Watermarking Technique for Tamper Detection of Cheque Image in CTS

Siddharth Hubli
Department of Information Technology
SDM College of Engineering and Technology,
Dharwad, India
siddharth.hubli93@gmail.com

Arati S. Nayak
Department of Information Science & Engineering
SDM College of Engineering and Technology,
Dharwad, India
arati_nyk@yahoo.com

Abstract - Digitalization of banking sector have brought all their operations online and even money transaction too. But still 70 – 80 percent of transaction takes place through movement of physical cheque. So to overcome the drawbacks of traditional cheque clearing system, RBI proposed an idea of Cheque Truncation System. This system has faster clearing cycles and captures the image of the cheque and sends it to the drawee bank and prevents the movement of physical cheque between the banks. As CTS involves transmission of cheque images, the content of the cheque images can be modified or tampered to commit fraud. So there is a need to protect the cheque image. Thus this paper proposes a digital watermarking technique to detect the tampered regions in the cheque image.

Keywords*-CTS, Image watermarking, Tamper detection*

*****

I. INTRODUCTION

CTS is online image based cheque clearing system used for faster clearing of cheques. When a customer submits the cheque to the presenting bank, the presenting bank captures the image of the cheque and along with the cheque image the MICR code, date and other relevant information is sent to the paying bank via the clearing house [1] which is shown in Fig.1. At the paying bank the cheque image is processed and all the information are authentic the amount from the account is released. The physical cheque remains with the presenting bank and CTS eliminates the movement of physical cheques between the banks. This system overcomes the limitation of traditional way of clearing the cheques and provide following benefits to bank and customers:

- Shorter clearing cycles
- Reduction in cost and time
- Improves the operational efficiency of bank.
- Reduction of manual error
- Faster verification or reconciliation process

According to RBI the transmission channel is secured, but there are certain flaws in the system like cheque images can be attacked before they are transmitted or the cheque images can be manipulated if the transmission channel is compromised. So there is a need to implement a system that can protect the integrity and authenticity of the digital image of cheque, thus digital watermarking technique is used to embed security signature or digital watermark on the digital images of the cheque. As digital images of the cheque are used by CTS it can undergo various attacks like modification of content in the cheque or insertion and deletion of the content, so we use digital watermarking technique to detect the region of attack or tampering done to the cheque images.

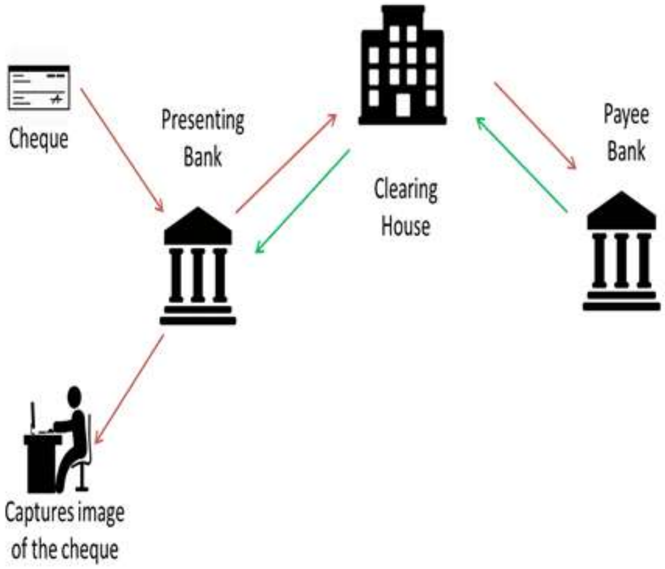

Fig. 1 Process flow of CTS

II. OVERVIEW OF DIGITAL WATERMARK

The evolution of internet and storage technology has led to tremendous growth of digital content being created and shared, which creates a need to protect the authenticity and copyrights of the digital content which can be in the form of audio, video or images. Thus digital watermarking techniques were implemented to protect unauthorized use and distribution of digital content and in the year 1992 the term digital watermark was coined. Digital watermarks are of two types, visible watermark and invisible watermark as shown in Fig. 2.

Digital watermark usually involves embedding a watermark into the content and extracting it for verification and authentication.

A. *Application of Watermark*

- To check the originality of the digital content.
- To protect the ownership rights or copyrights of the content.
- To detect tampered content.
- To trace illegal copies of the content.
- To prevent the copying of the original content.
- Broadcast monitoring.

B. *Watermarking Requirements*

Following requirements have to be considered for developing an efficient watermarking technique [2].

- Capacity of watermark to embed should be optimum so that it does not affect the quality of watermarked image.
- Watermarking should not degrade the perceptual quality of the image that is human vision system should not be able to identify the difference in the watermarked image and original image.
- Watermarked image should be robust to different kinds of attack.
- The watermark embedded into the image should not be easily removed or forged by the attacker.

C. *Types of Watermark*

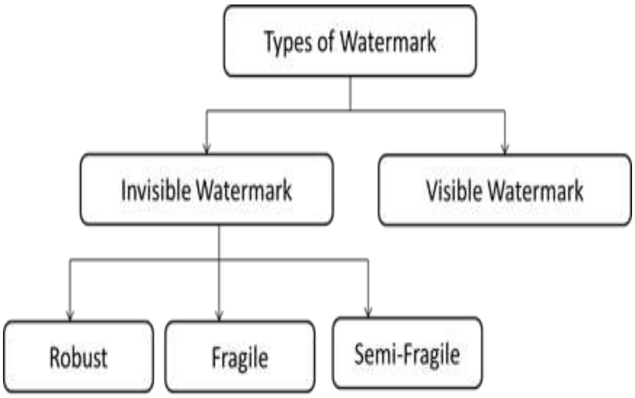

Fig. 2 Watermark Categories

Watermark can be classified into visible and invisible watermark. Visible watermark are different kind of logos that organization or content owners embed on their digital content to prove their ownership rights. Invisible watermark can further classified into three types:

- Robust: This kind of watermark is designed to resist attempts to remove or destroy the watermark.
- Fragile: This kind of watermark can be easily destroyed, but has the capabilities to detect the tampered regions.
- Semi-Fragile: This watermarking scheme is implemented with both the properties of robust and fragile watermarking scheme.

III. IMPLEMENTATION OF WATERMARKING ALGORTHIM

Watermark can be embedded into the cheque images in two ways, Spatial domain and Transform domain. This paper has used two of the transform domain techniques that are DWT and SVD to develop a semi-fragile watermark to detect the tampered regions in the cheque image.

In this watermarking technique a watermark image is not used, but watermark to be embedded is generated from the original image.

A. *Generating Watermark*

1) The original cheque image is quantized using the quantization matrix. Before quantization, divide the cheque image into blocks of size of quantization matrix. Perform quantization using equation 1

$$QI = (Blk/Q)*Q \qquad (1)$$

Here Q is quantization matrix and Blk is blocks of cheque image.

2) Divide the quantized image into the blocks of size 4X4.

3) Apply SVD to subblocks of block 4X4.

4) After applying SVD, singular values are obtained for each subblock. Using the top left singular values of each subblock generate the watermark bit.

5) The watermark bit is generated by comparing the singular values of each subblock. If singular value of one subblock is greater than the singular value of other subblock set the bit to 1 otherwise zero. In this way we get watermark bit for each subblock.

6) Perform xor operation between the watermark bits of each subblock to obtain a single watermark bit for each 4X4 block of cheque image.

7) After performing the above steps on each 4X4 block we obtain the watermark which is of the same size as of cheque image.

B. *Embedding Watermark*

The generated watermark is not embedded into the quantized cheque image. The quantized cheque image is used only for watermark generation.

1) The original cheque image is divided into the size of 4X4 block.

2) Apply DWT to each block to get four subbands (LL, LH, HL, HH).

3) Quantize the top left value of LL subband that is LL (1,1) by computing equation 2

$$Iq = \text{round}\ (LL\ (1,1)/q) \tag{2}$$

4) The watermark is embedded in LL (1,1). If I_q is equal to the watermark bit then modify the LL (1,1) as $I_q * q$ otherwise modify LL(1,1) to $I_q * q+q$.

5) Apply inverse DWT to each block to obtain the watermarked cheque image.

C. Extracting Watermark

1) The watermarked cheque image is divided into the size of 4X4 block.

2) Apply DWT to each block to get four subbands (LL, LH, HL, HH).

3) Quantize the top left value of LL subband that is $LL'(1,1)$ by computing equation 2.

4) Extract the watermark bit by performing modulus operation between the quantized $LL'(1,1)$ and two.

5) Perform the above steps on each 4X4 block to extract the watermark bit.

IV. TAMPER DETECTION AND RESULTS

To detect the tampered regions in the watermarked cheque image, a watermark is generated from the watermarked cheque image. The steps to generate watermark is similar to the steps explained in section ‘A’ of chapter III.

Once the watermark is generated, compute the difference between the generated watermark and extracted watermark. This result in a tamper map, if all the values in the tamper map are zero then the watermarked cheque image is not tampered. But if any of the value is 1 it indicates the tampered region. Fig. 3 shows the watermarked cheque image.

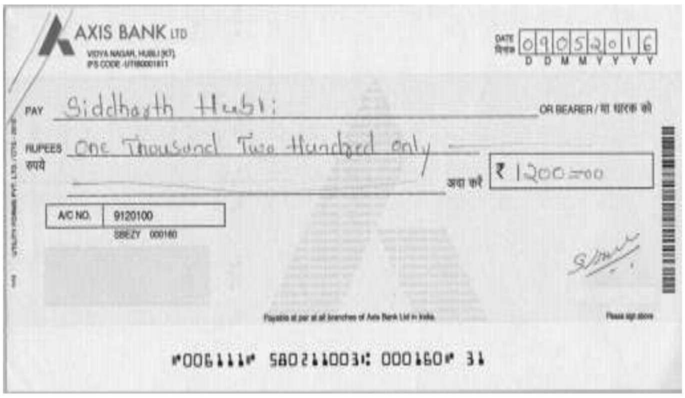
AXIS BANK LTD
VIDYA NAGAR, HUBLI (KT)
IFS CODE -UTIB0001811
DATE दिनांक 0 9 0 5 2 0 1 6
D D M M Y Y Y Y
PAY Siddharth Hubli
OR BEARER / या धारक को
RUPEES रुपये One Thousand Two Hundred only
अदा करें ₹ 1200=00
A/C NO. 9120100
SBEZY 000160
Payable at par at all branches of Axis Bank Ltd in India.
Please sign above
⑈006111⑈ 580211003⑆ 000160⑈ 31

Fig. 3 Watermarked Cheque Image

Modification and deletion attack is performed on the cheque image which is shown in Fig. 4. In the watermarked cheque image amount is changed to Rs. 2200 and a portion of MICR code is deleted which are highlighted in black box in Fig.4.

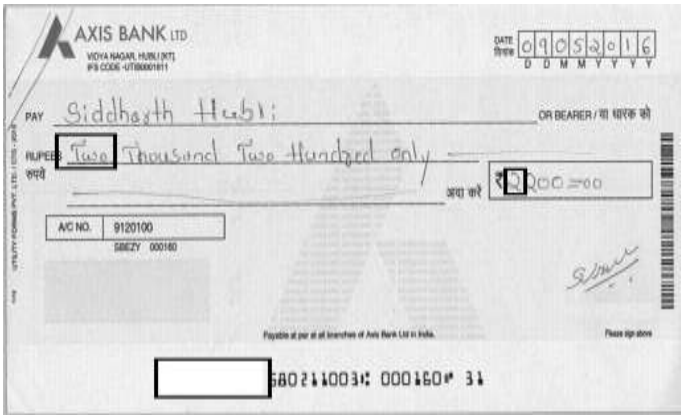
AXIS BANK LTD
VIDYA NAGAR, HUBLI (KT)
IFS CODE -UTIB0001811
DATE दिनांक 0 9 0 5 2 0 1 6
D D M M Y Y Y Y
PAY Siddharth Hubli
OR BEARER / या धारक को
RUPEES रुपये Two Thousand Two Hundred only
अदा करें ₹ 2200=00
A/C NO. 9120100
SBEZY 000160
Payable at par at all branches of Axis Bank Ltd in India.
Please sign above
580211003⑆ 000160⑈ 31

Fig. 4 Attacked Cheque Image

The watermark is extracted from the attacked image and Fig.5 shows the computed tamper map. The tamper map generated shows the exact position of tampered region on the cheque image.

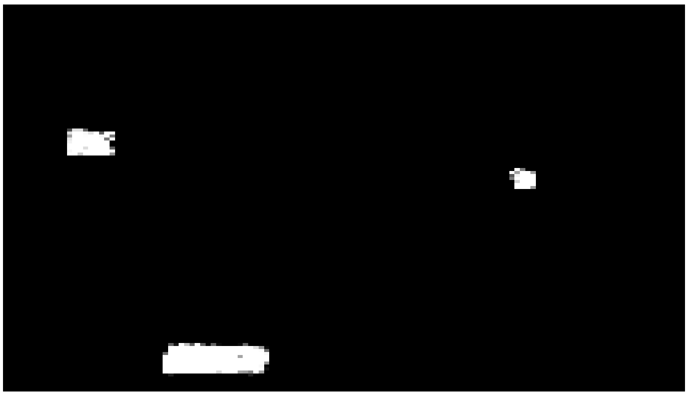

Fig. 5 Region Detected as Tampered

V. CONCLUSION

The technique implemented in this paper can easily detect the tamper done to the cheque images. It can enhance the security of cheque images in CTS and helps bank to detect fraud.

This technique can be further enhanced by embedding recovery information into the watermarked image which helps in recovering the tampered information.

REFERNCES

[1] Cheque Truncation System website. [Online]. Available: http://www.itsallaboutmoney.com/did-youknow/what-is-cheque-truncation-system-cts.

[2] Vallabha VH, ”Multiresolution Watermark Based on Wavelet Transform forDigital images”.

[3] Min Wu, Bede Liu, Watermarking For Image Authentication, Proc of the IEEE Int. Conf. on image processing, 1998,pp.437-441.

[4] M Rajender, R Pal, "Detection of Manipulated Cheque Images in Cheque Truncation System Using Mismatch in Pixels". Published in: Business and Information Management (ICBIM), 2014 2nd International Conference on Jan 2014 IEEE.

[5] Xuemei Jiang, Quin Liu, "Semi-fragile watermarking algorithm for image tamper localization and recovery", Journal of Electronics (China) May 2008, Volume 25, Issue 3, Springer.

[6] Xiaojun Qi, Xing Xin, Ran Chang, "Image authentication and tamper detection using two complementary watermarks", IEEE 2009.

[7] Chetan K R, S nirmal, "A new fragile watermarking approach for tamper detection and recovery of document images", Ineranational conference on Advances in computing, communication and informatics, New Delhi, Sept 2014.

[8] Shan Suthaharan, "Logistic Map-Based Fragile Watermarking for Pixel Level Tamper Detection and Resistance", EURASIP Journal on Information Security, October 2010.