Research Journal of Applied Sciences, Engineering and Technology 5(5): 1496-1502, 2013
ISSN: 2040-7459; e-ISSN: 2040-7467

Submitted: March 18, 2012 Accepted: April 20, 2012 Published: February 11, 2013

Twin Layer Iris Certification for Confidential Archive by Conceiving Shares (ICCA-CS)

R. Sinduja, R.D. Sathya and V. Vaithiyanathan
School of Computing, SASTRA University, Tamil Nadu, India

Abstract: Iris is one of the most challenging biometric techniques. In many proposed biometric recognition technique, template's are store in the database for comparison. But there exists a vital problem in storing the template in the database since it can be easily bootlegged. In order to overcome these issues a novel method for person identification by their Iris, through securely storing the template is proposed. Visual Cryptography Encryption (VCE) technique is used for securely storing the iris template. By means of VCE, shares are generated for the iris template which is stored in the database instead of storing the entire template. Shares are generated by pixel expansion method. Authentication is provided by comparing the shares. Comparison is done by using Hamming Code. So it is a very effective method of person identification. The proposed method gives an extra security in iris recognition.

Key words: Authentication, biometrics, encryption, visual cryptography

INTRODUCTION

In today's society, security has become a major issues and it is more important. Secured data can be easily hacked or misused now a days by using many types of attacks. So it is necessary to protect our data. One way of information protection can be done by setting password to our data, but passwords can be easily hacked. So it is not an efficient way. This limitation tends to the usage of Biometrics technique. Biometric techniques can easily identify a person by using their physical or behavioral traits. There are various application where personal identification is required such as passport control, computer login control, secure electronic banking, bank ATM, credit cards, premises access control, border crossing, airport, mobile phones, health and social services, etc. Biometric techniques have been developed for various features like fingerprint, facial image, voice, hand geometry, handwriting, iris and retina.

Among all these features, iris is the most efficient and powerful technique (Riad *et al*., 2010) because of two major reasons, they are

- Iris forms during gestation and remains the same for the rest of one's life and it is unique for individuals
- It is well protected and extremely difficult to be modified and also because of its stability, noninvasiveness and also uniqueness

Table 1 will forecast the comparison between the different biometrics and exhibit that the iris is more commanding when compared to all other methods.

Iris Biometric is a powerful technique but yet there is a bottle neck situation in storing the biometric template. If a user wants to access a secure resource, then they should be a authenticated person. For authentication purpose at first the biometric template of the real user should be stored in the central database and then it should be verified with the incoming user's template. If the biometric template is compromised then the whole authentication system will be collapsed. So there should also be a awareness concerning the privacy and the security while storing the biometric templates. There exist several types of attacks in a biometric system. (Nalini *et al*., 2001) describe eight basic sources of attack that can arise in the database. In order to beat this template protection problem, a dominant solution has been introduced in this study. A technique named Visual cryptography is used to store the template securely in the central database in the form of share (Revenkar *et al*., 2010)

LITERATURE REVIEW

Iris recognition: There are many existing methods for person identification by using biometric template. (Subba Rao *et al*., 2008; Hong and Jain, 2003) uses different biometrics to identify a person, they face a problem that, these biometrics can be easily changed by another. Iris biometric is a powerful technique as said by (Daugman, 1994; Masek and Kovesi, 2003). Iris recognition is done by various algorithms (Tan *et al*., 2010) they are mentioned below:

In Daugman's Integro-differential operator was used to locate the iris. And 2D Gabor filters and phase coding were used to obtain feature code for the iris representation. Different from Daugman, Wildes exploited the gradient-based Hough transform for

Corresponding Author: R.Sinduja, School of Computing, SASTRA University, Tamil Nadu, India

Table 1: Comparison of biometrics techniques

Btometric	University	Uniqueness	Permanence	Collectability	Performance	Acceptability	Circumvention
Face	H	L	M	H	L	H	L
Fingerprint	M	H	H	M	H	M	H
Hand Geometry	M	M	M	H	M	M	M
Hand veins	M	M	M	M	M	M	H
Iris	H	H	H	M	H	L	M
Retinal scan	H	H	M	L	H	L	H
Signature	L	L	L	H	L	H	L
Voice	M	L	L	M	L	H	L
Facial thermograph	H	H	L	H	M	H	H
Order	H	H	H	L	L	M	L
DNA	H	H	H	L	H	L	L
Gait	M	L	L	H	L	H	M
Ear Canal	M	M	H	M	M	H	M

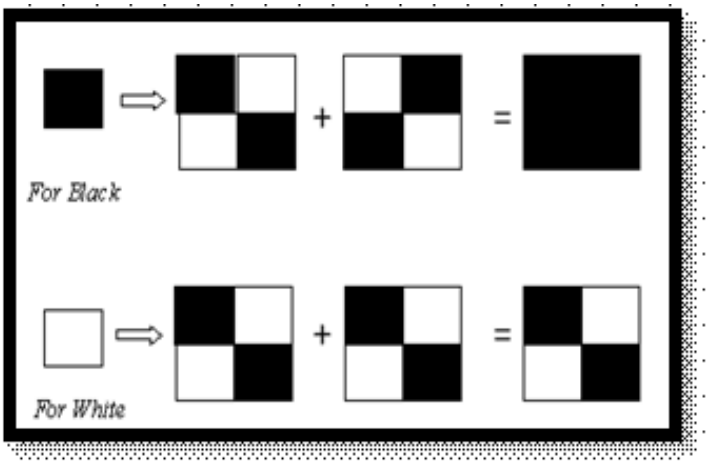


Fig. 1: Pixel expansion

localizing the iris area and made use of Laplacian pyramid constructed with four different resolution levels to generate iris code.

Wildes (1997) uses Hough transform for iris segmentation and extract the feature using various Gaussian filters and matching is done by using normalized correlation.

Boles (1996) used the knowledge based edge detector for iris localization and implemented the system operating the set of 1-D signals composed of normalized iris signatures at a few intermediate resolution levels and obtaining the iris representation of these signals via the zero crossing of the dyadic wavelet transform.

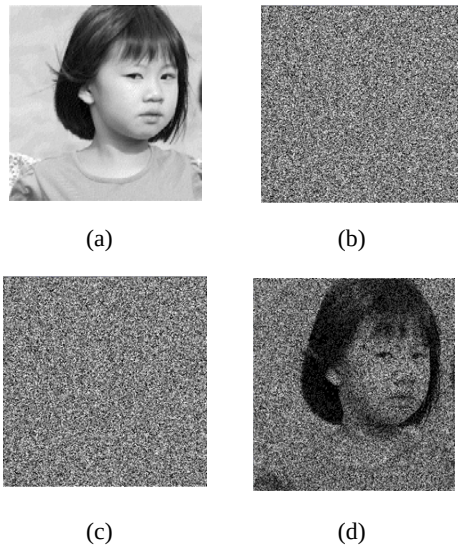
Lim and Kim (2001) exploited 2D Haar wavelet transform to extract high frequency information of the iris and a bank of Gabor filters was used to capture both local and global iris features in Ma *et al*. (2002) algorithm. Various algorithms for segmentation, normalization, feature extraction is proposed by Masek and Kovesi (2003).

Security protection for biometric template: As said before iris template should be securely stored. In recent years many ways for protecting the template was proposed, they are:

Tuyls *et al*. (2005) proposed a method for secure template protection by using fingerprint identification. In Chander *et al*. (2005) biometric template are stored by using stenography concept, by merging a key inside the picture and storing which is a complex approach. Nick *et al*. (2007) combines watermarking and cryptography scheme to store the template. In Zhifang *et al*. (2008) hash value of iris feature image is stored in the database instead of the entire image which is a time consuming method.

All the existing methods mainly uses watermarking and stenography to store the template, but in these methods the template can be easily extracted, which is a very serious issue. In order to overwhelmed this problem a new method of template protection is given by Visual cryptography.

Visual cryptography: Visual Cryptography is an emerging method which is used for security aspects. It is comparatively very easy and uses less complex algorithms for providing security when contrasted to other techniques. In this approach the original image is divided into shares and by stacking the one share on the another, the original information is retrieved back. A single share will not reveal the original information. Shares are generated by pixel expansion. The basic visual



(a) (b)

(c) (d)

Fig. 2: (a) original image (b) share S1 (c) share S2 (d) stacked image (S1 and S2)

cryptography scheme was proposed by Moni and Adi (1995). The pixels should be expanded in a such way that the stacking of the shares should produce the same pixel value without any loss. Performance of the scheme depends upon the pixel expansion and contrast. Pixel expansion is done in two combination, they are depicted in Fig. 1.

The visual cryptography technique has two parts encryption and decryption. Share generation process is called encryption and stacking of shares will produce the original image is decryption. But many decryption algorithm proposed will generate meaningless share (noisy image). So in the matching phase it will produce wrong results. Meaningless shares are shown in Fig. 2.

The proposed system (ICCA-CS) uses only the Encryption technique of VC (VCE). In this method matching is done only between the shares which r provides a better way for authentication, when compared to other existing methods.

PROPOSED SYSTEM

The proposed Iris Recognition System (ICCA-CS) has two rungs, they are: signing up rung and certification rung. Working of proposed ICCA-CS system is shown in algorithm 1.

Algorithm 1: ICCA-CS algorithm
Input: Incoming user Eye image and Id number
Output: Certificated Person (or) not.
Signing Up Rung

- Admin.
- Iris Preprocessing.
- Template extraction.
- Share Generation.
- Distribution of Shares.

Certification Rung

- Incoming user's iris preprocessing.
- Share Generation.
- Comparison between the shares.
- Certified person or not.

Signing up rung: This rung has the following procedures:

- Admin has to collect the eye image of the authenticated user and should register their iris template in the database.
- For fetching the template, iris should be preprocessed.
- Iris template is extracted.
- Two Shares A_{S1} and A_{S2} generated from the iris template.
- A_{S1} along with the user ID is stored in the Database and A_{S2} is given to the authenticated user.

Preprocessing consists of three steps (Ujwalla *et al*., 2010) they are:

Segmentation: Segmentation is done in order to extract the iris from the eye image. Iris can be extracted from the eye by using the Circular Hough Transform. It will first produce an edge map using the first order gradient and then votes are casted into the Hough space. Then it will detect the specific contour. Image Gradient is found using (1):

$$\begin{aligned} &\left|\nabla G(x,y) * I(x,y)\right| \\ &G(x,y) = \left(1/2\pi\sigma^2\right)\exp-\left(\left(\left(x-x_o\right)^2+\left(y-y_0\right)^2\right)/2\sigma^2\right) \end{aligned} \quad (1)$$

Hough Transform is written as following (2) ,[21]

$$\begin{aligned} &H\left(x_c y_c, r\right) = \Sigma\ {}_1^h h\left(x_i, y_i, x_c, y_c, r\right) \\ &h\left(x_i, y_i, x_c, y_c, r\right) = 1\ if\ g\left(x_i, y_i, x_c, y_c, r\right) = 0 \\ &\qquad\qquad 0\ otherwise \end{aligned} \quad (2)$$

where the parametric funcation

$$g\left(x_i, y_i, x_c, y_c, r\right) = \left(x_i, x_c\right)^2 + \left(y_i, y_c\right)^2 - r^2$$

Hough Transform is employed for pointing the radius and middle of pupil and iris. Hough transform will detect the eyelids and eyelashes using threshold technique using

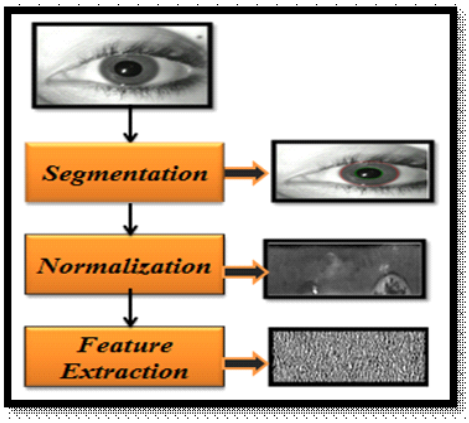


Fig. 3: Iris preprocessing

the horizontal and vertical coordinates. Formula (1) and (2) used for iris segmentation.

Normalization: Normalization Process is done by using Daugman's rubber sheet model. Normalization eliminates the dimensional inconsistency between iris regions and to allow comparisons. This process will unwrap the iris texture into a fixed-size rectangular block. Daugman's Rubber Sheet Model is given as follows: It transforms a localized iris texture from Cartesian to polar coordinates, called unwrapping process. The Cartesian to polar transformation is defined by (3). Where I (x, y)-iris area; (r, q)-Polar coordinates; (x_p; y_p)-points of pupil; (x_i; y_i)-points of iris.

Feature extraction: In order to provide accurate recognition of individuals, the most discriminating information present in an iris pattern must be extracted. The Gabor wavelet method with log-polar transformation is used.

$$I((x(r, \theta), y(r, \theta)) \rightarrow I(r, \theta)$$

where

$$x(r, \theta) = (1-r) \times x_p(\theta) + r \times x_i(\theta) \quad (3)$$
$$y(r, \theta) = (1-r) \times y_p(\theta) + r \times y_i(\theta)$$

and

$$x_p(\theta) = x_{p0}(\theta) + r_p \times \cos(\theta).$$
$$y_p(\theta) = y_{p0}(\theta) + r_p \times \sin(\theta).$$
$$x_i(\theta) = x_{i0}(\theta) + r_i \times \cos(\theta).$$
$$y_i(\theta) = y_{p0}(\theta) + r_i \times \sin(\theta).$$

$$G(w) = \exp(\log(w / w_0)2 / (2 \log(\sigma^2)) \quad (4)$$

Feature extraction is done by convolving the normalized iris pattern into one dimensional Log-Gabor wavelets. The resulting phase information for both the real and the imaginary response is quantized, generating a bitwise template which is of 20*480 size. The 1-D Log-Gabor Filter is done by using (4).

The overall preprocessing process is show in Fig. 3. From preprocessing steps, iris feature template is got. This template should be given as the input for the visual cryptography algorithm and two shares are generated.

After fetching the iris template, instead of storing the template entirely, shares of the iris template is generated by using the Visual Cryptography Encryption (VCE) concept.

Two shares of the template is conceived and only one share A S1 is registered in the database. Since only one share is registered in the database it gives an extra layer security protection for this iris recognition system. (ICCA-CS)

Conceiving shares: Share generation is a concept of visual cryptography. Shares are generated by pixel expansion. So each pixel in the original iris template isexpanded into four pixels in share S1 as P1 and another

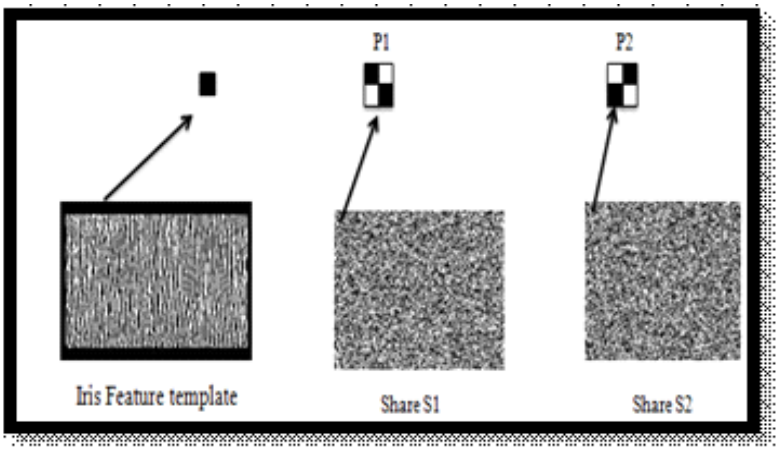


Fig. 4: Pixel expansion of iris template

C0

	0	1	2	3
W - White (0)	W	W	B	B
B - Black (1)	W	W	B	B

C1

	0	1	2	3
W - White (0)	W	W	B	B
B - Black (1)	B	B	W	W

Fig. 5: Pixel values in C_o and C_1.

Table 2: Matrix format of C_o and C_1

Share S1	Share S2
$C_0(\text{white}(0)) = \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix}$	$C_1(\text{white}(0)) = \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix}$
$C_0(\text{Black}(1) = \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix}$	$C_1(\text{Black}(1)) = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}$

four pixels in share S2 as P2. So a single share cannot reveal the original information. The pixel expansion of the iris template is shown in Fig. 4.

Pixel values are separated and represented in matrix format $A_{i,j}$ and $B_{i,j.}$ where i, j = 1….n. N depends on the size of the image. Figure 5 shows values of white and black pixel. C_0 (S1) and C_1 (S2) are the values of shares for 0(white) and 1(black). Binary image has two values 0 and 1 for white and black respectively.

The matrix format of pixels in S1 and S2 is shown in Table 2.

Using the idea in the pseudo-code and incorporating the concept of Visual Cryptography Encryption (VCE) technique shares are generated.

Pseudo-code for share generation is:

Input: Iris template T1 of size 320X 320.
Output: shares R1 and R2.
For (x = 0;x<320x++)
For (y = 0;j<320;y++)
Random assign R1[x][y] as white or black
If IT1[x][y] is white then
R2[x][y] = R1[x][y];
else
R2[x][y] = complement of R1[x][y];
end if
end for
end for

After generating the two shares. A $_{S1}$ share of the authenticated person is registered in the central database along with the user ID and Share A $_{S2}$ is given to the user. Signing up rung process is detailed in Fig. 6. So when the user comes in for accessing some resources, it should be verified and certificated that they are a authenticated person to use the resource. Certification process is done in the second rung of the system

Certification rung: In order to find whether a incoming user is authenticated person, the following process is done:

- Incoming user should give the Share A_{S2} (given by admin) along with ID.
- Iris template of the incoming user is got by iris preprocessing as said first rung.
- Two shares U_{S1} and U_{S2} are generated for the incoming user iris template.
- Then share A_{S2} and share U_{S2} should be compare. Only if both are same then share

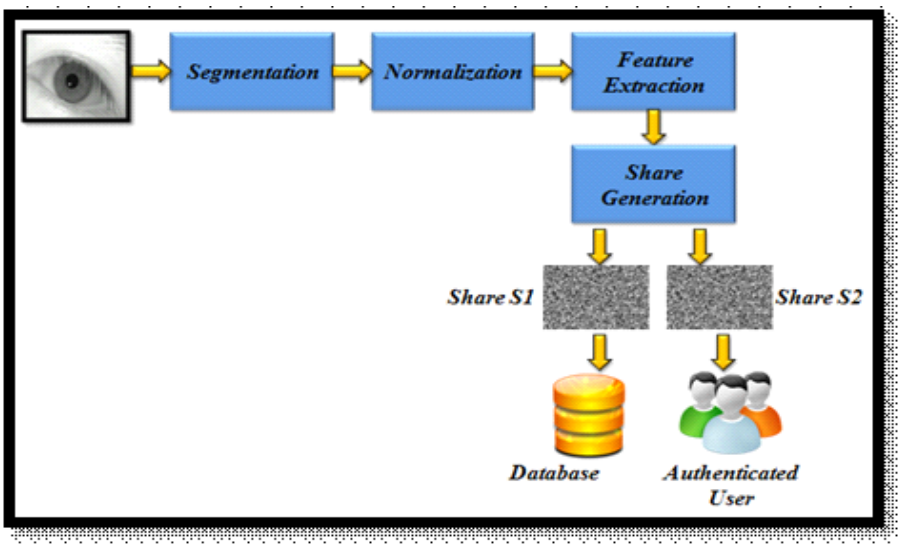


Fig. 6: Signing up rang

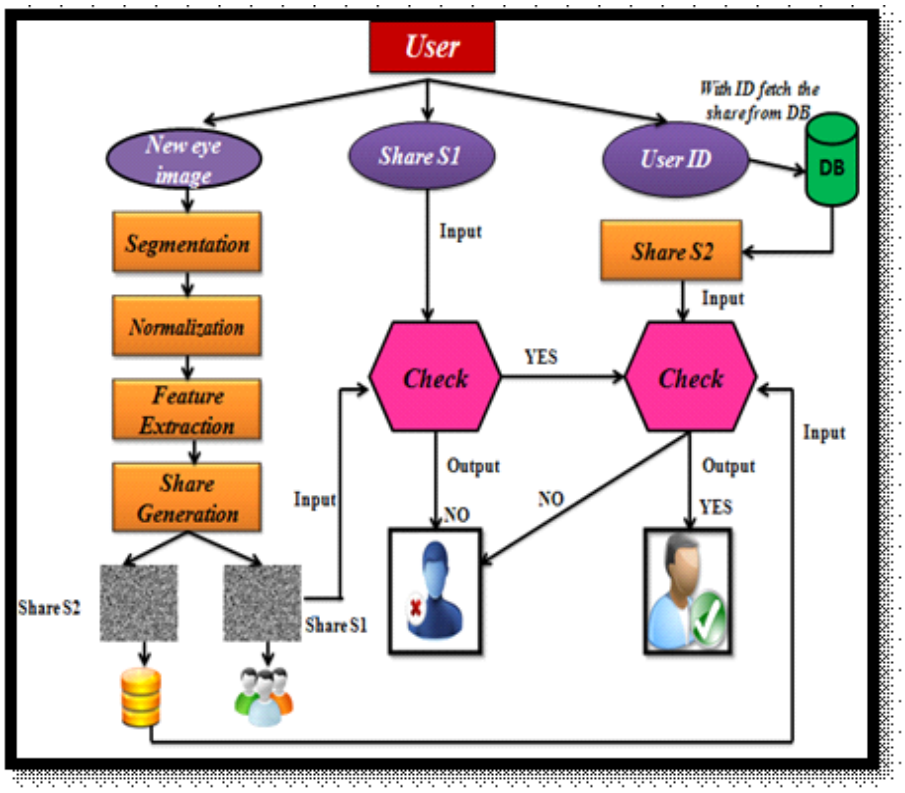


Fig. 7: Certification phase

- A_{S1} in the database and U_{S1} share of the user must be compared if they are same it means that they are authenticated person.

Shares are compared by using the Hamming Distance (HD). HD is found using formula (5)

$$HD = (1/n)\sum_{i=1}^{n}\left(A_i \oplus B_i\right) \quad (5)$$

Thus the shares are compared and a incoming user is certified for accessing some resources. The inclusive process of certification rung is shown in Fig. 7.

Advantage of (ICCA-CS) system: Like customary routine of iris recognition the entire iris template is not stored in the database. Compromising the single share in the database will not have any effect. Only if the share that admin gives to the user and share generated from the user matches, it will move for comparing the next share. If a person is not authenticated it will notify immediately in no time, by just comparing one share. It is not necessary to run the entire system. So it is a effective system and provides extra layer of protection by comparing two set of shares.

EXPERIMENTAL RESULTS

The experiment is tested for 2,215 eye images. Eye images are taken from MMU database. The proposed person recognition system will respond a person in 10 sec. The time taken by this system is very less when compared to the other proposed methods. Efficiency of the system is predicted by using, False Reject Rate (FRR), False Accept Rate (FAR) and Total Success Rate (TSR). All these factors have a powerful ratio when compared to many existing methods of iris recognition.

CONCLUSION

Thus a commanding method for person identification by iris biometric technique is proposed. Certification is given for a person to access resource by securely storing the iris template in share (image) format. The proposed system is less prone to attacks that commonly occurs in the database.

FUTURE WORK

The proposed idea works good for monochrome images and the same method of approach can be extended for colored eye images.

REFERENCES

Boles, W.W., 1996. A wavelet transform based technique for the recognition of the human iris. In Proceedings of the International Symposium on Signal Processing and its Application, ISS PA, Gold Coast, Australia, pp: 25-30.

Chander, K., N. Ranjender and Sheetal, 2005. Biometrics security using steganography. Int. J. Sec., 2(1): 1-5.

Daugman, J., 1994. Biometric personal identification system based on iris analysis. United States Patent, Paten No: 5,291,560.

Hong, L. and A.K. Jain, 2003. Integrating faces and fingerprints for personal identification. IEEE Trans. PAMI, 20(12): 1295-1307.

Lim, S. and T. Kim, 2001. Efficient iris recognition through improvement of feature vector and classifier. ETRI J., 23(2).

Ma, L., T. Tan and Y. Wang, 2002. Iris recognition using circular symmetric filters. National Laboratory of Pattern Recognition, Institute of Automation, Chinese Academy of Sciences.

Masek, L. and P. Kovesi, 2003. Recognition of human iris patterns for biometric identification. Tech. Rep., The School of Computer Science and Software Engineering, The University of Western Australia.

Moni, N. and S. Adi, 1995. Visual cryptography. In Proceedings of the advances in cryptology-Eurocrypt, pp: 1-12.

Nalini, K.R., H.C. Jonathan and M.B. Ruud, 2001. An analysis of minutiae matching strength. In Proceedings of 3rdAVBPA,Halmstad Sweden, pp: 223-228.

Nick, B., K. Nathan, C. Bojan and R. Arun, 2007. Protecting iris images through asymmetric digitalWatermarking. IEEE, 1-4244-1300-1.

Revenkar, P.S., A. Anisa and W.Z. Gandhare, 2010. Secure iris authentication using visual cryptography. Int. J. Comput. Sci. Inform. Sec., 7(3).

Riad, K.A., R.M. Farouk and I.A. Othman, 2010. Time of matching reduction and improvement of sub-optimal image segmentation for iris recognition. OSDA-2010, pp: 49-66.

Subba Rao, Y.V., S. Yulia, B. Chakravarthy and K.S. Umesh, 2008. Fingerprint based authentication application using visualcryptography method(Improved ID card). Tencon 2008, IEEE Region ,10 Conference.

Tan, T., Z. He and Z. Sun, 2010. Efficient and robust segmentation of noisy iris images for non-cooperative iris recognition. Image Vis. Comput., 28: 223-230.

Tuyls, P., A.H.M. Akkermans, T.A.M. Kevenaar, G.J. Schrijen, A.M. Bazen and R.N.J. Veldhuis, 2005. Practical biometric authentication with template protection. In Proceedings of the 5th International Confernce on Audioand Video-Based Personal Authentication. pp: 436-41.

Ujwalla, G., Z. Mukesh and K. Avichal, 2010. Improving iris recognition accuracy by score based fusion method. Int. J. Adv. Techn., ISSN 0976-4860. http://ijict.org/

Wildes, R.P., 1997. Iris recognition: An emerging biometric technology. Proc. IEEE, 85(9): 1348-1363.

Zhifang, W., H. Qi, N. Xiamu and B. Christoph, 2008. A novel template protection algorithm for iris recognition. Eighth International Conference on Intelligent Systems Design and Applications.