ISSN (Online): 2456-0448
International Journal Of Innovative Research In Management, Engineering And Technology
Vol. 1, Issue 10, November 2016

DIGITAL WATERMARKING ON BANK CHEQUE USING MATLAB

[1]Anupriya Goyal, [2]Mr. Izzaruddin
[1] [2]Computer Engineering Department, Aligarh Muslim University Aligarh, India
[1]anupriagoyal14@gmail.com, [2] izharuddinmuhammed67@gmail.com

Abstract: ***Cheque Truncation System (CTS) is an image based cheque clearing system to speed up the process of clearing the cheques. Cheque truncation means stopping the flow of the physical cheque issued by a drawer to the drawee branch. CTS of bank sends electronic cheques images to drawee branch for payment through the clearing house. The intruders may damage the data and can degrade the quality of cheque image or can duplicate cheque image. Therefore there is necessity of security and copyright protection. In this paper, Least Significant Bit Watermarking Technique is discussed. By using this watermarking technique, the bank cheques can be protected from the intruders who can damage the cheque while transferring to drawee bank.***

Keywords- ***Watermarking; Least Significant Bit; Cheque Truncation system; Cheque frauds.***

I. INTRODUCTION

Now a day's digital communication through wired/wireless network like internet and local network is used to transmit the data.Data of different format like audio, video, text or images are transferred from one device to another. As a result, the security of information against unauthorized access has become a prime objective. Growth of the Internet and networked multimedia systems has emphasized the need for copyright protection of the digitized multimedia data. This leads to lots of development of various techniques for data hiding. Media can be images, audio clips, videos etc. Digital watermarking is today extensively used for many applications such as authentication of ownership or identification of illegal copies. Digital watermark is an invisible or maybe visible structure added to the original media.

Bank cheque truncation system uses cheque image as data and transfer it to drawee branch of bank for payment through the clearing house. Thus, there is need of security and copyright protection for cheque images. The physical cheque is scanned to capture a digital image of the cheque. The digital image is routed to appropriate payee bank. At the payee bank, the signature appearing in the cheque image is verified against the stored signature of the account number mentioned in the cheque image. It is also checked whether the account mentioned in the cheque image has the balance to pay the amount of money appearing on the cheque image. After getting a positive result for verification, the payee bank signals the presenting bank to pay the money to the customer. Therefore, the payee bank should receive an unaltered image of a genuine cheque so that its decision does not support a case of fraud. In recent years, number of cheque related fraud cases were discovered. One of the fraud is manipulating like manipulation of genuine check image.

II. RELATED WORK

In this section a literature review of digital watermarking techniques used for images and the previous work which had been done on digital watermarks is also presented. Digital watermarking is a branch of information hiding which is used to multimedia, copyright protection .There are many solutions that have been proposed like Cryptography, Steganography and Watermarking [1, 2]. The embedded watermark should not degrade the quality of the image and should be perceptually invisible to maintain its protective secrecy [3]. In the frequency domain schemes, the watermark is embedded with the transformed coefficients of original image. It is more robust than spatial domain, less control of perceptual quality and mainly suits for copyright application [4,5]. The robustness and perceptual quality of the watermarking schemes mainly depends on how much percentage of the watermark is embedded into host image i.e., scaling factor . The main impediments of DFT&DST, SVD based watermarking schemes are as follows: 1.They are generated strong signals to rotation, scaling, translating.2.False positive Problem: when a specific watermark is detected from substance in which a different watermark was embedded, causing an hazy situation, [6, 7]. 3. Diagonal Line Problem: If we modify the singular values of the cover image directly with the watermark image then there will be a diagonal line in the reconstructed watermark from the attacked watermarked images [8].

Recent years have also witnessed a surge in number of cheque related fraud cases. Different kinds of cheque relate frauds are possible [9]. Alongside the age old cheque frauds like forgery, counterfeiting of cheques, a rising concern is about protecting the image of the cheque against malicious alterations. While the image of the cheque is accessed at the involved banks and also at the clearing house to carry out various tasks, someone (internal to these organizations) may

ISSN (Online): 2456-0448
International Journal Of Innovative Research In Management, Engineering And Technology
Vol. 1, Issue 10, November 2016

change the content of the image to have financial gain. Therefore, a need is felt to detect such kind of fraudulent attempts. The content of the cheque image can be authenticated using image watermarking techniques [10][11].

III. CHEQUE TRUNCATION SYSTEM BASIC PROCESS

The basic process flow of Cheque Truncation System is given in the following steps. Fig.1 depicts this process flow.

1. A customer presents the physical cheque in a bank (presenting bank).
2. Presenting bank captures an image of the physical cheque.
3. Then the presenting bank sends the image to the payee bank through the clearing house.
4. Payee bank verifies the genuineness of the cheque by matching the signature of the payee and other security features which are present in the cheque image. Checks whether the payee account has the balance required for this payment.
5. If all checks are positive, then the payee bank sends a confirmation message to the presenting bank (through clearing house) for the payment.
6. After receiving positive confirmation, presenting bank credits the amount to the customer.
7. Finally, settlement of amount between the involved banks is mediated by the clearing house.

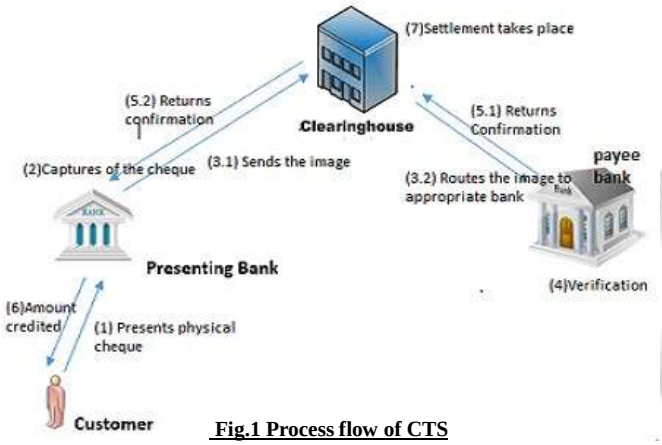

Fig.1 Process flow of CTS

IV. PROPOSED APPROACH

The least significant bit (LSB) technique is used for simple operation to embed information in a cover image. The LSB technique is that inside of a cover image pixels are changed by bits of the secret message. Fig.2 shows the framework of the proposed method .

EDGE DETECTION TECHNIQUE:

Since edge detection is in the forefront of image processing for object detection. Edges in images are areas with strong intensity contrasts. Edge detection refers to the process of identifying and locating sharp discontinuities in an image. The discontinuities are abrupt changes in pixel intensity which characterize boundaries of objects in a scene. The edge detected image can be obtained from the sobel gradient by using a threshold value.

The scanned image of the bank cheque is taken and after that it is read in matlab. It is then converted into two dimension i.e. grayscale image. After this edges of the scanned image are detected and then embedding at the edges is done so that all the important areas or portion of image are covered in watermarking (as shown in Fig.3). We have embedded the watermark on the edges which cover the most of the important portion of bank cheque image.

ISSN (Online): 2456-0448
International Journal Of Innovative Research In Management, Engineering And Technology
Vol. 1, Issue 10, November 2016

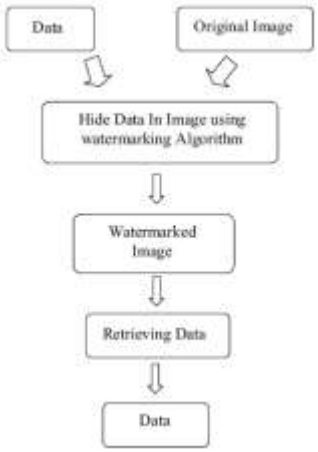

Fig. 2 Framework of the method proposed

Fig.3 Edges detection

The algorithm used for embedding is least significant bit (LSB). In this method of watermarking we are changing or modifying the least significant bit value of the pixel of the original image (grayscale bank cheque image). The least significant bit value of pixel of the original image is replaced by the bit value of watermark to be embedded one by one.

V. ALGORITHMS USED

Sobel Edge Detection

The gradient of image is calculated for each pixel position in the image. The magnitude of vector Δf is denoted as,

$$\Delta f = \text{mag}(\Delta f) = [G_X^2 + G_Y^2]^{1/2}$$

where G_X and G_Y are the mask for x-direction and y-direction respectively.

Explanation:

Read the original image. Convert image to grayscale. Convert the image into double. Then determine the mask for G_X and G_Y x-direction and y-direction respectively.

Let A be the original image matrix. As original image is converted into grayscale image therefore B matrix store the value of grayscale. C is the matrix defined as: C=double(B)

Mask for x-direction:

Gx (i, j) = ((2*C (i+2, j+1)+C (i+2, j)+C (i+2, j+2)) - (2*C (i, j+1) +C (i, j) +C (i, j+2)))

Mask for y-direction:

Gy (i, j) = ((2*C (i+1, j+2) +C (i, j+2) +C (i+2, j+2)) -
(2*C (i+1, j) +C (I, j) +C (i+2, j)))

ISSN (Online): 2456-0448
International Journal Of Innovative Research In Management, Engineering And Technology
Vol. 1, Issue 10, November 2016

The gradient of image is determined. The threshold value of image is set.

The gradient of the image

B (i, j) =sqrt (Gx (i, j). ^2+Gy (i, j). ^2);

Embedding Algorithm

- Using the edge detection method we first determined the pixel values on which embedding could be done.
- Read the image of logo (watermark).
- Convert the image of watermark to grayscale.
- The pixel values which are in decimal are converted to binary and a vector of binary values is created.
- Then LSB algorithm is applied.
- Each single bit of watermark is embedded using LSB

algorithm into original image where edges are present.

- As a result of embedding process, the original and watermarked image are displayed.

Extraction Algorithm

Extraction is reverse process of embedding

- The edges of watermarked image are determined.
- The pixel value on which embedding was done are determined and then they are converted into binary form.
- From these binary values, the first least significant bit are collected to form a matrix of the original logo (watermark) and hence watermark is extracted.

VI. RESULTS

The original image of cheque, watermarked image, original logo and extracted logo are compared on the basis of histograms and autocorrelation (as shown in Fig.4, Fig.5 and Fig.6).

Fig. 4 Watermarked image

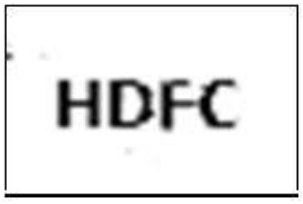

Fig. 5 Original logo

ISSN (Online): 2456-0448
International Journal Of Innovative Research In Management, Engineering And Technology
Vol. 1, Issue 10, November 2016

Fig. 6 Extracted logo

The histograms for original image of bank cheque and watermarked image are almost similar, which can be noticed by normal human eye (as shown in Fig.9 and Fig.10). The **correlation coefficient** measures the robustness of the relationship between two variables. The value of the **correlation coefficient**, denoted as r, ranges from **-1** to **+1**, which gives the strength of the relationship and whether the relationship is negative or positive. Exactly -1 means a perfect downhill (negative) linear relationship. 0 means no linear relationship. Exactly +1means a perfect uphill (positive) linear relationship.For more precise comparison autocorrelation coefficient is determined. The value of coefficient of autocorrelation for original image and watermarked image is 1 i.e they have linear relationship and for original logo and extracted logo is approximately equal to 1 (it depends on the value of threshold used for detecting edges).The experiment was performed on six different cheque images and results are presented in a table(as shown in fig.11).

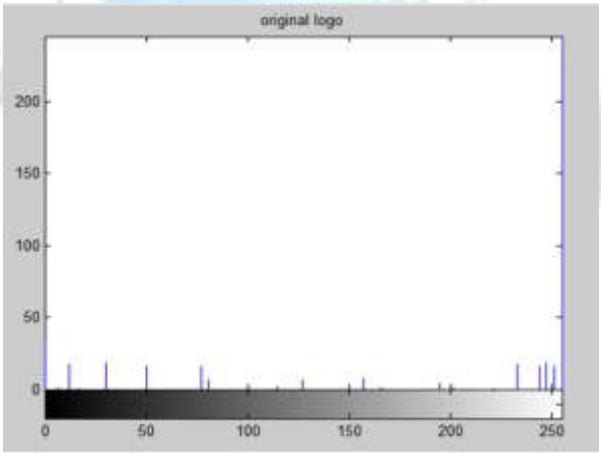

Fig. 7 Histogram for original logo

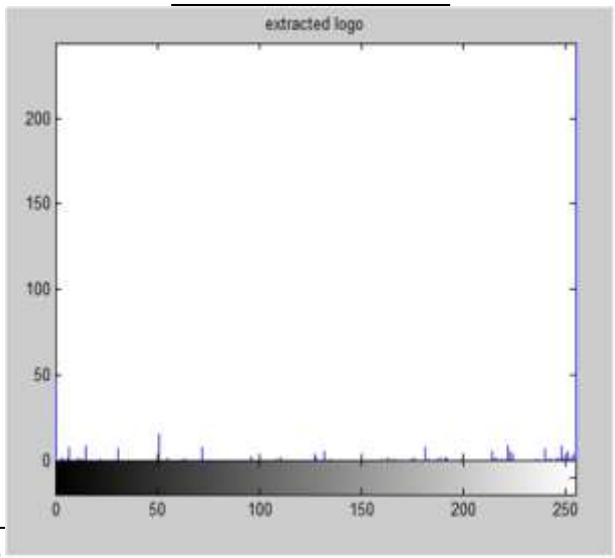

Fig. 8 Histogram for extracted logo

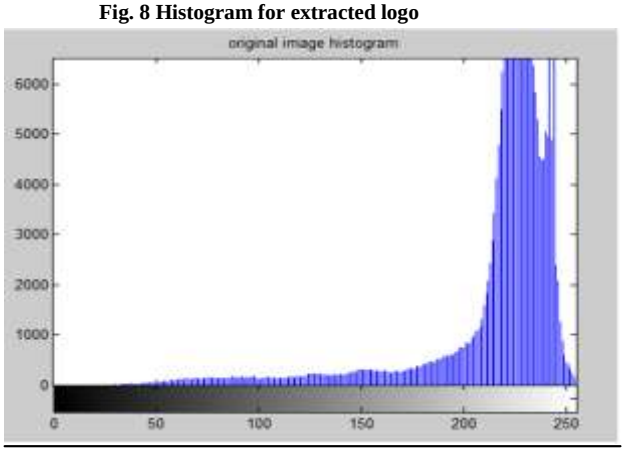

Fig. 9 Histogram for original cheque image

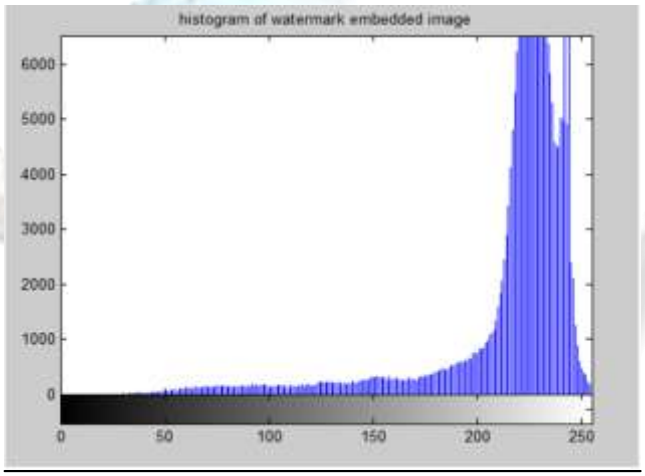

Fig. 10 Histogram for watermarked image

S.no.	Correlation Coffecient Between watermarked and original image	Correlation Coffecient Between extracted watermark and original watermark
1.	1	0.96
2.	1	0.92
3.	1	0.88
4.	1	0.87
5.	1	0.80
6.	1	0.78

Fig.11 Result table

CONCLUSION

This paper proposes a method to detect alterations in the cheque images. The method enables the payee bank to detect fraudulent modifications made in the bank cheque image while transferring to the paying bank. Verification has been

done on the basis of histogram and correlation coefficient and determined the original image and watermarked images are similar(as shown in Fig.11).On calculating the autocorrelation coefficient between extracted watermark and original

watermark image to be around 0.80 then we can conclude that no fraud has occurred while transferring. Success in detecting manipulated images of cheques in CTS environment will open up newer dimensions in the area of payment system.

ACKNOWLEDGMENT

I would like to pay special thanks, warmth and appreciation to my family members and my friend Shivangi Cial. They made my work successful and assisted me at every point to cherish my goals.

REFERENCES

[1] Hernandez, J.R., M., Amado, and F.P., Gonzalez, 2000. "DCT- domain watermarking techniques for still for still Images: Detector performance analysis and a new structure", IEEE Trans. on Image Processing,Vol. 9 , pp. 55-68.

[2] I.J. Cox, et al, "Digital watermarking and Steganography" (Second Edition), Morgan Kaufmann, 2008.

[3] T,Ramashri and A.Rajani, "Digital watermarking using dct, svd and edge detection technique" IJERA trans,vol-1, pp 1828-1834.

[4] Ante Poljicak,Lidija Mandic,Darko Agic Discrete Fourier transform– based watermarking method with an optimal implementation radius, journal of electronic imaging.

[5] Emir Ganic and Ahmet M. Eskicioglu, "Robust DCT,FFT-SVD Domain Image Watermarking: Embedding Data in All Frequencies," in
Proc. Workshop Multimedia Security, Magdeburg, Germany, pp. 166-174, 2004.

[6] G. Bhavnagar and B. Raman, "A new robust reference watermarking scheme based on DCT,DST AND FFT- SVD,"" Computer Standards Interfaces, vol. 31, no. 5, pp. 1002-1013, Sep. 2009.

[7] Pat yip, "sine and cosine transfoms" 2000 by CRC Press LLC.

[8] Xiao-Ping Zhang, Senior Member, IEEE, and Kan Li, Comments on "An SVD-Based Watermarking Scheme for Protecting Rightful Ownership",IEEE Trans on Multimedia, Vol. 7, no. 2, pp. 593-594, Apr. 2005

[9] Roman Rykaczewski. "Comments on "An SVD-Based Watermarking Scheme for Protecting Rightful Ownership," IEEE Transactions on Multimedia, Vol. 9, No. 2, pp. 421-423, Feb. 2007.

[10] Wikipedia, "Cheque fraud", en.wikipedia.orglwiki/Cheque_fraud

[11] F. Hartung and M. Kutter, "Multimedia watermarking techniques", Proc. of the IEEE, vol. 87, issue 7, pages 1079-1107, July 1999.

[12] V. M. Potdar, S. Han, and E. Chang, "A survey of digital image watermarking techniques", Proc. of 3rd IEEE International Conference on Industrial Informatics, pages 709-716, August 2005.

[13] Sudhanshu Suhas Gonge, Prof.Ashok A.Ghatol, "Combined DWT- DCT Digital Watermarking Technique Software Used for CTS of Bank,"2014 International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT)

[14] Maloth Rajender, Rajarshi Pal, " Detection of Manipulated Cheque Images in Cheque Truncation System Using Mismatch in Pixels," 2014 2nd International Conference on Business and Infonnation Management (lCBIM)