Journal of Information & Communication Technology
Vol. 2, No. 2, (Fall 2008) 90-100

Online Banking Transaction System

Adnan Alam Khan *
College of Business and Management Karachi, Pakistan.
Noor Zaman *
King Faisal University
College of Computer Science & IT , Saudi Arabia
Mansoor uz Zafar Dawood *
Institute of Business & Technology, Karachi, Pakistan.

ABSTRACT

Financial Institutions plays a vital role in development of any country. Each financial institution has to follow the rules of the country mother bank. The policy of any mother bank is to facilitate the nation and holding reserves and generate currency for its country. In this paper we are going to discuss and implement a system that helps our nation to draw or deposit money in more conventional way. This system is the combination of old and newly proposed cheque system, using computer technology this system is much more faster, secure and provide confidence and authenticity for any consumer.

INSPEC Classification : C0230, C03104, C5600, C6100, D2050E

1. INTRODUCTION

Thousands of banks performs millions of transactions every day and thousands of users follow the almost the same banking system. As we know that if number of users increases we need more banks and more staff it means we have to put more money in this system. If we developed advanced computerized based banking system so there is no need to open new branches in remote areas or same branch provides services to other banking system E.g ATM system.

Banking system requires authenticity and validity if a system provides these basic logic that mean we can developed a new system that authenticate and validate the user and user can do any type of virtual transaction any time any where in minimum amount of time. One of the most authentic codes for recognition of any person is signature. It always appear on almost all types of documents, such as property documents, bank cheques, and credit slips, thus signature has a great importance in our daily life, therefore automatic signature verification is important in the field of document analysis and processing for which a lot of work has been done in the past.

* The material presented by the authors does not necessarily portray the viewpoint of the editors and the management of the Institute of Business and Technology (BIZTEK) or College of Business and Management Karachi, Pakistan & College of Computer Science & IT , Saudi Arabia

* Adnan Alam Khan : adnan_hiit@yahoo.com
* Noor Zaman : nzaman@kfu.edu.sa
* Mansoor Uz Zafar : dr.mzdawood@biztek.edu.pk

In case of transaction signature validation provides authenticity to the bank. In e-banking system most of the banks used signature verification software to get the authorized data. Signature verification requires an image of a signature that is used for recognition, it has different steps. Basic step to register a person signature into database, the second step is the elimination of random forgeries defined as genuine signatures of other writers enrolled or not in the signature verification system. This class of forgeries should be eliminated in practice for real applications such as property documents and bank cheques authentication because in the human eye, color information is processed at lower spatial frequency than intensity. In fact, the elimination of random forgeries is a small task for human beings in general but it is still an open problem for the computer.

For signature verification, the accuracy of the present systems is not impressive and efficient. It is always seen in real life that either signatures are made on white paper or on colored paper. Several methods have already been developed for the verification of the signatures to eliminate the random forgeries. But it is still very difficult and complicated to verify and compare the signatures digitally with colored backgrounds because white paper has low intensity while the color paper has high intensity rate.

The aim of this research is to develop a fast, robust and a reliable BTS banking transaction system based on signature verification system, which will not only identify the genuine signature image, captured from colored paper but it also rejects all kinds of forgeries. In this paper, a mechanism is proposed that automates the BTS using signature verification even with different background colors. The work presented in this paper, is focused to examine whether an input signature having colored paper is a genuine one or a forgery by checking it through database and give its decision to the BTS weather this transaction is genuine or forgery. Comparing the collected signature samples with input signatures performs this task. For this purpose scientist follows two methods for feature extraction that confirms the performance of the verification system, which are: Grid Feature Comparison and Texture Feature Comparison.

Online signature verification is one of the most applicable authentication methods in e-business in affiliation with online banking transactions, electronic payments, access control and so on. Therefore, currently it is a very active research area (Rigoll G, Kosmala A, 1998) initiated the problem of variation in length and height that can be solved by balancing signatures through several HMM-based techniques (Rhee t. H, 2001) presented skilled forgeries that can be rejected through discriminative features by using segment-to-segment compression (Wessels T, 2000) stated hybrid system that reduces the clash between vast numbers of signatures and constructs an intensity verification system.

During the last two decades, several offline signature verification systems have been proposed, (Lecce V. D, 1999) took more signatures of the writer through which inconsistency can be removed validated and forged signature can be decided with multiple instances of test signature presented a new formula of Visual perception for signature representation that determines the shape descriptor and pertaining features in signature verification (Edson J.R.Justino, 2001)(Srihari S.N, 2004) initiated writer independent model and determined the temporal information of writer, through which identification of signatures become easier.

Recently, many research efforts have been put into the field of feature extraction, including feature construction, space dimensionality reduction, and spares representation and feature selection,(Edson J.R. Justino,2001) suggested, skilled forgeries can be discerned using pseudo dynamic feature extraction techniques of handwriting motion,(Dimauro G, 2002) initiates that performance of the signature verification improves by assigning weight to the strength of each part of the signature (Edson J.R, 2000) proposed robustness of one single static feature or the density of pixels in an off-line signature verification pertaining to cross-validation process, (Jalal M, 2005) demonstrated, by using feature analyzer; noises can be removed through extracting invariable information in signature verification than

system can be impressive and efficient, (Huang K, Yan H, 2000). put forth, the fractal transformation based signature verification technique effectively verifies the global signature shape.

A. Analysis of Document Image.

Signature verification contains two main areas: off-line signature verification, where signature samples are scanned into image representation and on-line signature verification, where signature samples are collected from a digitizing tablet which is capable of recording pen movements during the writing. A cheque document normally comprises machine printed and written texts as well as graphic images. In logical structure, each cheque is composed of the following logical objects:

(1) Name of Account Holder.
(2) Name of Financial Institution.
(3) Date of issue.
(4) Whom to pay.
(5) Payment amount in Numeric.
(6) Payment amount in Words.
(7) Authored signature.
(8) Account Number in OCR format.
(9) Cheque Number in printed form.
(10) Financial institution logo.
(11) Branch code as per definition of State Bank or country mother bank.

2. METHODOLOGY.

Authentications and validation is the key of success of any Algorithm. This paper presents the application and acceptance of conventional cheques in online e-banks. Financial institutions prints colored or textures back ground cheques usually to create the uniqueness and beauty in their cheques but if we deposit those cheques in any scanning machine in an electronic bank so it validate eleven features of cheques first and then it will proceed towards the signature authentication. In this regard we proposed and test an algorithm that will eliminate the background text and provide a binary image for verification or validation.

A conventional cheque contains at least eleven special mark of identification but the strongest mark of identification is the authorized person signature. In above algorithm we eliminate the background using special filters and then convert those signatures into readable binary image and those binary images is ready for authenticity.

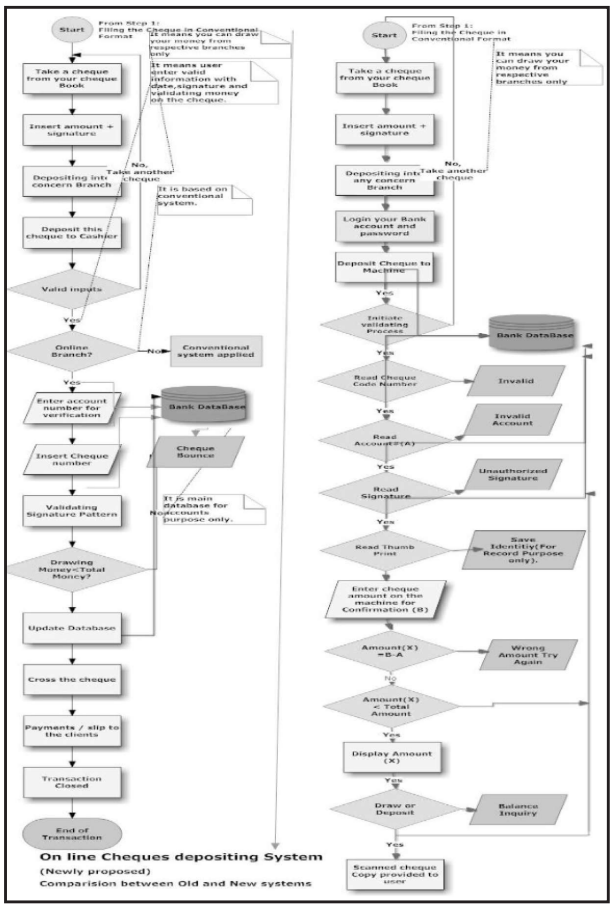
For the signature verification process, the first step is to extract the signature from a colored paper. The development of an effective signature extraction system is a difficult task, especially when the paper contains a complicated and a colorful background. Comparatively, there is very limited published work on the processing of signature verification on colored paper, it is noted that such kind of research is already made beforehand such as: (Liu K, 1996) approached, to extract item of the cheques even if there are complex colorful background and pictures on cheques. (Djeziri S, 1997) proposed to subtract between a virgin model and a filled specimen of a cheque that clearly extracts the items of cheques.

A.Problems in signature verification due to colored background

Grayscale values in digital imaging are represented as a non-negative integer value, where zero represents black and some positive values, Typically 255, represents the maximum white. The grayscale intensity is stored as an 8-bit integer giving 256 possible different shades of gray from black to white. A vector in the three-dimensional color space defines color. The length of the vector gives the intensity and the actual color by the two angles

describing the orientation of the vector in the color space. The amount of red, green, and blue are needed to form any color value.

Figure 1.
Comparison.



A grayscale image is the one in which colors are the shades of gray. The reason for differentiating such images from other sort of colored images is that less information needs to be provided for each pixel. In fact a gray color is the one in which all red, green and blue components have equal intensity in RGB space, so it is the only necessity to specify a single intensity value for each pixel, as opposed to the three intensities needed to specify each pixel in a colored image.

When the signature having a white background is compared with the signature having a colored background then the result is not accurate to automate the signature verification process, because white paper has low intensity, while the colored paper has high intensity rate. The gray scale signature image is digitally stored into a form of two dimensional vector matrixes whereas the colored signature image is stored into a form of three dimensional vector matrixes. It is always needed to perform different kinds of arithmetic operations on both types of signature images for the comparison and verification process. Due to different nature of vector matrixes, this is impossible.

3.THE PROPOSED SYSTEM.

Electronic banking transactions are mainly proposed in this paper. Figure 1 explains this system in detail. The proposed system initiate by proper login of the consumer then he deposits its cheque to the machine after that validating process initiated it reads cheque code then its amount if its valid it proceeds else it generate invalid messages. Steps of this system are as follows step 1 Predefined printed cheque book is proposed by the system which means separate area is allocated for signatures only. Step 2 Insert amount in predefined row plus authorized signature. Step3 Deposit your cheque in respective branch.Step4Login with your name and enter your password.Step5 Deposit your cheque in cheque receiving machines or ATM machines. Step6 Validating process initiates. Step7 Read cheque number or code number Step8 Read account number Step9Read signature of authorized person and cheque with database weather this signature is valid or invalid Step10 Read thumb print and cheque its authenticity with database. Step 11 Enter your cheque amount and verify it by subtracting it with original amount, weather this amount is valid for draw or not. Step 12-update database with new transaction. Step 13 Display the remaining amount. Step 14 prints out the copy of deposited cheque. All the extracted features are used by a k-nearest neighbor classifier that compares the extracted feature to a number of prototypes that are coming from signer with known identity. The main step of proposed SVCP system is to recognize or reject the signature. For each signature we queried the SVCP system 100 times, one time for each signer. The training database contained 600 signature images and that made 100 X 600 = 60,000 testing cases. The signature is recognized if systems response was positive and shows that signature belonged to the correct signer. The signature is rejected if systems response was negative and shows that signature belongs to a false signer. Reference database play a key role in this system additionally if we improve the searching capability of the database we got better results.

A. Data Collection

The signatures were collected using either black or blue ink (no pen brands were taken into consideration), predefined box in the cheque was used for recognition. A scanner subsequently digitized the signature on the cheque, with a 300-dpi resolution in 256 grey levels. Afterwards the images were cut and pasted in the rectangular areas of 3x10 cm and were each saved separately in files.

B. Signature Extraction

Signature plays a vital role in the whole system that's why our paper is more focused towards recognition. The problem of processing signature having colored background can be divided in two main branches: the extraction and the verification of the signature. Currently, two strategies are used for extracting the signature: thresholding techniques and image subtraction. Different thresholding techniques have been suggested to isolate the signature from the colored paper (Dimauro G, 1997), (Santos J. E. B., 1997), (Liu K, 1997) . It is seen in practice then these techniques have shown good results and are useful in those applications where the paper has only simple background colors. However, in real applications, property documents, bank cheques etc may contain a variety of complex colorful backgrounds. If these techniques were applied in which the background pattern has complex colors, it would be very difficult to find a threshold value to segment the background from the signature. On the other hand, the techniques based on image subtraction have shown more robustness to segment the signature from paper that has colorful pictures on the background pattern (Yoshimura M, 1994). From the practical point of view this approach has shown good results in terms of quality of the final images, but in terms of computational costs, it may not be feasible. The way of signature extraction that is captured in this research is the selection of threshold because it is observed; this method clearly extracts the signature especially where signature image characteristics can change over a broad range of intensity distribution.

The verification is based on the assumption that the similarities of an individual writer tend to cluster, while those of a population of writers are more widely scattered. The threshold value is determined for verification based on only the statistical property of genuine cluster.

Let $\{S_j$ (j=1,2,…….,n)}be the obtained similarities between the registered signature and its *n* genuine signatures for training. Moreover, let μ and s be the mean value and the standard deviation of $\{ S_j \}$ respectively. The threshold value *T* of the genuine signatures for each registered one is defined as the following equation.

$$T = \mu - a\sigma$$

Where *a* is certain value (called *threshold coefficient*). For unknown examined signature, if the similarity $S^{(u)}$ of an examined signature is larger than *T*, then the signature is classified as a genuine otherwise *forged*. Thresholding is a quick way to convert grayscale images into black-and-white images.

Figure 5.
Example of extracted signature from colored paper

1.Pre-processing

The preprocessing stage is divided into four different parts: size normalization, noise reduction, image thinning and skeletonization.

2.Size Normalization.

A signer may use an arbitrary baseline when writing the signature. The signature position information is normalized by calculating an angle θ of corrective rotation about the centroid of the (x,y) such that rotating the signature by θ brings it back to a uniform baseline. Calculate θ by maximizing the deviation of the data, one direction, e.g. the x direction. The image size is adjusted so that the width reaches a default value while the height-to-width ratio remains unchanged. The size normalization in offline signature verification is important because it establishes a common ground for image comparison. A low spatial resolution makes all signatures look like the same while a very high spatial resolution may highlight the variability (Wessels T, 2000).

3.Noise Reduction.

Dirt on camera or scanner's lens, imperfections in the scanner lighting, etc introduces noises in the scanned signature images. A filtering function is used for the removal of the noises in the image. Filtering function works like a majority function that replaces each pixel by its majority function.

A noise reduction filter is applied to the binary scanned image. The goal is to eliminate

single white pixels on black background and single black pixels on white background. In order to accomplish this, a mask of 3 x 3 is applied to the image with a simple decision rule: if the number of the 8-neighbors of a pixel that have the same color with the central pixel is less than two then reverse the color of the central pixel (Jalal M, 2005).

4. Thinning.

Thinning is a morphological operation that is used to remove selected foreground pixels from binary image, somewhat like opening. It can be used for several applications, but is particularly useful for skeletonization. In this mode it is commonly used to tide up the output of edge detectors by reducing all lines to single pixel thickness. Thinning is normally only applied to binary image, and produces another binary image as output.

5. Skeletonization.

A simplified version of the skeletonization technique described in (Lam L, 1991) is used. The simplified algorithm used here consists of the following three steps: **Step 1:** mark all the points of the signature that are candidates for removing (black pixels that have at least one white 8-neighbor and at least two black 8-neighbors pixels). **Step 2:** Examine one by one all of them, following the contour lines of the signature image, and remove these as their removal will not cause a break in the resulting pattern. **Step 3:** If at least one point was deleted go again to Step 1 and repeat the process once more. Skeletonization makes the extracted features invariant to image characteristics like the qualities of the pen and the paper the signer used and the digitizing method and quality.

6.The Feature Extraction Phase.

In texture feature group to be formed, a coarser segmentation scheme is adopted. The signature image is segmented in pixels, while, for each area, information about the transition of black and white pixels in the four different directions is used.

6.1Recognition using Texture Features.

To extract the texture feature group, the co-occurrence matrices of the signature image are used (Baltzakis H, 2001). In a gray-level image, the co-occurrence matrix Pd [i.j] is defined by first specifying a displacement vector d=(dx,dy) and counting all pairs of pixels separated by d and having gray level values i and j. In our case, the signature image is binary and therefore the co-occurrence matrix is a 2x2 matrix describing the transition of black and white pixels. Therefore, the co-occurrence matrix P_d [i.j] is defined as

$$P_d[i,j]= \begin{bmatrix} P\ 00 & P\ 01 \\ P\ 10 & P\ 11 \end{bmatrix}$$

Where p00 is the number of times that two white pixels occurs, separated by d. p_{01} is the number of times that a combination of a white and a black pixel occurs, separated by d. p_{10} is the same as p_{01}. p_{11} is the number of times that two black pixels occur, separated by d. The image is divided into six rectangular segments (3x2). For each region the P(1,0) , P(1,1) , P(0,1) and P (-1,1) matrices are calculated and the p_{01} and p_{11} elements of these matrices are used as texture features of the signature. The above procedure sums up to 48 features (six segments x four matrices x two elements).

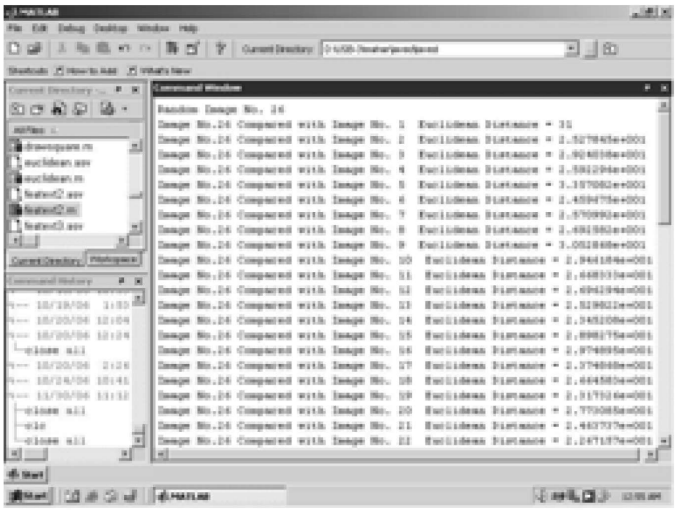
6.2The Result Classification Phase.

There are several ways to work out the distance between two points in multidimensional space. Which one to use is often a subject to debate? The most commonly used is the Euclidian distance measure (Santos C, 2004). It can be considered the shortest distance between two points.

$$d_e = \sqrt{\sum_{i-1}^{p} (xi - yi)^2}$$

All the extracted features are used by a *k*-nearest neighbor classifier that compares the extracted feature vector to a number of prototype vectors coming from writers with known identity. The squared Euclidean distance between a test vector and reference vector was measured (Santos J. E. B, 1997). For all experiments, a Euclidean-distance based *K*-Nearest Neighbor (*K*-NN) classifier is used.

Figure 6.
Sample output of distance measurement from SVCP software



This classifier determines the all nearest neighbors to each input feature vector and opts for the class that is most often represented. In case of a tie, the class with the smallest sum of distances is chosen. The number of nearest neighbors has been empirically determined. The sample output of distance measurement from SVCP software is shown in Figure 7.

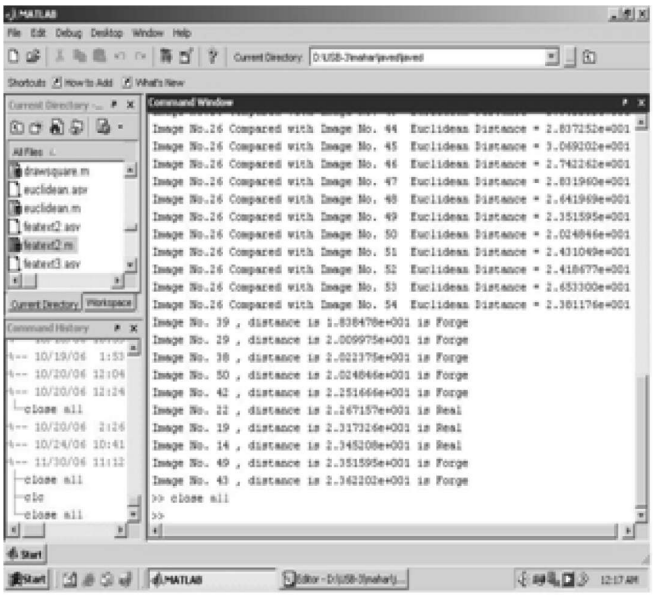
4. TESTING

To verify and test the signature images through designed software, it is executed 100 times. This training database contains 600 signature images which have developed 100x600=60,000 testing cases.

For verification process, one signature is taken from testing samples randomly, for compression with all training samples' signatures, if SVCP system finds it approximately 70% genuine & 30% forge then it could be considered genuine. If it is found 70% forge & 30% genuine then it could be considered forge. The sample output of comparisons from SVCP software is shown in Figure 8.

In this regards the proposed system did not required verification of signer with out checking public key of the signer (N.R.sunitha, 2007). But it depends upon condition or based on system requirement. Another method can be used in this regard to gain accuracy of writing recognition based on segmentation and presented by L. S. Oliveira .He introduced a verifier module in order to detect segmentation effects such us over-segmentation and under-segmentation (L. S. Oliveira, 2001).

Figure 7.
Sample output of signature comparison from SVCP software



Our proposed model worked with KNN and all signature images have been defined and evaluated using a KNN classifier. The performance of the verification system is reported in terms of type I (false rejection of genuine signatures) and Type II (false acceptance of forge signature) error rates evaluated for the 20 persons. Table 1 shows the error rate obtained using each feature separately.

Table 1.
Type 1 and Type II Error Rate Features

Features used	Type I	Type II
Texture Feature	3.73%	2.83%

5. CONCLUSION

Signature verification descry that it buttress automation in BTS. An automated signature verification process could be significantly beneficial & efficient for the different application areas like banking system and revenue departments particularly for signature forgeries, which can give a large monetary loss each year. In this paper a powerful mechanism has been proposed in which a complete automatic signature verification system has been designed. This system is capable of verifying the images of handwritten signature, which are captured from the colored paper. The SVCP system has been discussed and presented for the above purposes. This paper presents an algorithm and its application based on texture recognition using K-NN Classifier. Its performance and feature extraction methods are also developed in *K*-NN classifier. The test accuracy achieved through texture feature method is 96.9%. The performance of the verification system is reported in terms of type I & type II. It initiates from conventional cheque deposit to its features extraction and generate a unique code. That code helps system to record this transaction and updated database. It is zeal system and famous for automation.

6. REFERENCES

N.R.SUNITHA, B.B.AMBERKER, PRASHANT KOULGI, SIDDHARTH P, (2007). "Secure e-Cheque Clearance between Financial Institutions,"9th IEEE International Conference on E-Commerce Technology and The 4th IEEE International Conference on Enterprise Computing, E-Commerce and E-Services (CEC-EEE 2007) 2007.

L. S. OLIVEIRA, SABOURIN, BORTOLOZZI AND C. Y. SUEN (2001). " A Modular System to Recognize Numerical Amounts on Brazilian Bank Cheques" 2001 IEEE.

EDSON J.R. JUSTINO, BORTOLOZZI F, SABOURIN R, (2001). "Off-Line Signature Verification Using HMM for Random, Simple and Skilled Forgeries", Sixth International Conference on Document Analysis and Recognition, (2001).pp. 1031.

RIGOLL G, KOSMALA A, (1998). "A Systematic Comparison Between On-Line and Off-Line Methods for Signature Verification with HMM", 14th International Conference on Pattern Recognition-Vol II, 1755-1757, 1998.

RHEE T. H, CHO S. J, KIM J. H, (2001). "On-Line Signature Verification Using Model Guided Segmentation and Discriminative Feature Selection for Skilled Forgeries", Proc. of the 6th International Conference on Document Analysis and Recognition, 0 7695-1263-1, 2001.

LECCE V. D, DIMAURO G, GUERRIERO A, IMPEDOVO S, PIRLO G, (1999). "Selection of Reference Signatures for Automatic Signature Verification", 5th International Conference on Document Analysis and Recognition, pp.597, 1999.

WESSELS T, OMLIN C.W, "A HYBRID SYSTEM FOR SIGNATURE VERIFICATION", (2000). Proc. of the IEEE-INNS-ENNS International Joint Conference on Neural networks, 0-7695-0619-4,2000.

DIMAURO G, IMPEDOVO SINDHI, PIRLO G, (2002). "Analysis of Stability in Hand-Written Dynamic Signatures", Proc. of the 8th Int. Workshop on Frontiers in Handwritten Recognition, 0-7695-1692-0,2002.

DIMAURO G, IMPEDOVO SINDHI, PIRLO G, SALZO A, (1997). "Automatic Bank Cheque Processing: A New Engineering System", International. Journal of Pattern Recognition and Artificial Intelligence II, pp. 467-504,1997.

SANTOS J. E. B., BORTOLOZZI F., SABOURIN R., (1997). "Simple Methodology to Bank Cheque Segmentation", First Brazilian Symposium on Document Image Analysis, pp. 334-343,1997.

Liu K, Suen C. Y, Cheriet M., Said, C. Nadal J. N., Tang Y.Y., (1997). "Automatic Extraction of Baselines and Data from Cheque Images". International Journal of Pattern Recognition and Artificial Intelligence II, pp. 675-697,1997.

YOSHIMURA M, YOSHIMURA I, (1994). "Off-Line Verification of Japanese Signatures After Elimination of Background Pattern", International Journal of Pattern Recognition and Artificial Intelligence, 8, 693-708,1994.

LAM L., SUEN C.Y, (1991). "A Dynamic Shape Preserving Thinning Algorithm" Signal Processing 22, pp. 199-208,1991.

BALTZAKIS H, PAPAMARKOS N, (2001). "A new Signature Verification Technique Based on a Two-stage Neural Network Classifier", Engineering Applications of Artificial Intelligence, pp.95-103, 2001.

SANTOS C, EDSON J.R. JUSTINO, BORTOLOZZI F, SABOURIN R, (2004) " An Off-Line Signature Verification Method based on the Questioned Document Expert's Approach and a Neural Network Classifier", Proc. of the 9th Int. Workshop on Frontiers in Handwriting Recognition, 0-7695-2187-8,2004.

SRIHARI S.N, AIHUA X, KALERA M.K, (2004)."Learning Strategies and Classification Methods for Off-Line Signature Verification", 9th International Workshop on Frontiers in Handwriting Recognition, pp.161-166, 2004.

EDSON J.R.JUSTINO, BORTOLOZZI F, SABOURIN R, (2001). "Off-Line Signature Verification Using HMM for Random, Simple and Skilled Forgeries", Sixth International Conference on Document Analysis and Recognition, pp. 1031, 2001.

LIU K, SUEN C.Y, NADAL C, (1996). "Automatic Extraction of Items from Cheques Images for payment Recognition", International Conference on Pattern recognition,

798-802, 1996.
DJEZIRI S, NOUBOUND F, PLAMONDON R, (1997). "Extraction of Items From Checks", 4th International Conference on Document Analysis and Recognition, pp.749, 1997.
EDSON J.R, JUSTINO, A.E, YACOUBI, BORTOLOZZI F, SABOURIN R, (2000). "An Off-Line Signature Verification System Using Hidden Narkov Model and Cross Validation", Proc. of the 8th Brazilian Symposium on Computer Graphics and Image
JALAL M, CHOWDHURY M. R, (2005). "On the Power of Feature Analyzer for Signature Verification", Proc. of the Digital Imaging Computing: Techniques and Applications, 0-7695-2467-2,2005.
HUANG K, YAN H, (2000). "Signature Verification using Fractal Transformation", Proc. of the 15th International Conference on Pattern Recognition, 1051-4651,2000.