line signature verification including the representation of a signature throughout its curvature is generative for specify the knots in an rough calculation limited to a buffer region close to a template curvature, beside independent time warping scheme. In this case, prior shape information about the signature can be built

into the analysis. The observation model is related to additive white noise superimposed on the underlying curvature. This approach is implemented using Markov chain Monte Carlo (MCMC) algorithm and used as set of standards instances of Shakespeare's signature.

Support Vector Machine -Support Vector Machines (SVMs) are machine learning algorithms that use a high dimensional feature space and estimate differences between classes of given data to generalize unseen data. The system in [11] uses global, directional and grid features of the signature and SVM for classification and verification. The database of 1320 signatures is used from 70 writers. 40 writers are used for training with each signing 8 signatures thus a total of 320 signatures for training. Intended for first testing the approach uses 8 original signatures and 8 forgeries achieves FRR 2% and FAR 11%.
In[18] Discrete Radon Transform used for extract global features from the signatures. During enrollment, a number of reference signatures are used for each registered user and cross aligned to extract statistics about that user's signature. We experimented with SVM classifier and KNN classifier. Using a database of 2250 signatures (genuine signatures and skilled forgeries) from 75 writers our present system achieves a performance of approximately 80 % when used SVM classifier and a performance of approximately70 % in the case of KNN classifier.
In proposed system [22] Signature database was utilized for training the SVM .Then the signature verification accuracy of the model has been evaluated in terms of FAR, FRR and FIR. Accordingly, SVM described in this paper successfully verifies the off-line signature with 90% accuracy.

Structural or syntactic approach- Idea of structural and syntactic pattern recognition is to provide the patterns by means of symbolic data structures such as strings, trees, and graphs. To recognize an unknown pattern (forged signature), it's symbolic representation of comparing with a number of prototypes stored in a database. Structural features use modified direction and transition distance feature (MDF) which extracts the transition locations and are based on the relational organization of low-level features into higher-level structures. The Modified Direction Feature (MDF) [16] utilizes the position of transitions from environment of foreground pixels in the vertical and horizontal directions of the boundary represent an entity.
Nguyen et al [1] presents a new method in which structural features extraction from the signature's contour using the (MDF) which extended version: EMDF, then two neural network-based techniques and Support Vector Machines (SVMs) are investigated and compared for the process of signature verification. The classifiers were trained based on genuine specimens and some other randomly selected signatures taken publicly existing database of 3840 genuine signatures from 160 volunteers and 4800 targeted forged signatures. A distinguishing error rate (DER) of 17.78% was obtained with the SVM whilst keeping the false acceptance rate for random forgeries (FARR) below 0.16%.

VI. COMPARISON

All type of forgery requires different verification methods. Hence it becomes mandatory to compare these approaches with respect to various levels of forgeries.

Template matching is appropriate for rigid matching to detect genuine signatures however these methods are not very efficient in detecting skilled forgeries.

Neural networks are along with the generally used classifiers for pattern recognition problems. This approach offers a significant advantage that each time we want to add a set of signatures (a new person) to the systems database; we only have to train three new small neural networks which provides promising results with very low FAR and FRR.

When using HMMs for signature verification, we can easily determined that the Simple and random forgery error rates have shown to be low and close to each other, but the type II error rate in skilled forgery signatures are high. One of the most important properties is the existence of efficient algorithms to automatically train the models without any need of labeling pre segmented data.
Fuzzy set reasoning is a technique that employs fuzzy set elements to describe the similarities between the features of the characters. Fuzzy set elements give more realistic results when there is not a priori knowledge about the data, and therefore, the probabilities cannot be obtained. The literature informing different approaches related to this technique such as fuzzy graphs, fuzzy rules, and linguistic fuzzy.

Methods based on the statistical approach are generally used to identify random and simple forgeries. So that these approaches have proven to be suitable for relating characteristics based on the signature shape. The graphometry-based approach has many features that can be used as proportion, base behaviors, guideline and calibration. Extra features are pixel density and pixel distributions. Where, static features do not describe adequately the handwriting motion. So, it is not enough to detect skilled forgery.

Support Vector Machine (SVM) is based on the statistical learning theory (Vapnik, 1995) and quadratic programming optimization. An SVM is basically a binary classifier and multiple SVMs can be combined to form a system for multi-class classification. For a long times, SVM has received increasing attention in the community of machine learning due to its excellent generalization performance. More recently, some SVM classification systems have been developed for handwriting character recognition, and some hopeful results have been reporting in structural techniques the characters are represented as unions of structural primitives which are assumed that the character primitives extracted from handwriting are quantifiable, and one can find the relationship among them.

Structural techniques are fitting for detecting genuine signatures and targeted forged signatures, in this approach due to demand for large training sets and computational efforts.

VII. CONCLUSIONS

This paper presents a brief survey of the recent works on off-line signature recognition & verification. Different existing approaches are discussed .As we could observe that lots of work has already been done in the field of signature verification; there are still many challenges in this research area. The non-repetitive personality of variation of the signatures, because of age, sickness, geographic location and some extent the emotional state of the person, accentuates the problem. Another problem associated with this category is, for security reasons, it is not very easy to make a signature dataset of real documents such as banking documents, and academic certificates are available for signature verification community. Publicly available signature datasets of real documents would make it possible for researchers to achieve a better performance in this field.

VIII. REFERENCES

[1] Rasha Abbas and Victor Ciesielski, "A Prototype System for Off-line Signature Verification Using Multilayered Feed forward Neural Networks," February 1995.

[2] MI C. Fairhurst, "Signature verification revisited: promoting practical exploitation of biometric technology", Electronics & communication engineering journal, Dec 1997.

[3] B. Fang, Y.Y. Wang, C.H. Leung, Y.Y. Tang, P.C.K. Kwok, K.W. Tse and Y.K. Wong, "A Smoothness Index Based Approach for Off-line Signature Verification", 2000.

[4] Z. Lin. W. Liang. And R. C. Zhao, "Offline signature verification Incorporating the prior model," International Conference on Machine Learning and Cybernetics, vol. 3, pp. 1602–1606, 2003.

[5] B. Fang, C.H. Leung, Y. Y. Tang, K. W. Tse, P. C. K. Kwok, and Y. K. Wong, "Off-line signature verification by the tracking of feature and stroke positions," Pattern Recognition, vol. 36, pp. 91–101, 2003.

[6] Katsuhiko Ueda, "Investigation of Off-Line Japanese Signature Verification Using a Pattern Matching", Proc.Of the 7th ICDAR, 2003.

[7] S. Srihari. K. M. Kalera. And A. XU, "Offline Signature Verification and Identification Using Distance Statistics," International Journal of Pattern Recognition And Artificial Intelligence, vol. 18, no. 7, pp. 1339–1360, 2004.

[8] B. Herbst. J. Coetzer. And J. Preez, "Online Signature Verification Using the Discrete Radon Transform and a Hidden Markov Model," EURASIP.Journal on Applied Signal Processing, vol. 4, pp. 559–571, 2004.

[9] M. Blumenstein, X. Y. Liu, and B. Verma, "A Modified Direction Feature for Cursive Character Recognition," in International Joint Conference on Neural Networks, pp. 2983- 2987, 2004.

[10] T.S. enturk. E. O¨ zgunduz. And E. Karshgil, "Handwritten Signature Verification Using Image Invariants and Dynamic Features," Proceedings of the 13th European Signal Processing Conference EUSIPCO 2005, Antalya Turkey, 4th-8th September, 2005.

[11] T.S. enturk. E. O¨ zgunduz. And E. Karshgil, "Handwritten Signature Verification Using Image Invariants and Dynamic Features," Proceedings of the 13th European Signal Processing Conference EUSIPCO 2005, Antalya Turkey, 4th-8th September, 2005.

[12] M. Blumenstein. S. Armand. And Muthukkumarasamy, "Off-line Signature Verification using the Enhanced Modified Direction Feature and Neural based Classification," International Joint Conference on Neural Networks, 2006.

[13] Vu Nguyen; Blumenstein, M.; Muthukkumarasamy V.; Leedham G., "Off-line Signature Verification Using Enhanced Modified Direction Features in Conjunction with Neural Classifiers and Support Vector Machines", in Proc. 9th Int Conf on document analysis and recognition, volume 02, pp. 734-738, Sep 2007.

[14] S. I. Abuhaiba, "Offline Signature Verification Using Graph Matching," Turk J Elec Engine, vol. 15, no. 1, 2007.

[15] Check fraud statistics, "National fraud centre," http://www.ckfraud.org/statistics.html - Retrieved February 22, 2008,

[16] Bank of Uganda, "Bank fraud," http://www.bou.or.ug/BANKFRAUD.pdf-Retrieved February 22, 2008.

[17] Alan McCabe," Neural Network-based Handwritten SignatureVerification".JOURNAL OF COMPUTERS, VOL. 3, NO. 8, AUGUST 2008

[18]A. A Abdulla Ali," OFFLINE SIGNATURE VERIFICATION USING RADON TRANSFORM AND SVM/KNN CLASSIFIERS", ISSN 0136-5835. 2009.

[19] Dr. S. Adebayo damramola "Offline Signature Recognition using Hidden Markov Model (HMM)" International Journal of Computer Applications 2010.

[20]M.Nasiri, "A Fuzzy Approach for the Automatic Off-line Signature Verification Problem Base on Geometric Features"2012.

[21]Ms. Vibha Pandey **"**Signature Verification Using Morphological Features Based on Artificial Neural Network". International Journal of Advanced Research in Computer Science and Software Engineering Volume 2, Issue 7, July 2012.

[22] Mandeep Kaur Randhawa "Off-line Signature Verification based on Hu's Moment Invariants and Zone Features using Support Vector Machine". International Journal of Latest Trends in Engineering and Technology (IJLTET) Vol. 1 Issue 3 September 2012.