SHODH SANGAM - A RKDF University Journal of Science and Engineering
Volume 01, No. 01, 2018

A Novel Smart Card Authentication Scheme using Invisible Image Watermarking

Ravi Singh Pippal
Vedica Institute of Technology, RKDF University, Bhopal
ravesingh@gmail.com

Abstract

One of the primary issues of information technology and communication is the security of information from unwanted frauds. For every transaction over insecure channel authentication is required. Due to the rise of the Internet, smart card authentication schemes have been widely used to avoid the problems related to traditional password based authentication schemes. However, most of the smart card authentication schemes are exposed to one or the other possible attack. This paper describes a novel smart card authentication scheme using image watermarking which covers all the identified security pitfalls and satisfies the needs of a user. Its security is based on hiding the contents of the message in an image. In addition, it provides users to choose and change their passwords freely, mutual authentication and user anonymity. Moreover, it uses nonce instead of timestamp to resist replay attack. Security analysis proves that the proposed scheme is secure against impersonation attack, password guessing attack, replay attack, reflection attack, parallel session attack, insider attack, stolen verifier attack, smart card loss attack and man-in-the-middle attack.

Keywords: Authentication, Image watermarking, Mutual authentication, Nonce, Smart card.

1. Introduction

Authentication is the method to verify the identity of a user who wants to acquire access to server. In traditional password based remote user authentication schemes, server has to keep a verification table secretly in order to verify the legitimacy of a user over insecure channel. Based on one way hash function, a password authentication scheme has been proposed to authenticate remote users [1]. However, this scheme has a security pitfall as an intruder can penetrate the server and modify the contents of verification table. To solve the problems related to verification table, smart card authentication scheme has come into existence. A remote login authentication scheme based on Euclidean geometry has been offered [2] and claimed that the scheme eliminates use of verification table, provides security against impersonation attack and replay attack. Nevertheless, the scheme is vulnerable to impersonation attack [3]. An ID based scheme using RSA cryptosystem has been given [4]. However, it is exposed to impersonation attack [5]. Using ElGamal's cryptosystem, a remote user authentication scheme has been proposed [6]. It is claimed that the scheme is free from replay attack and there is no need to maintain any verification table to authenticate a legitimate user. Though, it is shown that the scheme has security flaws as an unauthorized user can easily forge a valid login request [7]. To improve the efficiency, a remote user authentication scheme using one-way hash function has been offered [8].

However, the scheme is weak against offline and online password guessing attacks [9]. An improved scheme has also been suggested to eliminate password guessing attacks [10]. It is declared that the scheme does not require any verification table and user can choose the password by itself. In addition, it provides mutual authentication between remote user and the server. It is found that the scheme is susceptible to parallel session attack [9].

A nonce based scheme has been given to solve time synchronization problem [11] and claimed that the scheme has an additional merit of session key generation. Nevertheless, it is analyzed that the scheme is vulnerable to insider attack and user is not allowed to change the password freely. A dynamic ID based remote user authentication scheme using one way hash function has been proposed [12]. It is declared that the scheme permits the users to choose and change their passwords freely, secure against ID theft and withstands replay attack, forgery attack, guessing attack, insider attack and stolen verifier attack. However, the scheme is weak against guessing attack, insider attack and fails to provide mutual authentication [13]. An improved scheme has also been suggested to preclude these weaknesses. It is demonstrated that the scheme mentioned in [12] is password independent [14] and further improvement has been suggested.

An efficient smart card authentication scheme based on symmetric key cryptography has been given [15] and claimed that the scheme provides security against impersonation attack, parallel session attack, replay attack and modification attack. Moreover, it provides mutual authentication and shared session key. Though, it is proved that the scheme is inadequate to withstand Denial-of-Service attack and provide perfect forward secrecy [16]. A biometrics based remote user authentication scheme using smart cards has been proposed [17]. Its security is based on one-way hash function, biometrics verification and smart card. It is claimed that the scheme provides users to change their passwords freely and mutual authentication. Moreover, it does not require synchronized clocks and resists replay attack, parallel session attack and impersonation attack. However, it is found that the scheme does not provide proper authentication and fails to resist man-in-the-middle attack [18]. An improved scheme has also been suggested to prohibit these security pitfalls.

Rest of the paper is organized as follows. The proposed smart card authentication scheme using image watermarking is described in section 2. Section 3 demonstrates the security analysis and at the end, section 4 concludes the paper.

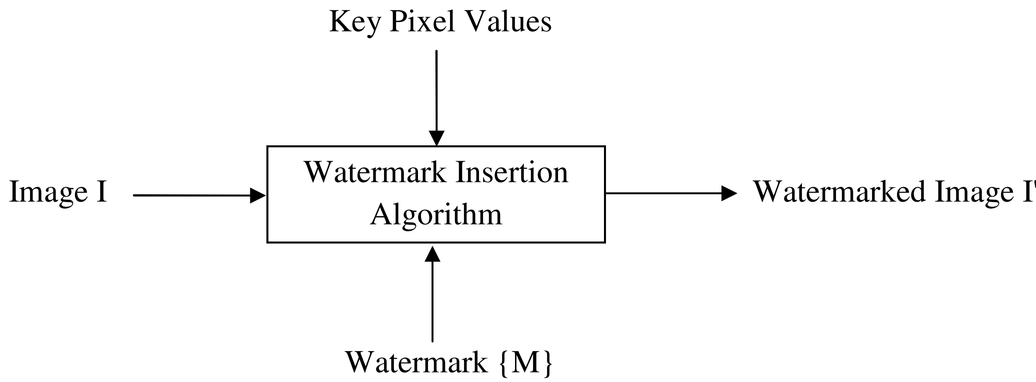
2. Proposed Smart Card Authentication Scheme

Cryptography is a technique to secure the secrecy of communication by encrypting and decrypting data. Sometimes, it is not enough to keep the contents of a message secret. It is essential to hide the existence of the message. Invisible Digital Image Watermarking is a technique used to hide information in an image so that the information is invisible to naked eyes. At the present time, hiding information inside images is a popular technique. An image with a secret message inside can easily be used to transfer secret information over insecure channel. For hiding secret information in images, several watermarking techniques have been proposed which have their own pros and cons. The principal idea behind the used invisible digital image watermarking technique is shown in Figure 1. In the proposed scheme, first two pixels are the key pixels which show the exact location of the hidden message in the image.

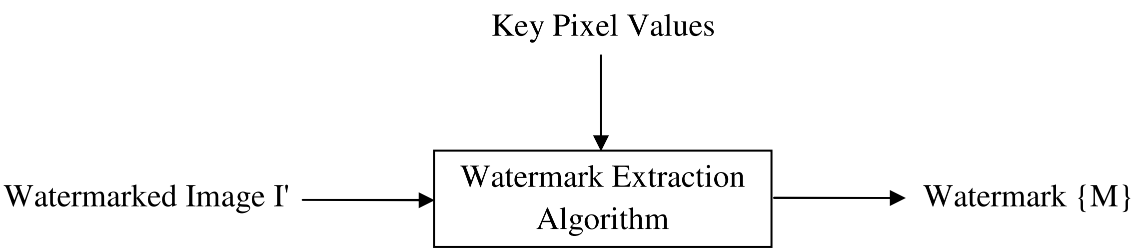
This section describes the proposed smart card authentication scheme using invisible digital image watermarking. The notations used throughout this article are summarized as follows

U_i	→	remote user
ID_i	→	identity of U_i
PW_i	→	password chosen by U_i
S	→	authentication server
PW_i^*	→	password guessed by the adversary
S_k	→	secret key of S
S_n	→	secret number of S
p	→	large prime number
g	→	primitive element
h(•)	→	cryptographic one way hash function
$\oplus$	→	bitwise XOR operation
$\|$	→	concatenation
I_iP_0	→	value of first key pixel of image I_i
I_iP_1	→	value of second key pixel of image I_i
$I_i$pixel	→	pixel array of image I_i
LOC_i	→	starting location of message M_i
LM_i	→	length of message M_i
N_1	→	random nonce generated by U_i
N_2	→	random nonce generated by S
- - - -►	→	secure channel
——►	→	insecure channel

SHODH SANGAM - A RKDF University Journal of Science and Engineering
Volume 01, No. 01, 2018



(a)



(b)

Key Pixels

0,0	0,1	0,2	-	-	-	-	0,j
1,0	1,1	1,2	-	-	-	-	1,j
2,0	2,1	2,2	-	-	-	-	2,j
-	-	-	-	-	-	-	-
-	-	-	-	-	-	-	-
-	-	-	-	-	-	-	-
-	-	-	-	-	-	-	-
i,0	i,1	i,2	-	-	-	-	i,j

(c)

Figure 1. (a) Watermark Insertion (b) Watermark Extraction (c) Image of size i × j with key pixels

The scheme consists of four phases: Registration phase, Login phase, Authentication phase and Password Change phase. First three phases are shown in Figure 2.

2.1 Registration phase

The registration phase is invoked only once when a new user U_i registers with the server. In this phase, U_i selects ID_i and PW_i, computes $h(PW_i)$ and submits $\{ID_i, h(PW_i)\}$ to S over a secure channel. After getting the registration request, S computes $x_i = g^{h(PW_i)} \times S_n \bmod p$, $y_i = h(ID_i \| S_k)$, $z_i = y_i \oplus h(PW_i)$ and issues a smart card over secure channel to U_i by storing $\{x_i, y_i, z_i, p, g, h(\bullet)\}$ into smart card memory.

2.2 Login phase

This phase is invoked when U_i wants to access the server. U_i inserts the smart card to the card reader and keys in ID_i and PW_i. The smart card randomly generates key pixels I_1P_0, I_1P_1 along with a random nonce N_1, computes $a_i = g^{y_i} \bmod p$, $b_i = a_i^{y_i \times N_1} \bmod p$, $c_i = a_i^{h(PW_i) \times N_1} \bmod p$, $d_i = (h(PW_i) + y_i \times h(ID_i \| x_i \| a_i \| b_i \| c_i \| N_1)) \bmod (p-1)$, $e_i = g^{h(PW_i)} \bmod p$, $o_i = b_i \oplus c_i$, LID_i, Ld_i, Le_i, Lo_i and LN_1. It is assumed that the reader has already some images stored in it and the location of the key pixels is shared between user and server. In the proposed scheme, $I_i$pixel[0] and $I_i$pixel[1] are used as the location of key pixels. The reader selects an image I_1 arbitrarily, gets I_1pixel, stores I_1P_0 to I_1pixel[0], I_1P_1 to I_1pixel[1], LID_i to I_1pixel[2], Ld_i to I_1pixel[3], Le_i to I_1pixel[4], Lo_i to I_1pixel[5], LN_1 to I_1pixel[6], computes $LOC_1 = \{(I_1P_0 \times imageI_1\_width) + I_1P_1 + 7\}$, stores the message $M_1 = \{ID_i \| d_i \| e_i \| o_i \| N_1\}$ from I_1pixel[LOC_1] to I_1pixel[$LOC_1 + LM_1$-1] and regenerates the watermarked image I_1' from I_1pixel. U_i sends the image $\{I_1'\}$ as a login request to S.

2.3 Authentication phase

Upon receiving the image $\{I_1'\}$; S first gets I_1'pixel, reads $I_1'P_0$ from I_1'pixel[0], $I_1'P_1$ from I_1'pixel[1], LID_i from I_1'pixel[2], Ld_i from I_1'pixel[3], Le_i from I_1'pixel[4], Lo_i from I_1'pixel[5], LN_1 from I_1'pixel[6], computes $LOC_1' = \{(I_1'P_0 \times imageI_1'\_width) + I_1'P_1 + 7\}$, extracts message $M_1' = \{ID_i \| d_i \| e_i \| o_i \| N_1\}$ from I_1'pixel[LOC_1'] to I_1'pixel[$LOC_1' + LM_1'$-1] and checks the validity of ID_i to accept/reject the login request. If true, S computes $x_i = e_i \times S_n \bmod p$, $y_i = h(ID_i \| S_k)$, $a_i = g^{y_i} \bmod p$, $b_i = a_i^{y_i \times N_1} \bmod p$, $c_i = b_i \oplus o_i$ and checks whether $g^{d_i} = e_i \times a_i^{h(ID_i \| x_i \| a_i \| b_i \| c_i \| N_1)} \bmod p$ is true or not.

$$g^{d_i} = g^{(h(PW_i) + y_i \times h(ID_i \| x_i \| a_i \| b_i \| c_i \| N_1))} \bmod p$$
$$g^{d_i} = g^{h(PW_i)} \times g^{y_i \times h(ID_i \| x_i \| a_i \| b_i \| c_i \| N_1)} \bmod p$$
$$g^{d_i} = g^{h(PW_i)} \bmod p \times g^{y_i \times h(ID_i \| x_i \| a_i \| b_i \| c_i \| N_1)} \bmod p$$
$$g^{d_i} = e_i \times a_i^{h(ID_i \| x_i \| a_i \| b_i \| c_i \| N_1)} \bmod p.$$

If this equation holds, S checks whether $a_i^{d_i \times N_1} = c_i \times b_i^{h(ID_i \| x_i \| a_i \| b_i \| c_i \| N_1)} \bmod p$ is true or not.

$$a_i^{d_i \times N_1} = a_i^{(h(PW_i) + y_i \times h(ID_i \| a_i \| y \| c_i \| d_i \| N_1)) \times N_1} \bmod p$$
$$a_i^{d_i \times N_1} = a_i^{h(PW_i) \times N_1} \times a_i^{y_i \times h(ID_i \| x_i \| a_i \| b_i \| c_i \| N_1) \times N_1} \bmod p$$
$$a_i^{d_i \times N_1} = a_i^{h(PW_i) \times N_1} \bmod p \times a_i^{y_i \times N_1 \times h(ID_i \| x_i \| a_i \| b_i \| c_i \| N_1)} \bmod p$$
$$a_i^{d_i \times N_1} = c_i \times b_i^{h(ID_i \| x_i \| a_i \| b_i \| c_i \| N_1)} \bmod p.$$

If both the equations hold, S generates a nonce N_2, computes $X_1 = y_i \oplus N_1 \oplus N_2$, $X_2 = a_i^{N_2} \bmod p$, LX_1 and LX_2. S selects an image I_2 arbitrarily, gets I_2pixel, randomly generates key pixels I_2P_0, I_2P_1, stores I_2P_0 to I_2pixel[0], I_2P_1 to I_2pixel[1], ID_i to I_2pixel[2], LX_1 to I_2pixel[3], LX_2 to I_2pixel[4], computes $LOC_2 = \{(I_2P_0 \times imageI_2\_width) + I_2P_1 + 5\}$, stores the message $M_2 = \{ID_i \| X_1 \| X_2\}$ from

I_2pixel[LOC_2] to I_2pixel[$LOC_2 + LM_2$-1], regenerates the watermarked image I_2' from I_2pixel and sends the image {I_2'} to U_i.

After getting the image {I_2'}; U_i first gets I_2'pixel, reads $I_2'P_0$ from I_2'pixel[0], $I_2'P_1$ from I_2'pixel[1], LID_i from I_2'pixel[2], LX_1 from I_2'pixel[3], LX_2 from I_2'pixel[4], computes $LOC_2' = \{(I_2'P_0 \times imageI_2'\_width) + I_2'P_1 + 5\}$, extracts the message $M_2' = \{ID_i \| X_1 \| X_2\}$ from I_2'pixel[LOC_2'] to I_2'pixel[$LOC_2' + LM_2'$-1], computes $N_2 = y_i \oplus X_1 \oplus N_1$, $X_2' = a_i^{N_2}$ mod p and checks whether X_2 and X_2' are equal or not. If it holds, S is authentic otherwise terminate the session. Subsequently, U_i computes $X_3 = a_i^{N_1 \times N_2}$ mod p, selects an image I_3 arbitrarily, gets I_3pixel, randomly generates key pixels I_3P_0, I_3P_1, stores I_3P_0 to I_3pixel[0], I_3P_1 to I_3pixel[1], ID_i to I_3pixel[2], LX_3 to I_3pixel[3], computes $LOC_3 = \{(I_3P_0 \times imageI_3\_width) + I_3P_1 + 4\}$, stores the message $M_3 = \{ID_i \| X_3\}$ from I_3pixel[LOC_3] to I_3pixel[$LOC_3 + LM_3$-1], regenerates the watermarked image I_3' from I_3pixel and sends the image {I_3'} to S. Once the image {I_3'} is received; S first gets I_3'pixel, reads $I_3'P_0$ from I_3'pixel[0], $I_3'P_1$ from I_3'pixel[1], LID_i from I_3'pixel[2], LX_3 from I_3'pixel[3], computes $LOC_3' = \{(I_3'P_0 \times imageI_3'\_width) + I_3'P_1 + 4\}$, extracts the message $M_3' = \{ID_i \| X_3\}$ from I_3'pixel[LOC_3'] to I_3'pixel[$LOC_3' + LM_3'$-1], computes $X_3' = a_i^{N_1 \times N_2}$ mod p and checks whether X_3 and X_3' are equal or not. If it holds, mutual authentication is achieved.

2.4 Password Change phase

This phase is invoked whenever U_i wishes to change the password. U_i inserts the smart card to the card reader and keys in ID_i and PW_i'. The smart card computes $z_i' = y_i \oplus h(PW_i')$ and checks whether computed z_i' equals stored z_i or not. If true, U_i enters a new password PW_{inew}. The smart card computes $z_{inew} = y_i \oplus h(PW_{inew})$, $x_{inew} = (x_i / g^{h(PW_i)}) \times g^{h(PW_{inew})}$ mod p and stores z_{inew}, x_{inew} instead of z_i, x_i respectively in the smart card memory. Thus, U_i can change the password without taking any assistance from S.

3. Security Analysis

The security of the proposed scheme depends on invisible watermarking. As the contents of all the communicating messages exchanged between user and server are hidden inside the image, no one can extract these contents from an eavesdropped image. Since the location of the key pixels is known only to user and server, it is not possible to get the invisible watermark correctly. Hence, the proposed scheme resists all the identified attacks related to smart card authentication scheme. Even if, attacker gets the contents of all the communicating messages, the proposed scheme resists the following attacks

3.1 Impersonation Attack

The login request prepared by U_i contains {ID_i, d_i, e_i, o_i, N_1}. Hence, the attacker has to guess the correct values of PW_i, x_i, y_i and a_i to create a forge message in order to masquerade as U_i. Even if attacker guesses the password PW_i*, the correct values of y_i and S_n are still needed to prepare a fake login request. In addition, attacker is unable to extract any of the nonce values from the eavesdropped

User U_i | **Server S**

Registration Phase

Select ID_i and PW_i
Compute $h(PW_i)$

$\{ID_i, h(PW_i)\}$ ⟶

Compute $x_i = g^{h(PW_i)} \times S_n \bmod p$, $y_i = h(ID_i \| S_k)$, $z_i = y_i \oplus h(PW_i)$
Store $\{x_i, y_i, z_i, p, g, h(\bullet)\}$ into smart card

⟵ {Smart card}

Login and Authentication Phase

Input ID_i and PW_i
Generate key pixels I_1P_0, I_1P_1, nonce N_1
Compute $a_i = g^{y_i} \bmod p$, $b_i = a_i^{y_i \times N_1} \bmod p$, $c_i = a_i^{h(PW_i) \times N_1} \bmod p$, $d_i = (h(PW_i) + y_i \times h(ID_i \| x_i \| a_i \| b_i \| c_i \| N_1)) \bmod (p-1)$
$e_i = g^{h(PW_i)} \bmod p$, $o_i = b_i \oplus c_i$, LID_i, Ld_i, Le_i, Lo_i and LN_1
Select I_1 and get I_1pixel
Store I_1P_0 to I_1pixel[0], I_1P_1 to I_1pixel[1], LID_i to I_1pixel[2], Ld_i to I_1pixel[3], Le_i to I_1pixel[4], Lo_i to I_1pixel[5], LN_1 to I_1pixel[6]
Compute $LOC_1 = \{(I_1P_0 \times imageI_1\_width) + I_1P_1 + 7\}$
Store $M_1 = \{ID_i \| d_i \| e_i \| o_i \| N_1\}$ from I_1pixel[LOC_1] to I_1pixel[$LOC_1 + LM_1$-1]
Regenerate the watermarked image I_1' from I_1pixel

$\{I_1'\}$ ⟶

Get I_1'pixel, read $I_1'P_0$ from I_1'pixel[0], $I_1'P_1$ from I_1'pixel[1], LID_i from I_1'pixel[2], Ld_i from I_1'pixel[3], Le_i from I_1'pixel[4], Lo_i from I_1'pixel[5], LN_1 from I_1pixel[6]
Compute $LOC_1' = \{(I_1'P_0 \times imageI_1'\_width) + I_1'P_1 + 7\}$
Extract $M_1' = \{ID_i \| d_i \| e_i \| o_i \| N_1\}$ from I_1'pixel[LOC_1'] to I_1'pixel[$LOC_1' + LM_1'$-1]
Check the validity of ID_i
Compute $x_i = e_i \times S_n \bmod p$, $y_i = h(ID_i \| S_k)$, $a_i = g^{y_i} \bmod p$,
$b_i = a_i^{y_i \times N_1} \bmod p$, $c_i = b_i \oplus o_i$
Verify the two equations holds or not
1) $g^{d_i} = e_i \times a_i^{h(ID_i \| x_i \| a_i \| b_i \| c_i \| N_1)} \bmod p$
2) $a_i^{d_i \times N_1} = c_i \times b_i^{h(ID_i \| x_i \| a_i \| b_i \| c_i \| N_1)} \bmod p$
Generate a nonce N_2
Compute $X_1 = y_i \oplus N_1 \oplus N_2$, $X_2 = a_i^{N_2} \bmod p$, LX_1 and LX_2
Select I_2 and get I_2pixel
Generate key pixels I_2P_0, I_2P_1
Store I_2P_0 to I_2pixel[0], I_2P_1 to I_2pixel[1], ID_i to I_2pixel[2], LX_1 to I_2pixel[3], LX_2 to I_2pixel[4]
Compute $LOC_2 = \{(I_2P_0 \times imageI_2\_width) + I_2P_1 + 5\}$
Store $M_2 = \{ID_i \| X_1 \| X_2\}$ from I_2pixel[LOC_2] to I_2pixel[$LOC_2 + LM_2$-1]
Regenerate the watermarked image I_2' from I_2pixel

⟵ $\{I_2'\}$

Get I_2'pixel, read $I_2'P_0$ from I_2'pixel[0], $I_2'P_1$ from I_2'pixel[1], LID_i from I_2'pixel[2], LX_1 from I_2'pixel[3], LX_2 from I_2'pixel[4]
Compute $LOC_2' = \{(I_2'P_0 \times imageI_2'\_width) + I_2'P_1 + 5\}$
Extract $M_2' = \{ID_i \| X_1 \| X_2\}$ from I_2'pixel[LOC_2'] to I_2'pixel[$LOC_2' + LM_2'$-1]
Compute $N_2 = y_i \oplus X_1 \oplus N_1$, $X_2' = a_i^{N_2} \bmod p$
Verify whether $X_2 = X_2'$
Compute $X_3 = a_i^{N_1 \times N_2} \bmod p$,
Select I_3 and get I_3pixel
Generate key pixels I_3P_0, I_3P_1
Store I_3P_0 to I_3pixel[0], I_3P_1 to I_3pixel[1], ID_i to I_3pixel[2], LX_3 to I_3pixel[3]
Compute $LOC_3 = \{(I_3P_0 \times imageI_3\_width) + I_3P_1 + 4\}$
Store $M_3 = \{ID_i \| X_3\}$ from I_3pixel[LOC_3] to I_3pixel[$LOC_3 + LM_3$-1]
Regenerate the watermarked image I_3' from I_3pixel

$\{I_3'\}$ ⟶

Get I_3'pixel, read $I_3'P_0$ from I_3'pixel[0], $I_3'P_1$ from I_3'pixel[1], LID_i from I_3'pixel[2], LX_3 from I_3'pixel[3]
Compute $LOC_3' = \{(I_3'P_0 \times imageI_3'\_width) + I_3'P_1 + 4\}$
Extract $M_3' = \{ID_i \| X_3\}$ from I_3'pixel[LOC_3'] to I_3'pixel[$LOC_3' + LM_3'$-1]
Compute $X_3' = a_i^{N_1 \times N_2} \bmod p$
Verify whether $X_3 = X_3'$

Figure 2. Proposed Scheme

response message as the value of y_i is unknown. It is difficult to derive $h(PW_i)$ from e_i because of discrete logarithm problem. Moreover, S verifies the validity of login request by comparing two different equations and accepts the login request only when both of them are equal else rejects the login request. If an attacker modifies any of the login request parameters, S easily detects them as both the equations are unsatisfied. Hence, attacker is unable to forge the login request to impersonate a valid U_i.

3.2 Password Guessing Attack

In the proposed scheme, $h(PW_i)$ is used to compute login request parameters $d_i = (h(PW_i) + y_i \times h(ID_i \| x_i \| a_i \| b_i \| c_i \| N_1)) \bmod (p-1)$ and $e_i = g^{h(PW_i)} \bmod p$. Let us assume that the adversary intercepts login request $\{ID_i, d_i, e_i, o_i, N_1\}$ during the transmission from U_i to S. It is hard to guess the all three parameters x_i, y_i and a_i correctly at the same time to check whether each of the guessed passwords is correct or not. Moreover, to derive PW_i from e_i, adversary needs to solve the discrete logarithm problem and break the security of one way hash function. Therefore, the scheme is secure against password guessing attack.

3.3 Replay Attack

An adversary may try to act as an authentic user by resending previously intercepted messages. This scheme uses random nonces N_1 and N_2 which are different from session to session. As a result, attackers cannot enter the system by resending the previously transmitted messages to impersonate legal users. Assume that the intercepted login request $\{ID_i, d_i, e_i, o_i, N_1\}$ is replayed to pass the authentication phase. Attacker is unable to retrieve N_2 correctly from the response message $\{ID_i, X_1, X_2\}$ to compute the correct message $\{ID_i, X_3\}$ for mutual authentication. Consequently, S rejects the message by comparing X_3 with X_3'.

3.4 Reflection and Parallel Session Attacks

To resist reflection and parallel session attacks, the given scheme employs asymmetric structure of communicating messages, i.e., $\{ID_i, d_i, e_i, o_i, N_1\}$, $\{ID_i, X_1, X_2\}$ and $\{ID_i, X_3\}$. There is no symmetry in the values of $d_i = (h(PW_i) + y_i \times h(ID_i \| x_i \| a_i \| b_i \| c_i \| N_1)) \bmod (p-1)$, $e_i = g^{h(PW_i)} \bmod p$, $o_i = b_i \oplus c_i$, $X_1 = y_i \oplus N_1 \oplus N_2$, $X_2 = a_i^{N_2} \bmod p$ and $X_3 = a_i^{N_1 \times N_2} \bmod p$. Hence, attacker is unable to launch parallel session attack by replaying server response message as the user login request or reflection attack by resending user login request as the server response message.

3.5 Insider Attack

An insider of S can obtain U_i's password during the registration phase and then impersonate U_i to access other servers if same password is used to access several servers. In this scheme, $h(PW_i)$ is sent to S instead of PW_i to resist insider attack. So, any insider of S cannot get U_i's password PW_i.

3.6 Stolen Verifier Attack

U_i's secret information stored at S is under extensive threat from the attackers. In the proposed scheme, S keeps secret key 'S_k' and secret number 'S_n' to avoid maintaining verification table used to verify U_i's login request. Hence, the scheme is secure against stolen verifier attack.

3.7 Smart Card Loss Attack

When a smart card is lost or stolen, unauthorized user who obtains the smart card can guess the password of U_i by using password guessing attacks or impersonate U_i to login into S. In the proposed scheme, if U_i's smart card is lost or stolen, no one can impersonate the smart card owner to login into S without knowing the correct ID_i and PW_i of U_i.

3.8 Man-in-the-Middle Attack

If an attacker intercepts the communicating messages between U_i and S, it does not generate any useful information as they are dissimilar from session to session due to property of randomness of N_1 and N_2. Moreover, to alter N_1, one needs to recalculate d_i and o_i. Similarly, y_i is needed to alter N_2. Attacker cannot pretend as U_i or S to authenticate each either of them since y_i, S_n and a_i are unknown. Hence, the proposed scheme is secure against man-in-the-middle attack.

3.9 The scheme solves time synchronization problem

The proposed scheme uses randomly generated nonces N_1 and N_2 instead of time-stamps to avoid time synchronization problem.

3.10 The scheme provides user anonymity

As the contents of all the communicating messages exchanged between user and server are hidden in the image, no one can get information about the identity of any of the communicated parties.

4. Conclusion

This paper enlightens a novel smart card authentication scheme using invisible image watermarking. It has been shown that the proposed scheme provides stronger security as the contents of all the communicating messages exchanged between user and server are hidden inside the image. An attacker is unable to extract these contents from an eavesdropped image as nobody knows the exact location of watermark except a legitimate user and the server. Even if, attacker is able to obtain the contents of all the communicating messages, this scheme provides security against impersonation attack, password guessing attack, replay attack, reflection attack, parallel session attack, insider attack, stolen verifier attack, smart card loss attack, man-in-the-middle attack and solves time synchronization problem. Moreover, to accomplish user's needs, the proposed scheme has the following merits (i) user can choose and change the password without any assistance from the server. (ii) It provides mutual authentication and anonymity to the user. This work has been implemented and tested in Java1.6 using a BMP image.

Acknowledgments

The author would like to thank Vedica Institute of Technology, RKDF University, Bhopal, India for providing the academic support.

References

[1] L. Lamport, “Password authentication with insecure communication”, Communications of the ACM, vol. 24, no.11, 1981, pp. 770-772.

[2] Tzong-Chen Wu, “Remote login authentication scheme based on a geometric approach”, Computer Communications, vol. 18, no. 12, 1995, pp. 959-963.

[3] M. S. Hwang, “Cryptanalysis of a remote login authentication scheme”, Computer Communications, vol. 22, no. 8, 1999, pp. 742-744.

[4] Wen-Her Yang and Shiuh-Pyng Shieh, “Password authentication schemes with smart cards”, Computers & Security, vol. 18, no. 8, 1999, pp. 727-733.

[5] C. K. Chan and L. M. Cheng, “Cryptanalysis of timestamp-based password authentication scheme”, Computers & Security, vol. 21, no. 1, 2002, pp. 74-76.

[6] M.S. Hwang and L.H. Li, “A new remote user authentication scheme using smart cards”, IEEE Transactions on Consumer Electronics, vol. 46, no. 1, 2000, pp. 28-30.

[7] C. K. Chan and L. M. Cheng, “Cryptanalysis of a remote user authentication scheme using smart cards,” IEEE Transactions on Consumer Electronics, vol. 46, no. 4, 2000, pp. 992-993.

[8] H.M. Sun, “An efficient remote user authentication scheme using smart cards”, IEEE Transactions on Consumer Electronics, vol. 46, no. 4, 2000, pp. 958-961.

[9] Chien-Lung Hsu, “Security of two remote user authentication schemes using smart cards”, IEEE Transactions on Consumer Electronics, vol. 49, no. 4, 2003, pp. 1196-1198.

[10] Hung-Yu Chien, Jinn-Ke Jan and Yuh-Min Tseng, “An efficient and practical solution to remote authentication: smart card”, Computers & Security, vol. 21, no. 4, 2002, pp. 372-375.

[11] Wen-Shenq Juang, “Efficient password authenticated key agreement using smart cards”, Computers & Security, vol. 23, no. 2, 2004, pp. 167-173.

[12] Manik Lal Das, Ashutosh Saxena, and Ved P. Gulati, “A dynamic ID-based remote user authentication scheme”, IEEE Transactions on Consumer Electronics, vol. 50, no. 2, 2004, pp. 629-631.

[13] I-En Liao, Cheng-Chi Lee and Min-Shiang Hwang, “Security enhancement for a dynamic ID-based remote user authentication scheme”, International Conference on Next Generation Web Services Practices, 2005.

[14] Yan-yan Wang, Jia-yong Liu, Feng-xia Xiao and Jing Dan, “A more efficient and secure dynamic ID-based remote user authentication scheme”, Computer Communications, vol. 32, no. 4, 2009, pp. 583-585.

[15] Ronggong Song, “Advanced smart card based password authentication protocol”, Computer Standards & Interfaces, vol. 32, no. 5-6, 2010, pp. 321-325.

[16] Ravi Singh Pippal, Jaidhar C. D. and Shashikala Tapaswi, “Comments on symmetric key encryption based smart card authentication scheme”, 2nd International Conference on Computer Technology and Development (ICCTD-2010), 2010, pp. 482-484.

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

[18] Xiong Li, Jian-Wei Niu, Jian Ma, Wen-Dong Wang and Cheng-Lian Liu, “Cryptanalysis and improvement of a biometrics-based remote user authentication scheme using smart cards”, Journal of Network and Computer Applications, vol. 34, no. 1, 2011, pp. 73-79.