World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:2, No:7, 2008

Automatic Authentication of Handwritten Documents via Low Density Pixel Measurements

Abhijit Mitra, Pranab Kumar Banerjee and Cemal Ardil

Abstract— We introduce an effective approach for automatic offline authentication of handwritten samples where the forgeries are skillfully done, i.e., the true and forgery sample appearances are almost alike. Subtle details of temporal information used in online verification are not available offline and are also hard to recover robustly. Thus the spatial dynamic information like the pen-tip pressure characteristics are considered, emphasizing on the extraction of low density pixels. The points result from the ballistic rhythm of a genuine signature which a forgery, however skillful that may be, always lacks. Ten effective features, including these low density points and density ratio, are proposed to make the distinction between a true and a forgery sample. An adaptive decision criteria is also derived for better verification judgements.

Keywords— Handwritten document verification, Skilled forgeries, Low density pixels, Adaptive decision boundary.

I. Introduction

HANDWRITTEN document authentication, in general, attempts to confirm that a given written sample of a person is genuine, or equivalently, to identify a questioned sample as a forgery. Offline handwriting authentication [1]- [7] is considered more difficult than online verification [8] due to the lack of dynamic information like the order of strokes, speed of signing, acceleration etc. This makes it difficult to define effective global and local features for verification purposes and thus the field is not as developed as the online detection. Nevertheless, the available common factors in the offline authentication such as slant writing, relative height of small and tall letters etc., have been used successfully in most of the reported works in free-hand forgery detection [7]. However, the skilled forgeries, often subclassified into traced and simulated forgeries, involve attempting to mimic the style of the writer and thus can be difficult to detect with only these static features. The main problem comes in designing a feature extraction method which gives stable features for the genuine written samples despite their inevitable variations, and salient features for the forgeries even if the imitations are skillfully done. Even though a genuine writer can never produce exactly the same handwriting twice, e.g., signatures, and many factors can affect signatures and other handwriting including injuries, illness, temperature, age and emotional state as well as external factors such as alcohols and drugs [3] – an original piece of writing has many natural personal characteristics like cursiveness, ballistic rhythm etc. But a forge sample, however skillful it may be, always lacks this rhythm and has poor line quality. Hence the features to provide efficient basis for verification for the case of offline authentication are the non-natural characteristics like hesitation, patching, retouching etc., which are generally concerned with the gray levels of the signature (and lost if we deal with the signature as a binary image). In the 1980s, Ammar *et. al.* [6], aiming at skilled forgery detection, used such feature sets. They considered the geometric information about the letters far less informative and the main emphasis was given on high-pressure regions which were actually the dark pixels in the signature image corresponding to high-pressure points on the writing trace. There, the focus was on the ratio of the number of dark pixels to the total number of pixels in the signature image, and it was one of the first attempts to consider dynamic information in the static image for verification. Subsequently, many other ideas were developed for skilled forgery verification like the orientations of the gradient vectors at each pixel of the signature [9], a fuzzy technique to add some pseudo-dynamic information such as pen-up and pen-down events [10], curve comparison algorithms [11], topological features like branch point, crossing point [12] etc. However, to the best of our knowledge, none of these works have given the emphasis on low pen-tip pressure points, or, in other words, low density pixel measurement, which can well be another basis for distinction between genuine and skillful forgery samples.

In this paper, we propose an effective approach of automatic handwriting authentication via low density pixel measurements with an adaptive threshold as decision boundary. For simplicity, we deal only with handwritten signatures in the proposed scheme, which can well be extended to any piece of handwritten samples without the loss of generality. Towards this, the low and high density pixel percentages are computed and ten effective features are proposed along with the ratio of above mentioned density percentages. An adaptive decision criteria is introduced then, leading towards betterment of system reliability. The simulation studies also exhibit better results than most of the existing schemes.

The paper is organized as follows. Section II and III briefly discuss about the types of forgeries and signature bank respectively. The measurement of pixel densities are dealt with in details in Section IV. The authentication process is given in

Manuscript received July 12, 2005.

A. Mitra is with the Department of Electronics and Communication Engineering, Indian Institute of Technology (IIT) Guwahati, North Guwahati - 781039, India. E-mail: a.mitra@iitg.ernet.in.

P. K. Banerjee is with the Department of Electronics and Tele-Communication Engineering, Jadavpur University, Kolkata - 700032, India. E-mail: pkbanj@rediffmail.com.

C. Ardil is with the Azerbaijan National Academy of Aviation, Baku, Azerbaijan. E-mail: cemalardil@gmail.com.

Section V, where, in particular, ten different features are given with the deviation measurement from these, followed by the proposed adaptive decision boundary. Section VI discusses about the experimental results and the paper is concluded in Section VII.

II. Classification of Forge Documents

Forge documents are generally classified into two types, namely, free-hand and skilled. These are discussed below.

Free-hand forgeries [7] are again subclassified into random and simple forgeries. When a forger simply uses an invalid signature without any prior knowledge of the authenticated person's name or style of writing, it is classified as random forgery. These are the simplest to detect because their characteristics differ globally from the genuine signature. Simple forgeries involve using the writer's name without any a-priori information of the genuine signature style. A majority of forgeries are free-hand forgeries, but are often overlooked when there are massive numbers of documents to be processed.

Skilled forgeries [5] on the other hand, with the further subclassification as traced and simulated forgeries, are almost alike the true samples. Simulated forgeries are those in which the forger imitates the original signature style from his/her memory, while a traced forgery is a fraudulent signature which has been executed by actually following the outline of a genuine signature with a writing instrument. Our work is aimed towards detecting these traced and simulated signatures.

III. Signature Data Bank

The signature data bank consists of 200 genuine and 200 forgery samples. True samples were written by 20 different persons as their own signatures with 10 samples each. Forgeries were written by 4 different forgers simulating and tracing original samples of those 20 persons. All samples were written using the same ball pen in a horizontally oriented limited space in order to elude the disparity of gray levels among several genuine signatures of the same person. The signature image is dealt with as a noise-free gray image where a dark pixel means high-pressure pixel. All the samples are scanned within a limited space of 256×512 pixels and are digitized to matrix $\mathbf{A} = [a]_{ij}$, with each a_{ij} having one of the values from 2^8 gray levels. In the sequel, we would denote the maximum and minimum density pixels of any signature by a_{max} and a_{min} respectively.

IV. Measurement of Pixel Density Features

In this section, we develop the extraction method of low and high density pen-tip points and respective density ratios. In order to distinguish among different density regions, two suitable threshold points are defined, one for high density pixels and the other for low density points, which are discussed below.

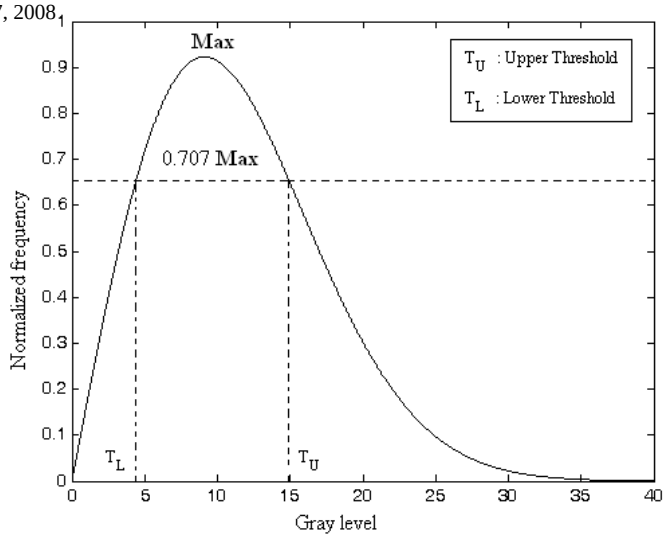

Fig. 1 An example of selecting T_L and T_U.

A. Threshold Selection

From the original gray level density information of the signature (i.e., the normalized histogram), we select a lower threshold point (T_L) and an upper threshold point (T_U) adaptively at the gray levels which correspond to the lower and upper $\frac{1}{\sqrt{2}}$ points respectively of the peak frequency of the same normalized histogram of the signature in question. An example of this selection procedure is given in Fig. 1, where Max represents the maximum number of pixels at a particular gray level in any given signature.

B. Low Density Pixel Percentage (LDPP)

Low density pixels (LDP) are those signature pixels which have gray level values lower than T_L. LDPs can be extracted by the relation

$$a_{ij}^{LDP} = \begin{cases} 1 & \forall\ a_{ij} \leq T_L \\ 0 & \text{otherwise} \end{cases} \tag{1}$$

where a_{ij}^{LDP} represent the LD pixels. We can now define a low density pixel percentage (LDPP) in a signature as the ratio of LDPs to the binarized signature area as

$$LDPP = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} a_{ij}^{LDP}}{\sum_{i=1}^{M}\sum_{j=1}^{N} a_{ij}^{bin}} \times \ 100 \tag{2}$$

with a_{ij}^{bin} being the binarized image [13] pixels.

C. High Density Pixel Percentage (HDPP)

High density pixels (HDP) are signature points which have gray level values higher than T_U. HDPs can be extracted [6] by the following relation:

$$a_{ij}^{HDP} = \begin{cases} 1 & \forall\ a_{ij} \geq T_U \\ 0 & \text{otherwise} \end{cases} \tag{3}$$

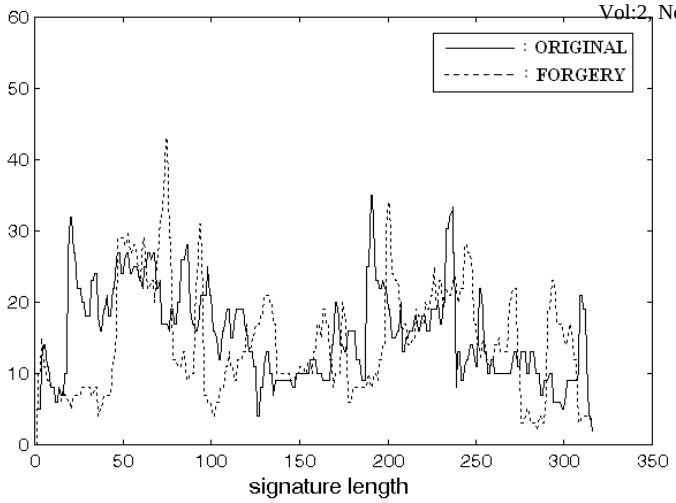

Fig. 2 Comparison of binarized images of a true and a forgery signature.

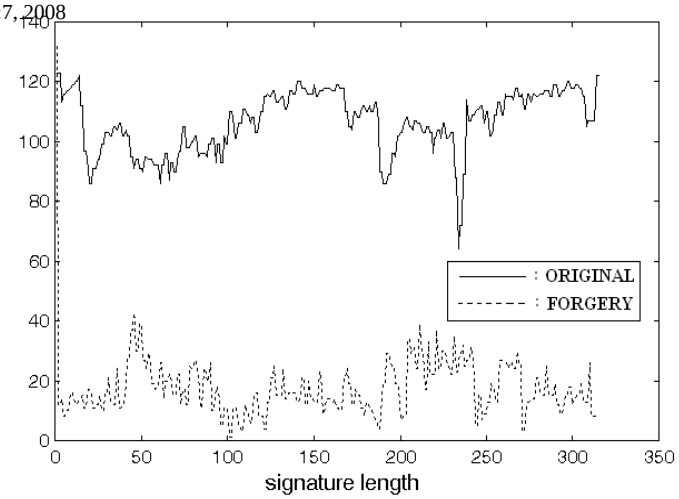

Fig. 3 Comparison of low density pixels of the same true and forgery samples.

where a_{ij}^{HDP} represent the HD pixels. Here we define a high density pixel percentage (HDPP) as the ratio of HDPs to the binarized signature area and express it as

$$HDPP = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} a_{ij}^{HDP}}{\sum_{i=1}^{M}\sum_{j=1}^{N} a_{ij}^{bin}} \times \quad 100 \tag{4}$$

where, in both the cases, $M \times N$ denotes the total signature area. Applying the aforesaid adaptive threshold selection procedure to the density ratios, we obtained $22 \leq HDPP \leq 41$ but in the case of LDPP, the range was specified by $10 \leq LDPP \leq 42$, where, most of the forgery samples have shown very poor values of LDPP. It was also observed in several signatures that almost same values of HDPPs were obtained from both the cases although the positions of HDPs for an original and a forgery sample have differed significantly. However, a forger could never match the value of LDPP obtained from a true sample. The observation is made clear in Fig. 2 and Fig. 3, where, Fig. 2 shows the almost similar binarized images of a true and a forgery sample, while Fig. 3 exhibits a significant mismatch between the low density points of the same samples.

V. Verification Procedure

Finding out a suitable feature set to establish a reasonable distinction basis between original and forgery samples is a difficult task. We, however, attempt the same with the following set, chosen by several observations with different kind of signatures.

A. Feature Set

Ten features (ϕ_1 to ϕ_{10}) have been used for verification purpose. The selection of these features is based on the experimental observation and are given below.

ϕ_1, ϕ_2, ϕ_3: Vertical position of the peak frequency in the vertical projection of the binarized image, HDP and LDP, respectively.
ϕ_4, ϕ_5, ϕ_6: Horizontal position of the peak frequency in the horizontal projection of the binarized image, HDP and LDP, respectively.
ϕ_7: High to low density ratio, i.e., HDPP/LDPP.
ϕ_8: Lower threshold point computed from the pressure histogram (T_L).
ϕ_9: Dynamic range of the siganture pixel values, i.e., $a_{max} - a_{min}$.
ϕ_{10}: Aspect ratio of the signature, i.e., length/width ratio of just the signature area.

B. Deviation Measurement

The total deviation of an unknown sample is measured by

$$D_{RMS} = \sqrt{\frac{1}{N}\sum_{i=1}^{N}\frac{(\phi_i - \mu_i)^2}{\mu_{NF_i}}} \tag{5}$$

where N is the number of used features (e.g., here $N = 10$), μ_{NF_i} is a normalization factor of any ith feature, computed by

$$\mu_{NF_i} = \sqrt{\frac{1}{T}\sum_{j=1}^{T}(\phi_i(j) - \mu_i)^2} \tag{6}$$

with T being the total number of known original samples for a particular person and μ_i is the mean of ϕ_i for known true samples, i.e.,

$$\mu_i = \frac{1}{T}\sum_{j=1}^{T}\phi_i(j). \tag{7}$$

The deviation parameter D_{RMS} is the key factor behind the verification criteria. If we now define $D_{T_{max}}$ as the maximum deviation in the true samples of a given signature, $D_{F_{min}}$ as

TABLE I
OPERATIONAL FLOW OF PROPOSED ADAPTIVE DECISION CRITERIA.

1. **Initialization:**
   $p(0) = 0$, $\lambda = 0.01$ (in this case), $c = 0$.
   Compute $SR(0)$.

2. **Loop operation:**
   For $n = 1$ to σ^2/λ, do:
(a) $c \leftarrow c + \lambda$.
(b) Compute V_{th}.
(c) Compute $SR(n)$.
(d) $p(n+1) = p(n) + \lambda sgn\{SR(n) - SR(n-1)\}$.
(e) Store $p(n)$.
   Loop complete.

3. **Postprocessing:**
   $c_{opt} = max\{p(n) \mid \forall n\}$.
   $c \leftarrow c_{opt}$.
   Find V_{th} and SR with this value.

the minimum deviation in the forgery samples of that person and D_{sep} as the minimum distance [6] separating original and forgery samples of the same person, then we can write

$$D_{sep} = D_{F_{min}} - D_{T_{max}}. \quad (8)$$

In this case, the efficiency of the chosen feature set stems from the fact that it has ensured $D_{F_{min}} > D_{T_{max}}$, i.e., $D_{sep} > 0$, for most of the cases.

C. Authentication Criteria

Having all the above parameters computed, we introduce a threshold value (V_{th}) closely related with the aforesaid deviations for the practical purpose of verification and the decision is taken as follows.

- If $D_{RMS} < V_{th}$, the input sample is considered to be a true sample.
- If $D_{RMS} \geq V_{th}$, the input sample is judged to be a forgery sample.

The threshold parameter V_{th}, therefore, must be a preestablished one. After investigating a few aspects, an adaptive decision criteria has been followed to select V_{th}.

C.1 Adaptive decision criteria for selecting V_{th}:

In [6], a simple threshold has been proposed by assigning V_{th} to the value $D_{T_{max}}$, i.e., $V_{thresh} = D_{T_{max}}$. This couldn't converge to good results for such a simplified model. Another modified threshold has also been taken into account to give an extra safety factor by setting $V_{thresh} = D_{T_{max}} + \frac{D_{sep}}{\sqrt{2}}$. This model, however, couldn't ensure a reasonable system reliability as D_{sep} doesn't come out to be positive all the time. We thus use a *flexible threshold* model by employing an observational formula to calculate V_{th}, and is given as

$$V_{th} = D_{T_{max}}(1 + \frac{c}{\sigma^2}) - \mu_D \quad (9)$$

where μ_D is the mean of the deviation D_{RMS} computed on the set of known genuine signatures of the person in question, σ^2 is the variance of the same set and the variable coefficient c, which can vary within $(0, \sigma^2]$, is set on a particular value (c_{opt}) that corresponds to the best system reliability (SR). The optimum value c_{opt} is found out with the following adaptive formaula.

A parameter p, updated with every nth iteration, is initially set to $p(0) = 0$ and then adapted as

$$p(n+1) = p(n) + \lambda sgn\{SR(n) - SR(n-1)\} \quad (10)$$

where $SR(n)$ and $SR(n-1)$ denote the system reliability value at any nth and $(n-1)$th iteration respectively, $sgn(.)$ indicates the conventional sign function and λ is the step size according to which $p(n)$ is either incremented or decremented. This λ can be set with respect to the rate of change of c. With this equation, c_{opt} is assigned the following value

$$c_{opt} = max\{p(n) \mid \forall n\} \quad (11)$$

and is passed on to eq. (9) to set c for having the final V_{th} value. The entire decision criteria is summarized in Table I.

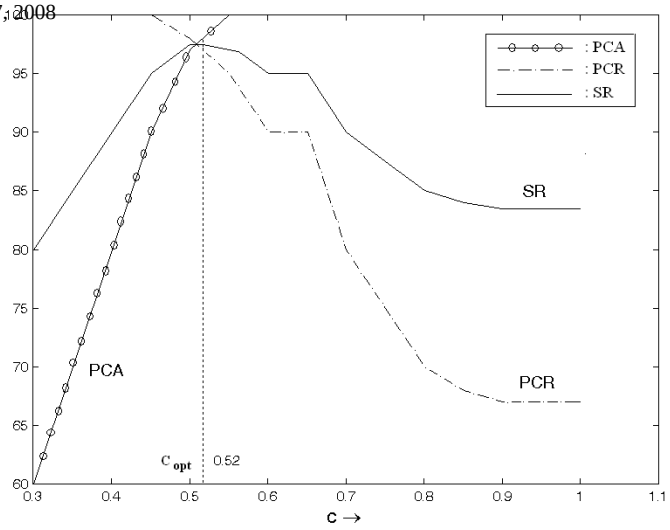

Fig. 4 Relation among PCA, PCR and SR with different values of c for a particular set of genuine and forgery signatures.

VI. EXPERIMENTAL RESULTS

The verification results on the real-life set are collectively judged by percentage of correct acceptance (PCA), percentage

of correct rejection (PCR) and system reliability (SR). PCA is defined as the ratio of the number of the accepted original samples and the number of known original samples. PCR is the ratio of number of rejected forgery samples and number of known forgery samples, while SR is defined as the average of these two (all of these three ratios should be multiplied by 100 to get percentage values). The proposed flexible threshold along with simple and modified ones have been applied to the entire signature data bank and the results have been calculated on an average basis. For the simple threshold, we obtained PCA=92, PCR=95, SR=93.5. For modified threshold, the values were PCA=94.5, PCR=95, SR=94.75, and for the proposed flexible threshold case with adaptive decision, PCA=97.5, PCR=96, SR=96.75. Fig. 4 shows that selecting V_{th} in the case of flexible threshold is not very critical as $SR > 95$ can be easily obtained for a considerable range of c.

VII. Conclusions

In this paper, a method for offline handwritten document authentication has been proposed, where the true and forgery samples were almost alike. Along with the high density pen-tip points, we have introduced the notion of low density points which have shown effectivity for such a problem by indicating the most important distinction with respect to the simulated or traced signatures, i.e., for non-natural signature characteristics. The features have been chosen very carefully so that the local characteristics of a forgery sample, like lack of ballistic rhythm and poor line quality, can easily be detected in our scheme. Experimental results have also supported the effectiveness of pressure regions, specially for low density pixels. The LDPs are expected to find their adequate utility in forensic applications in the future study.

References

[1] B. Fang *et al.*, "Offline Signature Verifiaction by the Analysis of Cursive Strokes," *Int. J. Pattern Recognition, Artificial Intelligence*, vol. 15, no. 4, pp. 659-673, 2001.

[2] A. Mitra, "An Offline Verifiaction Scheme of Skilled Handwritten Forgery Documents using Pressure Characteristics," *IETE Journal of Research*, vol. 50, no. 2, pp. 141-145, April 2004.

[3] J. K. Guo, D. Doermann and A. Rosenfeld, "Local Correspondence for Detecting Random Forgeries," in *Proc. 4th IAPR Conf. Document Analysis, Recognition*, Ulm, Germany, 1997, pp. 319-323.

[4] F. Leclerc and R. Plamondon, "Automatic Signature Verification: the state of the art – 1989-1993," *Int. J. Pattern Recognition, Artificial Intelligence*, vol. 8, pp. 3-20, 1994.

[5] M. Ammar, "Progress in Verification of Skillfully Simulated Handwritten Signatures," *Int. J. Pattern Recognition, Artificial Intelligence*, vol. 5, pp.337-351, 1991.

[6] M. Ammar, Y. Yoshida and T. Fukumura, "A New Effective Approach for Automatic Off-line Verification of Signatures by using Pressure Features," in *Proc. 8th Int. Conf. Pattern Recognition*, Paris, 1986, pp. 566-569.

[7] R. N. Nagel and A. Rosenfeld, "Computer detection of freehand forgeries," *IEEE Trans. Computers*, vol. 26, pp. 895-905, 1977.

[8] R. Baron and R. Plamondon, "Acceleration Measurement with an Instrumented Pen for Signature Verification and Handwriting Analysis," *IEEE Trans. Instrument., Measurement*, vol. 38, pp. 1132-1138, 1989.

[9] R. Sabourin and R. Plamondon, "Preprocessing of handwritten signatures from image gradient analysis," in *Proc. 8th Int. Conf. Pattern Recognition*, Paris, 1986, pp. 576-579.

[10] C. Simon, E. Levrat, R. Sabourin and J. Bremont, "A Fuzzy Perceptron for Offline Handwritten Signature Verification," in *Proc. Brazilian Symp. Document Image Analysis*, 1997, pp. 261-272.

[11] F. Nouboud and R. Plamondon, "Global parameters and curves for offline signature verification," in *Proc. Int. Workshop on Frontiers in Handwriting Recognition*, 1994, pp. 145-155.

[12] K. Han and K. Sethi, "Signature Identification via Local Association of Features," in *Proc. Int. Conf. Document Analysis and Recognition*, 1995, pp. 187-190.

[13] J. R. Ullman, *Pattern Recognition Techniques*. New York: Crane-Russak, 1973.