FRAUD DETECTION IN CHEQUE TRUNCATION SYSTEM (CTS)

Deebika M[1], Rathna I[2], Vairam Sujitha M[3]

[1]*Information Technology, Thiagarajar college of engineering, (India)*

[2]*Information Technology, Thiagarajar college of engineering, (India)*

[3]*Information Technology, Thiagarajar college of engineering, (India)*

***GUIDED BY** : **Meenakshi Sundaram P**(CTS Manager Cameo Corporates),*

***Uma K.V** (Thiagarajar College of Engineering)*

ABSTRACT

Cheque Truncation System or Image-based clearing system is image based cheque clearing system where the MICR(Magnetic Ink Character Recognition) code of the cheque is captured and it is classified according to bank , branch ,account no(SAN) and then the cheques are cleared accordingly. This is the modern technology introduced by the Reserve Bank Of India(RBI).The traditional method involves many paper works which may not be efficient and they may be not available for future references as they are documented as a hard copy. Thus, modern method is more efficient and accurate than the traditional one. Some of the frauds in CTS are altering the digital image of cheque(watermark),signature and other factors like damaged cheque will also be considered for the rejection of cheque. Many methods are there to detect the forged cheque but they are only done by considering the small factors and are not effectively implemented. Our idea is to mainly compare the scanned cheque with the base image(uv image) of the particular bank and detect the forged cheque in this method we cover the main factor uv image to detect the forged cheque thus this technique may be effective unlike the watermark method , because there will be no accuracy in watermark method. Due to confidentiality issues no bank has implemented any fraud detection method so far despite if a bank has implemented such method then they would only cover the small factor to do so. Thus ,this idea of ours would be a new method and greater improvement to the existing techniques.

Keywords :*Clearing House Interface, MICR code, OCR , text segmentation, UV image, watermark*

1. INTRODUCTION

Cheque Truncation System (CTS) or Image-based Clearing System (ICS)**,** in India, is a project undertaken by the *Reserve Bank of India – RBI*, for faster clearing of cheques. CTS is basically an online image-based cheque clearing system where cheque images are captured at the collecting bank branch and transmitted electronically. Truncation means, stopping the flow of the physical cheques issued by a drawer to the drawee branch. The physical instrument is truncated at some point en-route to the drawee branch and an electronic image of the cheque is sent to the drawee branch along with the relevant information like the MICR fields, date of presentation, presenting banks etc.

The CTS Clearing House Interface (CHI) provides an easy-to-use and standardized connectivity between the capture/drawee bank systems of a Bank to the RBI/NPCI Clearing House (CH). It provides a gateway for conduit of data and images. It provides the required validation to ensure that the data entering the CH is free of

operational errors. RBI/NPCI will provide or facilitate to provide each Bank participating in the clearing process with a license to install the CHI software on a server. Each Bank should be associated with a CHI for communication to the CH.

1.1 FUNCTIONALITY

- ❖ Capture the image of cheque , MICR code(data)
- ❖ Validate , analyze and combine the cheque of the same bank together
- ❖ The entire data will be stored in xml file and according to the validationthe cheque will be processed.
- ❖ It involves inward and outward clearing.

1.2 PROCESS FLOW

The MICR data and the image is captured by the bank. The SAN (Small Account Number) is the number in MICR code it indicates the compressed format of the account number. The captured image is converted to data in xml format and then send to the clearing house. The following is the follow of process:

- ❖ In CTS, the presenting bank (or its branch) captures the data (on the MICR band) and the images of a cheque using their Capture System (comprisingof a scanner, core banking or other application
- ❖ The collecting bank (presenting bank) sends the data and captured images duly signed and encrypted to the central processing location (Clearing House) for onward transmission to the paying bank (destination or drawee bank). For the purpose of participation the presenting and drawee banks are provided with an interface / gateway called the Clearing House Interface (CHI) that enables them to connect and transmit data and images in asecure and safe manner to the Clearing House (CH).
- ❖ The Clearing House processes the data, arrives at the settlement figureand routes the images and requisite data to the drawee banks. This is called the presentation clearing. The drawee banks through their CHIs receive the images and data from the Clearing House for payment processing. The drawee CHIs also generate the return file for unpaid Investments.The Reserve Bank had implemented CTS in the National Capital Region (NCR), New Delhi and Chennai with effect from February 1, 2008 and September 24, 2011. After migration of the entire cheque volume from MICR system to CTS, , the traditional MICR-based cheque processing has been discontinued in these two locations. Based on the advantages realised by the stakeholders andthe experienced gained from the roll-out in these centres, it was decided to operationalise CTS across the country by Jan 1 2013.

Fig 1.1

2. OBJECTIVES

- To detect fraud in cheque truncation system by comparing the ultraviolet image.
- To check and predict other factors that can be used to find the frauds involved in cheque and provide solution for the same (other factorsinclude forged signature, alternate payee names.

3. CHEQUE SPECIFICATIONS

- Cheque in 2010 was introduced with different features by RBI suitable for the electronic cheque clearing system.
- It also has minimum security features on cheque forms like quality of paper, watermark, bank's logo in invisible ink, void pantograph, etc., and standardization of field placements on cheques.

Features of CTS 2010

1. Branch address with IFSC code printed top of the cheque
2. Date in dd/mm/yyyy format with boxes
3. Printers name with CTS-2010 in left side of cheque
4. A pantograph which shows VOID/COPY while taking photocopy of the cheque below the account number
5. New rupee symbol instead of bilingual format
6. "Please sign above" is mentioned on bottom right of the cheque
7. Watermark "CTS INDIA" to be visible cheque is held against any light.
8. Ultra Violet logo of Bank printed at upper left corner of cheque to be visible in UV lamps.

Fig 3.1 Cheque CTS 2010

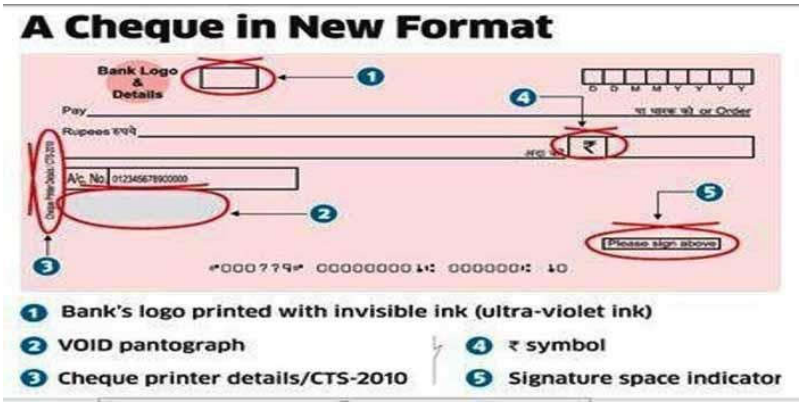


Fig 3.2 Cheque Features CTS 2010

4. LITERATURE SURVEY

Paper 1:

TITLE : Detecting tampered cheque images in cheque truncation system using difference expansion based watermarking.

PUBLISED IN : 2015 IEEE International Advance Computing Conference.

AUTHOR: saranya kota , rajarshipal

DESCRIPTION: This paper proposes a method to detect whether a cheque image has been tampered or not. A difference expansion based watermarking technique is applied for this purpose.

Paper 2:

TITLE : Detection of manipulated cheque images in Cheque Truncation System using mismatch in pixels

PUBLISED IN : 2014 2nd International Conference on Business and Information Management(ICBIM)

AUTHOR: maloth rajender

DESCRIPTION: This paper proposes a method to tackle this type of fraud. It is based on inserting a watermark signal in the image of the cheque.

Paper 3:

TITLE : Secret Image Sharing Based CTS with Cheating Detection

PUBLISED IN : International Journal of Information Processing 2015

AUTHOR: Sreela,Binu

DESCRIPTION: The proposed scheme suggests a method for cheating detection which identify any invalid shares submitted by the customers, using the hashing technique.

Paper 4:

TITLE : A Cheque Watermarking System Using Singular Value Decomposition for Copyright Protection of Cheque Images

PUBLISED IN : Springer, Cham 2015

AUTHOR: Ashok ghatol

DESCRIPTION: In this paper, it is going to discuss, “A Cheque Watermarking System Using Singular Value Decomposition for Copyright Protection of Cheque Images”.

Paper 5:

TITLE : Digital Check Forgery Attacks on Client Check Truncation Systems

PUBLISED IN:National Science Foundation grants 2016

AUTHOR: Rigel Gjomemo

DESCRIPTION: This paper presents a digital check forgery attack on check processing systems used in online banking that results in check fraud.

5. PROBLEM STATEMENT

5.1 PROBLEM DEFINITION

- Cheque Truncation System (CTS) is an image based cheque clearing system. It enables faster clearing of cheques. Indian banks have implemented this technology in selected areas of the country. Meanwhile, several fraud cases have already occurred by taking advantage of inadequate security mechanisms of this system.

- Thus, to enhance the security measure we can detect the forged cheque by comparing the digital image.

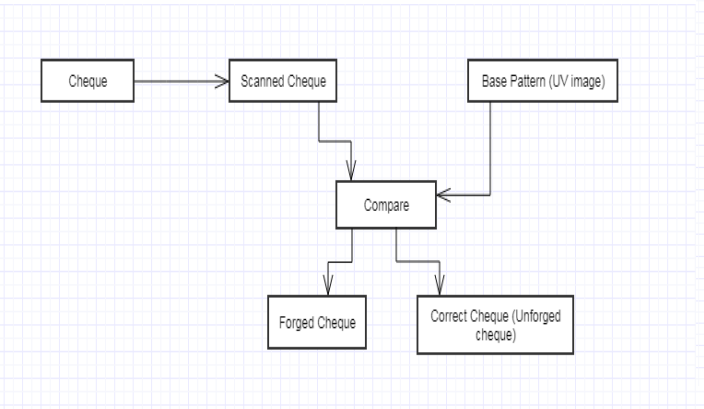


Fig 5.1 Overview Design

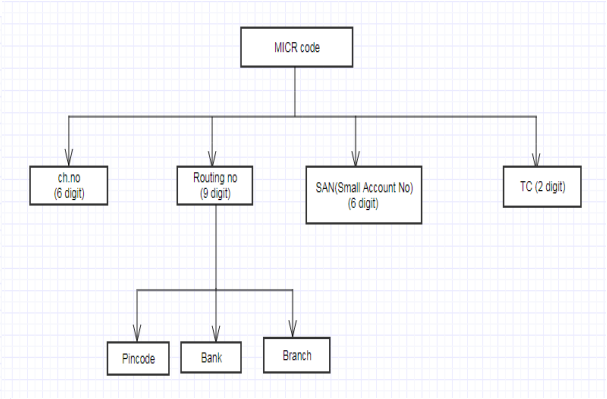


Fig 5.2 MICR Code Design

6. PROPOSED METHODOLOGY

a. Existing Method

The existing method is so simple that it involves the watermark based detection that the watermark of the cheque is brought into contact with the uv(Ultraviolet) light if the watermark of the cheque glows then it is a genuine cheque whereas if it fails then it may be a tampered(damaged) or forged cheque. In case of overwriting , change of signature , altering of MICR code , altering of digital image and signature these factors are also considered as the forged factors.

b. Proposed Method

i.Capturing (capturing of the cheque image)

ii.MICR Code classification

iii.Base pattern of Cheque(uv image)

iv.Comparing the scanned and base pattern

c. Concepts Used

i. Classification

ii. Prediction

iii. Comparing

iv. Image processing : It is done by scaning the check to segment the text using ocr trainer , identifying the bank and branch and compare the uv image of the bank with the scanned cheque and identify the matched pattern and mismatches.

d. Dataset Attributes

i. Name of the MICR centre

ii. City Code

iii. Bank Code

iv. Branch Code

v. Name of the Bank

vi. Name of the Branch

The above attributes are used to compare the micr code of the cheque with the dataset to identify the bank and its branch then the uv of the bank(base pattern) is used for the comparison with scanned cheque.

7. RESULT AND ANALYSIS

PROPOSED METHOD ALGORITHM AND IMPLEMENTATION:

Step 1: Image segmentation and extraction(Extraction of text from the Image.)(OCR Algorithm):

i. Read the image

ii. Show the image

iii. Convert to gray scale

iv. Convert to binary image

v. Remove all object containing fewer than 30 pixels

vi. Show image binary image

vii. Objects extraction

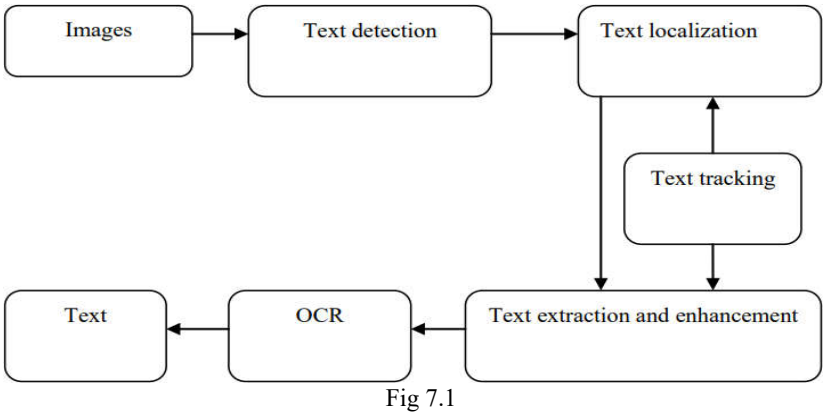


Fig 7.1

Step 2: Identification of the Bank from the dataset:

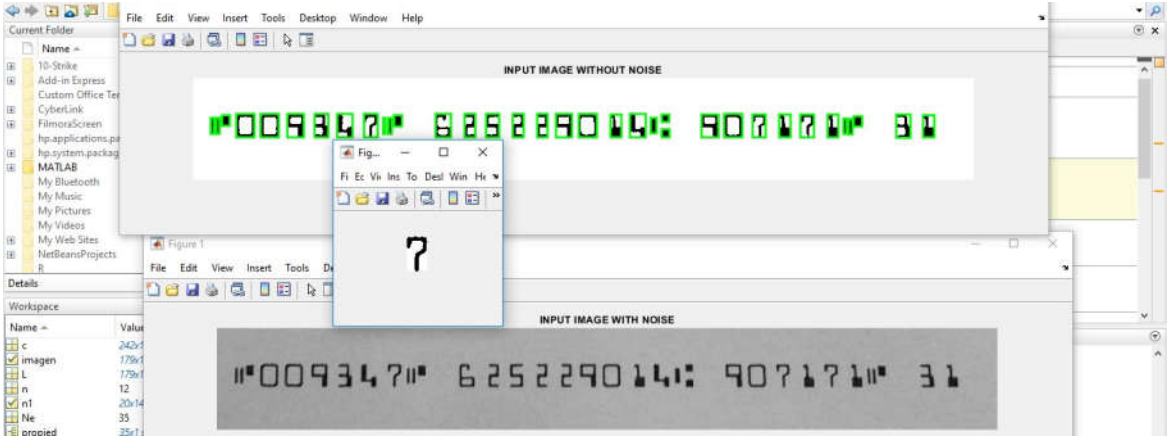
Now the extracted text from the MICR image is compared with the dataset to identify the bank and branch of the cheque so that now we can use the base uv image of the identified bank.

Step 3: Load the Scanned cheque and Base pattern.

Step 4: Comparison of scanned image with base pattern (UV image):

- Read the source (base pattern) image and scanned cheque.
- Then convert the image to a gray scale image for comparison.
- Now Compare the images using corr2(correlation relation).
- It compares and detects the forged cheque.

Fig 7.2 Text Segmentation



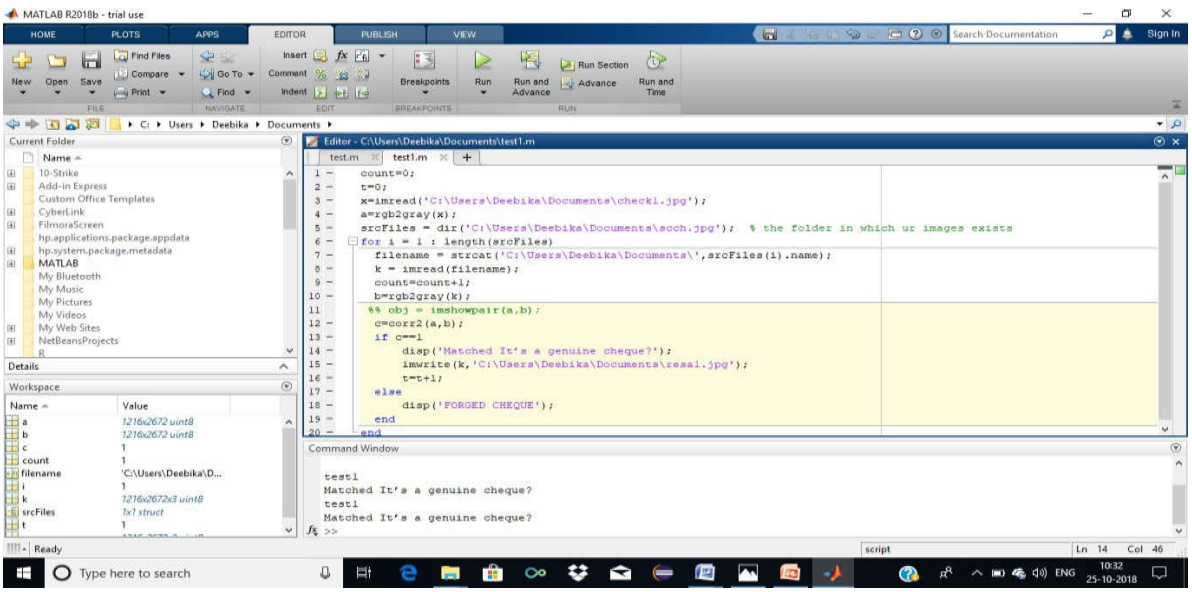
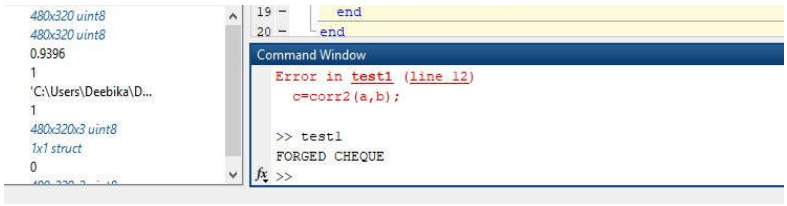


Fig 7.3Detection of genuine and forged cheque



- We have implemented fraud detection in cheque using matlab tool
- We scan the cheque using the ocr it is used to scan the image to recognise the fonts and other minute details in doing so we could recognise themicr code of the cheque.
- It improves text segmentation.
- When you click train you get ocr data using this we can comparethe entities(23 digits micr)
- Registration Estimator in matlab is used to compare two images
- In our application, we use it to compare the scanned and base patterns
- Fixed image and moving image are used
- In this the base pattern(standard uv) is the fixed image and scanned cheque is the moving image
- Now from this comparision we have done it detects the matching patterns.

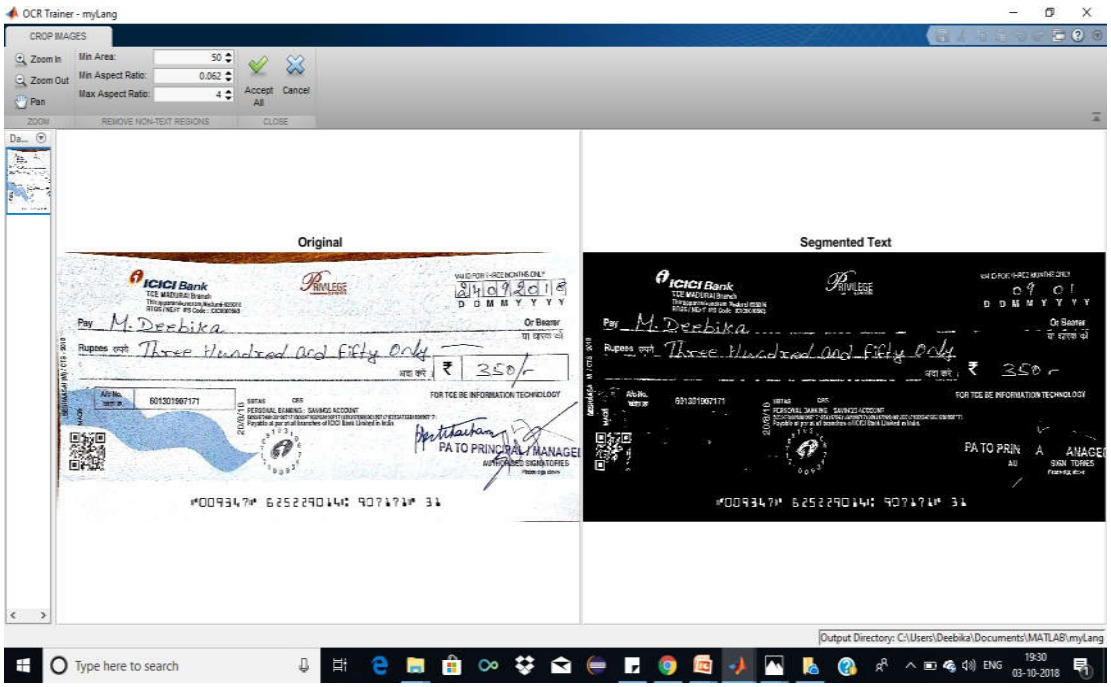


Fig 7.4OCR scan

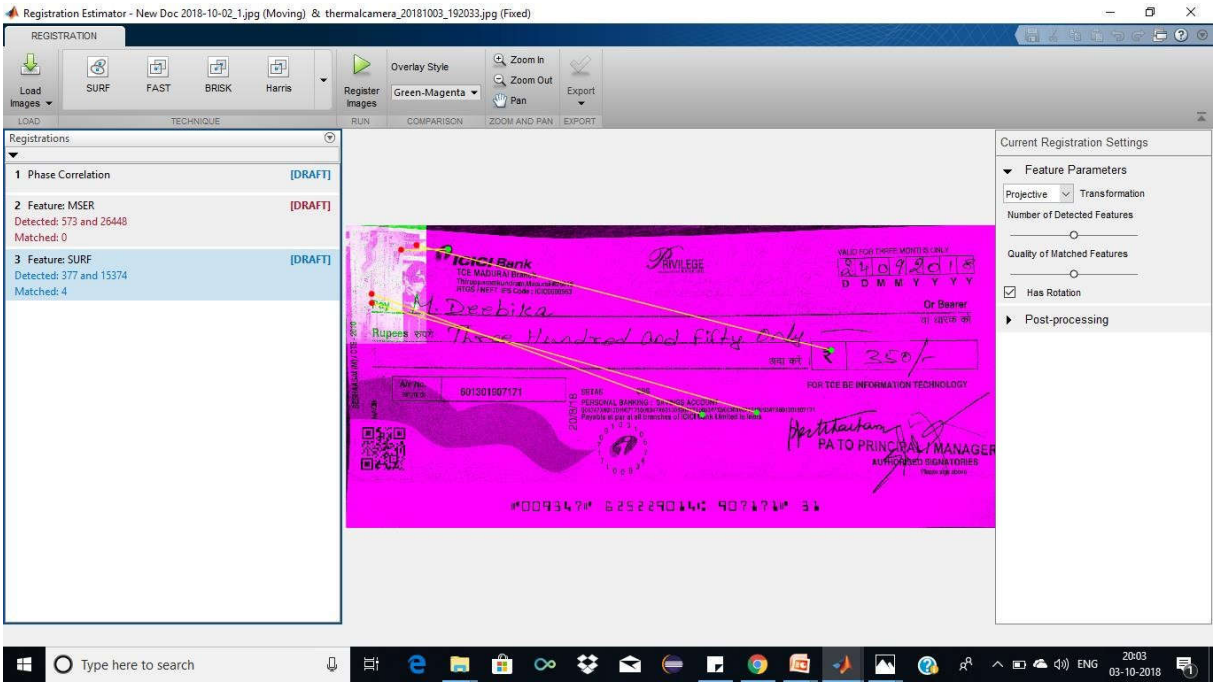


Fig7.5 Matching pattern checking

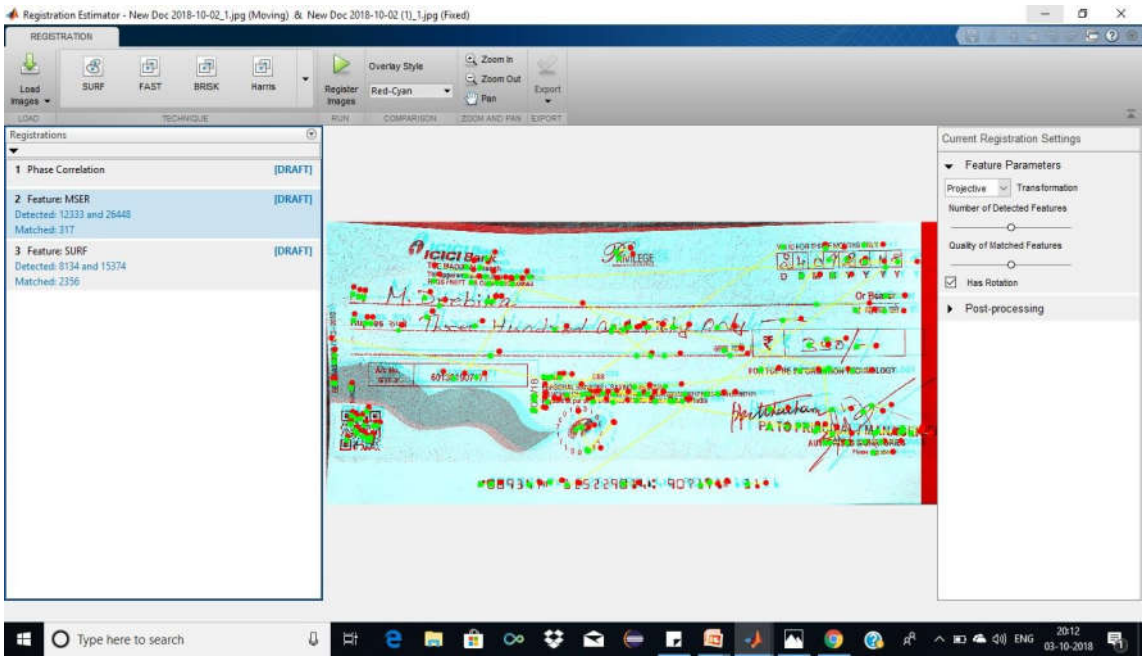


Fig 7.6Detection of matched patterns

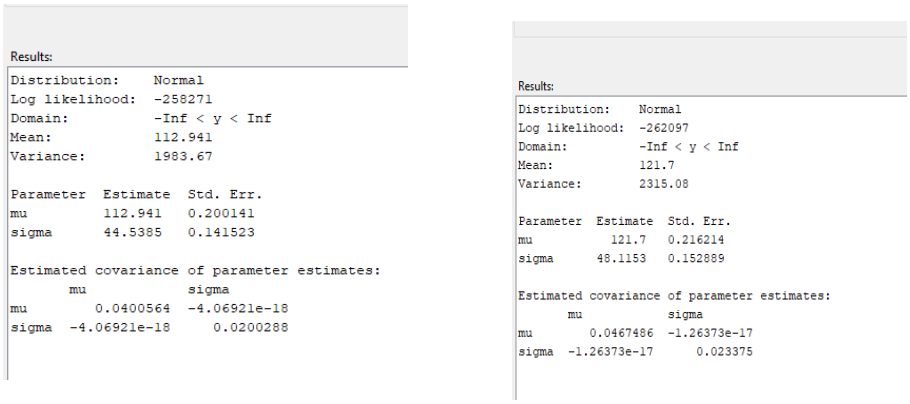


Fig 7.7 ACCURACY ANALYSIS

In the above image we have calculated the accuracy the left image is the accuracy of our proposed method where likelihood is max compared to right image that uses the normal uv image scan method. Thus, the accuracy of the proposed method is more accurate than traditional method.

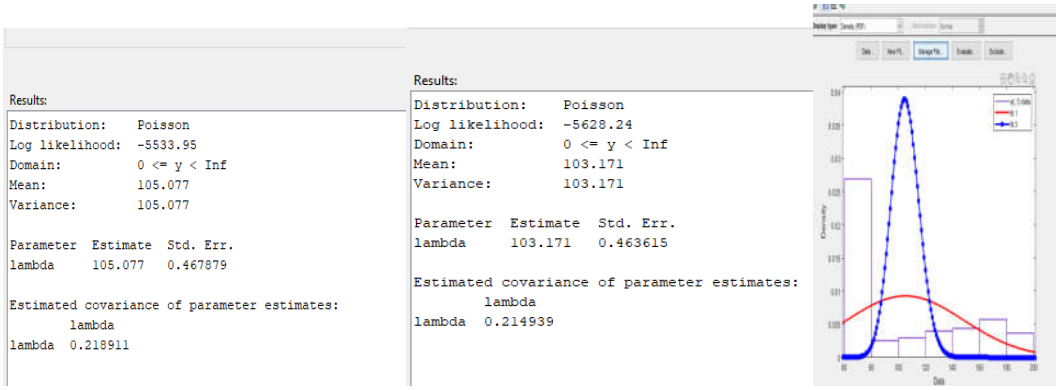


Fig 7.8

ACCURACY PARAMETERS	EXISTING METHOD	PROPOSED METH OD
	Watermark based method	UV image comparison
LOG LIKELIHOOD	-262097	-258271
MEAN	121	112
PROOF	"Detecting tampered cheque images in cheque truncation system using diff expansion based watermarking" IEEE paper	Implementation using matlab

TABLE 7.1

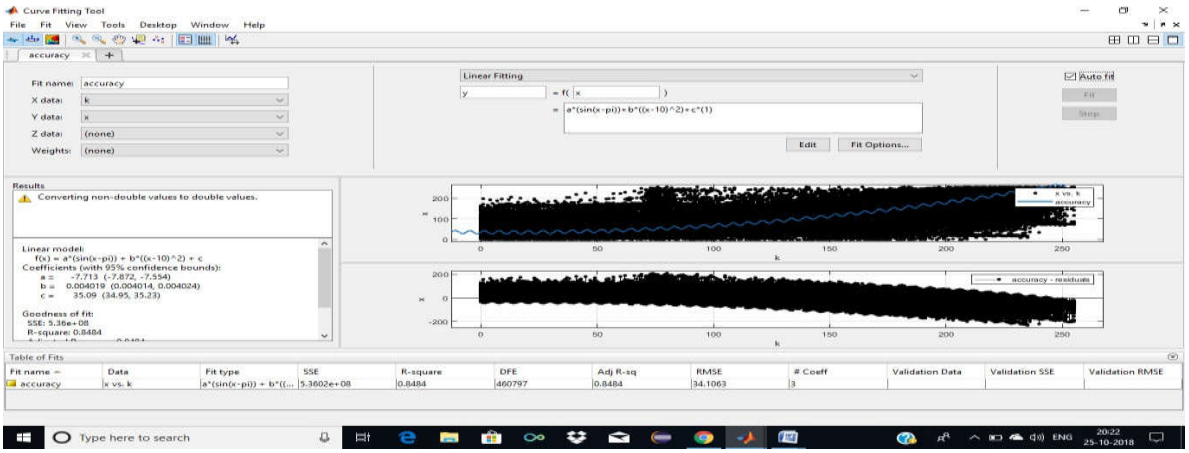


Fig7.9

The above image shows the blue line that represents the accuracy level that increases in the proposed method whereas the below graph represents the constant low level accuracy.

8. CONCLUSION

The methodology that is proposed will be the main factor to detect the forged cheque with high accuracy unlike the methods that are available also those methods will not cover or use the main factor(uv image) to detect the forged cheques. Though this domain involves high confidentiality to provide uv image of banks this is just the improvement and new method to detect the forged one from the genuine ones and separate accordingly to further process (whether to accept or reject).

REFERENCES

1. https://www.npci.org.in/sites/all/themes/npcl/images/PDF/NDBCH_Procedu ral_Guidelines.pdf
2. https://rbi.org.in/ , https://www.npci.org.in/
3. https://ieeexplore.ieee.org/document/6779469
4. https://www.researchgate.net/publication/287181531_Detection_of_manipulated_cheque_images_in_Cheque_Truncation_System_using_mismatch_in_pixels
5. https://www.researchgate.net/publication/273005565_Secret_Image_Sharing_Based_CTS_with_Cheating_Detection
6. Malik/1cd7d09cbc9097f76cf9b71aee415a6bf6ce769e
7. https://in.mathworks.com/company/newsletters/articles/systematic-fraud-detection-through-automated-data-analytics-in-matlab.html/