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

# Enhanced Graphical Captcha Framework and Applications to Strong Security Authenticated Scheme without Password Table

Hong-Feng Zhu, Yan Zhang and Yu Xia

Software College, Shenyang Normal University
No.253, HuangHe Bei Street, HuangGu District, Shenyang, P.C 110034 - China
zhuhongfeng1978@163.com; 1505733680@qq.com; 876526606@qq.com

Received June, 2015; revised July, 2015

Abstract. *Captcha technology as a new security primitive, aiming to provide mutual authentication for legal users availability and distinguish computer and human apart using the Turing test, which still has many hot spots to explore. Based on hard AI problems, Captcha evolves into graphical Captcha which is more suitable for touch-screen devices. However, to the best of our knowledge, almost all the legal servers must store a password table to authenticate legal users with a temporary Captcha by challenge-response process. So, the password table can lead to some defects, for example, centralized security and maintained fee of the password table. For the worst case, if the password table was stolen, an adversary can launch impersonation attack or denial of service attack. Based on these motivations, the paper firstly designs a general framework about no password tables scheme using Captcha. Then, we give an example which is a new strong security authenticated scheme based on graphical Captcha and chaotic maps without password table. On the one side, for risk diversification, the key idea of our proposed scheme is to convert centralized password table into many proofs and shift these proofs to each client, so each client only stores his own proof to be responsible for himself. On the other side, in order to protect the proof with password, using hard AI problems, our protocol can resist all kinds of automatic validation attacks, for example, lost smart device and carry out dictionary attack. Compared with the related literatures recently, our proposed scheme can not only own high efficiency and unique functionality, such as privacy protection, but is also robust to various attacks and achieves perfect forward secrecy. Finally, we give the security proof and the efficiency analysis of our proposed scheme.*
**Keywords:** Artificial Intelligence, Captcha, Mutual authentication, Chaotic maps

1. **Introduction.** Captcha-based cryptography is one of the most fundamental and variational cryptographic primitive. Captcha-based systems allow security functionalities to be provided on the basis of AI (Artificial Intellegence) problems which is immune to computer automatic validation attacks naturally. The importance of Captcha technology is that it can accomplish high efficiency and high security simply rather than trade off among complicated design, redundant algorithm and user experience.

Nowadays, more and more recearchers concern on Captcha-based cryptography to construct security protocols or kinds of applications. Captcha is a program algorithm to distinguish between computers and human [6]. The algorithm generates and evaluates the test that easily by human but not the computers, such as identifying distorted figures, describing burry images. In 2003, Luis et al. [1] first proposed the exciting new paradigm of using hard AI problems to ensure the security of communication. It is due to

this groundbreaking work, Captcha has drawn the attention of the public. Nevertheless, compared with the hard mathematical problems, no matter the application or cognition, this representative article based on AI problems has made a limit hit [2]. For further perfect, Zhu [3] introduced a new security primitive based on hard AI problems, which called CaRP (Captcha as graphical password [4]) to resist online guessing attacks, relay attacks and so on. So, Captcha is broadly divided into the following two forms: (1) text-based Captcha [7]: mainly focus on identify a range of random numbers or characters. (2) image-based Captcha [8]: recognize the real object and describe it briefly. Based on the above two kinds of traditional forms, several researchers have proposed FaceCaptcha [9] that require users identify the gender of image. Meanwhile, a Captcha based on the orientation of cropped sub-images has presented by Kim et al. [10]. In 2015, Aziz [11] proposed a character image semantic-based Captcha. However, all of these methods are simply meeting predetermined proportions that can not entirely validated users by Captcha. So far, we can clearly see that these traditional methods are to facilitate people to use on the computers, which has suitable screen, proper keyboard and mouse, rather than on the touch-screen mobile phone or tablet. In addition, some enhanced Captcha technology [12-15] only increases the distortion and fuzzy of the characters, causing users identification are becoming more difficult, yet insoluble the basic issues. Therefore, based on these motivations, constructing an optimal Captcha technology becomes more important. Graphical Captcha [16] is a comprehensive application of Captcha, which based on touch-screen to convert each ordinary Captcha into Graphical Captcha for every login, namely, users only need to click on the corresponding pictures that transmitted by the servers.

So what are the benefits and advantages of Graphical Captcha? (1) With the purpose of preventing users from executing automatic registration by robots, and due to the difficulty of computer recognition, many sites take numbers, letters and other interference pixels together to form a Captcha. However, spam [20] still remains, for example, in the e-banking and tieba. If using the Graphical method, the computer is bound to carry through more cumbersome calculations, which will lessen the spam traffic. (2) Since the popularity of touch-screen and online payment. Some Captchas require user to view the message first and then enter the numbers, it is so complicate to users login each time. Graphical avoid this situation that merely need users according to the prompt to click on the screen directly. Moreover, it does not require a huge number of the grounding in languages and common senses. (3) Now the online ticketing system [21] of railway has put the Graphical Captcha into practice, aiming at better curb the cattle grab votes. No matter the user login account or submit ticket orders, all should play a little game, only click on the corresponding to the text images can smoothly complete the operation.

But there exists an obvious loophole that each legitimate server requires to store a password table for authentication. Once the password table has stolen, an attacker will easy to obtain a registered users information and masquerade as a legitimate user to communicate with the server. Moreover, since users identity in clear text transmission over insure channel, the attacker will catch it lightly. Today, a number of Captchas authenticated schemes are based on password table [3, 17]. As we all know, password table is a root directory stored in the server, which contains every registered users password and other secret information. Once disclosed to the third party, both users and servers will suffer huge losses. In recent years, the password table has stolen repeatedly. In 2011, six million valid users information was leaked on CSDN website [18]. The reason is that these users registered mailbox and set passwords in plaintext form, so the attacker will got userID and users will suffer the password guessing inevitably. Meanwhile, Google [19] is also subjected to the similar crisis in 2014, hacker attacks their database, nearly

five million Gmail users account and passwords were missed. There is no doubt that it caused by security vulnerabilities equally. Therefore, in order to prevent the recurrence of such attacks, our Graphical Captcha scheme using public-key encryption and hash algorithm with no password table in severs to achieve authentication. In addition, users are maintaining anonymous in the entire communication.

In this paper, from the above analysis, we firstly proposed a new strong security authenticated scheme based on Graphical Captcha without password tables with privacy protection, aiming at both providing convenience for the user login and staying clear of password guessing attack. Considering the Chaotic system [5] has numerous advantages, such as extremely sensitive to initial parameters, unpredictability, boundedness, etc. Therefore, our scheme are based on hard AI problems and chaotic maps to achieve mutual authentication.

The rest of the paper is organized as follows: Some preliminaries are given in Section 2. Next, a new framework of Graphical Captcha authentication is described in Section 3. In Section 4, we give an instance of enhanced CaRP authentication scheme. The Security of our proposed protocol is given in Section 5. The efficiency analysis of our proposed protocol is given in Section 6. This paper is finally concluded in Section 7.

2. **Definition and hard problems of Chebyshev chaotic maps.** Let $n$ be an integer and let $x$ be a variable with the interval $[-1, 1]$. The Chebyshev polynomial [22-25] $T_n(x) : [-1, 1] \to [-1, 1]$ 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:
$T_n(x) = 2xT_{n-1}(x) - T_{n-2}(x)$, where $n \geq 2$,$T_0(x) = 1$, 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 $T_r(T_s(x)) = T_{rs}(x)$.

In order to enhance the security, Zhang [23] proved that semi-group property holds for Chebyshev polynomials defined on interval (-,+). The enhanced Chebyshev polynomials are used in the proposed protocol: $T_n(x) = (2xT_{n-1}(x) - T_{n-2}(x))(\mathrm{mod} N)$,
where $n \geq 2$,$x \in (-\infty, +\infty)$,and $N$ is a large prime number. Obviously,
$T_{rs}(x) = T_r(T_s(x)) = T_s(T_r(x))$.

**Definition 2.1.** *(Semi-group property) Semi-group property of Chebyshev polynomials:* $T_{rs}(x) = T_r(T_s(x)) = \cos(r\cos^{-1}(s\cos^{-1}(x))) = \cos(rs\cos^{-1}(x)) = T_s(T_r(x)) = T_{sr}(x)$, *where r and s are positive ingeger and* $x \in [-1, 1]$.

**Definition 2.2.** *(Chaotic Maps-Based Discrete Logarithm (CDL) problem)*
*Given x and y, it is intractable to find the integer s, such that* $T_s(x) = y$.*The probability that a polynomial time-bounded algorithm* $\delta$ *can solve the CDL problem is defined as* $Adv_\delta^{CDL}(p) = \Pr[\delta(x, y) = r : r \in Z_p^*, y = T_r(x) \bmod p]$.

**Definition 2.3.** *(CDL assumption) For any probabilistic polynomial time-bounded algorithm* $\delta$,$Adv_\delta^{CDL}(p)$ *is negligible, that is,* $Adv_\delta^{CDL}(p) \leq \varepsilon$,*for some negligible function* $\varepsilon$.

**Definition 2.4.** *(Chaotic Maps-Based Diffie-Hellman (CDH) problem)*
*Given* $x$,$T_r(x)$,*and* $T_s(x)$, *it is intractable to find* $T_{rs}(x)$.*The probability that a polynomial time-bounded algorithm* $\delta$ *can solve the CDH problem is defined as* $Adv_\delta^{CDH}(p) = \Pr[\delta(x, T_r(x) \bmod p, T_s(x) \bmod p) = T_{rs}(x) \bmod p : r, s \in Z_p^*]$.

**Definition 2.5.** *(CDH assumption) For any probabilistic polynomial time-bounded algorithm* $\delta$,$Adv_\delta^{CDH}(p)$ *is negligible, that is,*$Adv_\delta^{CDH}(p) \leq \varepsilon$,*for some negligible function* $\varepsilon$.

3. **Framework of Graphical Captcha Authentication.** Authentication is an interactive process between a user and an authentication server. According to the taxonomy in [38], authentication methods can be divided in three categories (see Fig.1): (1)

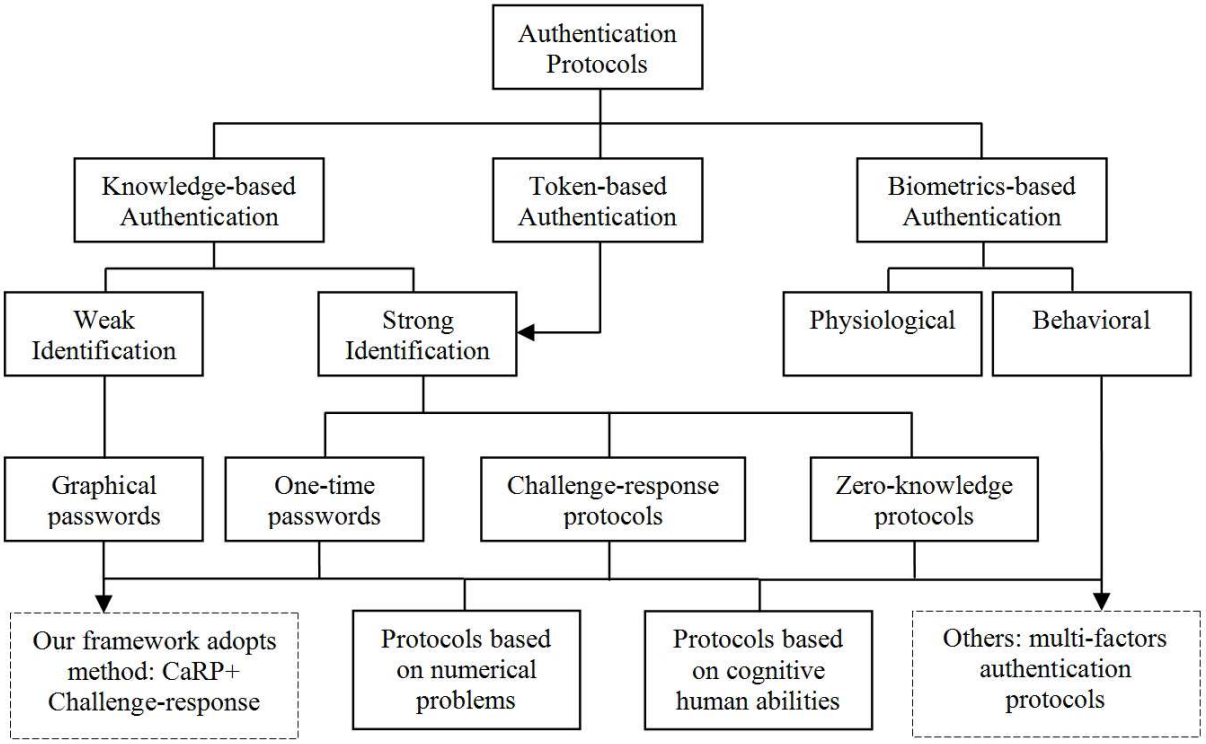


FIGURE 1. Jameels taxonomy of identification methods

Knowledge-based authentication: Systems based on the knowledge of a secret, e.g. passwords or PIN/TAN.

(2) Token- or possession-based authentication: Systems based on the possession of a token (a physical or electronic unique authentication resource). This could for example be a cryptographic key or certificate, a smart card, a number sequence generator.

(3) Biometric authentication: The use of unique personal, physical traits as input for authentication. Our new framework of Graphical Captcha authentication will adopt CaRP and Challenge-response to design. But firstly, we give the traditional framework about CaRP authentication scheme(see Fig.2):

The authentication server stores a salt s and a hash value $H(pw, s)$ for each user ID, where $pw$ is the password of the account and not stored. A CaRP password is a sequence of visual object IDs or clickable-points of visual objects that the user selects. Upon receiving a login request, the server generates a CaRP image, records the locations of the objects in the image, and sends the image to the user to click her password. The coordinates of the clicked points are recorded and sent to the server along with the user ID. The server maps the received coordinates onto the CaRP image, and recovers a sequence of visual object IDs or clickable points of visual objects, $pw^{\sim}$,which the user clicked on the image. Then the server retrieves salt s of the account, calculates the hash value of $pw^{\sim}$ with the salt, and compares the result with the hash value stored for the account. Authentication succeeds only if the two hash values match.

From the Fig.2, we can see that the traditional CaRP authentication has three main defects:

(1) In traditional CaRP authentication scheme due to password table (or called verification table), so the stolen/modified/deleted verifier attack will be a big issue.

(2) The userID is transmitted over the public channel in traditional CaRP authentication scheme which can lead to some potential attacks, such as the adversary can collect login history of user as least.

(3) Only the server authenticates the user (called server-to-user authentication), but there is no any countermeasure for the user to authenticate the server (called user-to-server authentication) which can lead any adversary to initiate impersonation attack.

Considering the above problems, we give a new framework (see Fig.3) about CaRP authentication with privacy protection, mutual authentication and without password table in the server side.

In general, authentication requirements can be specified as part of the code through so-called assumptions and assertions[27]. They can be thought of as a generalization of non-injective correspondence assertions [28] traditionally employed for modeling authenticity. An assumption introduces a new hypothesis, and an assertion is a formula that must be derived from the hypotheses made. In our framework, the assumptions are the key pair of the authentication server and the proof of the user, and the assertions are the process of the protocol and the local computations. This new framework has two phases: the registration phase and the authentication phase.

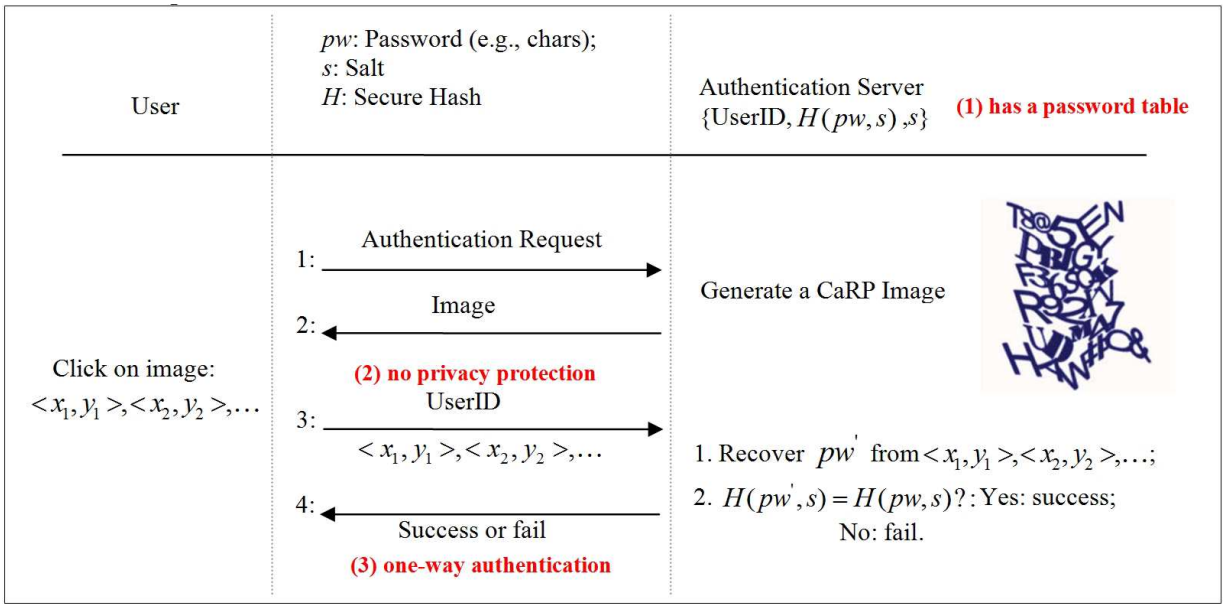


FIGURE 2. Traditional Flowchart of basic CaRP authentication

(1) In the registration phase, aiming to achieve risk diversification, we shift the password table of the server to the clients. So, the authentication server must has the long key pair (public key/secret key) and use its own secret key to generate a proof which will help the user to prove himself in the furture. At the same time, the authentication server eliminates password table and will use the secret key to generate temporary proof to authenticate the users proof.

**Remark 3.1.** *the proof is related some information: the secret key of the server, the memorable password or biometric.*

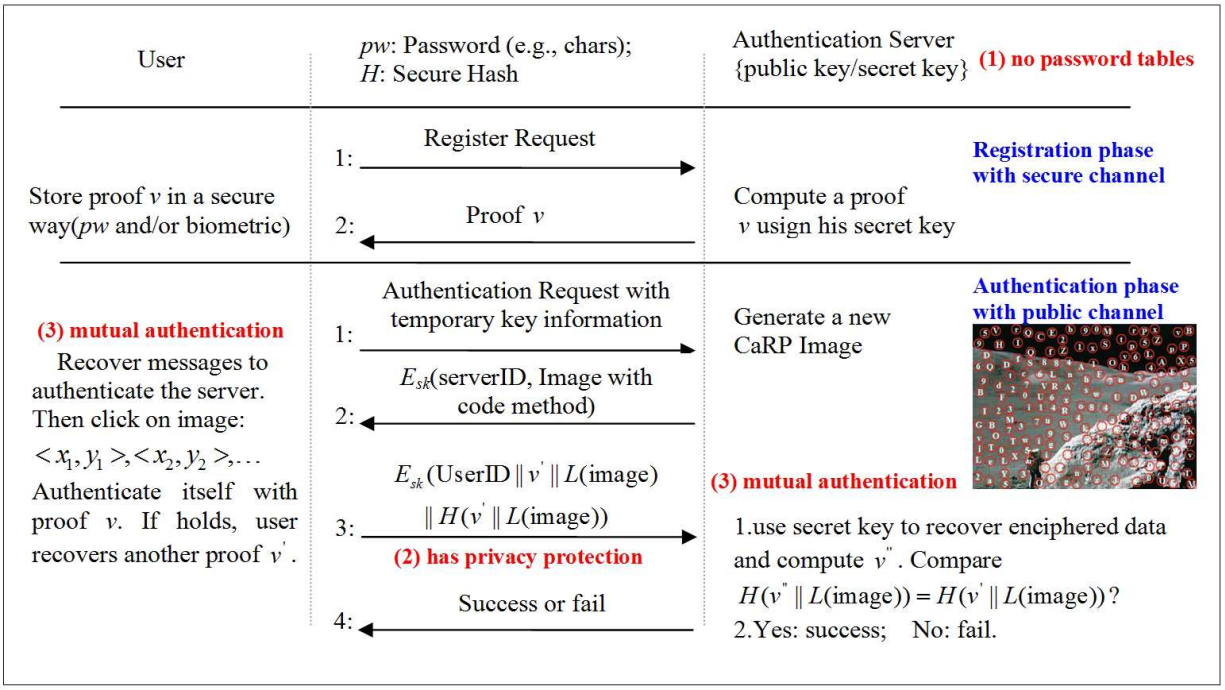


FIGURE 3. Flowchart of enhanced CaRP authentication

(2) In the authentication phase, we take full advantage of the proofs (secret key of the server, the proof of the user) to achieve privacy protection and mutual authentication. Due to the authentication server stores nothing for any user, if any user wants to login the server and s/he must firstly send an authentication request with some temporary key information (the information can generate session key only between the user and the server) to the server. Then, the server will generate a new CaRP Image and send this Image with code method to the user, and the information is encrypted by session key. The code method means that a new algorithm to record the locations between the objects in the image and the numbers or characters, so the user can click on image to retrieve the password for authenticating himself locally based on the proof v using hard AI problems. If the user can decrypt the encrypted information, we can deem that the user authenticates the server because the session key can be computed by the secret key of the server. After authenticating himself, the user will recover another proof $v^{\sim}$ for passing the servers validation. Next, based on public key of the server, the user can construct a temporary session key to encrypt userID, some necessary information and send them to the server. Finally, the server uses the secret key to recover enciphered data and compute $v^{\approx}$. Then the server calculates the hash value $H(v^{\approx}||L(\text{image}))$ , and compares the result with the recovered hash value $H(v^{\sim}||L(\text{image}))$. Authentication succeeds only if the two hash values match.

**Remark 3.2.** *L is an algorithm to transfer an image into fixed output bits (such as 128bits). The CaRP Image can be classified as numbers, characters and special characters in order to find quickly for humans.*

4. **An Instance of Enhanced CaRP Authentication Scheme.** In this section, we choose password as an instance to achieve our framework which has described in Section 3. The new chaotic maps-based and enhanced CaRP authentication scheme is made up of three phases: registration phase, authentication phase and password update phase.

4.1. **Notations.** The concrete notations used hereafter are shown in Table1.

TABLE 1. Notations

| Symbol | Definition |
|---|---|
| $ID_A$ | the identity of Alice |
| $ID_S$ | the identity of the server |
| $B,a$ | nonces |
| $(x,T_K(x))$ | public key of server based on Chebyshev chaotic maps |
| $K$ | secret key of server based on Chebyshev chaotic maps |
| $E_K()/D_K()$ | a pair of secure symmetric encryption/decryption functions with the key $K$ |
| $H$ | A secure one-way hash function |
| $\|$ | concatenation operation |
| $L$ | An algorithm to transfer an image into fixed output bits (such as 128bits) |

4.2. **Registration phase.** Fig.4 illustrates the user registration phase.

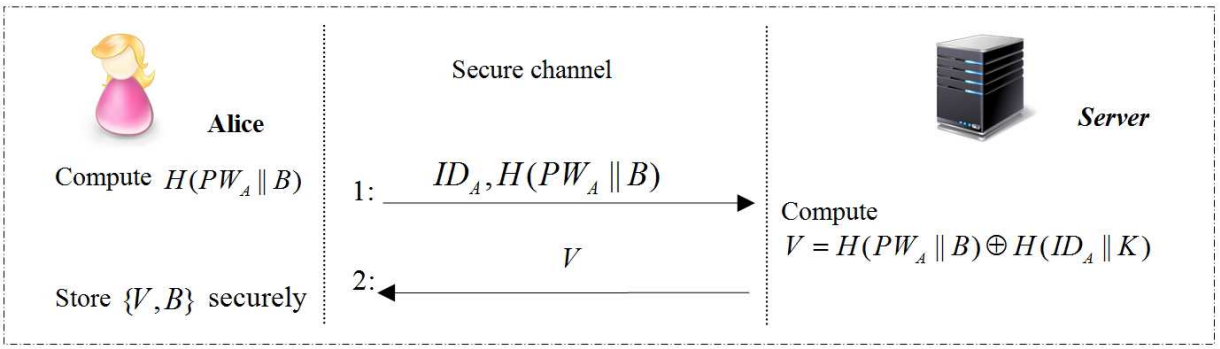


FIGURE 4. Registration phase

**Step 1.**When a user Alice wants to be a new legal user, she chooses her identity $ID_A$,password $PW_A$ and a random number B. Then Alice computes $H(PW_A||B)$ and sends $\{ID_A, H(PW_A||B)\}$ to the server via a secure channel.

**Step 2.**Upon receiving $\{ID_A, H(PW_A||B)\}$ from the Alice, the server computes $V = H(PW_A||B) \oplus H(ID_A||K)$ and sends V to the Alice.

**Step 3.**Alice stores $\{V, B\}$ securely. Storage carrier may be smart card, applications database or others.

4.3. **Authentication phase.** This concrete process is presented in the following Fig. 5.

**Step 1.**If Alice wishes to login in the service server, she firstly selects a large and random integer a and computes $T_a(x)$. Then Alice sends an authentication request with $T_a(x)$ to the server.

**Step 2.**After receiving the request message from Alice, the server will generate a new CaRP image and send the image with code method. Using his own secret key $K$ to compute $T_K T_a(x)$, the server computes $C_1 = E_{T_K T_a(x)}(ID_S||\text{Imagewithcodemethod})$ and sends $C_1$ to Alice.

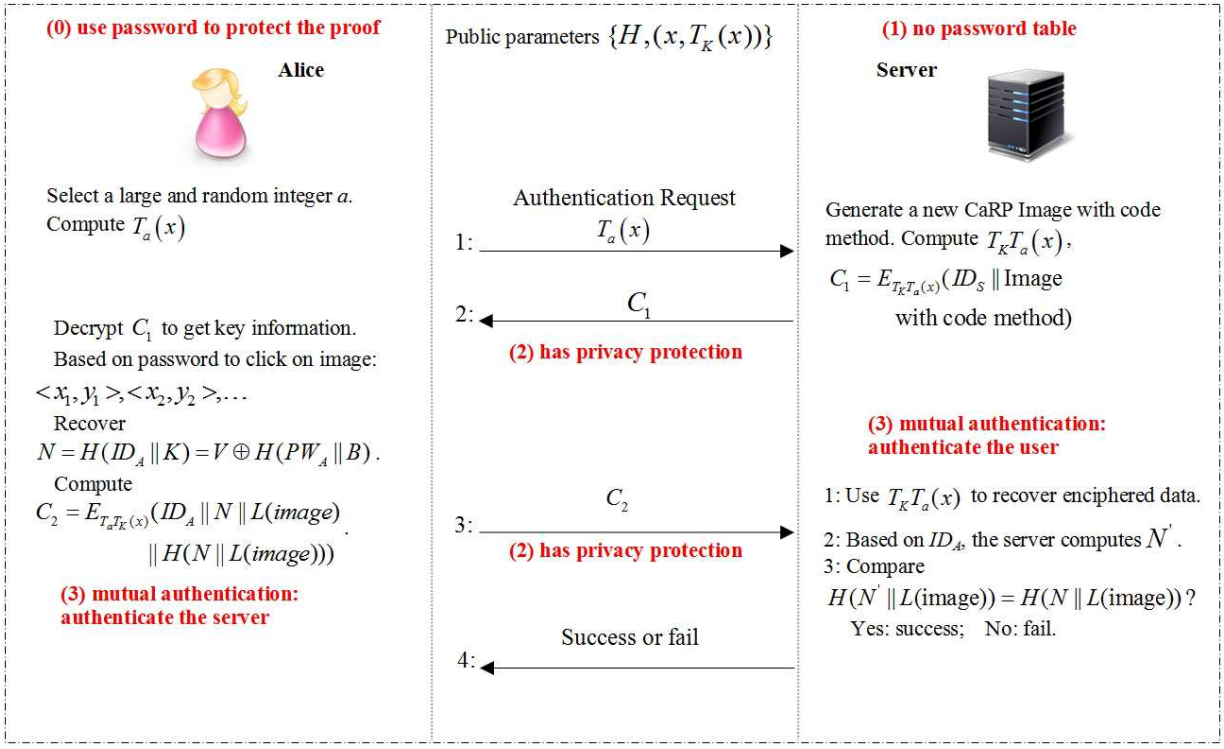


FIGURE 5. Authentication phase

**Step 3.**After receiving the Image with code method from the server, Alice will do the following tasks:

(1) Using the temporary and secret key a to compute $T_a T_K(x)$, Alice can decrypt $C_1$ to get the $ID_S$ and a new image with code method. If Alice achieves to get the $ID_S$ from the encrypted data, which means Alice authenticates the server.

(2) Using her own memorable password, Alice clicks the image:$< x_1, y_1 >, < x_2, y_2 >, \ldots$.

(3) Based on the code method from the server, Alices application can recover the password from the $< x_1, y_1 >, < x_2, y_2 >, \ldots$.

(4)Alice computes $N = H(ID_A||K) = V \oplus H(PW_A||B)$,
$C_2 = E_{T_a T_K(x)}(ID_A||N||L(image)||H(N||L(image)))$,and sends $\{C_2\}$ to the server.

**Step 4.**After receiving the message $\{C_2\}$ from Alice, the server will use $T_K T_a(x)$ to recover enciphered data for getting $ID_A||N||L(image)||H(N||L(image))$.Based on $ID_A$, the server computes $N^{\sim} = H(ID_A||K)$. Finally the server compares whether $H(N^{\sim}||L(\text{image}))$ equals to $H(N||L(\text{image}))$. If holds, the authentication will success. Otherwise, the authentication will fail.

If any authenticated process does not pass, the protocol will be terminated immediately.

4.4. **Password update phase.** This process is presented in the following Fig. 6.

**Step 1.**If Alice wishes to update her password with ServerA, Alice will choose a new memorable password $PW_A^{\sim}$ and a random number $B^{\sim}$ . Then the device of Alice will select a large and random integer a and compute $T_a(x)$, $N = H(ID_A||K) = H(PW_A||B) \oplus V$ and $C_1 = E_{T_a T_{K_A}(x)}(ID_A||H(PW_A^{\sim}|||B^{\sim})||H(N||H(PW_A^{\sim}|||B^{\sim})))$.After that, Alice sends $\{C_1, T_a(x)\}$ to the server where she registers on.

**Step 2.**After receiving the message $\{C_1, T_a(x)\}$ from Alice, the server will do the following tasks:

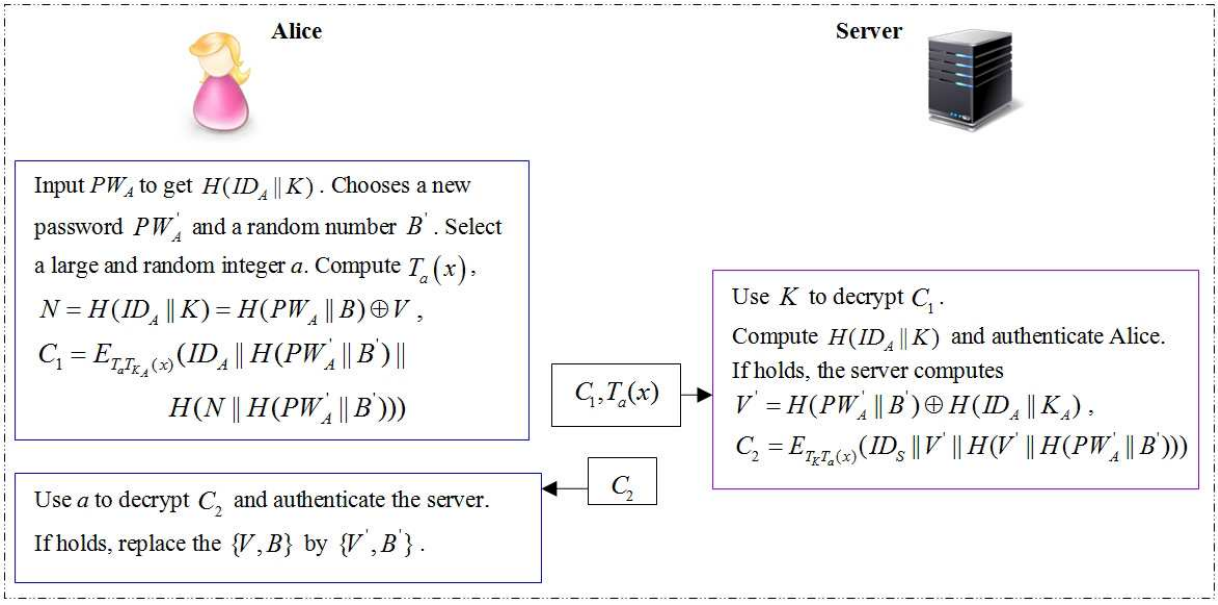


FIGURE 6. Password update phase

(1) The server uses $K$ to decrypt $C_1$ for getting the messages $ID_A||H(PW_A^{\sim}|||B^{\sim})||H(N||H(PW_A^{\sim}|||B^{\sim}))$.

(2) Based on $ID_A$, the server computes $N^{\sim} = H(ID_A||K)$,and $H^{\sim}(N^{\sim}||H(PW_A^{\sim}|||B^{\sim}))$.

(3) Finally the server compares whether $H^{\sim}(N^{\sim}||H(PW_A^{\sim}|||B^{\sim}))$ equals to $H(N||H(PW_A^{\sim}|||B^{\sim}))$.If holds, the authentication will success. Otherwise, the authentication will fail.

(4) If holds, the server computes $V^{\sim} = H(PW_A^{\sim}||B^{\sim}) \oplus H(ID_A||K_A)$, $C_2 = E_{T_K T_a(x)}(ID_S||V^{\sim}||H(V^{\sim}||H(PW_A^{\sim}|||B^{\sim})))$ and sends $C_2$ to Alice.

**Step 3.**After receiving the message $C_2$ from the server, Alice will uses a to decrypt $C_2$ for getting $ID_S||V^{\sim}||H(V^{\sim}||H(PW_A^{\sim}||B^{\sim}))$. Then Alices device will compute $H^{\sim}(V^{\sim}||H(PW_A^{\sim}||B^{\sim}))$ to verify $H(V^{\sim}||H(PW_A^{\sim}||B^{\sim}))$. If holds, Alice replaces the $\{V, B\}$ by $\{V^{\sim}, B^{\sim}\}$.

If any authenticated process does not pass, the protocol will be terminated immediately.

## 5. Security Consideration.

5.1. **Local authentication: AI problems security analysis.** Captcha relies on the gap of capabilities between humans and bots in solving certain hard AI problems. Image-Recognition Captcha (IRC) relies on recognition of non-character objects. Security of IRCs was found to be susceptible to machine-learning attacks [30]. IRCs based on binary object classification or identification of one concrete type of objects is likely insecure [31]. Multi-label classification problems are considered much harder than binary classification problems. A CaRP image typically contains 30 or more characters, and in our proposed protocol a CaRP image contains all the numbers and characters because the server has no idea about the password of the user. For improving user experience, a CaRP Image can be classified as numbers, characters and special characters in different realm of the image. Because there is no theoretic security model has been established, we just estimate the complexity of object segmentation. According to [32], we set C is exponentially dependent of the number M of objects contained in a challenge, and polynomially dependent of the size N of the Captcha alphabet:$C = a^M P(N)$, where $a > 1$ is a parameter, and $P()$ is a polynomial function. A Captcha challenge typically contains 6 to 10 characters, whereas a CaRP image contains 68 or more characters in our proposed protocol. The complexity to break a Click-Text image is about:$a^{68}P(N)/(a^{10}P(N)) = a^{58}$ times the complexity to

break a Captcha challenge generated by its underlying Captcha scheme. This is a huge space which is secure enough.

5.2. **Protocol interaction: Authentication proof based on the BAN logic [29].** First of all, based on hard AI problems (see Section 5.1), we can assume that the user can recover the authentication proof $N = H(ID_A||K) = V \oplus H(PW_A||B)$ securely. For convenience, we first give the description of some notations (Table 2) used in the BAN logic analysis and define some main logical postulates (Table 3) of BAN logic.

TABLE 2. 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 with the key $K$. |
| $P \overset{K}{\longleftrightarrow} Q$ | 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 $Q$. |
| $SK$ | The session key used in the current session. |

TABLE 3. 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. | | |

According to analytic procedures of BAN logic and the requirement of authentication protocol, our protocol should satisfy the following goals in Table 4:

First of all, we transform the process of our protocol to the following idealized form. $(Alice \rightarrow S)m_1 : S \lhd T_a(x)$ with authentication request;

TABLE 4. Goals of the proposed scheme

| Goals |
|---|
| Goal 1. $Alice \mid\equiv \left(Alice \xleftrightarrow{N} S\right)$; Goal 2. $Alice \mid\equiv S \mid\equiv \left(Alice \xleftrightarrow{N} S\right)$; |
| Goal 3. $S \mid\equiv \left(Alice \xleftrightarrow{N} S\right)$; Goal 4. $S \mid\equiv Alice \mid\equiv \left(Alice \xleftrightarrow{N} S\right)$; |
| **Where *S* means the authentication server, *N* means the recovered or computable proof:** $H(ID_A \| K)$ |

$(S \rightarrow \text{Alice})m_2 : \text{Alice} \triangleleft C_1, \{ID_S, \text{imagewithcodemethod}\}_{Alice \leftrightarrow S(T_K T_{a(x)})}$;
$(\text{Alice} \rightarrow S)m_3 : S \triangleleft C_2, \{ID_A, N, L(image), (H(N||L(image))\}_{S \leftrightarrow Alice(T_a T_{K(x)})}$.

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 5.

TABLE 5. Assumptions about the initial state of our protocol

| Initial states | |
|---|---|
| $P_1 : Alice \mid\equiv \xrightarrow{T_K(x)} S$ | $P_2 : Alice \mid\equiv \#(a)$ |
| $P_3 : S \mid\equiv \#(\text{Image with code method})$ | $P_4 : Alice \mid\equiv Alice \xleftrightarrow{T_a T_K(x)} S$ |
| $P_5 : S \mid\equiv Alice \xleftrightarrow{T_K T_a(x)} S$ | |

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 m2:

Because m1 is just a simple and temporary ciphertext, we view m2 is the beginning of the proof. According to the message m2 and $P_1, P_4$ and attributes of chaotic maps, and relating with $R_1$, we could get: $S_1 : S|\equiv Alice|\sim m_2$

Based on the initial assumptions $P_2, P_3$, and relating with $R_2$, we could get:
$S_2 : Alice| \equiv \#m_2$

Combine $S_1, S_2, P_4, P_5$ and $R_3$, we could get:
$S_3 : S| \equiv Alice| \equiv \#ID_S$,Image with code method

Based on $R_5$, we take apart $S_3$ and get:
$S_4 : S| \equiv Alice| \equiv \#$Image with code method

Next, Alice will use her password to click the new image to recover the proof $N = H(ID_A||K)$.
For m3:

Based on m3, and relating with $P_1, P_2$ and $R_1$, and relating with attributes of chaotic maps, we could deduce: $S_5 : Alice|\equiv S|\sim m_3$

Based on $R_2$ and $P_2, P_3$, we could get: $S_6 : S| \equiv \#m_3$

Based on $R_4, R_5, P_4, P_5$, we take apart $S_6$ and get:
$S_7 : S| \equiv Alice| \equiv \#$image with code method,$S_8 : S| \equiv (Alice \leftrightarrow S)(\text{N})$,
$S_9 : S| \equiv Alice| \equiv S \leftrightarrow Alice(\text{N})$
Combine:

Because the two-party $Alice, S$ communicate each other just now, they confirm the other is on-line. Moreover, since the user can get $ID_S$ from the $C_1$,
$H(N^{\sim}||L(\text{image})) = H(N||L(\text{image}))$ and based on $S_8, S_9, P_1, P_4, P_5$ with chaotic maps problems, we could get:

Goal 1.$Alice| \equiv (Alice \leftrightarrow S)$(N); Goal 2.$Alice| \equiv S| \equiv (Alice \leftrightarrow S)$(N);
Goal 3.$S| \equiv (Alice \leftrightarrow S)$(N); Goal 4.$S| \equiv Alice| \equiv (Alice \leftrightarrow S)$(N)

According to (Goal 1 Goal 4), we know that both Alice and $S_i$ achieve the mutual authentication based on the fresh nonces a and the new image with code method.

5.3. **Protocol interaction: Security analysis for security requirements.** Next, from the Table 6, we can see that the proposed scheme can provide known secure session key agreement, perfect forward secrecy and so on.

TABLE 6. Definition and simplified proof

| Attack Type | Security Requirements | Definition | Simplified Proof | Hard 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. | AI problems |
| | Losting smart device and guessing attacks | An adversary gets the user's smart device and then carries out the guessing attacks. | Human input obtained by performing a Captcha task on a CaRP image is useless for testing a password guess. | AI problems |
| | 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 | AI 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. | Every important message includes the $ID$ and some nonces. | 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. | Every important message includes the $ID$ and some nonces. | Chaotic maps problems |
| | Relay attack | In a classic relay attack, communication with both parties is initiated by the attacker who then merely relays messages between the two parties without manipulating them or even necessarily reading them. | If humans are hired to solve Captcha challenges for small payments, the lowest retail \$1 and the whole 1000 Captcha challenges will cost \$33600. | AI problems |
| No freshness verify attacks | 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. | Chaotic maps problems |
| | 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 |
| 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 the servers. | Chaotic maps problems |

## 6. Efficiency Analysis.

6.1. **The comparisons among different algorithms.** Compared to RSA and ECC , Chebyshev polynomial computation problem offers smaller key sizes, faster computation, as well as memory, energy and bandwidth savings. Chaotic maps encryption algorithm: As a special form of motion, Chaos means that in a certain nonlinear system can appear similar to the behavior of random phenomena without needing any random factors.

Chaotic system has the characteristics of certainty, boundedness, sensibility to initial parameters and unpredictability, etc. Chaotic maps encryption algorithm utilizes the unique semi-group mature of Chebyshev chaotic maps, based on two difficult problems-the chaotic maps discrete logarithm problem and the chaotic maps Diffie-Hellman problem, puts forward a kind of encryption algorithm. Compared with ECC encryption algorithm, Chaotic maps encryption algorithm avoids scalar multiplication and modular exponentiation computation, effectively improves the efficiency. However, Wang [22] proposed several methods to solve the Chebyshev polynomial computation problem. For convenience, some notations are defined as follows.

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 [26]. Moreover, the computational cost of XOR operation could be ignored when compared with other operations. Table 7 given the comparison for RSA, ECC and Chaotic maps.

Table 7. Comparison for RSA, ECC and Chaotic maps

| | **RSA encryption algorithm** | **ECC encryption algorithm** | **Chaotic maps encryption algorithm** |
|---|---|---|---|
| ***Items*** | ***Differences*** | | |
| Mathematical basis | Large prime number | Elliptic curve | Chebyshev polynomial |
| Difficult problem assumptions | large prime factorization problem | Discrete logarithm calculation problem on the elliptic curve | Chaotic maps discrete logarithm problem, Chaotic maps Diffie-Hellman problem |
| Operation Cost | √ √ | √ √ √ | √ √ √ |
| Operation Speed | √ | √ √ | √ √ √ |
| Security Level | √ | √ √ √ | √ √ √ |
| Normal √ | Good √ √ | Excellent √ √ √ | |

6.2. **Efficiency of CaRP.** In this section, we make a comparison between the CaRP and other Captchas to judge its function and competence. The standard for evaluation is easy to use, able to remember, scope of application and safety loopholes. We called up 50(30males and 20 females) from different positions of young people aged between 25 and 30, who living in more contact to network, testing them use the different Captchas respectively. According to this experiment, we conduct a comparison among Kim et al.s scheme [33], Olalere et al.s scheme [34], Rusu scheme [35], Athanasopouloss scheme [36], Kim et al.s scheme [37] and the proposed scheme. We allocate 1 to 10 to show Captchas superiority, where 1 indicates hard to use, not able to remember, mini range of application, much safety loopholes, while 10 indicates the opposite. Based on the experiment analysis, we can conclude that the CaRP not only has a widely use, but also can cater most human tastes. So CaRP will become the emphasis object for our study. Testing results are shown in Table 8.

7. **Conclusion.** In this paper, we conduct a comprehensive and general study of enhanced CaRP authentication scheme using chaotic maps. Most existing researches are concerning about Captcha or CaRP scheme with a password table in the server side, but they ignore the stolen-verifier attacks and privacy protection problem. However, through our exploration, we firstly give a general framework of enhanced CaRP authentication.

TABLE 8. Efficient between the CARP and other Captchas

| Scheme | [33] | [34] | [35] | [36] | [37] | CaRP |
|---|---|---|---|---|---|---|
| Easy to use | 7.6 | 7.5 | 7 | 6.5 | 8.3 | 10 |
| Able to remember | 6.5 | 5 | 4.5 | 4 | 6 | 10 |
| Scope of application | 4(C) | 4(MP) | 1 | 4(C) | 4(C) | 10(C,MP,T) |
| Safety loopholes | 9 | 8 | 6 | 6 | 7 | 10 |
| Note: C: computers, MP: mobile Phone, T: tablet | | | | | | |

Based on the new framework, many enhanced CaRP authentication schemes can be designed if you choose different algorithms. Next, we propose an instance of enhanced CaRP authentication scheme in our framework. Overall, our work is one step forward in the security protocol of using hard AI problems for capturing most existing security requirements. Of reasonable security and usability and practical applications, enhanced CaRP authentication scheme has good potential for refinements, which call for useful future work.

## REFERENCES


[1] V. A. Luis, L. Manuel, J. H. Nicholas, and L. F. John, CAPTCHA: Using Hard AI Problems for Security,*Lecture Notes in Computer Science*, vol.2656, pp.294-311, 2003.

[2] A. Caine, U. Hengartner, The AI Hardness of CAPTCHAs does not imply Robust Network Security , *IFIP International Federation for Information Processing*,vol.238, pp.367-382, 2007.

[3] B. B. Hu, J. Yan, G. Bao, M. Yang, N. Xu, Captcha as Graphical PasswordsA New Security Primitive Based on Hard AI Problems , *IEEE Transactions on Information Forensics and Security*,vol.9, pp.891-904, 2014.

[4] S. B. Sahu, A. Singh, Graphical Password Authentication Using Cued Click Points , *International Journal of Computer Trends and Technology*,vol.18, pp.156-160, 2014.

[5] M. Khan, T. Shah, S. I. Batool, A new implementation of chaotic S-boxes in CAPTCHA , *Signal, Image and Video Processing*,pp.1863-1711, 2015.

[6] M. J. M. Chowdhury, N. R. Chakraborty, CAPTCHA Based on Human Cognitive Factor , *International Journal of Advanced Computer Science and Applications*,vol.4, pp.144-149, 2013.

[7] Yi. L. Lee, C. H. Hsu, Usability study of text-based CAPTCHAs , *Displays*,vol.32, pp.81-86, 2011.

[8] J. W. Kim, W. K. Chung, H. G. Cho, A new image-based CAPTCHA using the orientation of the polygonally cropped sub-images ,*Visual Computer*,vol.26, pp.1135-1143, 2010.

[9] J. Kim, S. Kim, J. Yang, J.-H. Ryu, K. Y. Wohn, FaceCAPTCHA: a CAPTCHA that identifies the gender of face images unrecognized by existing gender classifiers ,*Multimedia Tools and Applications*,vol.72, pp.1215-1237, 2014.

[10] J. W. Kim, W. K. Chung, H. G. Cho, A new image-based CAPTCHA using the orientation of the polygonally cropped sub-images ,*Visual Computer*,vol.26, pp.1135-1143, 2010.

[11] A. Barbar, A. Ismail, Character Image Semantic-Based CAPTCHA ,*International Journal of Future Computer and Communication*, vol.4, pp.211-215, 2015.

[12] T. I. Yang, C. S. Koong, C. C. Tseng, Game-based image semantic CAPTCHA on handset devices ,*Multimedia Tools and Applications*,pp.1573-1588, 2013.

[13] A. Olalere, J. H. Feng, J. L., T. Brooks, Investigating the effects of sound masking on the use of audio CAPTCHAs ,*Behaviour and Information Technology*,vol.9, pp.919-928, 2014.

[14] E. Athanasopoulos, S. Antonatos, Enhanced CAPTCHAs: Using Animation to Tell Humans and Computers Apart , *Lecture Notes in Computer Science*,vol.4273, pp.97-108, 2006.

[15] C. Obimbo, A. Halligan, P. D. Freitas, CaptchAll: An Improvement on the Modern Text-Based CAPTCHA , *Procedia Computer Science*,vol.20, pp.496-501, 2013.

[16] H. C. Gao, X. Y. Liu (2009, July15-17), A new graphical password scheme against spyware by using CAPTCHA.

[17] H. C. Gao, X. Y. Liu, S. D. Wang, R. Dai, A new graphical password scheme against spyware by using CAPTCHA ,*Symposium On Usable Privacy and Security*,pp.15-17, 2009.

[18] Plugging an Information Leak , *Nation*,2012. http://www.bjreview.com.

[19] M. Kerner, Sean, WordPress Resets 100,000 Passwords After Google Account Leak. ,*eWeek*,2014.

[20] Y. Soupionis, R.-A. Koutsiamanis, P. Efraimidis, D. Gritzalis, A game-theoretic analysis of preventing spam over Internet Telephony via audio CAPTCHA-based authentication ,*Journal of Computer Security*,vol.22, pp.383-413, 2014.
[21] P. R. Newswire, Ticketmaster Launches New, Innovative CAPTCHA Solutions, Making The Fan Experience Better ,*PR Newswire US.*,2013.
[22] Wang X, and Zhao J, An improved key agreement protocol based on chaos,*Commun. Nonlinear Sci. Numer. Simul*,Vol. 15, pp. 4052-4057, 2010.
[23] LO. Zhang, Cryptanalysis of the public key encryption based on multiple chaotic systems,*Chaos Solitons Fractals*,Vol. 37, no. 3, pp. 669-674, 2008.
[24] L. R.Devaney, An Introduction to Chaotic Dynamical System,*Cummings Publishing Company Inc.*,The Benjammin, Menlo Park, 1986.
[25] J.C Jiang, Y.H. Peng, Chaos of the Chebyshev polynomials,*Nat. Sci. J. Xiangtan Univ*,vol. 19, no. 3, pp. 3739, 1996.
[26] L. Kocarev, and S. Lian, Chaos-Based Cryptography, *Theory, Algorithms and Applications*, pp. 5354, 2011.
[27] J. Bengtson, K. Bhargavan, C. Fournet, Gordon AD, Maffeis S. Refinement types for secure implementations.*ACM Transactions on Programming Languages and Systems (TOPLAS)*, vol. 33, no. 2, pp. 831845, 2011.
[28] A. D. Gordon, A. Jeffrey, Typing one-to-one and one-to-many correspondences in security protocols. In*Software Security Theories and Systems*,vol. 2609, Lecture Notes in Computer Science. Springer-Verlag: Berlin, Heidelberg, 2003; 263282.
[29] M. Burrows, M. Abadi, R. Needham, A logic of authentication.*ACM Trans. Comput. Syst.*, vol.8, pp. 1836 (1990).
[30] P. Golle, Machine learning attacks against the Asirra CAPTCHA, in*Proc. ACM CCS*, pp. 535542, 2008.
[31] B. B. Zhu et al., Attacks and design of image recognition CAPTCHAs, in*Proc. ACM CCS*, pp. 187200, 2010.
[32] K. Chellapilla, K. Larson, P. Simard, and M. Czerwinski, Building segmentation based human-friendly human interaction proofs, in*Proc. 2nd Int.Workshop Human Interaction Proofs*, pp. 110, 2005.
[33] J. W. Kim, W.-K. Chung, H.-G. Cho, A new image-based CAPTCHA using the orientation of the polygonally cropped sub-images ,*Visual Computer*, vol.26, pp.1135-1143, 2010.
[34] A. Olalere, J. H. Feng, J. Lazar, T. Brooks, Investigating the effects of sound masking on the use of audio CAPTCHAs ,*Behaviour and Information Technology*,vol.9, pp.919-928, 2014.
[35] Rusu, Thomas, Govindaraju, Generation and use of handwritten CAPTCHAs ,*International Journal on Document Analysis and Recognition*,vol.13, pp.49-64, 2010.
[36] E. Athanasopoulos, S. Antonatos, Enhanced CAPTCHAs: Using Animation to Tell Humans and Computers Apart ,*Lecture Notes in Computer Science*,vol.4273, pp.97-108, 2006.
[37] J. Kim, S. Kim, J. Yang, J.-h. Ryu, K. Y. Wohn, FaceCAPTCHA: a CAPTCHA that identifies the gender of face images unrecognized by existing gender classifiers ,*Multimedia Tools and Applications*,vol.72, pp.1215-1237, 2014.
[38] H. Jameel, Taxonomy of human identification protocols Korea: U-security Research Group, Ubiquitous Computing Laboratory, Kyung Hee University. 2007.