

## A High Efficiency Method for Automatic Signature Verification(ASV) in I-C-I Environment

Maan Ammar and Musbah M. Aqel

Faculty of Computer Science and Information Technology, Applied Science University  
Amman, Jordan-11931

---

**Abstract:** The billions of dollars of Commercial banks losses to check frauds make automatic verification of signatures of checks a major requirement in the new Interbank Check Imaging(ICI) environment. In this paper, we shed some light on the problem of check fraud, and introduce the application of an ASV method to the security of the financial transactions in electronic banks. The problem of transferring ASV research into an applicable system that can be integrated into electronic banks environment, with its implications, is dealt with in this paper, and a practical system that can be used with actual bank data is introduced. The system emanated from the material of this paper has already been in use in pilot projects in the USA and Singapore.

**Key Words:** Signature Verification, Check Fraud, Signatory, Ebanks, Interbank Check Imaging

---

### Introduction

US businesses and households write over 60 billion checks per year, and US financial institutions lose over 12 billion dollars to check frauds. In bank transactions, commercial banks lose 1% of their profits to check fraud. This problem becomes more serious in the new environment where major banks are beginning to exchange digitized computer images of paper checks using a new "open" system of computer platforms and technologies. This technological advancement, known as Interbank Check Imaging (ICI). However, the ICI environment is of a great help to Automatic Signature Verification (ASV) because it provides check images as a verification source.

Most checks written today are paid out by banks without having the signatures verified. This is because banks have too many checks to process each day, and they are forced to verify only a limited number of checks. Although banks may bear the ultimate financial responsibility, once criminals forge a check, inconveniences arising from this can be quite substantial to the banks and their customers.

The October 1996 report of the Board of Governors of the Federal Reserve System to the Congress on Funds Availability Schedules and Check Fraud at Depository Institutions stated the importance of the signature verification capability. "Of the six types of fraud, the largest proportion of losses were attributed to forgeries, either of the drawer's signature or of an endorsement. While prompt posting and return can identify certain problem checks, forged checks may not be detected until the check appears on the check writer's account statement." The American Bankers Association, in its 1998 Check Fraud Survey, said that forgery ranked number one. In fact, \$4 out of every \$10 lost was attributed to forgeries (Fig. 1).

Commercial banks lose 1% of their profits to check fraud. And yet, these banks must rely on either the

traditional visual verification method or the transaction analysis programs that leave out most of the checks from the verification process.

The Office of the Comptroller of the Currency ("OCC") writes, "Check fraud is one of the largest challenges facing financial institutions. Technology has made it increasingly easy for criminals, either independently or in organized gangs, to create increasingly realistic counterfeit checks and false identification that can be used to defraud banks."

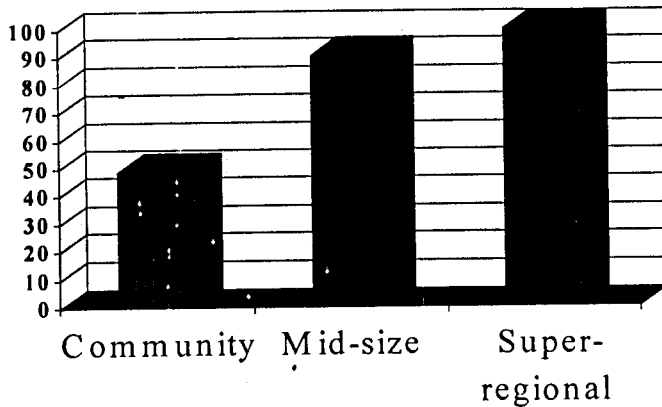
As well as bank checks signatures verification, the ASV method introduced in this paper is applicable in the fields of e-commerce, credit cards, government sector, insurance, brokerage, and national signature database.

**The Need for Automation:** The volume of checks for a bank like Citi-Corp may reach *one million* a day. A bank would have between 4 to 8 hours to have the signatures verified, 4 hours if the checks (check images) were available in the morning or 8 hours if the checks were available in the evening. With this huge amount of checks, the short period of time and the few number of people available (10 people or less) for visual verification of check signatures, ASV becomes highly required.

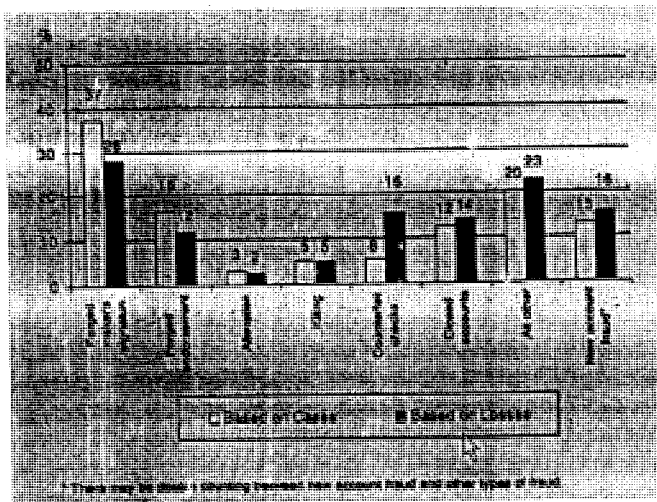
The situation explained above, assumes that the check images will be available only after the Check Imaging Operation. In an actual operation, however, check images may be sent to the ASV system server in batches, as they become available.

**The Scope of the Paper:** The importance of ASV and the size of the problem in both social and technical aspects, motivated many researchers and labs allow the world to conduct researches on this issue since about three decades (Nagel, 1973). Since 1980s, specialized International workshops have been held periodically for research on computer processing of handwriting including signatures (Ammar *et al.*, 1987). Researches in this field covered both on-line signatures

## Banks reporting Fraud Losses By Percentage



## 1997 Check Fraud Losses by Type (Percentage of Total)



- Forgery ranks 1.
- \$4 out of every \$10

ABA Check  
Fraud Survey  
1998

Fig. 1: Banks losses to Check Fraud

# Ammar et al.: A High Efficiency Method for Automatic Signature

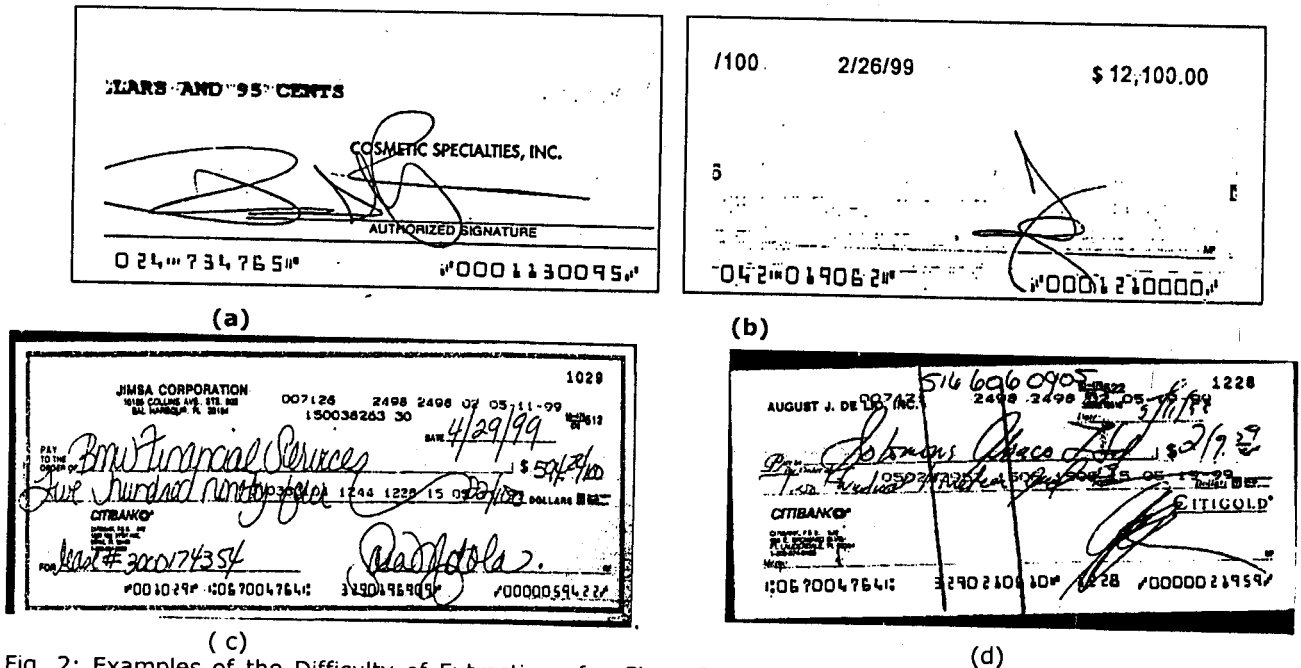


Fig. 2: Examples of the Difficulty of Extraction of a Clean Signature Image from Actual Bank Check Due to The Huge Variety in Space Occupied and the Overlapping Background. Such Cases are Not Faced in Lab Data

(Farag and Chien, 1972; Herbst and Liu, 1977; Crane and Ostrem, 1983; Brault and Plamondon, 1984) which many information like pressure, speed and time sequence are available, and offline ones in which the signature is dealt with just as an static image (Nagel and Rosenfeld, 1977; Sabourin et al., 1994; Ammar et al., 1988; Ammar, 1989; 1991 and Ammar et al., 1990), with a remarkable trend in which Ammar (Ammar et al., 1988) extracted some pseudo-dynamic features related to speed of writing and pressure on the pen, called High Pressure Regions, and used them in signature verification. Most published works (if not all) dealt with lab data in which the background cleaning from symbols, lines and background print is not needed, or not really a problem, however, in this paper we deal with actual bank checks (Fig. 2) in which extracting clean signature image, could be more difficult than the verification process itself because of the huge variety in the space occupied by the signature, and the background parts overlapping the signature.

Needless to say that if a clean signature can not be extracted, no verification can be done, regardless of the goodness of the verification procedure. The other issue which was not dealt with in the previous research works is the multi-signature checks and multi-signatories accounts, since all concentration was on the accuracy of the verification procedure and feature effectiveness.

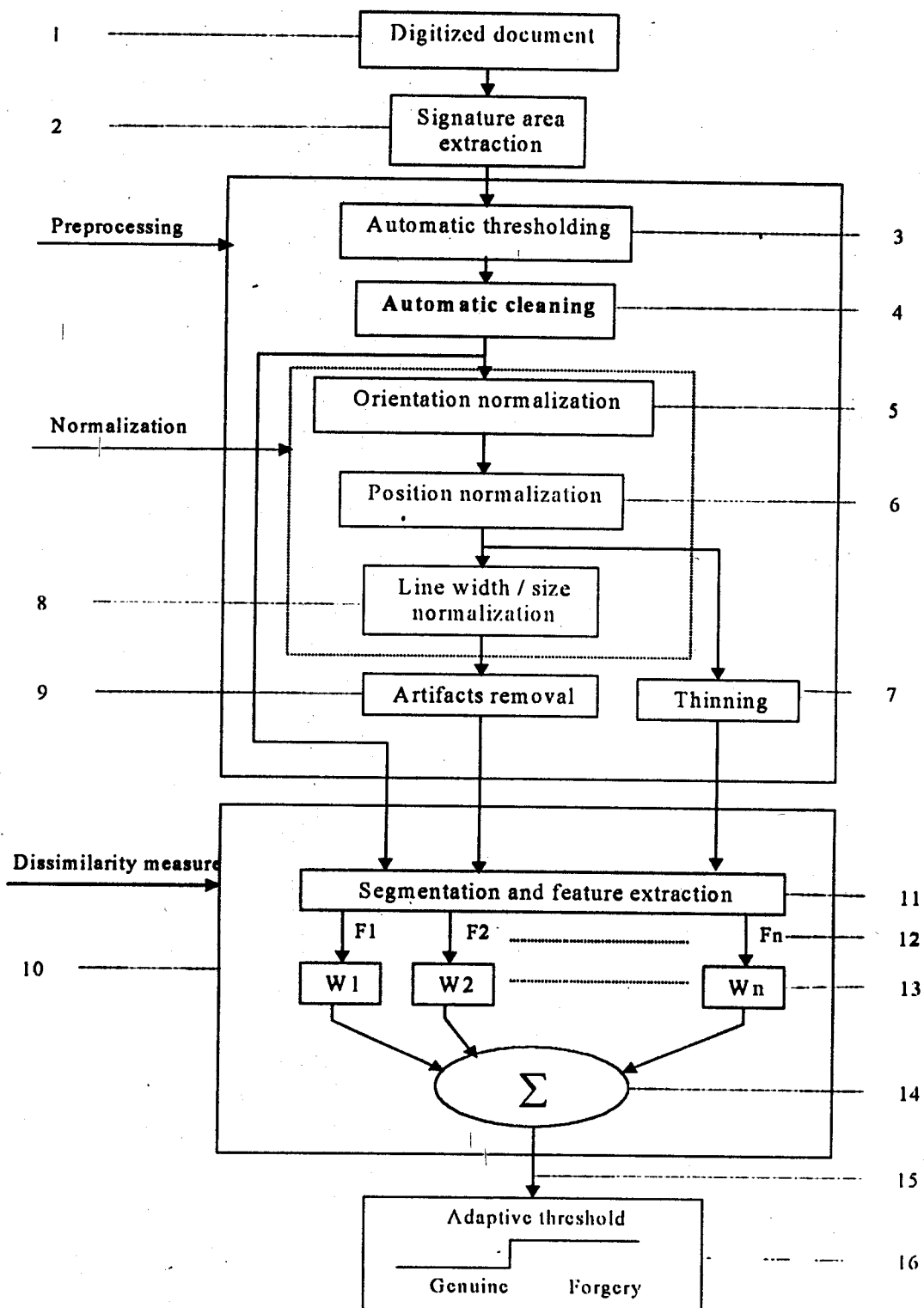
Although some researchers developed their research until reaching a simulated interactive systems that give their response of signature verification and analysis in natural language (Ammar, 1989), no paper seems to

be published on a verification system with the ability to deal with bank environment with all its implications.

In this paper, we do not introduce new image processing or classification techniques for signature verification, but we use different known techniques of image processing and classification in order to be able to extract clean signature images from actual bank checks, combine different feature extraction techniques in a suitable manner so that we could work with a resolution that may go down to 100 dpi with high efficiency ASV, while working with resolutions less than 150 dpi was considered to be not viable, recognize the writer of a check signature among multi-signatories, and finally, integrate all these components into a complete actual system supporting banks in the new ICI environment, providing higher security by being able to verify every signature with a reasonable cost and time.

**The ASV Method:** The ASV method proposed in this paper is illustrated in the block diagram shown in fig. 3. It consists of the following steps:

- An imaged check generated by check imaging systems, is used as an input image.
- From the digitized check image(1), a signature area(2) is extracted according to the coordinates of the signature area specified in the particular document type. This may differ from one check style to another. In this step, the signature area including the signature and the background is cut out into a new signature image like the one in fig. 2(a) to be processed for verification.
- If the original digitized check image is in gray level form, the image is thresholded to obtain a binary image(3).



**Fig. 3: The Block Diagram of the ASV Method**

Binary image is then automatically cleaned(4) using connected component labeling based cleaning. Here, the elimination of background components depends on their size, shape and relative position in the image. The horizontal and vertical lines are also eliminated. After the automatic cleaning process, a clean binary signature image without any background characters, lines and noise is obtained. Cleaned binary signature image is then prepared for binary-image features extraction.

- In this stage, the image is checked for orientation. If required, image is normalized to a horizontal position(5). The orientation formalization is only used if target signature(1) is found to be a forgery, since this finding could result from a change in the general orientation of a genuine signature from a normal position.
- The position of the signature is normalized in this stage(6). Position normalization is done by setting the origin of coordinates at the center of gravity of image(3). In such a way, the feature extraction is independent of the relative position of cleaned signature image within signature area(2).
- The binary signature image is thinned(7).
- The binary signature image is normalized with respect to writing line width by extracting the boundaries of the signature, and with respect to signature size by scaling(8).
- In this stage some debris or artifacts may appear due to the prior processing. This debris or artifacts are now removed by averaging(9) before sending this type of signature image to feature extraction.
- In this stage, features extraction and distance measure are done. Three types of signature image are used for segmentation and feature extraction (11). Cleaned binary image, size and line width normalized image (used as boundary detected image), and thinned signature image are used for dissimilarity measure block (10). Examples of the 3 types of images are shown in fig. 4.
- During signature segmentation and feature extraction process, all three signature image types are segmented into four quadrants using their gravity center. 'Adams' signature, for example(fig. 5), hows a gross approximation of a signature segmented into four quadrants. Three image types are also segmented into two vertical zones using a baseline detected from binary image using the method proposed by Ammar *et al.*(1988). They are also segmented into two horizontal zones using a geometrical mid point of the signature.
- Segments are used to compute horizontal, positive, vertical, and negative slant features (Ammar *et al.*, 1988). Slant features (12) of the input signature image are computed as follows: Four types of slant feature(percentage of horizontally, positively, vertically and negatively slanted pixels in the image are extracted in quadrants, vertical zones, horizontal zones, and in

the entire image) so that eventually, 36 slant features are extracted from the

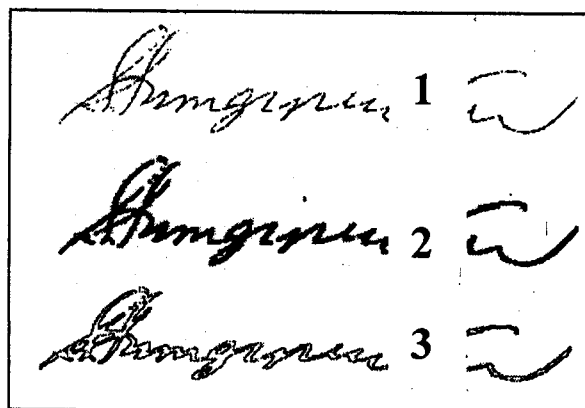


Fig. 4: Three Types of Signature Images Used in Feature Extraction: Thinned 1, Binary 2, And Boundary Detected 3

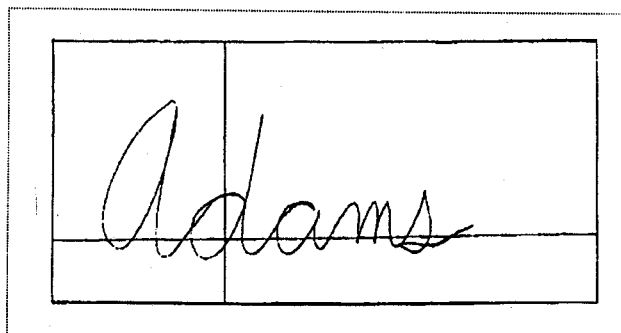


Fig. 5: Dividing the Signature Image Into 4 Quadrants

thinned image and 36 from the boundary detected one totaling to 72 features, represented as FI-Fn in the diagram.

- Features extracted are then used for dissimilarity measure using the weighted Euclidean distance(13). A feature set for dissimilarity measure is automatically selected using automatic evaluating program based on the method proposed by Ammar *et al.* (1989). The weighting of the Euclidean distance measure equations is computed automatically by the automatic evaluating program based on the mean and the standard deviation of the feature values computed on the training samples of the specific person.
- Dissimilarity measure (15) gives an indication of how far target signature is from a set of training, or authentic, samples of the same person's signature. For a specific person's signature, there is a natural degree of variation in the values of the features of the samples such that there is a *natural range of dissimilarity* measure of the person.
- If the dissimilarity measure of the target signature exceeds the natural range, the target signature is judged to be an attempted forgery, otherwise, it is accepted as genuine. The natural range is set up

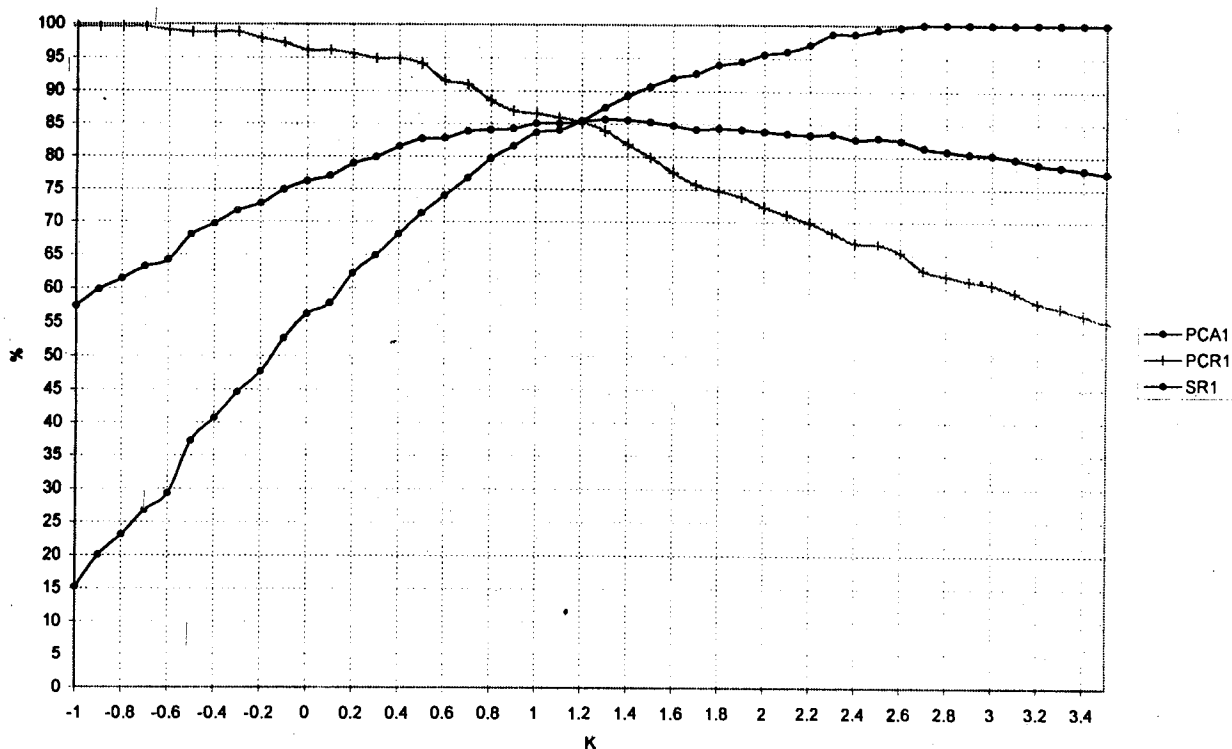


Fig. 6: PCA, PCR and SR Curves where, PCA: Percentage of Correctly Accepted Genuine Signatures, PCR: Percentage of Correctly Rejected Forgeries, and SR: System Reliability Calculated as  $(PCA+PCR)/2$ .  $k=1.2$  gives  $PCA=PCR=85\%$  for the Feature Set the Curves Computed for

by a predetermined threshold on the distance measure (Ammar *et al.*, 1988; Ammar, 1989; 1991; Ammar *et al.*, 1990 and 1989), obtained from PCA, PCR and SR curves computed on the training database, usually set to give  $PCA=PCR$ , or may be changed upon the desire of the user (bank). The training signature data we used consists of 1120 signatures. Fig. 6 Shows an example of these curves computed on our signature data.

**16- An adaptive decision threshold(16)** determines an upper limit of the natural range of the dissimilarity measure of a specific person. The upper limit of the adaptive threshold is computed using the predetermined threshold weighted by the standard deviation of the dissimilarity measures computed on the training samples of the specific person. Finally, if the distance measure(15) exceeded the adaptive threshold, the input signature is judged to be an attempted forgery, otherwise, it is accepted as genuine.

**Using the ASV Method Introduced Above in Bank Environment:** In research environment, the researcher selects his data to satisfy his requirements and assumptions, however, in the actual environment, a system developer must adapt to the environment the system must work in (type and quality of data, training data available, etc.). This point is a *very challenging*

*one* when a practical system is to be built, especially in an ASV system.

**Low Resolution Check Images:** In actual bank environment, some banks used very low resolution to digitize check images so that a 100 dpi was used in Citi-National bank, and some times 80 dpi was used in some American banks and some times 80 dpi was used in other when they started check imaging. When we were given such data to deal with it, the problem seemed to be unsolvable for the first time, because as it is known for specialists, and companies (SOFTPRO Company, 1999), developing such systems, going below 150 dpi gives bad results and no good verification can be realized, at any cost. Facing this dead lock, Intensive research was conducted on this topic because we had to do it since some banks have millions of such images, consequently, if we can not deal with them, the job can not be obtained. The result of research conducted on this issue led us to use features from binary, boundary detected and thinned signature images of the same signature, as showed in Fig. 4. In this way, we could go down to 100 dpi resolution without remarkable decrease in the accuracy. In order to get an idea of the difference in quality between 200 dpi signature images and 120 dpi ones, Fig. 7 shows examples of 200 dpi images, and Fig. 8 shows 120 dpi others from our signature data. It is obvious that the quality started to deteriorate seriously with the 120 dpi.

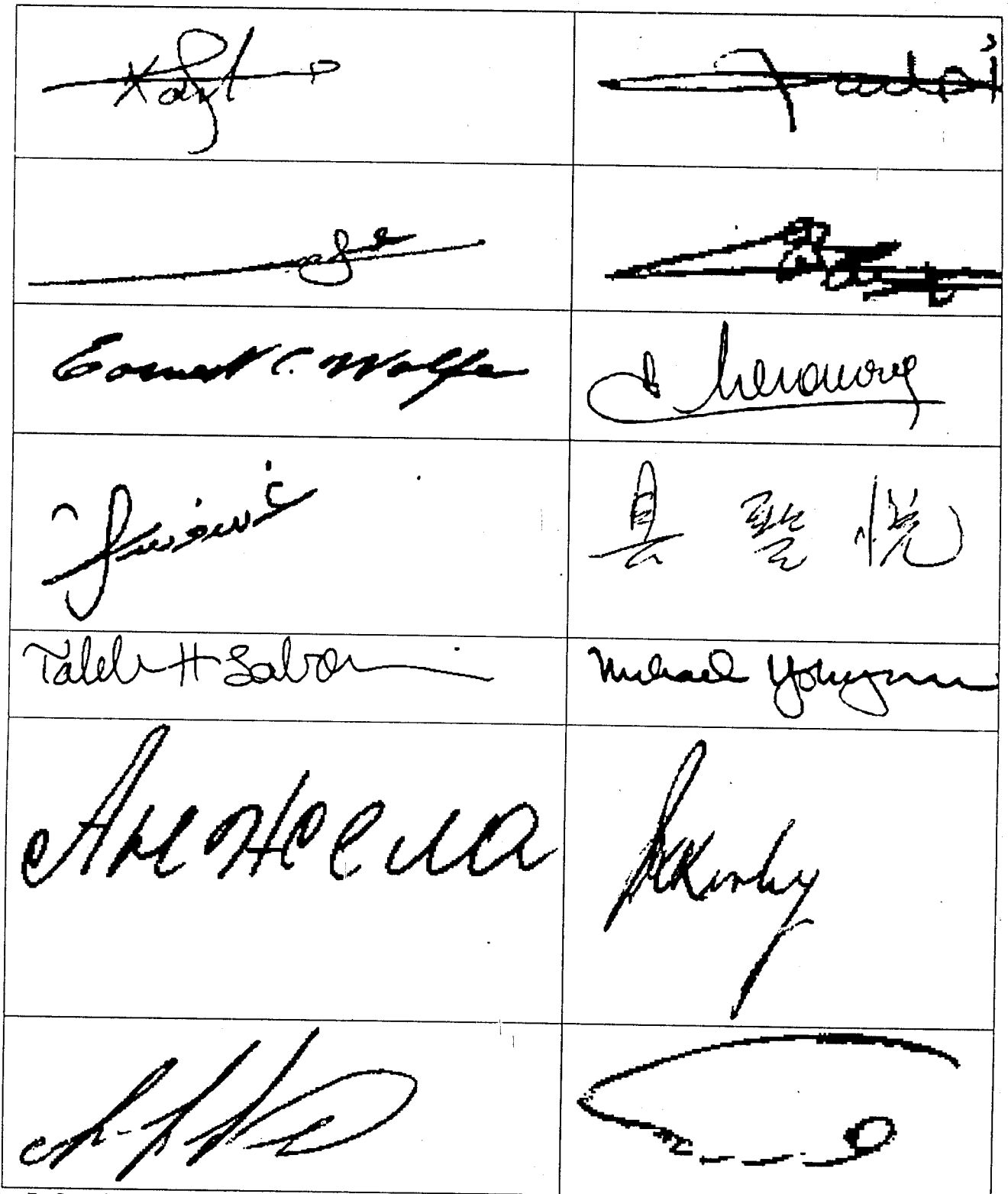


Fig. 7: Samples of the Signature Data Base Constructed Using Signatures of Writers from Different Nationalities with a Resolution of 200 Dpi


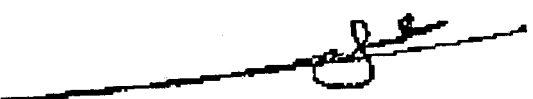

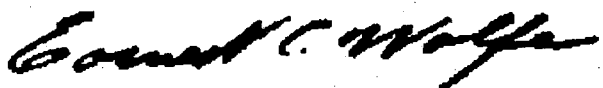

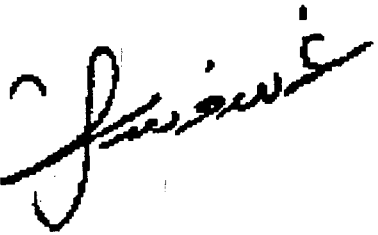


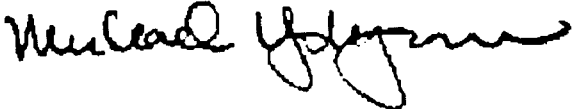


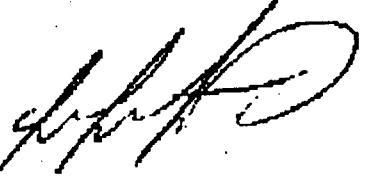

	
	
	
	
	
	
	

Fig. 8: Samples of the Signature Data Base Constructed Using Signatures of Writers From Different Nationalities with a Resolution of 120 Dpi





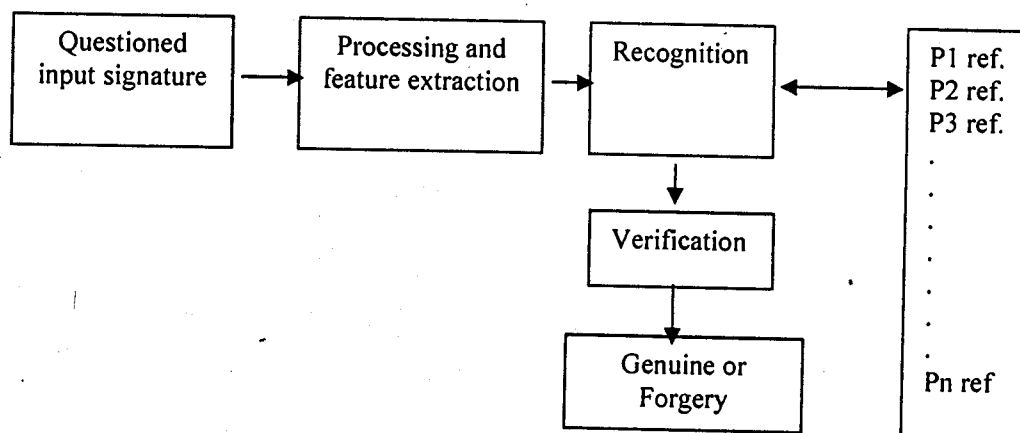


Fig. 10: Incorporation of Signatory Recognition Process in the ASV System

paper, we solved this problem as follows:

- The weights used in the distance measure for every person are computed from the training global signature data (1120 signatures).
- As new samples come from the new customer checks, these weights are modified gradually until 7 genuine samples become available, in which case, the weights are computed completely from the persons signatures.

It is important to note here that using the weights from the global signature database will lower the verification rate to about 80% when only one sample is available, but we must start with a single reference signature. As the new signatures become available, the training samples are accumulated and the weights from the global signature data are abandoned. In this way, the system automatically collects its training signatures for every person and starts with only one genuine signature. Fig. 9 illustrate how reference signature data are collected where:

**First Signature:** comes from the banks' existing electronic signature database or manual signature cards. This process is important because banking regulations dictate that banks refer to the original signature cards as reference.

**Additional Reference Data:** These signatures are picked up from the customer's checks that banks receive. The same process is performed to extract the customer's signature written on the checks as the first signature.

**Signatory Recognition:** In multiple accounts, it is necessary to recognize the writer of the signature in order to be able to retrieve his/her correct reference statistics to be used for verification, otherwise, the verification of the signatures of multiple signatory accounts become impossible. We solved this problem by recognizing the writer of the input signature of multiple signatory account check by computing the distance measure of the input signature with respect to all signatories of the account and recognizing the signatory as the one giving the minimum distance (minimum distance classifier). This method gave a recognition rate of up to 99% using our global signature data base (1120 samples). The signatories

may exceed in some cases 20 signatories for the same account according to the cases we encountered. Fig. 10 shows how this process is incorporated in the actual system.

**Verification Results:** The accuracy was tested in two environments:

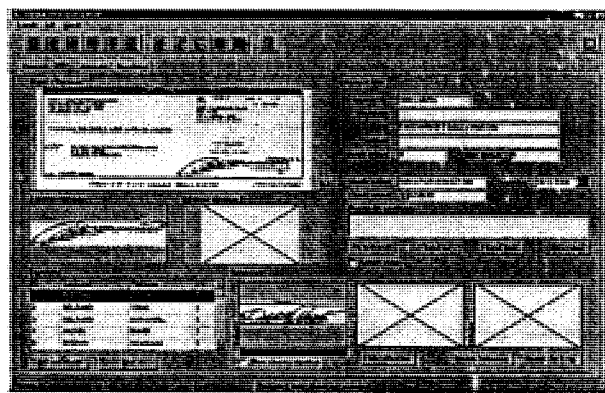
- **"Lab environment"** in which our signature database was used where the method introduced above provided a detection accuracy ratio of 100% for simple forgeries and over 90% for skilled forgeries. A PENTIUM II- 333 personal computer could process up to 20 verifications per second.
- **Field Test Environment** in which real batches from USA banks were used. Each batch contains 4300 - 5430 check images. The result was satisfactory were all known forgeries were detected.

During the verification process, as well as the verification result, the system can also provide the user with more details like displaying the suspect signature along with genuine ones for visual comparison, displaying values of irregular features, dissimilarity indicator, etc. . Fig. 11 (a) shows the actual verification screen in which the processed check appears as well as the questioned signature, a reference signature, and other information. Fig. 11 (b) shows displaying a forgery signature along with the dissimilarity measure, the ADT, and genuine samples for visual comparison. Fig. 11 (c) is the same as (b) but for a genuine signature.

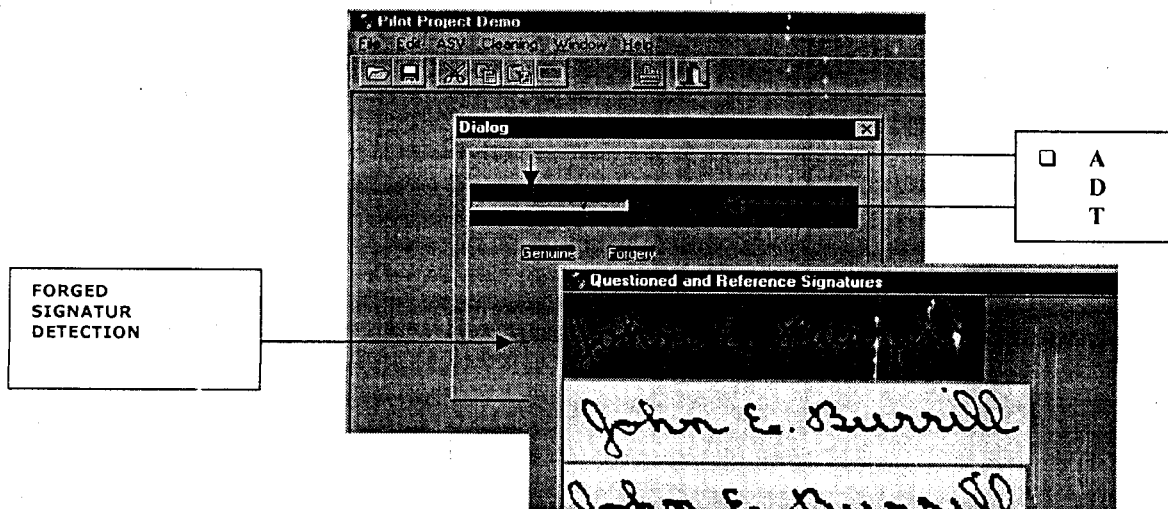
**The Pilot Project:** In the pilot project, the ASV server could be used as shown in fig. 12, in which the the ASV server receives its input from the check processor.

The above illustration assumes that the check images are available only after the Check Processing Operation. In an actual operation, however, check images will be sent to the ASV server in batches, as they become available. This will further reduce the processing time.

The other way is to incorporate a workflow between the ASV system and banks systems, as shown in fig. 13. Under this approach, banks can set up many different verification thresholds and the ASV system can route them to designated workstations.

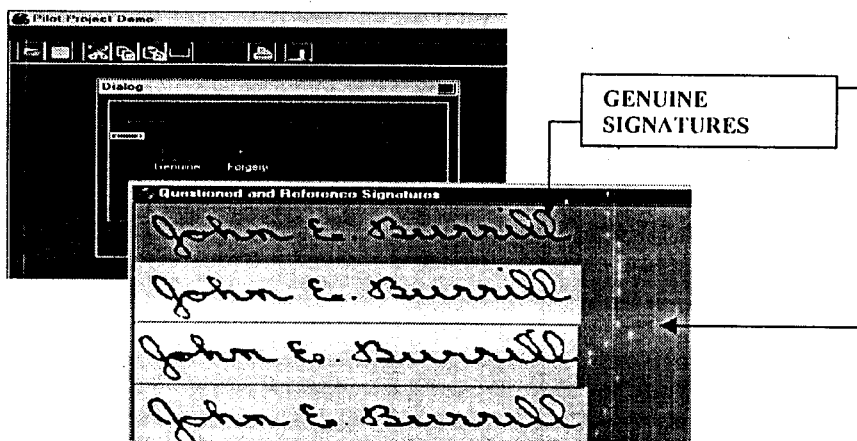


(a)



- ADT: Adaptive Decision Threshold (Adaptive to person's signature)
- DM: Dissimilarity Measure (Moving indicator shows how far the document signature is from the decision threshold ADT.)

(b)



(c)

Fig. 11: Response examples of the ASV system introduced: (a) main verification screen, (b) dissimilarity indicator for a forgery signature with the adaptive threshold ADT, and (c) dissimilarity indicator with the ADT for a genuine signature

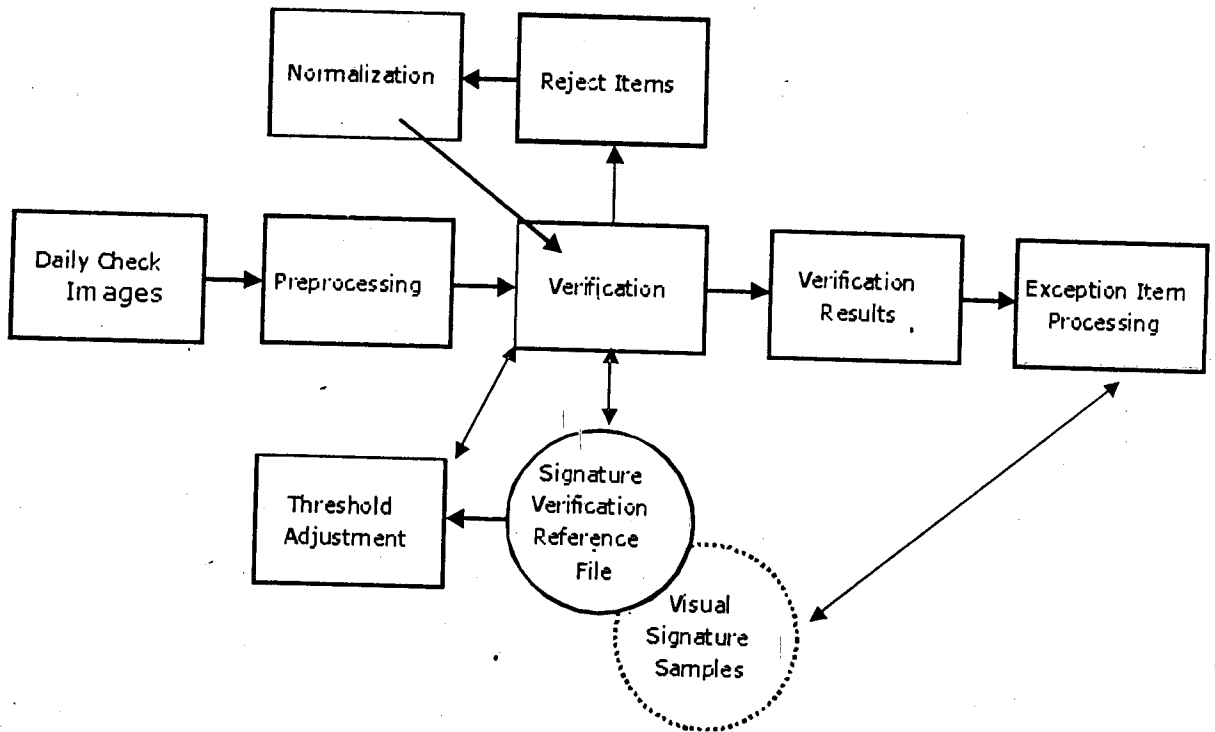


Fig. 11: Pilot System Flow

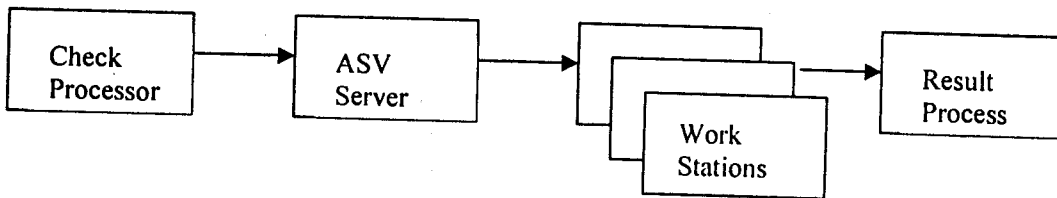


Fig. 12: A Method of using the ASV Server

**Conclusion**

In this paper, we introduced a method for ASV that can be used in actual bank environment. The method uses features extracted from different image types of the same questioned signature for verification. The way the features extracted enabled us to work with signature images of 100 dpi resolution without impact on the verification accuracy. We introduced also a method for recognizing signatories for verification of multiple signatures checks. The way of integrating the ASV method and the signatory recognition in a pilot project that can be used to support the security of financial transactions in e-banks in the new ICI environment was also introduced. The overall system proved to be reasonable in time response and cost where a Pentium II-333 can deliver 7200 verifications per hour tested on actual bank data.

**References**

- G. K. Gupta, and R. C. Joyce, 1997. A Study of Shape in Dynamic Handwritten Signature Verification. Technical Report, Computer Science Dept, James Cook Uni. of North Queensland.
- H. D. Crane and J. S. Ostrem, 1983. Automatic Signature Verification using a Three-axis Force-Sensitive Pen. IEEE Trans on Systems, Man and Cybernetics, SMC-13, 3, 329-337.
- H. Chang, J. Wang, and H. Suen, 1993. Dynamic Handwritten Chinese Signature Verification. Proc Second Int Conf on Document Analysis and Recognition, 258-261.
- J. Brault and R. Plamondon, 1984. Histogram Classifier for Characterization of Handwritten Signature Dynamic. Proc of 7th International Conf on Pattern Recognition, Montreal, 619-622.

## **Ammar et al.: A High Efficiency Method for Automatic Signature**

- M. Ammar, Y. Yoshida and T. Fukumura, 1987. Feature Extraction and Selection for Simulated Signature Verification, Proceedings of the 3rd Int. Sympo. on Handwriting and Computer Applications, Montreal, Canada, 167-169.
- M. Parizeau and R. Plamondon, 1990. A comparative Analysis of Regional Correlation, Dynamic Time Warping, and Skeletal Tree Matching for Signature Verification. Trans on Pattern Analysis and Machine Intelligence, 12: 7: 710-717.
- M. Ammar, Y. Yoshida and T. Fukumura, 1988. "Off-line preprocessing and verification of signatures", Int. Journal of Pattern Recognition and Artificial Intelligence, 2: 4: 589-602.
- M. Ammar, 1989. Applications of Signature Analysis by Computer and the Consequence of its Possible Misuse, Proceedings of the 5th Int. Conference on Image Analysis and Processing (SICIAP), Positano, 535.
- M. Ammar, 1991. "Progress in verification of skillfully Simulated Handwritten Signatures", International J. of Pattern Recognition and Artificial Intelligence (IJPRAI), 5: 1&2: 337-351.
- M. Ammar, Y. Yoshida and T. Fukumura, 1990. "Structural Description and Classification of Signature Images", Pattern Recognition J. 23: 7.
- M. Ammar, et al., 1989. Feature extraction and selection for simulated signature verification, Computer recognition and human production of andwriting, R. Plamondon et al. (editors), World scientific Publishing, 61.
- N. M. Herbst and C. N. Liu, 1977. Automatic Signature Verification Based on Accelerometry. IBM J Res Dev, pp 245-253.
- R. Nagel, 1973. "Computer screening of handwritten signatures: A proposal", Computer Science Center, Uni. of maryland, College Park, Technical Report, 220.
- R. N. Nagel and A. Rosenfeld (1977). Computer Detection of Freehand Forgeries, IEEE Trans on Computer. Vol C-26, No 9, pp 895-905.
- R. F. Farag and Y. T. Chien, 1972. On-line Signature Verification. Proc Int Conf on Online Interactive Computing, Brunel Uni., London, p 403.
- R. N. Nagel and A. Rosenfeld, 1977. Computer Detection of Freehand Forgeries, IEEE Trans on Computers. C-26, 9, pp 895-905.
- R. Sabourin, R. Plamondon and L. Beumier, 1994. Structural Interpretation of Handwritten Signature Images. in International J. of Pattern Recognition and Artificial Intelligence, 8: 3: Singapore, pp. 709-748.
- SOFTPRO Company, 1999. Press-release, 22.
- W. Nelson and E. Kishon, 1991. Use of Dynamic Features for Signature Verification. Proc IEEE Int Conf on Systems, Man, and Cybernetics, Charlottesville, pp. 201-205.
- W. Nelson, W. Turin and T. Hastie, 1994. Statistical Methods for On-line Signature Verification. In International J. of Pattern Recognition and Artificial Intelligence, 8: 3: Singapore, pp. 749-770.