Journal of Information Hiding and Multimedia Signal Processing ©2016 ISSN 2073-4212
Ubiquitous International Volume **7**, Number **5**, September **2016**

An Improved Password Authentication Scheme for Telecare Medical Information Systems Based on Chaotic Maps with Privacy Protection

Yang Sun

Software College
Shenyang Normal University
No.253, HuangHe Bei Street, HuangGu District, Shenyang, P.C 110034 - China
17247613@qq.com

Received April, 2016; revised May, 2016

Abstract. *Chaos theory has been widely studied and adapted in cryptography for achieving some security mechanisms, such as encryption/decryption, key agreement and hash function. In order to improve the scope of application, many recearchers consider that chaos theory should be used in telecare medicine platform. Telecare Medicine Information Systems (TMISs) is a new emerging thing which aims at constructing a communicating platform supporting the patients access health-care delivery services via internet or mobile networks. Recently, Lu et al. proposed a secure smart card based authentication scheme for TMISs using enhanced chaotic maps. In this paper, we show that Lu et al.s scheme has still some weaknesses such as smartcard denial of access, using XOR operation in a wrong way and some other flaws. Then, we give an improved scheme to revise these flaws. Finally, BAN logic proof and efficiency comparison are provided to show that our scheme is secure and more practical for telemedical environments.*
Keywords: Password; Telecare medicine information systems; Chaotic Maps; Authentication

1. **Introduction.** In the last few years, an increasing number people communicate with others over the network, including transfer information, exchange learning and even conduct online consultation. Meanwhile, with the rising demand for medical service and health industry which caused by the rapid growth of population and the exacerbation of aging, healthcare sector will fall into a shortage situation gradually. Hospital will appear the circumstance that the patient cannot be arranged proper and there will be many of the injured delay treatment. So considering the above reasons, some scholars construct a fresh system to help patients receive medical advice as soon as possible, which called telecare medicine information system (TMIS). Telecare medicine information system is a platform set for between the patient and the doctor, notes that wherever you are, you can contact with doctors via the network to get medical advices. TMIS will ensure the patients can obtain timely treatment from the network therapy center instead of come hospital in person. This low-cost and timesaving medical institution is greatly catering the fast-paced lifestyle of the contemporary. However, since TMIS meets the patients acquire information on any electronic equipment, the registered users may access this system via common network, which put the users into an insecurity situation. Under the public network, the attacker will catch users information easily. At the same time, due to the medical server preserves the electronic health record of the users, once the server

broken or the information was stolen, the patients will suffer enormous losses.

For the purpose of prevent the above loopholes and ensure a secure communication in TMIS, several researchers commence studying this system. In 2012, Wu et al. [1] proposed an efficient authentication scheme which utilized a pre-computing phase to reduce the calculation. This pre-computing phase assists the users store values on their mobile device. But He et al. [2] found that Wu et al.s scheme was unable to prevent impersonation attack, and followed put forward a new protocol. During the same year, Wei et al. [3] pointed out that He et al.s scheme was failed to meet the off-line password guessing requirement. If the users smart card was caught by the attacker, the data will be leaked entirely. So he presented an improved authentication scheme for TMIS. Then Zhu [4] demonstrated that Wei et al.s scheme cannot achieve the demand of off-line password guessing and proposed an enhanced scheme. However, Cao and Zhai [5] discovered that Zhus scheme is vulnerable to the denial of service attack. Considering all of the above-mentioned schemes are designed by modular exponentiation operation, and the complexity of this algorithm. Hence these schemes are not ideal for employ on mobile equipments.

In order to improve the efficiency of the algorithm, chaotic maps-based cryptography system attracts many researchers attention compared with traditional cryptography. Particularly, the chaotic maps theory is extremely suitable for two-party authentication schemes. Similarly, how to applying chaotic maps into TMIS successfully aroused researchers widespread attention. Lately, Guo et al. [6] demonstrated that all of these previous works cannot really satisfy the security demand for the agreement. Hence they first proposed an authentication scheme with smart card based on chaotic maps, and claimed that this scheme can resist various attacks. However, Hao et al. [7] found that Guos scheme unable to provide user anonymity and cause redundancy due to the double keys. So they proposed a fresh chaotic map-based authentication scheme and claimed that their scheme has better performance than Guo et al.s scheme. Unfortunately, Jiang et al. [8] identified that Hao et al.s scheme cannot avoid smart card stolen attack. At the same time, Lee [9] also opened a defect on Hao et al. that enable attackers easily hidden in session key. Hence, Jiang et al. and Lee proposed a novel scheme respectively, aiming to defect these flaws. In 2014, Li et al. [10] demonstrated that neither Jiangs scheme nor Lees scheme unable withstand service misuse attack, which vulnerable to non-registered users login telecare servers unconsciously. After that, they present a new authentication scheme based on chaotic maps to solve these problems. But in the second years, Lu et al. [11] discovered that Li et al.s scheme also exits some issues such as short the module of local authentication and suffered from impersonation attack easily. Then they add the way of biometric and hash operation to overcome these weaknesses, put forward a new chaotic map-based authentication scheme using smart card by biometric identification technique and hash function.

Just as Lu et al. said, their scheme displayed a more efficient environment for TMIS, but we find their scheme cannot resist the weakness like smartcard denial of access flaw, Potential Loophole of XOR Operation that will result attacker catches information easily. Hence, in our work, we will proposed a provable improved authentication scheme based on chaotic maps to remedy these flaws that appear in previous works, we will demonstrate that our scheme is more applying in telecare system and it will also enhance schemes efficiency.

The rest of the paper is organized as follows: Some preliminaries are given in Section 2. In Section 3, we give the proposed scheme. In Section 4, we discuss the security with two analysis methods. The efficiency analysis of our proposed scheme is given in Section 5. This paper is finally concluded in Section 6.

2. **Chebyshev chaotic maps.** Let n be an integer and let x be a variable with the interval $[-1,1]$.The Chebyshev polynomial.[13] $T_n(x) : [-1,1] \to [-1,1]$ is defined as $T_n(x) = \cos(ncos^{-1}(x))$ Chebyshev polynomial map $T_n : R \to R$ of degree n is defined using the following recurrent relation :

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

The first few Chebyshev polynomials are:
$T_2(x) = 2x^2 - 1$, $T_3(x) = 4x^3 - 3x$, $T_4(x) = 8x^4 - 8x^2 + 1$,
One of the most important properties is that Chebyshev polynomials are the so-called semi-group property which establishes that

$$T_r(T_s(x)) = T_{r \cdot s}(x) \tag{2}$$

An immediate consequence of this property is that Chebyshev polynomials commute under composition

$$T_r(T_s(x)) = T_s(T_r(x)) \tag{3}$$

In order to enhance the security, Zhang [14] proved that semi-group property holds for Chebyshev polynomials defined on interval $(-\infty, +\infty)$. The enhanced Chebyshev polynomials are used in the proposed protocol:

$$T_n(x) = (2xT_{n-1}(x) - T_{n-2}(x)) (\mathrm{mod} N) \tag{4}$$

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

$$T_{r \cdot s}(x) = T_r(T_s(x)) = T_s(T_r(x)) \tag{5}$$

Definition 2.1. *(Enhanced Chebyshev polynomials) The enhanced Chebyshev maps of degree $n (n \in N)$ are defined as: $T_n(x) = (2xT_{n-1}(x) - T_{n-2}(x))(\mathrm{mod}\ p)$, where $n \geq 2$, $x \in (-\infty, +\infty)$, and p is a large prime number. Obviously, $T_{rs}(x) = T_r(T_s(x)) = T_s(T_r(x))$.*

Definition 2.2. *(DLP, Discrete Logarithm Problem) Given an integer a, find the integer r, such that $T_r(x) = a$.*

Definition 2.3. *(CDH, Computational DiffieHellman Problem) Given an integer x, and the values of $T_r(x), T_s(x)$, what is the value of $T_{rs}(x) = ?$.*

It is widely believed that there is no polynomial time algorithm to solve DLP, CDH with a non-negligible probability.

3. Review and Flaws of Lus scheme for TMIS.

3.1. Review of Lus scheme [11].

In this section, we review Lus scheme, the notations are described in Table 1 and the main processes are shown in Fig.1:

Registration:
(1)U inputs his biometrics characteristic BIO, selects an identity ID, and a password PW. Then U computes $PWD = h_1(PW||H(BIO))$ and submits $\{ID, PWD\}$ to S through a secure channel.
(2)S computes $K = h_1(ID||PWD), IM_1 = K \oplus h_1(k_s)$, where k_s is $S's$ secret key. S then issues a smart card containing $\{IM_1\}$ to U.

TABLE 1. Notations

Symbol	Definition
U, S	User and server
ID, PW	Identity and password of an entity U
v, u	Nonces
$H(.)$	Biohash function
$h_1(.), h_2(.)$	Hash function $h_1 : \{0,1\}^* \rightarrow \{0,1\}^l$, Hash function $h_2 : [0,1] \rightarrow \{0,1\}^l$
k_u, k_s	Secret key selected by U and S, respectively
$\oplus, \|\|$	Exclusive-or operation and concatenation operation

(1)U selects a secret key k_u and computes $f = h_1(ID||k_u) \oplus PWD$. U then stores f into smart card. Thus, it is noted that the smart card of U contains the information $\{IM_1, f, h_1(\cdot), h_2(\cdot), H(\cdot)\}$.

Login and Authentication:

(1)U first inserts the smart card into a device reader and enters his identity ID, password PW, secret key k_u and also imprints biometric BIO at the sensor. U then checks whether $h_1(ID||k_u) \oplus h_1(PW||H(BIO)) \stackrel{?}{=} f$. If it holds, U computes $K = h_1(ID||h_1(PW||H(BIO))$, then generates a random number and computes $R_1 = K \oplus ID$, $R_2 = ID \oplus T_u(K)$, $R_3 = h_1(ID||T_u(K))$. Finally, U sends the message $\{R_1, R_2, R_3\}$ to S.

(2) Upon receiving the message from U, S uses his key k_s to derive K by computing $K' = IM_1 \oplus h(k_s)$, he then computes $ID = R_1 \oplus K, T_u(K) = ID \oplus R_2$ and checks $h_1(ID||T_u(K)) \stackrel{?}{=} R_3$.If it is correct, S then generates a random number v and computes $IM_2 = T_v(K) \oplus ID$, $Auth_s = h_1(K||T_v(K)||sk)$, $sk = h_2(T_u(K), T_v(K), T_{uv}(K))$. Finally, S sends the message $\{Auths, IM_2\}$ to U.

(3) After receiving the message from U, S derives $T_v(K)$ by computing $IM_2 \oplus ID$ and computes $sk = h_2(T_u(K), T_v(K), T_{uv}(K))$ to verify whether $Auth_s{}' = h_1(K||T_v(K)||sk)$ is equal to the received $Auth_s$. If it holds, U successfully authenticates S and computes $Auth_u = h_1(sk||T_v(K)||K)$ and then sends the message $\{Auth_u\}$ to S.

(4) Once receiving the message from U, S validates whether $h_1(sk||T_v(K)||K) \stackrel{?}{=} Auth_u$. If it is true, S successfully authenticates U; otherwise, S aborts this request. Finally, U and S have a common session key $sk = h_2(T_u(K), T_v(K), T_{uv}(K))$.

3.2. **Security flaws of Lus scheme. (1) SDOA flaw (Smartcard Denial Of Access flaw)**

Denial of access in biometric systems greatly impacts on the usability of the system by failing to identify a genuine user, and hence on the public acceptance of biometrics in the emerging technology. Biohash function can reduce these influence. But nothing is absoultely, no matter how biometric or biohash function, there still exists a predetermined threshold τ (τ is the predetermined threshold for biometrics certification) for biometrics certification.

In Lus scheme, only $H(\cdot)$ is the biohash function, and $h_1(\cdot), h_2(\cdot)$ are hash function. So you can authenticate biometric by comparing BIO and BIO' in the τ range, or comparing $H(BIO)$ and $H(BIO')$ in the τ range. But you must not use $h_1(\cdot), h_2(\cdot)$ to hash BIO and BIO' to compare. Because $h_1(\cdot), h_2(\cdot)$ are not biohash function, and one of the main features for hash function is that even if the input message only change one bit, and the output digital digest will change greatly.

We assume input biometric is BIO'. In Lus registration phase, the smartcard stores

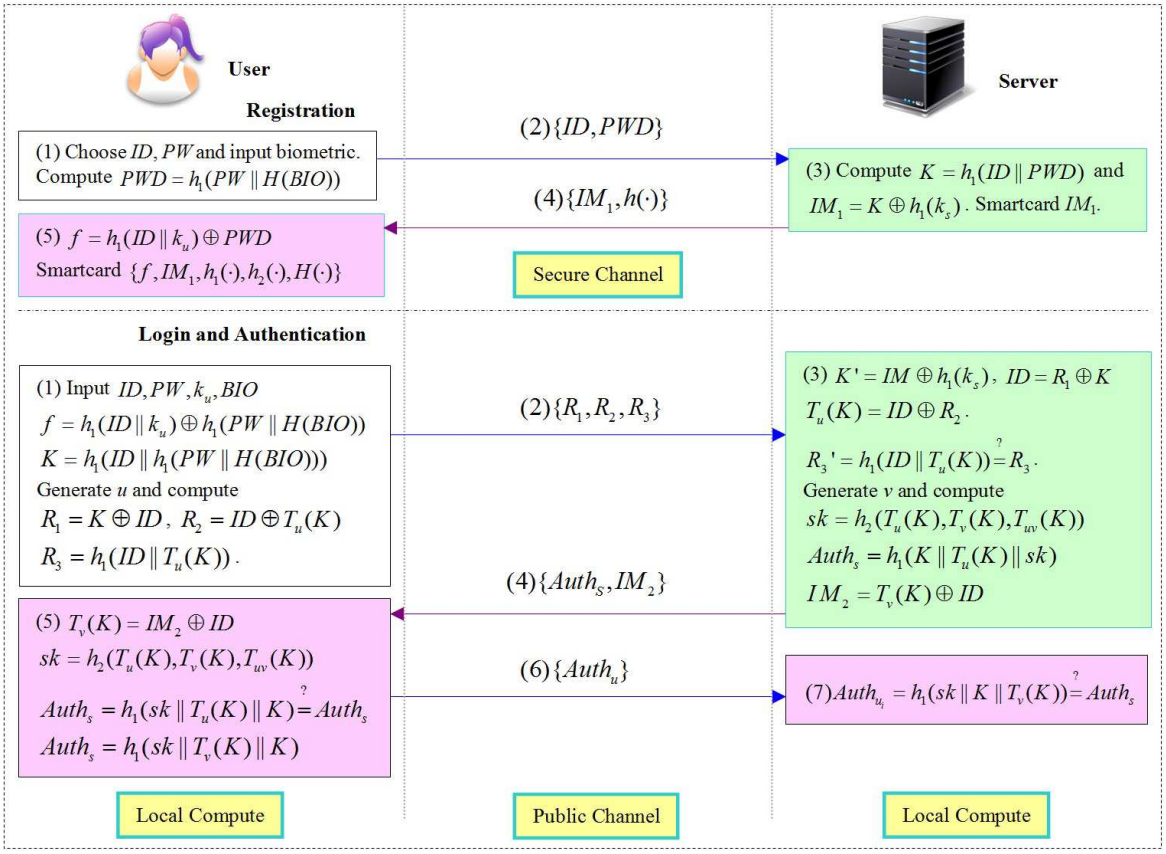

FIGURE 1. the process of Lus scheme

$f = h_1(ID||k_u) \oplus PWD = h_1(ID||k_u) \oplus h_1(PW||H(BIO))$. Because the input information can compute $f' = h_1(ID||k_u) \oplus h_1(PW||H(BIO'))$ which is not the same with f, the smartcard will denial the legal users access. The key mistake is to use hash function to compare instead of biohash function.

(2) PLXO (Potential Loophole of XOR Operation)

First of all, there exists a kind of Potential Loophole about using within the whole Lus scheme. The XOR operation must assure the same binary digits on both sides of.

Assume that $t = a \oplus b$, a is short and b is long.So there are three scenarios as follows:

Case 1: Extended a.

However, a may be the ID of user (such as in literature [11]), so the ID of user is not practical and friendly enough.

Case 2: Shorten b.

However, b may be a random number (such as in literature [11]), if b is shortened, it can be easily guessed. And if the protocol transmits a (may be the ID) in plaintext, anyone will get the b.

Case 3: Pad a.

Definition 3.1. Leak attack.

Leak attack is a kind of intercept attack that the attackers use various technologies to obtain the useful information from the messages eavesdropped from public channels.

Definition 3.2. XOR with pad operation leaking attack.

This kind of attack is due to use XOR operation in a wrong way, which will lead to leak some sensitive information, and finally an adversary can get part of useful information,

even the session key is not being detected. In literature [11], Trudy can launch a XOR with pad operation leaking attack.

For pad a method, on one side, according to Kerckhoffss principle: A cryptosystem should be secure even if everything about the system, except the key, is public knowledge. On the other side, the opposite peer must know the pad algorithm in order to decrypt the XORed cipher text. Based on above-mentioned, the pad method/algorithm must be opened, then $t = (a||pad) \oplus b$, and the values of a and b must be strictly private. The key reason of leaking partial information is to use low-entropy information to transmit secret message. For example, we consider $R_1 = K \oplus ID$, and the Fig 2 shows that partial of K will be leak. We have known R_1 and the ID is the low-entropy information, so there are two kinds of potential attack about ID: (a) the ID must be kept securely anytime and anywhere, it is difficult because ID is the low-entropy information and used frequently. (b) because ID is the low-entropy information, just like password that is often subjected to guessing attack (or called dictionary attack), the ID is also vulnerable about guessing attack.
Finally, we assess the leaking bits about K: Assuming that the ID has l bits, K has m bits. The leaking bits are $(m - l)$ bits. The shorter of the ID, the more of leaking information about K.

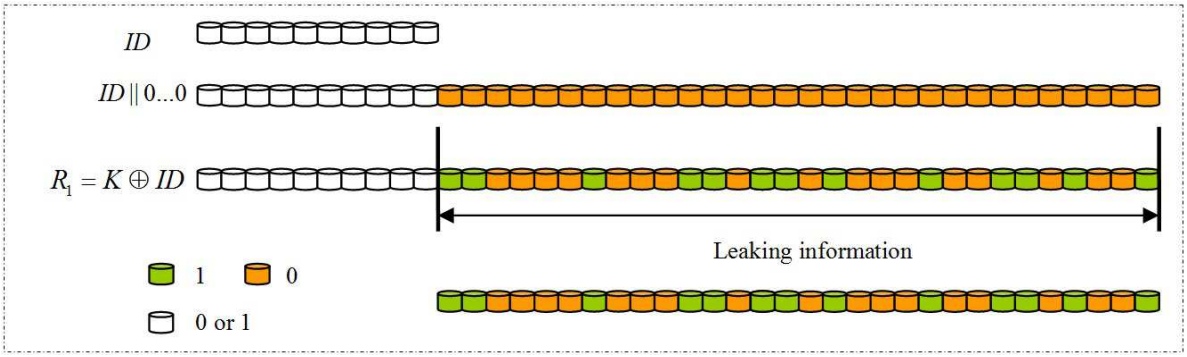

FIGURE 2. the process of how to leak some information

3.3. **Design flaws of Lus scheme.**

(1) The impractical secret key of a user

A smartcard with a users password is the common two-factor form in the authenticated scheme, and if we add biometric that is called three-factor authenticated scheme. So the secret key of the user k_u is unnecessary. The reasons are: **(a)** The k_u is the long and cryptography key (high-entropy), which cant be remembered by people. In Lus scheme, the k_u acts as the input parameter which is impractical. **(b)** The k_u cant be stored in the smartcard, because if the smartcard lost, it will be obtained by the adversary. **(c)** It will be secure enough by three-factor authenticated scheme and the k_u is useless.

(2) The redundant design

Many redundant design in Lus scheme.
Case1: $sk = h_2(T_u(K), T_v(K), T_{uv}(K))$. Because $T_{uv}(K)$ can be deduced by $T_u(K), T_v(K)$ with chaotic maps and $T_{uv}(K)$ has already including the two nonces u and v. We can view $T_u(K), T_v(K)$ are the redundant information.
Case2: For $Auth_s = h_1(K||T_u(K)||sk)$, the $K, T_u(K)$ are the redundant information. Because sk has already including the $K, T_u(K)$.

(3) The wrong defination of hash function $h_2(\cdot)$

Let n be an integer and let x be a variable with the interval $[-1, 1]$.The Chebyshev polynomial.[13] $T_n(x) : [-1, 1] \to [-1, 1]$ is defined as $T_n(x) = \cos(ncos^{-1}(x))$. So we can see the x and $T_n(x)$ are in the $[-1, 1]$. But Lus scheme is design with extended chaotic maps which is proposed by Zhang [16] proved that semi-group property holds for Chebyshev polynomials defined on interval $(-\infty, +\infty)$. So the definition $h_2 : [-1, 1] \to \{0, 1\}^l$ should be revised as $h_2 : \{0, 1\}^* \to \{0, 1\}^l$.

4. The Proposed Scheme.

4.1. Notations.

In this section, we present an improved authenticated agreement with chaotic maps. Some notations hereafter are shown in Table2.

Table 2. Notations

Symbol	Definition
U,S	User and server
ID, PW	Identity and password of an entity U
v, u	nonces
$H(.)$	Biohash function
$(x, T_{k_s}(x)), k_s$	Chebyshev chaotic maps: public/private key pairs of the server
$h_1(.), h_2(.)$	Different hash functions $h_1, h_2 : \{0,1\}^* \to \{0,1\}^l$
$\|$	Concatenation operation
τ	Predetermined threshold for biometrics certification
$d(\cdot)$	Symmetric parametric function

4.2. Notations.

4.3. The Proposed Scheme.

The improved TMIS scheme of using novel method is shown in Fig.3.

Registration:

Step 1. When U wants to set up one secure communication with S, he should select an identity ID, password PW, and inputs his biometrics characteristic BIO. Then computes $PWD = h_1(PW||H(BIO))$ and sends $\{ID, PWD\}$ to S through a secure channel.

Step 2.S computes $K = h_1(ID||PWD)$, $IM = K \oplus h_1(k_s||ID)$, where k_s is the servers secret key. Then S put IM into smart card and sends $\{IM\}$ to U.

Step 3.U stores a threshold for biometrics into smart card, so the smart card of U contains the information of $\{IM, h_1, h_2, H, H(BIO), d, \tau\}$.

Login and Authentication:

Step 1.U first insert the smart card into device and enters his identity ID and password PW, then imprints his biometrics $BIO^{'}$, then U verifies whether $d(H(BIO), H(BIO^{'})) < \tau$. If holds, U will exact $h_1(k_s||ID) = IM \oplus h_1(ID||PWD)$ and the smart card will choose a random number u and computes $x^{'} = h_2(ID||h_1(k_s||ID)||T_u(x))$, where $T_u(x)$ is $U's$ public key, then computes $C_1 = T_u T_{k_s}(x)||ID$, and $C_2 = h(T_u(x)||h_1(k_s||ID))$. Finally, U submits $\{C_1, C_2, T_u(x)\}$ to S. **Step 2.**After receiving the message from U, S obtains ID by computing $ID = C_1/T_{k_s}T_u(x)$ with screct key k_s. Then computes $h_1(k_s||ID)$ and checks $h_1(T_u(x)||h_1(k_s||ID)) \stackrel{?}{=} C_2$, if it holds, S will derive $x^{'}$ by computing $x^{'} = h_2(ID||h_1(k_s||ID)||T_u(x))$ and then chooses a random integer v to computes the session key $sk = h_2(ID||T_v T_u(x^{'}))$, and $Auth_s = h_1(T_u(x^{'})||sk)$. Finally, S sends the message $\{Auth_s, T_v(x^{'})\}$ to U.

Step 3. According to receiving the message from S, the smart card derive the session key by computing $sk = h_2(ID||T_u T_v(x^{'}))$. Then verifies if exists $Auth_s^{'} = h_1(T_u(x^{'})||sk) \stackrel{?}{=} Auth_s$,

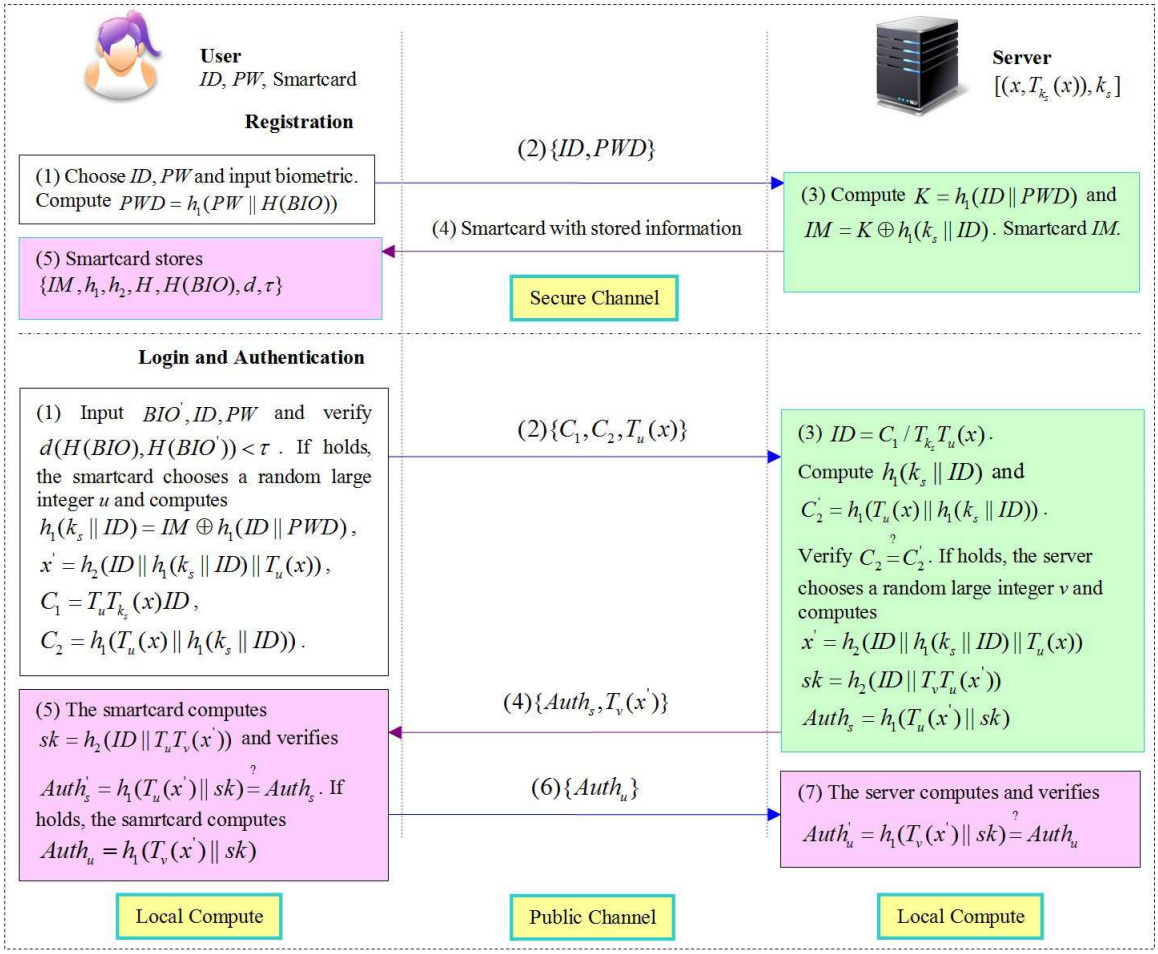

FIGURE 3. The proposed scheme

if the equation does not holds, means that U fails to authenticate S, the request will be refused, otherwise, the smart card computes $Auth_u = h_1(T_v(x')||sk)$. At last, sends the message $\{Auth_u\}$ to S.

Step 4. Upon receiving the message from U, S checks whether $Auth_u' = h_1(T_v(x')||sk) \stackrel{?}{=} Auth_u$, if it is true, notes that S authenticate U successfully, else S aborts the request.
Finally, U and S will use the session key $sk = h_2(ID||T_u T_v(x'))$ to communicate securely.

Remark 4.1. *About changing password and Biometric, we omit this phase for simplicity. The detailed changing password and Biometric phase can be refered the literature [21, 22].*

5. Security analysis.

5.1. **Security analysis for security requirements.** (1) The main difference between the improved scheme and three traditional methods
The main differences hereafter are shown in Table 3. (2) The Security of the changing x in chaotic maps about the proposed scheme

Theorem 5.1. *The new method in our proposed scheme is secure under the CMBDLP and CMBDHP assumptions.*

Proof: **(a)** For CMBDLP (see Definition 2.2. Definition 2.3.), if the traditional method is secure, then our new method is secure too. Because the traditional method is the

TABLE 3. Our new method using chaotic maps compared with three traditional methods

Basic methods using chaotic maps	Cryptosystem	Fundamental form	Fixed input variables	Examples	Hard Problems
I: Symmetric Encryption	Public key cryptosystem	$K = T_v T_K(x)$ $C = E_K(M \Vert H \Vert T \Vert ...)$	x with $T_K(x)$	[17]	Chaotic maps problems
II: Multiplication in Finite Field	Public key cryptosystem	$K = T_v T_K(x)$ $C = K \cdot (M \Vert T \Vert ...)$	x with $T_K(x)$	[18]	Chaotic maps problems
III: XORed Operation	Public key cryptosystem	$K = T_v T_K(x)$ $C = K \oplus (M \Vert T \Vert ... \Vert \text{Padding})$	x with $T_K(x)$	[12]	Chaotic maps problems
Our improved scheme	Mixed algorithm	$x = H(PW \Vert T \Vert ...)$ $C_1 = T_v(x), C_2 = T_u(x), SK = T_v T_u(x)$	ID and PW for user; x with $T_K(x)$ for server	[11] and our scheme	Chaotic maps problems
Mixed algorithm : means that Private key cryptosystem combines with Public key cryptosystem					

CMBDLP, given x and y, it is intractable to find the integer s, such that $T_s(x) = y$. Our method is the strong CMBDLP, just given y, it is intractable to find the integer s and PW, such that $T_s(H(PW||T||Ns||...)) = y$, where PW is password, T is the timestamp, Ns is the nonces and H is a secure one-way hash function.

(b) For CMBDHP (see Definition 2.4. Definition 2.5.), if the traditional method is secure, then our new method is secure too. Because the traditional method is the CMBDHP, given x, $T_r(x)$ and $T_s(x)$, it is intractable to find $T_{rs}(x)$. Our method is the strong CMBDHP, just given $T_r(H(PW||T||Ns||...))$ and $T_s(H(PW||T||Ns||...))$, it is intractable to find $T_{rs}(H(PW||T||Ns||...))$, where PW is password, T is the timestamp, Ns is the nonces and H is a secure one-way hash function. (3) The Freshness of the proposed

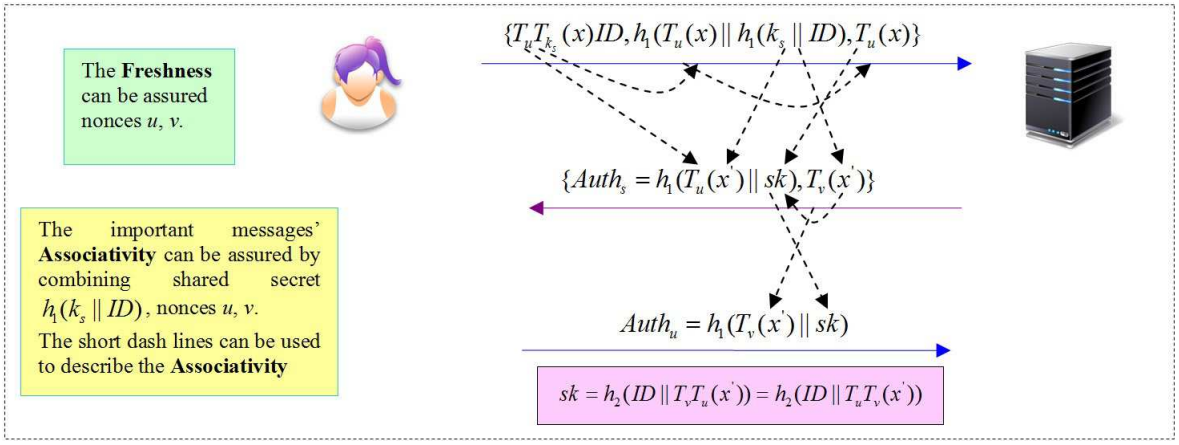

FIGURE 4. The Freshness and Associativity of Login and Authentication phase in the improved scheme

scheme

Theorem 5.2. *Each message in our proposed scheme is fresh under the CMBDLP and CMBDHP assumptions.*

Proof: Our proposed scheme uses three connected factors (Password, Biometric and Nonces) to acquire authentication, and then we only used one factornonces to achieve freshness. From Figure 4, we can see that all the important messages including the nonces which can be assure freshness. In the proposed scheme, u and v are the nonces which can satisfy the conditions of the CMBDLP and CMBDHP assumptions.

(4) The Associativity of the three messages in our proposed scheme

Theorem 5.3. *All the three messages in our proposed scheme are associative under the CMBDLP and CMBDHP assumptions.*

Proof: From Figure 2, we see the short dash lines is related with each other which mean the trust flow. By analyzing the trust flow, we can deduce the next message is fresh. The trust flow is as below:

$$\text{secret } PW \text{ with } BIO \xrightarrow[Hash]{Biohash} h_1(k_s||ID) \xrightarrow[CMBDHP,Hash]{CMBDLP} C_1, C_2, T_u(x)$$

Trust flow: $\xrightarrow[CMBDHP,Hash]{CMBDLP} sk$ and $Auth_s$ Based

$\xrightarrow[CMBDHP,Hash]{CMBDLP} sk$ and $Auth_u$

on the Theorem 4.1, Theorem 4.2 and Theorem 4.3, and from the Table 4, we can see that the proposed scheme can provide known secure session key agreement, impersonation attack and so on.

TABLE 4. Definition and simplified proof

Attack Type	Security Requirements	Definition	Simplified Proof	Hard Problems
Missing encrypted identity attacks	Man-in-the-middle attack(MIMA)	The MIMA 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.	All the information includes the *ID*, password and some nonces: *u*, *v* and the another form $T_u(x), T_v(x)$.	Chaotic maps problems
	Impersonation attack	An adversary successfully assumes the identity of one of the legitimate parties in a system or in a communications protocol.	All the information includes the *ID*, password and some nonces: *u*, *v* and the another form $T_u(x), T_v(x)$.	Chaotic maps problems
Design defect attacks	Stolen-verifier attacks	An adversary gets the verifier table from servers by a hacking way, and then the adversary can launch any other attack which called stolen-verifier attacks.	There are no any verification tables in any node.	Chaotic maps problems
Automatic validation attacks	Guessing attacks (On-line or off-line)	In an off-line guessing attack, an attacker guesses a password or long-term secret key and verifies his/her guess, but he/she does not need to participate in any communication during the guessing phase. In an undetectable on-line guessing attack, an attacker searches to verify a guessed password or long-term secret key in an on-line transaction and a failed guess cannot be detected and logged by the server.	Because any transferred message on the public channel can't construct the form $f(PW) = Y$, where Y is the message and only a input *PW*. Except for *PW*, there are more two secret input variables at least, such as *u*, *v*, *H(BIO)*.	Chaotic maps problems
	Losting smart device and guessing attacks	An adversary gets the user's smart device and then carries out the guessing attacks.	There is no useful information in the smart card.	Hash and Biohash
	Human Guessing Attacks	In human guessing attacks, humans are used to enter passwords in the trial and error process.	For 8-character passwords, the theoretical password space is $33^8 \approx 2^{40}$ for ClickText with an alphabet of 33 characters	Chaotic maps problems
No freshness verify attacks	Perfect forward secrecy	An authenticated key establishment protocol provides perfect forward secrecy if the compromise of both of the node's secret keys cannot results in the compromise of previously established session keys.	Different session has different nonces.	Chaotic maps problems
	Known session key security	Each execution of the protocol should result in a unique secret session key. The compromise of one session key should not compromise the keys established in other sessions.	Different session has different nonces.	Chaotic maps problems
	Replay attack	A replay attack is a form of network attack in which a valid data transmission is repeated or delayed maliciously or fraudulently.	Every important message includes the nonces: *u*, *v* and the another form $T_u(x), T_v(x)$.	Chaotic maps problems

5.2. **Security proof based on the BAN logic [11, 19].** For convenience, we first give the description of some notations (Table 5) used in the BAN logic analysis and define some main logical postulates (Table 6) of BAN logic. According to analytic

TABLE 5. Notations of the BAN logic

Symbol	Definition
$P \mid\equiv X$	The principal P believes a statement X, or P is entitled to believe X.
$\#(X)$	The formula X is fresh.
$P \mid\Rightarrow X$	The principal P has jurisdiction over the statement X.
$P \lhd X$	The principal P sees the statement X.
$P \mid\sim X$	The principal P once said the statement X.
(X,Y)	The formula X or Y is one part of the formula (X,Y).
$\langle X \rangle_Y$	The formula X combined with the formula Y.
$\{X\}_K$	The formula X is encrypted under the key K.
$(X)_K$	The formula X is hash function with the key K. If there is no K, and that means is no key input.
$P \overset{K}{\longleftrightarrow} Q$	The principals P and Q use the shared key K to communicate. The key K will never be discovered by any principal except P and Q.
$\overset{K}{\longrightarrow} P$	The public key of P, and the secret key is described by K^{-1}

TABLE 6. Logical postulates of the BAN logic

Symbol	Definition	
$\dfrac{P \mid\equiv P \overset{K}{\longleftrightarrow} Q, P\{X\}_K}{P \mid\equiv Q \mid\sim X}$	The message-meaning rule	(R_1)
$\dfrac{P \mid\equiv \#(X)}{P \mid\equiv \#(X,Y)}$	The freshness-conjuncatenation rule	(R_2)
$\dfrac{P \mid\equiv \#(X), P \mid\equiv Q \mid\sim X}{P \mid\equiv Q \mid\equiv X}$	The nonce-verification rule	(R_3)
$\dfrac{P \mid\equiv Q \mid\Rightarrow X, P \mid\equiv Q \mid\equiv X}{P \mid\equiv X}$	The jurisdiction rule	(R_4)
$\dfrac{P \mid\equiv Q \mid\equiv (X,Y)}{P \mid\equiv Q \mid\equiv X}$	The belief rules	(R_5)
Remark 3: Molecule can deduce denominator for above formulas.		

TABLE 7. Goals of the proposed scheme

Goals	
Goal 1. $Alice \mid\equiv (Alice \overset{SK}{\longleftrightarrow} Server)$;	Goal 2. $Alice \mid\equiv Server \mid\equiv (Alice \overset{SK}{\longleftrightarrow} Server)$;
Goal 3. $Server \mid\equiv (Server \overset{SK}{\longleftrightarrow} Alice)$;	Goal 4. $Server \mid\equiv Alice \mid\equiv (Server \overset{SK}{\longleftrightarrow} Alice)$;
Where SK means the session key and Alice means a common user.	

procedures of BAN logic, our scheme should satisfy the following goals in Table 7: First of all, we transform the process of our protocol to the following idealized form. $(Alice \rightarrow Server)m_1 : Server \lhd T_u T_{k_s}(x)ID, (T_u(x)||(k_s||ID)), T_u(x)$;
$(Server \rightarrow Alice)m_2 : Alice \lhd (T_u(x^{'})||sk), T_v(x^{'})$;
$(Alice \rightarrow Server)m_3 : Server \lhd (T_v(x^{'})||sk)$;
According to the description of our protocol, we could make the following assumptions about the initial state, which will be used in the analysis of our protocol in Table 8. Based on the above assumptions, the idealized form of our protocol is analyzed as follows. The main steps of the proof are described as follows:

For m_1:

According to the m_1 and P_2, P_5 and attributes of chaotic maps, and relating with R_1, we could get:
$S_1 : Server|\equiv Alice|\tilde{}m_1$

TABLE 8. Assumptions about the initial state of our protocol

Initial states	
$P_1 : Alice \mid\equiv Alice \xleftrightarrow{h_1(k_s \| ID)} Server$	$P_2 : Server \mid\equiv Alice \xleftrightarrow{h_1(k_s \| ID)} Server$
$P_3 : Alice \mid\equiv \#(u)$	$P_4 : Bob \mid\equiv \#(v)$
$P_5 : Alice \mid\equiv \xrightarrow{(x, T_{k_s}(x))} Server$	

Based on the initial assumptions P_2, P_3, P_5, and relating with R_2, we could get:
$S_2 : Server| \equiv \#m_1$
Based on R_5 and attributes of chaotic maps, we take apart S_2 and recover $T_u T_{k_s}(x) ID$:
$S_3 : Server| \equiv \#ID$, $S_4 : Server| \equiv \#(T_u(x)||(k_s||ID))$, $S_5 : Server| \equiv \#T_u(x)$
Based on S_3, S_4, S_5, attributes of chaotic maps and the secure hash function, the server can get $x^{'}, sk, Auth_s$. Next, Alice will receive m2 from the Server.
For m_2:
According to the m_2 and P_1, P_4 and attributes of chaotic maps, and relating with R_1, we could get:
$S_6 : Alice| \equiv Server| \tilde{} m_2$
Based on the initial assumptions P_1, P_4, and relating with R_2, we could get:
$S_7 : Alice| \equiv \#m_2$
Based on R_5, we take apart S_7 and get:
$S_8 : Alice| \equiv \#Auth_s$, $S_9 : Alice| \equiv \#T_v(x^{'})$
Based on S_8, S_9, attributes of chaotic maps and the secure hash function, Alice can get $Auth_s^{'}, sk, Auth_u$.
Next, the server will receive m3 from Alice.
For m_3:
According to the m_3 and P_2, P_3, P_7 and attributes of chaotic maps, and relating with R_1, we could get:
$S_{10} : Server| \equiv Alice| \tilde{} m_3$
Based on the initial assumptions P_2, P_3, P_7, and relating with R_2, we could get:
$S_{11} : Server| \equiv \#m_3$
Based on R_5, we take apart S_{11} and get:
$S_{12} : Server| \equiv \#Auth_u$
Based on S_{12}, attributes of chaotic maps and the secure hash function, the server can compute $Auth_u^{'}$
Combine:
Because Alice and the server communicate each other just now, they confirm the other is on-line. Moreover, since Alice and the server have shared their secret information $h_1(k_s||ID)$ and kept it safe, and based on $S_3, S_4, S_5, S_8, S_9, S_{12}, R_4$ with chaotic maps problems, we could get:
Goal 1. $Alice| \equiv (Alice \xleftrightarrow{SK} Server)$; Goal 2. $Alice| \equiv Server| \equiv (Alice \xleftrightarrow{SK} Server)$;
Goal 3. $Server| \equiv (Server \xleftrightarrow{SK} Alice)$; Goal 4.$Server| \equiv Alice| \equiv (Server \xleftrightarrow{SK} Alice)$;
According to (Goal 1 Goal 4), we know that both Alice and the server believe that the other peer can authenticate and output the same session key based on the fresh nonces u, v, the shared information $h_1(k_s||ID)$.

6. **Efficiency Comparison.** Compared to RSA and ECC, Chebyshev polynomial computation problem offers smaller key sizes, faster computation, as well as memory, energy and bandwidth savings. To be more precise, on an Intel Pentium4 2600 MHz processor

with 1024 MB RAM, where n and p are 1024 bits long, the computational time of a one-way hashing operation, a symmetric encryption/decryption operation, an elliptic curve point multiplication operation and Chebyshev polynomial operation is 0.0005s, 0.0087s, 0.063075s and 0.02102s separately [13, 20, 21]. Moreover, the computational cost of XOR operation could be ignored when compared with other operations. we sum up these formulas into one so that it can reflect the relationship among the time of algorithms intuitively. $T_p \approx 10T_m \approx 30T_c \approx 72.6T_s \approx 1263.24T_h$, where: T_p: Time for bilinear pair operation, T_m: Time for a point scalar multiplication operation, T_c: The time for executing the $T_n(x) \bmod p$ in Chebyshev polynomial, T_s: Time for symmetric encryption algorithm, T_h:Time for Hash operation.

About these algorithms, our proposed four frameworks only used the chaotic cipher and a secure one way hash/pseudo-random function as the main algorithm which are more efficient than bilinear pair operation and a point scalar multiplication operation ECC-based. Especially for hash operation, it can be ignored compared with the other three algorithms.

From Table 9, we can conclude that our four frameworks have reasonable-efficient and high-security property.

TABLE 9. Comparisons between our proposed scheme and the literature [11]

Protocols (Login and Authentication)			Lu et al. [11] (2015)	Ours
Efficiency	**Computation**	*User*	$1T_{Bh} + 5T_h + 2T_c + 4T_{xor}$	$1T_{Bh} + 5T_h + 2T_c + 1T_{xor}$
		Server	$5T_h + 2T_c + 4T_{xor}$	$6T_h + 2T_c$
		Total	$1T_{Bh} + 10T_h + 4T_c + 8T_{xor}$	$1T_{Bh} + 11T_h + 4T_c + 1T_{xor}$
	Communication	Messages	3	3
		rounds	3	3
Security	**Requirements**	Provide user anonymity	Yes	Yes
		Provide mutual authentication	Yes	Yes
		Provide perfect forward secrecy	Yes	Yes
		Provide Session key security	Yes	Yes
		Resist insider attack	Yes	Yes
		Resist impersonation attack	Yes	Yes
		Resist off-line password guessing attack	Yes	Yes
		Privacy Protection	Yes	Yes
		Resist SDOA flaw	No	Yes
		Resist PLXO	No	Yes
	Design	No synchronized	Yes	Yes
		Practical design	No	Yes
		Concise design	No	Yes
		Number of nonces	2	2
		Factors	3(password + BIO + k_u) for user 1(k_s) for server	2(password+BIO) for user 1(k_s) for server
		Model	Random Oracle	Random Oracle

T_h: Time for Hash operation
T_{Bh}: Time for BIOHash operation
T_{xor}: Time for XORed operation
T_c: The time for executing the $T_n(x) \bmod p$ in Chebyshev polynomial using the algorithm in literature [20]

7. **Conclusion.** In this study, we investigated the chaotic maps-based password authentication scheme for Telecare Medicine Information Systems. Firstly, we point out that Lus scheme has many flaws (see section 3.2). Then we give the deep and comprehensive analysis about the reasons why these flaws can occur. Next, we further proposed a secure biometric based authentication scheme for TMISs using enhanced chaotic maps to conquer the security flaws. Considering the security and efficiency provided by our scheme, we conclude that our scheme is more appropriate for telemedical applications in comparison with other related schemes. In a word, our scheme is not a panacea, but it offers reasonable security, preferable efficiency, easy usability, and appears to fit well with some

practical applicationspassword and smartcard based surroundings, whether in traditional network or in mobile network.

REFERENCES

[1] Wu, Z. Y., Lee, Y. C., Lai, F., Lee, H. C., Chung, Y., A secure authentication scheme for telecare medicine information systems, *Journal of Medical Systems*, vol.36, no.3, pp 1529-1535, 2012.

[2] D. B. He, J.H. Chen, R. Zhang, A More Secure Authentication Scheme for Telecare Medicine Information Systems. *Journal of Medical Systems*, vol.36, no.3, pp.1989-1995, 2012.

[3] J. Wei, X. Hu, W. Liu, An improved authentication scheme for telecare medicine information systems, *Journal of Medical Systems*, vol. 36, no. 6, pp.35973604, 2012.

[4] Z. Zhu, An efficient authentication scheme for telecare medicine information systems, *Journal of Medical Systems*, vol.36, no.3, pp.3833-3838, 2012.

[5] T. Cao,, and J. Zhai, Improved Dynamic ID-based Authentication Scheme for Telecare Medical Information Systems, *Journal of Medical Systems*, vol.37, no.2, pp.1-7, 2013.

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

[7] X. Hao, J. Wang, Q. Yang, X. Yan, P. Li, A chaotic map-based authentication scheme for telecare medicine information systems, *Journal of Medical Systems*, vol.37, no.2, pp.9919, 2013.

[8] Q.Jiang, J.Ma, X. Lu, Y.Tian, Robust chaotic map-based authentication and key agreement scheme with strong anonymity for telecare medicine information systems, *Journal of Medical Systems*, vol.38, no.2, pp.12, 2014.

[9] T.F.Lee, An Efficient chaotic map-based authentication and key agreement scheme using smart cards for telecare medicine information systems, *Journal of Medical Systems*, vol.37, no.6, pp.9985, 2013.

[10] C. T. Li, C.L. Cheng, Y.W. Chi, A secure chaotic maps and smart cards based password authentication and key agreement scheme with user anonymity for telecare medicine information systems, *Journal of Medical Systems*, vol.38, no.9, pp.1-11, 2014.

[11] Y. Lu, L. Li, H. Peng, D. Xie, Y. Yang, Robust and Efficient Biometrics Based Password Authentication Scheme for Telecare Medicine Information Systems Using Extended Chaotic Maps, *Journal of Medical Systems*, vol.39, no.6, pp.39-65, 2015.

[12] H. Zhu, Cryptanalysis and Provable Improvement of a Chaotic Maps-based Mobile Dynamic ID Authenticated Key Agreement Scheme, *Security Comm. Networks 2015*, 8:29812991.

[13] X. Wang , and J zhao, An improved key agreement protocol based on chaos, *Communications in Nonlinear Science and Numerical Simulations*, vol.15, no.12, pp.4052-4057, 2010.

[14] L. Zhang, Cryptanalysis of the public key encryption based on multiple chaotic systems, *Chaos Solitons Fractals*, vol.37, no.3, pp.669-674, 2008.

[15] Devaney, L.R, An Introduction to Chaotic Dynamical System, *Cummings Publishing Company Inc*, The Benjammin, Menlo Park, 1986.

[16] J. C. Jiang, Y. H. Peng, Chaos of the Chebyshev polynomials, *Nat. Sci. J. Xiangtan Univ*, vol.19, no.3, pp.37-39, 1996.

[17] C.C.Lee, C.T.Li, C.W. Hsu, A three-party passwordbased authenticated key exchange protocol with user anonymity using extended chaotic maps, *Nonlinear Dynamics*, vol.73, no.1-2, pp.125-132, 2013.

[18] H. Lai, M. A. Orgun, J. Xiao, et al, Provably secure three-party key agreement protocol using Chebyshev chaotic maps in the standard model, *Nonlinear Dynamics*, vol.77, no.4, pp.1427-1439, 2014.

[19] M. Burrows, M. Abadi, R. Needham, A logic of authentication, *ACM Trans. Comput. Syst*, vol.8, pp.18-36, 1990.

[20] L. Kocarev, and S. Lian, Chaos-Based Cryptography, *Theory, Algorithms and Applications*, vol.37, no.2, pp.53-54, 2011.

[21] H. J. Wang, H. Zhang, J. Li and X. Chen, A(3,3) visual cryptography scheme for authentication, *Journal of Shenyang Normal University* , vol.31, no.101, pp.397-400, 2013.

[22] H. F. Zhu, X. Hao, A provable authenticated key agreement protocol with privacy protection using smart card based on chaotic maps, *Nonlinear Dynamics*, vol.81, pp.311-321, 2015.