International Journal of Research
Available at https://edupediapublications.org/journals

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue14
November 2017

# Artificial Intelligence with Verifiable Digital Signature Patterns

Arun Kumar Silivery & Suvarna S
1 Dept of CSE, Raja Mahindra College of Engineering, Ibrahimpatnam, Hyderabad
2 Assistant Professor, Dept of CSE, Raja Mahindra College of Engineering, Ibrahimpatnam, Hyderabad

## Abstract

*To accomplish more reliable verification or reorganization we should utilize something that truly characterizes the given individual user. Biometrics offer computerized strategies for identity verification or recognition on the standard of measurable physiological or behavioral properties, for example, a signature or a voice test. To avoid from signature forgery and guarantee the secrecy of Information in the field of Information Technology Security an indivisible piece of it. Keeping in mind the end goal to manage security, Authentication plays a important part. This paper describes a view on the signature reorganization method and we additionally talked about an innovation of Signature Authentication by Back propagation Algorithm with application. The reason for this method is to guarantee that the rendered administrations are obtained to just by a trusted client, and not any other person. By utilizing this technique it is conceivable to confirm or build up an individual person's identity. This procedure is appropriate for different applications, for example, bank money transactions, visas etc. We have illustrated sentiments about the convenience of signature authentication frameworks, comparison between various procedures and their preferences and issues in this paper.*

***Keywords:*** - Recognition, neural network, signature, pattern recognition, authentication, and security.

## I. INTRODUCTION

Biometric security is an automated strategy for verifying a user’s identity in the view of his/her body and additional physical properties. Different types of biometric security exist including fingerprinting, iris identification, voice reorganization, heart sound identification, and keystroke reorganization. In any case, despite the curiosity what's more, seen security of the aforemention procedures, the longest standing and most regular technique for checking one's identity is using a written by hand signature. Handwritten Signature Verification (HSV) is an automated strategy for checking a signature by extracting features includes about a signature's shape and the characteristics of how the individual signs his/her name in present (i.e., dynamic features). HSV is all the more for the most part accepted by people in general and is less intrusive than other biometric authentication procedures. There are two procedures are available in the signature authentication techniques. To begin with approach requires discovering data and can identify signature as the outcome of the framework and it is seen that in a specific time interval, it is important to make the signature. This framework models the signing individual and other approach is to take a signature as a static two-dimensional picture which does not contain whenever related data. In short, signature reorganization can be classified into two types. Those are online and offline signature reorganizations. In online signature reorganization, where signatures are required during the writing process with an exceptional instrument, for example, pen tablet. Indeed, there is constantly dynamic data available if there should be an occurrence of online signature verification, for example, speed, acceleration and pen weight. The offline signature reorganization just manages signature pictures received by a scanner or a computerized camera. All in all, offline signature recognition and identification is a critical issue. Not at all like the online signature is verification, where dynamic parts of the signing activity are received specifically as the handwriting direction, the dynamic data contained in offline signature recognization very degraded. Handwriting functions, for example, handwriting arrange, writing speed variation, and skillfulness, should be accessed from the grey level pixels. Signature reorganization methodology utilizes the dynamic investigation of a signature to validate users. The method depends on measuring speed, pressure furthermore, point utilized by the individual user when a signature is generated. This method utilizes the person's handwritten signature as a basis for validation of entities and information. An electronic drawing tablet and stylus are utilized to record the signature direction, speed and facilitates of a handwritten signature. There is no encryption or message validation offered yet with signature flow; however more current examples utilize one way hash capacities to encrypt the signature elements and information and append it to the record being signed upon. In one cycle, made by Topaz Systems, the signature really disappears from see if the report is corrupted with after signature.

## ARTIFICIAL NEURAL NETWORK

Artificial neural systems are models proposed by the mind that is equipped of machine learning and pattern reorganization. They are generally exhibited as organization of interconnected "neurons" that can measure values from inputs by giving data through the network system. Neural systems are typically organized in layers. Layers comprise of various interrelated 'nodes' which hold an 'active work'. Examples are readily available to the system by methods for the 'input layer', which connects to at least one 'hidden layers' the place the solid processing is finished using a framework of subjective 'connections'. The hidden layers at that point join to a 'output layer' where the appropriate response is final output of the framework as appeared in the figure. To better understand artificial neural processing it is fundamental to be know how a conventional PC forms data. A serial system has a principal processor that can address a variety of memory areas where information and directions are put away. Calculations are made by the processor by interpretation of direction as well as information that guideline requires. At that point direction is executed and comes about are saved in a memory area as necessary. In a regular framework the computational steps are deterministic, sequential and proper rational, and the status of a given variable can be track from one operation to another. Interestingly, Artificial neural system i.e. ANNs are definitely not sequential or basically deterministic. There are no complicated central processors, to a specific degree there are various uncomplicated ones which for the most part do just take the weighted summation of their contributions from different processors. ANNs don't execute programmed statement protocols; they respond in parallel to the example of information sources offered to it. There are no different memory locations to accumulate information. Data is controlled in the general activation 'state' of the system. 'Knowledge' is described to by the system itself, which is genuinely more than the summation of its individual parts. In spite of the fact that there are numerous distinct types of information rules utilized by neural systems, this articulation is worried about the delta rule the show. The delta manage is often use by the most normal class of ANNs called 'back propagation neural systems'.

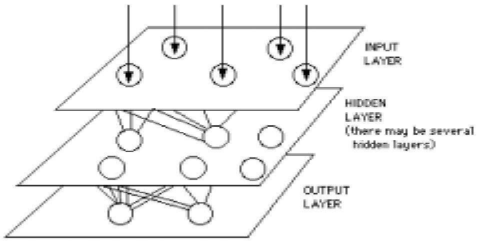


**Figure. Simple Neural Network Diagram.**

## II. IMPLEMENTATION

This implementation describes the methodology behind the system development. The signature recognition system is specifically classified into three major subparts. Preprocessing, Feature extraction, Recognition and Verification.

***2.1 Preprocessing:*** A signature database was designed in order to encourage the HSV experimentation. A standout amongst the most unfortunate aspects of present HSV research is the thousands of standard databases. This is a main burden for scientists who need to invest a lot of amount of time capturing their own information. Moreover, utilizing distinctive databases makes it practically difficult to perform important comparisions between various HSV frameworks. It describes the criteria for an efficient signature database:

*High sample size:* In HSV most analysts tend to work with dataset of more than one thousand signatures. The more signatures utilized and the more assorted the dataset, the more reliable the captured error rates are.

*Diversity of samples*: The framework must simulate a practical environment utilizing signers of various age groups, sex groups, nationalities, foundations and left and right handedness.

*No arbitrary prohibition:* It is unsuitable to remove "unwanted" or "inappropriate" signers, or those are not prone to functional work with the proposed framework. It is important to incorporate all accessed signatures in the database.

*Inclusion of skilled forgeries*: It is harder to get skilled forgeries than honest to goodness signatures, yet without the consideration of skilled forgeries, quoting false elimination rates is far less significant.

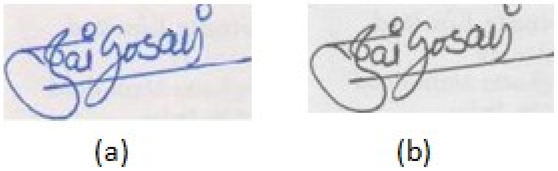


**Figure 1: (a) the sampled signature captured from the handwritten word. (b) Input Database signature image of the word.**

***a) Noise Reduction:*** Signatures are polluted because of originating from decoding issues or noisy channels. A picture additionally gets degraded on account of the inconvenient impacts due to illumination and different objects in the environment. Median filter is widely utilized for smoothing and reestablishing pictures despoiled by noise. This is a nonlinear process valuable basically in minimizing hasty noise. In a median filter, a window slides over the picture, and for every area of the window, the median convergence of the pixels inside it choose the power of the pixel situated in the middle of the window. As weight against to the mean filter, Median filter has striking properties for suppressing drive noise while safeguarding edges; because of this element we are suggested this filter in our proposed framework.

***b) Background Elimination***: Various picture processing applications require isolation of objects from the previous foundation. Thresholding is the most inconsequential and effortlessly proper strategy for this. We utilized Thresholding strategy for recognize the signature from the previous foundation. In proposed application, we are focuses in dark objects on light background and thus an edge value T entitled as the brightness threshold is appropriately selected and connected to picture. After the Thresholding, the pixels of the signature would be 1 and alternate pixels which have a place with the foundation would be 0. The brightness threshold can be picked with the end goal that it fulfills the following calculations; suppose image pixels f(x, y) then, If f(x, y) ≥ T Then f(x, y) = Background Else f(x, y) = Object.

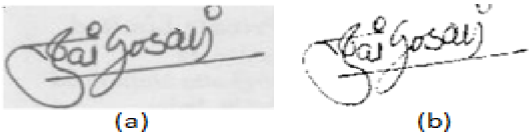


**Figure 2: (a) Image with background, (b) Image after Thresholding**

***c) Signature Normalization:*** Inconsistency in signature capturing and filtering process makes measurements of signature fluctuate. The picture measurements like height and width of signatures fluctuated from user to user and formally even a similar user may work out distinctive sizes of signatures. Along these lines it is expected to gain of the size variation and accomplish a benchmark signature size for all input signatures. All through the normalization process, the trademark ration between the width and height of a signature is kept undamaged what's more, after the procedure; every one of the signatures will have the comparable dimension. Normalization process made utilize of the given calculations:

$$X_{new} = [(X_{old} - X_{min})/\ (X_{max} - X_{min})]*M$$

$$Y_{new} = [(Y_{old} - Y_{min})/\ (Y_{max} - Y_{min})]*M$$

Where $X_{new}$ and $Y_{new}$ are pixel arguments for the normalized signature, $X_{old}$ and $Y_{old}$ are Pixel arguments for the original signature, M represents height and width meant for the normalized signature. The normalization procedure is confirmed in the subsequent figure.

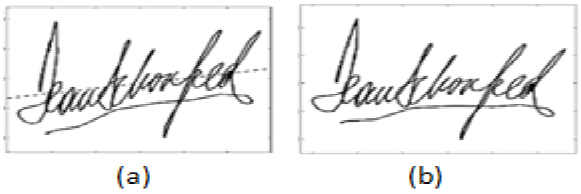


**Figure 3: (a) Original Signature and (b) Signature after Normalization**

***d) Thinning Process*** The aim of thinning is to minimize the thickness differences of pen by making the picture one pixel thick. Thinning was proposed to describe the global properties of objects and to minimize the original signature into a more compact representation. It uses a Stentiford algorithm for thinning process.

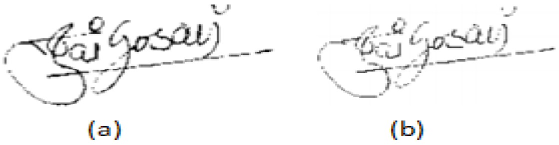


**Figure 4: (a) Signature before Thinning and (b) Signature after Thinning**

***2.2 Feature Extraction:*** The features accessed from signatures or handwriting acts an impartment role in the achievement of any feature based HSV framework. They are the most essential perspective, exceeding the selection of model or similarity means. In the event that a poorly designed feature set is utilized with little understanding into the writer's common style, at that point no amount of modeling or examination will bring about an effective framework. Further, it is important to have various, significant features in the input vector to ensure useful learning by the NN. The beginning decisions as to which features to fuse, to expand the accuracy, included a mix of concentrating different publications in the region (what other analysts have discovered helpful or helpless) and naturally considering which different features may be generally appropriate. The instinctive approach depended on investigation of the handwriting process, scientific investigation of handwriting by people and examination of features that are generally valuable to people in choosing whether a specific handwriting sample is delivered by some creator. The properties of "helpful" features must fulfill the following three necessities: 1) The author must have the capacity to write in a standard, predictable way (i.e., not unnaturally quick or moderate in request to deliver a specific feature); 2) The author must be fairly detachable from other authors in view of the feature; 3) The features must be condition invariant (remain steady independent of what is being written).

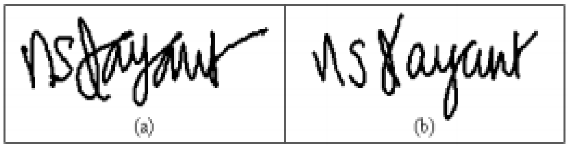


**Figure 5: This illustrates the difficulty that a potential forger has in trying to identify the pen-down ratio. (a) is a genuine signature and (b) is an attempted forgery based on the forger having seen an off-line version of the signature (both taken from the signature database used in this project).**

What takes after now is a description of each of the feature that is extracted from a given signature, also as their importance and technique for computation. Each of these features goes about as a solitary input to the Neural Networks.

***a) Feature extracted using vertical splitting:*** Split the signature picture with vertical line going through its geometric point to get left and right piece of signature .Find geometric point for left and right part. Partition the left part with even line going through its geometric points to get top and bottom part. Locate the geometric points for top and bottom parts of left part correspondingly. So also, the right part is part with a level line at its geometric points to get top and bottom parts of right part correspondingly. Find geometric point for the top and bottom of the correct part. Each piece of the picture is again split utilizing same technique to get thirty vertical feature focuses as appeared in Figure 6 (a).

***b) Feature extracted using horizontal splitting:*** Split the signature picture with horizontal line going through its geometric points to get top and bottom piece of signature. Find geometric points for top and bottom part. Partition the top part with vertical line going through its geometric points to get left and right part. Locate the geometric places for left and right parts of top part correspondingly. Also, the bottom part is part with a vertical line at its geometric points to get left and right parts of bottom part correspondingly. Find geometric place for the left and right of the bottom part. Each some portion of the picture is again part utilizing same technique to acquire thirty flat feature focuses as appeared in Figure 6(b).

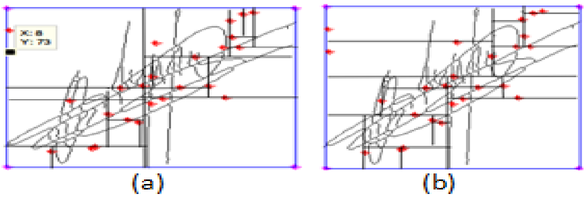
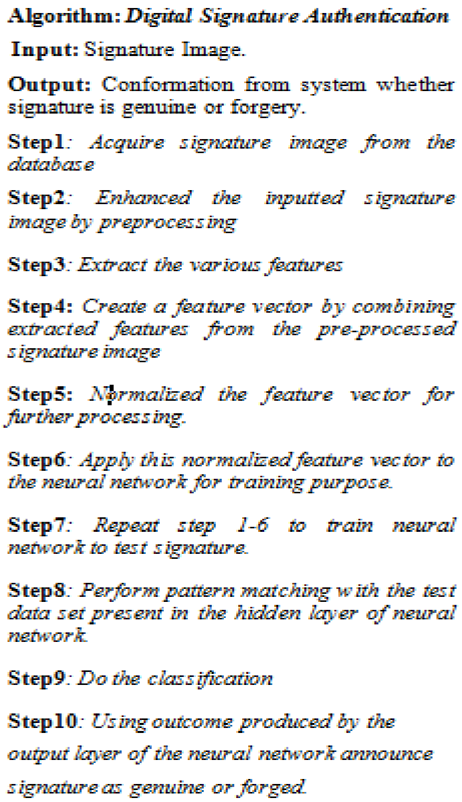


***Figure 6: (a)*** **Signature image after vertical splitting, (b) Signature Image after horizontal splitting**

***2.3 Recognition and Verification:*** The goal of the signature reorganization and verification framework is to describe between two signature classes the authorized and forgery signatures. A bundle of effort has been taken in the field of offline signature verification. Forgery is a fault that goes for corrupted users signatures. Since genuine forgeries are hard to acquire, the instrument and the outcomes of the verification based upon the kind of the forgery. There are fundamentally three types of forgeries as a) Random forgery can ordinarily be represented by a signature test. Forger has no data about the signature style and the name of the individual person. b) Simple forgery is a signature with the same shape or the authentic author's name. c) Skilled forgery is signed by a man who has approached an honest to goodness signature for training. Despite the fact that a vast amount of work is resolved on random and basic forgery detection, all the more hard work is still expected to handle the issue of skilled forgery detection. There is no verification methodologies are proposed which may be manage talented forgeries.

## III. OVERVIEW OF ALGORITHM

This section offers algorithm for the offline signature verification system in which artificial intelligence is used to confirm the trustworthiness of signatures.



**Algorithm:** ***Digital Signature Authentication***

**Input:** Signature Image.

**Output:** Conformation from system whether signature is genuine or forgery.

**Step1**: *Acquire signature image from the database*

**Step2**: *Enhanced the inputted signature image by preprocessing*

**Step3**: *Extract the various features*

**Step4:** *Create a feature vector by combining extracted features from the pre-processed signature image*

**Step5:** *Normalized the feature vector for further processing.*

**Step6**: *Apply this normalized feature vector to the neural network for training purpose.*

**Step7**: *Repeat step 1-6 to train neural network to test signature.*

**Step8**: *Perform pattern matching with the test data set present in the hidden layer of neural network.*

**Step9**: *Do the classification*

**Step10**: *Using outcome produced by the output layer of the neural network announce signature as genuine or forged.*

**Figure 7: Algorithm for Offline Signature Verification using Neural Network**

This described offline signature verification framework offers automated technique for check and recognition by extracting functions that describes each input signature. The approach begins by scanning pictures into the PC utilizing finger based biometric devices; at that point altering their quality through picture enhancement, taken after by feature extraction and neural system training, lastly verifies whether a signature is genuine or forgery.

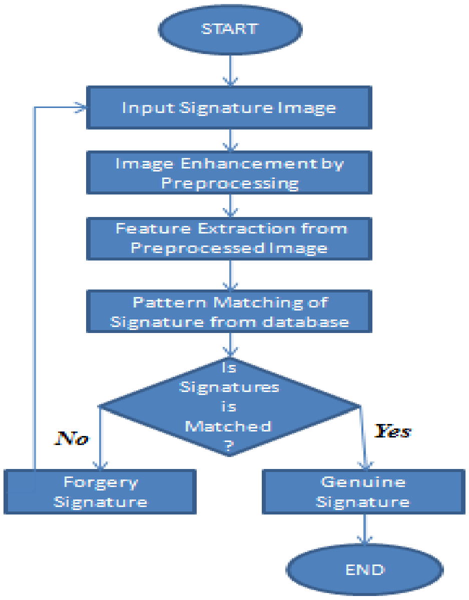

START
Input Signature Image
Image Enhancement by Preprocessing
Feature Extraction from Preprocessed Image
Pattern Matching of Signature from database
Is Signatures is Matched ?
No
Yes
Forgery Signature
Genuine Signature
END

**Figure 8: Flow Chart of system**

## IV. RESULTS AND DISCUSSION

The end result provided in this analysis for preparing and testing of the framework numerous signatures are used. The outcomes about determined in this paper are acquired utilizing the “Grupo de Procesado Digital de Senales" (GPDS) signature database. To prepare the framework, a subset of this database was taken containing of 19 genuine samples taken from each of the 30 individual people also, 19 frauds made by various users for one signature. The design of neural system utilized has input layer, hidden layer and output layer. Subsequent to relating a feature vector of test signature if the output neuron produces value near +1 test signature is described as authentic or on the off chance that it creates value near - 1 it is announced as forgery. The following Figure 9. demonstrates performance graph of the training a two layer feed forward neural network utilizing Error Back Propagation Algorithm (EBPTA).

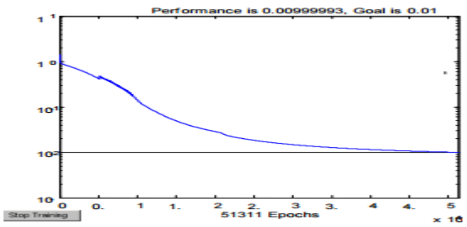


**Figure 9: Performance graph of training a NN using EBPTA**

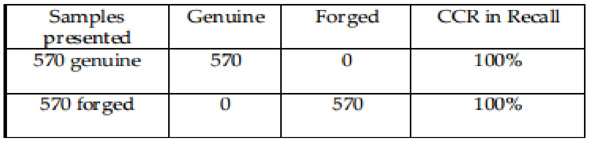
## V. PEROFORMENCE EVALUATION

The genuine and forgery signature tests utilized for training neural system is connected in the testing stage to check regardless of whether neural system classifies it accurately as genuine or forged. This is called Recall. The outcome of recall is as appeared in Table 1. At the point when the neural system was represented with 570 goodness signatures from 30 distinct people, it classified every one of the 570 goodness signatures as genuine and when 570 forged signatures from 30 distinct people were connected it perceived every one of the 570 signatures as forgeries. Up to this point and FRR of the framework is 0%.Hence, Correct Classification Rate (CCR) is 100% for Recall. False Acceptance Rate (FAR), False Rejection Rate (FRR) and Correct Classification Rate (CCR) are the three limitations utilized for measuring performance of framework. Every one of these limitations are measured by following calculations as, FAR = (*Number of forgeries approved/Number of forgeries tested*) * 100

FRR = (*Number of originals rejected/Number of originals tested*) * 100

CCR = (*Number of tests effectively recognized/Number of samples tested*) * 100

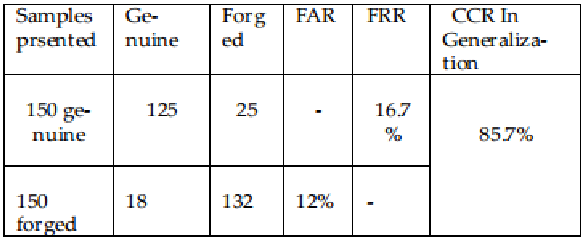
These errors for signature verification utilizing artificial intelligence system are computed during preparing using distinctive iterations.



| Samples presented | Genuine | Forged | CCR in Recall |
|---|---|---|---|
| 570 genuine | 570 | 0 | 100% |
| 570 forged | 0 | 570 | 100% |

**Table 1: Result of Testing Neural Network with Trained Signature Samples**

At the point when the signatures samples not utilized for preparing neural system are applied as sample signatures to the prepared neural system, it is called Generalization. The consequence of generalization is appeared in Table 2.



| Samples prsented | Genuine | Forged | FAR | FRR | CCR In Generalization |
|---|---|---|---|---|---|
| 150 genuine | 125 | 25 | - | 16.7 % | 85.7% |
| 150 forged | 18 | 132 | 12% | - | |

**Table 2: Result of Testing Neural Network with New Signature Samples from Database.**

The neural system when represented with 150 genuine signatures from 30 distinct people arranged 125 signatures out of 150 as real and 25 signatures as forgery. In this manner FRR of the framework is 16.7% .When 150 forgery signatures were given as input to neural system, it classified 18 signatures as authentic also, 132 as forgery. So FAR of the framework is 12%. What's more, thus the Correct Classification Rate is 85.7% for generalization.

## VI. CONCLUSION

This paper describes a technique for offline signature verification utilizing artificial neural system approach. Signatures are checked based on attributes extracted from the signature using different picture processing methods. For verification of signatures some novel functions should be extracted. The extracted functions are used to prepare a neural system utilizing error back propagation preprocessing algorithm. Our reorganization framework describes 100% achievement rate by identifying accurately all the signatures that it was prepared for. Be that as it may, it describes poor analysis when it was given signatures that it was not prepared for before. We didn't think about this as a "high risk" case since verification step is always given by verification step and these types of false positives can be easily caught by the verification framework. Reorganization and verification capacity of the framework can be expanded by utilizing extra features in the informational index. This analysis plans to minimize the instances of fraud in business transactions.

## REFERENCES

[1] O.C Abikoye M.A Mabayoje R. Ajibade "Offline Signature Recognition & Verification using Neural Network", Department of Computer Science University of Ilorin P.M.B 1515, Ilorin, Nigeria, International Journal of Computer Applications (0975 – 8887) Volume 35– No.2, December 2011

[2] Ashwini Pansare, Shalini Bhatia "Off-line Signature Verification Using Neural Network", International Journal of Scientific & Engineering Research, Volume 3, Issue 2, February-2012 1 ISSN 2229-5518

[3] Ms. Vibha Pandey, Ms. Sanjivani Shantaiya, "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 ISSN: 2277 128X

[4] Paigwar Shikha, Shukla Shailja, "Neural Network Based Offline Signature Recognition and Verification System", Department of Electrical Engineering, Jabalpur Engineering College Jabalpur, MP, INDIA, Research Journal of Engineering Sciences ISSN 2278 – 9472, Vol. 2(2), 11-15, February (2013)

[5] Guangyu Zhu, Yefeng Zheng, David Doermann, Stefan Jaeger, "Signature Detection and Matching for Document Image Retrieval", IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE, VOL. 31, NO. 11, NOVEMBER 2009

[6] Yu Qiao, Jianzhuang Liu, Department of Information Engineering The Chinese University of Hong Kong, Xiaoou Tang, Microsoft Research Asia Beijing, China, "Offline Signature Verification Using Online Handwriting Registration".

[7] S.T. Kolhe, S. E. Pawar, Dept. of Computer Engg, AVCOE, Sangamner, India, " Offline Signature Verification Using Neural Network", International Journal of Modern Engineering Research (IJMER), Vol.2, Issue.3, May-June 2012 pp-1171-1175

[8] Cemil OZ, Sakarya University Computer Eng.Department, Sakarya, Turkey, Fikret Ercal,UMR Computer Science Department, Rolla, MO 65401, Zafer Demir, Sakaraya University electric electronic eng. Department sakarya , Turkey, "Signature Recognition and Verification with ANN"

[9] "What is Artificial Neural Networks" http://www.psych.utoronto.ca/users/reingold/courses/ai/cache/neu ral2.html