Secret Image Sharing Based Cheque Truncation System with Cheating Detection

Sreela.S.R\textsuperscript{a}, G. Santhosh Kumar\textsuperscript{b}, Binu.V.P\textsuperscript{c}

\textsuperscript{a}Department of Computer Science, Cochin University of Science and Technology
\textsuperscript{b}Department of Computer Science, Cochin University of Science and Technology
\textsuperscript{c}Department of Computer Applications, Cochin University of Science and Technology

Cheque Truncation System (CTS) is an automatic cheque clearance system implemented by RBI. CTS uses cheque image, instead of the physical cheque itself, for cheque clearance thus reducing the turn around time drastically. This approach holds back the physical movement of cheque from presenting bank to the drawee bank. In CTS, digital image of the cheque is protected using standard public key and symmetric key encryptions like RSA, triple DES etc. This involves a lot of computation overhead and key management. The security also depends on the hard mathematical problem and is only computationally secure. Information theoretically secure, secret image sharing techniques can be used in the CTS for the secure and efficient processing of cheque image. In this paper, we propose two simple and efficient secret image sharing schemes and a Cheque Truncation System based on these algorithms. In the proposed scheme, the presenting bank is acting as the dealer and the participants are the customer, and the drawee bank. The dealer should generate the shares of cheque and distributes it to customer and drawee bank. The validity of the shares are important during the reconstruction process. The proposed scheme also suggests a method for cheating detection which identify any invalid shares submitted by the customers, using the hashing technique. The experimental results shows that the proposed scheme is efficient and secure compared with the existing scheme.

Keywords : Cheque Truncation System, Secret image sharing, PKI, Pixel expansion, Visual cryptography.

1. INTRODUCTION

Cheques represent a significant segment of payment instruments in India. Cheque Truncation System (CTS) or ICS (Image Based Clearing System) in India is a project undertaken by Reserve Bank of India (RBI) for faster clearing of cheques. CTS is basically an online image-based cheque clearing system where cheque images and Magnetic Ink Character Recognition (MICR) data are captured at the collecting bank branch and transmitted electronically. Manual clearing of cheque needs human intervention and is a time consuming task. Cheque truncation involves stopping the flow of the physical cheques issued by a drawer to the drawee branch. 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 point of truncation is left to the discretion of the presenting bank. Thus Cheque truncation, would eliminate the need to move the physical instruments across branches and hence result in effective reduction in the time required for payment of cheques, the associated cost of transit and delays in processing, etc. This will speed up the process of collection or realization of cheques and thus reduce the turn around time.

The system offers following benefits to the bank and customers. Banks can expect multiple benefits through the implementation of CTS, like faster clearing cycle, better reconciliation/verification process. Besides, it reduces operational risk by securing the transmission route. Reduction of manual tasks leads to reduction of errors. Customer satisfaction will be enhanced, due to the reduced turn around time (TAT). Real-time tracking and visibility of the
cheques, less fraudulent cases with secured transfer of images to the RBI are other possible benefits that banks may derive from this solution \[8\]. For Customers CTS / ICS substantially reduces the time taken to clear the cheques as well increases operational efficiency by cutting down on overheads involved in the physical cheque clearing process. In addition, it also offers better reconciliation and fraud prevention.

The use of the Public Key Infrastructure (PKI) ensures data authenticity, integrity and non-repudiation, adding strength to the entire system. The presenting bank is required to affix digital signature on the images and data from the point of truncation itself. The image and data are secured using the PKI through out the entire cycle covering capture system, the presenting bank, the clearing house and the drawee bank. This system needs a lot of computation and overhead in key management is high. In this paper a secret image sharing \[3\] based scheme is proposed. Two efficient schemes are proposed which are computationally secure and avoids the overhead in key management. A cheating detection scheme is also proposed which avoids the use of invalid shares during the reconstruction.

In the rest of the paper, section 2 describes the CTS Architecture. Section 3 describes the related work. Proposed system and algorithms are explained in section 4. Experimental results are discussed in section 5 and the conclusions are drawn in section 6.

2. CTS ARCHITECTURE

The process flow of CTS is explained below. 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 comprising of a scanner, core banking or other application. Images and data should meet the specifications and standards prescribed for data and images. The architecture of CTS is explained in figure 1.

To ensure security, end-to-end Public Key Infrastructure (PKI) has been implemented in CTS for protecting data and image. The presenting bank sends the data and captured images duly signed and encrypted to the Clearing House (the central processing location) 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 a secure and safe manner to the Clearing House (CH). The CTS uses public key infrastructure (PKI) like digital signature and encryption for protecting cheque images and data. The standards defined for PKI are hash algorithm SHA-1, padding algorithm, RSA asymmetric encryption with 1024 bit key length, Triple DES (3DES, TDES) symmetric encryption with 168 bit key length, and Certificates in x.509v3 format. Cheque image is protected using encryption techniques. These techniques need a lot of computation and usage of keys.

3. RELATED WORK

CTS system is implemented by RBI to reduce the complexity of cheque processing. CTS system is implemented in India in 2010. Grid based CTS is implemented in Chennai, Delhi, Kolkata etc. The different security schemes are applied in cheque. Pasupathiathan, Vijayakrishnan, Josef Pieprzyk, and Huaxiong Wang \[15\] de-
scribes privacy enhanced electronic cheque system in 2005. In 2011, Rigel Gjomemo, Ha.z. Malik, Nilesh Sumb, V.N. Venkatakrishnan and Rashid Ansari [13] explains the digital cheque Forgery attack on CTS. Kota, Saranya, and Rajarshi Pal [15] explains the method for detecting tampered cheque images in CTS Using Difference Expansion Based Watermarking in 2014.

The secret image sharing schemes are based on visual cryptography, number theory [6], information hiding theory, error diffusion technique, boolean operation etc. In Yan, Xuelu scheme [12], secret image sharing is based on information hiding theory. The important technique used in this scheme are MLE and LSBM. But this scheme is applicable only to the binary images. Chen and Chang [2] use quadratic residue technique for secret image sharing. They proposed a (2, 2) scheme which is lossy and the lossless scheme having the share size larger than the secret. The computations involved is also more. Chen, Wei-Kuei, and Hao-Kuan Tso [4] introduced a secret image sharing scheme for protecting medical images using Hill cipher method. Thein-Lins Scheme enhanced Shamir’s secret sharing scheme [9] (Lagrange interpolating polynomial) for protecting digital images.

Table1 explains a comparative study on different secret image sharing schemes.

4. PROPOSED SYSTEM

The system architecture describes how secret image sharing scheme happening in the CTS. In this architecture, the dealer should be the presenting bank. The participants are customer, clearing house (CH), and drawee bank. Figure 2 explains the system architecture.

In order to reduce the computation and usage of keys, cheque image can be protected using secret image sharing. In this paper, two secret image sharing methods are proposed for protecting cheque images. If any one of the participants do malpractice on the shares, then cheating occurs. Cheating detection is implemented in this paper. In secret image sharing technique, a secret image is distributed to some of the participants through splitting the image into different pieces called shares and recover the secret image by collecting the sufficient number of shares from authorized participants. This field of cryptography is called visual cryptography or visual secret sharing [5]. If any one of the participant do malpractice on their shares, cheating detection methods can be used. It consists of three phases: share generation phase, distribution phase and reconstruction phase. In the share generation phase, the digital image is split into different pieces called shares. In the distribution phase, the shares are distributed to authorized participants and in the last phase, the image is reconstructed using sufficient number of shares from authorized participants. In a secret image sharing scheme, there is a secret image S to be shared among a set of participants. The secret is known to a special person called dealer. The dealer generates and distributes partial information called shares to the participants.

(2,3) scheme is required for implementing security in CTS. Presenting bank generates the shares and distributed to the clearing house, drawee bank and to the customer. Customer should use the share to get the information of processing of cheque through online. Drawee bank should reconstruct the cheque image using the share from the CH and its own share. Drawee bank can’t reconstruct the cheque image using its own share. To implement security in CTS, xor scheme and partition scheme can be used.

The important steps involved in the proposed CTS using secret image sharing are as follows:

1. Customer submits the cheque to the presenting bank.
2. Capture image of cheque and data using capture system
3. Send the data and image to the presenting CHI.
4. Presenting CHI provide security to the cheque image using (3,2) secret image sharing scheme.
5. Send first share of the cheque image (SC1) and data to the clearing house through the CHI.
6. Send second share of the cheque image (SC2) to the customer if customer submits cheque through online and this share is used for authentication for viewing the details of cheque processing.

7. The clearing House send data and one share of the cheque image(SC1) to the drawee bank through receiving CHI.

8. The drawee bank request another share of the cheque image from the presenting bank through receiving CHI.

9. The presenting bank submit third share (SC3) to the drawee bank.

10. The receiving CHI reconstructs the cheque image using shares SC1 and SC3.

11. Send data to the drawee bank for processing cheque.

12. Bank process the cheque using image processing algorithm.

In figure 3 the numbers represent the above steps.

4.1. XOR scheme

XOR scheme is a (2,3) scheme. In this scheme, three shares are created and the original image is reconstructed using at least two shares. The image is not reconstructed using only one share. The share images are created by dividing pixel into four bits. In this scheme, the share image pixel is 4 bits. Share generation algorithm is explained in Algorithm 1. Recovery algorithm is explained in Algorithm 2. The original secret image is reconstructed by using any of the two shares from three shares.

Consider an image matrix is

\[
\begin{bmatrix}
157 & 160 & 190 & 130 \\
89 & 255 & 224 & 192 \\
10 & 220 & 255 & 224 \\
64 & 128 & 192 & 255
\end{bmatrix}
\]

Consider the secret image pixel is 190. Its binary representation is 10111110. The share1 pixel(sc1=6(0110)) is created using even bits. The share2 pixel(sc2=15 (1111)) is created using odd bits. The share3 pixel(sc3=9(1001)) is created by xor of s1 s2. The xor scheme is applied on the above image S. The three shares obtained SC1, SC2 and SC3 are as follows:

SC1 =

\[
\begin{bmatrix}
7 & 0 & 6 & 0 \\
13 & 15 & 8 & 8 \\
0 & 14 & 15 & 8 \\
8 & 0 & 8 & 15
\end{bmatrix}
\]
Secret Image Sharing Based CTS with Cheating Detection

Algorithm 1: Algorithm: Share generation

1. Input: M X N Secret grayscale image S
2. Output: Share images SC1, SC2, SC3
3. begin
4. For each pixel (i,j) ∈ \{(i,j)|1 ≤ i ≤ M, 1 ≤ j ≤ N\} repeat steps 2-4
5. Pixelvalue, pv = S(i,j) which is the binary array containing the pixel intensity binary representation.
6. Create share1 SC1(i, j) pixel using even bits of S(i,j) pixel
   \[ SC1(i, j) = \sum_{k=0}^{3} (pv(2k) \times 2^k) \]
7. Create share2 SC2(i, j) pixel using odd bits of S(i,j) pixel
   \[ SC2(i, j) = \sum_{k=0}^{3} (pv(2k + 1) \times 2^k) \]
8. Create share3 SC3(i, j) pixel by xor ing SC1(i, j) and SC2(i, j)
   \[ SC3(i, j, k) = SC1(i, j) \oplus SC2(i, j) \]
9. Output shares SC1, SC2, and SC3.
end

SC2=
\[
\begin{bmatrix}
10 & 12 & 15 & 9 \\
2 & 15 & 12 & 8 \\
3 & 10 & 15 & 12 \\
0 & 8 & 8 & 15 \\
\end{bmatrix}
\]

SC3=
\[
\begin{bmatrix}
13 & 12 & 9 & 9 \\
15 & 0 & 4 & 0 \\
3 & 4 & 0 & 4 \\
8 & 8 & 0 & 0 \\
\end{bmatrix}
\]

In this scheme, the size of the share is half of the size of the original image. The number of bits for representing a pixel in share is 4 bits. If the \( M \times N \) secret gray scale image has a size of \( 8 \times M \times N \) bits, then the size of the share is only \( 4 \times M \times N \) bits. So the storage space of the share is reduced.

Algorithm 2: Recovery algorithm

1. Input: Share images SC1, SC2, SC3
2. Output: Reconstructed Secret image S
3. begin
4. The secret image can be reconstructed from shadow images SC1, SC2
5. For each position, \((i, j)\) ∈ \{(i,j)|1 ≤ i ≤ M, 1 ≤ j ≤ N\} repeat step 2-4
6. S(i, j) is obtained by intermixing bits of SC1(i, j) and SC2(i, j) in even and odd positions respectively.
7. Output image S.

The secret image can be reconstructed from shadow images SC1, and SC3
8. For each position, \((i, j)\) ∈ \{(i,j)|1 ≤ i ≤ M, 1 ≤ j ≤ N\} repeat step 2-3
9. \( b = SC1(i, j) \oplus SC3(i, j) \)
10. S(i, j) is obtained by intermixing bits of SC1(i,j) and \( b \) in even and odd positions respectively.
11. Output image S.

The secret image can be reconstructed from shadow images SC2, and SC3.
12. For each position, \((i, j)\) ∈ \{(i,j)|1 ≤ i ≤ M, 1 ≤ j ≤ N\} repeat step 2-3
13. \( b = SC2(i, j) \oplus SC3(i, j) \)
14. S(i, j) is obtained by intermixing bits of \( b \) and SC2(i,j) in even and odd positions respectively.
15. Output image S.
end
The quality of the reconstructed image is same as the original image. In this scheme, there is no pixel expansion on reconstructed image. It is a lossless scheme.

4.2. Partition Scheme

**Algorithm 3:** Algorithm: Share generation

1. Input: M X N Secret grayscale image S
2. Output: Share images SC1, SC2, SC3
3. begin
   1. Let s be the pixel of the secret image(S) and r be a random number in 0-255.
   2. s is divided into s1 and s2 and r into r1 and r2.
   3. Share1 pixel is created by combining $s_2 \oplus r_2$ and r1
   4. Share2 pixel is created by combining $s_1 \oplus r_1$ and r2
   5. Share3 pixel is created by combining $s_2 \oplus r_1$ and $s_1 \oplus r_2$
   6. repeat step 1-5 until all pixels of image are processed.
   7. Output three shares share1(SC1), share2(SC2), share3(SC3).

Partition scheme is a (2,3) scheme. It uses boolean xor operations. This method uses random number for creating shares. The share generation algorithm is explained in Algorithm 3. Algorithms 4, 5, 6 describe the reconstruction of image.

4.3. Cheating detection scheme using Hash function

A threshold scheme for secret sharing can protect a secret with high reliability and flexibility. These advantages can be achieved only when all the participants are honest, i.e. all the participants willing to pool their shadows shall always present the true ones. Cheating detection is an important issue in the secret sharing scheme. However, cheater identification is more effective than cheating detection in realistic applications. If some dishonest participants exist, the other honest participants will obtain a false secret, while the cheaters may individually obtain the true one. By applying a one-way hashing func-

**Algorithm 4:** Algorithm: Reconstruction using share1 and share2

1. Input: Share images SC1, SC2
2. Output: Reconstructed Secret image S
3. begin
   1. The share1(sc1) pixel is divided into two equal parts sc11 and sc12.
   2. The share2(sc2) pixel is divided into two equal parts sc21 and sc22.
   3. The second part of the original image pixel (s2) is reconstructed by XOR-ing first part of the share1 pixel(sc11) and second part of the share2 pixel(sc22).
      
      $s_2 = sc_{11} \oplus sc_{22}$

   4. The first part of the original image pixel(s1) is reconstructed by XOR-ing second part of the the share1 pixel(sc12) and first part of the share2 pixel(sc21).
      
      $s_1 = sc_{12} \oplus sc_{21}$

   5. The original image pixel(s) is obtained by combining s1 and s2.
      
      $s = s_1 . s_2$

   6. repeat the above steps until all pixels are processed.
   7. Output image S
    end
Algorithm 5: Algorithm: Reconstruction using share1 and share3

1. Input: Share images SC1, SC3
2. Output: Reconstructed Secret image S
3. begin
4. Original image is reconstructed from share1 and share3 by applying following steps.

1. The share1 pixel is divided into two equal parts \( sc_{11} \) and \( sc_{12} \).
2. The share3 pixel is divided into two equal parts \( sc_{31} \) and \( sc_{32} \).
3. The second part of the original image pixel(s2) is obtained by XOR-ing second part of the share1 pixel(s12) and first part of the share3 pixel(s31).

\[
  s_2 = sc_{12} \oplus sc_{31}
\]

4. \( b = s_1 \oplus s_2 \) is obtained by XOR-ing first part of the share1 pixel(s11) and second part of the share3 pixel(s32).

\[
  b = sc_{11} \oplus sc_{32}
\]

5. The first part of the original image pixel(s1) is obtained by \( s_1 = b \oplus s_2 \).
6. Secret image pixel(s) is reconstructed by combining s1 and s2.

\[
  s = s_1.s_2
\]

7. Repeat above steps until all pixels are processed.
8. Output image S

end

Algorithm 6: Algorithm: Reconstruction using share2 and share3

1. Input: Share images SC2, SC3
2. Output: Reconstructed Secret image S
3. begin
4. Original image is reconstructed from share2 and share3 by applying following steps.

1. The share2 pixel is divided into two equal parts \( sc_{21} \) and \( sc_{22} \).
2. The share3 pixel is divided into two equal parts \( sc_{31} \) and \( sc_{32} \).
3. The first part of the original image pixel(s1) is obtained by XOR-ing second part of the share2 pixel(s22) and second part of the share3 pixel(s32).

\[
  s_1 = sc_{22} \oplus sc_{32}
\]

4. \( b = s_1 \oplus s_2 \) is obtained by XOR-ing first part of the share2 pixel(s21) and first part of the share3 pixel(s31).

\[
  b = sc_{21} \oplus sc_{31}
\]

5. The second part of the original image is obtained by \( s_2 = b \oplus s_1 \).
6. Secret image pixel(s) is reconstructed by combining s1 and s2.

\[
  s = s_1.s_2
\]

7. Repeat above steps until all pixels are processed.
8. Output image S

end
tion along with the use of arithmetic coding, the proposed method can be used to deterministically detect cheating and identify the cheaters, no matter how many cheaters are involved in the secret reconstruction.

Two important theorems used in cheating detection using hash function are as follows. Let $a_i$ be the random shares of the secret data and $p$ be the randomly generated prime number.

Theorem 1 [22]: Let $T = \sum_{i=1}^{n} a_i p^{i-1}$, where $0 \leq a_i < p$. Then

$$\left\lfloor \frac{T}{p^{j-1}} \right\rfloor \pmod{p} = a_j \quad (1)$$

Extended from Theorem 1, we have the following result.

Theorem 2 [22]: Let $T = \sum_{i=1}^{n} a_i p^2(i-1) + \sum_{i=1}^{n-1} c p^{2i-1}$, where $-p < a_i < p$ and $1 \leq c < p$. Then

$$\left\lfloor \frac{T}{p^{2(j-1)}} \right\rfloor \pmod{p} = a_j \pmod{p} \quad (2)$$

Combining this result with secret image sharing scheme, the following method is used for cheating detection and cheater identification. Algorithm for cheating detection and cheater identification is explained in Algorithm 7.

The hash value of the image is generated using content of the image. The hash value of the image is also generated using feature vector of the image. In the secret image sharing, any simple change in the shares is treated as a cheating. Any mild change in the image is reflected in the hash value of image using content of image rather than using feature vector of image. So we use the hash generation method using content of the image.

4.4. Cheque processing

Cheque processing is implemented in Drawee bank. In our work, the courtesy amount region and account number field is recognized. The important steps associated with cheque processing are as follows:

1. Load cheque in grayscale.
2. Find courtesy amount region in cheque using cheque template method.
3. Find account number region in cheque using cheque template method.
4. Segment digits in courtesy amount and resize each digit having a size of $28 \times 28$.
5. Apply digit recognition method for recognizing digit in courtesy amount.
6. Combine each digit and generate courtesy amount.
7. Segment digits in account region and resize each digit having a size of $28 \times 28$.
8. Apply digit recognition method for recognizing digit in account number.
9. Combine each digit and generate account number.
10. Process the amount from the account and deduct the amount from the account.
11. Send the information to the presenting bank through clearing house.
12. At last customer gets the amount from the presenting bank.
4.4.1. Digit recognizer

In our work, digit recognition is done using K Nearest neighbour classification technique [28]. The isolated components after segmentation are fed into a digit recognizer. The accuracy in recognizing constituent digits plays a big role in the recognition accuracy of the handwritten courtesy amount numeral string. After successful segmentation of individual digits from the numeral string, they have to be correctly recognized to get the value of the cheque. In this, there is two steps: training phase and testing phase. In training phase, handwritten images are trained. In the testing phase, the following steps need to be carried out.

- The digit in the image is centered.
- Convert two dimensional array to one dimensional array using reshape operation.
- Apply the one dimensional array to the KNN classifier.
- The digit is recognized as output.

5. EXPERIMENTAL RESULTS

The algorithms are implemented in Java. The experimental result obtained for partition scheme using the 500 × 225 gray scale cheque image is shown in figure 4. The reconstructed image has the same quality as original image. This algorithm is also useful for color images. If this algorithm is applied in color images, the algorithm is applied on each channel (Red, Blue, Green) separately. The bit depth of the share of color image is 12 bits. So this scheme is enhanced for color images also. The comparison of above schemes are described in table 2.

![Figure 4. Result of partition scheme](image)

### Table 1

| Scheme             | (k,n)  | Developing Method | Lossless | Pixel Expansion | size of share |
|--------------------|--------|-------------------|----------|-----------------|---------------|
| VCS [5]            | (k,n)  | Stacking          | No       | Yes             | Increase      |
| Extended VCS [11]  | (k,n)  | Stacking          | No       | Yes             | Increase      |
| (k, n2) [10]       | (k, n2)| Mod and Boolean / addition and comparison | Yes      | No              | same as original image |
| (2,3) [6]          | (2,3)  | Mod and Multiplication | Yes      | No              | same as original image |
| Thein-Lin [12]     | (r, n) | Shamirs SSS (Lagrange Interpolating polynomial) | No       | No              | Reduces by half |
| Boolean VSS [13]   | (r, n) | Boolean operations | Yes      | No              | Increase      |
Table 2

| Scheme      | Recovering Measure | Lossless | Pixel Expansion | size of share |
|-------------|--------------------|----------|-----------------|---------------|
| xor         | Boolean            | Yes      | No              | half of the image size |
| Partition   | Boolean            | Yes      | No              | same as cheque image |

The mean square error (MSE) is used to measure the mean square error between original (I) and recovered image (I’) and is calculated by using the equation

\[ MSE = \frac{1}{MN} \sum_{i=1}^{M} \sum_{j=1}^{N} (I'(i,j) - I(i,j))^2 \]

The MSE between original and recovered image is 0.

In the cheating detection phase, the hash value of the share images are calculated in the sender side. The value of T is 4.59080713E8. In the receiver side, the hash value is not computed. The value of T’ is computed in the receiver side. If the remainder is zero, the cheating does not occur in the shares of the cheque image. If the cheating does not occur in the shares, the cheque image is reconstructed from the shares. Otherwise, the drawee bank request for the correct shares from the participants.

In Cheque processing, the courtesy amount and account number region are recognised using image processing technique. The courtesy amount region in cheque image is shown in fig. 5.

The courtesy amount recognised in fig. 5 is 125795.75. The account number recognised in fig. 6 is 12781151507. The account number and amount is fed to the core banking software and do the transaction operations in software. Drawee bank returns the transaction details or error message to the presenting bank through Clearing House.

6. CONCLUSIONS

Cheque Truncation system accelerates the process of collection of cheques resulting in better service to customers, reduces the scope for clearing-related frauds or loss of instruments in transit, lowers the cost of collection of cheques, and removes reconciliation-related and logistics-related problems, thus benefit the system as a whole. In this paper, two secret image sharing schemes are proposed for providing security to the cheque image in the CTS. The proposed XOR scheme is simple and efficient but it is not ideal. It can be used in low storage device where memory is a constraint. The share size is only half of the original image and it is a lossless scheme. Partition scheme have the properties such as no pixel expansion and lossless scheme. The scheme is also ideal.
The experimental result shows that the proposed system provides better security and efficiency in Cheque Truncation System. The operations involved are simple XOR and it also avoids the complicated encryption decryption operations which are time consuming. The secret image sharing scheme doesn’t need any key management and authentication of the shares are done with simple hash function. The shares are also verified with the help of public parameters. We are looking forward for improved cheque processing using advanced image processing technique which helps in automatic cheque processing. The operational efficiency, speed accuracy, security and authentication are the major design objectives.

REFERENCES

1. CTS Clearing House Interface Specification, NCR Corporation and RBI/NPCI, 24th August, 2010
2. Chang-Chu Chen and Chin-Chen Chang. Secret image sharing using quadratic residues. In Intelligent Information Hiding and Multimedia Signal Processing, 2007., volume 1, pages 515–518. IEEE, 2007.
3. Sreekumar, A. Secret sharing schemes using visual cryptography. In Diss. Cochin University of Science and Technology, 2009.
4. Wei-Kuei Chen and Hao-Kuan Tso. Visual sharing protection method for medical images. Journal of medical systems, 37(1):1–8, 2013.
5. Adi Shamir Naor, Moni. Visual cryptography. Advances in Cryptology EUROCRYPT’94, pages 1–12, 1995.
6. Binu V. P and A. Sreekumar. Lossless secret image sharing schemes. International Journal of Computational Intelligence and Information Security, 2013.
7. RBI. RBI CTS. http://www.rbi.org.in
8. Cheque Truncation System. http://www.banknetindia.com/banking/chqtruncation.htm
9. Adi Shamir. How to share a secret. Communications of the ACM, 22(11):612–613, 1979.
10. Xuehu Yan, Shen Wang, Ahmed A Abd El-Latif, and Xiamu Niu. New approaches for efficient information hiding-based secret image sharing schemes. Signal, Image and Video Processing, pages 1–12, 2013.
11. Ateniese, Giuseppe, et al. Extended capabilities for visual cryptography. Theoretical Computer Science 250.1, pages 143-161, 2001.
12. Thien, Chih-Ching, and Ja-Chen Lin. Secret image sharing. Computers and Graphics 26.5, pages 765-770, 2002.
13. Chen, Tzung-Her, and Chang-Sian Wu. Efficient multi-secret image sharing based on Boolean operations. Signal Processing 91.1, pages 90-97, 2011.
14. Rigel Gjoneno, Ha.z.Malik, Nilesh Sumb, V.N. Venkatakrishnan and Rashid Ansari. Digital Check Forgery Attacks on Client Check Truncation Systems. Signal Processing 91.1, pages 90-97, 2011.
15. Pasupathinathan, Vijayakrishnan, Josef Pieprzyk, and Huaxiong Wang. Privacy Enhanced Electronic Cheque System. CEC, 2005.
16. Kota, Saranya, and Rajarshi Pal. Detecting tampered cheque images in cheque truncation system using difference expansion based watermarking.” Advance Computing Conference (IACC), 2014 IEEE International. IEEE, 2014.
17. Calin A. Sandru, 125 Neptune Drive, Suite 606, North York (CA), M6A 1X3 Apparatus and method for enhancing the security of negotiable documents. Patent No.:US 6,233,340 B1, Date of Patent:May 15, 2001
18. R. Jayadevan, S. R. Kolhe, P. M. Patil, U. Pal. "Automatic processing of handwritten bank cheque images: a survey" International Journal on Document Analysis and Recognition (IJDAR) 15.4 (2012): 267-296.
19. Chen, Yu-Chi, Du-Shian Tsai, and Gwoboa Horng. "Visual secret sharing with cheating prevention revisited.” Digital Signal Processing 23.5 (2013): 1496-1504.
20. Chen, Yu-Chi, Du-Shian Tsai, and Gwoboa Horng. "A new authentication based cheating prevention scheme in Naor-Shamir’s visual cryptography.” Journal of Visual Communication and Image Representation 23.8 (2012):
21. Zhao, Rong, et al. "A new image secret sharing scheme to identify cheaters." Computer Standards & Interfaces 31.1 (2009): 252-257.

22. Wu, T-C., and T-S. Wu. "Cheating detection and cheater identification in secret sharing schemes." Computers and Digital Techniques, IEEE Proceedings. Vol. 142. No. 5. IET, 1995.

23. Ahmed, Fawad, Mohammed Yakoob Siyal, and Vali Uddin Abbas. "A secure and robust hash-based scheme for image authentication." Signal Processing 90.5 (2010): 1456-1470.

24. Askari, Nazanin, Cecilia Moloney, and Howard Heys. "Application of visual cryptography to biometric authentication." 2011.

25. Fatma, E-Za Elgamal, Noha A. Hikal, and F. E. Z. Abou-Chadi. "Secure Medical Images Sharing over Cloud Computing environment." International Journal (2013).

26. Guo, Huiping, and Nicolas D. Georganas. "A novel approach to digital image watermarking based on a generalized secret sharing scheme." Multimedia Systems 9.3 (2003): 249-260.

27. Horng, GwoBoa, Tzungher Chen, and Du-Shian Tsai. "Cheating in visual cryptography." Design, Codes and Cryptography 38.2 (2006): 219-236.

28. Larose, Daniel T. "kNearest Neighbor Algorithm." Discovering Knowledge in Data: An Introduction to Data Mining (2005): 90-106.

29. Lee, Yuchun. "Handwritten digit recognition using k nearest-neighbor, radial-basis function, and backpropagation neural networks." Neural computation 3.3 (1991): 440-449.

30. Guillevic, Didier, and Ching Y. Suen. "HMM-KNN word recognition engine for bank cheque processing." Pattern Recognition, 1998. Proceedings. Fourteenth International Conference on. Vol. 2. IEEE, 1998.

S R Sreela is a Research Scholar in the Department of Computer Science, Cochin University of Science and Technology (CUSAT). She holds a Bachelor Degree in Information Technology and Masters Degree in Computer and Information Science. Her research area includes image processing, secret sharing and security.

Dr. G. Santhosh Kumar received his MTech Degree in Computer and Information Science from CUSAT, in 1999 and PhD in Wireless Sensor Network from Cochin University of Science and Technology.

Currently he is working as an Associate Professor in CUSAT. He had more than 15 years of teaching experience. His research interest includes Wireless Networks, Mobile Communications and Software Architecture.

V P Binu is a Research Scholar in the Department of Computer Applications, Cochin University of Science and Technology (CUSAT). He holds a Bachelor Degree in Computer Science and Engineering and Masters Degree in Computer and Information Science. His research area includes cryptography, secret sharing and security.