http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 4 (1): 96-105, 2005
ISSN 1812-5638

Functions, Structure and Operation of a Modern System for Authentication of Signatures of Bank Checks

Musbah M. Aqel and Maan Ammar
Faculty of Computer Science and Information Technology,
Applied Science University, Amman, 11931, Jordan

Abstract: This study introduces in detail the functions necessary for the full work of a modern system for authentication of signatures of bank checks. It covers also the detailed structure necessary to implement these functions in an actual modern banking environment. The operation of such a system, the practical considerations and sample results are also presented.

Key words: Signature, verification, reference making, data model, accuracy, DLLs, automatic evaluation, visual verification

INTRODUCTION

It has been an established fact that verifying static (off-line) signatures is more difficult than verifying dynamic (on-line) ones so that the impressive results obtained in on-line related works attracted more researchers than that on off-line verification[1]. Verification of simple forgeries started in the early 1970s[2]. The research on verification of skilled forgeries, on the other hand, started about one decade later with modest results[3,4]. In 1986, Ammar *et al.*[5] reported the first successful work on verification of skilled forgeries, using mainly dynamics-related features extracted from gray-level signature images. Figure 1 shows examples of simple and skilled forgeries. Later, Ammar *et al.*[6,7] reported that carefully selected shape features can give a 14% average error rate and if the shape feature set is augmented by one density feature (high density factor, HDF extracted in a relative manner for stability), the average error rate may become lower than 9%. The encouraging results obtained by using dynamics-related features(High Pressure Regions)[6] and that obtained by using structural features[8] stimulated Sabourin *et al.*[9] to conduct further research in the direction of combining the effectiveness of the dynamics-related features and the structural ones for the final goal of eliminating skilled forgeries in off-line systems.

Ammar *et al.*[10,11] proposed a unique method for conceptual description of signature images and used it to analyze a signature database. This conceptual description was essentially developed for the purpose of building a signature database that can be accessed using the pictorial information of the signatures, since, in general, the signature is not readable. Dramatically, during the next year, this method of description led to developing an image understanding system using a friendly natural language interface and used in simulation of several interesting applications in the field of signature analysis and verification[12,13]. The conceptual description in conjunction with Artificial Intelligence and Computer Vision techniques has been recently used by Ammar[14] to realize an intelligent signatory recognition approach.

All researches mentioned above share one aspect that they are research works using lab signature data. In the late 1980s and early 1990s, visual signature

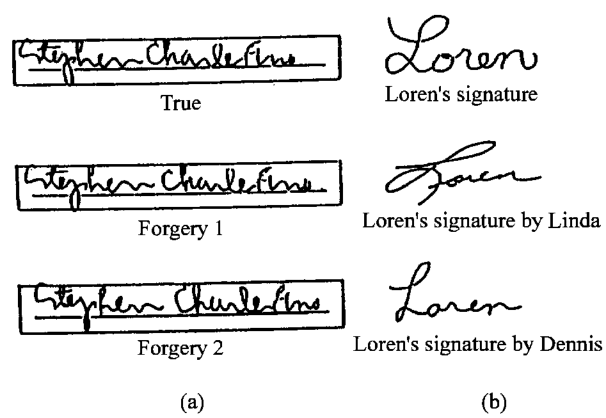

Fig. 1: (a) Samples of skilled forgeries used in Dr. Ammar researches and (b) Sample forgeries used by Nemcek *et al.*[2]

Corresponding Author: Dr. Musbah M. Aqel, Faculty of Computer Science and Information Technology, Applied Science University, P.O. Box 174, 11931, Amman, Jordan
E-mail: m_aqel@asu.edu.jo

verification systems that retrieve a reference signature to the screen of a computer to compare with check signature started to be used in some banks replacing the card index systems. This fact, stimulated Dr. Ammar to concentrate efforts to transform his achievements developed using giant computers (Nagoya University, FUJITUSU FACOM-382 of Japan) to work on PCS and with actual data. These efforts led in 1995 to finishing an automatic signature verification system that can be used with IBM compatible PCS under DOS, SIGVA 1.0[15].

In the late 1990s, bank losses due to checks forgeries reached astronomical figures (12 billion dollars in the USA only, in 1998) and Financial Systems Technology Consortium FTSC in the USA formed an automatic signature verification initiative. This initiative is a call to place further importance and urgency on the need to verify signatures automatically, which gave ASV increasing importance. This situation stimulated some people from the private sector to search for an ASV software and through the Internet, an agreement made with Dr. Ammar, so that SIGVA 1.0, was developed to work under windows and modified to work with actual bank checks with the ability to deal with distinctly low resolution. This system is based on the method reported in reference[16].

In the late 1990s also, SOFTPRO (a signature software company) used SIVAL (a signature validation program) developed by IBM based on neural networks to validate English written signatures, but can not work with signatures written in other languages, does not perform automatic cleaning of check background and can not work with resolutions less than 150 dpi[17], while eBankDiscovery developed under supervision of Dr. Ammar and USA patented[18], automatically cut out the check signature, cleans background, accepts all kinds of signatures and may work with resolutions as low as 80-100 dpi[16].

In this study, we introduce the functions, the detailed structure, the practical consideration and operation of a modern ASV system (the Discovery) based on the method reported in Ammar *et al.*[16] and used in USA and Singapore in some banking sites. It has the advantage of being able to improve its performance as new data is processed in actual use in bank and it is based on forensic science principles in forgery detection. Details concerning the system setup, reference making, verification, confirmation, DLL's, data model, accuracy, as well as a performance report will be covered in the study.

The system: The system which is based on forensic science principles in forgery detection and decision making, accepts any kind of signatures as an input

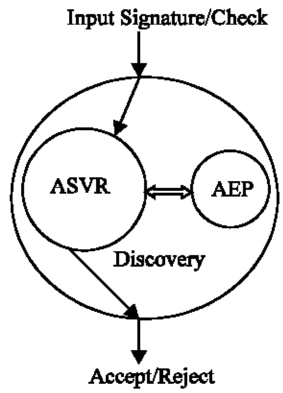

Fig. 2: The general schematic diagram of the ASV system. ASVR: Automatic Signature Verifier and AEP: Automatic Evaluation Program

(written in any language or as an arbitrary shape) and its performance will continue to improve as it collects more reference data while in actual use, will be covered in detail in the following sections. The very general diagram of the system is shown in Fig. 2, as listed in the patent document.

Figure 2 shows the system consists mainly of two subsystems: the automatic signature verifier ASVR and the automatic evaluation program.

Setup

AEP (Automatic Evaluation Program)

1. The Discovery obtains different verification reference data from each signature. They vary by image type, quality and background. Each new incoming data is studied and the discovery reconfigures and finely tunes the cleaning, segmentation, reference building and verification procedure for optimized performance. AEP automates this process by examining the quality of data and selecting a proper set of DLL's depending on the characteristics of clients' check images. The role of AEP is to:

    - Find the best combination of features for a specific kind of data.
    - Evaluate the performance of the DLL's.
    - Study the effects of specific features on verification and if negative, not use them.
    - Make interactive evaluation with cleaning and segmentation, by using different versions or functions of cleaning and segmentation DLL's in different tests to find the best combination of DLL's.

2. Even when the Discovery is in use, new features/methods can be added to the system without building or modifying any software.
3. When a bank using the Discover gains sufficient knowledge of the Discovery's capabilities and workings, AEP can frequently be run to enhance the system's overall performance.

System flags:

- Stamped signature
- No. of signatures on check (1 or 2. Blank or 0 is 1.)
- Signatory check (0: no, 1: yes. If yes, go to signatory matrix. $ amount requires a specific signature identified by account-sequence number.)
- Fraud history (0: no, 1: yes)

Check types:

- Size and background color
- Signature location
- Multiple signatures (Vertical, V or Horizontal, H)

REFERENCE MAKING

Signature holding tank: Signatures to be used as reference are collected at two separate stages and stored in the holding tank. The first stage is when the Discovery is installed for the first time. The second stage is during the normal run (Fig. 3). As each signature is extracted from checks for verification, its written habits and Stability Degree are examined. When it is determined that a signature would enhance its particular data integrity, it is added to the holding tank.

Each account has up to 10 signature references and each reference has 2 sets of features. Each reference signature is identified by Account number and by sequence number (e.g. first reference: account no.-1; tenth reference: account no.-10)

Each record has the following data.

a) Multiple or single
b) Signatory matrix code
c) Source code (from signature card, check, pen pad, SQN, etc.)
d) Date it was acquired
e) Date it was used as reference
f) Status code
g) Stability degree
h) Type of signature
I) Signature image

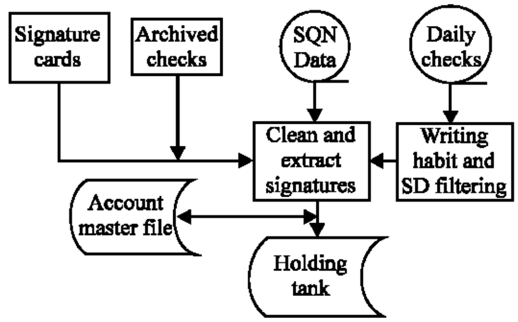

Fig. 3: Signature collection

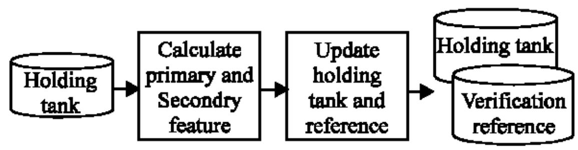

Fig. 4: Creation of verification reference database

Reference making: From the holding tank, primary feature sets and secondary feature sets are extracted and form a verification reference database (Fig. 4). Each record has the following data:

a) Account and seq. No.
b) Status code
c) Multiple of single
d) Signatory matrix code
e) Source code
f) Stability degree
g) Type of signature (quality, category, etc.)
h) Primary features
I) Secondary features

Used signatures will either remain in the holding tank or be filed away. These signatures will be used later for two-dimensional Reference Pattern Based Features[1].

Update: At each day's and month's end (or at any other time designated by the user), the system will search out new signatures to update from the holding tank. Parameters are:

1. New accounts
2. Account changes
3. New style signature (exemplary or higher SD)
4. Manual override (Display all available signatures for selective update - audit trail needed)
5. Replace the oldest one with new signature every 6 months.

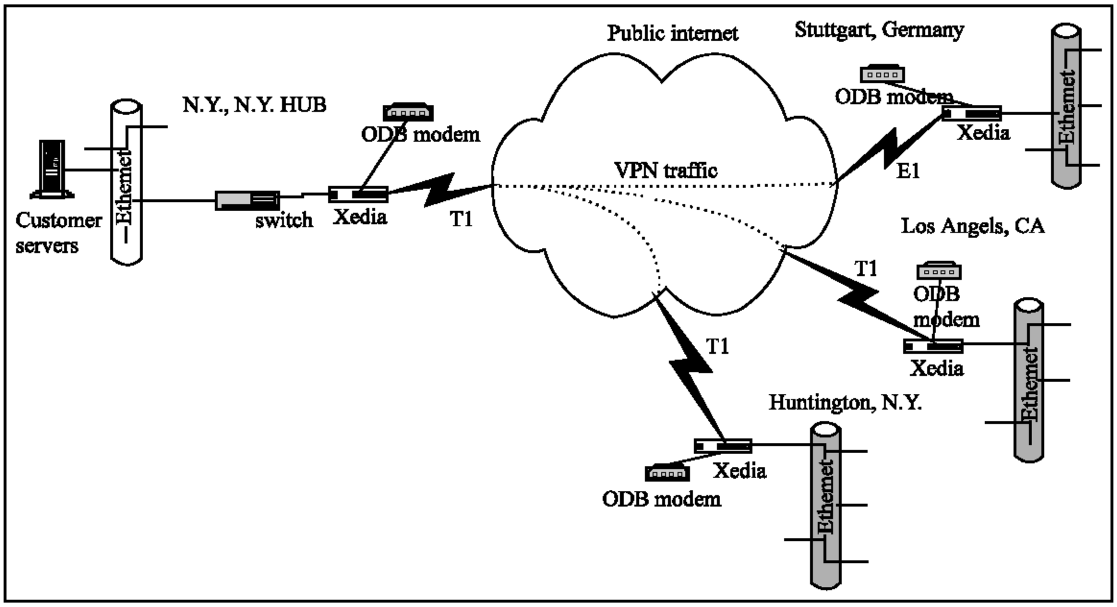

Fig. 5: ASV support network (LA and Huntington are client sites)

Reports and inquiries: An authorized user can view all signatures in any sequence and print out reports showing statistics, movements, etc. Under no circumstances, should a record be deleted.

The discovery support network: During the use of the system, the need may arise any time to ask for support or explanations by users, therefore, a support network is set for this purpose. Figure 5 shows the support network.

VERIFICATION

In terms of function, the Discovery delivers the following capabilities.

1. Verification processing (batch)
2. Result processing work flow
3. Verification processing (On-line)
4. Remote signature capture (Check scanner, pen pad)

The diagrams in the following figures show processing flows of each program.

Verification processing (batch): Most of the Discovery's verification run is performed in batch mode. In a typical configuration mode, the Discovery have two servers: a verification server and a database server, as shown in Fig. 6.

The verification server is positioned within the check processing environment to receive check images and return verification results. In case of A, results are passed on to the bank's existing visual verification system. In case of B, results are passed on to the Discovery's own visual verification process. In this study, we will discuss only the case B.

As the case in one of the banks using the Discovery (current bank), they process checks daily (Fig. 7). There are two types of checks they receive every day. One is in-transit, which are the checks drawn on other banks but deposited with current bank. The other is checks drawn on them (their own checks). These are the only ones that concern the Discovery here.

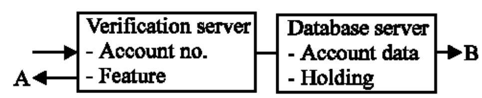

Fig. 6: The Discovery's two servers

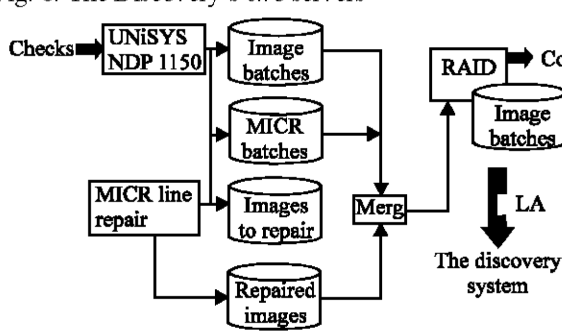

Fig. 7: Daily processing of checks

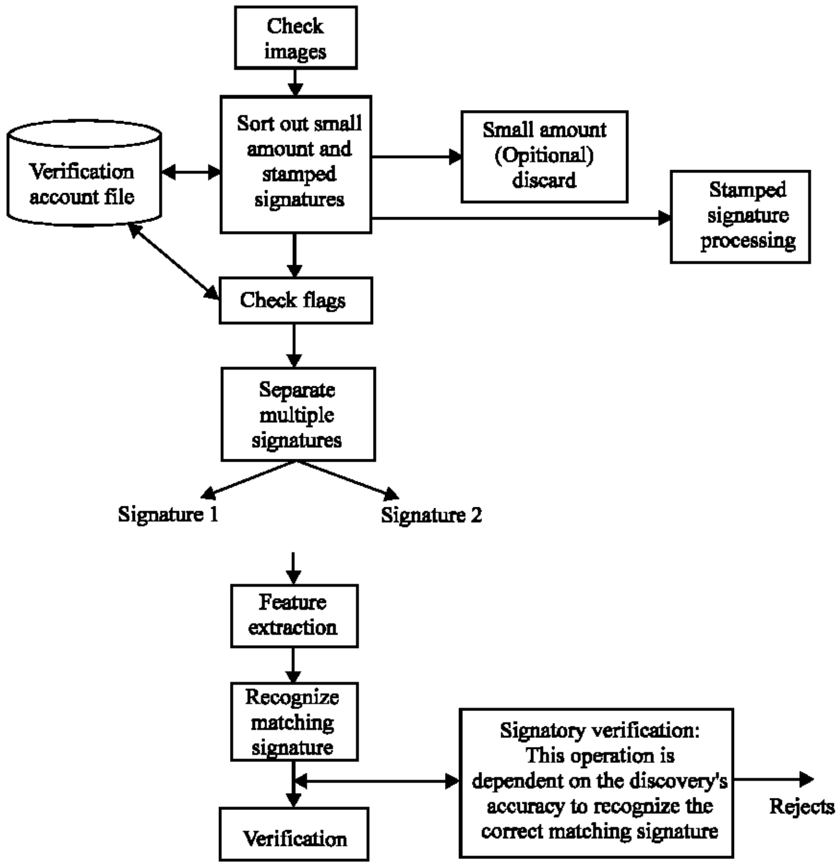

Fig. 8: Process 1: From check images to verification point

The Discovery may receive the images as they become available or straight from the RAID system. RAID stores the bank's work-in-process images and COLD stores the bank's entire image archives that services all images inquiries. Update from RAID to COLD generally takes place between 2:00 and 6:00 a.m.

In certain cases, the image file containing checks-to-be-verified may be in the form of a CD, such as the case in Singapore bank.

Verification processing of batches is done in two processes:

Process 1: From Check Images to Verification Point, as shown in Fig. 8

Process 2: Signature Verification

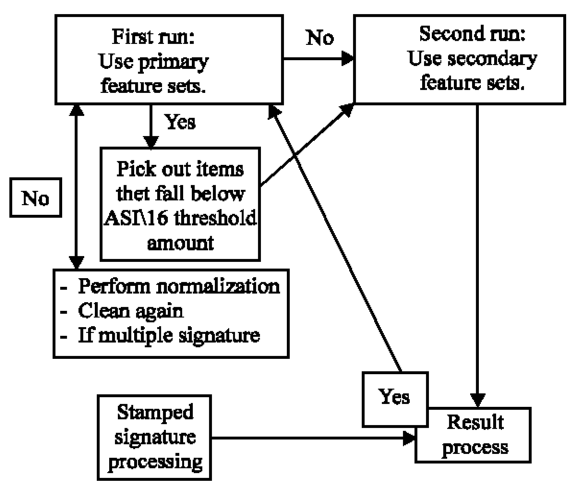

Fig. 9: Process 2: Signature verification

A stamped signature should be considered a seal rather than a signature, thus requiring a separate process (Fig. 9). ASI\16 sorts out items with out-of-range check numbers and amounts pretty accurately. It is therefore expected that other fraudulent items will be found in the dollar range less than ASI\16. The user, however, should be allowed to set his own verification parameters.

Result processing workflow: Server One and Server Two can be two machines or one machine, depending on the bank's daily volume, on the size of database and on the usage of other applications. Upon receiving the verification result from Server One, Server Two creates verification process data by linking the results to the account master.

Summary Report lists all verification results.

- Total no. of items processed
- No. of items verified
- No. of items rejected.

Details by Reason report lists suspect items, items bypassed because the amounts were too small, signatory unmatched items and missing database. Each reason category is linked to detail transaction items.

Confirmation process: Typically, a bank would require more than one person to approve a transaction. With the Discovery, it is approached in two ways. In the case of a small volume operation, we will assume that the person who examines suspect items has the authority to accept or forward. All items accepted will only be supported by producing a detail log (Fig. 10) . In the other situation where the items need to be distributed to more than one person, the Discovery will provide an option for secondary review.

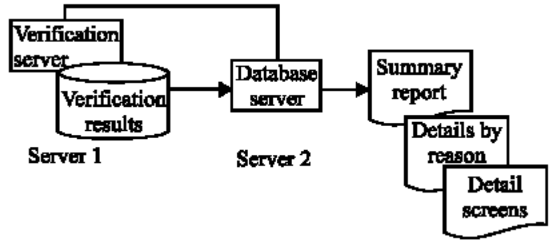

Fig. 10: Verification process and summary report

Items requiring visual verification are distributed to a predetermined persons. Larger items are distributed to a more experienced verifier, or the items can be grouped by reject types or by account group (Fig. 11). This methodology will be individually tailored within the system's parameter grouping and no customization of the software should be allowed for this process. Figure 12 shows a visual verification screen of the Discovery.

Once an item is viewed, only one of three decisions can be made: accept, reject or investigate.

Accept: A bank will accept items from the questionable group because they are either:

1. False rejects
2. Initials or abbreviated signatures

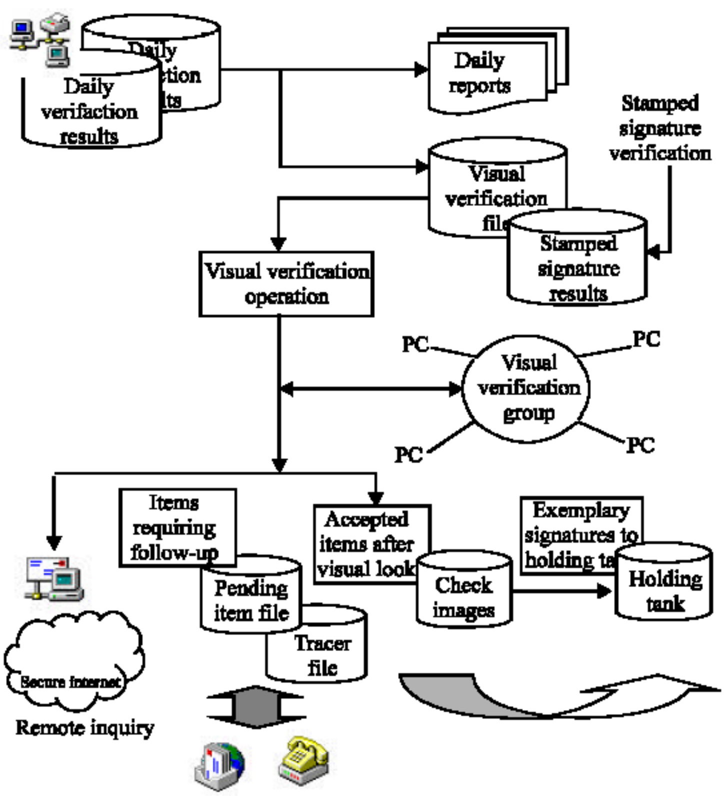

Fig. 11: Visual verification in the verification process

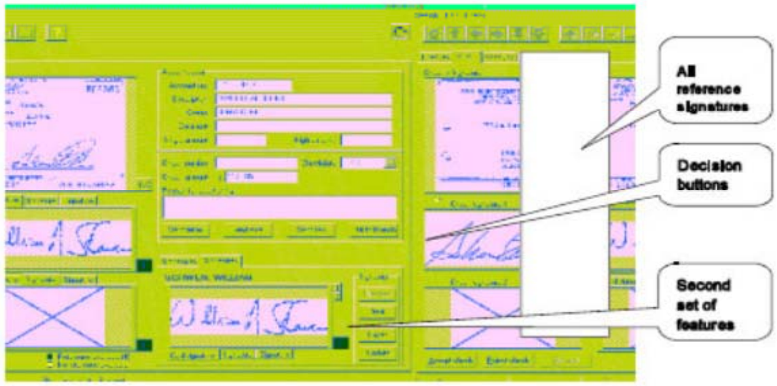

Fig. 12: Visual verification screen

3. Too close to call by the Discovery (Distance Measures between 101 to 110, or the range selected by the user)
4. Missing signatory

In the case of these items, no action is taken. Once approved, these items should go to the holding tank for a reference update with a code showing the reason for acceptance.

Reject: These items should be considered forgeries. The Discovery should print them and their respective account records should be updated/ and update their respective account records. During the verification run, all accounts with this flag will go through multiple passes or through increased ADT.

Investigate: These items will be:

1. Too close to call (Distance Measures between 110 to 150, or the range selected by the user).
2. DM is too low (Distance Measures between 1 to 20, or the range selected by the user).

The Discovery presents several options to the user.

1. Email to signer. An email message alerts the signer that he should examine the questionable signature, by accessing the account file through the Internet. A separate copy of the email may be forwarded to the branch.
2. Fax to branch. A fax message shows the check image and contains the reason for questioning, the amount and sample signatures.
3. Hardcopy printout. Although the request for one is highly unlikely, this option should be provided.

All items should be kept in the pending file. Periodically (time intervals to be determined by user), the system should produce a pending file list. Also, at the user's discretion, the system should generate automatic tracers.

In the corresponding banking situation a S.W.I.F.T. message is added. At this point, no direct interface with the S.W.I.F.T. system is considered; however, a file containing the S.W.I.F.T. messages should be dumped on a diskette for manual transport to the S.W.I.F.T. system.

Accuracy: The accuracy of the Discovery is related to two main factors:

1. The accuracy is determined completely by effectiveness of the features and decision making process. In this case there are no effects of background and cleaning. With the features when they are selected, the highest possible accuracy is almost reached. The improvement that can be achieved will be determined by the CMBAEP which will tell us exactly what is the highest possible PCA, PCR and SR with a specific feature set among the possible feature sets of a given n number of features extracted. Theoretically, for every n features, we have n! combinations or (feature sets). For a large number of features like 80, 50 or even much lesser number, it is prohibitive, practically speaking, to search all these feature sets. The CMBAEP reduces the required number to n x n, which is a more realistic figure. We need to apply it several times to see the best feature set possible, bearing in mind the way they are extracted. It can not be blind application of the program. Once we made this we know the best feature set or the best few feature sets that we can use to select the best one among them according to the desired possible PCA and PCR.

2. The goodness of the extraction and cleaning which will affect the result if some background elements remained or some parts of the signatures are cut out during cleaning and extraction. These will affect and reduce the nominal accuracy measured on cleaned data like the one used for test. The goodness of the extraction and cleaning algorithms can be seen on actual bank data[19].

CMBAEP: The Circulant Matrix Based AEP enables us to discover the potential power in different feature sets in one program run on the whole data. It is a very powerful tool in optimizing the accuracy of the Discovery.

Online verification: When a signer writes his signature on a pen pad or scan a check, the captured image is forwarded to the Discovery server for verification. Only one attachment will be allowed-either pen pad or scanner. When the image from the scanner is used, it will be desirable to have the system read the MICR line codes.

In both cases, a detailed log should be provided. The log will record who did what and when. Aside from the plug-in's, no program should reside in the user's Personal Computer.

Remote user inquiry station: Inquiry station is a standard Personal Computer (Fig. 13).

- Connections to Check Scanner or Pen Pad should be plug-in's.

This program is intended for use by the Branch (teller, platform officer and service desk), merchants and other banks and has three basic functions.

- Visual inquiry
- New account setup
- Online verification

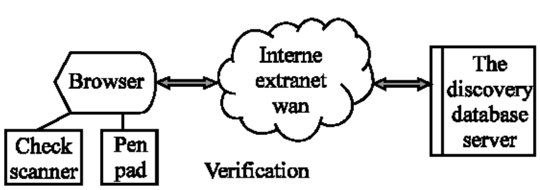

Fig. 13: Remote inquiry station

Visual inquiry: The user logs on and enters his account number. Account data and three (3) sample signatures are displayed. For multiple signature accounts, or for signatory-defined accounts, scrolling ability is provided.

New account setup: The screen displays the new account screen layout. The user fills in all of the appropriate boxes and activates the pen pad to capture the customer's signature(s). When a new customer signs his/her signature on a pen pad, we can get up to three samples.

DLL's

The functions (DLL's) built in the Discovery are five main functions:

1. Cleaning of signature cards and extraction of signatures.
   Input: Card Image+cleaning and extraction parameters.
   Output: Extracted cleaned signatures.
2. Cleaning of checks and extraction of signatures.
   Input: Check image+cleaning and extraction parameters.
   Output: Extracted cleaned signatures.
3. Feature extraction of signatures.
   Input: signature image.
   Output: Features.
4. Making reference.
   Input: Features of signature(s).
   Output: Reference Statistics (RS).
5. Verification.
   Input: Features of questionable signature + RS of all signatories related to the account.
   Output: Distance and verification result (Genuine, Forgery, no decision).

CONFIGURATION

The following is a configuration used for the Discovery:

Hardware:
> 1 ProLiant 3000R 6/600 Model 1 Rack (128MB)
> 1 128MB SDRam DIMM kit
> 1 256MB SDRam DIMM kit
> 3 9.1 GB Wide Pluggable Ultra2 SCSI Drive (1")
> 1 Internal 20/40 Gigabyte DLT Drive
> 1 64-Bit Dual Channel Wide Ultra3 SCSI Adapter
> 1 Storage Works Enclosure Model 4214R - Rack
> 1 ProLiant 3000/5000 Redundant Power Supply
> 1 Storage Works Enclosure 4200 Redundant Power Supply
> 1 ProLiant 3000/5000 Redundant Fan Kit
> 1 R3000h-NA UPS
> 1 Compaq Rack Model 9142 (42U height)
> 1 Rack Internal Trackball Keyboard

Table 1: Performance Report (randomly selected items)

Account No.	Check No.	Amount	DM	No. of Signatures	Reason
9474943	2547	120.00	129	2	Forgery
75031831	2687	1,500.00	167	1	Teller
75031831	2688	639.45	141	1	Forgery
1141988	27036	1,015.06	87	5	Accepted
1141988	27133	2,874.37	102	5	Rejected but should be added as additional reference
1141988	27207	3,000.00	227	5	Missing signature
13197555	114132	303.75	178/207	9	Only one signature
13017255	21474	4,256.64	187	14	Missing signature
1160087	9485	1,049.10	165	2	Forgery (Bad DB)
1160087	9498	5,000.00	186	2	Forgery (Bad DB)
1127357	7102	1,000.00	167	3	Forgery
1112368	6533	116.96	184	2	Forgery
1347632	6474	1,125.00	288	4	Forgery
1857533	304327	125.00	283	5	Forgery
1113577	23651	717.32	50	2	Accepted
1113577	23600	825.00	268	2	Rejected
10324505	2383	1,178.65	214	4	Forgery
1378453	1039769	1,387.09	230	8	Stamped, must be flagged.
1375695	7478	209.68	213	4	Forgery
10065781	3214	175.68	212	2	Bad data
1268961	3856	3,217.80	211	2	Missing signature

Date and Time: 20.11.2000, Total No. Of Checks: 4367, No. Of Checks Accepted: 3670, No. Of Checks Questioned: 697

> 1 42U Side Panel Kit
> 1 Keyboard Drawer Kit (1U)
> 1 Monitor/Utility Shelf Kit
> 1 Rack Stabilizing Feet
> 1 12' CPU-to-Switch Cable
> 2 Rack Blanking Panel Kit (15U)
> CD & Floppy drives

Software:
Windows NT Server.
SP 4.
MDAC 2.0.
Explorer 5.0.
MS SQL Server full (VB Scripting).
MDAC_TYP_ENG.
ASV Server.
ASV Client.

These software components are installed properly on the hardware mentioned above to achieve the full functions of the Discovery.

PERFORMANCE REPORT

Table 1 shows a sample performance report.

CONCLUSIONS

We introduced in this study the details of setting up testing and operation of a modern system for the authentication of bank checks signatures. We presented in details the diagrams necessary for the explanation of the actual verification process, reference making, automatic and visual verification as well as the confirmation process. Finally we presented a sample of result report in which the parameters related to the verification and decision making process can be found as concrete facts. This study, which presented an actual modern ASV system gives an insight into the ASV process in modern banking environment, its complications and how much work is needed to achieve the complete solution of the ASV.

REFERENCES

1. Ammar, M., 1991. Progress in verification of skillfully simulated handwritten signatures. Intl. J. Pattern Recognition and Artificial Intelligence., 5: 337-351.
2. Nemcek, W.F. *et al.*, 1974. Experimental investigation of automatic signature verification. IEEE Trans. Syst. Man Cybern, 4: 121-126.
3. Brocklehurst, E., 1985. Computer methods for signature verification. Forensic Sci. Soc., 25: 445-457.
4. DeBruyne, P. and R. Porre, 1986. Signature verification with elastic image matching. Proc. Int. Granaham Conf. Security Tech., Gothenburg, Sweden, pp: 113-118.
5. Ammar, M., Y. Yoshida and T. Fukumara, 1986. A new effective approach for off-line verification of signatures by using pressure features. IEEE Trans on Systems, Man and Cybernetics, SMC-16: 39-47.
6. Ammar, M., Y. Yoshida and T. Fukumura, 1988. Off-line preprocessing and verification of signatures. Intl. J. Pattern Recogn. Artif. Intel., 2: 589-602.

7. Ammar, M., Y. Yoshida and T. Fukumura, 1989. Feature Extraction and Selection for Simulated Signature Verification. Computer Recognition and Human Production of Handwriting, Eds. Plamondon, R., C.Y. Suen and M.L. Simner, World Scientific, pp: 61-76.
8. Sabourin *et al*., 1987. On the implementation of some graphometric techniques for interactive signature verification. Proc. 3rd Intl. Symp. on Handwriting and Computer Applications, pp: 160-162.
9. Sabourin, R. *et al*., 1988. Segmentation of handwritten signature images using the statistics of directional data. Proc. 9th Intl. Conf. on Pattern Recognition (91CPR), pp: 76-79.
10. Ammar, M. *et al*., 1988. Description of signature images and its application to their classification, Proceedings of the 9th Intl. Conf. on Pattern Recognition, Rome, pp: 23.
11. Ammar, M., Y. Yoshida and T. Fukumura, 1990. Structural description and classification of signature images. Pattern Recognition, 23: 697-710.
12. Ammar, M., 1989. Applications of signature analysis by computer and the consequence of its possible misuse. Proc. 5th Intl. Conf. on Image Analysis and Processing (5ICIAP), Positano, pp: 535-542.
13. Ammar, M., 1989. Signature verification and description. Ph.D. Thesis, Nagoya University, Japan.
14. Ammar, M., 2002. Application of Artificial Intelligence and Computer Vision techniques to signatory recognition. Pak. J. Inform. Technol., 2: 44-54.
15. Ammar, M., M. Aita, B. Younaki and B. Takwa, 1995. A Practical software system for automatic off-line verification of signatures, usable with IBM-PC compatible machines. 7th Biennieal Conf. Intl. Graphonomics Society, London, Ontario, Canada, Aug. 1995.
16. Ammar, M. and M.A. Musbah, 2002. A high efficiency method for Automatic Signature Verification (ASV) in I-C-I environment. Pak. J. Inform. Technol., 1: 160-172.
17. SOFTPRO Company, Press-release, 22 March, 1999.
18. Ammar, M., 1999. Development and production of method and apparatus for signature verification, Patent No. 09/453730, 2/12/1999, USA.
19. Ammar, M. and M.A. Musbah, 2003. Verification of signatures of bank checks at very low resolutions and noisy images. Applied Science University J., (Submitted).