Banknote authentication using chaotic elements technology.

AMBADIYIL, S., KRISHNENDU, P.S., PILLAI, V.P.M., PRABHU, R.

2017

Banknote Authentication Using Chaotic Elements Technology

Sajan Ambadiyil[a], Krishnendu P S[b],V P Mahadevan Pillai[c] and Radhakrishna Prabhu[d]
[a]Center for Development of Imaging Technology, Thiruvananthapuram-695027, Kerala, India
[b]Jawaharlal College of Engineering and Technology, Palakkad-679301, Kerala, India
[c]Department of Optoelectronics, University of Kerala, Thiruvananthapuram-695581, Kerala, India
[d]Robert Gordon University, School of Engineering, Aberdeen, United Kingdom

ABSTRACT

The counterfeit banknote is a growing threat to the society since the advancements in the field of computers, scanners and photocopiers, as they have made the duplication process for banknote much simpler. The fake note detection systems developed so far have many drawbacks such as high cost, poor accuracy, unavailability, lack of user-friendliness and lower effectiveness. One possible solution to this problem could be the use of a system uniquely linked to the banknote itself. In this paper, we present a unique identification and authentication process for the banknote using chaotic elements embedded in it. A chaotic element means that the physical elements are formed from a random process independent from human intervention.The chaotic elements used in this paper are the random distribution patterns of such security fibres set into the paper pulp. A unique ID is generated from the fibre pattern obtained from UV image of the note, which can be verified by any person who receives the banknote to decide whether the banknote is authentic or not. Performance analysis of the system is also studied in this paper.

Keywords: Chaotic element, Counterfeiting, Authentication, Banknote, SURF, Image Registration, Feature extraction,

1. INTRODUCTION

A counterfeit banknote is an imitation intended to be passed off fraudulently or deceptively as genuine. Newspaper reports that the growing menace of banknote counterfeiting is increasing day by day. The advancements in the field of computers, photocopiers and scanners have made duplicating banknote very simple. The counterfeiters are becoming harder to track down because of their rapid adoption and adaptation of highly advanced technologies. There are many devices to detect the fake notes. But, only some particular institutions can make use of these devices. Other fake banknote detection systems developed so far have the least acceptance situation among the end-users due to the unavailability, high cost, poor accuracy and lack of user-friendliness. Moreover, the effectiveness of these techniques is decreasing, mainly because of the advancements in reprographic technologies. Thus, the unsuspecting masses have no efficient mechanism of differentiating the fake from the genuine [1][2].

One possible solution to this problem could be the use of a system uniquely linked to the banknote itself and use of easily available and efficient counterfeit detection tools/software for verification. To do this, it is necessary for a single banknote to find unique, unrepeatable, and unchangeable characteristics. If these features are present, it is possible to identify the banknote and to distinguish it from the others [3][4][5]. Using this approach, it is possible for mass products like banknotes to have a high-security element, which remains secure for an extended period, easy to produce and to use. In this paper, a unique identification and authentication technology for the banknotes is reported, utilising chaotic elements present in it. A chaotic element means that the physical elements are formed from an entirely random process independent from human intervention. Chaotic elements are physically unclonable. Because of the randomness, it is practically impossible to duplicate physical unclonable function (PUF), even given the exact manufacturing process that produced it [6][7][8]. Indian banknotenotes have an invisible security fibre embedded into it during the manufacturing process which is visible only under Ultra Violet (UV) light. These invisible security fibres have a random pattern [9]. Just like the human biometric traits that have a random pattern and are unique for each, the security fibre pattern is also unique for each currency. Such random features that are unique and display the property of randomness from the chaotic elements and can be used in the process of authentication. The chaotic elements used in this paper are the random distribution pattern of the security fibres set into the paper pulp. From the UV image of the banknote, features with chaotic properties are extracted. These features are converted into a numerical value and then encrypted. The result is used to create the unique ID in the form of a Quick Response (QR) code, and this is printed on the banknote during the production. The authenticity of the banknote can be verified by any person who receives the note.

2. THE PROPOSED METHOD

In the proposed system, the chaotic elements in the banknotes are exploited for the authentication and unique identification. These unique features are extracted and converted into a QR code which is imprinted on the banknote. This QR code can be verified for authentication of a banknote possessed by the end user. The whole system can be broadly divided into three phases as follows:

- QR code generation phase: During this juncture, features with chaotic properties are extracted from the image of the banknotes. This feature is then converted into numerical value, encrypted and converted to the QR code.
- QR code integration phase: During this juncture, QR code having encrypted features of chaotic properties is integrated into the banknotes
- QR code verification phase: During this juncture, QR code from the received banknote and an image of the banknote are given as input. If the information from the image and the QR code output from the scanned document are matched, the banknote is authenticated.

2.1 QR code generation phase

After identifying the features that form the chaotic element in the banknote, they are extracted in a standardized manner. Then these extracted features are converted to numerical values. These numerical values are encrypted. The resulting cipher text is used to generate a unique ID in the QR code format using any QR code generating software. Fig. 1 illustrates the block diagram of the generation phase.

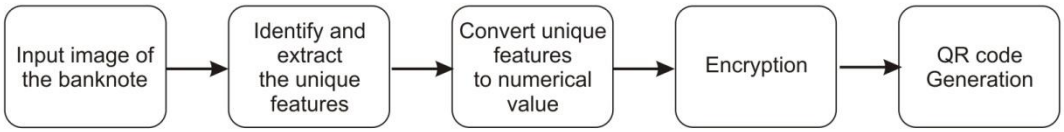

Fig.1 Generation of the QR code

The detailed image processing steps involved in the QR code generation is shown in Fig. 2. The whole procedure can be classified into three main stages: (1) Image acquisition, (2) Feature extraction, (3) Encryption and QR code generation.

2.1.1 Image acquisition

The banknote image can be obtained using a UV lamp and a camera. The UV source used in the experiment emits light of wavelength 366 nm.

2.1.2 Feature extraction

This stage is the main functional item of the system. All image processing steps are carried out during this juncture. This stage can be again sub divided into the following steps:

- Image registration
- ROI extraction
- Fibre detection
- Conversion to numerical value

(a) Image registration

The process of geometrically arranging two or more images into the same outlook is known as Image registration. The images captured at different instants show misalignment as the capturing device, angle and time at which they are taken are different. In order to align these images, image registration can be effectively applied. Here, one of the images is set as the reference image and other images are brought into line with the reference image. This is done by mapping feature points of reference and input images, defining a transformation corresponding to matched points and applying this transform to recover the scale and angle of given image. Image registration can be a feature-based or intensity-based mechanism. Feature-based image registration using SURF (Speeded Up Robust Features) is employed in the proposed

system. SURF is a local feature detector and a descriptor is used for tasks such as object recognition or registration or classification or 3D reconstruction [10].

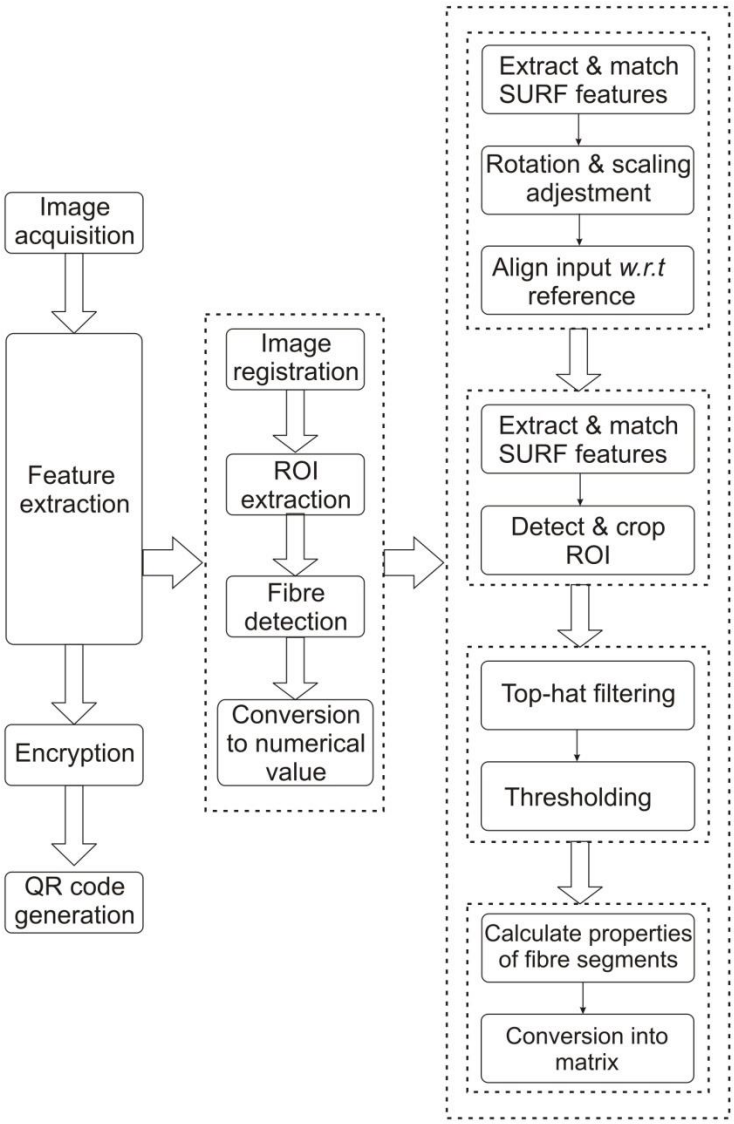

Fig. 2 Detailed image processing steps involved in the QR code generation

(b) ROI extraction

The main challenge faced while separating fibre portions from rest of the image is that the banknote image bears some portion with same intensity value as that of the fibre. So a suitable Region of Interest (ROI) should be specified to separate the desired fibre portions. The ROI is selected such that fibre intensity values at that region of currency are clearly distinguishable. Fig. 3 shows the required ROI in the UV image of currency. The ROI is detected using SURF features, and then it is cropped out. A reference image of the required ROI is matched with the input image by finding point correspondences between both images. A corresponding transformation is obtained and then boundary points of the reference image are transformed into the coordinate system of the input image. The transformed points thus obtained indicate the location of the ROI in the given input.

Fig. 3. UV Image of a banknote with ROI

(c)Fibre detection

To extract fibre portions, we use image enhancement techniques. Here, to enhance the image, the Top-Hat transform is used. Top-hat transform is a morphological operation which is used to extract small elements and details from images. There are two types of top-hat transforms - white and black. The white top-hat transform or peak detector highlights objects brighter than their surroundings in an image by subtracting the image opened by the structuring element from the original image. The black top-hat transform or valley detector highlights darkest areas in an image by taking the variation between the closing and the input image. The white top-hat transform is used here since the fibre portions are brighter than their surroundings. The block diagram of top-hat filtering is shown in Fig. 4.

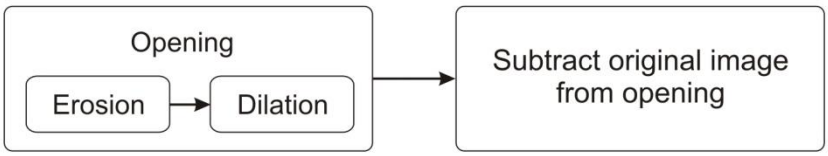

Fig. 4. Block diagram of top-hat filtering.

The top-hat filtered image is then applied a threshold to separate the fibres out. The suitable threshold is determined by plotting the intensity profile of the filtered image. On applying the threshold, the result obtained is a binary image with logic 1 at the portions where fibre segments are present and logic 0 at portions where they are absent

(d) Conversion into numerical value

The random pattern of fibre distribution is described using n- tuple vectors. These vectors are generated using the properties of fibre segments obtained after thresholding and binarising. The properties used are the following:

- Centroid (C)
- Area (A)
- Eccentricity (E)
- Orientation (O)
- Extrema (Ex)

The resultant is a matrix having number of rows is equal to the number of fibre segments. Fig. 5 shows the block diagram for the numerical value conversion

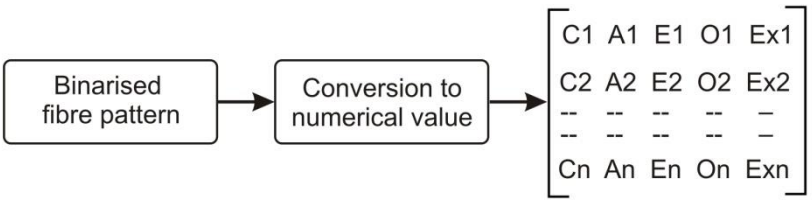

Fig. 5. Block diagram of conversion to numerical value.

2.1.3 Encryption and QR code generation

The matrix with data values corresponding to the fibre patterns is encrypted using RSA crypto system. RSA is a public key cryptographic algorithm that can be used to encrypt and decrypt messages. RSA comes from the names of three creators Rivest, Shamir and Adleman. It is an asymmetric algorithm and uses a pair of keys: a private key and the public key. RSA implements a public-key cryptosystem that allows secure communications and digital signatures [11]. The cipher text is provided as input to the QR code generation software to obtain corresponding QR code as shown in Fig. 6.

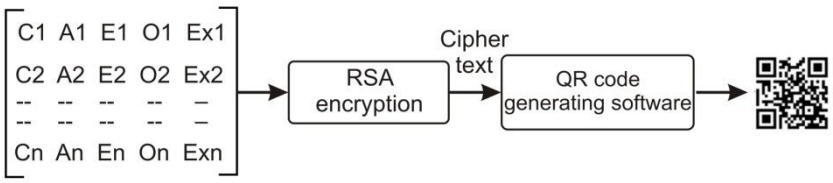

Fig. 6. Block diagram of encryption and QR code generation.

2.2. QR code integration phase

During the banknote production, major steps involved are security paper production, printing, and cutting and finishing of the banknote. At every stage of the banknote production, the primary aim is to ensure that the banknote is as difficult as possible to counterfeit. The primary ingredient of the banknote is "paper", which is in fact made from special cotton fibres. This is what gives the banknotes their distinctive "feel" and crispness, as well as durability. While producing the paper, certain security features, such as watermarks, security optical fibres or embedded threads, are integrated into the paper itself. During the paper preparation, the security fibres are put inside the paper in a non-scalable manner; their distribution, position and number are random. Then the banknote paper is distributed to high-security printing works. The main processes are offset silkscreen and intaglio printing. After this, the process of letterpress printing is used for the cipher and serial numbers on the front of the banknote. Finally cutting and finishing followed by the final inspection and quality checking makes the banknote ready for circulation. To generate the unique QR code in the bank note, the image capturing devices can be integrated into, between the final printings to numbering stages as shown in Fig. 7. In synchronism with the mechanical numbering device, the Variable Data Printing Device (VDP) prints the unique QR code to the banknote in a convenient position of the banknote

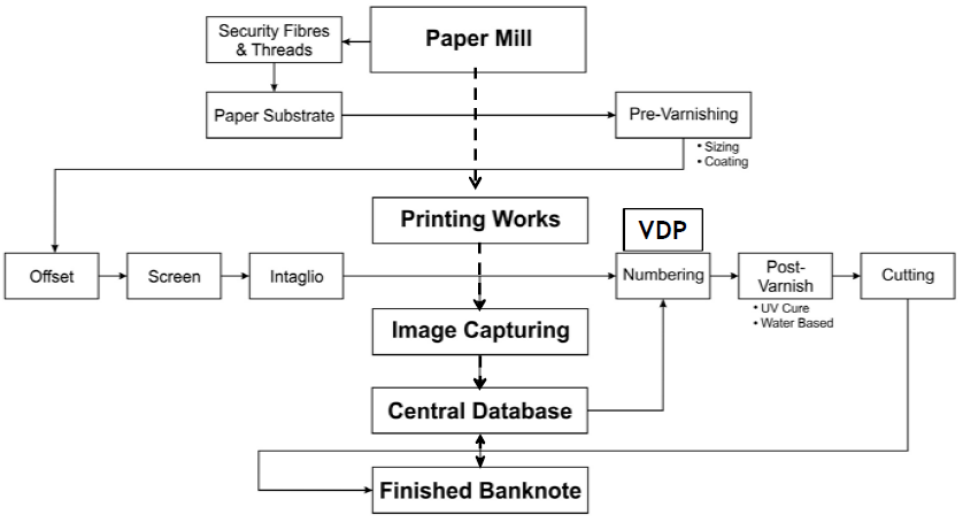

Fig. 7 Stages of banknote production and QR code integration

2.3 QR code Verification stage

During the verification, the authenticity of the banknote is tested. The input to the verification system is the banknote with QR code embedded in it. First, the QR code alone is taken and decoded to get the numerical value. Then, the UV

image of the same note is obtained and the feature extraction steps used in QR code generation stage are applied. The numerical values obtained from QR code and the UV image are then correlated and compared for equality to determine whether the banknote is original or fake. The numerical values obtained are in the form of matrices. Each row in the obtained matrices corresponds to the properties of the corresponding fibre segments. To find the match between the two matrices, each row of the first matrix is compared with every row of the second matrix. For each row of the first matrix, a row with maximum correlation is obtained from the second matrix. The corresponding rows are compared for equality with a tolerance of +/- 5. If the match is greater than 75%, the banknote is authentic. Otherwise, the banknote is fake.The flow chart for the verification process is shown in Fig. 8.

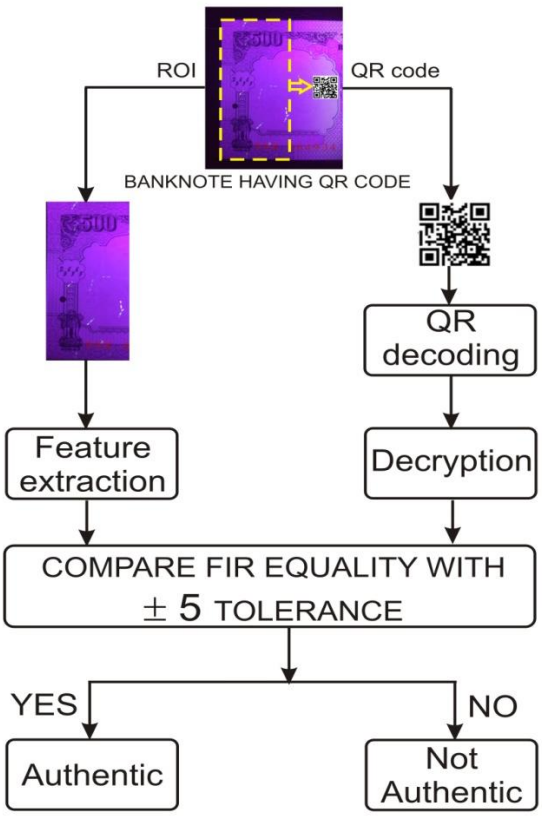

Fig. 8. Block diagram of QR code verification stage.

3. ANALYSIS AND DISCUSSION

To analyze the proposed system, UV images of more than ten banknotes were collected, and their corresponding fibre patterns were extracted. To check the authenticity of the method ten fibre pattern samples from each of these banknotes were also collected. The proposed system is evaluated by finding out the following parameters.

3.1 Score

The score is calculated to verify whether the two banknote images are matching and is given by:

$$Score = \frac{Number\ of\ matched\ fibre\ elements}{Total\ number\ of\ fibre\ elements}$$

Higher value of score indicates that the similarities between two images are high. Here we take two UV images of currency notes as matched if score is greater than 75. If more than 75% of the fiber elements in two images are matched, the images are assumed to be that of the same currency note. Otherwise, they are assumed to be that of different bank notes.

3.2 False Acceptance Rate (FAR)

FAR is the outcome when the system accepts an identity claim that is not actually the true identity. It is the ratio of number of times the system incorrectly declares a successful match between two non-matching images, to the total number of images. FAR is given by ratio.

$$FAR = \frac{Number\ of\ false\ matchings}{Total\ number\ of\ images}$$

Procedure employed to find FAR

- Select a UV image of a currency.
- Select images of 10 different banknotes. This is the database.
- Look the matching between the selected image with the 10 other images
- If there is a match with any of the other images in database it is a false match.

In the above mentioned way the FAR for about 10 banknotes were obtained. Ideally the value of False Acceptance Rate must be very low. Low False Acceptance Rate indicates that the system does not falsely match the fingerprints of two different individuals. Fig. 9(a) shows the graph for False Acceptance Rate of the proposed system.It can be seen from the graph that the average False Acceptance Rate of about 3%. It is a very low value and hence system shows good false acceptance properties.

3.3 True Acceptance Rate (TAR)

True acceptance happens if system accepts identity of a genuine banknote. It is given by the ratio.

$$TAR = \frac{Number\ of\ true\ matchings}{Total\ number\ of\ images}$$

Procedure is as given below:

- Take 11 UV images of the same note.
- Take one of these image as the base image
- Find matching between the base image and 10 other images.
- Find the number of times the images are matched. Ideally all the images must show match.

The above mentioned procedure was repeated for 10 images to find the TAR. The obtained valuesare shown in Fig. 9(b). TAR must ideally be very high. High TAR indicates that when a particular image of a given note is compared with other images in the database the system shows matching. The value of TAR is high here with an average value of almost 92%.

3.4 False Rejection Rate (FRR)

False rejection happens when the identity claim of the true identity is rejected. FRR is given by the ratio.

$$FRR = \frac{Number\ of\ times\ true\ identity\ is\ rejected}{Total\ number\ of\ images}$$

Procedure for determining FRR is as given below:

- Take 11 UV images of the same note.
- Take one of these image as the base image
- Find matching between the base image and 10 other images.
- Find the number of times the images show non-matching. Ideally there should not be any non match.

The above procedure was repeated for 10 banknotes and that is used to calculate FRR. The value of FRR must be low. The obtained results are shown in Fig. 9(c).The proposed system has a low FRR. Low FRR means that the system will not show match if an image of given banknote is compared with another banknote image in the data base. Hence the system proposed here gives good false rejection performance. The average FRR value of the present system is around 8%.

3.5 True Rejection Rate (TRR)

True rejection means that the claim of false identity is rejected. If an image of a given banknote is compared with images of 10 different notes then it should not show a match. This can be obtained by the ratio.

$$TRR = \frac{Number\ of\ times\ false\ identity\ is\ rejected}{Total\ number\ of\ images}$$

Procedure to find TRR

- Select a UV image of a currency.
- Select images of 10 different banknotes. This is the database.
- Look the matching between the selected image with the 10 other images
- If after the comparison with images of other bank notes it is not matched it is called as false identity rejection.

Here, in order to analyze the system, the above procedure is repeated for about 10 notes and using the result TRR is calculated. The result of TRR is shown in Fig. 9(d). It can be seen from the graph that the values of TRR of the proposed system are very high. Ideally the value of TRR must be high because a high TRR indicates that the system does not match fibre patterns of two different banknotes.

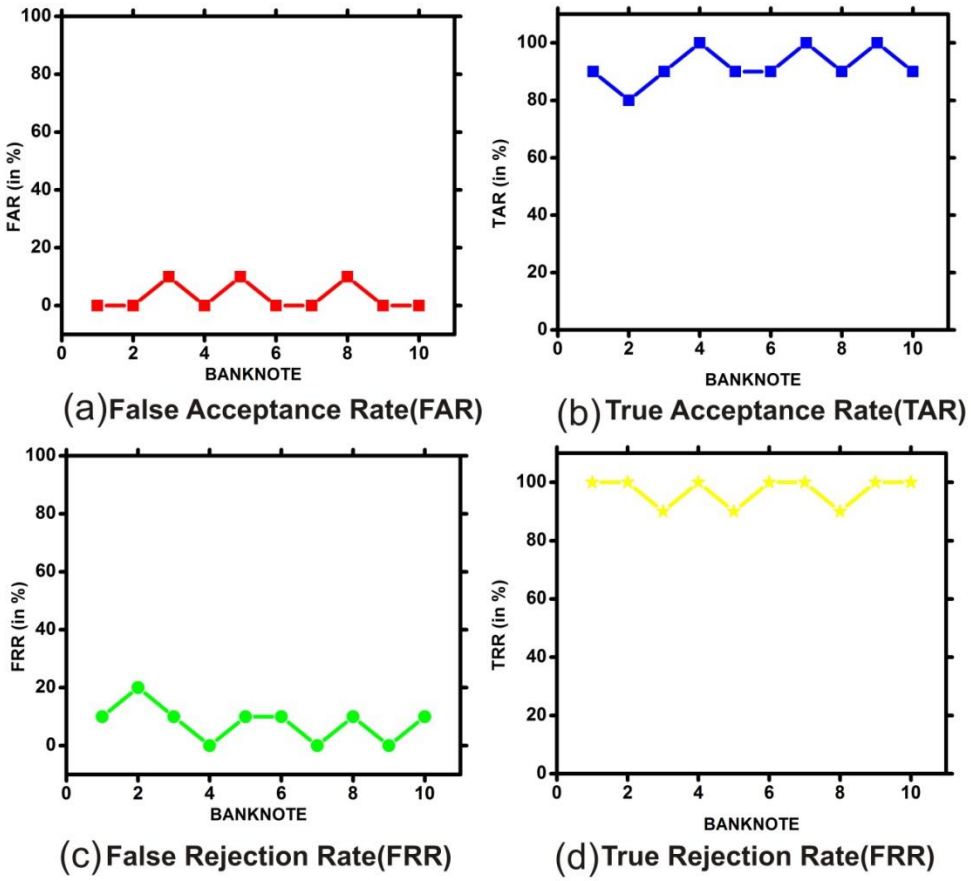

Fig. 9 (a) False Acceptance Rate (b) True Acceptance Rate (c) False Rejection Rate (d) True Rejection Rate

The values of performance parameters evaluated for the proposed system are satisfactory. Ideally, the values of False Acceptance and False Rejection must be low and True Acceptance and True Rejection Rates must be high. From the analysis, it can be seen that the system satisfies the standard requirements. Thus the proposed system presents a cost effective, robust method for banknote authentication.

4. CONCLUSION

In this paper, authentication and unique identification of the banknote are achieved using the chaotic elements present in it. Most of the banknotes have an invisible security fibre embedded into it during the manufacturing process which is visible only under Ultra Violet (UV) light. These invisible security fibres generate a random pattern which is unique for each note. The chaotic elements used in this paper are the random distribution pattern of the security fibres set into the paper pulp. The features of the chaotic element are extracted, encrypted and converted to QR code and embedded on the banknote as a unique ID. The system performance was evaluated using different parameters, and the result was found to be satisfactory. Apart from security, such unique ID can facilitate automation, secure track and trace, effective maintenance of inventory at various levels; knowledge based identification and added protection. This technology can also be integrated with smart phones which enables the public for easy and automated verification of banknotes. The proposed system thus presents a cost effective, robust method for banknote authentication.

REFERENCES

[1] Mahajan S., Rane K. P., "A Survey on Counterfeit Paper Banknote Recognition and Detection," in International Conference on Industrial Automation and Computing (ICIAC), Nagpur, April (2014).

[2] Alekhya D., Prabha G. D. S., Rao G. V. D., "Fake Currency Detection Using Image Processing and Other Standard Methods," IJRCCT 3(1), January (2014).

[3] Bulens P., Standaert F. X., Quisquater J. J., "How to strongly link data and its medium: the paper case," IET Inf. Secur. 4(3), 125–136 (2010)

[4] Sharma A., Subramanian L., Brewer E. A., "Paper-Speckle: Microscopic Fingerprinting of Paper," CCS'11, October 17–21, Chicago, Illinois, USA (2011).

[5] Clarkson W, Weyrich T, Finkelstein A, Heninger, Alex Halderman J, Felten E.W, "Fingerprinting Blank Paper Using Commodity Scanners," Proc. IEEE Symposium on Security and Privacy, May (2009).

[6] Pappu R., "Physical one-way functions," PhD thesis Massachusetts Institute of Technology, (2001)

[7] Herder C, Yu M. D., Koushanfar F., and Devadas S., "Physical Unclonable Functions and Applications: A Tutorial," Proceedings of the IEEE, 102(8) August (2014).

[8] Maes R., Verbauwhede I., "Physically Unclonable Functions: a Study on the State of the Art and Future Research Directions," Towards Hardware-Intrinsic Security. Information Security and Cryptography Sadeghi A R., Naccache D. (eds). Springer, Berlin, Heidelberg (2011).

[9] Spagnolo. G. S, Cozzella L., and Simonetti C., " Banknote security using a biometric-like technique: a Hylemetric approach," Meas. Sci. Technol., 21(5), 055501(2010).

[10] Bay H., Ess A., Tuytelaars T., and Gool L. V., "Speeded-Up Robust Features (SURF)," Elsevier,10 September (2008).

[11] Stallings W., [Cryptography and Network Security Principles and Practices], Prentice Hall (2005).