Secure User Authentication using Sclera in Quick Response Codes

S.Brindha[#1], Dr.Ila.Vennila[*2] and B.Nivedetha[#3]

# Department of Computer Networking, PSG Polytechnic College,
Coimbatore, India
[1] hod@dcn.psgtech.ac.in [3] vini_2019@yahoo.co.in
* Department of Electrical and Electronics Engineering, PSG College of Technology,
Coimbatore, India
[2] iven@eee.psgtech.ac.in

Abstract - **In this paper, an authentication method using sclera embedded in Quick Response codes is proposed. Quick response codes are two dimensional barcodes which can hold more data and can be fastly readable by Personal computers and Handheld devices like mobile phones, smart phones and tablet PCs. Biometrics though noted for their accuracy suffer from the innate disadvantage of time consumption during enrolment and verification process. Together Biometrics and QR codes will provide a fast authentication system. This approach will be suitable for mobile ticketing applications. Cancelable sclera templates have been embedded in Quick Response codes and used for two factor authentication. The proposed Cancelable sclera template embedded in Quick response codes approach was evaluated using publicly available UBIRIS and IUPUI multi wavelength database. The experimental results show that this technique is efficient and provides accurate identity verification than other biometric traits.**

Keywords-Biometrics, Sclera, QR code, Cancellable Template, Authentication, Mobile Ticket.

I. Introduction

New generation smart phones possess a unique two dimensional (2D) barcode, or Quick Response (QR) [1] code which can be used for a multitude of applications technology. Phones that are equipped with a QR code reader have the ability to quickly scan an appropriately embedded barcode. To enable the mobile phone to understand what action it needs to take when the QR-Code is scanned a service type is embedded within the QR-Code. By scanning the QR code depending on the type of data recognized and the nature of the application, alternative actions can follow the decoding stage: a phone number can be automatically dialled, a short text message can be sent, a web page corresponding to the decoded URL can be displayed in a mobile browser, or a definite application can be executed.

QR codes can be used for a variety of applications in mobile commerce like ticketing, banking, purchasing and advertisement. Mobile Ticketing applications [2] require personnel to authenticate the ticket. Automatic identification without human involvement will considerably increase the speed and user convenience. In this paper QR codes with embedded cancellable sclera codes have been used for authentication.

The QR codes can be scanned on mobile devices [4] such as smartphones and tablet PCs. The content of the QR code will be an authentication token which the user will use in his/her entry card. On successful authorization, the access token is validated for that particular user account. The QR code can also be printed on a paper document, such as a nominative ticket. A nominative train ticket using QR code is shown in Fig.1.

Fig. 1. Ticket with QR code

During verification the sclera image of the user is taken as input, to represent the owner of the document, and compared with the information stored in the QR code to verify automatically the identity of its owner. In other words, this mechanism allows to verify quickly the claimed identity of the person holding the paper document (such as an admission ticket), without requiring human intervention, by just comparing locally the output of his/her sclera scan with the data stored in the document itself. There are few typical scenarios for this application. For example, there are several cases of sports and recreational events, temple services with nominative admission tickets. Such tickets are to be used only by the nominated person, but authentication has to be done for huge population in the temple or sports premises. In such cases the mobile ticketing with automatic verification will be of great use.

In addition, the biometric data can be secured within the barcode by using either digital signature or other cryptographic algorithms, in order to prevent malicious tampering. Note that neither a network connection nor a remote repository is needed as the QR code is able to store enough biometric information [3] which is necessary for discriminating people on the basis of their sclera features.

New mobile capabilities enable its users to buy tickets and also gain access to concerts, sporting events, and other live performances without even having to touch a piece of paper. This type of authentication can be used for high security access like military, research centres, scientific organisations etc.

II. QR CODE TECHNOLOGY

QR Code (2D Code) contains information in both the vertical and horizontal directions, whereas a bar code contains data in one direction only. QR Code holds a considerably greater volume of information than a bar code. QR (Quick Response) code is the trademark name for the two dimensional barcode systems. It was originally invented in 1994 by Denso Wave [1], a Toyota subsidiary, as a way to track vehicles as they were assembled, and to scan components at high speeds.

The code consists of black modules arranged in a square pattern on a white background. The information encoded can be made up of any kind of data (e.g. binary, alphanumeric, or Kanji symbols). The QR code was designed to allow its contents to be decoded at high speed. The technology has seen frequent use in Japan and South Korea and United Kingdom. A QR-code is structured in a standard manner, which is briefly sketched on the Figure below (Fig.2):

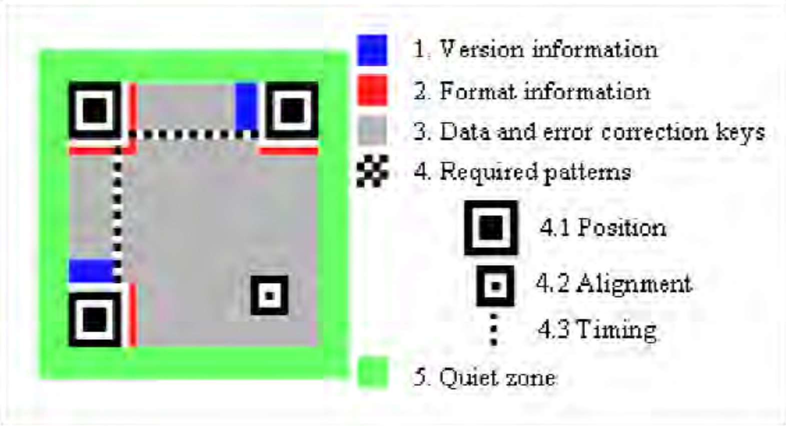


Fig. 2. Structure of QR code

The three large squares act as alignment targets, while the smaller square in the remaining corner acts to normalize the size and angle of the shot. As shown in Fig. 2, the strips near the alignment squares contain formatting information, and the remaining area is the actual data that is converted into binary code and checked for errors before being displayed. QR Code is faster to read than other two-dimensional code, because it contains three large square patterns in the corners that are used for position detection. Additionally, the patterns are used to detect the size, the angle and the outer shape of the symbol. When a reader scans a symbol, it first detects these patterns. Once the position patterns have been detected the scanner can rapidly read the inside-code in all directions. The inside code consists of several small blocks where the information is encoded. The encoded data can be interpreted as one of four primary modes - numeric, alphanumeric, byte/binary, and Kanji. Other forms of data can also be displayed with the appropriate extensions.

As QR code technology evolved, it began to contain more and more information. The initial version was 21 x 21 pixels and held just 4 characters worth of data. The most recent version is 177 pixels square, and it holds 1852 characters—enough for a few pages of information. Specifically, its capacity can encode 7089 numeric characters for numeric data alone. The QR code has many desirable features such as high capacity encoding of data, small printout size, Chinese/Japanese _kanji and kana_ capability, dirt and damage resistance, readability from any direction in 360°, and a structure append feature. QR code can be easily generated using free on-line generators. They can be printed on plain paper using an ordinary printer and attached to any object.

III. SCLERA BIOMETRICS

Biometric authentication uses data taken from measurements of a person’s body, such as fingerprints, faces, irises, retinal patterns, palm prints, voice prints, hand-written signatures and so on, to identify individuals by means of image processing. Such data is unique to the individual and remains throughout one’s life. It is important to have reliable personal identification due to growing importance of information technology.

The sclera [10] is the white portion and it completely surrounds the eye as opaque outer protective covering of the eye. They are made up of four layers of tissue — the episclera, stroma, lamina fusca, and endothelium. For young children, the sclera blood vessels are blue in color and for adults it is red in color. The goal of this sclera recognition system is to identify and extract the vein portions of sclera from the original eye image for processing and identification.

Sclera is the most popular modality that is widely used in various authentication Applications; Aadhaar identification card, gate access control systems, and so on. The reason can be considered that sclera can achieve the best balance among authentication performance, cost, size of device, and ease of use. However, most of iris authentication has some problems to be solved. One is that iris can be spoofed easily by using fake lenses and it can degrade authentication performance. The other problem is that when medically pupil or contour region gets affected, it has been pointed out. To solve these problems, an algorithm is developed as new sclera authentication that has a novel sensing principle. Sclera recognition can achieve comparable recognition accuracy to iris recognition in the visible wavelengths. The goal of this section is development of a system that can consistently identify users from their extracted vein pattern descriptors in the presence of noise, unusual vein presentations, and deformations.

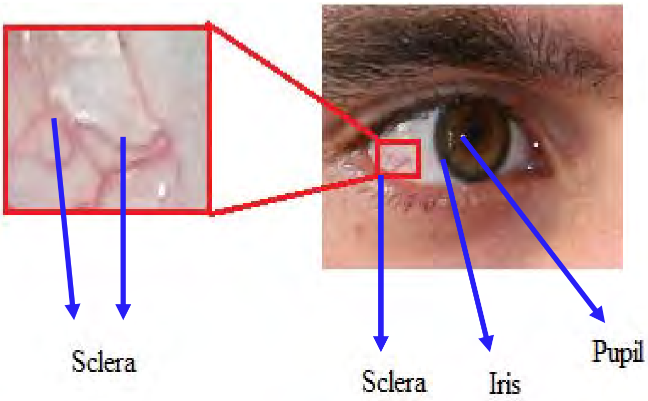


Fig. 3. Human eye pattern

The blood vessel structure of the sclera is shown in Fig.3. which is unique to each person, so it is well suited for biometric identification. Eye image can be remotely obtained non-intrusively in the visible wavelengths. In this work, we have proposed new sclera recognition for human ID. Acquisition of sclera vessel patterns are quite challenging because the images are often defocused and saturated since the vessel structure of sclera image is multilayered and has complex nonlinear deformations.

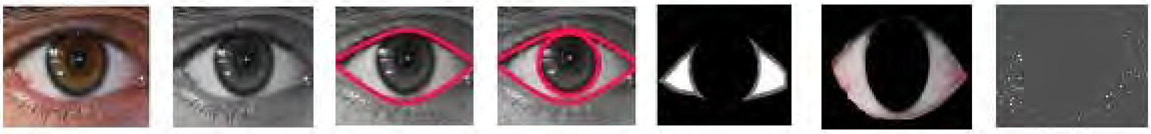
Automated sclera recognition is yet another alternative for non-invasive verification and identification of people. Images of the individual's eyes, whose complex random patterns are unique and can be seen from some distance, are used for authentication. It is completely safe for all, including those who wear glasses, use contact lenses and children.

IV. CANCELABLE SCLERA CODE

To segment the sclera from eye image the process involved are segment sclera, extract sclera features and enhance the vessel patterns, matching the features of sclera veins, and decision matching. First we have to downsample the UBIRIS database image, this downsampling reduces the size of original image to required size. The image is converted from the RGB colorspace to HSV colorspace. Second, detect the eyelid boundary and segment iris region using active contour method. Gabor filter is used for extraction of vein pattern from the segmented sclera region and enhanced. The enhanced vein patterns are thresholded using an adaptive threshold method to emphasize and binarize the sclera vein pattern, and thinned to a pixel wide skeleton using morphological operations as shown in Fig.4.

Finally, line descriptor based feature extraction method is used to describe and store the extracted vein pattern for recognition, registration, and matching method that is scale, orientation, and deformation-invariant, and can mitigate the multi-layered deformation effects and tolerate segmentation error. The feature matching system uses an enrolment system to register the sclera vein templates [9] to achieve translation, rotation, and scaling-invariance. Then, cross-correlation distance measure is used to match the templates using their line descriptor sets. Finally, the matching score is determined from the weighted matching scores.

Although biometrics-based authentication systems exhibit many usability advantages over traditional authentication systems, they suffer from several security and privacy concerns [7]. As a result, many template protection techniques have been proposed in the last few years to deal with these issues. Cancellable biometrics attempt to solve this by constructing revocable biometric templates. Cancellable biometrics [6] refers to the intentional and systematically repeatable distortion of biometric features in order to protect sensitive user-specific data. If a cancellable feature is compromised, the distortion characteristics are changed, and the same biometrics is mapped to a new template, which is used subsequently.



(a) (b) (c) (d) (e) (f) (g)

Fig. 4. (a) Input eye image (b) Grayscale image (c) Eyelid detection (d) Iris boundary detection (e) Sclera mask (f) Segmented Sclera (g) Vessel pattern- after morphological operation

```
  000001000000000110000000100000001000000000001000000110000000100000000110000000000000011
100000110000011100000111000001110000011100000110000001110000001100000110000000011000011
1000000011111110000000000110001000001001000000000110000000100010000000010000000000000101
```

Fig. 5. Generated 256 bit key

As shown in Fig. 5, a 256 bit cryptographic key [5] is generated for sclera vein pattern. The last step of the proposed sclera recognition system is the generation of the k-bit cryptographic key from extracted sclera vessel patterns template BT. The template vector BT can be represented as, BT = [b_{T1} b_{T2} ..… b_{Th}]

The set of distinct components in the template vector BT are identified and are stored in another vector UBT.

$$U_{BT} = [\, u_1\ u_2\ u_3 \ldots u_d \,];\ |UBT| \leq |BT|$$

The vector UBT is then resized to k components suitable for generating the k-bit key. The resize procedure employed in the proposed approach,

$$B = \begin{cases} [u_1\ u2 \ldots u_k] & ;\ \text{if } |U_{BT}| > k \\ [u_1\ u2 \ldots u_d] \ll u_{i;}\ d+1 \geq i \geq k & ;\ \text{if } |U_{BT}| < k \end{cases}$$

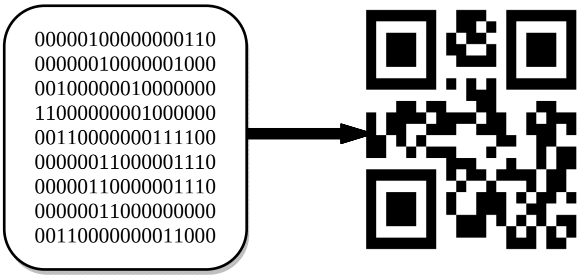
Where $u\,\text{i} = \frac{1}{d}\sum_{j=1}^{d} \text{U}\, j$

Finally, the cryptographic key K_B is generated from the vector B as,

$$K_B \ll B_i \bmod 2,\ i = 1, 2, 3 \ldots k$$

V. IMPLEMENTATION

In order to test the effectiveness of the proposed approach, experiments were conducted using sclera codes embedded in QR codes. QR code was generated using online QR code generating software [2].The Kaywa QR code generator was used in this experiment. The sclera code is given as input and QR code of size 300*300 was generated. The sample QR code is shown in Fig. 6.



```
00000100000000110
00000010000001000
00100000010000000
11000000001000000
00110000000111100
00000011000001110
00000110000001110
00000011000000000
00110000000011000
```

Fig. 6. QR code with embedded sclera code

The generated QR code can be issued to the user as a nominative ticket. The publicly available UBIRIS and IUPUI multi wavelength database was used in the experiments. The image quality in this database varies due to illumination, sharpness and other factors. For the same eye we have good quality, mid quality and poor quality images [11]. The images are 800*600 color images The algorithm in this proposed method are implemented using MATLAB (version 2011a) on a PC with Intel Core2 CPU, 1.86GHz processor,1GB RAM. The QR code decoding was implemented both in mobile phone and PC. The mobile phone used was Samsung Galaxy Duos mobile phone with android 4.0 operating system, 1 GHz processor and 512MB RAM.

As we are focusing our proposed authentication system for large population where users can bring their nominative tickets in any form i.e., either in paper or through their mobile phones, the QR codes can be decoded from various input forms using QR code reading software. If the matching is successful, the user will be authenticated. The process of encoding and decoding [8] is shown in Fig. 7.

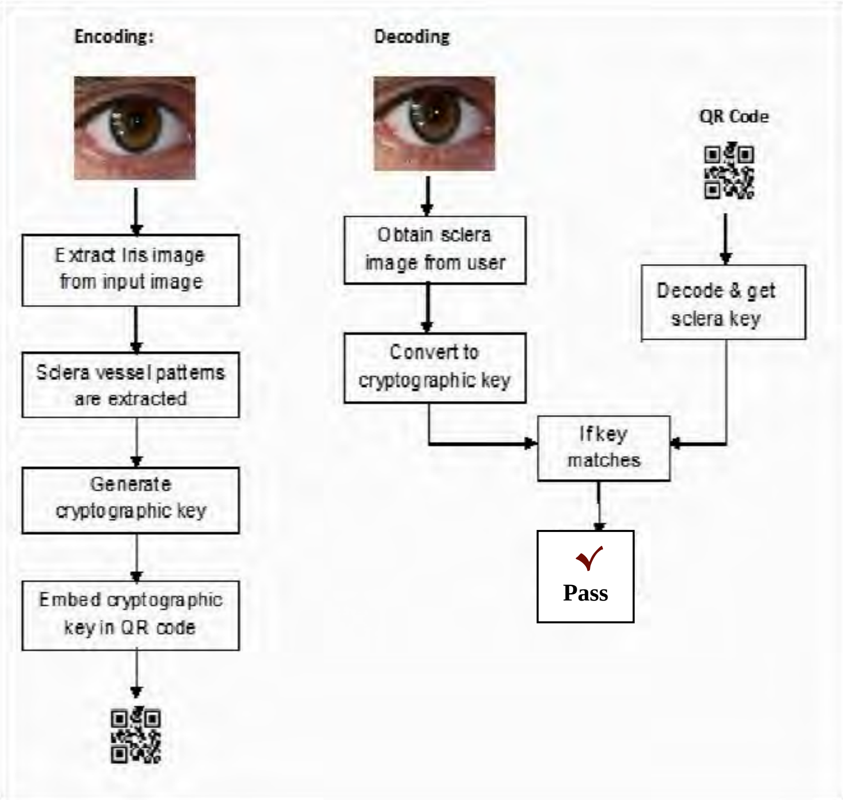

Encoding:
Decoding
QR Code
Extract Iris image from input image
Sclera vessel patterns are extracted
Generate cryptographic key
Embed cryptographic key in QR code
Obtain sclera image from user
Convert to cryptographic key
Decode & get sclera key
If key matches
✓
Pass

Fig. 7. Encoding and Decoding

Two factor authentication involving one hardware token (the mobile device) and sclera has been proposed in the above model. Attackers require both tokens in order to reconstruct the necessary information. There are several threats related to the user device: (i) attackers might steal a mobile phone in which case a printed QR codes can be used ii) attackers staying close to the screen which displays the QR-code might try to steal information or to guess QR-code. These attacks are hard since, it is not feasible for a person to recognize information stored into a QR-Code.

VI. RESULTS

The metrics used for evaluation are False Acceptance rate (FAR) and False Rejection Rate (FRR). The FRR is the frequency that an authorized person is rejected access. The evaluation of sclera recognition was carried out with 100 images taken from UBIRIS and IUPUI database were grouped into ten users and the results are tabulated for FAR and FRR. Table I and Fig.8 shows the resulted (FRR) as obtained from Eqn 1 for the proposed sclera vein and existing iris technique. From the result, it can be observed that the proposed technique results in lesser False Rejection Rate when compared to the existing techniques.

$$FRR(n) = \frac{Number\ of\ rejected\ verification\ attempts\ for\ a\ qualified\ person\ n}{Number\ of\ all\ verification\ attempts\ for\ a\ qualified\ person\ n}$$

$$FRR = \frac{1}{N}\sum_{n=1}^{n} \mathrm{FRR}\,(\mathrm{n})$$

Eqn 1

The FAR is the frequency that a non-authorized person is accepted as authorized.

$$FAR(n) = \frac{Number\ of\ successful\ independent\ fraud\ attempts\ against\ a\ person\ n}{Number\ of\ all\ independent\ fraud\ attempts\ against\ a\ person\ n}$$

$$\mathrm{FAR} = \frac{1}{N}\sum_{n=1}^{n} \mathrm{FAR(n)}$$

Eqn 2

Table I
FRR (%) for various users

No. of Users	Iris	Proposed Sclera
1-10	88.7	83.8
11-20	87.9	84.1
21-30	89.1	84.4
31-40	88.5	83.7
41-50	88.9	85.1
51-60	89.3	84.9
61-70	88.6	85.2
71-80	89.4	85.2
81-90	88.1	84.6
91-100	88.2	84.9

Table II
FAR (%) for various users

No. of Users	Iris	Proposed Sclera
1-10	0.35	0.15
11-20	0.33	0.12
21-30	0.37	0.14
31-40	0.39	0.15
41-50	0.36	0.09
51-60	0.33	0.11
61-70	0.35	0.15
71-80	0.39	0.12
81-90	0.38	0.11
91-100	0.36	0.13

Table II and Fig. 9 shows the resulted False Acceptance Rate (FAR) for the proposed and existing technique which is obtained using Eqn 2. From the result, it can be observed that the proposed technique results in lesser False Acceptance Rate for all the persons, whereas the existing techniques results with higher percentage of False Acceptance Rate. From all the results obtained, it can be said that the proposed technique results in better security than the existing technique.

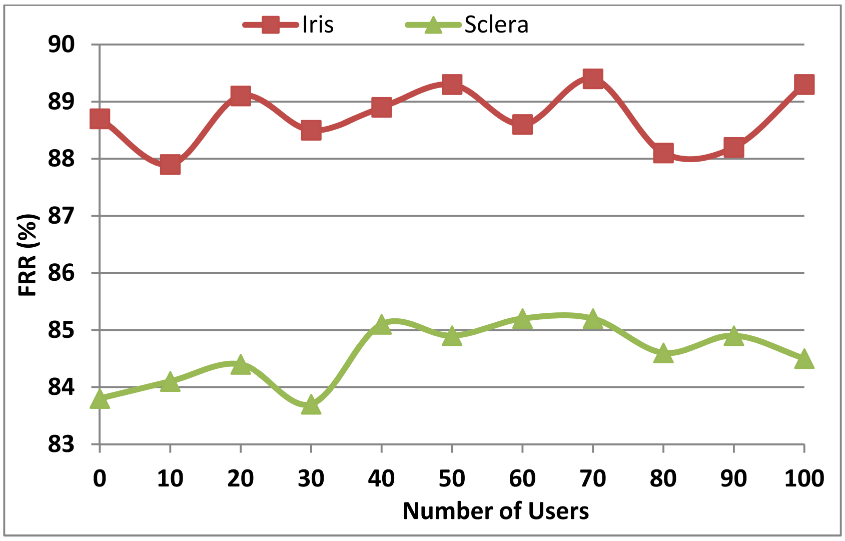


Fig. 8. Resulted False Rejection rate

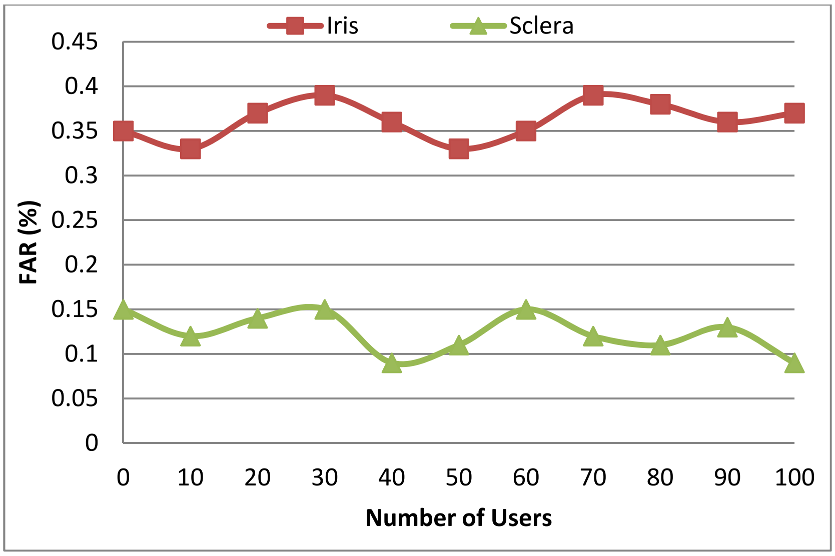


Fig. 9. Resulted False Acceptance rate

VII. CONCLUSION

Biometrics and QR codes are combined to provide a two factor authentication where nominative tickets are required. The proposed model has improved the security of the system as verified using FAR and FRR. Automatic authentication is possible with state of art technologies like sclera recognition on the move. Accordingly, without maintaining a database file to verify the user's authentication request can decrease the risk of tampering and maintenance cost successfully. As future improvements the cryptographic key of multimodal biometrics [9] like sclera and iris can be encoded in QR code and issued for enhancing security.

REFERENCES

[1] *"Denso wave incorporated,"* http://www.denso-wave.com/qrcode / index.html.

[2] *"QR code software,"* http://www.quickmark.cn/En/basic /index.asp.

[3] Querini, M.; Italiano, G.F., "*Facial biometrics for 2D barcodes," Computer Science and Information Systems (FedCSIS), 2012* Federated Conference on , vol., no., pp.755,762, 9-12 Sept. 2012

[4] Shiyang Liu, *"Anti-counterfeit System Based on Mobile Phone QR Code and Fingerprint," Intelligent Human-Machine Systems and Cybernetics (IHMSC),* 2010 2nd International Conference on , vol.2, no., pp.236,240, 26-28 Aug. 2010

[5] Ouda, O.; Tsumura, N.; Nakaguchi, T., "*Tokenless Cancelable Biometrics Scheme for Protecting Iris Codes," Pattern Recognition (ICPR)*, 2010 20th International Conference on , vol., no., pp.882,885, 23-26 Aug. 2010

[6] Yan Sui et al., "*Secure and privacy-preserving biometrics based active authentication," Systems, Man, and Cybernetics (SMC),* 2012 IEEE International Conference on , vol., no., pp.1291,1296, 14-17 Oct. 2012

[7] Mathew et al., "*An improved three-factor authentication scheme using smart card with biometric privacy protection," Electronics Computer Technology (ICECT)*, 2011 3rd International Conference on , vol.3, no., pp.220-223, 8-10 April 2011

[8] S.Brindha, Ila.Vennila; , "*Secure Smart card using CRC based Steganography ," Mathematical modeling and Applied Soft Computing(MMASC)*, 2012 International Conference on , July 2012

[9] Zhi Zhou, Eliza Y.Du, N.Luke Thomas, Edward J.Delp, *"A comprehensive multimodal eye recognition". "Springer", DOI* 10.1007/s11760-013-0468-8, published online on April 2013.

[10] Zhi Zhou, Eliza Y.Du, N.Luke Thomas, Edward J.Delp, *"A new human identification method: sclera recognition". "IEEE Transactions on systems, man and cybernetics"* vol. 42, no. 3, pp. 571-583, May 2012.

[11] Simona Crihalmeanu and Arun Ross, *"Multispectral scleral patterns for ocular biometric recognition", "Elsevier Pattern Recognition Letters"* vol. 33, no.14, pp. 1860-1869, January 2012.