A Novel Smart Card Authentication Scheme using Image Encryption

Ravi Singh Pippal
Radharaman Institute of Research and Technology
Ratibad, Bhopal, M.P.

Pradeep Gupta
Gwalior Engineering College
Gwalior, M.P.

Rakesh Singh
Gwalior Engineering College
Gwalior, M.P.

ABSTRACT
From the user point of view, security and efficiency are the two main factors for any authentication scheme. However, most of the smart card authentication schemes are vulnerable to one or the other possible attack. In this paper, highly secured smart card authentication scheme is proposed using image encryption that resists all the possible attacks and satisfies the needs of a user. Its security is based on encryption of text with a key image. Moreover, it provides mutual authentication, session key establishment and uses date and time as a timestamp to resist replay attack. Security analysis proves that the proposed scheme is more secure and practical.

Keywords
Authentication, Image encryption, Mutual authentication, Password, Replay attack, Session key, Smart card.

1. INTRODUCTION
Authentication is the process of verifying the identity of a user who wants to get 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. In 1981, Lamport [1] proposed a password authentication scheme to authenticate remote users. However, an intruder can penetrate the server and modify the contents of the password or verification table. In 1995, Wu [2] developed a remote login authentication scheme based on a geometric approach and claimed that the scheme eliminates the use of verification table, provides security against impersonation attack and replay attack. Nevertheless, Hwang [3] showed that Wu's scheme is vulnerable to impersonation attack. In 1999, Yang and Shieh [4] proposed an ID based scheme using RSA cryptosystem. However, Chan and Cheng [5] proved that Yang and Shieh's scheme is susceptible to impersonation attack. In 2000, Hwang and Li [6] developed a remote user authentication scheme based on ElGamal's cryptosystem and claimed that their scheme is free from replay attack and there is no need to maintain any verification table to authenticate a legitimate user. Though, Chan and Cheng [7] showed that Hwang and Li's scheme is exposed to impersonation attack. In 2000, Sun [8] proposed a remote user authentication scheme using one-way hash function. In 2003, Hsu [9] found that Sun's scheme is weak against offline and online password guessing attacks. An improved scheme was presented by Chien et al. [10] to eliminate password guessing attacks and claimed that their scheme does not require any verification table and the user can choose the password by itself. In addition, it provides mutual authentication between the remote user and the server. However, Hsu [9] showed that Chien et al.'s scheme is susceptible to parallel session attack.

In 2004, Juang [11] proposed a nonce based scheme to solve time synchronization problem and claimed that the scheme has an additional merit of session key generation. Nevertheless, this scheme is weak against insider attack and user is not allowed to change the password freely. In 2004, Das et al. [12] developed a dynamic ID based remote user authentication scheme using one way hash function. The authors claimed that their scheme allows users to choose and change the passwords freely. Moreover, it provides security against ID theft and resists forgery attack, replay attack, insider attack, stolen verifier attack and guessing attack. In 2005, Liao et al. [13] found that Das et al.'s scheme is weak against guessing attack, insider attack and fails to provide mutual authentication. An improved scheme was also developed to preclude these weaknesses. In 2009, Wang et al. [14] demonstrated that Das et al.'s scheme is password independent and further improvement was also suggested. In 2010, Song [15] presented an efficient smart card authentication scheme based on symmetric key cryptography 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, Pippal et al. [16] showed that Song's scheme is inadequate to withstand Denial-of-Service attack and provide perfect forward secrecy.
In 2010, Li and Hwang [17] proposed a biometrics based remote user authentication scheme using smart cards. The security of Li and Hwang's scheme relies on the one-way hash function, smart card and biometrics verification. They claimed that their scheme provides mutual authentication, does not require synchronized clocks between users and the remote server, the users change their passwords freely and resists replay attack, parallel session attack and impersonation attack. In 2011, Li et al. [18] found that Li and Hwang's scheme does not provide proper authentication and fails to resist the man-in-the-middle attack. An improved scheme was also developed to prohibit these security pitfalls.
The remainder of the paper is structured as follows. The proposed smart card authentication scheme using image encryption is described in section 2. Section 3 demonstrates the results and security analysis of the proposed scheme. Finally, section 4 concludes the paper.

2. PROPOSEDSMART CARD AUTHENTICATION SCHEME
Steganography is an art and science of information hiding and invisible communication. Hiding information inside images is a popular technique nowadays. This work satisfies the aim that says 'Steganography' is an effective way to obscure data and hide sensitive information. Today, information security is

becoming more vital in transmission and data storage. Due to this, images are widely used in many applications. In the field of information hiding, image encryption plays a significant part. Several image encryption techniques have been proposed to hide the data inside an image. However, most of these schemes have their pros and cons. The principal idea behind the used image encryption technique is that two pictures are used to calculate differences between their pixels, which are converted into UTF char code (text). The UTF char code is distributed randomly between the R, G and B which are added or subtracted from the original RGB. Here, the first pixel behaves like a flag pixel and the decrypter decrypts the received image by calculating the distance between each received data-pixel. It, then, starts to read the picture.

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

U_A	→	Remote user
ID_A	→	Identity of U_A
PW_A	→	Password chosen by U_A
S	→	Authentication server
x	→	Secret key of the server S
p, q	→	Prime numbers
T_A	→	Date and time at which user login request is created
T_S	→	Date and time at which server response message is created
R_A	→	Random number
I_1	→	Key image
$E(I_1, t)$	→	Encryption of image I_1 with text 't'
$D(I_1, I_2)$	→	Decryption of image I_1 with image I_2
$h(\bullet)$	→	Cryptographic one way hash function
$\oplus$	→	Bitwise XOR operation
$\|\|$	→	Concatenation

This scheme consists of five phases: Initial phase, Registration phase, Login phase, Authentication phase and Password Change phase. These phases are shown in Fig. 1.

2.1 Initial Phase

Server selects two large prime numbers p and q such that $p = 2q + 1$, chooses its secret key 'x' in Z_q, a one-way hash function $h(\cdot)$, image encryption $E(\cdot)$ and decryption $D(\cdot)$ operations and a key image I_1. The server keeps p, x and I_1 secret.

2.2 Registration Phase

This phase is invoked whenever user U_A initially registers to the authentication server S. User U_A selects ID_A, PW_A, computes $h(PW_A)$ and submits $\{ID_A, h(PW_A)\}$ to the server. Upon receiving the registration request, server computes $C_A = h(ID_A^x \bmod p)$, $B_A = C_A \oplus h(PW_A)$ and issues a smart card to user U_A by storing $\{ID_A, B_A, C_A, h(\cdot), E(\cdot), D(\cdot), I_1\}$ into smart card memory. It is assumed that the data stored in the smart card is secure and no one can extract it from smart card memory.

2.3 Login Phase

User U_A inserts the smart card to the card reader and keys in ID_A and PW_A'. The smart card computes $C_A' = B_A \oplus h(PW_A')$ and checks if computed C_A equals C_A' or not. If true, generates a random number R_A, gets the current timestamp T_A, computes $Q_A = C_A' \oplus R_A \oplus T_A$, $D_A = h(T_A \| R_A \| Q_A \| ID_A)$, $I_2 = E(I_1, ID_A \| D_A \| Q_A \| T_A)$ and sends the login request $\{ID_A, T_A, I_2\}$ to the server.

2.4 Authentication Phase

Upon receiving the login request $\{ID_A, T_A, I_2\}$, server first checks the validity of ID_A and T_A to accept/reject the login request. If it does not hold, the request is rejected else consider for next step of check. The server computes $C_A = h(ID_A^x \bmod p)$, $ID_A \| D_A \| Q_A \| T_A = D(I_1, I_2)$, $R_A' = Q_A \oplus C_A \oplus T_A$ and checks whether D_A equals to $h(T_A \| R_A' \| Q_A \| ID_A)$. If it is true, user is authenticated. The server gets the current timestamp T_S and computes $D_S = h(ID_A \| R_A' \| T_S)$, $I_3 = E(I_1, ID_A \| D_S \| T_S)$ and sends the message $\{ID_A, T_S, I_3\}$ to the user. Upon receiving the message $\{ID_A, T_S, I_3\}$, the smart card validates ID_A and T_S, computes $ID_A \| D_S \| T_S = D(I_1, I_3)$ and checks whether D_S equals to $h(ID_A \| R_A \| T_S)$. If they are equal, server is authenticated. Both the user and server compute a common shared secret session key $SKey = h(ID_A \| D_A \| D_S \| R_A) = h(ID_A \| D_A \| D_S \| R_A')$.

2.5 Password Change Phase

This phase is invoked when user U_A wants to change the password. User U_A inserts the smart card to the card reader and keys in ID_A and PW_A'. The smart card computes $C_A' = B_A \oplus h(PW_A')$ and checks if computes C_A equals C_A' or not. If true, user U_A enters a new password PW_A^{new}. The smart card computes $B_A^{new} = B_A \oplus h(PW_A') \oplus h(PW_A^{new})$ and replaces B_A with B_A^{new}. Thus, user U_A can change the password without taking any assistance from the server S.

3. RESULTS AND SECURITY ANALYSIS

This work has been implemented on Windows XP2, Pentium 4 CPU 2.80 GHz using Java1.6. Fig. 2 shows the key image I_1, Image $I_2 = E(I_1, ID_A \| D_A \| Q_A \| T_A)$ is the login request parameter and Image $I_3 = E(I_1, ID_A \| D_S \| T_S)$ is the parameter contained in response message transmitted from the server to user for mutual authentication.

As the contents of all the communicating messages exchanged between user and server are encrypted with the key image I_1, no one can extract these contents from an eavesdropped image. Even if, an attacker gets the contents of all the communicating messages, the proposed scheme resists the following attacks:

3.1 Impersonation Attack

In the proposed scheme, the login request contains $\{ID_A, T_A, I_2\}$ where $I_2 = E(I_1, ID_A \| D_A \| Q_A \| T_A)$. Suppose an attacker has derived the text $ID_A \| D_A \| Q_A \| T_A$ from the image I_2. To modify D_A and Q_A, the attacker needs to guess the correct values of R_A and C_A. Hence, attacker is unable to create a forged login request to impersonate a valid user.

3.2 Password Guessing Attack

Since $h(PW_i)$ is used only in the verification of computed C_A' which is not a part of login request, this scheme is secure against password guessing attack.

3.3 Replay Attack

This scheme uses date and time as a timestamp. Thus, attackers cannot enter the system by resending messages previously transmitted by legal users.

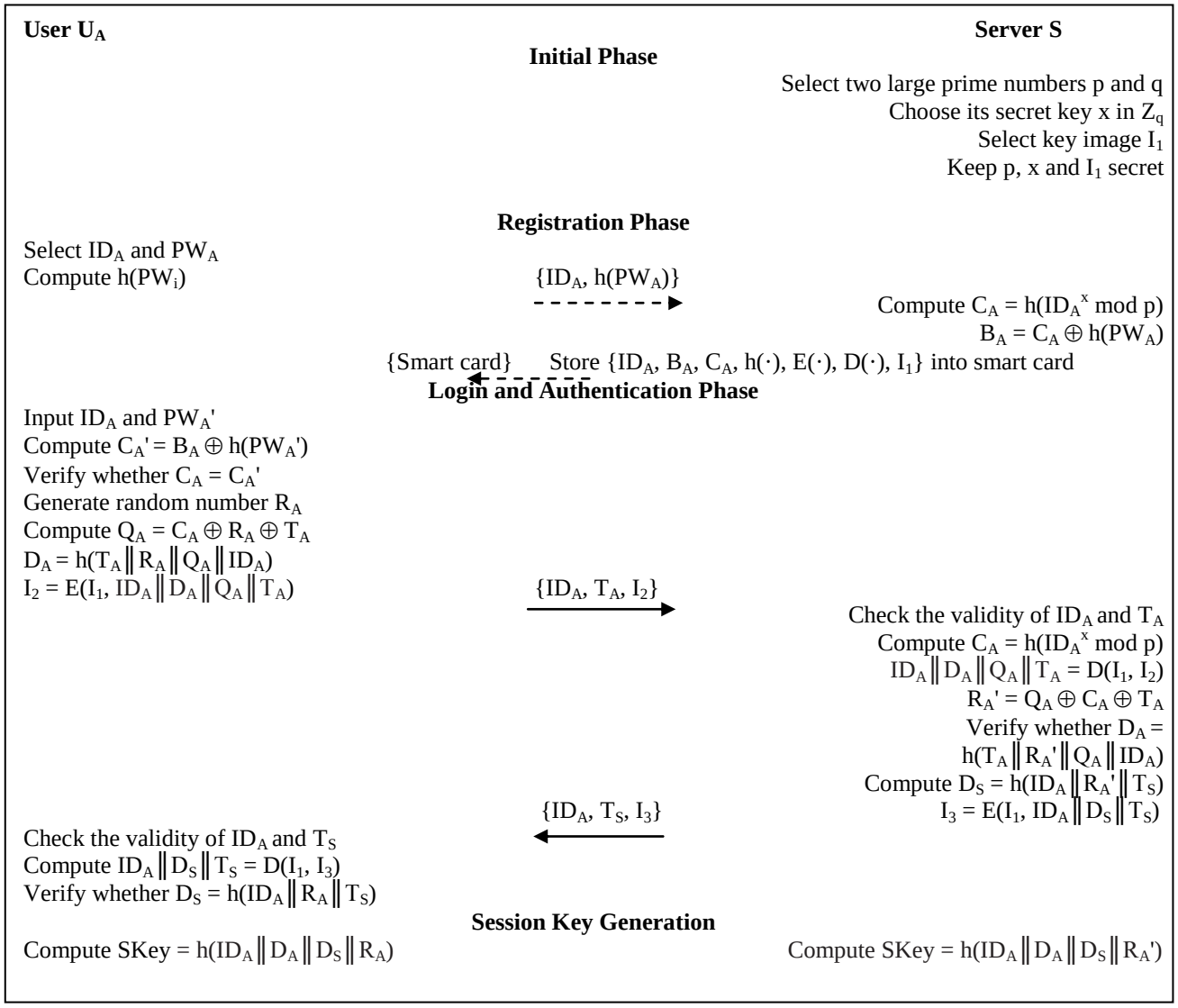

Fig 1: Proposed scheme

3.4 Impersonation Attack

In the proposed scheme, the login request contains $\{ID_A, T_A, I_2\}$ where $I_2 = E(I_1, ID_A \| D_A \| Q_A \| T_A)$. Suppose an attacker has derived the text $ID_A \| D_A \| Q_A \| T_A$ from the image I_2. To modify D_A and Q_A, the attacker needs to guess the correct values of R_A and C_A. Hence, attacker is unable to create a forged login request to impersonate a valid user.

3.5 Password Guessing Attack

Since $h(PW_i)$ is used only in the verification of computed C_A' which is not a part of login request, this scheme is secure against password guessing attack.

3.6 Replay Attack

This scheme uses date and time as a timestamp. Thus, attackers cannot enter the system by resending messages previously transmitted by legal users.

3.7 Reflection and Parallel Session Attack

To resist reflection and parallel session attacks, the scheme employs asymmetric computations of parameter values of communicating messages, i.e., $\{ID_A, T_A, I_2\}$ and $\{ID_A, T_S, I_3\}$, where $I_2 = E(I_1, ID_A \| D_A \| Q_A \| T_A)$ and $I_3 = E(I_1, ID_A \| D_S \| T_S)$.

3.8 Insider Attack

During the registration phase, $h(PW_i)$ is sent to server S as an alternative of PW_i. So, any insider of S cannot get user password PW_i. Hence, this scheme is secure against insider attack.

3.9 Stolen Verifier Attack

The server does not maintain any password or verification table to verify the user's login request. Therefore, the scheme withstands stolen verifier attack.

Fig 2: (a) Key Image I_1, (b) Image I_2 contained in login request, (c) Image I_3 contained in response message

3.10 Smart Card Loss Attack

If a user U_i's smart card is lost or stolen, no one can impersonate the smart card owner to login the server. Without knowing the correct ID_i and PW_i of the user, attacker cannot prepare a valid login request.

3.11 User can choose and change the password securely without any assistance from the server

In the scheme, the smart card verifies the old password first in the password change phase. So, unauthorized users cannot change the authorized user's password even if they get the corresponding smart card.

3.12 The scheme provides session key generation

The proposed scheme generates a session key SKey = $h(ID_A \| D_A \| D_S \| R_A)$ during the authentication phase which will be different for each login session.

3.13 Attack on Perfect Forward Secrecy

In the scheme, the session key SK = $h(D_i \| N_i \| N_j \| B_i')$ is calculated using randomly generated nonces N_i and N_j which are different for each login session and are not a part of any of the transmitted messages between user U_i and the server S. Even if an attacker gets X_s, server's secret key, there is no way to get any information about present session key or previous session keys. Hence, the scheme provides perfect forward secrecy.

3.14 Denning-Sacco Attack

If an attacker captures a session key then there is no way to get any information about nonces N_i and N_j or server's secret key X_s due to the property of one-way hash. As PW_i is not involved directly in the calculation of session key, no one can get user's password from the eavesdropped session key.

3.15 Denial-of-Service Attack

If the user U_i inputs a wrong password by mistake, this password will be quickly detected by the card reader since reader compares $B_i' = A_i \oplus h(ID_i' \| h(PW_i'))$ with the stored B_i during the login phase. Hence, the scheme resists this type of Denial-of-Service attack.

3.16 Man-in-the-Middle Attack

In the proposed scheme, if an attacker intercepts the communicating messages between the user and the server then it will not generate any useful information because nonces N_i and N_j (used in the calculation of session key) are not a part of the communicating messages. Moreover, to alter Z_i or Z_j, one needs the value of A_i. Hence, the proposed scheme resists man-in-the-middle attack.

4. CONCLUSION

This paper describes a highly secured smart card authentication scheme using image encryption. It has been shown that the proposed scheme provides stronger security as it prevents impersonation attack, password guessing attack, replay attack, insider attack, reflection attack, parallel session attack, stolen verifier attack, smart card loss attack, Denial-of-Service attack, attack on perfect forward secrecy and denning-sacco attack. Moreover, the proposed scheme offers the following properties: user can choose and change the password without any help from the server, provides mutual authentication and session key generation.

5. 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", Computer & 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), November 2-4, 2010, Cairo, Egypt, 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.