USING MULTI ADAPTIVE NEURO FUZZY INFERENCE SYSTEMS TO IDENTIFY FRAUD BANK CHECKS

Ying Bai[1] and Dali Wang[2]
[1]*Johnson C. Smith University*
100 Beatties Ford Rd., Charlotte NC 28216, USA
[2]*Christopher Newport University*
One Avenue Arts, Newport News, VA 23606, USA

ABSTRACT

This research is to use multiple Adaptive Neuro Fuzzy Inference Systems (ANFIS) to design and build an image processing algorithm to quickly and easily detect a fraud or altered bank check in real time. With the help of MATLAB Fuzzy Logic and Image Processing Toolboxes, this algorithm can be used to quickly detect most fraud or altered bank checks via an ATM scanner when a fraud or altered check is deposited to an ATM. The testing and validation processes have been performed to confirm the effectiveness and correctness of this detecting algorithm. The current correct detecting rate is about 80% for checks deposited via ATMs.

KEYWORDS

Fraud Bank Checks Detections, Altered Check Inspections, Multi Adaptive Neuro Fuzzy Inference Systems, Image Signal Processing and Detections

1. INTRODUCTION

Today check fraud is incredibly widespread at any corner in nationwide and worldwide. In fact, due to so many various types of check frauds, no one can have the exact numbers on how many people are affected and how much money has been lost each year.

Check frauds are also one of the largest challenges and lost to all financial and commercial related businesses and institutions today. With the fast developments of modern computer and micro-controller technology, it becomes easier for criminals, either in personal or in organized groups, to alter or modify checks in such a way as to deceive innocent victims expecting value in exchange for their money.

A great amount of check fraud is partly because of counterfeiting via advanced desktop printing and copying technologies to generate or duplicate some actual financial documents, or chemical fluid alterations, which consists of removing part or all of the information and modifying it to the benefit of the criminals. Most victims include financial related institutions and commercial related businesses that accept and issue personal or business checks, as well as the consumers. Generally, these crimes start with the theft of some financial documents or hand-writing customer bank checks. It can be perpetrated as easily as someone stealing a personal or a business blank check from victim's home or vehicle during a burglary, searching for a voided or old check in the garbage tanks, or stealing a check the victim has mailed to pay a bill from his/her home or office mailboxes.

Some typical fraud bank checks can be categorized into the following two categories based on their processes:

- Counterfeiting can be either wholly fabricating a check --using modern office desktop printing devices consisting of a personal computer (PC), scanner, professional software and high-level laser printer - or simply duplicating a bank check with advanced laser or color photocopiers.

- Alterations primarily refer to using chemical materials and solvents such as acetone, brake fluid, correction fluid to remove, or cover and modify the original handwriting and information on the check. When performed on specific locations on the check such as the payee's name or the amount area, it is called spot-alteration; when an attempt to erase information from the entire check is made, it is called check-washing.

It has been estimated that the annual losses could be around in the billions of dollars due to check fraud and this amount continues to grow steadily as criminals continue to seek ways to earn a living by defrauding others (Mary 2015). For the consumer, the amount of inconvenience and anxiety caused by resolving problems with the account, local merchants, as well as possible repercussions with credit bureaus can be considerable.

According to a global fraud study reported by the Association of Certified Fraud Examiners (ACFE) in 2022 (ACFE, 2022), a typical organization could lose 5% of its revenue every year due to fraud. The total loss caused by the cases in that study exceeded $3.6 billion, with an average loss per case of $1.7 million. That study was performed based on 133 countries around the world in 2022.

Although the check fraud case number is continuously increased around the world day by day, few related technologies and tools have been developed and built to protect victims from losing their funds. SQN Banking Systems reported their SENTRY Inspect™ software package called Check Image Analysis, which is used to detect fraud checks via an image processing tool (SQN 2014). SmartSearch reported their Anti-Money Laundering (AML) Check Monitoring and Alerts package to monitor and inspect the truthfulness of personal and business checks (SmartSearch, 2020). Kofax built and developed a FraudOne® fraud check image detection platform used to help customers to detect fraud checks in real time (KoFax, 2023). OrboGraph reported their Anywhere Fraud image analysis tool to perform check image detection for possible fraud checks (OrboGraph, 2022). ToolCASE released its Informant system that is an AI-Based solution for financial services industries (ToolCase, 2022). Parascript reported a machine learning software used to help commercial and retail banking organizations to combat fraud and support compliance such as Know Your Customer (KYC) and AML initiatives (Parascript, 2022). Experfy reported a fraud & risk detection system used to detect possible check tampering related issues (Experfy, 2022). CSI released fraud check detection software used to scan for check fraud and identify counterfeit, altered and unauthorized checks (CSI, 2022).

In addition to software packages and tools developed by various financial companies above, some researches and studies related to detect fraud checks are also reported in recent years. Lydia M. Rose, 2022 provided a review study for detecting methods used for inspecting the fraud bank checks and money orders with machine learning. Ayushi Maurya and Arun Kumar, 2022 reported a method to detect fraud credit card using machine learning technique. Badis Hammi, Sherali Zeadally and et al, 2022 built an algorithm to detect and prevent fake check scams by using a Blockchain-Based Solution.

Pradheepan Raghavan and Neamat El Gayar, 2019 reported a general way to perform the fraud detection using machine learning and deep learning. Saheb Chhabra et al., 2017 reported a method used to detect fraudulent bank checks. Abd-ElZaher, 2014 discussed certain inks' affection to physically erased handwriting in fraud checks. Kennard, Barrett and Sederberg, 2012, reported a strategy used to perform signature verification and forgery detection using a 2-D geometric warping approach. Kumar and Gupta, 2016, released a method used to identify and detect the authentication of bank checks. Lampert, Mei and Breuel, 2006, analyzed some popular printing technique classifications for document counterfeit detection. Patil and Takale, 2015, reported a distance matrix method to verify signatures on bank checks. Prakash and Sharma, 2014, built a detection method used to verify signatures on bank checks with computer vision and fuzzy logic offline strategy. Moises Diaz et al., 2019, developed technique to analyze handwritten signatures for most bank checks. Rajendar and Pal, 2014, developed a method to detect manipulated check images using mismatched pixels. Xie et al., 2009, reported a new method to identify the authenticity of banknotes based on texture roughness. S. Tayeb *et al*., 2017, used a convolution neural network (CNN) to analyze pixels from a signature image to recognize abnormalities in bank checks.

Most of studies and researches mentioned above are concentrated on financial data analysis, check security data identifications, check signature authentications and verifications, manipulated check identifications and analysis. However, one of the most important and often-occurred check frauds is the modification or manipulation of the payee's names on bank checks, either business or personal, to steal funds by depositing them into the perpetrators' accounts via ATMs. Compared with all other check frauds, the check alteration on the payee's name area is a major crime and it is more crystal and serious since it

totally steals other party's funds and put them into the perpetrator's pockets and makes financial institutions lose significant funds year by year in recent years. There are so many cases in which only the payee's names were altered but all other areas kept with no change at all in either business or personal checks. It would be rare and weird if all other areas were changed without payee's name altered for a bank check since that kind of crime is very easy to be tracked and captured.

Also most studies and researches listed above involved complicated and overlong algorithms and mathematical derivations, and therefore made the detection system more complicated and time consuming on fraud check detecting and identification processes.

In this study, we developed a multi ANFIS algorithm to quickly detect and identify fraud bank checks in which only the payee's name area is altered with some chemical or correction fluid and a perpetrator's name is rewritten to cover the original payee's name. The detecting correct rate is about 80%.

This study is divided into five sections; after this Introduction part, the detailed fraud check detection types and definitions are given in section 2. An introduction to ANFIS is discussed in section 3. The experimental results are provided in section 4, and the conclusion and future works are given in section 5.

2. THE FRAUD CHECK TYPES AND DEFINITIONS

2.1 Types of Fraud Checks

The major types of fraud checks can be categorized into the following sections:

1) The payment amount alterations or modifications
2) The payee's name alterations and modifications
3) The signature alterations or modifications
4) Both payee's name and payment amount alterations or modifications
5) The entire check making or alterations

Among all of these alterations or modifications, the payee's name alteration or modification is one of the most often-used methods by perpetrators due to its easy and simple in operations, and have been widely implemented by most criminals. The popular way to do this kind of crime is to cover the original payee's name on bank checks by using some chemical or correction fluid, and rewrite the perpetrator's name to replace the original payee's name, and deposit that altered checks to the perpetrator's account via ATMs. The possibility of success for this kind of crime is relatively higher than other fraud checks since any ATM did not have any ability to detect and identify this kind of alteration or modification when this check is scanned via a scanner in an ATM and deposited into a valid checking or saving account.

Some examples of altered checks are shown in Figure 1. Alterations include to replacing the entire original payee's name, or the partial payee's name by covering the original payee's name via correction fluid or a piece of cut-off paper, and rewriting the perpetrator's name on the payee's name areas. Regularly, the first case will be appeared in most alterations since it is not common to have both persons with the same first or the last names, of course, this case is really occurred in some situations.

To detect or identify these kinds of alterations or modifications, the ANFIS combined with MATLAB Image Processing Toolbox is a good tool or a candidate among available software tools. In fact, the core of this kind of image processing involved the image identifications via an ANFIS algorithm.

3. ADAPTIVE NEURO FUZZY INFERENCE SYSTEM (ANFIS)

3.1 The typical structure of an ANFIS

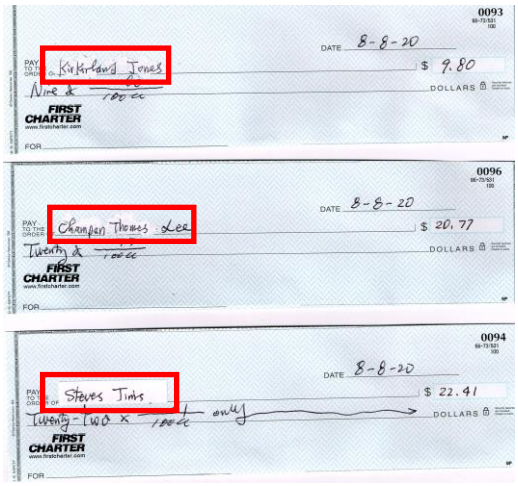


Figure 1. Examples of some altered checks

The so-called ANFIS is exactly a combination of two soft-computing techniques: Artificial Neural Network (ANN) and Fuzzy Inference System (FIS), which was first introduced by Jyh-Shing Roger Jang in 1992. The FIS used a Sugeno fuzzy inference system and its structure is similar to a multilayer feed forward neural network structure, but the difference is that the links between nodes in ANFIS define the signals' flow direction and there are no associated weight factors with the links. It consists of a network of neurons that communicate between the input and hidden layers and the hidden and output layers. Each layer consists of neurons constructed according to the principles of fuzzy control. Figure 2 shows a Sugeno fuzzy model with nine rules along with a corresponding ANFIS architecture. In our case, four rules in the method of "If-Then" for the Sugeno model are considered with x and y as inputs and f as output (Mohammed Imran, Sarah A. Alsuhaibani, 2019). Four rules are defined as below (*pixels in x direction = x, pixels in y direction = y*):

R_1: If x is H and y is L, then $f_{11} = p_{11}x + q_{11}y + c_{11}$

R_2: If x is H and y is H, then $f_{12} = p_{12}x + q_{12}y + c_{12}$

R_3: If x is L and y is L, then $f_{21} = p_{21}x + q_{21}y + c_{21}$

R_4: If x is L and y is H, then $f_{22} = p_{22}x + q_{22}y + c_{22}$

where H and L means reflection rates on the paper checks. The detection key for true and fake checks is based on the reflection rate on the bank checks. The checks covered with any correction fluid have different reflection intensity compared with the normal checks.

The input layer includes a check image taken by an ATM scanner or a camera, which is to be identified and detected. That image can be considered as a 2D matrix with different intensities. The first layer is the fuzzification layer to get desired membership functions in both x and y direction for the input image. The layers 2 and 3 are the fuzzy inference process combined with our rules. The fourth layer is the defuzzification layer to prepare to get the final or real outputs. Combined with layer 5, the actual output can be obtained.

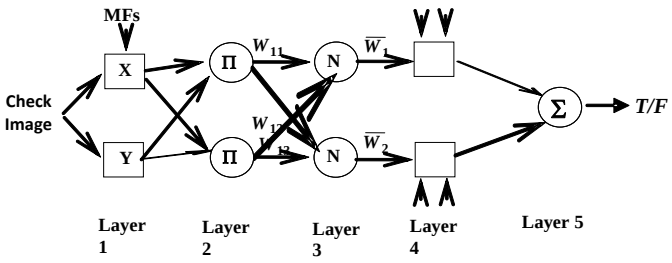


Figure 2. Architecture of the ANFIS for our study

3.2 The Fraud Checks Detection Implementation

Prior to applying the ANFIS algorithm to identify bank checks, some pre-processing jobs are necessary due to the requirements for inputs to the ANFIS. All check images are colored with relatively large size, and maybe inappropriate to be processed. Thus we must do some pre-processing for those images or 2D matrices.

Another important point is the limitation on the input size or the number of inputs to an ANFIS. The running time and the fuzzy rule numbers would be significantly increased if the number of the input variables is equal or more than to ten. In some worst cases, the ANFIS even cannot generate the outputs corresponding to the inputs. In order to solve those issues, we need to do some necessary preprocessing jobs for our input images. These pre-processing jobs include:

1) Change the colored images to the grayscale images since we do not need any color information for this detection or identification process.
2) Reduce the size of each detected check image and only concentrate on the payee's name area, as shown in Figure 1. In this way, the detecting time can be greatly shorter and the identification speed can be significantly faster.
3) Convert each image or each 2D matrix to a 1D array due to the input requirement of the ANFIS.
4) Configure or divide each 1D input image array (1 × N) to M pieces of 1 × (L – 1) array, and set the L column as the output value (Boolean value) with 1 as true and 0 as false. In this way, if the number of input images is K, all those input images can be made as M group of K × L sub-matrix. Each sub-matrix is a K × L matrix, which will be used as a training matrix to be applied as the input to an ANFIS later to train it.

As shown in Figure 1, for three different types of checks, the size of this area is identical. In fact, the actual size of this rectangular area should be finally determined based on the real inspection process. Regularly, this size should be big enough to cover the monitoring area as much as possible. However, the detecting algorithm would be too time-consuming with larger size of selected area if this size is too big. Therefore a trade-off should be taken between the large size of detecting area and quick detecting speed.

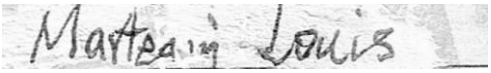
Figure 3 shows some example rectangular area samples for payee's name blocks on detected checks for both true and false check images. The detecting principle is based on the following facts.

It can be seen from both true (Figure 3a and c) and false check (Figure 3b and d) images, the refraction rate and roughness of the background for both checks are different. The reason for that is due to the alterations or modifications for the background on the altered checks, and these differences can be mapped to the intensities in the backgrounds on inspected checks.

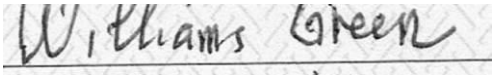
1) By implementing the ANFIS algorithms on these detected checks, these differences can be effectively distinguished and identified.

2) By comparing these differences on detected intensities, the altered checks can be easily detected and identified by applying this ANFIS algorithm.

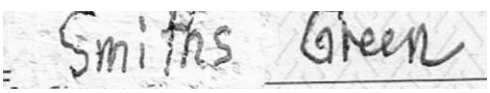
(a)



(b)



(c)



(d)

Figure 3. Testing samples for true and false checks

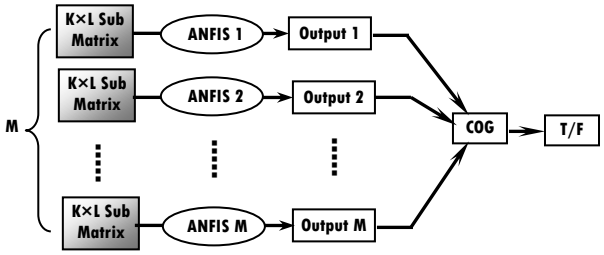


Figure 4. The structure of the multi ANFIS algorithm

One point to be noted is for the true (Figure 3c) and altered or false (Figure 3d) checks, the false check is only partially altered by modifying the first name without touching the last name. This is a coincidental case in which the perpetrator's last name is identical with that of the victim.

In order to effectively and accurately detect any altered or modified checks, an algorithm made by multi ANFIS with MATLAB Fuzzy Logic Toolbox is adopted (Benyamin Khoshnevisan, 2014). The inputs to this algorithm are a set of testing check images in grayscale format, and the outputs (**Y**) are a Boolean value, true for normal check and false for a fake check.

This detection algorithm must be trained first with a set of input arrays or input images represented by M group of K × L sub-matrix. Each row (1 × N) represented one image, which can be considered as an input row, and it can be decomposed into M pieces of 1 × L array and each last column (L – 1) is the output represented by a Boolean value, either a normal, true (1) or a fake (0) check.

The output values for all ANFIS algorithms can be fed into a Center of Gravity (COG) unit to derive the final Boolean output. The structure of this multi ANFIS algorithm is shown in Figure 4.

Determining or selecting an appropriate rectangular area for the payee's name block on the detected check needs some testing and checking processes to get a so-called optimal size for this area to make sure that a good trade-off between a big detecting size and a quick detecting speed can be achieved.

After the ANFIS algorithm has been trained and tested, it can be implemented to identify and detect real bank checks. A graphic user interface (GUI) maybe built to allow users to make different selections to do the detection to get real-time detection results.

4. DETECTING AND EXPERIMENTAL STUDY RESULTS

Due to difficulty to find a data set, in which both sufficient and good quality bank checks were involved, we collected forty (40) real checks coming from five (5) different US banks, including Bank of America, First Charter, ADVANTA Bank Corp., Ally Bank and Fifth Third Bank, and use them as samples to be tested and detected by this detecting system. These checks have different sizes, such as standard personal and business checks with a width × height of 6 × 2-3/4 inches, 7-1/2 × 3 inches and 8-1/4 × 3 inches, and different styles with various backgrounds (plain, color, palm trees, snow mountains and oaks tree).

All of these checks are transferred to 300 dpi color photos or images by using scanner and conversion software with their original sizes and styles, and stored in computers.

Figure 5 shows a sample testing result for this ANFIS algorithm. The training RMSE is 0.00094 and the checking RMSE is 0.528.

A GUI is developed with the MATLAB GUIDE tool, and the ANFIS algorithm built with MATLAB Fuzzy System Toolbox will be called by this GUI to perform related detecting and inspecting jobs when the detecting system works. Figure 6 shows the working status of this fraud check detecting system.

As the detecting system starts, a tested check should be selected from the ListBox, and the detecting process starts as the **Start** button is clicked. The testing result should be displayed with a textbox and the detected check image is also displayed, as shown in Figure 6.

With a total of 40 checks, 25 of them are used for the training and checking purpose and the other 15 are used to detecting purpose. The detecting results are: 3 of them are incorrect but 12 are correct, with a correct detection rate as 80%.

Figure 5. A sample testing results

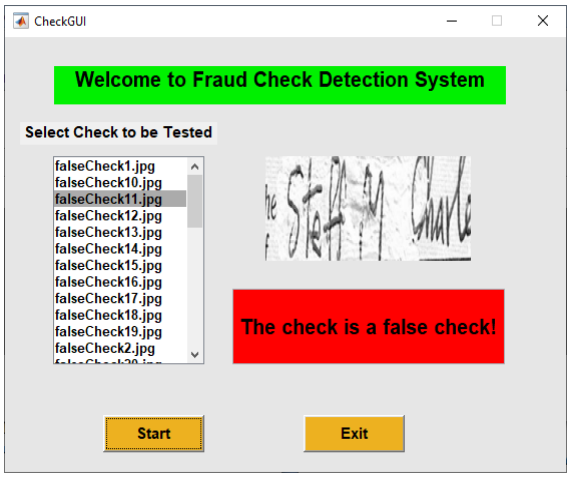


Figure 6. The running status of the fraud check detecting system

5. CONCLUSION AND FUTURE WORKS

With the help of an algorithm made by multi ANFIS built with MATLAB Fuzzy System and Image Processing Toolboxes, a fraud bank check detection system is developed and built in this study. Some real checks coming from five US banks with different sizes and styles are tested and detected via this detecting system. The current correct detecting rate is 80%.

For better detecting results, a similar system developed by using Deep Learning or Machine Learning techniques are needed, with which a better detecting result can be achieved. The correct detecting rate could be around 98% or better as that system is developed.

REFERENCES

Abd-ElZaher, M., 2014, Different types of inks having certain medicolegal importance: Deciphering faded and physically erased handwriting. Egyptian Journal of Forensic Sciences **4**(2), pp.39–44.

ACFE, https://acfepublic.s3.us-west-2.amazonaws.com/2022 +Report+to+the+Nations.pdf

Ayushi Maurya and Arun Kumar, 2022, “Credit card fraud detection system using machine learning technique”, *2022 IEEE International Conference on Cybernetics and Computational Intelligence* (CyberneticsCom), Malang, Indonesia, June 16-18, pp 500-504.

Badis Hammi, Sherali Zeadally and et al, 2022,” Blockchain-Based Solution for Detecting and Preventing Fake Check Scams”, *IEEE Transactions on Engineering Management*, Volume: 69, Issue: 6, December, pp. 3710 – 3725.

Benyamin Khoshnevisan, ShahinRafiee et al. 2014, “Development of an intelligent system based on ANFIS for predicting wheat grain yield on the basis of energy inputs”, *Information Processing in Agriculture*, Vol 1, Issue 1, pp. 14-22.

Chhabra S., Gupta G., Gupta M., Gupta G., 2017, “Detecting Fraudulent Bank Checks”. Peterson G., Shenoi S. (eds), Advances in Digital Forensics XIII. Digital Forensics. *IFIP Advances in Information and Communication Technology*, Vol 511. Springer, pp. 245-266.

CSI, https://www.csiweb.com/how-we-help/platform-banking/core-bank-processing/fraud-risk-management/

Experfy, https://www.experfy.com/fraud-risk/banking-fraud-management

J. -. R. Jang, 1992. "Self-learning fuzzy controllers based on temporal back propagation," in *IEEE Transactions on Neural Networks*, vol. 3, no. 5, pp. 714-723, doi: 10.1109/72.159060.

Kennard, D., Barrett, W., Sederberg, T., 2012, “Offline signature verification and forgery detection using a 2-D geometric warping approach”. *Proceedings of the Twenty-First International Conference on Pattern Recognition*, pp. 3733–3736.

KoFax, https://www.kofax.com/Products/fraudone/overview

Kumar, R., Gupta, G., 2016, “Forensic authentication of bank checks”. Peterson, G., Shenoi, S. (eds.) Digital Forensics 2016. IFIPAICT, Vol. 484, Springer, pp. 311–322.

Lampert, C., Mei, L., Breuel, T., 2006, “Printing technique classification for document counterfeit detection”. *Proceedings of the International Conference on Computational Intelligence and Security*, Vol. 1, pp. 639–644.

Lydia M. Rose, 2022. https://www.proquest.com/openview/5e7cd136814fe3b4c32ffa3384e6cf8c/1?pq-origsite=gscholar&cbl=18750&diss=y.

Mary, http://www.ckfraud.org/ckfraud.html

Mohammed Imran, Sarah A. Alsuhaibani, 2019, Chapter 7 - A Neuro-Fuzzy Inference Model for Diabetic Retinopathy Classification, Editor(s): D. Jude Hemanth, Deepak Gupta, Valentina Emilia Balas, In Intelligent Data-Centric Systems, Intelligent Data Analysis for Biomedical Applications, Academic Press, Pages 147-172, ISBN 9780128155530.

Moises Diaz, Miguel A. Ferrer, Donato Impedovo, Muhammad Imran Malik, Giuseppe Pirlo, and Réjean Plamondon, 2019, “A Perspective Analysis of Handwritten Signature Technology”. *ACM Comput. Surv*. 51, 6, Article 117, p. 39.

OrboGraph, https://orbograph.com/anywhere-fraud/

Parascript, https://www.parascript.com/products-technology-solutions/fraud-prevention/

Patil, R., Takale, S, 2015, “Signature verification by distance matrix method for bank check process”. *Proceedings of the International Conference on Electrical, Electronics, Signals, Communication and Optimization*, India, pp.1281-1285.

Pradheepan Raghavan and Neamat El Gayar, 2019. “Fraud Detection using Machine Learning and Deep Learning”, 2019, International Conference on Computational Intelligence and Knowledge Economy (ICCIKE), Dubai, United Arab Emirates, pp 334-339.

Prakash, G., Sharma, S., 2014. “Computer vision and fuzzy logic based offline signature verification and forgery detection”. *Proceedings of the IEEE International Conference on Computational Intelligence and Computing Research*, 2014, pp. 1-6, doi: 10.1109/ICCIC.2014.7238363.

Rajendar, M., Pal, R., 2014, “Detection of manipulated check images in a check truncation system using mismatch in pixels”. *Proceedings of the Second International Conference on Business and Information Management*, Durgapur, India, pp. 28–33.

S. Tayeb *et al*., 2017. "Toward data quality analytics in signature verification using a convolutional neural network," *2017 IEEE International Conference on Big Data (Big Data)*, Boston, MA, 2017, pp. 2644-2651, doi: 10.1109/BigData.2017.8258225.

SmartSearch, https://www.smartsearch.com/us/solutions/aml-monitoring-and-alerts

SQN, https://sqnbankingsystems.com/solutions/check-image-analysis/

ToolCase, https://www.toolcase.com/products/informant/index.html

Xie, J., Qin, C., Liu, T., He, Y., Xu, M., 2009, “A new method to identify the authenticity of banknotes based on texture roughness”. *Proceedings of the IEEE International Conference on Robotics and Biomimetics*, Guilin, China, pp. 1268–1271.