Journal of Advanced Computing and Communication Technologies *(ISSN:* 2347 - 2804*)*
Volume No.2Issue No. 4, August 2014
(ETACICT-2014)

Computer Vision Approaches for Offline Signature Verification & Forgery Detection: A Survey

By

Gautam. S. Prakash, Shanu Sharma
Student, CSE Department, ASET, Amity University, Noida,Uttar Pradesh, India
Assistant Professor, CSE Department,
ASET, Amity University Noida,Uttar Pradesh, India
gautamsprakash@gmail.com , shanu.sharma1611@gmail.com

ABSTRACT
Automated signature verification and forgery detection has many applications in the field of Bank-cheque processing, document authentication. ATM access etc. Handwritten signatures have proved to be important in authenticating a person's identity, who is signing the document. In this paper, reviews of previous studies and systems to verify signatures and detect forgery is provided and analyzed. Brief summary of computer vision techniques are presented to automate the process. Also, the important features and shortcomings of these systems and studies in this field are summarized in this paper.

Keywords Forgery detection, Signature verification, Artificial Neural Network (ANN), Fuzzy Logic, Computer Vision.

1. Introduction
Forgery is a process by which, identity documents of a person are copied or modified by such a person who is not authorized to do so, or are involved in modification, for the purpose of deceiving others.

Signature, from the Latin word "Signare" meaning "Sign" is a stylized handwritten representation of a person's name or an identification mark that a person writes on documents/texts. For many centuries, signatures have been used as an important element in authentication of any person's identity, who is signing the document. The unique characteristics of a person's signature represents the person's identity and the person's consent for the terms of the document/text. The field of signature authentication is very important and hence the problem of verification and forgery detection is of the utmost importance. Handwritten stylized signatures vary largely from person to person. They differ in their sizes and shapes, and the variations are so much, that for a human being, just by having a glance at the signature, it is very difficult to separate out a genuine signature from a one that is forged.
An automatic signature verification system can either be online or offline. In an online verification system, as the person signs the document/text, the person's signatures are recorded. The merit of such a system is that, a person's dynamic information characteristics can also be accounted. But the problem with such a system is that, in reality, most of the documents are already pre-signed.

Hence to deal with such situations, an offline verification system is used, which only accounts for the static features of a signature.

Image Processing has found number of applications in the field of forensic examination. Image processing has proved to be very effective tool to analyze thousands of signatures in the database, and apply techniques for detailed analysis such as fuzzy logic and artificial neural network to decrease the amount of time, and increase the effectiveness of the system.

For better understanding of further studies, it is important to be acquainted with the basic common concepts such as computer vision technology, and the need for automated signature verification. A brief explanation about them are given below.

1.1. Computer Vision Technology
Computer Vision Technology is used for automating the vision perception process. Computer vision is a field that includes methods for acquiring, processing, analyzing, and understanding images and, in general, high-dimensional data from the real world in order to produce numerical or symbolic information, *e.g.*, in the forms of decisions. Computer vision covers the core technology of automated image analysis which is used in many fields. As a scientific discipline, computer vision is concerned with the theory behind artificial systems that extract information from images. The image data can take many forms, such as video sequences, views from multiple cameras, or multi-dimensional data from a medical scanner. As a technological discipline, computer vision seeks to apply its theories and models to the construction of computer vision systems.

1.2. Need For Automated Signature Verification
Signature verification is very important in realizing tele-banking and tele-networking systems, where signatures can be used to identify and authenticate a subscriber. An automated verification process would enable banks and other financial institutions to significantly reduce check and money order forgeries, which account for a large monetary loss each year. Reliable signature verification can be of great help in many other application areas such as law enforcement, industry, security control and so on. Handwritten signatures appear on many types of documents such as bank checks and credit slip etc. The large volume of such documents makes automatic signature verification desirable. A system for signature verification requires high reliability.

2. Review of Computer Vision and Soft Computing techniques for Offline Signature Verification & Forgery Detection

The problem of signature verification and forgery detection of documents ha long been an interest field in the field of image processing. Many studies have been done till now in order to develop offline signature verification systems using computer vision technology and soft computing techniques. Many researchers are still working on design, development and implementation of an automatic system for fast and much more effective as well as reliable signature verification system.

2.1. Computer Vision Technology

Computer vision is described as automation and integration of a wide range of processes and representations for vision perception. Images can be formed by the system for perception by a range of physical devices, which can include still and video cameras, x-ray devices, electron microscopes, radar, and ultrasound, and used for several purposes, including entertainment, medical, business, industrial, military, civil, security, and scientific. For each case the aim is for an observer, human or machine, to excerpt essential information about the scene being imaged. Computer vision, in some ways, is the inverse of computer graphics as computer graphics produces image data from 3D models, computer vision often produces 3D models from the image data.

2.2 Digital Image Processing

Digital image processing refers to the use of computer algorithms in order to perform image processing on digital images. Through this image processing, one aims to enhance the features of the image that are of interest, while removing the details which are irrelevant to the given application, and then extract the vital information from the enhanced image. The operations of image processing can be divided broadly into three categories, Image Compression, Image Enhancement and Restoration, and Measurement Extraction. Defects in images which could be a result of the digitization process or faults in the imaging set-up (for example, bad lighting & image noise) can be rectified by using Image Enhancement techniques. As soon as the image is in a good condition, the Measurement Extraction operations can be utilized to obtain essential information from the image.

2.3. Soft Computing

Soft Computing refers to a collection of various techniques which uses human mind to formalize cognitive processes. It basically is a term used to refer to the problems whose solutions are unpredictable, uncertain and lies between 0 and 1. It deals with imprecision, uncertainty, partial truth, and approximation to achieve practicability, robustness and low solution costs.

2.4. Soft Computing Techniques

2.4.1. Fuzzy Logic

Fuzzy logic is relatively young theory. Major advantage of this theory is that it allows the natural description, in linguistic terms, of problems that should be solved rather than in terms of relationships between precise numerical values. This advantage, dealing with the *complicated* systems in *simple* way, is the main reason why fuzzy logic theory is widely applied in technique. Using Fuzzy Logic it is also possible to classify the remotely sensed image (as well as any other digital imagery).

Fuzzy logic is a form of many-valued logic. It deals with reasoning that is approximate rather than fixed and exact. Compared to traditional binary sets (where variables may take on true or false values) fuzzy logic variables may have a truth value that ranges in degree between 0 and 1. Fuzzy logic has been extended to handle the concept of partial truth, where the truth value may range between completely true and completely false. Furthermore, when linguistic variables are used, these degrees may be managed by specific functions. Irrationality can be described in terms of what is known as the fuzzjective.

2.4.2. Artificial Neural Networks (ANNs)

In computer science and related fields, artificial neural networks are computational models inspired by animal central nervous systems (in particular the brain) that are capable of machine learning and pattern recognition. They are usually presented as systems of interconnected "neurons" that can compute values from inputs by feeding information through the network.

For example, in a neural network for handwriting recognition, a set of input neurons may be activated by the pixels of an input image representing a letter or digit. The activations of these neurons are then passed on, weighted and transformed by some function determined by the network's designer, to other neurons, etc., until finally an output neuron is activated that determines which character was read.

Like other machine learning methods, neural networks have been used to solve a wide variety of tasks that are hard to solve using ordinary rule-based programming, including computer vision and speech recognition.

For any research work, the literatures are very helpful for the researchers to motivate for the innovation of new ideas for more fruitful results. Till now, researchers have proposed numerous features extraction and classification techniques based on image processing techniques and different classification algorithms. These are the literature surveys regarding the digital image processing in this particular field. By taking the help of these types of researches new research work is evolving in image processing field with the work.

2.5. Related Systems

Md. Iqbal Quraishi et al. [1] have proposed in their paper an Artificial Neural Network approach which implements an Automated Signature Verification and Authentication system. Their method comprises of various transformation techniques from the spatial as well as frequency domain. It also implements the use of Riplet-II transformation to extract the region of interest. To enhance the image, further it implements the use of Log Polar Transformation. They have implemented a Feed Forward Back Propagation Neural Network for the verification and authentication. They have considered 30 neurons in the hidden layer of the ANN The system proposed by the authors, has the accuracy of 96.15%, with the forgery detection rate of 92%. The False Acceptance Rate (FAR) is found to be 5.28%, and False Rejection Rate (FRR) of 2.56%. The authors have compared their system with other existing system and have found that their proposed system has better performance as compared to others. The drawback is that the test needs to be trained before the implementation, which is

time consuming. There can be further improvement is the system with better performance rates.

Othman o-khalifa, Md. Khorshed Alam et al. [2] have reviewed offline signature verification schemes in their paper. They have considered the Artificial Neural Network Technique, and have compared various offline signature verification approaches and their issues. For the pre-processing of the data acquired the have used techniques such as Background Elimination, Noise Reduction, Thinning and Width Normalization. For the purpose of feature extraction, they have considered the global, geometric, texture, mask and grid features. They have explained how the ANN approach works in the signature Verification and what steps are involved. The authors have also pointed out that the main concern of the signature verification system is to provide the high security to access any confidential things those are highly restricted.

Rameez Wajid et al. [3] have evaluated the performance of various classifiers for offline signature verification based upon the local binary patterns (LBP) feature set. They have performed the feature vector by dividing the signature images into twelve local regions and forming a code matrix by their LBPs. The authors have investigated the performance of seven classifiers on The FUM-Persian Handwritten Signature Database (FUM-PHSDB) comprising of 20 classes of genuine and forged signatures of depth 20 and 10 respectively. The classifiers considered by them are Support vector Machines(SVM), Least Squares-Support Vector Machines (LS-SVM), Distance Likelihood ratio Test (DLRT), Artificial Neural Network (ANN), Fisher's Linear Discriminant (FLD), Logistics Discriminant and Naive Bayes. Their experimental findings depict that LS-SVM performs the best among the seven classifiers, achieving the Equal Error Rate (EER) of 13%.

Muhammad Imran Malik et al. [4] have evaluated the impact of two state of the art offline signature verification systems which are based on local and global features respectively. The authors have investigate the performance of automated systems on disguised signatures. The systems were evaluated upon the publically available datasets from signature verification competition. The ICDAR 2009 Offline Signature Verification Competition dataset and the ICFHR 2010 4NSignComp datasets were considered. The offline signature verification systems considered for evaluation were Local Features combined with Gaussian Mixture Models (GMMs) and Global Features combined with k-Nearest Neighbour (kNN). In their experiments it was observed that global features are capable of providing good results if only a detection of genuine and forged signatures is needed. Local features are much better suited to solve the forensic signature verification cases when disguised signatures are also involved.

Juan Hu et al. [5] have presented an offline signature verification system using three different pseudo-dynamic features, two different classifier training approaches and two datasets. Three separate pseudo-dynamic features based on gray level: Local Binary Pattern (LBP), Gray Level Co-occurrence Matrix (GLCM) and Histogram Oriented Gradients (HOG) have been used. The classification is performed using the wrier dependent Support Vector Machine (SVMs) classifier and Global Real Adaboost method. In their experiments, the results of the Equal Error Rate (EER) of skilled forgery test using the writer-dependent approach obtained were 11.73% for LBP, 11.54% for GLCM and 9.83% for HOG. The combination of the three resulted in EER of 7.66%. The results of EER of skilled forgery test using the writer-independent approach obtained were 13.09% for LBP, 19.33% for GLCM, 13.18% for HOG and combination of all three resulted in EER of 9.94%.

Vaibhav Shah et al. [6] have proposed an architecture for offline signature verification that makes the use of runtime signature instead of scanned images for recognition. Their system uses a set of shape based geometric features and focuses on the distance based parameters such as the continuity of the signature and matching of the curve of the signatures generated by the critical points of the respective signature by analyzing the polynomial equation. Curve fitting and the analyzing of polynomial equations is one of the least explored methods and is very efficient. The authors have used feed forward back propagation neural network to verify the authenticity of the signatures. Based on the inputs, the neural network was trained and according to the target values specified, the corresponding outputs and error values are obtained for the particular parameter under test. The authors implemented their code using 75 samples of genuine signatures and received FAR=2% and FRR=5.26%.

M.Nasiri et al. [7] have proposed a system based on fuzzy approach for automatic signature verification. The authors have presented their methodology where they propose to find the points as control points of the boundary of the signature. These boundaries clearly show the structural characteristics of the signature. The authors have extracted four types of local features which are extracted from the control points of the training set of signatures and then these features have been fuzzified for training the Fuzzy Inference System (FIS). Depending on the output of the FIS, the system classifies that the signature is genuine or forged. For each signature, a MAX and MIN value are assigned, if the output of the FIS is between MAX and MIN, thn the signature is classified as genuine and if the output is more than MAX, then it is classified as unskilled forgery and if the value is less than MIN it is classified as skilled forgery. The system proposed by the authors has FRR of 10.3% and FAR of 8.105%.

Surabhi Garhawal et al. [8] have presented a brief survey of the recent works on offline signature recognition & verification. The paper explains the significance of offline signature verification systems and explains about the common used terms related t signature verification. Various techniques such as Template Matching, Statistical techniques, Structural techniques, Neural Networks, Fuzzy-logic technique and Evolutionary Computing Techniques have been discussed in the paper and the merits and demerits of all have been provided and compared.

L.B. Mahanta et al. [9] have presented basic concepts of signature verification and have explored the different approaches for verification. The factors such as physical and psychological state of the person, writing surface and writing material that affect the signature have been discussed. Various performance evaluation techniques such as False Acceptance Rate (FAR), False Rejection Rate (FRR), Equal Error Rate (EER) and Error Tradeoff Curve also have been discussed in the paper. The authors have also thrown light upon the various verification approaches such as Statistical approach, Fuzzy based approach, Neural Network based approach , Wavelet

based approach, Combination of approaches, Clustering technique approach and Support Vector Machine approach.

Pradeep Kumar et al. [10] have proposed an offline signature verification system based upon neural network approach. The signatures are captured and presented to the user in an image format and are verified based upon the parameters extracted from the signature using various image processing techniques. Along with the proposed system, the authors discuss about various other approaches to Hand Written Signature Verification (HSV). The model presented uses neural network classifier for verification. Post the pre-processing, the image is used to train the system. The authors chose the Back Propagation ANN technique as it is easiest to implement, while preserving efficiency of the network. The authors used "Grupo de Procesado Digital de Senales" (GDPS) signature database for testing purposes. The database comprised of 2000 signatures, which comprised of 50 sets from different people. When their proposed system was presented with the signatures used in training, the success rate of the system was 100%. When the system was presented signature samples from a database different than the ones used for training, the success rate of 82.66% was obtained.

3. Analysis & Discussion

A brief survey of the recent works in the field of offline signature verification and forgery detection has been presented in the paper. By performing this survey it was observed that already a lot of work done in the field, but still there are many challenges in this research area.

It was observed that the most successful systems implemented the Artificial Neural Network approach, but the results varied depending upon the choice and the combination of classifiers used and the amount of training provided to the system. It was also observed that the least explored classifier using Curve fitting and the analyzing of polynomial equations showed great success rates.

The variation in personality of signatures, because of age, sickness, geographic location and emotional state of the person actuates the problem. Another problem associated with offline signature verification is that, for security reasons, it is not very easy to make a signature dataset of real documents such as banking documents.

References

[1] Md. Iqbal Quraishi, Arindam Das and Saikat Roy (2013), "A Novel Signature Verification and Authentication System Using Image Transformation and Artificial Neural Netwrok", Narula Institute of Technology, Kolkata.

[2] Othman o-khalifa, Md. Khorshed Alam and Aisha Hassan Abdalla (2013), "An Evaluation on Offline Signature Verification using Artificial Neural Network Approach", International Conference on Computing, Electrical and Electronic Engineering (ICCEEE).

[3] Rameez Wajid and Atif Bin Mansoor, "Classifier Performance Evaluation For Offline Signature Verification Using Local Binary Patterns", Institute of Avionics & Aeronautics, Air University, Islamabad, Pakistan.

[4] Muhammad Imran Malik, Marcus Liwicki and Andreas Dengel, "Evaluation of Local and Global Features for Offline Signature Verification", German Research Center for AI (DFKI GmbH).

[5] Juan Hu and Youbin Chen (2013), "Offline Signature Verification Using Real Adaboost Classifier Combination of Pseudo-dynamic Features", 12th International Conference on Document Analysis & Recognition.

[6] Vaibhav Shah, Umang Sanghavi, Udit Shah, "Off-line Signature Verification Using Curve Fitting Algorithm with Neural Networks", Dwarkadas J. Sanghvi College of Engineering, Mumbai.

[7] M.Nasiri, S.Bayati and F.Safi, "A Fuzzy Approach for the Automatic Off-line Signature Verification Problem Base on Geometric Features", Azad University, Iran.

[8] Surabhi Garhawal and Neeraj Shukla (2013), "A Study on Handwritten Signature Verification Approaches", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), Volume 2, Issue 8, August 2013.

[9] L B. Mahanta, Alpana Deka (2013), "A Study on Handwritten Signature", International Journal for Computer Applications (0975-8887), Volume 79 - No. 2, October 2013.

[10] Pradeep Kumar, Shekhar Singh, Ashwani Garg and Nishant Prabhat (2013), "Hand Written Signature Recognition & Verification using Neural Network", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 3, March 2013.