Journal of Information Hiding and Multimedia Signal Processing ©2015 ISSN 2073-4212
Ubiquitous International Volume **6**, Number **2**, March **2015**

A Biometrics-based Multi-server Key Agreement Scheme on Chaotic Maps Cryptosystem

Hongfeng Zhu, Xin Hao, Yifeng Zhang and Man Jiang
Software College, Shenyang Normal University
No.253, HuangHe Bei Street, HuangGu District, Shenyang, P.C 110034-China
{zhuhongfeng1978; haoxin20110202}@163.com; {1548452125; 459589817 }@qq.com

Received May, 2014; revised Octobe, 2014

Abstract. *Nowadays chaos theory is widely used in cryptography. In the real world, in order to ensure secure communication, many chaotic maps-based key agreement protocols have been proposed. Most of them used a smart card on account of the inherent ability of anti-interference. Popularly, many related protocols using smart card are used for a single server environment. However, existing single server authentication protocols more or less have some defects. For a single server environment, if a remote user feels like using a number of network services, it is so complicated and boring to repeatedly register a new identity and password. To address this problem, numerous multi-server authentication schemes have been proposed. However, these existing proposed schemes pay attention to efficiency to ignore confidentiality, or focus on the message integrity to ignore efficiency. In our proposed paper, we propose a robust biometrics-based multi-server password-authenticated key agreement scheme on chaotic maps cryptosystem. In terms of the analysis of the security and functionality, the proposed scheme has a mass of merits, for instance, prefect forward secrecy, session key secrecy, robust biometrics authentication, password update secrecy, mutual authentication and key agreement. In addition, the proposed scheme can resist common attacks such as guessing attack, replay attack, man-in-the-middle attack and so on. In terms of the efficiency analysis, the proposed scheme is more practical.*

Keywords: Biometrics, Multi-server, Key agreement, Smart card, Chaotic maps

1. **Introduction.** With the development of information technology and Internet, network information security problem has become the key problem affecting social stability and national security. Cryptosystem, as the core of information security technology, can provide information confidentiality, integrity, availability and non-reputation. Cryptosystem is mainly composed of cryptography and cryptanalysis. Briefly, cryptography mainly researches how to encode plaintext in order to realize information hiding, and cryptanalysis mainly researches how to decode ciphertext in order to gain corresponding plaintext. Cryptography and cryptanalysis are contradictory and interdependent, thus promoting the rapid development of cryptosystem. Chaos is a special form of motion. It means that in a certain nonlinear system, with no need for any random factors also can appear similar to the behavior of random phenomena. Chaotic system is extremely sensitive to initial parameters and the chaotic sequence produced by chaos has the nature of non-periodicity and pseudo-randomness. In short, chaotic system has the characteristics of certainty, boundedness, sensibility to initial parameters and unpredictability, etc. As the characteristics of chaotic system and cryptosystem are similar, chaos theory has widely noted by cryptographic circle, and chaotic system has opened up a new way for cryptography

technique research. Biological recognition technology is a technology based on our own inherent physiological or behavioral characteristics. Usually, common passwords, IC card, bar card, magnetic card have many disadvantage factors: easily forgotten, replication, lost, stolen, etc. It is worth mentioning that the human body characteristics have unrepeatable uniqueness. They could not be copied, stolen or forgotten. It is safe and reliable to use biological recognition technology for identity authentication. Obviously, smart card has powerful information confidentiality and flexible portability. However, many protocols using smart card are used for a signal server environment. For a multi-server environment, if a remote user feels like using a number of network services, it is so complicated and boring to repeatedly register a new identity and password. To address this problem, we propose a robust biometrics-based multi-server password-authenticated key agreement scheme. At present, many chaotic maps-based schemes have been come up and widely used [1,15-19,21-27]. In 2013, Guo et al. [15] proposed a chaotic maps based password–authenticated key agreement protocol with smart cards, the scheme avoids modular exponential computing or scalar multiplication on an elliptic curve. In the same year, Xie et al. [1] proposed a first chaotic maps-based three-party password-authenticated key agreement (3PAKA) scheme without using a timestamp. As a single-server authentication scheme, it has the same mentioned defects with other similar schemes [2,5-8]. If a remote user feels like using a number of network services, it is so complicated to repeatedly register a new identity and password at numerous servers. To address this problem, many multi-server authentication schemes have been proposed [3,4,9,10,14,28-30]. In 2004, Juang [3] proposed a user authentication and key agreement scheme using smart cards for multi-server environment with low computation and communication costs. However, in the same year, Chang et al. [4] pointed out that Juangs scheme lacks efficiency, and proposed an efficient and secure authentication scheme to improve the weakness. However, Changs scheme cannot resist insider attack. In 2008, Tsai [9] proposed an alternative multi-server scheme using smart cards based on one-way hash function, which did not use any verification table. It avoided the computation cost problem. However, Tsais scheme suffers from server spoofing attacks and privileged insider attacks which were referred by some adversaries [12,13]. In 2010, Wu et al. [14] proposed a user authentication and key exchange protocol using bilinear pairings for mobile client-server environment. In the same year, Wu et al. [35] proposed another protocol using bilinear pairings which was well suited for a client-server environment with low-power mobile devices. In 2010, Yoon et al. [10] proposed an efficient and secure biometrics-based multi-server authenticated with key agreement scheme for smart cards on elliptic curve cryptosystem. The presented scheme had many practical merits: prefect forward secrecy, session key secrecy, robust biometric authentication and password update secrecy, and it can withstand common attacks. Meanwhile, it can reduce the total execution time and memory requirement. As the scheme cannot avoid modular exponential computing or scalar multiplication on an elliptic curve, it lacks efficiency and needs heavy computation costs. In 2012, Chuang et al. [36] proposed an ID-based mutual authentication and key agreement scheme based on bilinear maps for mobile multi-server environment. However, the efficiency of bilinear maps computation is low. In our paper, we propose a biometrics-based multi-server authentication key agreement scheme on chaotic maps cryptosystem. Compared the properties with related schemes, our proposed scheme has more satisfactory and practical merits. Our contributions are mainly embodied in the following respects: (1) We effectively combine biometrics authentication with chaotic maps. (2) We avoid modular exponential computing or scalar multiplication on an elliptic curve. (3) The proposed scheme not only provides prefect forward secrecy, session key secrecy, robust biometrics authentication and password update secrecy, but also can resist common attacks. In addition, the proposed scheme has better practicability. The rest of the paper is organized as follows: In the next section, we review some preliminaries. Sect. 3 describes our proposed scheme. Sect. 4, 5 and 6 discuss the security, functionality and efficiency of the proposed scheme. Finally, the paper is concluded in Sect. 7.

2. Preliminaries.

The concepts of multi-server environment, Chebyshev chaotic maps, biometrics authentication are introduced in this section, respectively.

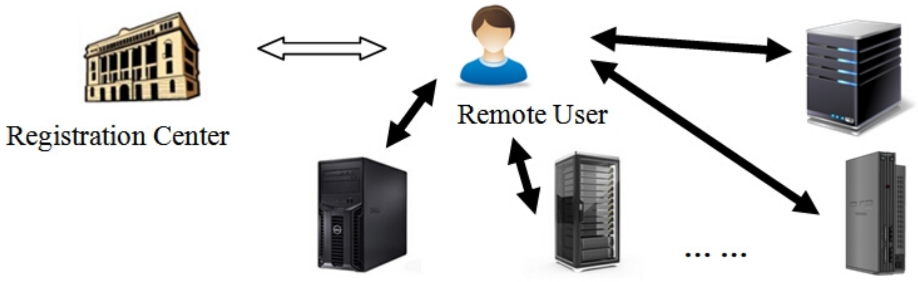


FIGURE 1. Multi-server environment

2.1. Multi-server environment.

In a single-server environment, if a remote user feels like using a number of network services, it is so complicated to repeatedly register a new identity and password at various servers and accurately remember them. To address the problem, several multi-server environment schemes for remote user have been proposed [3,4,9,10,14,28-30]. In a multi-server environment, firstly, each remote user must register he/her identity and password with the registration center to get a smart card, and then he/her uses the smart card to login various servers. For a communication, each remote user must perform authentication procedure to login servers. Fig. 1 shows the multi-server environment.

2.2. Chebyshev chaotic maps.

This part introduces some knowledge about Chebyshev polynomial and Chebyshev chaotic maps [1,18].

Definition 2.1. *Let be an integer, and let be a variable, the value of belongs to the interval. Chebyshev polynomial $T_n(x):[-1,1]\to[-1,1]$ is defined as*

$$T_n(x)=\cos(narccos(x)) \tag{1}$$

In accordance with Definition 1, the recurrence relation of Chebyshev polynomial is defined as

$$T_n(x)=2xT_{n-1}(x)-T_{n-2}(x), n\geq 2, where T_0(x)=1 \text{ and } T_1(x)=x \tag{2}$$

Definition 2.2. *Chebyshev polynomial has the following two important properties:*
(1) The chaotic property
When $n\geq 1$, Chebyshev polynomial map $T_n(x):[-1,1]\to[-1,1]$ of degree is a chaotic map with its invariant density $f^*(x)=1/(\pi\sqrt{1-x^2})$, for positive Lyapunov exponent $\ln n$
(2)The semi-group property

$$T_r\left(T_s\left(x\right)\right)=\cos\left(r\cos^{-1}\left(s\cos^{-1}\left(x\right)\right)\right)=\cos\left(rs\cos^{-1}\left(x\right)\right)=T_{rs}\left(x\right)=T_s\left(T_r\left(x\right)\right) \tag{3}$$

In 2008, Zhang [20] proved that the semi-group property of Chebyshev polynomial defined on the interval $(-\infty, +\infty)$ holds, as follows:

$$T_n(x) \equiv (2xT_{n-1}(x) - T_{n-2}(x)) \bmod p \tag{4}$$

where $n \geq 2, x \in (-\infty, +\infty)$, and p is a large prime number. Evidently,

$$T_r(T_s(x)) \equiv T_{rs}(x) \equiv T_s(T_r(x)) \bmod p \tag{5}$$

The following problems about Chebyshev polynomials are assumed to be intractable within polynomial time.

Definition 2.3. *Given two variables x and y , it is intractable to find the integer s, such that $T_s(x) = y$. It is called the Chaotic Maps-based Discrete Logarithm (CM-DL) problem.*

Definition 2.4. *Given three elements x, $T_r(x)$, $T_s(x)$, it is intractable to find $T_{rs}(x)$, such that $T_r(T_s(x)) = T_{rs}(x)$ or $T_s(T_r(x)) = T_{rs}(x)$. It is called the Chaotic Maps-Based DiffieHellman (CM-DH) problem.*

2.3. **Biometrics authentication.** Each user has their inherent physiological or behavioral characteristics. At present, there have been many biometrics technologies such as voice recognition, fingerprint recognition, iris recognition hand geometry recognition, face recognition, etc. Biological recognition technology has irreplaceable advantages: reliability, availability, non-repudiation, less cost, etc. As is well-known, biometrics authentication has widely used. In addition, smart card has powerful information confidentiality and flexible portability. When performing a biometrics recognition process, a user inputs a smart card, and makes use of a simple touch with a glance at a camera to authenticate herself/himself [5-7]. Fig.2 is the flow chart of biometrics recognition process. In Fig.2, firstly, the user needs to input the image which wants to be identified in the biometrics recognition system. Secondly, on the one hand, the system performs detection, location and pretreatment, and then extracts the feature; on the other hand, the system draws on the stored sample library. Next, the system compares the extracted feature sample with the stored sample, and outputs the result.

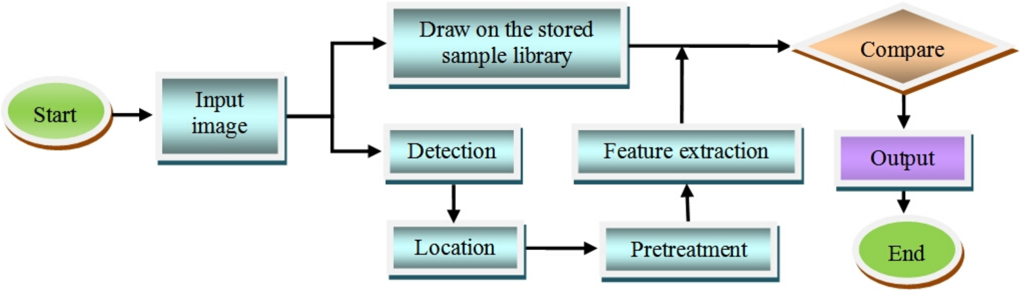


FIGURE 2. The flow chart of biometrics recognition process

3. **The proposed protocol.** This part describes the proposed scheme in detail. The proposed scheme consists of four phases: multi-environment setup phase, the user registration phase, the authentication key agreement phase, and the biometrics and password update phase, respectively. Symbols used in the proposed scheme are defined in Table 1 as follows:

Table 1. Symbols

Symbol	Definition
U,ID_U,PW_U	user, the identity of user, the password of user, respectively
S_j,ID_{S_j}	the$j$thserverthe identity of the$j$thserver, respectively
RC	registration center
B	the biometrics sample of user
τ	predetermined threshold for biometrics authentication
$d(\cdot)$	symmetric parametric function
$(x, T_k(x)), k$	the public key and secret key of RC, respectively
$E_K(\cdot)$,$D_K(\cdot)$	secure symmetric encryption/decryption algorithm with secret key$K$
$a.b$	random integer number
SK	session key
$h(\cdot)$	secure one-way hash function
$\oplus$,$\|\|$	XOR operationconcatenation operationrespectively

3.1. Multi-server environment setup phase.

In the multi-server environment setup phase, RC released its public key $(x, T_k(x))$ to all servers, for all servers $S_j(1 \leq j \leq n)$ shown in Fig.3, they send their identities ID_{S_j} to RC, RC computes $R_{S_j} = h(ID_{S_j}||k)$, $S_{S_j} = R_{S_j} \oplus h(ID_{S_j})$, where k is the secret key of RC, and sends S_{S_j} to S_j. S_j stores S_{S_j} in it.What calls for special attention is that all servers must be authenticated by registration center before they provide services for users.

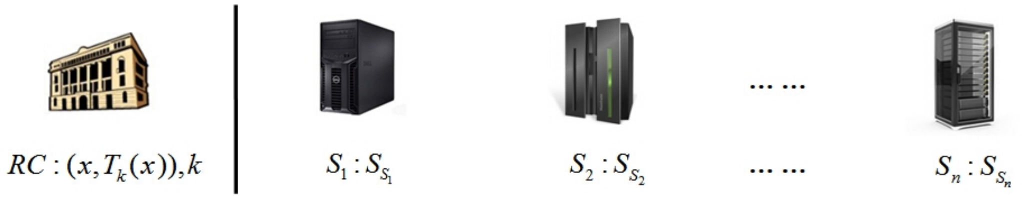


Figure 3. The multi-server environment setup phase

3.2. User registration phase.

Fig.4 illustrates the user registration phase. The steps are performed as follows.

Step 1 When a user U wants to be a new legal user, U chooses his/her identity ID_U , password PW_U at liberty, and also inputs his/her personal biometrics image sample B at the sensor. Then U submits $\{ID_U, h(PW_U||B), B\}$ to RC via a secure channel.

Step 2 Upon receiving $\{ID_U, h(PW_U||B), B\}$, RC computes $R_U = h(ID_U||k)$ and $Z_U = R_U \oplus h(PW_U||B)$. Then RC stores $\{Z_U, B, h(\cdot), d(\cdot), \tau\}$ in a smart card, and gives the smart card to U via a secure channel, where $d(\cdot)$ is a symmetric parametric function and τ is predetermined threshold for biometrics authentication.

3.3. Authenticated key agreement phase.

Fig.5 illustrates authenticated key agreement phase. The steps are performed as follows.

Step 1 If U wishes to establish a session key with S_j , he/her inputs the smart card into a card reader, opens the login application software, and imprints biometric B^* at the sensor. Then the biometrics authentication process of smart card compares the newly captured B^* with the stored B. If $d(B^*, B) \geq \tau$, that means U will get a connection

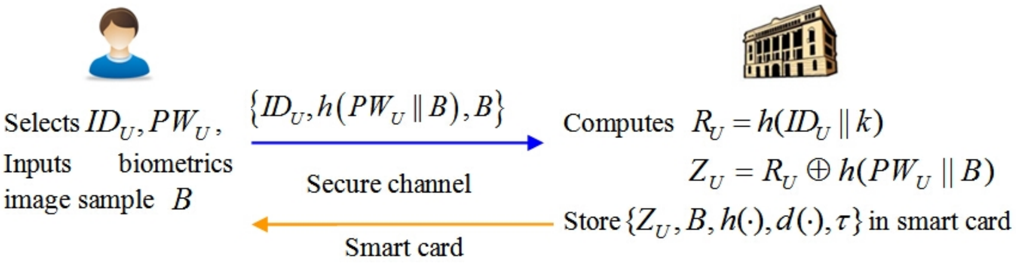
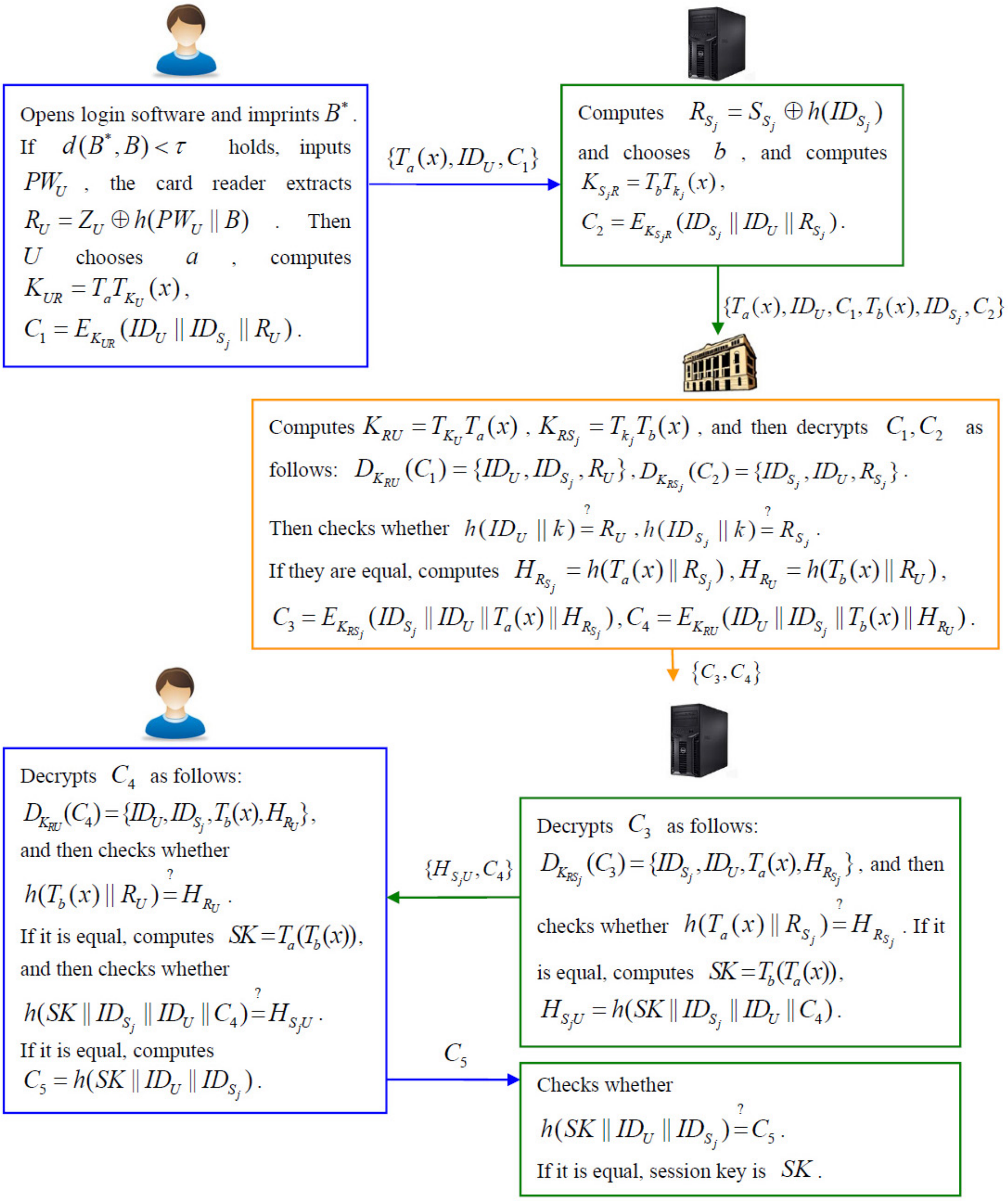

Selects ID_U, PW_U,
Inputs biometrics image sample B
$\{ID_U, h(PW_U \| B), B\}$
Secure channel
Smart card
Computes $R_U = h(ID_U \| k)$
$Z_U = R_U \oplus h(PW_U \| B)$
Store $\{Z_U, B, h(\cdot), d(\cdot), \tau\}$ in smart card

FIGURE 4. The user registration phase

refused response. If $d(B^*, B) < \tau$, that means U will get a connection accepted response. Then U will get a connection accepted response. Then U inputs his/her password PW_U, and the card reader extracts R_U by computing $Z_U \oplus h\,(PW_U||B)$. Then U chooses a random integer number a, computes $K_{UR} = T_aT_k(x)$, $C_1 = E_{K_{UR}}(ID_U||ID_{S_j}||R_U)$. After that, U sends $\{T_a(x), ID_U, C_1\}$ to S_j.
Step 2 Upon receiving $\{T_a(x), ID_U, C_1\}$, S_j computes $R_{S_j} = S_{S_j} \oplus h(ID_{S_j})$, and chooses a random integer number b, computes $K_{S_jR} = T_bT_k(x)$, $C_2 = E_{K_{S_jR}}(ID_{S_j}||ID_U||R_{S_j})$. Then S_j sends $\{T_a(x), ID_U, C_1, T_b(x), ID_{S_j}, C_2\}$ to RC .
Step 3 Upon receiving $\{T_a(x), ID_U, C_1, T_b(x), ID_{S_j}, C_2\}$, RC computes $K_{RU} = T_kT_a(x)$, $K_{RS_j} = T_kT_b(x)$,and then decrypts C_1, C_2 as follows:$D_{K_{RU}}(C_1) = \{ID_U, ID_{S_j}, R_U\}$, $D_{K_{RS_j}}(C_2) = \{ID_{S_j}, ID_U, R_{S_j}\}$, and then checks whether $h(ID_U||k) \overset{?}{=} R_U$, $h(ID_{S_j}||k) \overset{?}{=} R_{S_j}$. If they are equal, RC computes $H_{R_{S_j}} = h(T_a(x)||R_{S_j})$, $H_{R_U} = h(T_b(x)||R_U)$,
$C_3 = E_{K_{RS_j}}(ID_{S_j}||ID_U||T_a(x)||H_{R_{S_j}}), C_4 = E_{K_{RU}}(ID_U||ID_{S_j}||T_b(x)||H_{R_U})$ .Then RC sends $\{C_3, C_4\}$ to S_j.
Step 4 Upon receiving $\{C_3, C_4\}$, S_j decrypts C_3 as follows:$D_{K_{RS_j}}(C_3) = \{ID_{S_j}, ID_U,$ $T_a(x), H_{R_{S_j}}\}$, and then checks whether $h(T_a(x)||R_{S_j}) \overset{?}{=} H_{R_{S_j}}$. If it i.s equal, S_j computes the session key $SK = T_b(T_a(x))$ and $H_{S_jU} = h(SK||ID_{S_j}||ID_U||C_4)$ .Then S_j sends $\{H_{S_jU}, C_4\}$ to U .
Step 5 Upon receiving $\{H_{S_jU}, C_4\}$, U decrypts C_4 as follows:$D_{K_{RU}}(C_4) = \{ID_U, ID_{S_j}, T_b, H_{R_U}\}$, and then checks whether $h(T_b(x)||R_U) \overset{?}{=} H_{R_U}$. If it is equal, U computes the session key $SK = T_a(T_b(x))$, and then checks whether$h(SK||ID_{S_j}||ID_U||C_4) \overset{?}{=} H_{S_jU}$. If it is equal, U authenticates S_j, and then computes $C_5 = h(SK||ID_U||ID_{S_j})$, and sends C_5 to S_j .
Step 6 Upon receiving C_5 , S_j checks whether $h(SK||ID_U||ID_{S_j}) \overset{?}{=} C_5$.If it is equal, S_j authenticates U.
Finally, U and S_j authenticate each other and establish the session key SK to communicate with each other.

3.4. **Biometrics and password update phase.** Fig.6 illustrates biometrics and password update phase. The steps are performed as follows.
Step 1 U inputs the smart card into a card reader, opens the update application software, and imprints biometrics B^{new} at the sensor.
Step 2 Firstly, the biometrics authentication process compares $B^{new}$with$B$ If$d(B^{new}, B) \geq \tau$, that means U will get a connection refused response. If $d(B^{new}, B) < \tau$, that



Opens login software and imprints B^*. If $d(B^*,B)<\tau$ holds, inputs PW_U, the card reader extracts $R_U = Z_U \oplus h(PW_U \| B)$. Then U chooses a, computes $K_{UR} = T_a T_{K_U}(x)$, $C_1 = E_{K_{UR}}(ID_U \| ID_{S_j} \| R_U)$.

Computes $R_{S_j} = S_{S_j} \oplus h(ID_{S_j})$ and chooses b, and computes $K_{S_jR} = T_b T_{k_j}(x)$, $C_2 = E_{K_{S_jR}}(ID_{S_j} \| ID_U \| R_{S_j})$.

Computes $K_{RU} = T_{K_U} T_a(x)$, $K_{RS_j} = T_{k_j} T_b(x)$, and then decrypts C_1, C_2 as follows: $D_{K_{RU}}(C_1) = \{ID_U, ID_{S_j}, R_U\}$, $D_{K_{RS_j}}(C_2) = \{ID_{S_j}, ID_U, R_{S_j}\}$.

Then checks whether $h(ID_U \| k) \overset{?}{=} R_U$, $h(ID_{S_j} \| k) \overset{?}{=} R_{S_j}$.

If they are equal, computes $H_{R_{S_j}} = h(T_a(x) \| R_{S_j})$, $H_{R_U} = h(T_b(x) \| R_U)$,

$C_3 = E_{K_{RS_j}}(ID_{S_j} \| ID_U \| T_a(x) \| H_{R_{S_j}})$, $C_4 = E_{K_{RU}}(ID_U \| ID_{S_j} \| T_b(x) \| H_{R_U})$.

Decrypts C_4 as follows: $D_{K_{RU}}(C_4) = \{ID_U, ID_{S_j}, T_b(x), H_{R_U}\}$, and then checks whether $h(T_b(x) \| R_U) \overset{?}{=} H_{R_U}$. If it is equal, computes $SK = T_a(T_b(x))$, and then checks whether $h(SK \| ID_{S_j} \| ID_U \| C_4) \overset{?}{=} H_{S_jU}$. If it is equal, computes $C_5 = h(SK \| ID_U \| ID_{S_j})$.

Decrypts C_3 as follows: $D_{K_{RS_j}}(C_3) = \{ID_{S_j}, ID_U, T_a(x), H_{R_{S_j}}\}$, and then checks whether $h(T_a(x) \| R_{S_j}) \overset{?}{=} H_{R_{S_j}}$. If it is equal, computes $SK = T_b(T_a(x))$, $H_{S_jU} = h(SK \| ID_{S_j} \| ID_U \| C_4)$.

Checks whether $h(SK \| ID_U \| ID_{S_j}) \overset{?}{=} C_5$. If it is equal, session key is SK.

Figure 5. The authenticated key agreement phase

means U will get a connection accepted response. Then the smart card sends the password input request message to U.

Step 3 inputs the old password PW_U and the new password PW_U^{new}.

Step 4 Smart card computes $Z_U^{new} = Z_U \oplus h(PW_U||B) \oplus h(PW_U^{new}||B^{new})$,and then replaces Z_U and B by Z_U^{new} and B^{new}, and then stores Z_U^{new} and B^{new} into the smart card.

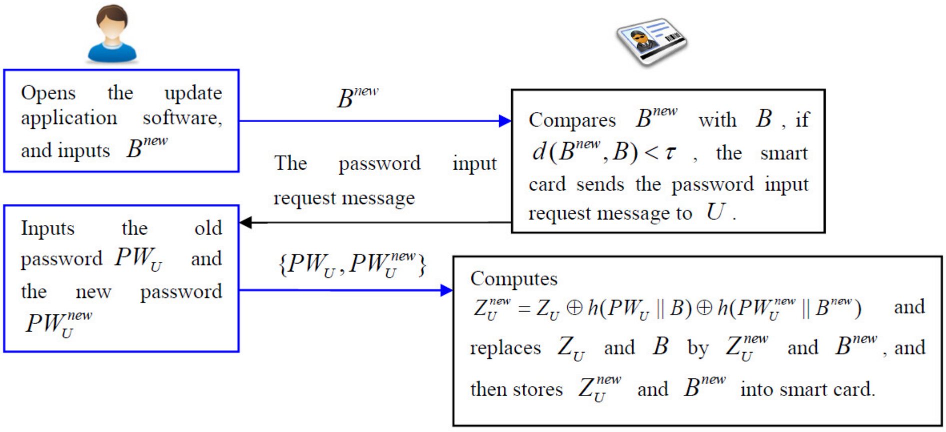

Opens the update application software, and inputs B^{new}
B^{new}
Compares B^{new} with B , if $d(B^{new}, B) < \tau$, the smart card sends the password input request message to U .
The password input request message
Inputs the old password PW_U and the new password PW_U^{new}
$\{PW_U, PW_U^{new}\}$
Computes $Z_U^{new} = Z_U \oplus h(PW_U \| B) \oplus h(PW_U^{new} \| B^{new})$ and replaces Z_U and B by Z_U^{new} and B^{new}, and then stores Z_U^{new} and B^{new} into smart card.

Figure 6. The biometric and password update phase

4. Security analysis.

In this section, we analyze the security of the proposed scheme. We suppose some specific situations to prove that our proposed scheme can provide secrecy and resist the common attacks. Now, we suppose that Trudy is an adversary, who can get any message transmitted between U, S_j and RC. In the following subsections, we complete the security analysis of our proposed scheme.

4.1. Perfect forward secrecy.

Definition 4.1. *An authenticated multiple key establishment protocol provides perfect forward secrecy if the compromise of both the nodes secret keys cannot results in the compromise of previously established session keys* [31].

Theorem 4.1. *The proposed scheme can realize perfect forward secrecy.*
Proof. Supposing that Trudy eavesdrops all session medium and recovers some foregoing parameters $T_a(x)$ and $T_b(x)$, she cannot compute the next session key $SK = T_a(T_b(x))$. That is because a and b are random chosen by U and S_j, respectively. Due to the intractability of the Chaotic Maps-based Diffie-Hellman (CM-DH) and Discrete Logarithm (CM-DL) problems, Trudy cannot previously obtain the next established session key.

4.2. Known-key secrecy.

Definition 4.2. *A protocol can protect the subsequent session keys from disclosing even if the previous session keys are intercepted by the adversaries, what will not affect other session keys is called known-key security.*

Theorem 4.2. *The proposed scheme can realize known-key security.*
Proof. As a and b are independent and different in all sessions, if Trudy knows a session key $SK = T_a(T_b(x))$ and a pair random a and b , she cannot compute the previous and the future session keys without knowing the previous and the future a and b.
Therefore, our proposed protocol can realize known-key secrecy and session key secrecy.

4.3. Mutual authentication and key agreement.

Definition 4.3. *Mutual authentication and key agreement refers to two parties authenticating each other suitably and establishing the session key simultaneously.*

Theorem 4.3. *The proposed scheme can realize mutual authentication and key agreement.*

Proof. In Step 3 of the authenticated key agreement phase, RC authenticates U by checking whether $h(ID_U||k) \overset{?}{=} R_U$.Because only RC knows the secret key k, which is an important parameter for computing R_U. The same process will happen for RC to authenticate S_j .In Step 4, S_j authenticates RC by checking whether $h(T_a(x)||R_{S_j}) \overset{?}{=} H_{R_{S_j}}$.$R_{S_j}$ is the server authentication key, only RC and S_j can compute R_{S_j}. The same process will happen for U to authenticate RC in Step 5. In addition, in Step 5, U authenticates S_j by checking whether $h(SK||ID_{S_j}||ID_U||C_4) \overset{?}{=} H_{S_jU}$. In Step 6, S_j authenticates U by checking whether $h(SK||ID_U||ID_{S_j}) \overset{?}{=} C_5$, since the hashed message included SK , S_j can believe that C_5 is originally sent from U.

After U and S_j authenticate each other, they can obtain the temporary session key SK.

4.4. Secure password and biometrics update protocol.

Definition 4.4. *Secure password and biometrics update protocol refers to users are free to change their passwords which can be easily remembered and biometrics in a secure environment.*

Theorem 4.4. *The proposed scheme can realize secure password and biometrics update agreement.*

Proof. If Trudy steals the smart card of a legal user, she cannot do anything because the proposed protocol provides an update agreement which cannot work off-line. If not, it is so easy for Trudy to guess and change the password. In addition, if the old password and biometrics were stored in the smart card, the proposed update protocol can utilize the pre-password and biometrics check to check the correctness of B.

4.5. Password guessing attack.

Definition 4.5. *Password guessing attack is an attack in which an adversary can guess and confirm the password of user in a system or in a communication protocol.*

Theorem 4.5. *The proposed scheme can resist password guessing attack.*

Proof. If Trudy starts an on-line password guessing attack, she will fail because after Step 3 of the authenticated key agreement phase, RC can authenticate U . However, the Off-line password guessing attack also will fail. Because the password PW_U and the biometrics B are used for defending the smart card, and there is no authenticated information encrypted by PW_U. Besides, only U can extract R_U by computing $Z_U \oplus h(PW_U||B)$. In addition, Trudy may try her best to get the secret key k of RC , it is infeasible because it is non-public.

4.6. Replay attack.

Definition 4.6. *A replay attack is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed.*

Theorem 4.6. *The proposed scheme can resist replay attack.*

Proof. Trudy cannot start a replay attack because new information transferred in the authenticated key agreement phase is protected by $T_a(x)$, $T_b(x)$ and SK . Supposing that Trudy impersonates U and sends the message $\{T_a(x), ID_U, C_1 \text{to} S_j\}$, she cannot check H_{S_jU} and send C_5 to S_j because she cannot decrypt C_4 and compute SK without knowing $T_b(x)$.The same process will happen for Trudy to impersonate S_j and send the message $\{T_b(x), ID_{S_j}, C_2\}$ to RC. In addition,supposing that Trudy impersonates RC and sends $\{C_3, C_4\}$ to start a replay attack, she will not succeed because a and b are random chosen by U and S_j , the replayed message$\{C_3, C_4\}$ cannot pass the authenticated process between U and S_j .

4.7. **Impersonation attack/Man-in-the-middle attack.**

Definition 4.7. *An impersonation attack is an attack in which an adversary successfully impersonates the identity of one of the legitimate parties in a system or in a communications protocol.*

Definition 4.8. *The man-in-the-middle attack is a form of active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker.*

Theorem 4.7. *The proposed scheme can resist impersonation attack.*

Theorem 4.8. *The proposed scheme can resist man-in-the-middle attack.*
Proof 4.7.1 If Trudy impersonates U to send $\{T_a(x), ID_U, C_1\}$ to S_j ,and then impersonates S_j to send$\{T_a(x), ID_U, C_1, T_b(x), ID_{S_j}, C_2\}toRC$,however, when receiving$\{C_3, C_4\}$from RC,Trudy cannot decryptsC_3 and C_4 by K_{RS_j} and K_{RU} because she cannot compute $K_{RS_j} = T_kT_b(x)$ and $K_{RU} = T_kT_a(x)$ because of the the CM-DH and CM-DL problems, respectively. So Trudy cannot succeed to start forgery and impersonation attacks.
Proof 4.7.2 Because the cryptographic messages C_1,C_2,C_3 , and C_4 contain the identity of U , a man-in-the-middle attack can be resisted.

4.8. **Spoofing attack.**

Definition 4.9. *A spoofing attack is an attack in which one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage.*

Theorem 4.9. *The proposed scheme can resist spoofing attack.*
Proof. Case 1 Server spoofing attack
It is impossible for Trudy to disguise S_j to trick U because of the user authentication key R_U shared between U and RC ,rather than the server S_j .If S_j wants to authenticate U, S_j must have been authenticated by RC and then RC sends $R_U = h(ID_U||k)$ to S_j .
For this reason, if Trudy disguises S_j to trick RC ,it is difficult for her to know the serve authentication key $R_{S_j} = h(ID_{S_j}||k)$.
Proof. Case 2 Registration center spoofing attack
It is impossible for Trudy to disguise RC because every server S_j has a authentication parameter R_{S_j} and every user U has a authentication parameter R_U . S_j and U can use their authentication parameters to authenticate the identity of RC. In other words, S_j and$U$ authenticate RC by $h(ID_{S_j}||k) \overset{?}{=} R_{S_j}$ and $h(ID_U||k) \overset{?}{=} R_U$ respectively.
According to Case 1 and Case 2, the proposed protocol can resist spoofing attack.

4.9. **Insider attack.**

Definition 4.10. *An insider attack is a malicious attack perpetrated on a network or computer system by a person with authorized system access.*

Theorem 4.10. *The proposed scheme can resist insider attack.*
Proof. In the proposed scheme, U registers on RC by $h(PW_U||B)$,which based on a one-way hash function, the insider of RC cannot immediately obtain PW_U.
According to all of above, we can prove that the proposed scheme is secure. Table 2 shows the security comparisons between our scheme and related scheme.

Table 2. Security comparisons between our scheme and related scheme

	S1	S2	S3	S4	S5	S6	S7	S8	S9	S10	S11
Khan et al. [8]	$--$	$--$	Yes	No	Yes	$--$	Yes	Yes	Yes	Yes	$--$
Guo et al. [15]	Yes	Yes	Yes	Yes	Yes	Null	Yes	Yes	$--$	$--$	Yes
Our scheme	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

S1: Perfect forward secrecy; S2: known-key secrecy; S3: Mutual authenticatio; S4: Key agreement;S5: Secure password update l; S6: Secure biometrics update; S7: Resist Password guessing attack; S8: Resist replay attack; S9: Resist impersonation attack/Man-in-the-middle attack; S10: Resist spoofing attack; S11: Resist insider attack $--$:Not mentioned Yes/No: Support/Not support the security Null: Not involve

5. **Functionality analysis.** In this section, we discuss the functionality of our proposed scheme, and make some corresponding comparisons with related scheme. Table 3 shows the functionality comparisons between our scheme and related scheme.

5.1. **Application environment.** In our proposed scheme, chaos theory is applied to multi-server environment. In a single server environment, when a user needs a variety of services or users need a service, the server may not be able to meet the requirements or cannot work. Usually, a user wants to login a new single server environment, he/she must re-register new ID and PW .That is so trouble and may be waste of limited network resources. However, these problems can be avoided in a multi-server environment. A multi-environment is more practical for users.

5.2. **Timestamp.** Timestamp is a string generated by the current server time, and can represent the generated random numbers of the server at some point with a nonce. However, if the message is maliciously delayed by an adversary, it is likely to cause that the interval time for transmission delay is always equal or greater than ΔT , then the server rejects the legal login request all the time. However, there is no timestamp in our proposed scheme. Our proposed can avoid this condition.

5.3. **Changing of password and biometrics by users.** In the registration phase, the user can select his/her password and extracts the biometrics sample, and then sends them to RC .In the biometrics and password update phase, the user U firstly imprints biometrics B^{new} at the sensor. If $d\left(B^{new}, B\right) < \tau$,U inputs the old password PW_U and the new password PW_U^{new} , and then smart card computes $Z_U^{new} = Z_U \oplus h(PW_U||B) \oplus h(PW_U^{new}||B^{new})$,and then replaces Z_U and B by Z_U^{new} and B^{new}, and then stores Z_U^{new} and B^{new} into the smart card to finish the changing of password and biometrics.

Table 3. Functionality comparisons between our scheme and related scheme

	F1	F2	F3	F4
Khan et al. [8]	No	Yes	Yes	No
Guo et al. [15]	No	Yes	Yes	−−
Our scheme	Yes	No	Yes	Yes

F1: Multi-server environment; F2:Timestamp;F3:Changing of password;
F4: Changing of biometricsYes/No: Have/Not have the functionality
−−: Not involve

6. **Efficiency analysis.** In this section, we analyze the efficiency of our proposed scheme. In our proposed scheme, we proposed a biometrics-based multi-server authenticated key agreement scheme on chaotic maps cryptosystem. According to the required operations for different entities, Table 4 summarizes the communication costs of our proposed scheme and related schemes in different phases. In Chang et al. [32] scheme, they coded a C language program of hash function, they input a 512-bit random string and implemented the program 10,000 times in a Window 7 workstation with an AMD X4 945 processor running at 3.00GHZ, 8,192MB of RAM, and a 7,200 RPM Western Digital WD5000AAKS-22V1A0465 GB ATA drive. They showed that the average time for one hash value was 0.605ms. In [34], Lee showed that one hash function operation was about one time faster than one Chebyshev chaotic maps operation. We can draw a conclusion that the average time for one Chebyshev chaotic maps operation was about 1.21ms. In addition, according to [33], we can come to a conclusion that one hash function operation is about 10 times faster than a symmetric encryption/decryption. So a symmetric encryption/decryption operation was about 6.05ms. According to [32-34], the execution times of each phase in our proposed scheme and related schemes are shown in Table 5. Table 5 shows that the execution time of the authenticated key agreement phase is longer than related schemes. However, our proposed scheme has good practicability. It is worthy of using more a little time.

Table 4. The communication costs of our proposed scheme and related schemes

	C1	C2	C3	C4	C5	C6	C7	C8	C9
Khan et al. [8]	−−	−−	2H	−−	3H	3H	−−	2H	−−
Guo et al. [15]	−−	−−	1H	1S+1T	2T+2H+2S	2H+3S+3T	−−	2H+1S+1T	$3S + 1T$
Our scheme	−−	1H	1H	1H	2T+4H+2S	2T+4H+2S	1T+4H+4S	2H	−−

C1/C2:Communication cost of the serve/registration center in the server registration phase;
C3/C4:Communication cost of the user/registration center in the user registration phase;
C5/C6/C7: Communication cost of the user/server/registration center in the authenticated key agreement phase; C8/C9: Communication cost of the user/server in the biometrics and password update phase H:Hashing operation; T: Chebyshev chaotic maps operation;
S:Symmetric encryption/decryption −−: Not involve the operations

7. **Conclusion.** In the proposed scheme, we propose an efficient and secure biometric-based multi-server authenticated key agreement scheme on chaotic maps cryptosystem. Our scheme has many practical merits: it refuses timestamp and verification table, modular exponentiation and scalar multiplication on an elliptic curve, and provides secure biometric authentication, chaotic maps-based authenticated key agreement, secure update protocol, in the same time, it can resist various common attacks. The security and efficiency analysis shows that our proposed scheme has high quality.

Table 5. The communication costs of our proposed scheme and related schemes

	T1	T2	T3
Khan et al. [8]	2H≈1.21	6H≈3.63	2H≈1.21
Guo et al. [15]	1H+1S+1T≈7.865	5T+4H+5S≈43.73	2H+4S+2T≈1.21
Our scheme	13H≈1.815	5T+12H+8S≈66.71	2H≈1.21

T1:The execution time of registration phase(C1-C4);

T2: The execution time of authenticated key agreement phase(C5-C7);

T3:The execution time of password and biometrics update phase(C8-C9)

REFERENCES

[1] Q. Xie, J.M. Zhao and X.Y. Yu, Chaotic maps-based three-party password-authenticated key agreement scheme, *Nonlinear Dynamics*, vol. 74, no. 4, pp. 1021-1027, 2013.

[2] T. Hwang, Y.H. Chen and C.S. Laih, Non-interactive password authentications without password tables, *IEEE region conference on computer and communication systems*, pp. 429431, 1990.

[3] W.S. Juang, Efficient multi-server password authenticated key agreement using smart cards, *IEEE Trans. on Consumer Electronics*, pp. 251-255, 2004.

[4] C.C. Chang and J. S. Lee, An efficient and secure multi-server password authentication scheme using smart cards, *IEEE information conference on Cyberworlds*. pp. 417-422, 2004.

[5] N.Y. Lee and Y.C. Chiu, Improved remote authentication scheme with smart card, *Computer Standards and Interfaces*, vol. 27, no. 2, pp. 177-180519-524, 2005.

[6] M.K. Khan and J.S. Zhang, Improving the security of a flexible biometrics remote user authentication scheme, *Computer Standards and Interfaces*, vol. 29, no. 1, pp. 82-85, 2007.

[7] C.T. Li and M.S. Hwang, An efficient biometrics-based remote user authentication scheme using smart cards, *Journal of Network and Computer Applications*, vol. 33, no. 1, pp. 1-5, 2010.

[8] M.K. Khan, J.S. Zhang and X.M. Wang, Chaotic hash-based fingerprint biometric remote user authentication scheme on mobile devices, *Chaos, Solitons and Fractals*, vol. 35, no. 3, pp. 519-524, 2008.

[9] J.L. Tsai, Efficient multi-server authentication scheme based on one-way hash function without verification table, *Computers and Security*, vol. 27, no. 3-4, pp. 115-121, 2008.

[10] E.J. Yoon and K.Y. Yoo, Robust biometrics-based multi-server authentication with key agreement scheme for smart cards on elliptic curve cryptosystem, *The Journal of Supercomputing*, vol. 63, no. 1, pp. 235-255, 2013.

[11] J.S. Cho, C.H. Huang and C.C. Ding, Security weaknesses in two multi-server password based authentication protocol, *IACR Cryptology ePrint Archive*, 2009.

[12] Y.L. Chen, C.H. Huang and J.S. Chou, Comments on two multi-server authentication protocols. *IACR Cryptology ePrint Archive*, 2009.

[13] S.G. Lee, Cryptanalysis of Multiple-Server Password-Authenticated Key, *IACR Cryptology ePrint Archive*, 2009.

[14] T.Y. Wu and Y.M. Tseng, An efficient user authentication and key exchange protocol for mobile client-server environments, *Computer Networks*, vol. 54, no. 9, pp. 1520-1530, 2010.

[15] C. Guo and C.C. Chang, Chaotic maps-based password-authenticated key agreement using smart cards, *Communications in Nonlinear Science and Numerical Simulation*, vol. 18, no. 6, pp. 1433-1440, 2013.

[16] K. Chain and W.C. Kuo, A new digital signature scheme based on chaotic maps, *Nonlinear Dynamics*, vol. 74, no. 4, pp. 1003-1012, 2013.

[17] C.C Lee, C.L. Chen, C.Y. Wu and S.Y. Huang, An extended chaotic maps-based key agreement protocol with user anonymity, *Nonlinear Dynamics*, vol. 69, no. 1-2, pp. 79-87, 2012.

[18] D.B. He, Y.T. Chen and J.H. Chen, Cryptanalysis and improvement of an extended chaotic maps-based key agreement protocol, *Nonlinear Dynamics*, vol. 69, no. 3, pp. 1149-1157, 2012.

[19] P. Gong, P. Li and W.B. Shi, A secure chaotic maps-based key agreement protocol without using smart cards, *Nonlinear Dynamics*, vol. 70, no. 4, pp. 2401-2406, 2012.

[20] M. Inuma, A. Otsuka and H. Imai, *Theoretical framework for constructing matching algorithms in biometric authentication systems*, LNCS5558, Springer, pp. 806-815, 2009.

[21] A. Anees, A.M. Siddiqui, J. Ahmed and I. Hussain, A technique for digital steganography using chaotic maps, *Nonlinear Dynamics*, vol. 75, no. 4, pp. 807-816, 2014.

[22] H. Khanzadi, M. Eshghi and S.E. Borujeni, Image encryption using random bit sequence based on chaotic maps, *Arabian Journal for Science and engineering*, vol. 39, no. 2, pp. 1039-1047, 2014.

[23] S.N. George and D.P. Pattathil, A novel approach for secure compressive sensing of images using multiple chaotic maps, *Journal of Optics*, vol. 43, no. 1, pp. 1-17, 2014.

[24] Y.P. Hu, C.X. Zhu and Z.J. Wang, An improved piecewise linear chaotic map based image encryption algorithm, *The Scientific World Journal*, Published online 2014, Article ID 275818, http://dx.doi.org/10.1155/2014/275818.

[25] C.C. Lee, C.T. Li and C.W. Hsu, A three-party password-based authenticated key exchange protocol with user anonymity using extended chaotic maps, *Nonlinear Dynamics,* vol. 73, no. 1, pp. 125-132, 2013.

[26] C. Guo, C.C. Chang and C.Y. Sun, Chaotic Maps-Based Mutual Authentication and Key Agreement using Smart Cards for Wireless Communications, *Journal of Information Hiding and Multimedia Signal Processing*, vol. 4, no. 2, pp. 99-109, 2013.

[27] I. Hussain, T. Shah and M.A. Gondal, Application of S-box and chaotic map for image encryption, *Mathematical and Computer Modelling*, vol. 57, no. 9-10, pp. 2576-2579, 2013.

[28] B. Wang and M.D. Ma, A smart card based efficient and secured multi-server authentication scheme, *Wireless Personal Communications*, vol. 68, no. 2, pp. 361-378, 2013.

[29] D.B. He and S.H. Wu, Security flaws in a smart card based authentication scheme for multi-environment, *Wireless Personal Communications*, vol. 70, no. 1, pp. 323-329, 2013.

[30] X. Li, J. Ma, W.D. Wang, Y.P. Xiong and J.S. Zhang, A novel smart card and dynamic ID based remote user authentication scheme for multi-server environments, *Mathematical and Computer Modelling*, vol. 58, no. 1-2, pp. 85-95, 2013.

[31] J. Kar and B. Majhi, An Efficient Password Security of Multiparty Key Exchange Protocol based on ECDLP, *International Journal of Computer Science and Security*, vol. 3, no. 4, pp. 405-413, 2009.

[32] C.C. Chang and C.Y. Sun, A Secure and Efficient Authentication Scheme for E-coupon Systems, *Wireless Personal Communications*, vol. 77, no. 4, pp. 2981-2996, 2014.

[33] B. Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C, Second Edition*, New York, USA, 1996.

[34] C.C. Lee, A simple key agreement scheme based on chaotic maps for VSAT satellite communications, *International Journal of Satellite Communications and Networking*, vol. 31, no. 4, pp. 177-186, 2013.

[35] T.Y. Wu and Y.M. Tseng, An ID-based mutual authentication and key exchange protocol for low-power mobile devices, *The Computer Journal*, vol. 53, no. 7, pp. 1062-1070, 2010.

[36] Y.H. Chuang and Y.M. Tseng, Towards generalized ID-based user authentication for mobile multi-server environment, *International Journal of Communication Systems*, vol. 25, no. 4, pp. 447-460, 2012.