IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Traitement du Signal
Vol. 39, No. 2, April, 2022, pp. 441-447
Journal homepage: http://iieta.org/journals/ts

Biological Image Identity Detection and Authentication in the Field of Financial Payment Security

Haibo Gao[1*], Zhujun Wang[2], Xialong Sun[3]

[1] School of Economics and Management, Northwest University, Xi'an 710127, China
[2] School of Marxism, Shaanxi Normal University, Xi'an 710119, China
[3] Xianyang Branch of China Construction Bank, Xianyang 712000, China

Corresponding Author Email: gaohaibo@stumail.nwu.edu.cn

https://doi.org/10.18280/ts.390205

Received: 25 November 2021
Accepted: 28 February 2022

Keywords:
financial payment security, biological features, identity detection, image processing

ABSTRACT

The detection and authentication of consumer identity directly support the security supervision, security guarantee, and consumer privacy protection of Internet financial payment. But the immature biological detection technology brings various security risks. The relevant studies have not supervised the security of Internet financial payment or detected consumer identity from the perspective of financial security. Therefore, this paper investigates the biological image identity detection and authentication in the field of financial payment security. Section 2 displays the functions and data interaction models of the Internet financial payment platform, and enumerates the hidden dangers of Internet financial payment and their probabilities. Section 3 adopts the active shape model to extract image features like fingerprints, faces, palm prints, and auricles. Section 4 details the process of matching and fusion of consumer biological features, and demonstrates the fusion procedure of multiple biological features. The proposed model and algorithm were proved valid through experiments.

1. INTRODUCTION

Internet financial payment has developed and will develop rapidly [1-7]. The traditional financial payment model can no longer meet consumers' demand for real-time, convenient, and paperless payment. The Internet financial payment, which involves various payment instruments, brings a fresh payment experience to consumers, and penetrates various payment scenes, by virtue of its high flexibility [8-15]. In the 5G era, China has gained an edge in Internet financial payment technology over the other countries. Due to the lack of precedents, however, innovative Internet financial payment technology has not been extensively implemented, and may result in supervision loopholes. The detection and authentication of consumer identity directly support the security supervision, security guarantee, and consumer privacy protection of Internet financial payment. But the immature biological detection technology brings various security risks [16-20].

In recent years, biological features have been widely used in Internet financial payment. Although the technical requirements for secure payment are met, the authentication standards and consistency requirements for user identity in payment have not been fulfilled. Wang et al. [21] presented an anonymous authentication and management process of mobile payment, which supports secure transactions, prevents user information leakage, and reduces identity theft. The proposed management process integrates various things, including the generation, encryption, and decryption of transaction keys, and processes the users' personal information and biological features based on mobile devices for identity authentication. Chen and Roscoe [22] demonstrated how the human interaction security protocol supports the authentication of different types of identity, when the Public Key Infrastructure (PKI) is unsuitable, misunderstood, or too costly, and highlighted the payment situation. Majumder et al. [23] recognized the leapfrog development of mobile computing, and emphasized that the near-field communication (NFC) function, which is embed into smartphones by Google, Samsung, and Apple, has provide mobile payment functions and eliminate the demand for payment cards. However, the technology is not suitable for everyone, owing to limitations of interoperability and cost. Jin et al. [24] explored the authentication of collective payment of debit cards, and put forward two cardholder identity authentication protocols. The first protocol processes the personal identity number (PIN) in the secure electronic transaction (SET) protocol, exerting the minimum influence. The second protocol checks the balance based on the server wallet mode. The two protocols apply to different environments, and meet the needs of collective payment of debit cards. Bascuñana et al. [25] developed an open, cross-domain, and platform neutral system to illustrate the services of different devices and applications. The developed technology can save the cost and time of starting new devices and applications. The store architecture is based on advanced communication networks and network technology.

After combing through the domestic and foreign studies, it can be learned that scholars at home and abroad have made fruitful research into the security of Internet financial payment, which consolidates the foundation of security supervision for Internet financial payment. However, there is no comprehensive research of security supervision, or consumer identity detection / authentication in Internet financial

payment, from the angle of financial security. To fill the gap, this paper investigates the biological image identity detection and authentication in the field of financial payment security. Section 2 displays the functions and data interaction models of the Internet financial payment platform, and enumerates the hidden dangers of Internet financial payment and their probabilities. Section 3 adopts the active shape model to extract image features like fingerprints, faces, palm prints, and auricles. Section 4 details the process of matching and fusion of consumer biological features, and demonstrates the fusion procedure of multiple biological features. The proposed model and algorithm were proved valid through experiments.

2. FUNCTIONS AND HIDDEN DANGERS

Figure 1 demonstrates the functions of the Internet financial payment platform. During the consumption on the online shopping platform, each consumer generates an order. Then, the client of the online shopping platform will display the payment interface to the consumer, according to the interface model provided by the client of the Internet financial payment platform. The payment request will be made by transmitting the identity authentication result of the program to the server of the Internet financial payment platform. The platform server will accept the request, and execute the payment task. Next, the Internet financial payment platform will provide step -by - step feedback on the result of the payment task.

Figure 2 shows the data interaction models of the Internet financial payment platform. The client of online shopping platform is capable of summing up sales data, sending payment request, and accepting and displaying the payment result. The client of Internet financial payment platform has the ability to update the databases of payment requests and confirmations. The server of Internet financial payment platform can respond to payment requests, and provide the feedback on payment result. The server of online shopping platform is responsible for accepting and feeding back on payment result.

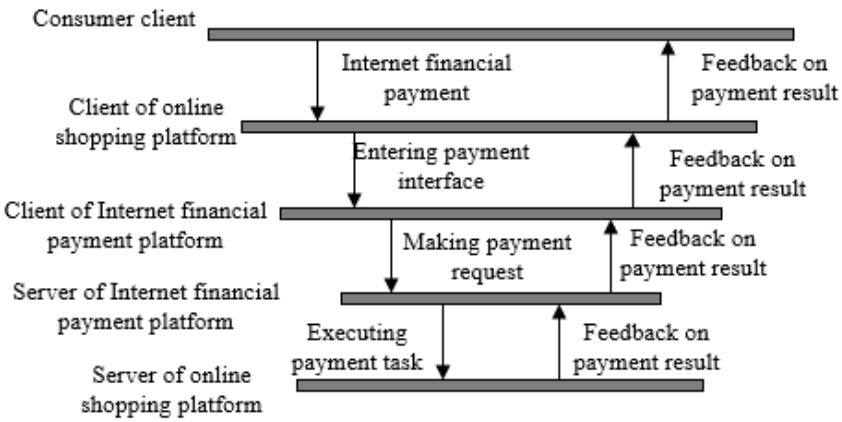


Figure 1. Functions of the Internet financial payment platform

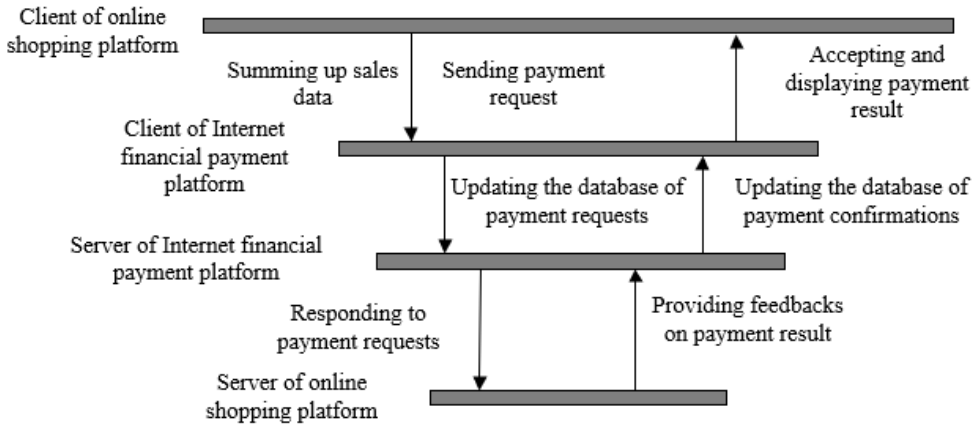


Figure 2. Data interaction models of the Internet financial payment platform

Table 1. Hidden dangers of Internet financial payment

Hidden dangers	Probability
Insecure communication between the client of online shopping platform and the server of online shopping platform	32.15%
Failure to display complete payment information by the client of online shopping platform	37.48%
Omission of signature authentication by the server of online shopping platform /the client of online shopping platform	2.95%
Unsigned messages from the server of online shopping platform	1.57%
Incomplete authentication of payment result by the server of online shopping platform	4.81%
Generation of incorrect order number and order details by the client of online shopping platform	15.62%
Private signature key in the client of online shopping platform	5.42%

Table 1 lists the hidden dangers of Internet financial payment and their probabilities.

3. EXTRACTION OF BIOLOGICAL FEATURES

In the context of consumer identity detection, the security supervision of Internet financial payment mainly detects biological features like fingerprints, faces, palm prints, and auricles. This paper relies on the active shape model to extract these features from images. The active shape model is displayed in Figure 3.

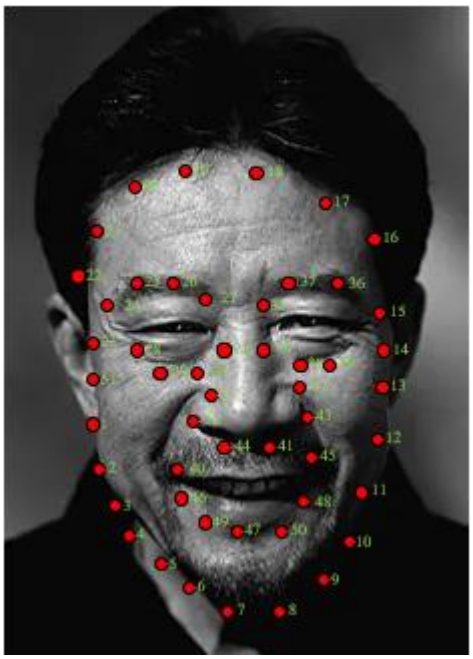


Figure 3. Active shape model

With superior speed in image processing, the active shape model is suitable for identity detection and authentication tasks that require good real-time performance. Before building a shape model for extracting consumers' biological features, it is necessary to construct the shape vector, which is composed of the coordinates of all feature points in the original image. Let l be the number of feature points; i be the serial number of each sample image. Then, the shape vector of the sample image can be expressed as:

$$A_i = \left(a_{i1}, b_{i1}, a_{i2}, b_{i2}, \cdots, a_{il}, b_{il}\right)^T \tag{1}$$

To obtain the feature point of image sample a, the first step is to compute the distance S_{ij} from the feature point of the current sample to that of another sample. Suppose there are a total of M samples, and the mean of a satisfies $\bar{a}=(1/M)\sum^{m}_{i=1}a_i$. Then, the variance R of sample a can be calculated based on S_{ij}:

$$R = \sqrt{\left(1/M-1\right)\sum_{i=1}^{M}\left(a_i-\bar{a}\right)^2} \tag{2}$$

Next the weight of each feature point is solved, i.e., the reciprocal of the sum of the variances between each feature point and the other points:

$$q_j = \left(\sum_{i=1}^{m} U_{S_{ji}}\right)^{-1} \tag{3}$$

The sample images are different in size. The size difference may lead to variations in feature point coordinates and image orientation, which in turn influence the extracted features. To prevent the influence, this paper carries out Procrustes normalization on the shape vector of every sample image through rotation, scaling, and translation. Let r be the scale of transform; ω be the rotation angle. Then, the geometric transform can be expressed as:

$$N = \left(r, \omega\right) = \begin{bmatrix} x & -y \\ y & x \end{bmatrix} = \begin{bmatrix} r\ cos\omega & -r\ sin\omega \\ r\ sin\omega & r\ cos\omega \end{bmatrix} \tag{4}$$

Firstly, the shape vector of the target is normalized to the unit size:

$$\begin{aligned} &A_j \\ &= \left(a_{j0}, b_{j0}, a_{j1}, b_{j2}, \cdots, a_{jn}, b_{jn}, a_{j(l-1)}, b_{j(l-1)}\right) \end{aligned} \tag{5}$$

Then, the target shape vector in every training sample image is aligned with the target shape vector. Let R_j be the scale of transform; ω_j be the rotation angle; P_j be the length of displacement. Then, the feature points of the target can be transformed by:

$$A_j = N\left(r_j, \omega_j\right)\begin{bmatrix} a_j \\ b_j \end{bmatrix} + p_j \tag{6}$$

Then, the mean shape vector is solved for the targets in the sample image, and used to align all the target shape vectors. The parameter selection may cause the target feature points in the sample image to shift. To obtain the new feature point positions after the shift, this paper constructs local grayscale models, and uses the Mahalanobis distance to characterize the displacement. Let j be the serial number of sample images; i be the serial number of target feature points in an image. Then, the sample images are normalized by:

$$h_i \to \frac{1}{\sum_j h_{ij}} h_i \tag{7}$$

The mean of each local grayscale model in the sample image can be calculated by:

$$h_i = \frac{1}{m}\sum_{j}^{1} h_{ij} \tag{8}$$

The covariance matrix of the model for each feature point can be calculated by:

$$R_i = \frac{1}{m}\sum_{j=1}^{m}\left(h_{ij}-\bar{h}_i\right)^T\left(h_{ij}-\bar{h}\right) \tag{9}$$

During model matching, the parameters are adjusted to obtain the new position of each target feature point. The similarity between old and new features is measured by the Mahalanobis distance. The new local features can be expressed as:

$$g\left(h_i\right)=\left(h_r-\bar{h}_i\right)^T R_{h_i}^{-1}\left(h_r-\bar{h}_i\right) \tag{10}$$

For the biological features of consumers, the shape vectors of the images of fingerprints, faces, palm prints, and auricles normally overlap each other, which complicates the feature extraction. This paper reduces the dimensionality of the shape vectors with overlapping sample images through principal component analysis (PCA), and builds up a statistical shape model. This approach is simple, and able to suppress the influence of feature point shift.

Before building the statistical shape model for the shape vectors with overlapping sample images, it is important to carry out dimensionality reduction. The mean shape vector of targets in the sample image can be calculated by:

$$\bar{A}=\frac{1}{m}\sum_{i=1}^{m}a_i \tag{11}$$

The mean shape vector obtained by formula (11) is subtracted from the aligned target shape vector:

$$da_i=a_i-\bar{a} \tag{12}$$

The covariance matrix R is calculated for the target shape vector:

$$R=\frac{1}{m}\sum_{1}^{m}da_i da_i^T \tag{13}$$

The first ε eigenvectors of R solved by the above computing is denoted as T. Each eigenvector corresponds to an eigenvalue $T=(t_1,t_2,t_3,...,t_\varepsilon)$. The eigenvalue that affects the change direction of the target model can be recorded as y. Finally, the target shape vector of any sample image can be generated based on the mean target shape, and the shape change parameters of targets:

$$a=\bar{a}+Ty \tag{14}$$

To minimize the gap between the biological feature points in consumers' identity detection and the actual feature points, the agreement between each model and the actual target contour is continuously improved by affine transform and eigenvalue y adjustment, after obtaining the active shape model of the image target.

Let K be the distance between two key positions of the target; $R=J/K$ be the scaling parameter of the model. To obtain the translation vector of the original model, the distance between the centers of each key point of the target, and of the corresponding key point of the target in the sample image can be calculated by:

$$\varepsilon=\begin{bmatrix}\varepsilon_a & \varepsilon_b\end{bmatrix}^T \tag{15}$$

Similarly, the angle ω between the line connecting two key points in the mean model, and that line in the object model of the sample image is solved. Let $[\dot{a}_i,\dot{b}_i]^T$ be the feature points in the mean target model of the sample image. Then, the coordinates of each feature point can be expressed as:

$$\begin{aligned}\begin{bmatrix}a_i^0\\ b_i^0\end{bmatrix}&=N\left(r,\omega\right)\begin{bmatrix}\dot{a}_i\\ \dot{b}_i\end{bmatrix}+\varepsilon\\ &=\begin{bmatrix}r\cos\omega & -r\sin\omega\\ r\sin\omega & r\cos\omega\end{bmatrix}\begin{bmatrix}\dot{a}_i\\ \dot{b}_i\end{bmatrix}+\begin{bmatrix}\varepsilon_a\\ \varepsilon_b\end{bmatrix}\end{aligned} \tag{16}$$

To improve the search efficiency of the model, the candidate feature points can be selected in the direction vertical to the line between feature points, thereby reducing the computing complexity of the model.

4. IDENTITY DETECTION AND AUTHENTICATION

The preceding section relies on the active shape model to extract the feature points of consumers' biological features, such as fingerprints, faces, palm prints, and auricles. This section intends to detail the feature matching and fusion of the images on consumers' fingerprints, faces, palm prints, and auricles. The fusion process of the multiple biological features is illustrated in Figure 4.

Among the collected images on consumers' biological features, two were randomly selected for training, and the rest were reserved for testing. After pairwise comparison of in-class biological feature images, the matching result was expressed as $MR=\{mr_1,mr_2,mr_3,...,mr_n\}$, and the number of successfully matched biological feature points was expressed as $FP=\{fr_1,fr_3,fr_4,...,fr_m\}$. Finally, MR was combined with FP:

$$\begin{aligned}U&=MR\bigcup FP\\ &=\left\{mr_1,mr_2,...,mr_n,\ fr_1,\ fr_2,...,\ fr_m\right\}\end{aligned} \tag{17}$$

The combination in formula (17) is not a mathematical AND operation, but a connection between arrays. The length of U is equal to the sum of the length of MR and that of FP.

The array variables FP_{MR}, FA_{MR}, PP_{MR}, and AU_{MR} correspond to the number of successfully matched in-class feature points for fingerprint, face, palm print, and auricle images, respectively. The array variables FP_{FP}, FA_{FP}, PP_{FP}, and AU_{FP} correspond to the number of successfully matched between-class feature points for fingerprint, face, palm print, and auricle images, respectively. The fusion methods for the eight array variables can be expressed as:

$$\begin{aligned}MRU&=\theta_1\times FR_{MR}+\theta_2\times FA_{MR}\\ &+\theta_3\times PP_{MR}+\theta_4\times AU_{MR}\end{aligned} \tag{18}$$

$$\begin{aligned}FPU&=\theta_1\times FP_{FP}+\theta_2\times FA_{FP}\\ &+\theta_3\times PP_{FP}+\theta_4\times AU_{FP}\end{aligned} \tag{19}$$

where, weights θ_1, θ_2, θ_3, and θ_4 fall in [0,1], and satisfy $\theta_1+\theta_2+\theta_3+\theta_4=1$. The eigenvectors of fingerprint, face, palm print, and auricle images can be expressed as:

$$GG = (ug_1, ug_2, ug_3, ug_4) \quad (20)$$

$$GT = (ut_1, ut_2, ut_3, ut_4) \quad (21)$$

$$GY = (uy_1, uy_2, uy_3, uy_4) \quad (22)$$

$$GD = (ud_1, ud_2, ud_3, ud_4) \quad (23)$$

The fusion of the four types of eigenvectors can be expressed as:

$$GU = \begin{pmatrix} ug_1 + ut_1 + uy_1 + ud_1, ug_2 + ut_2 \\ +uy_2 + ud_2, \cdots, ug_n + ut_n + uy_n + ud_n \end{pmatrix} \quad (24)$$

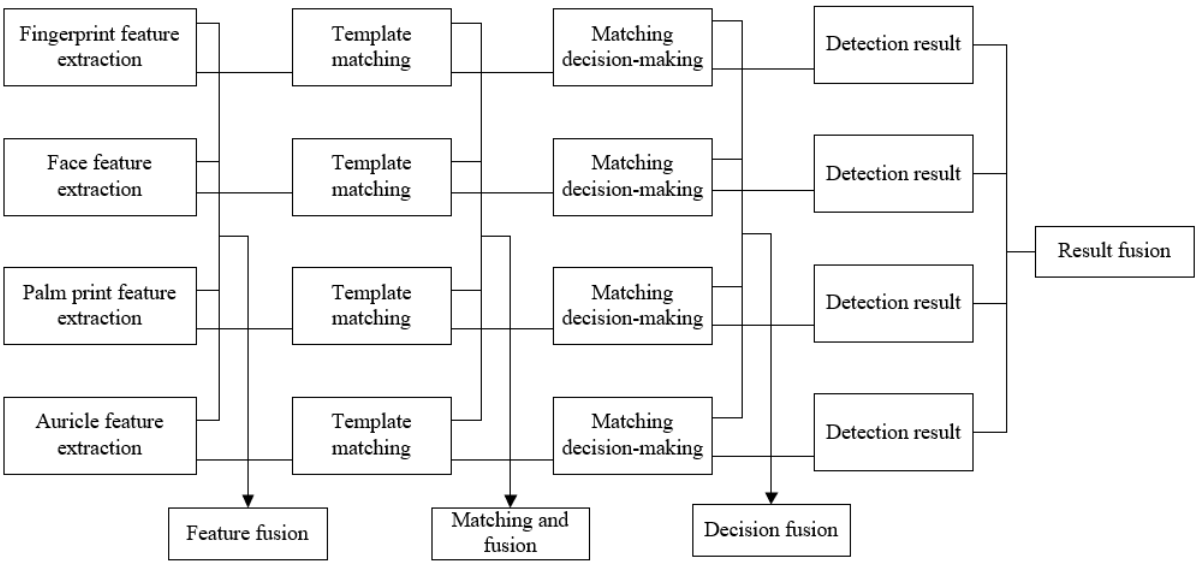


Figure 4. Flow of the fusion of the multiple biological features

5. EXPERIMENTS AND RESULTS ANALYSIS

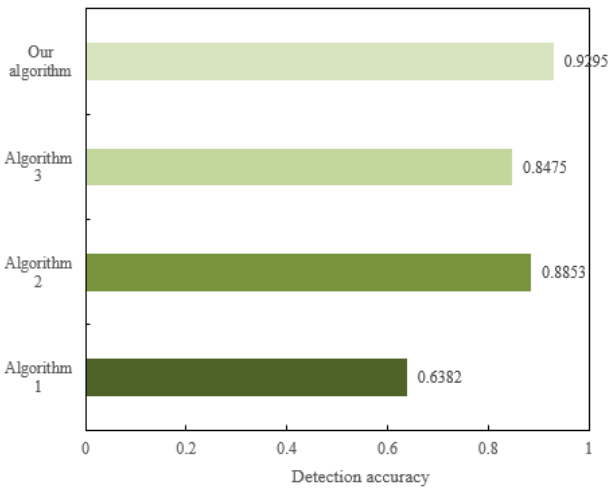


Figure 5. Feature detection accuracies of different algorithms

Figure 5 compares the feature detection accuracies of different algorithms, including our algorithm, PCA algorithm, local binary pattern (LBP) algorithm, and latent Dirichlet allocation (LDA) algorithm. It can be clearly observed that our biological feature extraction approach, which is based on active shape model, achieved the highest accuracy (92.95%) on the fingerprint, face, palm print, and auricle features. The feature detection accuracies of PCA (Algorithm 1), LBP (Algorithm 2), and LDA (Algorithm 3) were 84.75%, 88.53%, and 63.82%, respectively.

Table 1. Training durations of different algorithms

	1	2	3	4	5	Mean duration
Algorithm 1	125.184	121.508	128.015	125.682	123.227	126.085
Algorithm 2	415.263	341.051	263.597	215.418	395.624	652.032
Algorithm 3	851.247	892.364	817.259	861.295	948.362	857.964
Our algorithm	52.184	56.935	47.152	49.263	47.205	52.806

Table 2. Identity detection accuracies of multi-biological feature fusion with different weights

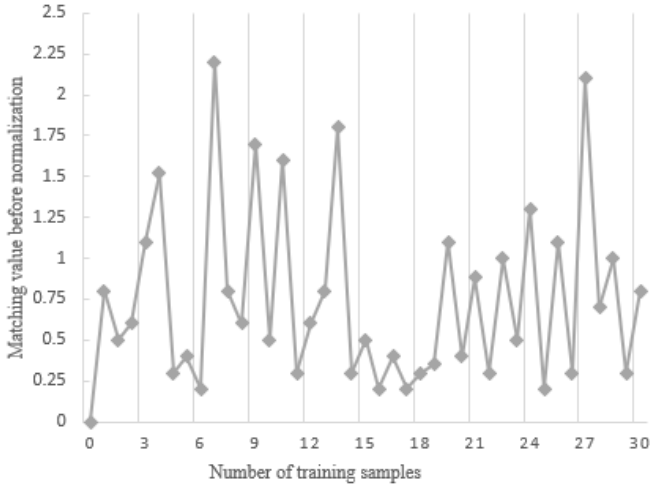
θ_1	θ_1	θ_1	θ_1	FAR	FRR	Accuracy
1	0	0	0	0.0184	0.0518	0.7162
0	1	0	0	0.0629	0.0605	0.7648
0	0	1	0	0.0415	0.0152	0.7312
0	0	0	1	0.0362	0.0485	0.7495
0.2	0.5	0.2	0.1	0.0439	0.0348	0.9602
0.1	0.3	0.2	0.4	0.0618	0.0641	0.8215

Note: FAR and FRR are short for false acceptance rate, and false rejection rate, respectively.

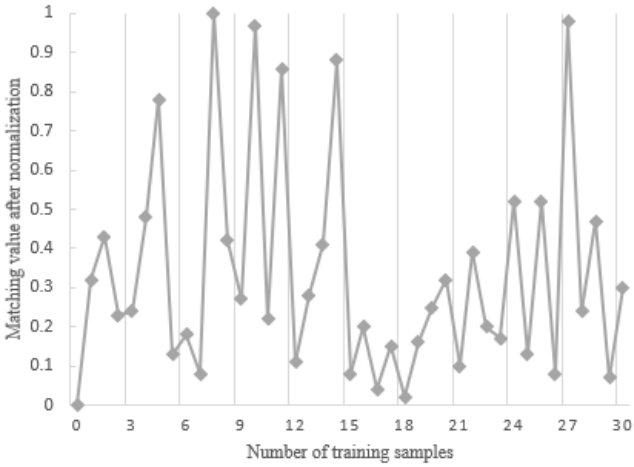
Figure 6 compares the biological feature matching values before and after normalization. The comparison shows that the covariance of training samples reflects the stability, balance, and difference of the number of successfully matched biological feature points of consumers. Hence, the proposed model can obtain highly discriminative biological features from consumers.

The time efficiency is very important to the identity detection and authentication of consumers based on the fusion of multiple biological features. Table 1 shows the training

durations of different algorithms measured through experiments. The time efficiency was measured by the mean duration for five runs of each program. It can be seen that our method consumed the fewest time in training, while the LDA was the most time-consuming algorithm.



(1) Before normalization



(2) After normalization

Figure 6. Biological feature matching values before and after normalization

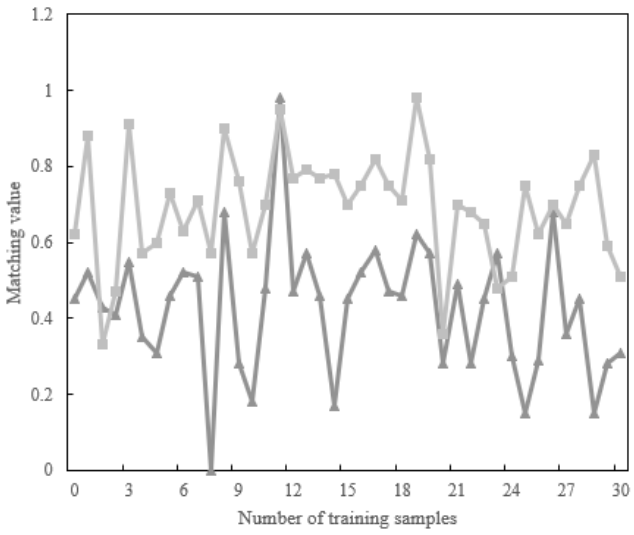


Figure 7. Variation of biological feature matching value with weights

In addition, the feature images of fingerprints, faces, palm prints, and auricles were tested to compute the accuracies of identity detection. Table 2 summarizes the detection accuracies of multi-biological feature fusion with different weights. It can be seen that the identity detection using a single type of feature images was below 80%. The highest accuracy was achieved (96.02%), when the different types of feature images were assigned weights of 0.2, 0.5, 0.2, and 0.1, respectively. Figure 7 shows the variation of biological feature matching value with weights.

The experimental results show that the weight combination of 0.2, 0.5, 0.2, and 0.1 led to a higher matching value than that of 0.1, 0.3, 0.2, and 0.4. Therefore, the proposed fusion method for multiple biological features can significantly avoid the incorrect identity detection through nonlinear programming with the optimal weight assignment. The real-time performance and applicability of our approach are satisfactory in Internet financial payment.

6. CONCLUSIONS

This paper explores the biological image identity detection and authentication in the field of financial payment security. Section 2 displays the functions and data interaction models of the Internet financial payment platform, and lists the hidden dangers of Internet financial payment and their probabilities. Section 3 adopts the active shape model to extract image features like fingerprints, faces, palm prints, and auricles. Section 4 details the process of matching and fusion of consumer biological features, and demonstrates the fusion procedure of multiple biological features. In the experimental section, the feature detection accuracies of different algorithms were compared, revealing that our biological feature extraction method, which is based on the active shape model, had the highest detection accuracy of consumers' biological features. Furthermore, the authors compared the biological feature matching values before and after normalization, and found that the proposed model can obtain highly discriminative biological features from consumers. In addition, the feature images of fingerprints, faces, palm prints, and auricles were tested to compute the accuracies of identity detection, the identity detection accuracies of multi-biological feature fusion at different weights were summarized, and the variation of biological feature matching value with weights was observed. The results show that the highest accuracy was achieved, when the different types of feature images were assigned weights of 0.2, 0.5, 0.2, and 0.1, respectively.

REFERENCES

[1] Prasanna, P.L., Nagarjuna, N., Karthik, K., Kallinatha, H.D., Nandakumara, R.P. (2018). A smart parking system using Internet of Things with automated payment system for smart cities. In 2018 3rd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), pp. 1128-1135. https://doi.org/10.1109/RTEICT42901.2018.9012565

[2] Hattori, Y., Sakai, Y., Saito, T. (2012). Development and evaluation of order and payment systems via internet in-vehicle use. In 19th ITS World Congress, Vienna, Austria.

[3] Khanfar, K., El Shaikh, A., Alazzah, I., Alqousini, A. (2009). Closed circle internet E-payment system schema. International Review on Computers and Software, 4(3): 414-421.

[4] Orozova, D., Sotirova, E., Sotirov, S. (2008). Generalized net model of electronic payment processes via Internet. In 2008 4th International IEEE Conference Intelligent Systems, 2: 16-12. https://doi.org/10.1109/IS.2008.4670539

[5] Zhang, W., Ma, W., Shi, H., Zhu, F.Q. (2012). Model checking and verification of the internet payment system with SPIN. Journal of Software, 7(9): 1941-1949. https://doi.org/10.4304/jsw.7.9.1941-1949

[6] Yang, D., Wang, Q. (2011). The study on the application of RFID-based mobile payment to the Internet of Things. In 2011 International Conference on Multimedia Technology, 908-911. https://doi.org/10.1109/ICMT.2011.6001856

[7] Wang, F.Q. (2011). Research on the methods of payment via the Internet and mobile phones. 2011 International Conference on E-Business and E-Government, ICEE2011 - Proceedings, 7234-7237. https://doi.org/10.1109/ICEBEG.2011.5886914

[8] Ally, M., Toleman, M., Cater-Steel, A. (2010). Traditional and alternative internet payment systems: the merchant perspective. In Proceedings of the 5th International Conference on Qualitative Research in IT & IT in Qualitative Research: The Traditions and Innovations of Qualitative Approaches in ICT Research (QualIT 2010). QualIT.

[9] Abdellaoui, R., Pasquet, M. (2010). Secure communication for Internet payment in heterogeneous networks. In 2010 24th IEEE International Conference on Advanced Information Networking and Applications, pp. 1085-1092. https://doi.org/10.1109/AINA.2010.45

[10] Abrazhevich, D., Markopoulos, P., Rauterberg, M. (2009). Designing internet-based payment systems: Guidelines and empirical basis. Human–Computer Interaction, 24(4): 408-443. https://doi.org/10.1080/07370020903038144

[11] Song, J., Yang, F., Choo, K.K.R., Zhuang, Z., Wang, L. (2017). SIPF: A secure installment payment framework for drive-thru internet. ACM Transactions on Embedded Computing Systems (TECS), 16(2): 1-18. https://doi.org/10.1145/3014584

[12] Kumar, A., Anusha, N., Prasad, B.S.S.V. (2017). Automatic toll payment, alcohol detection, load and vehicle information using Internet of things & mailing system. In 2017 International Conference on Intelligent Computing and Control (I2C2), pp. 1-5. https://doi.org/10.1109/I2C2.2017.8321775

[13] Song, J., Yang, F., Wang, L. (2017). Secure authentication in motion: A novel online payment framework for drive-thru Internet. Future Generation Computer Systems, 76: 146-158. https://doi.org/10.1016/j.future.2016.06.011

[14] Maharoesman, Z.R., Wiratmadja, I.I. (2016). Technology Acceptance Model of Internet banking service for student's tuition fee payment (Case study: Public government university). In 2016 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM), pp. 616-620. https://doi.org/10.1109/IEEM.2016.7797949

[15] Djuric, Z., Gasevic, D. (2015). FEIPS: A secure fair-exchange payment system for internet transactions. The Computer Journal, 58(10): 2537-2556. https://doi.org/10.1093/comjnl/bxu120

[16] Bayaga, A. (2018). Predicting and explaining security and control of mobile payment transaction: Financial/health institution. IMCIC 2018 - 9th International Multi-Conference on Complexity, Informatics and Cybernetics, Proceedings, 2: 160-165.

[17] Kang, J. (2018). Mobile payment in Fintech environment: Trends, security challenges, and services. Human-centric Computing and Information Sciences, 8(1): 1-16. https://doi.org/10.1186/s13673-018-0155-4

[18] Choi, D., Lee, Y. (2018). Eavesdropping of magnetic secure transmission signals and its security implications for a mobile payment protocol. IEEE Access, 6: 42687-42701. https://doi.org/10.1109/ACCESS.2018.2859447

[19] Gao, F., Rau, P.L.P., Zhang, Y. (2018). Perceived mobile information security and adoption of mobile payment services in China. International Journal of Mobile Human Computer Interaction, 9(1): 45-62. https://doi.org/10.4018/978-1-5225-2599-8.ch055

[20] Khalilzadeh, J., Ozturk, A.B., Bilgihan, A. (2017). Security-related factors in extended UTAUT model for NFC based mobile payment in the restaurant industry. Computers in Human Behavior, 70: 460-474. https://doi.org/10.1016/j.chb.2017.01.001

[21] Wang, F., Shan, G.B., Chen, Y., Zheng, X., Wang, H., Mingwei, S., Haihua, L. (2020). Identity authentication security management in mobile payment systems. Journal of Global Information Management (JGIM), 28(1): 189-203. https://doi.org/10.4018/JGIM.2020010110

[22] Chen, B., Roscoe, A.W. (2011). Mobile electronic identity: securing payment on mobile phones. In IFIP International Workshop on Information Security Theory and Practices, 22-37. https://doi.org/10.1007/978-3-642-21040-2_2

[23] Majumder, A., Goswami, J., Ghosh, S., Shrivastawa, R., Mohanty, S.P., Bhattacharyya, B.K. (2017). Pay-Cloak: A Biometric Back Cover for Smartphones: Facilitating secure contactless payments and identity virtualization at low cost to end users. IEEE Consumer Electronics Magazine, 6(2): 78-88. https://doi.org/10.1109/MCE.2016.2640739

[24] Jin, L., Feng, L., Zhenhua, G. (2001). Identity Authentication for Debit Card Secure Electronic Transaction Payment. Journal-Xi'an Jiaotong University, 35(12): 1255-1258.

[25] Bascuñana, A., Gorricho, M., Rentería, S., Alcolea, E., Ferveur, C., Ahonen, P., Chichignoud, J.P. (2006). SHOPS: Towards a Secure System for Identity Management and Payments in the New Electrical Market. In Proceedings of I International Conference on Ubiquitous Computing: ICUC 06; Alcalá de Henares, Spain, June 7-9, 2006, 239-246.