Modern Applied Science

www.ccsenet.org/journal.html

Vol. 3, No. 5

May 2009

The Network Identity Authentication System Based on Iris Feature Identification

Hua Jiang

College of Computer Science, Liaocheng University, Shandong 252059, China

E-mail: jianghua@lcu.edu.cn

Shasha Zhang

College of Computer Science, Liaocheng University, Shandong 252059, China

Abstract

By researching the mothed of iris identification integrating the iris features with the secure network communication, this paper designs a new Iris-Based Network Authentification System. The system can complete access control in security. The system has many merits, such as finer security, high identification rate, and so on.

Keywords: Identity authentication, Iris feature, Nnetwork security

In computer network applications, especially in e-commerce applications, the computer's identity authentication method which can effectively prevent fake identity log in is very important technology. However, the biological features of humanity like appearance, fingerprint, iris, sound, gait, and signature, etc, because they have the characteristics of uniqueness, invariability and conveniency, ect, and they can be gathered on real-time once identity authentication will be carried on,thus the case of password being forgotten and ID being stolen totally eliminated. So the identity authentication based biological features is more securing. The iris has many unique features such as “can not transform, difficult to camouflages, non-offensive (or non-contact type)” (Daugman, 1998, p.33-39), etc, and the iris recognition technology is the highest precision of the biometric technology. (Tian,2005,p.230-232, 257).Therefore the iris recognition will become an important ways of identity recognition in the future.

1. Iris Characteristic Recognition Technology

Iris is the part which surround the pupils in the eyeball, above it covers extremely complex extremely complex zigzag network-like pattern and each person's iris pattern is different (shown in Figure 1.The iris recognition technology is to use computer to quantify and analysis data for the Iris feature, to confirm the real identity of the person. Iris identity recognition constitutes several parts (Daugman,2004, p. 21-30): iris acquisition, iris image’s pretreatment (localization, normalizing), iris image feature’s extraction, match and recognition. Among them, The acquisition of iris images is the first step of iris recognition, it can be acquired by corresponding apparatus.

1.1 Iris localization and normalization

The initial Iris image contains much invalid information, so it should be divided from the image at first, that’s iris localization. The iris localization algorithm bases on the canny edge detection and the Hough transform algorithm, and it has good localization effect (shown in Figure 2).The annulu between 2 rings in figure 2 is the iris texture part.

In order to realize exactly match, we use the method of polar coordinates to normalize the located iris (Wang, 2002, p. 1-10)(as shown in Figure 3), it is to standardize the iris annulus to the unified template region to compensates variations caused by the pupil's zoom. Take the pupil center as the polar coordinate center, make a ray which can form angle θ with the horizontal line. The intersection point between the ray and iris inside and outside boundary respectively are (xp(θ),yp(θ)and (xs(θ),ys(θ). Formula (1) can be used to map each point in iris image to the polar coordinate (r, θ).

$$\begin{cases} x(r,\theta) = (1-r)x_p(\theta) + rx_s(\theta) \\ y(r,\theta) = (1-r)y_p(\theta) + ry_s(\theta) \end{cases} \quad r \in [0,1], \quad \theta \in [0,2\pi] \tag{1}$$

In the polar coordinate(r, θ),The normalized image can be unwrap into a rectangle in the size of 64×1024 (shown in Figure 3).For improving the effect of iris recognition and reducing the influence of nonuniform illumination, the iris image is transformed by hisotgram eaqualization(Huang,2002, p.404-409) (shown in Figure 4).

1.2 Iris feature extraction and recognition

Iris feature can be extracted after localization and normalized. One of the effective strategies to extract texture information from the image is to convolute the image and the bandpass filter, the bandpass filter can be realized by choosing 2D Gabor filter, shown as formula(2), then transforms it to formula (3) of the polar coordinate, and coding the characteristic of the iris using complex 2D Gabor wavelet demodulation (process seen in reference 4).

$$G(x,y) = \exp\left\{-\pi[(x-x_0)^2 a^2 + (y-y_0)^2 \beta^2]\right\} \times \exp\left\{-2\pi j[u_0(x-x_0) + v_0(y-y_0)]\right\} \quad (2)$$

$$G(r,\theta) = e^{-iw(\theta-\theta_0)} e^{-(r-r_0)/\alpha^2} e^{-(\theta-\theta_0)/\beta^2} \quad (3)$$

α, β is the scale factor of the filter, and it is in reverse proportion with ω, then a group of Self-Similar,multi-criterion wavelet whose frequency modulation direction along the direction of θ be created, andθ0 and r0.determinet its position. The texture image includes DC(Direct Current) component, in order to make the calculated iris code independent of the illumination intensity, bandpass filter should be used to remove the DC component, high frequency component and high frequency noise in the image. The filter imaginary part is a bandpass, therefore this filter can extract the texture reliably; and an iris characteristic only needs 256 bytes to express.

The iris characteristic recognition is realized by comparing Hamming distance (HD) (Daugman,2003,p.279-291) between two iris characteristic codes,the different iris codes are compared according to the bit XOR (shown as formula 4).

$$HD = \frac{1}{3200}\sum_{j=1}^{3200} A_j (XOR) B_j \quad (4)$$

A and B express different iris code, j expresses the bit of the iris code.In order to avoid the shifting of the 8 segments iris quantitative results for iris turning,so the two iris corresponding segment codes should be shifting compared, each segment code's shifting number is 10. From these shifting comparisons the smallestHD as this segment's Hamming distance. These 8 segments'HD average is the two iris's HD.Experiments show that the HD of the same iris's maximum value <0.25[6],and the different iris's minimum value>0.35, so the separation point can be choosed from 0.25 to 0.35. In order to reduce the error rate, we choose 0.27 as the separation point, if HD<0.27, they are the same iris, or they are difference.

2. Design and Analysis of Network Identity Authentication System on Iris Recognition

2.1 System Architecture

In foundation of iris recognition, this article uses client/server pattern, designs a completely long-distance identity authentication system based on iris, its structure shown in Figure 5.The client side mainly completes the preparatory work of the iris recognition, including iris image gathering, image preprocessing,iris characteristic code's extraction,then transmits the 256 bit iris characteristic codes and user's other identity information to server to request authenticate. The server side has the database of iris characteristic and other identity information,mainly completes the iris characteristic's compariton,finds the corresponding iris from the characteristic base, then return the match result and the user information to the client side.

2.2 Authentication Process

The authentication process of this identity authentication system including two stages: registration stage and authentication stage. Considering the security, the iris characteristic code and other information should be encrypted during the communication process between client and server. This system uses the RSA encryption algorithm.

(1) Registration stage. If the user uses this system first time, then the first request to the server should be the identity registration.The server add user's iris characteristic and other information to the database to prepare for authentication.

1) User inputs ID,the system collects iris image,and extracts 256 bit iris characteristic codes after image preprocessing, and then add it and the user ID to the database.

2) The server produces server public key (KUs) and the private key (KRs) on real-time, and KRs is saved on the server.

(2) Authentication stage. Authentication process shown in figure 6.

Client: ①Collects user's iris, inputs user's ID, obtains iris condition code Irfeature after analysis.②Produces user public key KUc and private key KRc on real-time using RSA encryption algorithm.③ Encrypts user ID,KUC,Irfeature, time stamp and other information to W by server public key,and sends W to sever,W= EKU s[ID+KUC+Irfeature+T+others], T is time stamp, it is used for make identify the interaction uniquely.

2) Server:① After receiving W at time stamp T', the server decrypts W to W1 using KRs, W1=DKRs[W] .②Takes out ID, Irfeature, T, KUc in W1, match the characteristic database and judge whether it is a valid user.③If (T'-T) ≥ΔT, the server refuses to request, the user registers,Δt is a expected value of transport delay(Zhou,2004,p.52~55).④If

authenticates successfully, the server sends message W'= EKUc [T, T'] to the user.Because only the server can decrypts W, then obtains T, KUc,and T makes the user confirm W' is send by the server, and the information has not been distorted.⑤The user returns a encrypted W' by KUs to make the server convinced that the other side is the user itself.

After this connection's end, the key Kuc and KRc are not saved to reduces the possibility of the keys being stolen and ensure the security of communication.

2.3 Analysis of System Performance

Compares with the traditional network identity authentication method, this system combines recognition technology based on the iris trick with the RSA encryption technology.This system not only has advantages such as the Strong Robustness, high flexible, high recognition rate, quickly recognition speed etc., but also has following characteristics:

(1)The user produces KUc and KRc in the client side on real-time. This can reduces the possibility that the key is stolen and assures the communication security.

(2) This system make use of iris's uniqueness and conveniences. The client collects iris on real-time every time when authenticates, so that the possibility of invader stealing the user's iris information from the client side greatly reduced.

(3) Iris feature which in database on server have been encrypted, so the invader unable to obtain the user's true iris information from the server.

(4) The server accepts the cryptographic KUc information which transmits from the client only when the user has been passed the iris authentication. Therefore user's public key KUc and private key KRc are unknowable in the entire process of communication.

(5) Database on server saves the user name, user ID, iris characteristic code, registration date,connection condition and so on. When the user registers,the user iris information can be retrieved by user ID directly.So the massively search is avoided, and the efficiency is greatly raised.

(6) There are 3 interactions between the server and the user during the entire process of communication, it guarantees that the information is not stolen or distorted at all.So the the degree of information security is strengthened.

To testify the feasibility and correctness of the proposed systems, 36 people's irises are collected under different time and conditions.Each person has 5 iris samples, they constitute a small database which is composed of 180 iris images, and each iris image is 8 bit gray images with 640×480 pixel.Then the person's identity be Recognized randomly, each person's identity can be distinguished successfully in 2 seconds. The ARR (accurate recognition rate) can reache above 99%; the WER(word error rate) is 0. But this system also has some insufficiencies simultaneously, for instance, the registration time is longer because the distance between eyes and collection can not control well. Because the system's recognition efficiency is decided by the scale of the characteristic base and the network complexity, the system need to be optimized and improved in the further.

3. Conclusion

This article utilzed the iris' characteristic of uniqueness, stability and convenience and RSA encryption systems, studied and designed a remot identity authentication system.. The practical test results shows that the identity authentication system combines recognition with encryption algorithm can achieve the goal of the remote login of identity authentication truly. Along with the reduction of the cost of iris' collection and further optimization of the match efficiency, network identity recognition technology based on iris will be promoted to more domains.

References

Daugman,J. (1998). Recognizing people by their iris pattern.Informa-tion.Security Technical Report, 3(1), 33-39.

Daugman,J. (2003). The importance of being random: Statistical principles of iris recognition. *Pattern Recognition,* 36(2), 279-291.

Daugman,J. (2004). How Iris Recognition Works. IEEE Trans. CSVT, 14(1), 21-30.

Huang Huifang & Hu Guangshu. (2002). The iris recognition algorithm's research and realizes. The Infrared and Laser Engineering, 31(5), 404-409.

Tian Qichuan,Pan Quan & Cheng Yongmei etc. (2005). Iris Encoding Algorithm Based on Local Edge Detection, Application Reasearch of Computers, 22(8), 230-232, 257.

Wang Yunhong, Zhu Yong & Tan Tieniu. (2002). Identity authtication based on iris. Automation journal, 28(1), 1-10.

Zhou Gongye & Liu Zhiqin. (2004). A long-distance status authentication plan based on fingerprint recognition. Computer project and science, 26(7), 52~55.

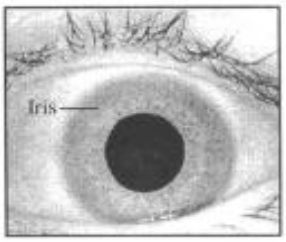

Figure 1. original image

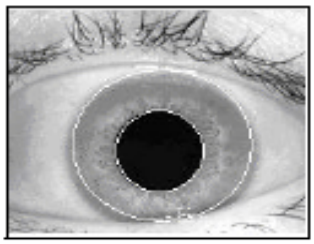

Figure 2. iris location

Figure 3. the normalized iris

Figure 4. the histogram equalization

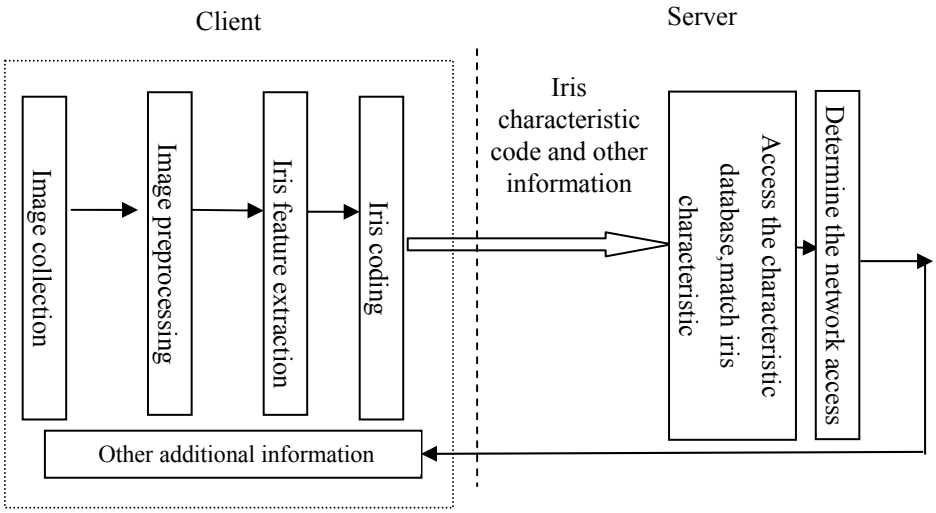

Figure 5. the remote authentication system based on iris characteristic

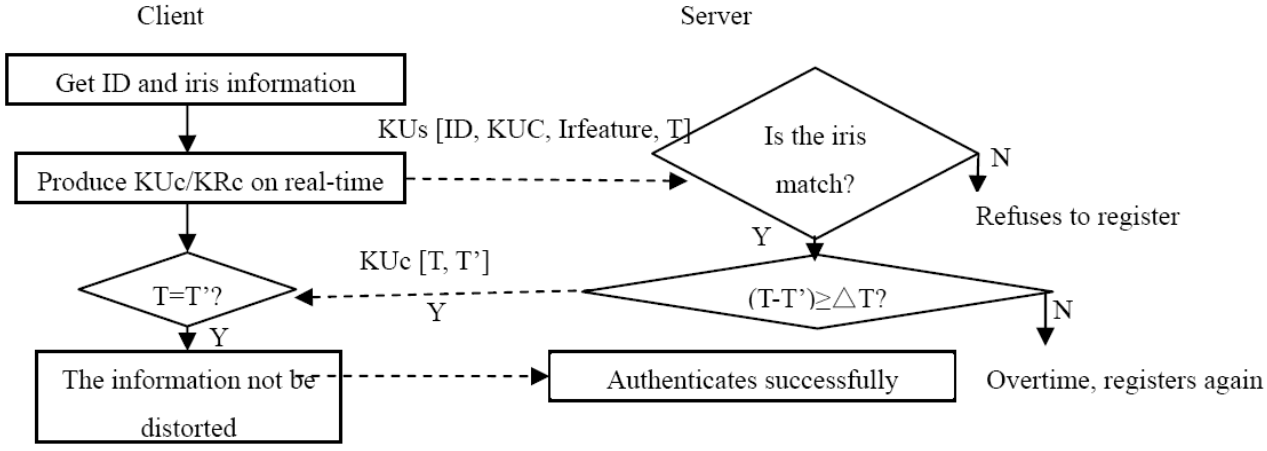

Figure 6. schematic drawing of status authentication process