SIGNATURE RECOGNITION SYSTEM USING ARTIFICIAL NEURAL NETWORK

Yirga Yayeh Munaye[1] and Getaneh Berie Tarekegn[2]

[1]MSC, Department of Information Technology, Collage of Computing and Informatics, Assosa University, Assosa, Ethiopia
[2]PG, Department of Computer Science, Collage of Computing and Informatics, Assosa University, Assosa, Ethiopia,

ABSTRACT: *Security is generally a state or feeling of being saved and protected, an assurance that something of value will not be taken. Security has been described in many ways depending on the area which is been put into consideration. Signatures are used every day to authorize the transfer of funds of millions of people, Bank checks, credit cards and legal documents, all of which require our signatures. Different people sign their signatures with different orientation, size, deviation, etc. Even the signatures of the same individual change temporarily in the aforementioned attributes under different circumstances (e.g. the size of the signing space). To minimize the variation in the final results, all signatures are normalized for duration, rotation, position and size. The pre-processing includes some operations such as scaling and rotation to get a fixed size and direction.*

KEYWORDS: Signature Recognition, Signature

INTRODUCTION

Signatures are a special case of handwriting subject to intra-personal variation and inter-personal differences. Many documents such as forms and bank checks necessitate the signing of a signature, to provide secure means for authentication and authorization [1].

Signature recognition is the process of verifying the writer's identity by checking the signature against samples kept in the database mostly to describe the ability of a computer to translate human writing into text. The result of this process is usually between 0 and 1 which represents a fit ratio (1 for match and 0 for mismatch) [4]. Signature recognition and verification involves two separate but strongly related tasks: one of them is identification of the signature owner, and the other is the decision about whether the signature is genuine or forged. This may take place in one of two ways:

An offline technique, signature is signed on a piece of paper and scanned to a computer system. By using peripheral units for measuring hand speed and pressure on the human hand when it creates the signature **An On-line Technique,** signature is signed on a digitizer and dynamic properties. Like speed, pen pressure (that makes the signature more unique and more difficult to forge) is captured in addition to the shape of the signature.

Types of forgery

The main task of any signature verification system is to detect whether the signature is genuine or counterfeit. Forgery is a crime that aims at deceiving people. Basically there are three types that have been defined: **Random forgery**: this can normally be represented by a signature sample that belongs to a different writer i.e. the forger has no information whatsoever about the signature style and the name of the person. **Simple forgery**: this is a signature with the same shape or the genuine writer's name. **Skilled forgery**: this is signed by a person who has had access to a genuine signature for practice [2].

Statement of the problem

- The closest similarity of signatures in different persons
- The intra variation of signatures in the same persons
- The spread of forgery from time to time

Objective of the study

- To avoid forgery and ensure the confidentiality of Information in the field of Information Technology

Methodology

- Collect genuine signatures from the registered users as a sample from the whole users with a specified period of time.

Preprocessing stage

According to T. Samuel Ibiyemi,S, S. eta.l, (2010). **Primarily,** Two major steps are conducted

i. Training signatures

ii. Recognition and verification of given signature

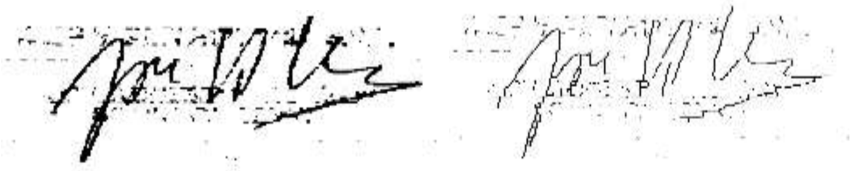
Signature images were scanned, to reduce the impact of pen thickness used when signing, and to simplify the structural shape of signatures, they are thinned to obtain the corresponding signature skeletons. The preprocessing stage includes 3 steps: (a) background elimination, (b) Width Normalization and (c) thinning

a) Background Elimination: Many image processing applications require differentiation of objects from the image background. Thresholding technique used for differentiating the signature pixels from the background pixels. After the thresholding, the pixels of the signature would be 1 and the other pixels which belong to the background would be 0(match and not match).

b) Width Normalization: Irregularities in the image scanning and capturing process may cause signature dimensions to vary. Furthermore, height and width of signatures vary from person to person and sometimes even the same person may use different size signatures. First there is the need to eliminate the size differences and obtain a standard signature size for all signatures. During the normalization process, the aspect ratio between the width and height of a signature is kept intact and after the process, all the signatures will have the same dimension.

c) Thinning: The goal of thinning is to eliminate the thickness differences of pen by making the image one pixel thick.

Sample signatures:



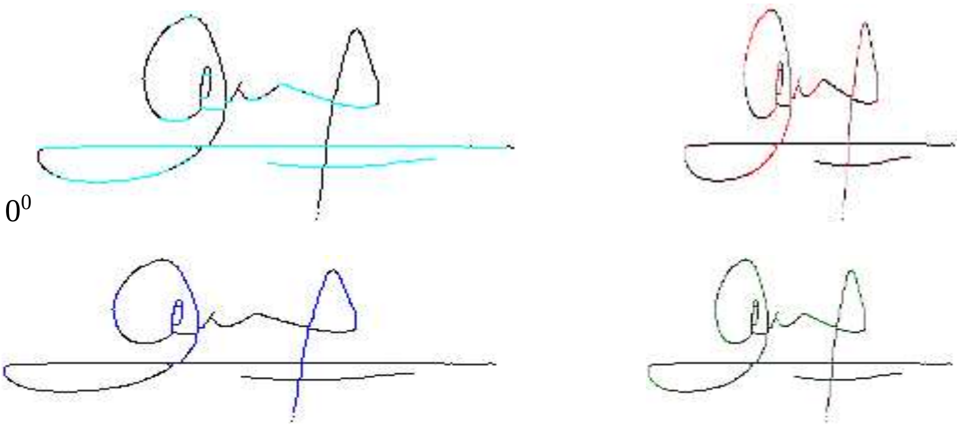
Original noisy signature corresponding skeleton

Feature extraction

Which requires determining the orientations of component signature pixels (angles of 0°, 45°, 90° or 135°, respectively), the signature stroke extraction through pixel tracking, and a final stroke normalization process; and, this task requires an initial pixel labeling process according to some predetermined orientations. Then, a pixel tracking algorithm using the estimated prearranged pixel orientations is applied. As a result of this feature extraction, the set of strokes for a given signature is obtained. Finally, a stroke normalization process is carried out prior to the recognition stage [5].

Algorithms used

Pixel labeling or Mask Features: provides information about directions of the lines of the signature because the angles of signature have inter-personal differences. The initial pixel labeling process considers four predetermined directions: 0°, 45°, 90° and 135°, respectively.



A. 0^0

b. 45^0

d. 135^0

C. 90^0

Pixel tracking: The aim of pixel tracking process is to extract the component strokes of a given signature. This algorithm has been adapted to the specific aspects of our signature problem. Consider four predominant angles, the pixel tracking algorithm is independently applied four times for each set ai of labeled pixels (where iε{0°,45°,90°,135°}) in the four different orientations

Grid Features: Provide over-all signature appearance information. An input into Signature Recognition greatly affects the accuracy level of training and the overall performance of the application. As a result, Signature Recognition accepts predominantly 2 types of input:

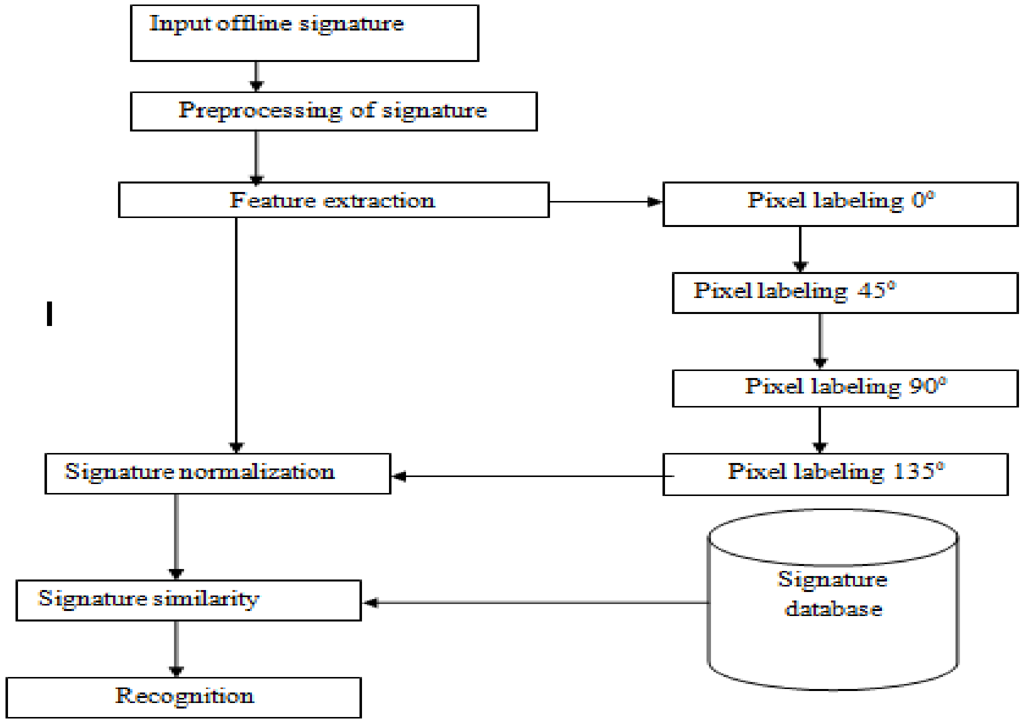
- User Bio-data: contain the name, id nos, of the users in the organization
- Signature images: may contain different training signatures.

Recognition

During the recognition phase, a given signature is compared with all stored signatures (database) to retrieve the most similar one to the test signature according to some similarity or distance measure.

In the signature recognition or identification problem, a given signature is searched in the database to establish the signer's identity. Signature verification problem is concerned to determine if a particular signature is authentic or a forgery.

Fig: 1. Architecture of the system



Tools used

- MATLAB for math work
- **Radon Transform:** The radon transform is projections of the application of active deformable models for an image matrix along specified directions. The Radon approximating the external shape of a signature has been Transformation.

- **Fractal Dimension:** Fractal dimension values indicate the complexity of a pattern, or the quantity of information embedded in a pattern. Applications of fractal dimension have been found in different signal processing fields.

- **Support Vector Machine:** The SVM is a classifier derived these problems using kernel. The main advantages of SVM when used image for classification problems are: (1) ability to work with high-dimensional data and (2) high generalization performance without the need to add a prior knowledge, even when the dimension of the input space is very high. The problem that SVMs try to solve is to find an optimal hyper plane that correctly classifies data points by separating the points of two classes as much as possible.

Challenges

- Challenge of creating a system with the ability to recognize hand written signature and verify its authenticity. This poses a problem because we are trying to get the computer to solve a problem with a method of solution that goes outside the convention of writing an algorithmic process.

- The failure to recognize/verify a signature was due to poor image quality and high similarity between 2 signatures.

- how to extract more effective features and with other signature recognition methods

Applications

- Application areas of Online Signature Verification include protection of small personal devices (e.g. PDA, laptop), authorization of computer users for accessing sensitive data or programs and authentication of individuals for access to physical devices or buildings.

- The main task of any signature verification system is to detect whether the signature is genuine or counterfeit. Forgery is a crime that aims at deceiving people.

- Signature Recognition examines behavioral aspects that manifest themselves when we sign our name.

- It is essential to recognize the signatures, with high accuracy and no time consuming processes.

- For different Internet applications (i.e. e-commerce). It could be possible to recognize a registered user for Internet purchases using his/her signature. A client-server solution is now needed. The signature scanning and some preprocessing to extract the component signature strokes can be performed at the client’s side, and the recognition task using the database of signatures is preformed at the server’s side.

- To avoid forgery and ensure the confidentiality of Information in the field of Information Technology Security an inseparable part of it. In order to deal with security, Authentication plays an important role.

CONCLUSIONS

The handwritten signature is one of the ways to authorize transactions and authenticate the human identity compared with other electronic identification methods such as fingerprints scanning and retinal vascular pattern screening. Signatures are composed of special characters and flourishes and therefore most of the time they can be unreadable. Also intrapersonal variations and interpersonal differences make it necessary to analyze them as complete images and not as letters and words put together. Excellent recognition results can be achieved by comparing the robust model of the query signature with all the user models using appropriate classifier.

Recommendations

- We recommend that most of the researches are conducted based on offline recognition techniques but can develop a system by using online recognition techniques
- Most of the researches are conducted on some organizations like bank, but can develop for other organizations which need signature recognition.
- The adaptation of our signature recognition method to possible Internet connection.

Acknowledgment

The Authors would like to thank Assosa University by providing full time internet service to do this research and development. And also would like to thank the reviewers for their constructive comments.

REFERENCES

[1]. Farhad Shamsfakhr (2011). System of “Analysis of Intersections Paths” for Signature Recognition: International Journal of Image Processing (IJIP), Volume (5): Issue (5): farhad_sm@ymail.com

[2]. Mehdi Radmehr, Seyed Mahmoud Anisheh, Mohsen Nikpour and Abbas Yaseri,(2011). Designing an Offline Method for Signature Recognition, World Applied Sciences Journal 13 (3): 438-443, 2011 ISSN 1818-4952 © IDOSI Publications,

[3]. T. Samuel Ibiyemi,S. Adebayo Daramola November (2010). Offline Signature Recognition using Hidden Markov Model (HMM), International Journal of Computer Applications (0975 – 8887) Volume 10– No.2.

[4]. A. Perez Hernandez, A. Sanchez and J.F. Vélez(1997)Simplified Stroke-based Approach for Off-line Signature Recognition Departamento de Informática, Estadística y Telemática Universidad Rey Juan Carlos Campus de Móstoles 28933 Móstoles (Madrid), SPAIN.

[5]. O.C Abikoye, M.A Mabayoje, R. Ajibade dec.(2011). Offline Signature Recognition & Verification using Neural Network, International Journal of Computer Applications (0975 – 8887) Volume 35– No.2.