Personal Information Two-dimensional Code Encryption Technology in the Process of E-commerce Logistics Transportation

Ju Ouyang, and Xianping Chen

***Abstract*—The popularity of the Internet has given birth to e-commerce and promoted the development of logistics industry. Traditional logistics is frail in personal information confidentiality, and it is easy to leak privacy information in the process of logistics. This paper briefly introduced the channels of privacy information disclosure in the process of e-commerce logistics and the privacy information encryption system based on two-dimensional code. Then, the privacy protective effect of the system was tested on the laboratory server. The results showed that mobile terminals with different permissions only obtained some necessary logistics information within their respective permissions in the normal process; the mobile terminals distinguished two-dimensional codes that did not belong to express mails, and only meaningless error codes were obtained after the mobile terminal without permissions scanned the code in the abnormal process. In conclusion, the encryption technology of personal information based on two-dimensional code can effectively protect the privacy information in the process of logistics.**

***Index Terms*—E-commerce, logistics, two-dimensional code, personal information encryption**

I. Introduction

The development of e-commerce logistics has greatly facilitated people's lives, enabling them to purchase goods without leaving home [1]. Compared with traditional face-to-face shopping, e-commerce does not require face-to-face, but its anonymity brings some risks [2], especially when people need to provide private information such as address to guarantee successful transaction. Once the customer's private information is leaked in the transaction and logistics process of e-commerce, it will cause serious hidden dangers [3]. Therefore, the protection of customers' personal privacy information in e-commerce logistics is critical. Zhang et al. [4] proposed a logistics information privacy protection system based on the encrypted two-dimensional code. By means of the segmentation encryption method, personal information was encrypted and the ciphertext was stored in the two-dimensional code. The experiment verified the confidentiality of personal information. Qi et al. [5] proposed a rapid management system based on the encrypted two-dimensional code, which used the encrypted two-dimensional code to store all the information about the goods. The simulation experiment showed that this method could effectively protect the client's privacy and improve the efficiency of express service. Lin [6] designed a secret two-dimensional code sharing method to protect private two-dimensional code data through a secure and reliable distributed system. With the cooperation of authorized participants, the system could retrieve lossless secrets. Experiments showed that this method had the characteristics of readability of contents, detection of spoofs and adjustable secret payloads of two-dimensional codes. This paper briefly introduced the channels of privacy information disclosure in the process of e-commerce logistics and the privacy information encryption system based on two-dimensional code and then tested the privacy protective effect on the laboratory server.

J. Ouyang, Zhejiang Yuying College of Vocational Technology, Hangzhou, Zhejiang 310018, China.

X. P. Chen, Zhejiang Yuying College of Vocational Technology, Hangzhou, Zhejiang 310018, China (e-mail: p7939x@yeah.net).

II. The Leakage Of Privacy Information In E-Commerce Logistics

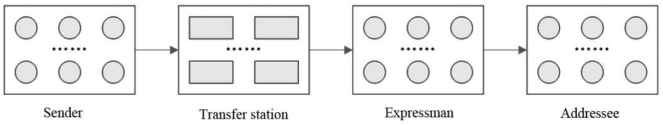

Fig. 1. Basic flow of e-commerce logistics transportation.

With the popularity of the Internet, business activities such as sales and procurement are no longer confined to face to face. Instead, orders are placed through the Internet. After that, merchants allocate goods according to orders and deliver them to customers by express. Some large companies have their own logistics system, such as Jingdong Corporation and Suning Corporation. The basic process of logistics distribution [7] is shown in Fig. 1. Firstly, logistics companies obtain express from different senders and centralize it to logistics sites for unified planning and delivery; then the logistics company classifies the express according to the address information provided by the sender, and transports them to the corresponding transfer station; upon arrival at the final transfer station, the parcels shall be collected by the respective dispatchers and transported to the addressee; finally, different addressees receive the corresponding express. Generally speaking, the logistics mode of logistics companies is

"scattered concentration and unified transportation", in which there are risks and hidden dangers of the sender and addressee's privacy information disclosure. In the process of express transportation, a courier document is usually posted outside the package of the goods to provide the necessary information for delivery. Usually, the information contained in the posted courier documents includes the name, address and contact information of the addressee, the name, address and contact information of the sender and the destination. There is also some other information, such as company name and transportation conditions, which varies according to the requirements.

Almost all the information in traditional express documents is clearly marked. Combined with the basic logistics and transportation processes mentioned above, three links with privacy risks can be analyzed, namely, the sender link, the transfer station link and the sender link [8]. First of all, the sender links. In order to ensure that the express mail is sent to the destination accurately, it is necessary to provide a complete address and contact information, which are clearly marked. It is easy to obtain such privacy information for the centralized service point. Secondly, when the express is sent by centralized classification in the transfer station, the staff of the transfer station can easily obtain privacy information from the plaintext posted on the courier receipt. Finally, the dispatcher link is similar to the transfer station link. Because of express documents, dispatchers can also obtain a large amount of private information centrally. In summary, the degree of privacy confidentiality in the traditional logistics process almost completely depends on the professional ethics of the worker in the logistics company, and there is a great risk of privacy disclosure.

III. Privacy Information Encryption System Based On Two-Dimensional Code

Two-dimensional code [9] uses geometric figures to distribute black and white on the plane according to certain rules to record data information. Compared with one-dimensional barcode, which can only store information in horizontal or vertical directions, two-dimensional code can store more information in horizontal and vertical directions at the same time, and one-dimensional barcode can only store numbers and letters, while two-dimensional code can also store data such as Chinese characters and pictures. After entering the 4G era, the emergence of cloud services has greatly promoted the use of two-dimensional codes, such as the encryption of privacy information in this paper.

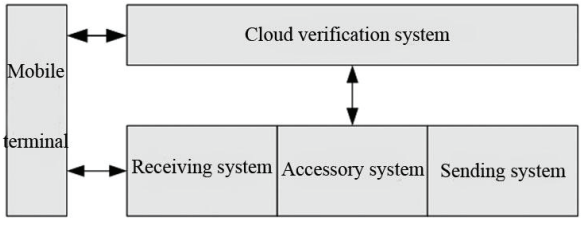

Fig. 2. Simple structure of the privacy information encryption system based on two-dimensional code.

In this paper, rapid reading and writing of two-dimensional code and large storage capacity are used to realize the encryption of personal information in the process of logistics distribution. As shown in Fig. 2, the two-dimensional code based privacy information encryption system consists of a mobile terminal, a cloud verification system, a pick-up system, a distribution system and a delivery system. The pick-up system, distribution system and delivery system are relatively independent, with selective interactive information only through the cloud verification system. Mobile terminals, cloud verification system and pick-up, distribution and delivery system are connected to each other through the Internet. The pick-up system, distribution system and delivery system are relatively independent, with selective interactive information only through the cloud verification system. The mobile terminal, cloud verification system and pick-up, distribution and delivery system are interconnected through the Internet.

Mobile terminal: it is held by the staff of the logistics company and used to input and read express information. In addition, it also has the functions of employee authentication and key management. Employees input their job number or other identity certificates into the terminal and obtain corresponding permission and keys after verification by the cloud verification system.

Cloud verification system: It is the core of the entire encryption system and exists in the cloud server [10] of the system. This system mainly provides employee authentication, key distribution, data storage and management, information transmission, logistics tracking and other functions. The purpose of the employee authentication function is to confirm the employee's identity permission. Staffs will register their corresponding accounts in the cloud verification system after on-boarding and be assigned the corresponding permission. The identities will be authenticated first before work to ensure the consistency of people and permission. The key distribution function is to distribute private keys for decryption according to permission of employees. The data storage and management function is to store and manage the public key, logistics path data and express mail privacy data. The information transmission function is to send the processing results of requests from the mobile terminal to the mobile terminal. The logistics tracking function is to track express mail. When the express mail reaches the station on the logistics path, the mobile terminal scans the express mail and uploads the information to the cloud server to record the location of the express mail.

Pick-up system: It can be regarded as the information input port of the encryption system. Its main functions include information input, data encryption, and two-dimensional code generation and printing. After employees input the information provided by the sender into the pick-up system through mobile terminals, the system encrypts and generates two-dimensional codes, and meanwhile, important information is uploaded to the cloud verification system through the Internet.

Distribution system: It is generally held by the logistics transfer station, the main functions of logistics scanning and information feedback. The employees of the logistics transfer station obtain the corresponding authorization key after being

authenticated by the mobile terminal, scan the two-dimensional code in the goods, obtain some necessary logistics information through the authorization key, and update the logistics status in the cloud verification system through the Internet.

Delivery system: It is generally held by the delivery stations. Its principal functions include out-of-warehouse scanning, information printing, bill of lading verification and information feedback. The staff of dispatch site scans the two-dimensional code of the goods through the mobile terminal to obtain some logistics information, and the cloud verification system sends pick-up information to the addressee.

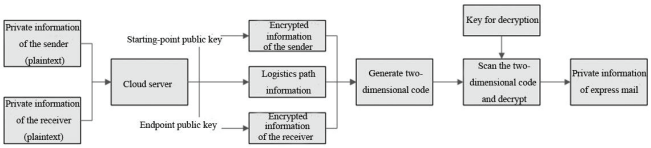

Fig. 3. Logistics privacy information encryption and decryption process based on two-dimensional code.

Encryption of logistics privacy information is the core function of this system. Its flow chart is shown in Fig. 3.

① First, the express private information provided by the sender and receiver is collected, including name, address, contact information, etc. The above information is plaintext and will not be directly printed on the express document [11].

② The collected private information is uploaded to the cloud server that includes public key database and logistics address database. The public key database provides the starting-point public key to the private information of the sender for Rivest-Shamir-Adleman (RSA) encryption [12] and provides the endpoint public key to the private information of the receiver for Rivest-Shamir-Adleman (RSA) encryption. The logistics address database plans the logistics path based on the address information provided by the sender and receiver. The logistics path information will not be encrypted and does not include the address of the starting point and endpoint.

③ The encrypted information of the sender and receiver and logistics path information obtained in the cloud server are integrated, and the logistics path information integrated with the encrypted information in the practical application is a string of links that accesses to the logistics address database of the cloud server. The former and later station information is obtained from the logistics address database according to the scanned station. The integrated encrypted information and logistics path information are converted into two-dimensional codes.

④ Logistics transfer stations and dispatch stations use mobile terminals to scan two-dimensional codes, and then decrypt the ciphertext through the decryption keys of corresponding privileges. The plaintext obtained by decryption varies according to the permission of the decryption key used. For example, the mobile termination held by the staff in the transfer station has no permission to view, i.e., no private key for decryption, and can only obtain the link of the logistics path and search the address of the former and later stations from the link of the located station after scanning the two-dimensional code; the mobile terminal held by the deliveryman has permissions to checking and has the decryption key for the encrypted information of the assigned receiver, and the deliveryman can obtain not only the link of the logistics path but also the address information of the receiver after scanning the two-dimensional code, but cannot obtain the private information of the sender, which effectively guarantees privacy security [13].

In the above encryption and decryption process, apart from the initial encryption of two-dimensional code, RSA algorithm is used to encrypt the private data. RSA algorithm is a kind of asymmetric encryption algorithm. Its encryption principle is explained from the perspective of mathematics as follows: it can simply obtain the product of the multiplication of two large prime numbers, but it is difficult to get the original two prime numbers by inverse factorization of the product [14]. In RSA encryption and decryption algorithm, the public key is (n, e_1) and the private key is (n, e_2), where n is the length of the key in binary and e_1, e_2 are two related values, which are randomly selected to some extent, but the following conditions should be followed: ① e_1 and $(p-1)\cdot(q-1)$ are prime numbers; ② $(e_2 \cdot e_1) \bmod ((p-1)\cdot(q-1)) = 1$ is satisfied , where $(p-1)$ and $(q-1)$ are two factors.

In the encryption algorithm, the public key is published publicly and can be used by anyone, while the private key is confidential and only held by those with permission [15]. In the above encryption process, different key pairs are used according to the permissions of different employees, in which the private key is assigned to the employees with corresponding permissions, so as to ensure that employees can only obtain the information conforming to their permissions from the two-dimensional code.

IV. System Testing

A. Test Environment

This paper used C++ language to compile the system. The main system ran in the laboratory server. Server parameters were i7CPU, 16G memory and 1024G hard disk. Four virtual machines were divided on the server to run cloud validation, pick-up, distribution and delivery system. The configuration parameters of the four virtual machines were: dual-core CPU, 4 G memory and 40 G hard disk.

B. Testing Purposes

The test was to verify the privacy protection effect of the personal information two-dimensional code encryption technology based on e-commerce logistics transportation.

C. Test Project

(1) Protection of privacy information in normal process

Three smart phones of the same specification were used as mobile terminals for scanning two-dimensional codes in the process of pick-up, distribution and delivery. Five clear-text courier documents with different names, addresses and contact information were compiled at first, and then they were inputted into the pick-up system and printed out courier documents with

two-dimensional codes. The key information was hidden from the personal information in the courier documents. The logistics path was set as $A-B-C$, where A is the starting station of centralized pick-up, B is the transfer station of the distribution link, and C is the terminal station of the delivery link. Two-dimensional codes of five courier documents were scanned by mobile terminals of pick-up, distribution and delivery respectively.

(2) Protection of privacy information in abnormal process

① A two-dimensional code without logistics information was generated and printed randomly. The mobile terminals of the pick-up, distribution and delivery were used to scan the two-dimensional code of five express documents.

② The fourth smart phone with the same specifications as the mobile terminals of pick-up, distribution and delivery was adopted to scan two-dimensional codes on the five express mails. The fourth smart phone was not connected to the logistics privacy encryption system.

The above scanning results were forwarded to the computer for display.

D. Testing Results

The test results of the protection of the system for privacy information in the normal process are shown in Fig. 4~ 7. Fig. 4 is the scanning result of one of the express documents by the pick-up mobile terminal. After aiming the pick-up mobile terminal at the two-dimensional code, the two-dimensional code image was displayed in the system. After clicking the button of "identify and scan", the terminal entered the cloud verification system through the address in the two-dimensional code, and obtained the information through its own privileged private key. Then it was transmitted the information back to the terminal through the wireless network and the information was obtained in the scanning result area: only the sender's name and the address of the next station were displayed, and the sender's name only shows the last name. In addition, logistic privacy information was displayed. Fig. 5 is the scanning result of one of the express documents by the mobile terminal. After scanning the two-dimensional code, the system displayed the two-dimensional code image. After clicking "identify and scan", the process was the same as above. The final scan results only showed the last station address, the addressee's last name and the addressee's address, and the rest of the information was displayed. At the same time, compared with Fig. 4 and 5, it was found that the "Contact Communication" button in the system interface was available. The interface after clicking on "Contact Communication" is shown in Fig. 7. The staff cannot know the contact number, but could contact the addressee to complete the dispatch notification. In this process, the contact information of the addressee was effectively hidden.

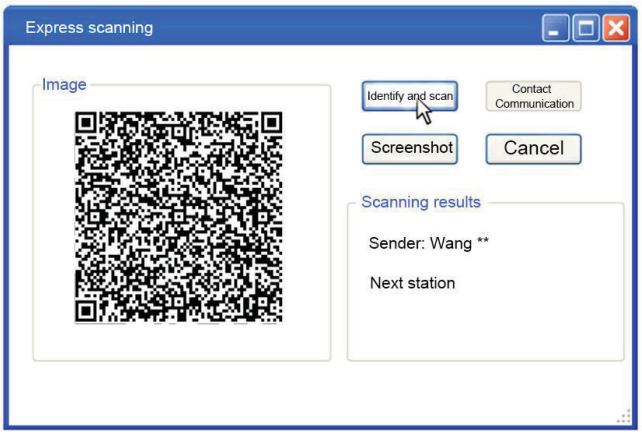

Fig. 4. Scanning results of the pick-up mobile terminal.

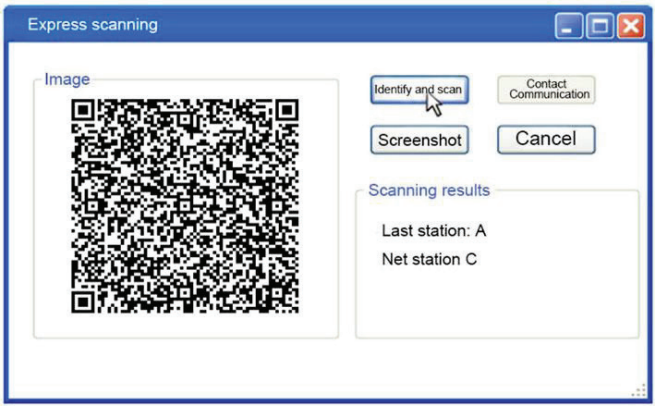

Fig. 5. Scanning results of the distribution mobile terminal.

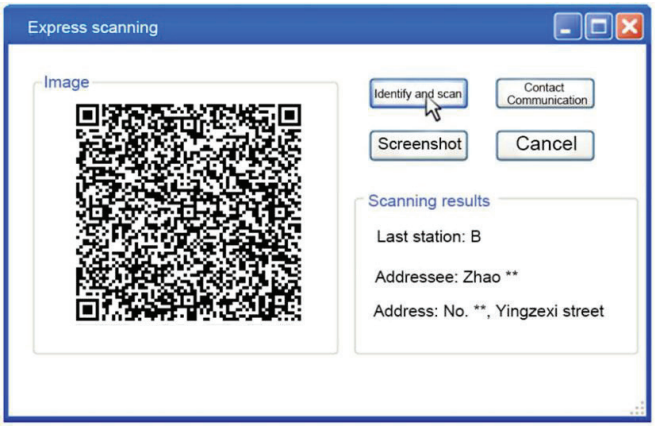

Fig. 6. Scanning result of the mobile terminal.

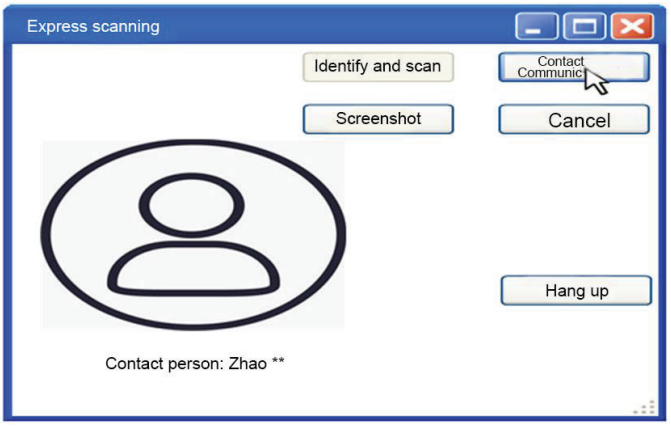

Fig. 7. Mobile terminal communication interface.

The same operation was performed on the other four express documents, and the final test results were similar. The mobile terminals of pick-up, distribution and delivery could only scan the two-dimensional code of documents to obtain partial information about corresponding permission. Meanwhile, the sender could contact the addressee without knowing the contact number, effectively concealing the addressee's contact information.

Test results of system privacy protection in the abnormal flow are shown in Figs. 8 and 9. Fig. 8 is the result of the mobile terminal scanning the non-express two-dimensional code. After scanning the two-dimensional code, the system displayed the two-dimensional code image. And after clicking “identify and scan”, the information in the two-dimensional code was only a series of numbers. The final scan results showed that the two-dimensional code did not have effective logistics information and please confirm whether the two-dimensional code was wrong. Fig. 9 is the scanning result of two-dimensional code of the express by the unauthorized mobile terminal. “Identify and scan” is clicked after the terminal scans the two-dimensional code. The sender and receiver were presented as a string of messy codes, from which helpful information can not be obtained. This operation was also carried out on the other four two-dimensional codes of express mail, all of which could only obtain meaningless error code. The only effective information was a string of website, which is served as the address of the cloud server in the experimental process to store the logistics path that did not include the starting point and endpoint. The above test results indicated that the system could distinguish non-express two-dimensional codes and realize privacy encryption of mobile terminals without permission.

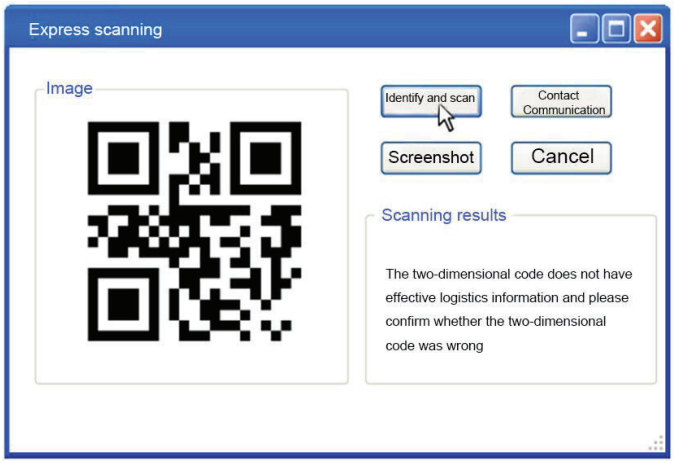

Fig. 8. Scanning results of the mobile terminal for a two-dimensional code that do not belong to express

Fig. 9. Scanning result of two-dimensional code of express by unauthorized mobile terminal.

V. Conclusion

This paper briefly introduced the channels of privacy information disclosure in the process of e-commerce logistics and the privacy information encryption system based on two-dimensional codes and then tested the privacy protective effect on the laboratory server. In the normal process, the pick-up, distribution and delivery mobile terminals had distinct permission. After scanning the two-dimensional code, the pick-up terminal only obtains the sender’s name and the address of the next station. The distribution terminal could only get the address of the last and next stations, while the delivery terminal could only obtain the address of the last station, the recipient’s last name and the recipient’s address, and the sender could contact the recipients without their phone numbers. In the abnormal process, mobile terminals could effectively distinguish non-express two-dimensional codes, and unauthorized mobile terminals could only get a string of meaningless error code and an address of the logistics path that did not include the starting point and endpoint after scanning the express two-dimensional codes.

REFERENCES

[1] J. Qian, X. Du, B. Zhang, B. Fan, and X. Yang, "Optimization of QR code readability in movement state using response surface methodology for implementing continuous chain traceability," *Comput. Electron. Agr*., vol. 139, pp. 56-64, Jun. 2017. DOI: 10.1016/j.compag.2017.05.009

[2] X. Xiao, Z. Fu, Y. Zhang, Z. Peng, and X. Zhang, "SMS-CQ: A Quality and Safety Traceability System for Aquatic Products in Cold-Chain Integrated WSN and QR Code," *J. Food Process Eng*., vol. 40, no. 1, 2017. DOI: 10.1111/jfpe.12303

[3] Y. J. Di, J. P. Shi, and G. Y. Mao, "A QR code identification technology in package auto-sorting system," *Mod. Phys. Lett. B*, vol. 31, no. 19-21, pp. 1740035, May 2017. DOI: 10.1142/S0217984917400358

[4] X. Zhang, H. Li, Y. Yang, G. Sun, and G. Chen, "LIPPS: Logistics Information Privacy Protection System Based on Encrypted QR Code," *2016 IEEE Trustcom/BigDataSE/ISPA,* Aug. 2016. DOI: 10.1109/TrustCom.2016.0167

[5] Q. Han, C. Du, Y. Yao, and L. Lei, "A New Express Management System Based on Encrypted QR Code," *International Conference on Intelligent Computation Technology & Automation*., 2016. DOI: 10.1109/ICICTA.2015.22

[6] P. Y. Lin, "Distributed Secret Sharing Approach with Cheater Prevention based on QR Code," *IEEE T. Ind. Inform*., vol. 12, no. 1, pp. 384-392, Feb. 2016. DOI: 10.1109/TII.2015.2514097

[7] B. Jiang, and E. Prater, "Distribution and logistics development in China," *Int. J. Phys. Distr. Log*., vol. 32, no. 9, pp. 783-798, 2015.

[8] H. Xiang, H. Xiao, and W. Yuan, "Research optimization on logistics distribution center location based on adaptive particle swarm algorithm," *Optik - Int. J. Light Electr. Opt.*, vol. 127, no. 20, pp. 8443-8450, Jun. 2016. DOI: 10.1016/j.ijleo.2016.06.032

[9] R. Kumar, B. Bhaduri, and B. Hennelly, "QR code-based non-linear image encryption using Shearlet transform and spiral phase transform," *J. Mod. Optic*., pp. 1-10, 2017. DOI: 10.1080/09500340.2017.1395486

[10] G. Fimiani, "Supporting Privacy in a Cloud-Based Health Information System by Means of Fuzzy Conditional Identity-Based Proxy Re-encryption (FCI-PRE)," *International Conference on Advanced Information Networking & Applications Workshops*, pp. 569-572, May 2018. DOI: 10.1109/WAINA.2018.00146

[11] Z. Hua, Y. Zhou, C. M. Pun, and C. L. P. Chen, "2D Sine Logistic modulation map for image encryption," *Inform. Sciences*, vol. 297, no. C, pp. 80-94, 2015.

[12] L. Yang, S. Tang, L. Ran, L. Zhang, and Z. Ma, "Secure and robust digital image watermarking scheme using logistic and RSA encryption," *Expert Syst. Appl*., vol. 97, pp. 95-105, 2018. DOI: 10.1016/j.eswa.2017.12.003

[13] Y. Aono, T. Hayashi, T. P. Le, and L. Wang, "Privacy-Preserving Logistic Regression with Distributed Data Sources via Homomorphic Encryption," *IEICE T. Inf. Syst*., vol. E99.D, no. 8, pp. 2079-2089, Aug. 2016. DOI: 10.1587/transinf.2015INP0020

[14] M. Sujatha, V. C. Noronha, A. T. Monteiro, R. Johar, and M. M. Roja, "Dual-Layer Video Encryption using RSA Algorithm," *Int. J. Comput. Appl.*, vol. 116, no. 1, pp. 3-40, Apr. 2015. DOI: 10.5120/20302-2341

[15] G. Iovane, A. Amorosia, E. Benedetto, and G. Lamponi, "An Information Fusion approach based on prime numbers coming from RSA algorithm and Fractals for secure coding," *J. Discrete Math. Sci. C*., vol. 18, no. 5, pp. 25, Sep. 2015. DOI: 10.1080/09720529.2014.894311

Ju Ouyang, born in December 1976, He has received the master's degree from Public Administration of Peking University. He works at Zhejiang Yuying College of Vocational Technology. He is the president of Digital Commerce Branch and an associate professor. He is engaged in e-commerce.

Xianping Chen, born in July 1979, graduated from Zhejiang Sci-Tech University in 2007. She works at Zhejiang Yuying College of Vocational Technology and is vice president of Digital Commerce Branch. She is an associate professor. Her research interests are higher vocational education and technology and innovation management.

CONTENTS PAGE