computers

Article

Strong Authentication Scheme Based on Hand Geometry and Smart Card Factors

Ali A. Yassin [1,2], Jian Yao [1,*] and Shiyao Han [1]

[1] School of Remote Sensing and Information Engineering, Wuhan University, Wuchang District, Wuhan 430079, China; hanshiyao2010@whu.edu.cn

[2] Computer Science Deptment, Education College for Pure Sciences, Basrah University, Basrah 61004, Iraq; Aliadel79yassin@gmail.com

* Correspondence: jian.yao@whu.edu.cn; Tel.: +86-27-6877-1218

Academic Editor: Thomas Strang
Received: 28 March 2016; Accepted: 9 June 2016; Published: 11 July 2016

Abstract: In 2009, Xu et al. presented a safe, dynamic, id-based on remote user authentication method that has several advantages such as freely chosen passwords and mutual authentication. In this paper, we review the Xu–Zhu–Feng scheme and indicate many shortcomings in their scheme. Impersonation attacks and insider attacks could be effective. To overcome these drawbacks, we propose a secure biometric-based remote authentication scheme using biometric characteristics of hand-geometry, which is aimed at withstanding well-known attacks and achieving good performance. Furthermore, our work contains many crucial merits such as mutual authentication, user anonymity, freely chosen passwords, secure password changes, session key agreements, revocation by using personal biometrics, and does not need extra device or software for hand geometry in the login phase. Additionally, our scheme is highly efficient and withstands existing known attacks like password guessing, server impersonation, insider attacks, denial of service (DOS) attacks, replay attacks, and parallel-session attacks. Compared with the other related schemes, our work is powerful both in communications and computation costs.

Keywords: smart card; user authentication; hand geometry; key agreement

1. Introduction

Password-based authentication schemes consider the most widespread protocol used to validate authentication between legitimate customers and the remote server. The single-factor authentication (SFA) considers the first process for securing access to a specified system, such as a web site or e-business system, that identifies the party demanding access over only one type of credential. One of the major worries with passwords is that users face many challenges to understand how to make robust and remarkable passwords, or undervalue the need for security. Furthermore, most users tend to select something such as phone numbers, birthdays, favorite games, and names of movies. These matters are easy to memorize. Accordingly, adversaries can build a table of important words in order to enter the system by applying a dictionary attack. Additionally, these passwords can be broken in a matter of a few short minutes. As a result, this type of password can be detected from a simple note, either in use or heedlessly rejected. While those ways need to be secured against, passwords are also required to be less predictable by machines. Moreover, the predications of password entropy mean how difficult an obtained password would be to crack via guessing, dictionary, brute force cracking attacks or other well-known schemes. In short, passwords are still one of the most simply stolen/broken categories of authentication. Multi-factor authentication (MFA) collects two or more separate credentials: what a user knows (PIN), what a user has (smart card) and what a user is (fingerprint). The purpose of MFA is to generate a layered protection and make it more troublesome for an illegal person to arrive at a target such as a server, computing device, web system, or network. If one factor is assumed to be disclosed or detected, the adversary still has at least one more fence to get around before successfully reaching the target. On the other side, the typical costs for prevailing multi-factor authentication techniques are a little money per month, per device. However, this can add up to thousands of dollars per year for budget companies that have a lot of customers or devices, or both. Obviously, multi-factor authentication tools are worthwhile, principally as the number of passwords continues to rise and make headlines. Businesses have been set-up to provide better methods to preserve user login information beyond an easy username/password mixture [1–5].

Furthermore, there are many challenging issues that raise concerns about using multi-factor authentication including the high costs, not being easy to carry, not providing the functionalities of revocation, and failing to resist well-known attacks such as off-line guessing of passwords, Man-in-the-Middle (MITM), and user/server impersonation attacks. Principally, the user's password refers to the first factor while the second factor can be one of tokens, smart cards, fingerprints, voices, etc. Only the genuine user has registered his second factor to the server in advance. However, the token cannot resist the MITM seed-tracing, comes at a high cost, and when it is lost or stolen, the service provider security may be compromised. Furthermore, how to arrange tokens issued by several servers is a big problem for both users and servers. The shortcomings of users' biometric factors, when a large number of users try to authenticate in the system at the same time, the mechanism of the system becomes unacceptably slow.

Moreover, biometric factors require extra hardware and software. In this paper, we propose a strong scheme based on smart card and feature extraction of hand geometry to overcome the above-mentioned issues. Therefore, this section introduces biometrics features and smart cards, and then explains the main goals of this paper that lead to the presentation of our proposed scheme [1–6].

Accountability with articular authentication is significant for security in the communication world. Several physiological features of humans such as biometrics, are characteristically time stable, easy to acquire, and unique for every individual. Biometric features such as palm prints, handwriting, signatures, fingerprints, irises, faces, and hand geometry have been proposed for security in many fields such as access control, authentication, and authorization. There is a lot of research focused on fingerprints and faces [6–9]. The trustworthiness of personal identification applied to the face is considered low, as researchers currently continue to fight with the issues of orientations, gestures, poses, and lighting [2]. Fingerprint identification is extensively used in biometric identification, as it leads to good results in most cases. Conversely, it is not easy to obtain fingerprint features such as minutiae for elderly people. Minutiae indicate specific points of user's fingerprints, the small details of user's fingerprints that are most significant for fingerprint recognition.

Consequently, other biometric characteristics receive more attention for personal identification. Similarly, additional biometric features like hand geometry, can be easily added into the current authentication scheme to provide an improved level of reliability in personal authentication.

There are several authentication schemes that are proposed in [8–13] to use the smart card as a second authentication factor. Das et al. [14] proposed a scheme that is secure against replay attack, password guessing attacks, forgery attacks, dictionary attacks and identity theft. The researchers [15,16] denoted drawbacks of Das et al.'s scheme, which suffers from disclosing the identity of user's authentication messages. Shih [16] also explained that Liou et al.'s [15] scheme cannot achieve mutual authentication and fails to resist off-line password guessing attacks. Xu–Zhu–Feng [3] refers to a forgery attack on Lee–Chiu's scheme [17], and Lee–Kim–Yoo's scheme [18] cannot resist the password dictionary attack. Additionally, Wang et al. [19] describe weaknesses of the schemes proposed by Kumar [20] and Awasthi-Lal [12]. Currently, Chun-Ta et al. [21] presented an improved scheme of Khan et al. [22] that fails to preserve user's anonymity. Continuously, their improved scheme can satisfy several of the main security and functionality features for remote login systems. However, it also cannot support the biometric factor for enabling the revocation feature when the valid user loses his smart card or gets its stolen.

Regarding the advantages of biometric factors, the low value of secret-key entropy is the fault of biometric factors, which can be hacked in polynomial time. For instance, there is no way to avoid an adversary from applying his impersonation attack to the victim user if both the user's password and smart card were lost/stolen. Therefore, several schemes [16–19] ensure the security of the system when either his password or his smart card is lost/stolen, but not both of them at the same time. On the opposite side, there is a sturdy secret key that combines smart cards and biometrics with passwords (called Multi-Factor Authentication (MFA)) that enjoy high entropy. Furthermore, the essential feature of the biometric is uniqueness in that everybody has various sources of biometrics such as fingerprints and eye recognition, and it is hard for genuine user's biometrics to be lost/stolen because only the actual user enters personal biometrics with his smart card to login to the system. There are many schemes based on biometrics with smart cards [9,13], but these schemes require extra hardware and software for each login phase.

Moreover, smart cards are considered small devices and require low computation capability, mingy energy resources and small memory size. It is more desirable to only use symmetric-key manners such as crypto-hash functions, symmetric encryptions instead of applying costly asymmetric cryptographic schemes. Moreover, smart cards are generally widespread in sensitive environments such as bank services and health-care. On the other hand, the conventional security risks are exposed to many malicious attacks and are prone to more dangerous attacks. As a result, an esteemed multi-factor authentication scheme for smart cards should be able to prevent various common malicious attacks like insider, impersonation, MITM, replay and online/offline password guessing.

Additionally, the privacy of users is considered very important in the smart card industry. There is an imperious need for preserving user's data access privacy, when important data is submitted in the login phase, and what data types the user is interested in, since the infiltration of such information could be hard-done by an adversary to use it when the legal user logout the system. There is an increasing demand for preserving user privacy information from being leaked and abused, which borders the needs for protecting strong schemes that can acquire asymmetric-key encryption, preserving user's privacy, and user anonymity [19].

Furthermore, imposing efforts have been focused on producing schemes with user anonymity by only applying lightweight symmetric-key primitives like crypto hash functions and modern block ciphers. In this paper, we focus on two parts. In the first part, we analyze Xue et al.'s scheme, and present the main challenges in designing an authentication scheme with user anonymity. In the second part, we refer to the practical solutions for using user anonymity in our proposed scheme.

Additionally, we embed users' hand geometry features as a biometric factor with the smart card in an effective manner that does not require extra hardware and software in the login phase. In the registration phase, a user submits his hand geometry and hashed user name and password into the server. Then, the server extracts the features of hand geometry and sends back the features, and smart card to the user. After that, the user keeps his hand geometry features in his USB to use in the next phases. Therefore, the adversary will have difficulty obtaining the user's smart card and USB for applying malicious attacks. Furthermore, we review a security analysis of the Xu–Zhu–Feng scheme that is not immune to password guessing attacks and impersonation attacks. We also propose a new efficient and secure smart card based on a remote password authentication scheme that overcomes not only the weaknesses of the Xu–Zhu–Feng scheme, but also enjoys several features such as efficiency, flexible password-based remote mutual authentication, user anonymity, users being able to freely select and update their passwords, and the server and user being able to construct authenticated session keys. In fact, our scheme generates a key once for each user's login request in the authentication phase. Moreover, our scheme can resist many kinds of attacks such as replay attacks, insider attacks, off-line attacks, reflection attacks, and DOS attacks. Continuously, compared with the other related schemes, our work is powerful both in communications and computation costs.

The remainder of the paper is organized as follows. Section 2 reviews the Xu–Zhu–Feng scheme. Feature extraction of hand geometry and design issues of the proposed scheme are discussed in

Section 3. Our proposed scheme is presented in Section 4. Security analysis is reviewed in Section 5, and Section 6 presents the discussion and comparison with state-of-the-art methods. Section 7 provides our conclusions.

2. The Xu–Zhu–Feng Scheme

In this section, we focus on review and cryptanalysis of the Xu–Zhu–Feng scheme as follows:

2.1. Review of the Xu–Zhu–Feng Scheme

Some notations of the Xu–Zhu–Feng scheme will be presented. Then, we will explain the main phases of the Xu–Zhu–Feng scheme, which consists of a registration phase, login phase, verification phase and password change phase. Figure 1 presents the Xu–Zhu–Feng scheme.

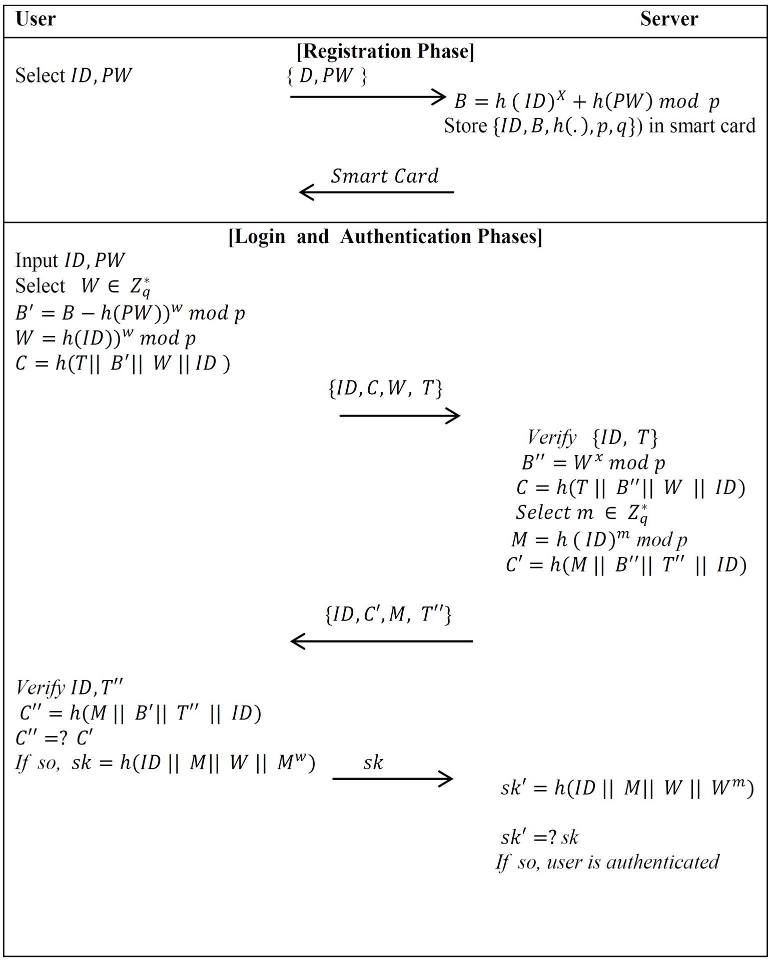
User
Server
[Registration Phase]
Select ID, PW
$\{ D, PW \}$
$B = h\,(ID)^X + h(PW) \bmod p$
Store $\{ID, B, h(.), p, q\})$ in smart card
$Smart\ Card$
[Login and Authentication Phases]
Input ID, PW
Select $W \in Z_q^*$
$B' = B - h(PW))^w \bmod p$
$W = h(ID))^w \bmod p$
$C = h(T \| B' \| W \| ID)$
$\{ID, C, W, T\}$
$Verify\ \{ID, T\}$
$B'' = W^x \bmod p$
$C = h(T \| B'' \| W \| ID)$
$Select\ m \in Z_q^*$
$M = h\,(ID)^m \bmod p$
$C' = h(M \| B'' \| T'' \| ID)$
$\{ID, C', M, T''\}$
$Verify\ ID, T''$
$C'' = h(M \| B' \| T'' \| ID)$
$C'' =?\ C'$
$If\ so,\ sk = h(ID \| M \| W \| M^w)$
sk
$sk' = h(ID \| M \| W \| W^m)$
$sk' =?\ sk$
$If\ so,\ user\ is\ authenticated$

Figure 1. Explanation of the Xu–Zhu–Feng scheme.

- **Notations**
  In order to make future references more easy to understand, frequently repeated notations are enumerated below with their descriptions (see Table 1).

- **Initial Phase**
  The server picks large prime numbers, p and q, such that $p = 2q + 1$, and selects its secret key $x \in Z_q^*$.

- **Registration Phase**
  The user sends his identity *ID* and password *PW* to the authentication server via a secure channel. Then, the server calculates $B = h(ID)^x + h(PW)\ mod\ p$ when he receives the registration request message {*ID*,*PW*} from the valid user. After that, the server saves the important data $\{ID, B, h(.), p, q\}$ into a new smart card and pushes it to the user.

- **Login Phase**
  The user attaches his smart card to a device reader and enters his *ID* and *PW*. The smart card selects a random number $w \in Z_q^*$, establishes the time-stamp with the current time, and computes the following:
  $B' = B - h(PW)^w\ mod\ p, w = h(ID)^w\ mod\ p, C = h(T||B'||w||ID)$.
  It then submits the login message $\{ID, C, w, T\}$ to the server. However, we notice that the smart card is required to run the modulus exponentiation computation twice in this phase.

- **Authentication Phase**
  After receiving the user's login message at time T', the server verifies the identity of the user *ID* and the time-stamp T by checking $(T' - T) \leq \Delta T$, where ΔT is a threshold defined in advance. Then, the server calculates $B'' = w^x mod\ p$ and tests whether C is equal to $h(T||B''||w||ID)$. If the above validations go through effectively, the user is genuine and the server continues with the following procedure. Otherwise, it terminates the login request. The server selects a random number $m \in Z_q^*$, sets the time-stamp T'', $M = h(ID)^m\ mod\ p, C' = h(M||B''||T''||ID)$, and submits the message $\{ID, C', M, T''\}$ to the user. After receiving the message, the smart card verifies ID and T'' and then compares C' with $h(M||B''||T''||ID)$. If they are equal, the server is valid. Both the user and server compute $s_k = h(ID||M||w||M^w) = h(ID||M||w||w^m)$.

Table 1. Notations used through the Xu–Zhu–Feng scheme.

Symbol	Description
Id_A	Identity of user A.
Id_B	Identity of user B.
PW_A	Password of user A.
R_A	The one-time random number generated by the user A.
T_A	The time-stamp of user A.
T_S	The time-stamp of server S.
$\triangle T$	Threshold's time defined in advance by the system.
$h(.)$	A cryptography one-way hash function.
$E_K(M)$	The message M encrypted by session key K.
$x\ mod\ p$	The remainder of x divided by p.
$\oplus$	The bitwise XOR operation.
$\|\|$	The concatenation operation.
p,q	The two large prime numbers.
Z_q^*	The multiplicative set of Z_q.
Z_q	The ring of integers modulo q.

2.2. Cryptanalysis of the Xu–Zhu–Feng Scheme

We demonstrate that the Xu–Zhu–Feng scheme has many drawbacks such as user impersonation attacks in the authentication phase. Assume the user A is attempting to impersonate the user B using his ID_B. First, A tries to draw out the data B_A saved on B's smart card. With A's password, he can easily retrieve $h(ID_A)^x$ by $h(ID_A)^x = B_A - h(PW_A)\ mod\ p$. Then, he selects a random number $w \in Z_q^*$, sets the time-stamp T with the recent time, and computes the following steps:

$$B'_A = \ mod\ p,$$
$$w = h(ID_A)^w mod\ p,$$
$$C = h(T||B'_A(h(ID_A)^x)^w||ID_B).$$

Then, he sends the login message $\{ID_B, C, w, T\}$ to the authenticated server. Upon receiving user A's login message, the authenticated server checks the identity of user $B(ID_B)$ and the time-stamp T. The verification of the user identity $B(ID_B)$ and the time-stamp T is effective since the user A employs a legal user identity (ID_B) and selects the current time as the time-stamp. Furthermore, the authenticated server computes $B'' = w^x\ mod\ p$ and $C'' = h(T||B''||w||ID_B)$, and examines whether $C = C''$. Since $B'' = w^x = (h(ID_A)^w)^x = B'_A\ mod\ p$, the verification of C's data is also successful. As a result, an adversary A, who poses as the user B, is successfully validated by the authenticated server. An adversary cannot access the rest of the process for authenticating the server, unlike a genuine user, as an adversary does not need to authenticate server. He is successful as long as the authenticated server accepts his login request.

3. Design Issues

In this section, we explain the feature extraction of hand geometry, our proposed scheme for design issues, our proposed scheme, and security analysis of our proposed scheme.

3.1. Feature Extraction of Hand Geometry Images

The geometry image is required to be arranged in a preferred way in order to obtain the same features for identical images. The image thresholding operation has been applied to get a binary hand-shape image. The value of the threshold is automatically calculated based on Otsu's scheme [23]. Furthermore, the geometry's background is stable (black) and the threshold value can be computed at once and then used consequently for remaining images. In fact, the binarized shape of hand geometry can be approximated to an ellipse. The factors of the most-appropriate ellipse for an obtained binary hand shape is computed depending on some objects such as hand-printed characters [24]. Additionally, the orientation of the binarized hand image is approached by the main axis of the ellipse, and the vital angle of rotation is the variance between regular and the orientation regions of image. As revealed in Figure 2, the binarized image is rotated and applied for gaining the hand geometry features. The appreciated orientation of the binarized image is also applied in order to rotate the gray-level hand geometry image. Consequently, the features are classified as follows:

(1) Lengths connection the base of the hand and tips of finger;
(2) Points viewing the base point of each finger;
(3) Area surrounded by the registered points.

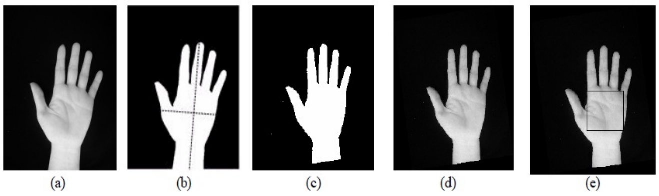

Figure 2. Extraction features of hand image; (**a**) captured image from the digital camera; (**b**) binarized image and ellipse fitting to compute the orientation; (**c**) binary image after rotation; and (**d**,**e**) gray scale images after rotation.

3.2. Our Proposed Scheme for Design Issues

The traditional authentication scheme based on smart cards consists of four phases: registration, login, authentication, and changing the password. In the registration phase, the user registers his username and password with the server. Then, the server prepares the important information that will be saved in the user's smart card. After that, the server provides the user with his smart card used in the login and authentication phases. There are many schemes [25–27] based on this traditional model that have faced several issues such as failing to preserve user's anonymity, not being able to resist well-known attacks, and not having the ability to use revocation features when the legitimate user loses or has his smart card stolen.

Our proposed scheme overcomes the above-mentioned issues by depending on the feature extraction of a user's hand geometry as an additional factor. In the registration phase, the valid user submits the hash of his username, password, and his hand geometry to the server in a secure channel. The server provides the credentials (smart card and features of hand geometry) to the user. This credential has an essential factor that will be applied by the valid user in the subsequent phases. Therefore, the user saves his features of hand geometry in his USB. In the login phase, the genuine user sends his hashed username and password to the server. Then, the server sends the challenge to the user requiring him to send his smart card and features of hand geometry. Then, the user will test the validity of the server by checking his challenge in the first step and submitting his information to the authenticated server in the second step. Finally, the user can access the server's resources when the server verifies the user's smart card and features of his hand geometry. Figure 3 shows the essential differences between our proposed scheme and the traditional authentication scheme based on smart cards.

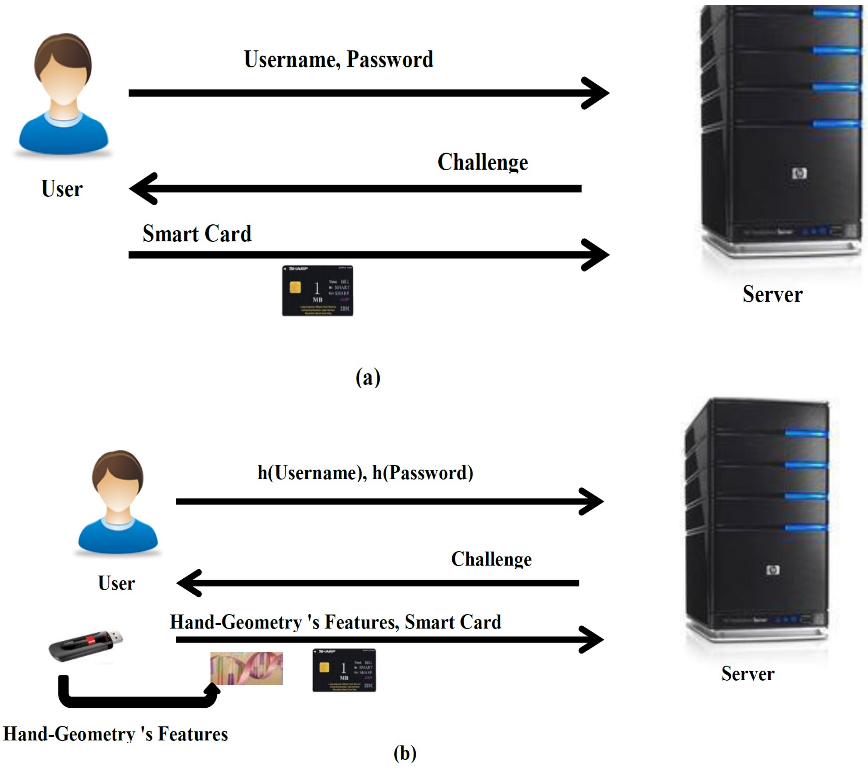

Figure 3. The main differences between traditional smart card authentication scheme (**a**) and our proposed scheme (**b**).

3.3. Comparison

We compare our proposal with Xu–Zhu–Feng's scheme and another generic design of multi-factor authentication in [28,29]. All protocols employ smart-card-based password authentication and fuzzy extractors as the building blocks to realize multi-factor authentication, but our design has made significant improvements in computation and communication. As shown in Figure 4, the authors in [28] have used three factors in the login and authentication phases. Their scheme was to run one factor in login and other factors executed in the authentication phase that may need multi-round message exchanges for Message Authentication Code (MAC) generation/verification. The proposed scheme from the authors in [29] requires three factors for authentication. The first two factors consist of login and authentication phases, and the third one is related to MAC generation/verification (only one message exchange). In terms of cost, the third factor requires extra hardware and software for extracting MAC keys from biometrics. Our proposed scheme is made up of four factors: the first two for login and the authentication phase and the other factors for MAC authentication. Our proposed scheme focuses on mutual authentication between servers and users based on feature extraction of the user's hand geometry and smart cards. Additionally, our work does not need extra devices or software for hand geometry in the login phase because the features save the user's USB in the registration phase. In terms of security and communication, our proposed scheme needs only one round to obtain MAC, which generates one time in the mutual authentication phase between users and servers. Additionally, the proposed scheme only needs lightweight symmetric-key operations compared with the Xu–Zhu–Feng scheme.

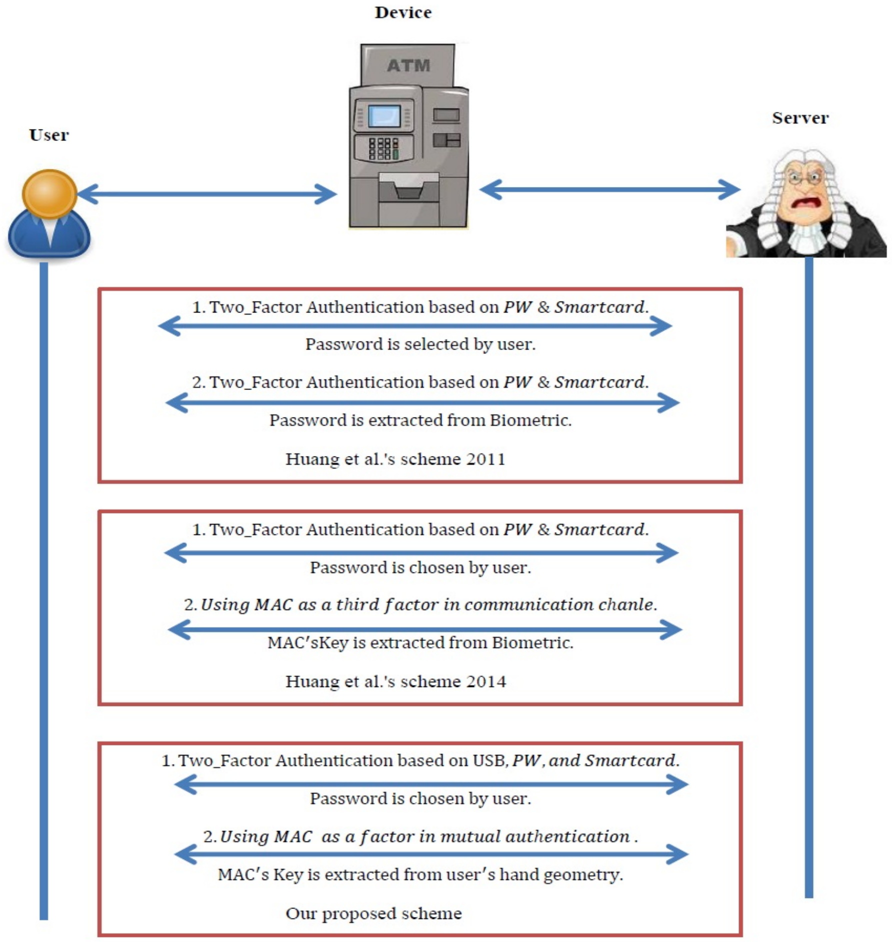
Device
ATM
User
Server
1. Two_Factor Authentication based on PW & Smartcard.
Password is selected by user.
2. Two_Factor Authentication based on PW & Smartcard.
Password is extracted from Biometric.
Huang et al.'s scheme 2011
1. Two_Factor Authentication based on PW & Smartcard.
Password is chosen by user.
2. Using MAC as a third factor in communication chanle.
MAC'sKey is extracted from Biometric.
Huang et al.'s scheme 2014
1. Two_Factor Authentication based on USB, PW, and Smartcard.
Password is chosen by user.
2. Using MAC as a factor in mutual authentication .
MAC's Key is extracted from user's hand geometry.
Our proposed scheme

Figure 4. Comparison with related works.

On the other hand, there are several schemes [30–36] that use synchronization mechanism(s) to preserve the tenacity of the one-time identity between legal users and authenticated servers. We notice that all of these schemes using similar steps to obtain user anonymity fail to resist de-synchronization attacks, which means that the synchronization of one-time identities between two entities is broken when an attacker prevents single message flow. Recently, this risk has also been revealed in [30,31], who refer to the de-synchronization weakness of the schemes in [37,38], yet no practical solution to manage this type of problem has been discovered. Lastly, the authors in [39] proposed a good scheme that can process this threat while staying efficient and accomplishing provable security. On an ongoing basis, our proposed scheme can support user anonymity based on generating one time keys for each user's login. This key is used to encrypt a user's message in the login phase, and the server also applies it in the mutual authentication phase. In addition, identification messages for each user and server are generated one time based on a random number that has worked as a salt key (see Theorem 3). Our proposed scheme does not rely directly on the principle of synchronization to obtain user anonymity compared with the other related schemes [14,15,25,26]. We proposed a new scheme that prevents an adversary from applying a de-synchronization attack or revealing the user's identity.

4. Our Proposed Scheme

There are four phases in our scheme: the registration phase, the login phase, the mutual authentication with key agreement phase, and changing the password phase. The symbols used in our proposed scheme are discussed in Table 2. Figure 5 shows our proposed scheme.

Table 2. Meaning of symbols used throughout our proposed scheme.

Symbol	Description
U_i	A legitimate user U_i.
S	A trustworthy server.
ID_i	Identity of user U_i.
PW_i	Password of user U_i.
$h(PW_i)$	Hashed password of user U_i.
$h(ID_i)$	Hashed identity of user U_i.
Hg_i	Hand geometry of user U_i.
P_i	Features of $U_i^{\prime}s$ hand geometry.
X_s	A secret key kept by S in private.
$h(.)$	A cryptography one-way hash function.
r_i	The one-time random number generated by the user U_i.
K_i	The one-time key generated for each user's login request.
T, T'	The time-stamp of the user U_i.
T''	The time-stamp of server S.
$\triangle T$	Threshold's time defined in advance by the system.
E_{K_i}	Symmetric encryption function based on key K_i.
M	Login request message from the user U_i to the remote server S.
f_i, Z', Z'', a, a'	Other miscellaneous values that are applied in the verification.
$\oplus$	The bitwise XOR operation.
$\|\|$	The concatenation operation.

- **Registration Phase**
  In this phase, everyone that will be registered on the remote server is provided with a smart card and features of hand geometry. To initialize, the user U_i submits his biometric hand geometry Hg_i, and his hashed password $h(PW_i)$ and identity $h(ID_i)$ to the remote server over a secure channel. Upon receiving the user's registration request, the server performs the following operations:

  (1) S extracts the features of the user's hand geometry Hg_i and computes $P_i = h(Hg_i)$, $N_i = h(h(PW_i)||P_i) \oplus h(ID_i)^{X_s}$, $M_i = P_i \oplus h(X_s)$, where X_s is a secret key kept by S in private;
  (2) S saves the data $\{h(.), N_i, M_i\}$ on a new smart card. S sends each of the user's smart cards and hashes of his personal biometrics (hand-geometry's features) P_i to U_i over a secure channel;
  $S \Rightarrow U_i$: smart card, P_i;
  (3) U_i saves P_i in his USB.

- **Login Phase**

  When the user U_i wishes to login to S, then U_i attaches his smart card in the card reader, his USB in the USB device to read P_i, and inputs his password PW_i. The smart card fulfills the following steps:

(1) Compute $Z' = h(h(PW_i)||P_i)$ and $h(X_s) = P_i \oplus M_i$;

(2) Generate a random number r_i and perform the following steps:

  – Compute $K_i = h(r_i \oplus Z')$, $C_i = K_i \oplus (Z' \oplus N_i)^{r_i} \oplus h(X_s)$, $f_i = h(ID_i)^{r_i}$;
  – Calculate $CID_i = Z' \oplus h(r_i \oplus T)$, where T is the current time-stamp of the input device;
  – Encrypt $E_{K_i}(r_i, T, N_i, CID_i)$ by using K_i;

(3) The user's smart card sends a login request message M to the remote server;
Smart card→ S: $M = (C_i, f_i, E_{K_i}(r_i, T, N_i, CID_i))$.

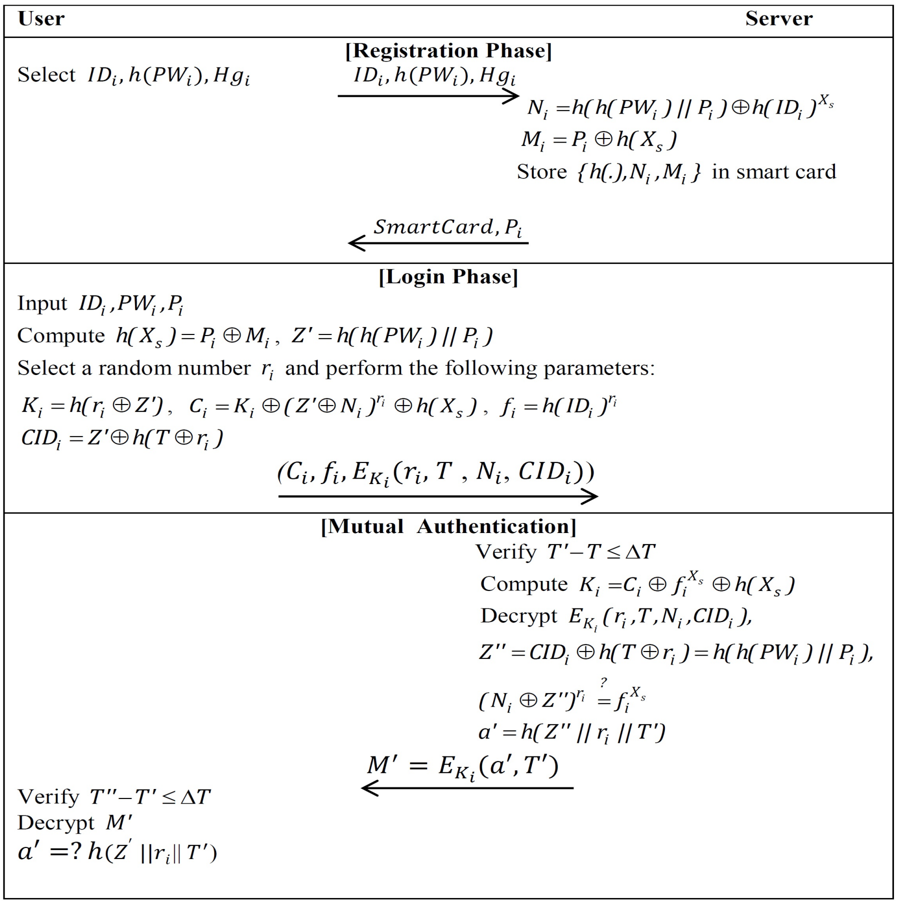
User
Server
[Registration Phase]
Select $ID_i, h(PW_i), Hg_i$
$ID_i, h(PW_i), Hg_i$
$N_i = h(h(PW_i) || P_i) \oplus h(ID_i)^{X_s}$
$M_i = P_i \oplus h(X_s)$
Store $\{h(.), N_i, M_i\}$ in smart card
$SmartCard, P_i$
[Login Phase]
Input ID_i, PW_i, P_i
Compute $h(X_s) = P_i \oplus M_i$, $Z' = h(h(PW_i) || P_i)$
Select a random number r_i and perform the following parameters:
$K_i = h(r_i \oplus Z')$, $C_i = K_i \oplus (Z' \oplus N_i)^{r_i} \oplus h(X_s)$, $f_i = h(ID_i)^{r_i}$
$CID_i = Z' \oplus h(T \oplus r_i)$
$(C_i, f_i, E_{K_i}(r_i, T, N_i, CID_i))$
[Mutual Authentication]
Verify $T' - T \leq \Delta T$
Compute $K_i = C_i \oplus f_i^{X_s} \oplus h(X_s)$
Decrypt $E_{K_i}(r_i, T, N_i, CID_i)$,
$Z'' = CID_i \oplus h(T \oplus r_i) = h(h(PW_i) || P_i)$,
$(N_i \oplus Z'')^{r_i} \overset{?}{=} f_i^{X_s}$
$a' = h(Z'' || r_i || T')$
$M' = E_{K_i}(a', T')$
Verify $T'' - T' \leq \Delta T$
Decrypt M'
$a' =? h(Z' || r_i || T')$

Figure 5. Our proposed scheme.

- **Authentication Phase**

  Upon receiving the user's login request message at time T', S performs the following computations:

(1) S computes $K_i = C_i \oplus f_i^{X_s} \oplus h(X_s)$, and decrypts $E_{K_i}(r_i, T, N_i, CID_i)$;

(2) S checks the legitimacy of the time-stamp T. If $T' - T \leq \Delta T$, then the authenticated server S accepts user's login request and then executes the next step. Otherwise, S terminates this phase;

(3) S computes $Z'' = CID_i \oplus h(T \oplus r_i) = h(h(PW_i)||P_i)$, and checks whether $(N_i \oplus Z'')^{r_i}$ is equal to $f_i^{X_s}$. If so, S accepts the user's login request;

(4) S computes $a' = h(Z''||r_i||T')$ and sends message $M' = E_{K_i}(a', T')$ to U_i.
$S \rightarrow U_i : M'$;

(5) When U_i receives the message $M' = E_{K_i}(a', T')$ at time T'', U_i executes the following steps:

- Check whether $T'' - T' \leq \Delta T$. If this does not hold, then U_i overthrows the message M' and terminates this phase. Otherwise, U_i continues the next step;
- U_i decrypts message M' by using K_i, computes $a = h(Z'||r_i||T')$, and compares a with a'. If so, U_i decides that the remote server S is authenticated.

- **Password Change Phase**

  When U_i wants to change his password from PW_i to PW_i^n, U_i runs this phase. The password change phase needs to go through the following steps:

  (1) U_i needs to be executed in the above phases login and mutual authentication. The server S authenticates his old password PW_i;

  (2) After the successful mutual authentication, U_i enters a new password PW_i^n. Then, the smart card computes $N_i^n = N_i \oplus h(h(PW_i)||P_i) \oplus h(h(PW_i^n)||P_i)$ and replaces the old N_i with a new N_i^n.

5. Security Analysis of Our Proposed Scheme

In this section, we analyze our proposed scheme and display that our work can withstand several famous attacks and enjoy several security properties. Moreover, we supply a comparative analysis with other authentication schemes.

Theorem 1. *Our proposed scheme can support mutual authentication.*

Proof. A mutual authentication feature requires both the server and the user to authenticate each other. In our work, authentication of U_i to S is represented by $M = (C_i, f_i, E_{K_i}(r_i, T, N_i, CID_i))$. In addition, the authentication of U_i to S depends on generating a new key K_i . After that, the user computes $E_{K_i}(a', T')$. An adversary is not able to generate $(K_i, h(X_s), h(PW_i), P_i, r_i)$. In addition, U_i and S securely exchange $C_i = K_i \oplus (Z' \oplus N_i)^{r_i} \oplus h(X_s)$ and $K_i = C_i \oplus f_i^{X_s}$ in the login and authentication phases, respectively. The authenticated session key is demonstrated as follows:
$C_i = K_i \oplus (Z' \oplus N_i)^{r_i} = K_i \oplus (h(ID_i)^{X_s})^{r_i}, K_i = C_i \oplus f_i^{X_i} \oplus h(X_s) = C_i \oplus h(ID_i)^{r_i})^{X_s} \oplus h(X_s)$. Thus, our proposed scheme provides mutual authentication (see Figure 5).
□

Theorem 2. *Our proposed scheme can support known-key security.*

Proof. The definition of known-key security is that the jeopardy of a session key will not lead to further endangerment of other session keys. However, if a session key $f_i = h(ID_i)^{r_i}$ is exposed to an attacker, he incapacitates inferring other session keys that are produced from the random numbers $(Z'' \oplus N_i)^{r_i}$ and the $f_i^{X_s}$ dependent Diffie–Hellman key exchange scheme. In addition, it is impossible for an attacker to get a server's secret key X_s. Furthermore, if we assume that an adversary can eavesdrop on K_i, he cannot gain any advantages from eavesdropping on K_i. Thus, it generates one time for each user login request. □

Theorem 3. *Our proposed scheme can support user anonymity.*

Proof. If an attacker eavesdrops on the user's login request message, he fails to infer the user's identity from encrypting message $E_{K_i}(r_i, T, N_i, CID_i)$, since it is encrypted with K_i, which is anonymous to the attacker. In addition, the ciphertext does not possess the real user's identity ID_i where the server verifies the user's identity in an anonymous manner between $(Z'' \oplus N_i)^{r_i}$ and $f_i^{X_s}$. Additionally, we used the time-stamp in the login phase; the user's login request message is changed each login time when its parameters $\{T, r_i, K_i, f_i, T, CID_i\}$ change in each login session. Therefore, it is impossible for the attacker to reveal the user's identity. Obviously, our proposed scheme can support user anonymity. □

Theorem 4. *Our proposed scheme can support revocation of smart cards and also does not require extra hardware and software, as it resists side-channel attacks.*

Proof. If a user's smart card is lost or stolen, an adversary cannot derive or change the password because he fails to pass the biometric verification. In addition, the secret information saved on the user's smart card is as robust as the password. In the login phase, the user inputs his biometric key which is saved in his USB. Compared with Chuang et al.'s scheme in [9], their scheme needs extra hardware and software to complete the verification of a user's biometric. Our scheme requires a USB device that is available in most of the terminate machines and focuses on features of hand geometry for increasing performance and decreasing costs.

Side-channel attacks commonly exploit the presence of data-dependent and physically noticeable phenomenons caused by the implementation of computing functions in microelectronics [40,41]. The main examples of such information outflows are comprised of power consumption and the electromagnetic radioactivity of integrated circuits. We focus on side-channel analysis against subscriber identity module (SIM) cards in smart cards that our proposed scheme does not cause overloading on smart cards because the important information of users was saved on USBs. Our proposed scheme retrieves $\{h(.), N_i, M_i\}$ from a smart card that connects with a USB's information to complete the login and authentication phase. Therefore, an adversary cannot complete the login phase even if he already has the smart card because the rest of the information has been previously saved in the USB. Eventually, the performance of the smart card is very high since the power consumption of the device is very low. □

Theorem 5. *Our proposed scheme can support security of the stored data and resist a password guessing attack.*

Proof. In our proposed scheme, the remote server S stores only secret information $\{h(.), N_i, M_i\}$ in the smart card. The secret information $\{h(.), N_i, M_i\}$ derived from the user's smart card does not assist an attacker without the user's password $h(PW_i)$, the user's personal biometric (hand geometry (P_i)) and server's secret key $h(X_s)$ to retrieve the user's secret key K_i, since $h(X_s) = P_i \oplus M_i$, $Z' = h(h(PW_i)||P_i), K_i = h(r_i \oplus Z')$ and $C_i = K_i \oplus (Z' \oplus N_i)^{r_i} \oplus h(X_s)$. If an attacker is attempting to retrieve K_i by combining dictionary attacks with the recover secret information $\{h(.), N_i, M_i\}$, he requires locating both $h(X_s)$ and $h(h(PW_i)||P_i)$ to compute $K_i = h(r_i \oplus Z')$. On the other hand, the attacker can gain (C_i, f_i) by eavesdropping on the insecure channel between U_i and S. The attacker cannot get useful information about the user's password/hand geometry from these values because other information is encrypted by the user's secret key K_i and only the user can access his biometric key. Thus, our proposed scheme provides security of the stored data and resists a password guessing attack. □

Theorem 6. *Our proposed scheme can resist the server impersonation attack.*

Proof. A user's smart card contains two values: $N_i = h(h(PW_i)||P_i) \oplus h(ID_i)^{X_s}$ and $M_i = P_i \oplus h(X_s)$. Since the user knows his password PW_i and his biometric key P_i, he can obtain the value of $h(ID_i)^{X_s}$. However, this value is based on the user's identity, and it is not the same for all users. The attacker cannot play the role of the server with this value and fails to get the values $\{X_s, K_i, P_i\}$. They are used to decrypt the ciphertext $E_{K_i}(r_i, T, N_i, CID_i)$ sent by U_i, where K_i is computed by $K_i = C_i \oplus f_i^{X_s} \oplus h(X_s)$. Therefore, the proposed scheme can resist the server impersonation attack. □

Theorem 7. *Our proposed scheme can withstand insider attacks and user impersonation attacks.*

Proof. In our proposed scheme, when U_i wishes to register with a remote server, he sends $(ID_i, h(PW_i), P_i)$ instead of ID_i, PW_i. Due to the utilization of the one-way hash function *h(.)*, it is difficult for the server to extract the password of the user from the hashed value. In addition, when the attacker wants to impersonate the valid user, he requires the forging of a legal login request message $(C_i, f_i, E_{K_i}(r_i, T, N_i, CID_i))$, in which $K_i = h(r_i \oplus Z'), C_i = K_i \oplus (Z' \oplus N_i)^{r_i}, f_i = h(ID_i)^{r_i}, and\ CID_i = Z' \oplus h(r_i \oplus T)$. However, the attacker cannot obtain the server's secret key $h(X_s)$ and fails to forge such a message or obtain a user's biometric key. Clearly, our proposed scheme resists insider attacks and user impersonation attacks. □

Theorem 8. *Our proposed scheme can resist DOS attack.*

Proof. This attack means that an attacker changes the password verification information of a user's smart card to other information. As a result, an illegal user cannot complete his login to the server request successfully. In our proposed scheme, a user's smart card checks the legitimacy of a user's biometric key based on hand geometry P_i, user identity ID_i and password PW_i before the password change phase. If we assume that the attacker inserts the user's smart card into the terminated machine, he must guess the values of the user identity and password. These values are not stored directly in the smart card, but they are combined with other values, e.g., $h(ID_i)^{X_s}, h(PW_i||P_i)$, where X_s, P_i are not stored in the smart card. Additionally, an attacker cannot access the features of a user's hand geometry saved on his preferred USB. Therefore, the attacker cannot obtain X_s, P_i, PW_i, ID_i to apply a DOS attack. □

Theorem 9. *Our proposed scheme can resist a replay attack.*

Proof. In our proposed scheme, the user's login request message combines a random number r_i with the time-stamp T to protect a login message from replay attack. However, if an attacker eavesdrops on a user's previous login message, he still cannot apply a replay attack to the next login request since $CID_i = Z' \oplus h(r_i \oplus T)$ combines several values with the time-stamp T. The attacker cannot get these values, and r_i generates one time for each user's login request. □

Theorem 10. *Our proposed scheme can withstand a parallel-session attack.*

Proof. In our work, an attacker cannot impersonate a valid user by constructing a legal login message in another continuous execution from the authentic execution since the server's submitted message $M_i = E_{K_i}(a', T')$ is encrypted by K_i, which is anonymous to the attacker and a' generates one time for each mutual authentication phase. Hence, our proposed scheme can withstand the parallel-session attack. □

Theorem 11. *Our proposed scheme can resist the common attacks when a USB device is lost or stolen.*

Proof. If a user's USB is lost or stolen, an adversary cannot complete the login or authentication phase because he fails to get the smart card, K_i,PW_i, and X_s. In addition, the secret information saved on the user's smart card is as robust as the password. Our scheme requires a USB, and a user's password and smart card to apply to the login phase. First, a user submits his message $M = (C_i, f_i, E_{K_i}(r_i, T, N_i, CID_i))$ to the server. Continuously, the server checks the validity of users and he will send a challenge $(M' = E_{K_i}(a', T'))$ to the user. After that, the authenticated user should retrieve Z', r_i to decrypt M based on K_i. Additionally, he computes $a = h(Z'||r_i||T')$ for comparison with a' to ensure authority of the server. Therefore, the adversary cannot apply malicious attacks when the USB is lost or stolen. □

As a result, we notice that the proposed scheme is more robust and flexible for practical applications such as online payment environments and e-business in protecting user privacy compared with other related schemes. Additionally, we propose a good authentication scheme based on a smart card and feature extraction of a user's hand geometry. The proposed scheme aims to support more functionality to resist well-known attacks and provides several security features such as revocation, user anonymity, known-key security, and mutual authentication. The mechanism of the proposed scheme can be compatible with ubiquitous computing models such as cloud computing. Additionally, a USB provides a biometric factor for multi-factor authentication.

6. Discussion and Comparison with the State-of-the-Art Methods

We compare security properties and computational costs of our proposed scheme with one of six authentication schemes including Xu–Zhu–Feng [3], Das et al. [14], Liao et al. [15], Wang et al. [25], Khan et al. [26], and Yoon and Yoo [27].

Table 3 describes comparison of security properties based on the main security features as follows:

C1 : Freely chosen password;
C2 : User anonymity;
C3 : Secure password change;
C4 : Session key agreement;
C5 : Mutual authentication;
C6 : No password revealed;
C7 : Revocation by using personal biometrics.

Table 3. Comparison of authentication schemes.

Scheme	C1	C2	C3	C4	C5	C6	C7
Our Scheme	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Das et al. [14]	Yes	Yes	No	No	No	No	No
Liao et al. [15]	Yes	Yes	Yes	No	Yes	Yes	No
Wang et al. [25]	No	No	No	No	Yes	No	No
Yoon and Yoo [27]	Yes	Yes	Yes	No	Yes	Yes	No
Khan et al. [26]	Yes	No	Yes	No	Yes	Yes	No
Xu–Zhu–Feng [3]	Yes	No	Yes	Yes	Yes	No	No

The time requirement of our scheme is briefly listed in Table 4. The details of communication costs are viewed in Table 5. We depend on the measurements for computing communication cost in [27]. They supposed that the output size of a crypto one-way hash function equals 128 bits. For comparison, they also supposed that, without wasting generality, the lengths of a user's identity ID_i and password PW_i are 128 bits. Finally, the sizes of the both random numbers and time-stamps equal 64 bits.

In Table 4, a comparison of computational cost is shown, where the following notations are used.

(1) T_h: Time for performing a one-way hash function.
(2) $T_{\oplus}$: Time for performing the XOR operation.
(3) $T_{\Vert}$: Time for performing a concatenation function.
(4) T_{Exp}: Time performing for exponentiation function.
(5) T_{Enc}:Time performing for a symmetric encryption function.
(6) T_{Dec}:Time performing for a symmetric decryption function.

Table 4. Comparison of computational cost.

Scheme	Registration Phase	Login & Authentication Phase	Total Cost
Our Scheme	$5T_h + T_{\Vert} + 2T_{\oplus}$	$10T_h + 5T_{\Vert} + 8T_{\oplus} + 4T_{Exp} + 2T_{Enc} + 2T_{Dec}$	$15T_h + 6T_{\Vert} + 10T_{\oplus} + 4T_{Exp} + 2T_{Enc} + 2T_{Dec}$
Das et al. [14]	$2T_h + T_{\oplus}$	$7T_h + 14T_{\oplus}$	$9T_h + 15T_{\oplus}$
Liao et al. [15]	$2T_h + T_{\oplus} + T_{\Vert}$	$9T_h + 20T_{\oplus}$	$11T_h + 21T_{\oplus} + T_{\Vert}$
Wang et al. [25]	$2T_h + 2T_{\oplus}$	$8T_h + 14T_{\oplus}$	$10T_h + 16T_{\oplus}$
Yoon and Yoo [27]	$3T_h + 2T_{\oplus} + 3T_{\Vert}$	$10T_h + 3T_{\oplus} + 21T_{\Vert}$	$13T_h + 5T_{\oplus} + 24T_{\Vert}$
Khan et al. [26]	$2T_h + T_{\oplus} + 3T_{\Vert}$	$10T_h + 9T_{\oplus} + 8T_{\Vert}$	$12T_h + 10T_{\oplus} + 13T_{\Vert}$
Xu–Zhu–Feng [3]	$2T_h + T_{Exp} + 2T_{Enc}$	$9T_h + 6T_{Exp} + 4T_{Enc} + 18T_{\Vert}$	$11T_h + 7T_{Exp} + 6T_{Enc} + 18T_{\Vert}$

In Table 5, we notice that our proposed scheme has a good performance compared with related works. Although our proposed scheme is based on biometric factors (features of user's hand geometry), the efficiency and flexility remain at a good level.

Table 5. Comparison of communication costs.

Scheme	From User to Server		From Server to User		Total Communication Cost (Numbers of Bits)
	Login Message	**Cost (Bits)**	**Mutual Message**	**Cost (Bits)**	
Our Scheme	C_i, f_i, E_{K_i}	384	M'	192	576
Das et al. [14]	CID_i, N_i, C_i, T	448	-	-	448
Liao et al. [15]	CID_i, N_i, C_i, T	448	D,T''	192	640
Wang et al. [25]	CID_i, N_i, N_i, T	448	a', T''	192	640
Khan et al. [26]	CID_i, C_i, d, T	384	C_2, T_s	192	576
Yoon and Yoo [27]	ID_i, C_i, N_i, T	448	D,T''	192	640

7. Conclusions

In this paper, we review a cryptanalysis of the Xu–Zhu–Feng scheme and present the weaknesses of their scheme. Our proposed scheme has good properties such as freely chosen passwords, user anonymity, mutual authentication, session key agreement, no password revealed, and the features of user's hand geometry provide our work with the ability to prevent an adversary from applying eavesdropping attacks. Furthermore, we have also demonstrated that our proposed scheme is immune against attacks such as password guessing, server impersonation, DOS attacks, replay attacks, and parallel-session attacks. Moreover, compared with related works, our scheme is more secure and practical.

Acknowledgments: This work was partially supported by the National Natural Science Foundation of China (Project No. 41571436) and the South Wisdom Valley Innovative Research Team Program.

Author Contributions: Jian Yao works as a supervisor to work in general by giving guidance and discussions on any update on the paper. Ali A. Yassin has been presented the main idea and responsible to design, analyzed the data, write the paper. Shiyao Han has been worked as co-author by discussion and write some theorems and figures.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Lamport, L. Password Authentication With Insecure Communication. *Commun. ACM* **1981**, *24*, 770–772.
2. Khan, S.H.; Akbar, M.A.; Shahzad, F.; Farooq, M.; Khan, Z. Secure biometric template generation for multi-factor authentication. *Pattern Recognit.* **2015**, *48*, 458–472.
3. Xu, J.; Zhu, W.T.; Feng, D.G. An improved smart card based password authentication scheme with provable security. *Comput. Standards Interfaces* **2009**, *31*, 723–728.
4. Acar, T.; Belenkiy, M.; Kupsu, A. Single password authentication. *Comput. Netw.* **2013**, *57*, 2597–2614.
5. Gao, C.; Chang, C.C.; Sun, C.Y. Chaotic Maps-Based Mutual Authentication and Key Agreement using Smart Cards for Wireless Communications. *J. Inf. Hiding Multimed. Signal Process.* **2013**, *4*, 99–109.
6. Marimuthu, K.; Saravanan, R. A secure remote user mutual authentication scheme using smart cards. *J. Inf. Secur. Appl.* **2014**, *19*, 282–294.
7. Madhusudhan, R.; Mittal, R.C. Dynamic ID-based remote user password authentication schemes using smart cards: A review. *J. Netw. Comput. Appl.* **2012**, *35*, 1235–1248.
8. Xu, L.; Wu, F. An improved and provable remote user authentication scheme based on elliptic curve cryptosystem with user anonymity. *Secur. Commun. Netw.* **2015**, *8*, 245–260.
9. Chuang, M.C.; Chen, M.C. An anonymous multi-server authenticated key agreement scheme based on trust computing using smart cards and biometrics. *Expert Syst. Appl.* **2014**, *41*, 1411–1418.
10. Chien, H.Y.; Jan, J.K.; Tseng, Y.M. An efficient and practical solution to remote authentication: Smart card. *Comput. Secur.* **2002**, *21*, 372–375.

11. Lin, H.Y. Improved chaotic maps-based password-authenticated key agreement using smart cards. *Commun. Nonl. Sci. Numer. Simul.* **2015**, *20*, 482–488.
12. Awasthi, A.K.; Lal, S. An enhanced remote user authentication scheme using smart cards. *IEEE Trans. Consum. Electron.* **2004**, *50*, 583–586.
13. Tang, H.B.; Liu, X.S. Cryptanalysis of a dynamic ID-based remote user authentication with key agreement scheme. *Int. J. Commun. Syst.* **2012**, *25*, 1639–1644.
14. Das, M.L.; Saxena, A.; Gulati, V.P. A dynamic ID-based remote user authentication scheme. *IEEE Trans. Consum. Electron.* **2004**, *50*, 629–631.
15. Liao, I.E.; Lee, C.C.; Hwang, M.S. Security enhancement for a dynamic ID-based remote user authentication scheme. In Proceedings of the 2005 Inernational Conference on Next Generation Web Services Practice, Souel, Korea, 22–26 August 2006; pp. 437–440.
16. Shih, W.; Hsiang, H.C. Improvement of the secure dynamic ID based remote user authentication scheme for multi-server environment. *Comput. Standards Interfaces* **2009**, *31*, 1118–1123.
17. Lee, N.Y.; Chiu, Y.C. Improved remote authentication scheme with smart card. *Comput. Standards Interfaces* **2005**, *27*, 177–180.
18. Lee, S.W.; Kim, H.S.; Yoo, K.Y. Improvement of Chien et al.'s remote user authentication scheme using smart cards. *Comput. Standards Interfaces* **2005**, *27*, 181–183.
19. Wang, D.; Wang, P. On the anonymity of two-factor authentication schemes for wireless sensor networks: Attacks, principle and solutions. *Comput. Netw.* **2014**, *73*, 41–57.
20. Kumar, M. New remote user authentication scheme using smart cards. *Trans. IEEE Trans. Consum. Electron.* **2004**, *50*, 597–600.
21. Li, C.T.; Lee, C.C.; Weng, C.Y. A dynamic identity-based user authentication scheme for remote login systems. *Secur. Commun. Netw.* **2015**, *8*, 3372–3383.
22. Khan, M.K.; Kim , S.K.; Alghathbar, K. Cryptanalysis and security enhancement of a more efficient and secure dynamic ID-based remote user authentication scheme. *Comput. Commun.* **2011**, *34*, 305–309.
23. Otsu, N. A threshold selection method from gray-scale histogram. *IEEE Trans. Syst. Man Cyber. Syst.* **1978**, *9*, 62–66.
24. Luque-Baena, R.M.; Elizondo, D.; Lopez-Rubio, E.; Palomo, E.J.; Watson, T. Assessment of geometric features for individual identification and verification in biometric hand systems. *Expert Syst. Appl.* **2013**, *40*, 3580–3594.
25. Wang, Y.Y.; Liu, J.Y.; Xiao, F.X.; Dan, J. A more efficient and secure dynamic ID-based remote user authentication scheme. *Comput. Commun.* **2009**, *32*, 583–585.
26. Li, X.; Niu, J.; Khan, M.K. An enhanced smart card based remote user password authentication scheme. *J. Netw. Comput. Appl.* **2013**, *36*, 1365–1371.
27. Yoon, E.J.; Yoo, K.Y. Improving the Dynamic ID-Based Remote Mutual Authentication Scheme. In *Meaningful Internet Systems 2006: OTM 2006 Workshops*; Meersman, R., Tari, Z., Herrero, P., Eds.; Springer: Berlin, Germany, 2006; pp. 499–507.
28. Huang, X.; Xiang, Y.; Chonka, A.; Zhou, J.; Deng, R.H. A Generic Framework for Three-Factor Authentication: Preserving Security and Privacy in Distributed Systems. *IEEE Trans. Parall. Distrib. Syst.* **2011**, *22*, 1390–1397.
29. Huang, X.; Xiang, Y.; Bertino, E.; Zhou, J.; Xu, L. Robust Multi-Factor Authentication for Fragile Communications. *IEEE Trans. Depend. Secur. Comput.* **2014**, *11*, 568–581.
30. Wang, D.; He, D.; Wang, P.; Chu, C.H. Anonymous two-factor authentication in distributed systems: Certain goals are beyond attainment. *IEEE Trans. Depend. Secur. Comput.* **2015**, *12*, 428–442.
31. Wang, D.; Wang, P. On the usability of two-factor authentication. In Proceedings of the Secure Comm 2014, Beijing, China, 9–11 December 2015; pp. 1–9.
32. Wang, D.; Wang, P.; Liu, J. Improved privacy-preserving authentication scheme for roaming service in mobile networks. In Proceedings of 15th IEEE Wireless Communications and Networking Conference (WCNC'2014), Istanbul, Turkey, 6–9 April 2014; pp. 3178–3183.
33. Ma, C.G.; Wang, D.; Zhao, S.-D. Security flaws in two improved remote user authentication schemes using smart cards. *Int. J. Commun. Syst.* **2014**, *27*, 2215–2227.
34. Wang, D.; Ma, C.-G.; Zhang, Q.-M.; Zhao, S.-D. Secure password-based remote user authentication scheme against smart card security breach. *J. Netw.* **2013**, *8*, 148–155.

35. Wang, D.; Ma, C.-G.; Wang, Y.H. On the security of an improved password authentication scheme based on ECC. In Proceedings of the Third International Conference (ICICA'2012), Chengde, China, 14–16 September 2012; pp. 181–188.
36. Hafizul, S.K. Design and analysis of an improved smartcard based remote user password authentication scheme. *Int. J. Commun. Syst.* **2014**, doi:10.1002/dac.2793.
37. Li, C.-T. A new password authentication and user anonymity scheme based on elliptic curve cryptography and smart card. *IET Inf. Sec.* **2013**, *7*, 3–10.
38. Tsai, J.-L.; Lo, N.-W.; Wu, T.-C. Novel anonymous authentication scheme using smart cards. *IEEE Trans. Ind. Inf.* **2013**, *9*, 2004–2013.
39. Wang , D.; Wan, N.; Wang, P.; Qing, S. Preserving privacy for free: Efficient and provably secure two-factor authentication scheme with user anonymity. *Inf. Sci.* **2015**, *321*, 162–178.
40. Kim, T.-H.; Kim, C.-K.; Park, H. Side channel analysis attacks using AM demodulation on commercial smart cards with SEED. *J. Syst. Softw.* **2012**, *85*, 2899–2908.
41. Liu, J.; Yu, Y.; Standaert, F.-X.; Guo, Z.; Gu, D.; Sun, W.; Ge, Y.; Xie, X. Small Tweaks Do Not Help: Differential Power Analysis of MILENAGE Implementations in 3G/4G USIM Cards. In Proceedings of the 20th European Symposium on Research in Computer Security (ESORICS'2015), Vienna, Austria, 23–25 September 2015; pp. 1–20.