AUTOMATIC OFFLINE SIGNATURE VERIFICATION SYSTEM

Morufu, O.
Cyber Security Science Department
Federal University of Technology, Minna.
Niger State, Nigeria
E-mail: lerejide@gmail.com

Abstract
Automated offline verification system that verifies genuine signature and detects signature forgeries of any types is presented. The system used various algorithms to pre-processed signature images before presented for feature extraction. Scale Invariant Feature Transform was used as a feature extraction technique. Samples of three genuine signatures of writer were taken and their Scale Invariant Feature Transforms were extracted using MATLAB function. Euclidean distance was used to calculate variability within the same writer. This variability is computed as intra-class Euclidean distances. The feature vector Euclidean distances, the image distances and intra-class thresholds are computed and stored as templates for a known writer. For any test signature scale Invariant Feature transforms is extracted and inter-class Euclidean distances is calculated, that is, the Euclidean distances between feature vectors of test signature and those of stored template. The intra-class threshold stored in the template is compared with the inter-class threshold for the test signature to be considered as authentic or forgery. The system was implemented on a database of 140 signatures consisting of training set and test set. The system is not only able to verify genuine signature but also detects all types of forgeries (Random, unskilled and skilled).

Keyword: Forgeries, verification system, offline, Scale Invariant Feature Transform.

Introduction
Signature can be defined as a behavioural biometric, which can be represented by a person's name, usually in his or her own handwriting. These handwritten signatures have three major important used which are socially and legally well accepted. These uses are document authentication, authorization and writer identification. For example, a bank cheque need to be signed by the account owner of the cheque before any withdraw is made from a bank cashier and the cashier needs to compare the signature on the cheque with the one on the computer database. In this case, the cashier is using the handwritten signatures as an authentication mechanism, to verify whether the signature on the cheque is for the account owner or not. This kind of verification is referred to as visual verification.

In modern society where fraud relating to signature forgeries is rampant, there is need for Automatic signature verification system. Since introduction of computer, many researchers have worked on automatic signature verification system. Two distinct categories of automatic signature verification systems have been investigated by researchers as a result of their diverse applications. These system are: offline system (static) and online system (dynamic). In offline system, hard copies of signatures are digitized using a hand-held or flat-bed scanner and only the complete writing is stored as an image. These images are referred to as static signature. Automatic verification of signature on a bank cheque is a good example of offline system. In the case of online system, special pen is used on an electronic surface such as digitizer combined with a liquid crystal display. Features like two-dimensional coordinates of successive points of

the writing, pen pressure, angle and direction of the pen, are captured dynamically and then stored as a function of time. The stored data is referred to as dynamic signature. Automatic signature verification for point of sale and security applications is a good example of an online system.

In general, offline signature verification is a challenging problem. Unlike the online system, where dynamic attributes of the signing action are captured directly as the handwritten trajectory, the dynamic information contained in offline signature is highly degraded. In offline system, features such as handwritten order, writing-speed variation and skillfulness need to be recovered from the grey-level pixels. The challenging aspects of automatic offline signature verification have been, for a long time, a true motivation for researchers. A great deal of work has been done in the area of automatic offline signature verification over the past two decades, yet, problem of affordability and reliability has not been overcome. In this research work, automatic offline signature verification system that is affordable (economically) and reliable (efficient) is developed.

The remaining part of this paper is organized as follows: Section 2 presents some related works done in the field of offline signature verification. Section 3 presents pre-processing and feature extraction. Experimental results of the system develop are presented in Section 4. Finally, Section 5 presents conclusion.

Related work:

Most of the work in automatic offline signature verification system has always been on different types of forgeries. Before looking into the landmark contribution of various researchers in the area of automatic offline signature verification, let us briefly explain types of forgeries. Madasu et al, (2005) classified forgeries as follows:

Random forgery:

The forger does not have the shape of the writer signature but comes up with scribble of his own. The forger may derive the forged signature from the name of the owner. This kind of forgery is very easy to detect with naked eyes. This forgery is also called simple forgery

Unskilled forgery:

The forger knows the shape of the writer's signature and tries to imitate it without much practice. The forger imitates the signature in his own style without any knowledge of spelling and does not have any prior experience. The imitation is preceded by observing the signature closely for a while. This forgery is also called casual forgery.

Skilled forgery:

This is where the forger has unrestricted access to genuine signature of the owner and comes up with a forged sample. This kind of forgery is the most difficult forgery to detect and is created by professional forger or person who has experience in copying the signature.

Survey of the state of the art off-line signature verification system designed up to 1993 appears in plamondon & Leclerc 1994 and Sabourin et al. 1992. Another survey article(plamondon & srihari 2000) has summarized the approaches used for offline signature verification from 1993-2000. Most of the work in off-line forgery detection however has been on random or casual forgeries and less on skilled forgeries.

Ammar et al. (1986) started the work on the detection of different kinds of forgeries. Apart from introducing a method for separation of signature from noisy backgrounds, this paper was one of the first of its kind, which tried to solve the problem of skilled forgeries based on the shape and density features of the signature. They calculated the statistics of dark pixels and used them to identify changes in the global flow of the writing. The later work of Ammar et al. 1990 is based on reference patterns, namely the horizontal and vertical positions of the signature image. The projection of the questioned signature and reference are compared using Euclidean distance. They also compared the performances of parametric and reference pattern based features in the verification of skillfully simulated handwritten signatures.

Many researchers used neural networks and their variants for static signature verification. For example, Sabourin and Drouhard (1992), employed neural networks to classify signature images with probability density function of the stroke directions serving as a global characteristics vector. Neural networks offers an advantage over other techniques as the system is trained to perform class separation through a continuous process of learning but this requires large number of signature samples for training, which may not be possible in a commercial environment(madasu et al, 2005). Guo et al. (2002) presented an algorithm for the detection of skilled forgeries based on a local correspondence between a questioned signature and a model obtained a priori. Writer-dependent properties are measured at the sub-stroke level and a cost function is trained for each writer.

Lee 1996 attempted to use various neural network algorithm to classify a signature as either genuine or imposter. He examined three neural network based approaches: Bayes Multilayer Perceptrons (BMP), Time Delay Neural Networks (TDNN), and Input Oriented Neural Networks (IONN). Preprocessing steps such as linear time normalization and signal resembling were performed. The input to the neural networks was a sequence of instantaneous absolute velocities extracted from the spatial coordinate time functions (X and Y signals). The only problem with the use of neural network for signature verification is that examples of forgeries are required to train the network for a user. The networks cannot be properly trained by being given only genuine samples.

The proposed system in Blumenstein et al, (2006) uses structure features from the signatures contour, modified direction feature and additional features like surface area, length skew and centroid feature in which a signature is divided into two halves and for each half a position of a centre of gravity is calculated in reference to the horizontal axis. For classification and verification two approaches are compared; the resilient Back propagation (RBP) neural network and Radial Basic Function (RBF) using a database of 2106 signatures containing 936 geniue and 1170 forgeries. These two classifications register 91.21% and 88% true verification respectively.

Hidden Markov Models were also explored in the field of signature verification. El-Yacoubi et al. 2000 presented a HMM based approach to dynamically and automatically derive the author dependent parameters in order to set up an optimal decision rule for off-line verification process. The cross validation principle is used to obtain not only the best HMM models, but also an optimal acceptance/rejection threshold for each author. This threshold led to a high discrimination between the authors and imposters in the context of random forgeries but was not successful for other kinds of forgeries. Yang et al. 1995 trained HMMs to model the sequence of normalized angles along the trajectory of a signature. The normalized angles were

computed by extracting the sequence of absolute angles along the points of the signature and subtracting the starting angle from each absolute angle. This calculation is used to make the features rotational invariant. Also, size normalization is performed by uniformly dividing the signature into K segments, where K is the observation length for input to the HMMs.

In Srihari et al, (2004), the uniqueness of writers' handwriting is mapped with that of the signature. Signature is signed in a predefined space of 2X2 inches and rotation is normalized with the horizontal axis, the gradient, structural and concavity are used as image descriptors. The gradient detects the local features of the image and concavity detects the relationship between the structural and local features. The verification model is based on the Bayesian classifier that uses mean and variance measures to classify. The system uses two databases of signatures with a total of 106 writers and 3960 samples.

Most of the automatic offline signature verification systems discussed above have some limitations due to the techniques used in pre-processing and feature extraction thereby making it difficult for them to detect skilled forgeries effectively. In this paper, automatic offline signature verification system that uses various algorithms in the pre-processing stage and Scale Invariant Feature Transforms for feature extraction is proposed.

Methodology

Data Acquisition

The signatures used for database were collected using both black and blue ink on a white A4 sheet of paper with 20 signatures per page. The signature database consists of a total of 140. Out of these, 60 were authentic signatures and others were forged ones. 10 male students and 10 female students were used to carry out this exercise. Each A4 sheet has 20 boxes of a fixed size 2inch by 1.5inch, so as to create a uniform database of signatures. In other to account for variation in the signature with time, the signatures were collected in multiple sessions which were spaced over a period of a few weeks. Each student provided 3 genuine signatures.

The random forgeries were obtained by supplying only the names of the individuals to the random forgers who did not have any access to the actual genuine signatures. The casual forgeries were obtained by providing sample of genuine signatures to the forgers. Each forger had to provide 1 imitation of any of the genuine signatures, apart from his or her own signature. A few expert forgers provide 1 forgery of each genuine signature in the database to create the skilled forged samples of all the persons. Each volunteer of these skillful forgeries were asked and tested before they were allowed to skillfully forge the genuine signatures on the database. All together 20 each of random ,unskilled and skilled forgeries were provided.

A flat- bed scanner was used to scan the signature images with 300dpi resolution in 256 grey-level. After the scanning the images were resized to their original sizes and saved in a separate file. At this point the scanned image is ready for pre-processing.

Pre-processing

In the development of an offline automatic signature verification system, a signature need to undergo pre-processing stage before being presented for feature extraction. The pre-processing operation will not only remove the noise introduced during the scanning process, but also simplifies feature extraction of the signature. In this proposed system, pre-processing of

signature passed through 5 stages as shown in fig. 1. Fig.2 shows the results of various stages of pre-processing of signature.

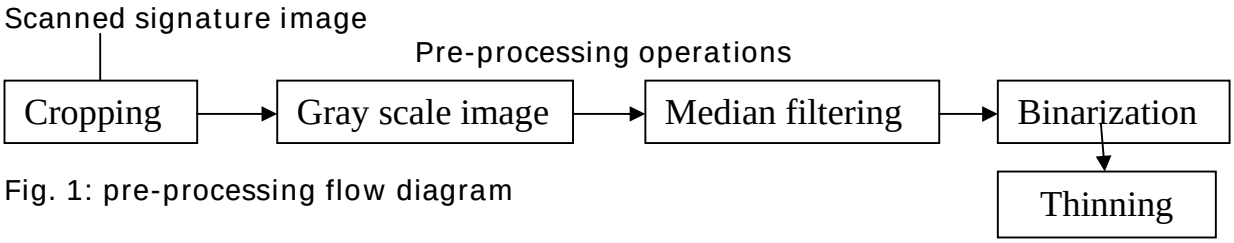


Fig. 1: pre-processing flow diagram

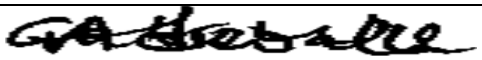
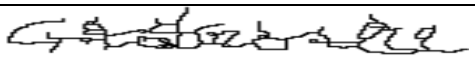
Process	Before	After
Load Image		
Cropping		
GrayScale		
Median filtering		
Binirization		
Thinning		

Fig. 2: Result of various stages of pre-processing operation

Feature extraction

The pre-processed signature image is presented for feature extraction. Feature extraction involved identifying stable shape descriptor from the pre-processed signature image. In this paper, Scale Invariant Features Transform (SIFT) is used to extract feature vectors. SIFT features have been used in pattern recognition and classification, mostly in object recognition. Kim et al, (2006) uses SIFT features for robust digital watermarking. (David, 2004) used Scale Invariant Feature Transform to extract distinctive invariant feature from image. The SIFT algorithm is robust for identifying stable key locations in the scale-space of a grey scale image (David, 1999) and (David,2004). (David,2004) used Scale-Space extrema detection, Accurate Keypoint localization, Orientation assignment and keypoint description to extract a set of descriptors from a given image. Sharath et al, (2008), investigated the use of SIFT features in fingerprint verification.

MATLAB was used to extract SIFT features of the pre- processed signature image. The MATLAB function that was used to extract SIFT features of the signature images was written by El-Maraghi. The implementation of this MATLAB function resulted in SIFT feature with 128 values, which is a vector. This vector is normalized to enhance invariance to illumination.

Classification

In order to measure the variability between the SIFT features of two given signature images, Euclidean distances need to be calculated. Let two signatures be represented by S_1 and S_2. Let s_i be the i^{th} vector in signature S_1 and s_j be the j^{th} vector in signature S_2 . The distance

$D(s_i,s_j)$ was calculated as the Euclidean distance between s_i and s_j. Let a and b be the number of vectors in signature S_1 and S_2 respectively. $D(s_i,S_2)$ was taken as the average Euclidean distance from the i^{th} vector in signature S_1 to all the vectors of signature S_2. The image distance between signature S_1 and signature S_2 is given by:

$$D(S_1,S_2) = \frac{1}{a}\sum_{i=1}^{a} D(s_i,S_2) \quad (1)$$

Template creation and Threshold calculation

Individual signer template has to be created. The template has the following information

- The Euclidean distances between vectors
- The distances between the signature images
- Intra-class thresholds: the maximum and minimum among the distances between the signature images
- The average of distances between the signature images

For each writer, samples of three signatures say S_1, S_2 and S_3 were taken to cater for intra-personal variations. The Euclidean distances between vectors is calculated as follows

$D(s_i,S_2), D(s_i,S_3)$ and $D(s_j,S_3)$

The distance between the three signature samples are calculated as follows:

$D(S_1,S_2), D(S_1,S_3), D(S_2,S_3)$,

The intra-class threshold is calculated as follows:

the maximum among $D(S_1,S_2), D(S_1,S_3)$ and $D(S_2,S_3)$ is denoted by

$\max(D(S_1,S_2), D(S_1,S_3), D(S_2,S_3))$ and

the minimum among $D(S_1,S_2), D(S_1,S_3)$ and $D(S_2,S_3)$ is denoted by

$\min(D(S_1,S_2), D(S_1,S_3), D(S_2,S_3))$

The average of $D(S_1,S_2), D(S_1,S_3)$ and $D(S_2,S_3)$ is denoted by

$\text{avg}(D(S_1,S_2), D(S_1,S_3), D(S_2,S_3))$

Verification

When a test signature say T claimed to be of a particular writer, the Euclidean distances were calculated between the test signature and each of the three sample signatures (as discussed above) resulting to distances between the images. The distances between test signature and each of the three signatures were calculated. That is, $D(T,S_1), D(T,S_2)$ and $D(T,S_3)$. The inter-class thresholds, $\max(D(T,S_1), D(T,S_2), D(T,S_3))$ and $\min(D(T,S_1), D(T,S_2), D(T,S_3))$ are calculated. $avg(D(T,S_1), D(T,S_2), D(T,S_3))$ is also computed.

For comparison and decision criteria, inter-class maximum and minimum distances were compared with threshold of intra-class maximum and minimum distances. Also, average of inter-class distances is compared with the threshold of average of intra-class distance.

Let $X = (D(T,S_1), D(T,S_2), D(T,S_3))$ and

$Y = (D(S_1,S_2), D(S_1,S_3), D(S_2,S_3))$

T is classify as genuine if the conditions

$\max(Y) \geq \max(X)$

$\min(Y) \geq \min(X)$ and

$avg(Y) \geq avg(X)$ hold

Otherwise T is classified as not genuine.

Experimentation and result discussion

The proposed system was experimented on a signature database that consists of 60 genuine signatures from 20 writers. Each writer contributed a sample of 3 signatures of their own. Only genuine signatures were trained for the system as forged samples of a genuine signature are readily available in the real-world scenario (that is the system learned only from the training signature for a specific individual). The test set made up of 20 genuine signature and 60 forged signatures (20 signatures for each type of forgeries) giving a total of 80 signatures for the test set. For both training set and test set a database of 140 signatures was used to experiment the system. Table 1 show the signature database for the system developed. The result of the experimentation is shown in table 2.

Table 1: Signature database for the system developed

Signature types	Trained signature	Tested signature	Total
Genuine	20*3	20	80
Skilled forgeries	__	20	20
Unskilled forgeries	__	20	20
Random forgeries	__	20	20

Table 2: Result of experimentation

Signature types	Total	Accepted	Rejected
Genuine	20	20	0
Skilled forgeries	20	1	19
Casual forgeries	20	0	20
Random forgeries	20	0	20

Conclusion

Automatic offline signature verification and forgery detection is presented. Starting from pre-processing of signature image, an automatic offline signature verification system that employed Scale Invariant Features transform as feature extraction technique is presented. The use of Scale Invariant feature Transform for feature extraction provides the system with fine information and more detailed features. The use of Euclidean distance in the computation of threshold enables the system to perform excellently. Apart from high level degree of accuracy, the system worked better than traditional (manual) way of verifying signature. Unlike other systems, the system developed does not require too many signature samples for training set. Only three samples of a writer is required for training set. This in turn bring about reduction in the amount of storage required to store features from a large number of trained signature samples. The system is not only able to verify genuine signatures but also detects all types of forgeries (Random, unskilled and skilled).

References

Ammar, M., Yoshida, Y. & Fukuruma, T. (1986). *A new efftive approach for off-line verification of signatures by using pressure features*. Proceedings of the International Conference on Pattern recognition.

Ammar, M., Yoshida, Y. and Fukuruma, T. (1990). Structural description & classification of images. *Pattern Recognition, 23(7), 697-710*.

David, L. (1999). Object recognition from local scale invariant features. *International Conference on Computer Vision, pp. 1150-1157.*

David, L. (2004). Distinctive image feature from scale-invariant keypoints. *International Journal of Computer Vision., 60(2). 91-110.*

El-Maraghi, T. F. (nd). Matlab sifttutorial ftp://ftp.cs.utoronto.ca/pub/jepson/teaching/vision/2503/SIFTtutorial.zip.

El-Yacoubi, A., Justino, E. J. R, Sabourine, R., & Bortolozzi, F. (2000). *Offline signature verification using HMMs and cross-validation.* IEEE International Workshop on Neural Networks for Signal processing, pp. 859-868.

Guo, J. K., Doermano, D., & Rosenfeld, A. (2001). Forgery detection by local correspondence. *International Journal of pattern Recognition and Artificial Intelligence, 15(4).579-641.*

Kim, H., Lee, H. & Lee, H. K. (2006). *Robust image watermarking using local invariant features.* Proceeding of SPIE, 45(3).

Leclerc, F. & Plamondon, R. (1994). Automatic signature Verification: The state of the art, 1989-1993. *International Journal of pattern Recognition and Artificial intelligence: Special Issue on Signature Verification, 8(3), 643-600.*

Lee, L. L. (1996). *Neutral approaches for human signature verification*. Proceedings of third International Conference on Signal Processing, pp. 1346-1349.

Lee, L., Berger, T. & Aviczer, E. (1996). Reliable online human signature verification system. *IEEE Transactions in Pattern Recoginition and Machine Intelligence, 18(6).643-647.*

Plamonon, R. & Lorette, G. (1989). Automatic signature verification and writer identification. *The state of the art Pattern Recognition, 22(2).107-131.*

Plamondon, R. & Shihari, S. N. (2000). On-line and off-line handwriting recognition: A comprehensive Survey. *IEEE Transactions on Oattern Analysis and Machine Intelligence, 22(1).63-84.*

Sabourin, R. & Drouhard, J. P. (1992). *Offline Identification with hand-written signature images: Survey and perspectives*. Structural Document Image Analysis. New York: Springer-Verlag, pp. 219-234.

Sharath, P., Unsang, P. & Jain, A. K. (2008). *Robust image watermarking using local invariant features.* Proceedings of SPIE Defence and Security symposium Orlando, florida.

Srihari, S., Kalera, K. M. & Xu, A. (2004). Offline signature verification and identivation using distance statistics. *International Journal of Pattern Recognotion and Artificial Intelligence, 18(7).1339-1360.*

Yang, L., Widjaja, B. K., & Prasad, R. (1995). *Application of hidden markov models for signature verification.* Pattern Recognition, 28, 161-170.