A Secure E-coupon System for Mobile Users

***Chin-Chen Chang*†,††, *Chia-Chi Wu*††, *Iuon-Chang Lin*†††**

†*Department of Information Engineering and Computer Science Feng Chia University, Taichung, Taiwan*
††*Department of Computer Science and Information Engineering National Chung Cheng University, Chiayi, Taiwan*
†††*Department of Management Information Systems National Chung Hsing University, Taichung, Taiwan*

Summary
Since nowadays mobile phone messages are flourishing, the application of electronic coupon (e-coupon) will become a trend for mobile users. E-coupon for mobile commerce can provide mobility for users and distribution flexibility for issuers. However, most of the existed e-coupon schemes usually apply public-key cryptosystem to achieve the security, which will not be implemented in mobile devices due to the complex computations. In this paper, we propose a novel mobile e-coupon system that just applies some simple cryptographic techniques, such as one-way hash function and message authentication code. In our system, the issuer can control the number of issued e-coupons and prevent them from double-redeeming. The merchant can verify the validity of the e-coupon and the customers can securely transfer the e-coupon to others. The customer does not need to perform any exponential computation in redeeming and transferring the coupons.
Key words:
e-commerce, e-coupon, mobile commerce

1. Introduction

Issuing coupons is a useful and effective strategy to prompt the customer's purchase desires to increase sales volume. For example, the on-line store can issue the e-coupon to customers when they browse the web sites, or when they complete their purchases. Conventionally, customers can obtain coupons from Internet and print out such a coupon with printer and redeem them like any other coupon. Differently, the electronic coupon (e-coupon) earlier was defined as [10]: "a customer needs not print e-coupons as they can be captured electronically in an electronic coupon-caddy, and later redeemed electronically." The idea of e-coupons is raised and we can anticipate that the results of using e-coupons are very obvious.

With the development of SMS (Short Message Service), WAP (Wireless Application Protocol) and MMS (Multimedia Message Services), mobile communications have become very popular around the world, and many applications and services are provided in mobile environment. Thus, if an e-coupon system can allow a customer to receive an e-coupon through his/her mobile device, the customer can not only redeem the coupon over Internet but also can forward this e-coupon to others or merchant through SMS (Short Message Service) or Bluetooth. Thus, the coupon issuer can cooperate with telecommunications industry to carry out marketing activities. Due to this kind of e-coupon is convenient and mobile, hence, that can be applied to E-commerce widely, such as gift certificates, new products promotion, advertisement, and so on. We believe that the e-coupon will soon become a life style for mobile users. A practical e-coupon system must be designed concerning security, efficiency and manageability [11], however, relative researches are few.

Anand et al. [1] designed a distributing e-coupon method in the Internet, they focus on discussing e-coupon content, life cycle and the way distributing the e-coupon to the customer for stimulating her/his purchase desire. Chang et al. [4,5] designed about digital gift certificates and mobile payment mechanisms. Bao designed a kind of digital ticket [3]. He focused on the format of the digital ticket and application cases. Shojima et al. [16] proposed a peer to peer (P2P) e-coupon system. In that system, a service provider provides incentives to mediators who forward e-coupons to potential users. Thus, it is required that the service provider must get the distribution history; nevertheless, the history may be altered in P2P system. They apply the queue structure and some cryptographic techniques to maintain distribution history and prevent altering attack. They use public key cryptosystem that must perform complex exponential computations, it is more suitable to implement in the personal computers and Internet.

However, the conventional e-coupon schemes

Manuscript revised August 22, 2005.

may be not suitable for mobile environment. If the e-coupon system can be used in mobile devices, we have to consider the processing cost. According to Rivest and Shamir's evaluation [15] that hash functions are about 100 times faster than RSA signature verification, and about 10,000 times faster than RSA signature generation. In general, the mobile equipments have small memory space and low computational capability. Thus, a practical e-coupon system for mobile users must be efficiently performed with low computational cost, low communication cost, and small memory space overhead.

In this paper, we proposed a novel complete e-coupon transaction system, which uses the smart card and the hash computations to solve the e-coupon transaction problems with security and processing efficiency, and the whole process can be performed mobility. The rest of this paper is organized as follows. In Section 2, we shall propose the requirements of e-coupon system. Then, in Section 3, we present our proposed system, followed by some discussions as to how the new system performs in terms of security and efficiency in Section 4. Finally, a concluding remark will be given in Section 5.

2. The Requirements of the e-coupon system

The e-coupon system must satisfy the following requirements to achieve security and manageability.

1. Identification: Each e-coupon must be identified its ownership so as to prevent the attacker masquerading as eligible owner to consume it.
2. Transferability: Each e-coupon can be transferred among customers, but the original owner must authorize it.
3. Unforgeability: Only issuer can offer valid e-coupons, any other entities cannot forge them.
4. Non-repudiation: Each entity cannot deny the transactions in which she/he has participated.
5. Expired: E-coupon can set expired date [6,7].
6. States manageability [8,9]: Whether the e-coupon is consumed or not must be considered in the system.
7. Independence: E-coupon system can be implemented in heterogeneous platforms.
8. Machine-understandability: E-coupon implemented by XML language [9] can achieve machine-readability to enhance efficiency.

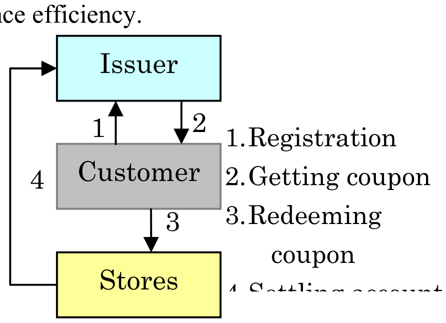

Fig. 1 The e-coupon system mode

3. The Proposed Scheme

In this section, we will propose a secure e-coupon system for mobile users. Generally, if the enterprises want to increase sales, they might make effort in sales promotion; for example, give some coupons when the customer buys a considerable amount of merchandises or services. However, they must issue coupons in a limited number, or sales revenue will be reduced. Therefore, we simply construct the e-coupon model as Fig. 1.

In this model, the issuer, such as enterprise headquarter or manufacture, issues and controls the number of coupons; the branch stores (the service providers) provide the merchandises or services for customers when they redeem the coupons. Besides, the customer may redeem the coupon using the mobile device, so low computation power and communication capabilities must be considered in the customer end. On the other hand, the issuers do not want the coupons to be suffered from forging, which will result in great damage. The e-coupon system can be divided into four phases: registration phase, issuing phase, redemption phase and transferring phase. We first explain the notations in Section 3.1, and then, describe the proposed system in Section 3.2.

3.1 The notations

We divide notations into four parts such that we can observe clearly that each entity must maintain parameters and store information.

The public parameters and computation functions are listed as follows.

$Cert_A$: Certification for entity A.

b: The identification number for service provider S_b.

W: The upper bound of the service provider's identification number.

EXD: Expiration Date of the coupon, which is a public data.
Now: Current date.
$H^t(\ )$: The collision free one way hash function [2,14] of performing t times.
$Sign_A(m)$: The message m is signed by A's private key.
$E_k(\ )$: A symmetric encryption function using the key k.
$||$: The concatenation symbol.
The notations regarded to the customer are listed as follows.
C: Standing for the customer.
RI: Registration Information including the customer personal information.
CID: Customer's Identification after she/he completes the registration.
$\alpha_1, \alpha_2, \alpha_3, \alpha_4$: Four long length random numbers.
The notations regarded to the issuer are listed as follows.
ISU: Standing for the Issuer.
SN: Serial Number of the coupon.
k: The shared key between ISU and the registered customer.
Redeemed table: Collecting the redeemed SN of the coupon.
In addition, the notation S stands for the issuer (service provider).

3.2 The proposed system

Initially, we assume that Public Key Infrastructure (PKI) has already existed in the network; each entity has its own public key, private key and certificate. Four procedures of coupon system will be described in detail.

Registration Phase

Ci must register to *ISU* before she/he gets the coupon from ISU. In this phase, since pre-shared key must store into smart card securely, all the communications are performed in a secure channel. We demonstrate the steps as follows:

1. C_i sends the RI_i and the personal $Cert_i$ to *ISU* for registration.
2. After receiving the message, *ISU* verifies it, and then generates a unique CID_i and k_i , which are sent to C_i. At the same time, *ISU* stores (CID_i, RI_i, $Cert_i$, k_i) to the *Registration table*.
3. C_i must store (CID_i, k_i) into smartcard or SIM (Subscriber Identity Module) card. The k_i must be well protected, because it is the shared key.

Issuing phase

When *ISU* determines to issue an e-coupon to the customer C_i, he must notify and deliver related messages to C_i for verifying. In this phase, all messages can be transferred in a public channel. This phase performs communications as Fig.2.

1. First, *ISU* sends (W, EXD) to C_i and notifies her/him to get the coupon. C_i generates four random numbers α_1, α_2, α_3, α_4 and sets D=[$H^W(\alpha_1)||H^W(\alpha_2)||H^{EXD}(\alpha_3)||H^{EXD}(\alpha_4)$], then computes $E_{k_i}[\alpha_1, \alpha_2, \alpha_3, \alpha_4, D]$ and sends the outcome to *ISU*.
2. Once receiving the above message, *ISU* decrypts it using the key k_i to get [$\alpha_1, \alpha_2, \alpha_3, \alpha_4, D$]. Then, *ISU* computes $H^W(\alpha_1)$, $H^W(\alpha_2)$, $H^{EXD}(\alpha_3)$, $H^{EXD}(\alpha_4)$ and compares the result with the received D. If they are equal, *ISU* generates the *SN* to set m = ($SN||D$) and computes s=$Sign_{ISU}(H(m))$ and delivers (SN, s) to C_i.
3. C_i computes $H(SN||D)$ and uses *ISU*'s public key to get $H(m)$ from s. If they are equal, C_i can make sure that she/he has gotten the coupon :{ m, s}.

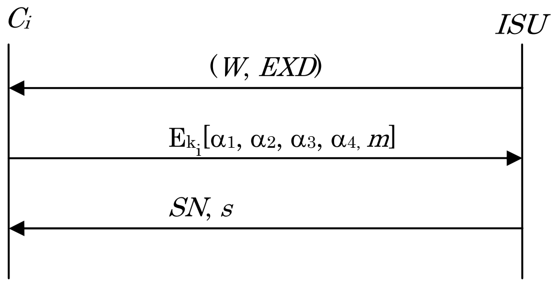

Fig. 2 The protocol of issuing phase

Redemption phase

In this phase, C_i can redeem the coupon to exchange proper services to the service provider S_b. S_b can verify the coupon, and prevent double spending through checking redeemed e-coupons by *ISU*. All the communications can be performed via a public channel as Fig.3, since the messages are protected and verified.

1. If C_i wants to redeem the coupon, she/he computes β_1=$H^b(\alpha_1)$, β_2=$H^{W-b}(\alpha_2)$, β_3= $H^{NOW}(\alpha_3)$, and β_4= $H^{EXD-NOW}(\alpha_4)$ and then sends (EXD, β_1, β_2, β_3, β_4, coupon) to S_b. S_b computes x_1=$H^{W-b}(\beta_1)$, x_2=$H^b(\beta_2)$, x_3= $H^{EXD-NOW}(\beta_3)$, and x_4= $H^{NOW}(\beta_4)$.
2. Then, S_b computes $H(SN||x_1|| x_2|| x_3|| x_4)$ which can be verified by the signature s using *ISU*'s public key. If it holds, then the coupon is valid. S_b must forward (EXD, β_1, β_2, β_3, β_4, coupon) to *ISU*.
3. *ISU* uses the received information to compute y_1=$H^{W-b}(\beta_1)$, y_2=$H^b(\beta_2)$, y_3=$H^{EXD-NOW}(\beta_3)$, and y_4=$H^{NOW}(\beta_4)$. After completion, *ISU* then executes the following two checking:
   (1) She/he computes $H(SN||y_1||y_2|| y_3||y_4)$ which can be verified by the signature s using *ISU*'s public key. If

it holds, then *ISU* checks whether this *SN* exists in *Redeemed table*, else notifies S_b that the transaction does not pass the validation checking.

(2) If *SN* does not appear in *Redeemed table*, *ISU* must record it into *Redeemed table* and deliver the valid information to S_b, or else *ISU* notifies S_b that this coupon is redeemed.

4. After S_b receives the valid response from *ISU*, S_b must provide the merchandises or services to C_i according to the coupon declared.
5. If the coupon passes the *ISU* validation, S_b must keep the coupon for settling the account with *ISU* to obtain subvention.

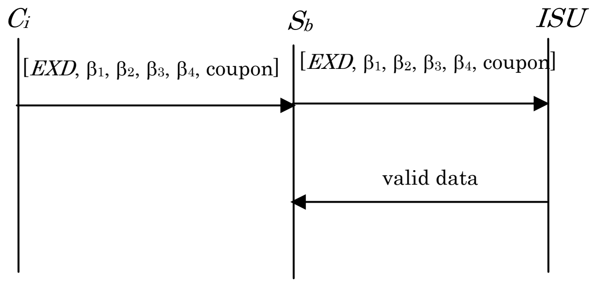

Fig. 3 The protocol of redemption phase

Transferring phase

When C_i wants to transfer his/her coupon to C_j, since C_j cannot know the transferred coupon's status (unredeemed/redeemed), this coupon must be transferred to *ISU* for checking its status and changing the signature of the coupon. Assuming that C_i and C_j are registered already, this phase performs communications as Fig.4, we describe the procedures as follows.

1. C_j delivers a transfer request to C_i. Once receiving the request, C_i immediately transmits E_{k_i}(coupon|| CID_j) to *ISU*.
2. When *ISU* receives the message, she/he can decrypt it using k_i and verify validation of the coupon via signature s. If they are valid, then *ISU* checks *Redeemed table* to confirm this coupon has not been redeemed.
3. *ISU* generates four random numbers (γ_1, γ_2, γ_3, γ_4) to compute $H^W(\gamma_1)$, $H^W(\gamma_2)$, $H^{EXD}(\gamma_3)$, $H^{EXD}(\gamma_4)$, and $s'=\mathrm{Sign}_{ISU}[H(SN||H^W(\gamma_1)||H^W(\gamma_2)||H^{EXD}(\gamma_3)||H^{EXD}(\gamma_4))]$. Then, *ISU* transfers $\{E_{k_j}(\gamma_1, \gamma_2, \gamma_3, \gamma_4)||SN|| s'||W||EXD\}$ to C_j.
4. Upon receiving the above message, C_j decrypts the (γ_1, γ_2, γ_3, γ_4) using the key k_j. At last, C_j computes $H(m')=H(SN||H^W(\gamma_1)||H^W(\gamma_2)||H^{EXD}(\gamma_3)||H^{EXD}(\gamma_4))$ to verify the signature s' using *ISU*'s public key. If it holds, the coupon (m', s') is confirmed to be transferred.

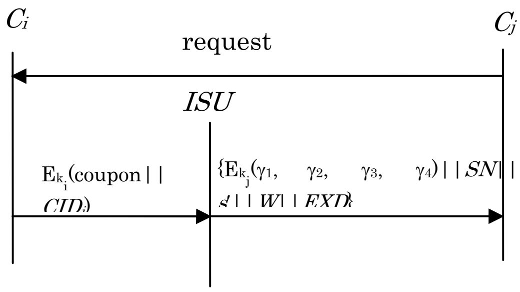

Fig. 4 The protocol of transferring phase

4. Security and Practicability Discussions

In this section, we analyze the security and efficiency of our e-coupon system. The security requirements are explained in Section 4.1. The performance is discussed in Section 4.2.

4.1 Security Discussions

This system can satisfy the security characteristics as follows.

1. Confidentiality: The system protects the secure parameters (α_1, α_2, α_3, α_4) using symmetric encryption scheme from eavesdropping.
2. Verifiability:
   (1) The coupon can be verified by any entity, since s was signed by *ISU*.
   (2) *ISU* can easily validate the *Redemption date* and *S*s identification number, because (α_1, α_2, α_3, α_4) are secret and the hash values are unique and not reversible. If S_b tampers b, she/he will lose the subvention from *ISU*. Without knowing (α_1, α_2, α_3, α_4), the attacker cannot tamper $H^b(\alpha_1)$, $H^{W\text{-}b}(\alpha_2)$, $H^{NOW}(\alpha_3)$or $H^{EXD\text{-}NOW}(\alpha_4)$.
3. Preventing forgery: The coupon is not forged, because it must be signed by *ISU*, anyone else is unable to get the *ISU*s private key.
4. Preventing alternation:
   This system can prevent two kinds of alternation attack:
   -- No one can change the content of the coupon, since it is signed by *ISU*.
   -- The service provider S_a cannot change $H^b(\alpha_1)$, $H^{W\text{-}b}(\alpha_2)$, $H^{NOW}(\alpha_3)$or $H^{EXD\text{-}NOW}(\alpha_4)$, because she/he can not get (α_1, α_2, α_3, α_4).
5. Preventing duplicate-redemption: *ISU* can collect each *SN* of the redeemed coupon. If a customer repeatedly redeems it, *ISU* will find out immediately.
6. Preventing reproduction: If the malicious customer reproduces the coupon that will not be feasible, since both the coupon and owner have been signed by *ISU*.
7. Non-repudiation:
   (1) In issuing phase, the customer generates [α_1, α_2, α_3, α_4, D] and *ISU* signs the coupon, so that they can not deny them.
   (2) In redemption phase, S_b gets the (EXD, β_1, β_2, β_3, β_4, coupon) from C_i and *ISU* stores

the redeemed *SN* of the coupon. The customer thus cannot to deny this redemption, since the customer knows (α_1, α_2, α_3, α_4). *ISU* will not generate a fake coupon, though he/she got (α_1, α_2, α_3, α_4). Because *ISU* is a payer in this scenario, the fake coupon will damage *ISU*'s profit.

(3) In the coupon transferring, *ISU* can manage the transferring process to achieve non-repudiation between C_i and C_j.

8. Expired: E-coupon uses $H^{EXD}(\alpha_3)$ and $H^{EXD}(\alpha_4)$ to set expired date. When the customer uses the coupon out of the expired date, he/she will not to redeem it, because he/she can not generate β_4=$H^{EXD\text{-}NOW}(\alpha_4)$. If he/she changes *EXD* to generate β_4'= $H^{EXD'\text{-}NOW}(\alpha_4)$, then S_b computes x_4= $H^{NOW}(\beta_4')$ will not be equal to $H^{EXD}(\alpha_4)$ of the *D*.
9. States manageability: *ISU* can easily manage the status of the coupon, because he/she has *redeemed table* to collect *SN* of the redeemed coupon.

4.2 Efficiency analyses

1. Computation efficiency: In redemption phase, the customer only computes hash values. In coupon transferring, the original customer performs symmetric encryption, unlike a public key system that needs a great deal of computation resources. According to Xiao et al.'s measurement [17], DES [12] computation is about 1000 times faster than RSA [13] computation. This system can be implemented in mobile phone or PDA, since customers do not perform any exponential computations in the redemption phase.
2. Controllability: The *ISU* can control the number of *SN*'s that issued, which can avoid damaging estimated profits.
3. Trust manageability: In the coupon transferring, *ISU* can manage the transaction and check coupon content to achieve reliability for customers.

5. Conclusions

In this paper, we have proposed the first secure electronic coupon system for mobile users. In our system, the e-coupon can be applied to e-commerce flexibly and securely. The issuer can control the number of issued coupons and prevent double spending. Furthermore, the coupon can be verified by anyone to prevent forging attack. According to the analyses above, our system's computation cost is less than that of public key system, which is more practical and convenient for applications using mobile devices or smart cards.

References

[1] R. Anand, M. Kumar and A. Jhingran, "Distributing E-Coupon on the Internet," *Proceedings of the 9th Annual Conference of the Internet Society* (INET'99), 1999. http://www.isoc.org/inet99/proceedings/1d/1d_1.htm

[2] E. Biham and A. Shamir, "Differential Cryptanalysis of the Data Encryption Standard," *Springer Verlag*, Belin, 1993.

[3] Feng Bao, "A Scheme of Digital Ticket for Personal Trusted Device," *Proceedings of the 15th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC 2004)*, Vol. 4, pp. 3065-3069, 2004.

[4] C. C. Chang and Y. F. Chang, "Schemes for Digital Gift Certificates with Low Computation Complexity," to appear in *Informatica*, 2005.

[5] C. C. Chang, Y. F. Chang and J. S. Lee, "Mobile Payment for Off-line Vender Machines," *International Journal of Computer Science and Network Security*, pp. 119-126, Sept. 2005.

[6] C. C. Chang, J. Y. Kuo and J. S. Lee, "Time-bounded Based Password Authentication Scheme," to appear in 2005 *International conference on Cyberworlds*, Singapore, 2005.

[7] C. I. Fan, W. K. Chen and Y. S. Yeh, "Date Attachable Electronic Cash," *Computer Communications*, Vol. 23, Issue: 4, pp. 425-428, Feb. 2000.

[8] K. Fujimura, H. Kuno, M. Terada, K. Matsuyama, Y. Mizuno, and J. Sekine, "Digital-Ticket-Controlled Digital Ticket Circulation," *Proceedings of the 8th USENIX Security Symposium,* Washington D.C., USA, pp. 229-238, Aug. 1999.

[9] K. Fujimura and Y. Nakajima, "General-Purpose Digital Ticket Framework," *Proceedings of the 3rd USENIX Workshop on Electronic Commerce,* Boston, Massachusetts, USA, pp. 177-186, Aug. 1998.

[10] M. Kumar, A. Rangachari, A. Jhingran, and R. Mohan, "Sales Promotions on the Internet," *Third USENIX workshop on Electronic Commerce*, Boston, pp. 167-176, Sept. 1998.

[11] K. Matsuyama and K. Fujimura, "Distributed Digital-Ticket Management for Rights Trading System," *Proceedings of the 1st ACM conference on Electronic commerce,* pp.110-118, Nov. 1999.

[12] NBA FIPS PUB 46-1, "Data Encryption Standard," National Bureau of Standards, U.S. Department of Commerce, Jan. 1988.

[13] R. Rivest, A. Shamir and L.Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Communications of the ACM, Vol.21, No.2, pp.120-126, Feb. 1978.

[14] R. Rivest, "The MD5 Message Digest Algorithm," RFC 1321, 1992.

[15] R. Rivest and A. Shamir, "PayWord and MicroMint: Two simple micropayment schemes," May 1996. Available at http://theory.lcs.mit.edu/~rivest/RivestShamir-mpay.ps

[16] T. Shojima, Y. Ikkai and N. Komoda, "A Method for Mediator Identification Using Queued History of Encrypted User Information in an Incentive Attached Peer to Peer Electronic Coupon System," *Proceedings of the 2004 IEEE International Conference on System, Man and Cybernetics*, pp. 1086-1091, 2004.

[17] Li Xiao, Zhichen Xu, and Xiaodong Zhang, "Low-Cost and Reliable Mutual Anonymity Protocols in Peer-to-Peer Networks," *IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS*, VOL. 14, NO. 9, pp.829-840, Sep. 2003.

Chin-Chen Chang received his BS degree in applied mathematics in 1977 and his MS degree in computer and decision sciences in 1979, both from the National Tsing Hua University, Hsinchu, Taiwan. He received his Ph.D in computer engineering in 1982 from the National Chiao Tung University, Hsinchu, Taiwan. During the academic years of 1980-1983, he was on the faculty of the Department of Computer Engineering at the National Chiao Tung University. From 1983-1989, he was on the faculty of the Institute of Applied Mathematics, National Chung Hsing University, Taichung, Taiwan.From 1989 to 2004, he has worked as a professor in the Institute of Computer Science and Information Engineering at National Chung Cheng University, Chiayi, Taiwan. Since 2005, he has worked as a professor in the Department of Information Engineering and Computer Science at Feng Chia University, Taichung, Taiwan. Dr. Chang is a Fellow of IEEE, a Fellow of IEE and a member of the Chinese Language Computer Society, the Chinese Institute of Engineers of the Republic of China, and the Phi Tau Phi Society of the Republic of China. His research interests include computer cryptography, data engineering, and image compression.

Chia-Chi Wu was born on December 9, 1967 in Taoyuan, Taiwan, Republic of China (ROC.). He received the B.S. in Information Management from National Defense Management College, Taipei, Taiwan, Republic of China, in 1991; the M.S. in Information Management from National Defense Management College, Taiwan, in 1999. He is currently pursuing his Ph.D. degree in computer science and information engineering from National Chung Cheng University, Chiayi, Taiwan. His current research interests include electronic commerce, information security, cryptography, and mobile communications.

Iuon-Chang Lin was born on December 21, 1974 in Taipei, Taiwan, Republic of China (ROC.). He received the B.S. in Computer and Information Sciences from Tung Hai University, Taichung, Taiwan, Republic of China, in 1998; the M.S. in Information Management from Chaoyang University of Technology, Taiwan, in 2000. He received his Ph.D. in Computer Science and Information Engineering in March 2004 from National Chung Cheng University, Chiayi, Taiwan. From 2004 to 2005, he was an assistant professor of the Department of Information Management, National Kaohsiung University of Applied Sciences, Taiwan, ROC. He is currently an assistant professor of the Department of Management Information Systems, National Chung Hsing University, Taichung, Taiwan, ROC. His current research interests include, but not limited to, electronic commerce, information security, cryptography, neural networks, and electronic image processing.