International Journal of Information & Network Security (IJINS)
Vol.3, No.4, August 2014, pp. 257~265
ISSN: 2089-3299

Using Steganography to Product a New Message Authentication Code Scheme inside Cloud Environment

Ali A.Yassin Al-Amrei

Computer Science Dept., Education College for Pure Science, Basrah University,
Basrah, 61004, Iraq,
Email: ali.yassin@uobasrah.edu.iq, AliAdel79yassin@gmail.com

Article Info

Article history:

Received
Revised Aug
Accepted Aug

Keyword:

MAC
LSB
Cloud Computing
MITM attack
Forgery attack

ABSTRACT

In the era of cloud computing, the securities of cryptography schemes play more attention in key-dependent plaintexts. Preserving the confidentiality and integrity of the message transmitted between the components of the cloud environment is one of the most important goals of *Message Authentication Code* (MAC). Furthermore, the MAC protocol suffers from several malicious attacks such as forgery attack, *Man-In-The-Middle* (MITM) attack; reflect attack, and key recovery attack. In this paper, an efficient MAC scheme based on data hiding technique of image is proposed. This scheme is embedded the bits of MAC using *least significant-bit* (LSB) to enable a large message capacity. Furthermore, our proposed scheme overcomes above aforementioned issues. Additionally, our proposed scheme includes many security characteristics like user's message anonymity, data integrity for user's message, session key agreement, and one time message code for each user's session. Security analysis and experimental results illustrate that our proposed scheme can withstand the common security attacks as well, and has a good performance of message authentication code.

Corresponding Author:

Ali A. Yassin Al-Amrei,
Computer Science Dept., Education College for Pure Science,
Basrah University,
61004, Basrah, Karmat Ali, Iraq.
Email: AliAdel79yassin@gmail.com

1. INTRODUCTION

Cloud computing era has always been the expedition of human society for the improvement of our living conditions. Cloud computing technology is always at the head of all other technologies. Nowadays, in addition to the modern technologies, people completely depend mainly on the Internet for their everyday activities like e- banking, e-business transaction, pay as you go, etc. All of these users' activities mange by the cloud computing. Additionally, there are many advantages from migrating user's data to the cloud side, since he can use data from the cloud side on-demand, using any device, without any attention at the cost of software and hardware infrastructures. The users can avoid extra cost and achieve the flexibility to scale exploitations on-demand [2, 3]. The security is a constitutive trouble that hinders its widespread adoption.

Obviously, the message that generated from a legal user is known as User Authentication and is supported by Message Authentication code (MAC) for ensuring from the integrity and authenticity of received message. MAC functions require possessing several security tools such as SHA-1. For more security, a MAC

function should be having ability to resist well-known attacks such as forgery and insider attacks. As a result, even if an adversary can be achieved an oracle which holds the shared key and produces MACs for messages of an adversary's selecting; an adversary cannot guess MAC for other messages without execution infeasible amounts of computation. The main components (sender and receiver) of MAC values are used the same secret key. This means that the components of a message should be agreed on the same key in the setup phase, as is the state with symmetric encryption. Additionally, any user has ability to verify a MAC is also capable of producing MACs for other messages [4, 5].

Constantly, MACs are very sensitive to any modification of the message. If one or more bits of user's message update, MAC changes about 50 percent of their bits and cause to be the message impractical. Furthermore, the successful verification of MACs demands equivalence of all of bits of the received sender's MAC with calculated receiver's MAC. Such a hard condition for the successful verification of messages protected by MACs is not suitable for some applications. There are several schemes in this topic that suffered from many drawbacks such as replay attacks, reflection attacks, and guesting secret key between the sender and receiver [5].

In this paper, we present a new message authentication scheme for cloud environments that consists of two phases—setup and verification. Furthermore, our proposed scheme enables authentication and integrity protection of messages exchanged over a secure communication channel between entities that based on shared secret key and steganography. Where, the sender and receiver have been agreed to the shared secret key at setup phase. The construction of our proposed scheme enables a sender to encode any message as a first step while the second step hides this code inside image based on Least Significant Bit (LSB). In the other side, the receiver has ability to detect the validity of sender's MAC that he uses the same secret keys to complete the integrity of message at verification phase. Additionally, we also propose a well-organized procedure with respect to probabilistic queries and regular verification to cut down the audit costs per verification phase. Our proposed scheme contains important merits as follows: (1) the service provider and a user can achieve authenticated session's keys; (2) it describes by low cost, simple integration with available infrastructure, and essay to deploy and manage; (3) Our scheme can resist many attacks such as forgery replay attack, insider attacks, and reflection attacks; (4) we propose an efficient scheme for choosing a best parameter value to reduce computational cost of cloud audit services.

The rest of this paper is organized as follows. The necessary primitives and requirements of our scheme exist in Section 2. An overview of related work is displayed in Section 3. Our proposed scheme is presented in Section 4. We detail the security analysis and implementation results in Section 5, and Section 6 concludes the paper.

2. PRIMITIVES AND REQUIREMENT

For more clarity, we show briefly some of the cryptographic primitives that are employed during our construction.

2.1 Least Significant Bit Insertion Approach

LSB insertion scheme is a well-known and simple scheme to embed a secret message in a digital image. In this approach the LSB substitution changes the least significant bit with a confidential bit stream. This method performs well for audio, video, and image steganography. In image sample, a grid for 3 pixels can be showed as follows:

(00101101 00011100 11011100)

(10100110 11000100 00001100)

(11010010 10101101 01100011)

The binary representation of A's letter is 01000001 and we wish to embed into the least significant bits of this segment of the image, the resulting grid is known as follows:

(00101100 00011101 11011100)

(10100110 11000100 00001100)

(11010010 10101100 01100011)

The underlined bits are the only three essentially changed. On average, LSB needs that only half of the bits in an image require being change. As a result, The A's data can hide in the least and second least significant

bits. So, the human eye does not have ability to see the change [6, 7]. Assume that the A's data is to be embedded inside the R-rightmost LSBs of a cover image. We can first recover the rightmost R-bit LSB from each pixel of a cover image and then reorganize the important data to a R-bit by decomposing each pixel. As a final point, the embedding procedure is done by substituting the k-bit rightmost LSBs, and the stego-image is gotten by substituting R-bit with cover image and secret data as viewed in Fig.1. In the extraction phase, we can directly retrieve the important data without any information about a cover image. The R-bit rightmost LSBs of each pixel are picked for the stego-image and lined up to rebuild the important data.

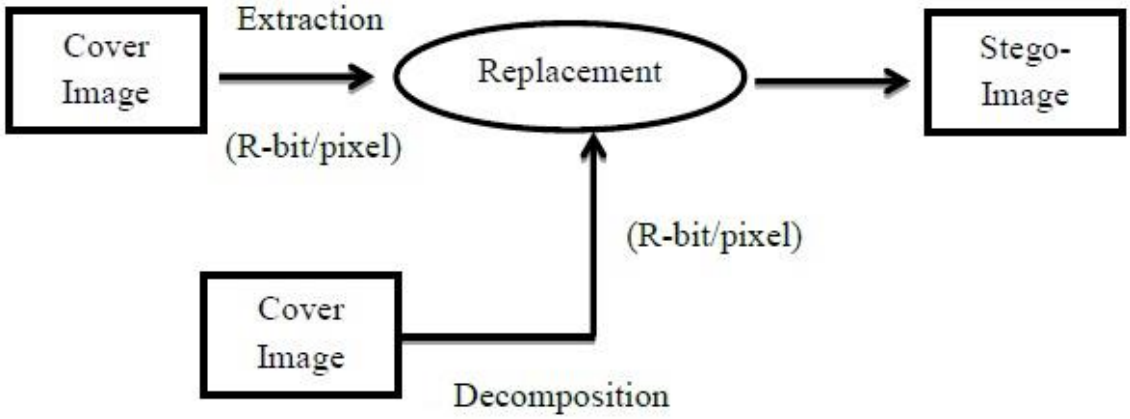

Figure 1. The embedding phase of LSB substitution

2.2 Hash Function

There are several famous and acknowledged hash algorithms such as Message-Digest algorithm (MD), Message-Digest algorithm 5 (MD5), SHA-0, SHA-1, and RIPEMD-160 in information security fields [8]. Now, we briefly review these hash functions:

MD Family: In 1992, Ronald L. Rivest successively presented two hash functions called *Merkle-Damgard* (MD) and its revised version named MD5. In cryptography field, MD5 is used hash function based on 12 -bit hash value as output of this function. The input is worked in 512-bit blocks. Additionally, the MD5 function is aimed to be quite fast on 2-bit machines. Furthermore, it does not limit to use any large substitution tables, here; MD5 have ability to cod quite compactly. MD5 considers slightly more difficult and slower than MD, but it increases the security level in design.

SHA Family: The *secure hash function* (SHA) family is a set of associated with cryptographic hash functions and presented by the *National Institute of Standards and Technology* (NIST). SHA-0 considers the first member of SHA, was issued in 1993. SHA-1 represents as a developed version of SHA-0, was issued in 1995. Four irregular models have been published by NIST with improved output ranges and a marginally different design as follow: SHA-22, SHA-256, SHA-384, and SHA-512. However, SHA-1 runs on digital message blocks contained 512 bits for a 160-bit digest is produced. SHA-1 is considerably sturdier against malicious attacks [5, 8].

3. Releated Work

In [9] authors have presented an adjusted least significant bit spatial domain embedding scheme. This scheme splits an image pixels ranges (0-255) and creates a stego-key. This key has 5 several gray-level ranges of image and each range refers to update fixed number of bits to insert in least significant bits of image. The limitation of their scheme is to hide extra bits of signature with hidden message for its integrity purpose. It also their scheme for color image just to change the blue channel for hide information.

In [10] authors have introduced an adaptive LSB substitution based on data hiding scheme for image. To perform improved visual quality of stego-image it takes care of noise sensitive area for embedding. Proposed scheme differentiates and gets benefit of normal texture and edges part for embedding. This scheme focus to analyze the edges, brightness, and texture masking of the high at non-sensitive image area and over sensitive image region r value stay small to equilibrium overall visual quality of image. The LSB's (r) for embedding is calculated by the high-order bits of the image. Additionally, it also uses the pixel adjustment scheme for enhanced stego-image visual quality through LSB substitution scheme. The experiential results view a good high hidden capability, but dataset for results are limited; there is not a single image which has many edges with noise region like 'Baboon.tif'.

In [11] authors have proposed a high capability of hidden data using the LSB and hybrid edge detection approach. For edge computation two kinds of canny and fuzzy edges detection scheme used and LSB substitution is applied to embed the hidden data. Furthermore, their scheme is effective to embed data with higher *peak signal to noise ratio* (PSNR) with usual LSB depended on embedding mechanism. This scheme is checked on limited images dataset. This scheme is not checked on wide edges based image such as 'Baboob.tif'.

Madhu *et* al. [12] presented an image steganography scheme, based on LSB substitution and choosing of random pixel of required image region. This scheme is target to develop the security where password is inserted by LSB of pixels. It creates the random numbers and picks the area of interest where secret message has to be hidden. Additionally, the strength of this scheme is its security of hiding message in stego-image, but has not represents any kind of perceptual transparency.

Shensheng Yu et al. [13] have suggested an authentication scheme in which content relied on watermark is created from the LL3 factor of three-level Haar wavelet decomposition based on Sobel edge detection technique and then the hash is calculated using MD5 as the main hash function. Additionally, the computed hash is then entrenched in the middle frequency coefficients.

Fridrich and Goljan [14] presented a scheme for self-embedding an image as a scheme of preserving the content of image. Their proposed scheme also permits the regions of the image that have been interfered with, cropped, or changed, to be partially repaired. The main principle of this scheme is to embed a compressed version of the image inside the LSB of image's pixels. The major weakness of this scheme is that embedded information is not strong.

In [15] Ashwin Swaminathan et al. have improved an algorithm for producing an image hash, using Fourier-Mellin transform features which are constant to two-dimensional affine transformations. The method also includes key-dependent randomization into the Fourier-Mellin transform productions to form a secure and strong image hash.

In this paper, we propose a secure scheme and use it to implement a cloud-based message authentication code by using simple cryptographic primitives. Our proposed scheme is armed by high-security level, can withstand the above-mentioned malicious attacks as well, and does not require any cost compare with MACs' schemes. Our proposed scheme based on data hiding technique of image is proposed. This scheme is embedded the bits of MAC using *least significant-bit* (LSB) to enable a large message capacity. Additionally, our proposed scheme includes many security characteristics like user's message anonymity, data integrity for user's message, session key agreement, and one time message code for each user's login. The experimental results view the efficiency and sturdiness of our proposed scheme.

Table 1. Notations of our proposed scheme

Symbol	Definition
$h(.)$	A cryptographic hash function.
CSP	Cloud Service Provider.
n, p, q	Large primes numbers to compute shared key.
S, R	Sender and Receiver.
Sk	Secret key
Im_s, Im_r	CSP sends the sender's image and receiver's image, respectively.
M'	Sender sends Message Authentication Code to the receiver.
M''	Receiver computes Message Authentication Code.
r_i, r_i'	Random number uses to generate one time anonymous message code.
P_i, P_i'	Position of random number that extracted from sender's image and receiver's image, respectively.
$\|\|$	Concatenation function.
Stego-MAC	Covered Image

4. OUR PROPOSED SCHEME

In this section, we present a new message authentication code scheme for cloud environments. The following notations in Table 1 will be used throughout our scheme.

Our proposed scheme is involved with three components, *Cloud Service Provider* (CSP), *Sender* (S), and *Receiver* (R). Our work consists of two phases— Configuration and Verification. Configuration phase is executed only once, and the verification phase is performed whenever a sender/receiver wishes to submitted his message.

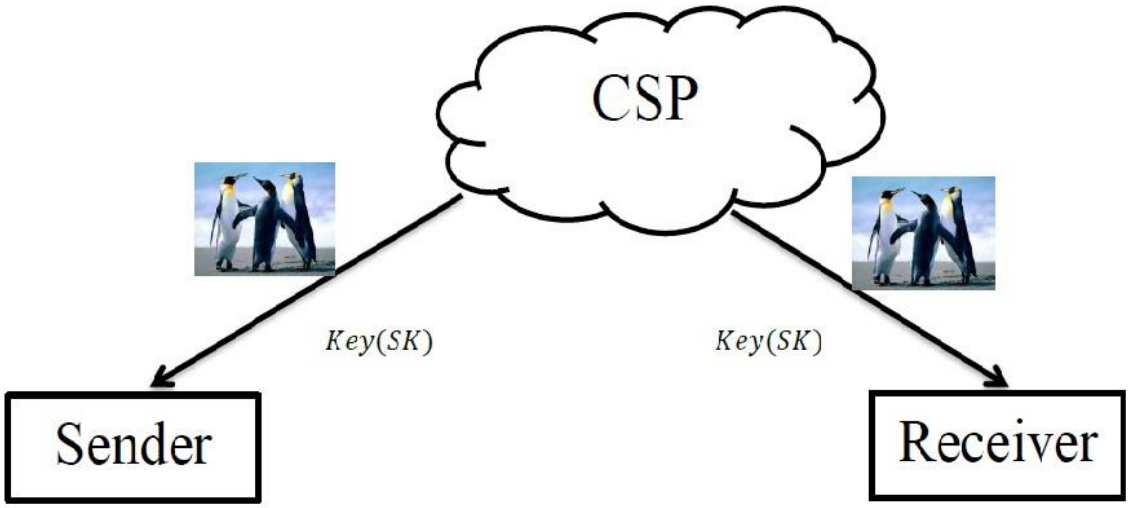

Figure 2. Configuration phase of our proposed scheme

In the configuration phase, the sender and receiver register their identities into *CSP* who provides secret key SK and cover image (Img) to both the sender and receiver in the secure channel. We can describe this step as follows (see Fig. 2).

The main components (CSP, Sender, Reciver) also uses a cryptographic hash functionh(.), symmetric key for crypto-hash function, CSP sets up $n = p * q$; where both p and q are two large primes and secret key is $Sk \in Z_n$. The both *sender* (S) and *receiver* (R) register their identities to the *CSP* through a secure channel.

After that, CSP sends important information (Sk, Im_s, Im_r) to Senders and Receiver, respectively, in the secure channel. After configuration phase, the sender/receiver can use his secret key to complete verification phase.

Verification phase is qualified as follows (see Fig. 3).

1. S $\rightarrow$ R: M, P_i', Stego-MAC. S performs the following steps:
   - Assume sender's message is M.
   - Generate random number $r_i \in Im_s = Im_s(\text{Index})$ and compute one time anonymous message code $M' = h(M||\ Sk||\ r_i)$, (If the sender resends the same message to the receiver or vice versa). Then, S computes the position P_i of r_i from sender's image (see Fig. 4). Finally, he applies the LSB algorithm to hide M' and produce covered image which known Stego-MAC ($M' = h(M||\ Sk||\ r_i)$).
   - Compute $P_i' = P_i \oplus Sk$.
   - Send M, P_i', Stego-MAC to R.
2. R checks the integrity of receiver's message as follows:
   - Compute $P_i'' = P_i' \oplus Sk$ and extract r_i' based on $r_i' = Im_s(P_i'')$. Then, R computes $M'' = h(M||\ Sk||\ r_i')$; he retrieves M' from covered image which is has been called as Stego-MAC by using LSB algorithm to retrieve hidden message M'. Finally, if the M'' matches with M', the Receiver ensures from integrity of message that submitted from the sender and authority of sender. Otherwise, R terminates verification phase.

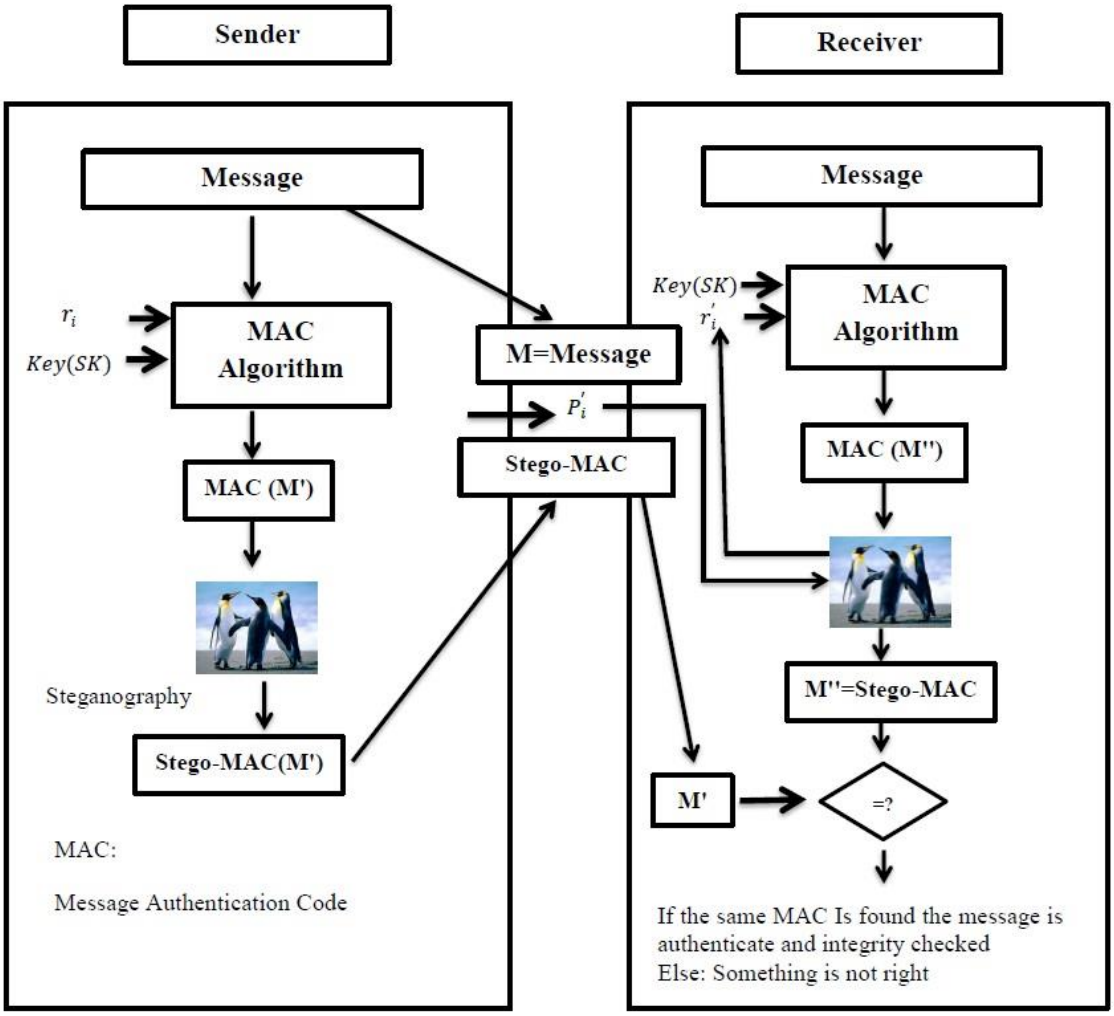

Figure 3. Verification phase of our proposed scheme

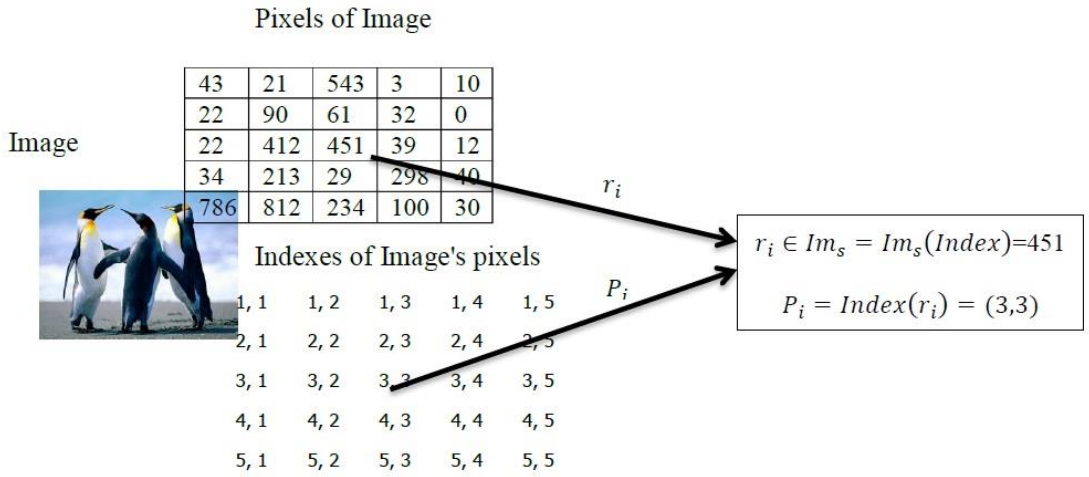

Figure 4 shows the mechanism of computing P_i

5. EXPERIMENTAL RESULTS

In this section, we provide the security analysis of our proposed scheme and performance investigation.

5.1 Security Analysis

We will view that our scheme is secure against replay attack, forgery attack, insider attack, reflection attack, MITM attack, and provides several merits such as one time anonymous message code and session key agreement.

Theorem 1. Our scheme can prevent a replay attack.

Proof. An adversary performs a replay attack by eavesdropping the login message which sent by a rightful sender to the receiver. Then an adversary reuses this message to impersonate the valid sender/ receiver when logging into the system in a next session. In our proposed scheme, each new sender's/ receiver's request should be identical with $CSP's$ keys $(Sk, r_i,\ P_i', Im_s)$. Therefore, an adversary cannot pass any replayed message to the R$'$s verification. Moreover, our work can resist this attack without synchronization clocks. So, our scheme depends on random r_i instead of timestamp and the secret parameters ($r_i,\ P_i'$) are used once for each sender's/receiver's login message request. As a result, an adversary fails to apply this type of attack.

Theorem 2. Our scheme can resist the forgery attack and parallel-session attack.

Proof. If any attacker tries to impersonate sender/receiver, he should be accessed a valid session message $(M, \text{Stego} - \text{MAC}, P_i')$ by using secret parameters $(Sk, r_i, Im_s/Im_r, P_i')$. An attacker does not possess any idea about $(Sk, Im_s/Im_r)$ to compute *(Stego-MAC,* M', P_i'). Thus, our proposed scheme prevents the forgery attack.

Theorem 3. Our scheme can prevent an insider attack.

Proof. In our work, when any user wishes to register with CSP for remote-access services, has to submit his identities information. Due to the utilization of secret key (Sk), authenticated sessions keys (r_i, P_i), and one-way hash function h, they are considered practically impossible for CSP to gain the user's MAC from the cover image *Stego-MAC*. Furthermore, the main values (*Stego-MAC,* M', r_i, P_i) are generated once time for each user's login request. Therefore, even the service provider does not know the user's main values (*Stego-MAC,* M', r_i, P_i). Obviously, our scheme can preclude the insider attack and Cloud service provider impersonation attack.

Theorem 4. Our scheme can resist a reflection attack.

Proof. This type of attack is happen, when a valid user submits his login message to the cloud service provider, the adversary tries to catch user's message and sends it (or an updated version of the message) back to the same user. In our proposed scheme, the adversary fails to cheat the service provider since he cannot use the main values *(Stego-MAC,* P_i) that sent from the sender to the receiver. An adversary fails to use these values again because generate once time for each sender's/ receiver's login request. Thus, our proposed scheme prevents the reflection attack.

Theorem 5. Our proposed scheme can resist the MITM attack.

Proof. This type of attack is intended that an adversary has the ability to intercept the messages between a sender and a receiver. Then, he uses this message when the one entity signs out the cloud service provider. In our proposed scheme, the parameters are securely encrypted and sent from sender to receiver or vice versa. Generation of the random value r_i is through the creation of sensitive data *(Stego-MAC ,* $M', r_i, Im_s/\ Im_r, P_i'$) by the sender as a session request to the receiver. This sensitive data becomes useless when sender/receiver signs-off the CSP. Therefore, an adversary spotting communication between sender and receiver can learn r_i which is used only once; he is unable to compute M' which hides in cover image called *Stego-MAC.* As a result, the proposed scheme can resist MITM attack.

Theorem 6. Our proposed scheme can supply user's message anonymity.

Proof. Assume a sender/receiver tries to resend the same message which has been sent previously. If an adversary attempts to eavesdrop on the sender's login request, he cannot use the same the sender's message authentication code (M') which hides inside sender's image (Im_s) to produce cover image called *Stego-MAC.* At the same time, the sender generates r_i once for each sender's request. So, r_i has been extracted from sender's image ($r_i \in Im_s$) existed just in R and S. Additionally, an adversary does not have main keys ($Im_s,\ Im_r, Sk, r_i$) to compute crypto hash function $M' = h(M, Sk, r_i)$. Hence, it is difficult for an adversary to disclose the sender's message authentication code. Clearly, our proposed scheme can support user's message anonymity.

Theorem 7. The proposed scheme can support Known-key security and session key agreement.

Proof. In our proposed scheme, when the sender sends the his messages to the receiver or vice versa, he uses secret Sk to compute $M' = h(M, Sk, r_i)$. Furthermore, he uses this key to encrypt the position (P_i) of r_i inside sender's image (Im_s). An adversary cannot access to the session keys, he is still unable to get fresh values of Sk which generates at registration phase by CSP. So an adversary cannot get these secret parameters.

5.2 Investigation Performance

In this section, we conduct several experiments for gauging the efficiency and the effectiveness of our work. Figure 5 shows time processing of verification phase. However, the average time for the verification phase of our work is equal to 0.0723 seconds for each user who indicates the high speed of our solution. The estimation parameters are declared in Table 2. The time requirement of our scheme is brief in Table 3. We test the effectiveness in terms of authentication accuracy. We have registered during our experiments 1000 users.

Table 2. Estimation Parameters

Symbol	*Definition*
T_h	Time processing of a hash function.
T_{Xor}	Time processing of Xor function.
T_{Opr}	Time processing of mathematical operations such as multiplication, addition and subtraction.
$T_{\|\|}$	Time processing of concatenation function.

Table 3. Performance of our proposed scheme

Phase	*CSP*	*Sender*	*Receiver*
Setup & Registration	$2T_{OPr}$	-------	-------
Verification	-------	$T_h + 3T_{Opr} + 2T_{\|\|} + T_{Xor}$	$T_h + 3T_{Opr} + 2T_{\|\|} + T_{Xor}$
Total	$2T_{OPr}$	$T_h + 3T_{Opr} + 2T_{\|\|} + T_{Xor}$	$T_h + 3T_{Opr} + 2T_{\|\|} + T_{Xor}$

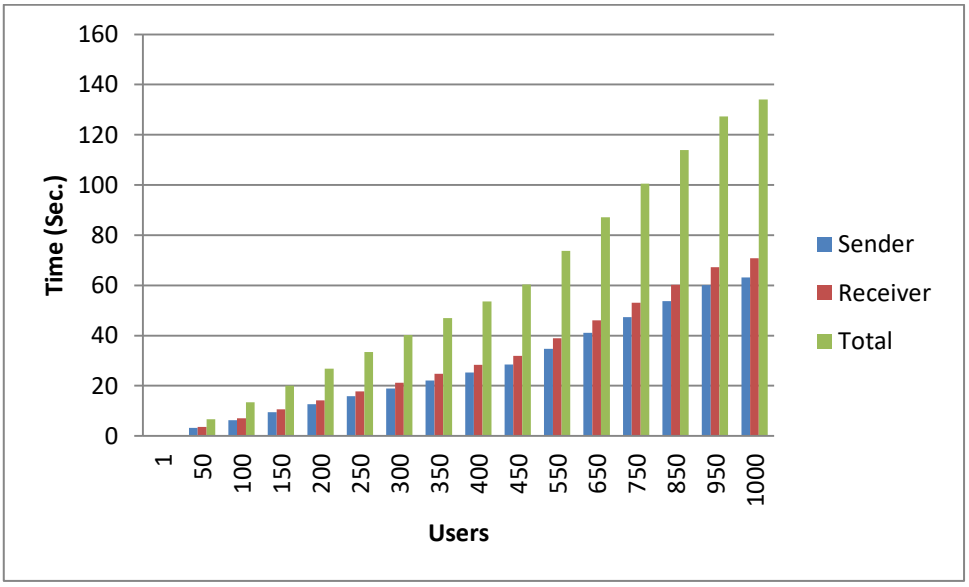

Figure 5 shows the performance of our proposed scheme

6. CONCLUSION

In this paper, a new scheme of using steganography to hide message authentication code is proposed. It is experimentally shown that proposed scheme is more effective than existing scheme. Our proposed scheme aims to support more flexibility and to resist familiar attacks. These vital merits include (1) our proposed scheme provides a secret MAC between the sender and receiver; (2) it achieves one-time message anonymity; (3) Using image as a secret factor to extract secret keys that making an adversary fails to obtain main keys; (4) our proposed scheme uses LSB algorithm to hide MAC that makes the task of an adversary more hardly. Moreover, our scheme can resist MITM attacks, replay attacks, and forgery attacks. The results showed that the proposed scheme has a very good hidden invisibility, good security and robustness for a lot of MAC attacks. The proposed scheme is better in security and capacity as shown experimentally than existing schemes.

REFERENCES

[1] S. Subashini, V. Kavitha, A survey on security issues in service delivery models of cloud computing, Journal of Network and Computer Applications , Vol. 34, no.1, pp. 1-11, 2011.
[2] D. Zissis, D. Lekkas, Addressing cloud computing security issues, Future Generation Computer Systems Vol. 28, pp. 583-592, 2012.
[3] Md. T. Khorshed, A.B.M. S. Ali, S. A. Wasimi, A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing, Future Generation Computer Systems, Vol. 28, pp. 833-851, 2012.
[4] K. Matusiewicz, Analysis of Modern Dedicated Cryptographic Hash Functions, PhD thesis, Macquarie University, 2007.
[5] R.L. Rivest. The MD message digest algorithm, In S. Vanstone, editor, Advances in Cryptology - CRYPTO' 10, LNCS 5 , pp. 0 - 11, 2011.
[6] S. Gupta, G. Gujral, N. Aggarwal, Enhanced Least Significant Bit Algorithm For Image Steganography. International Journal of Computational Engineering & Management, Vol. 15, no. 4, 2012, July.
[7] V. O. Waziri, Steganography and Its Applications in Information Dessimilation on the Web Using Images as Security Embeddment: A Wavelet Approach. International Journal of Computer and Information Technology, Vol.1, no. 2, 2012, November.
[8] W. Stallings, Cryptography and Network Security: Principles and Practices. 2nd ed. Prentice Hall International, 2010.
[9] Y. K. Jain and R. R. Ahirwal, A Novel Image Steganography Method With Adaptive Number of Least Significant Bits Modification Based on Private Stego-Keys, International Journal of Computer Science and Security (IJCSS), vol. 4, 2010, March.
[10] H. Yang, X. Sun and G. Sun, A High-Capacity Image Data Hiding Scheme Using Adaptive LSB Substitution", Journal: Radioengineering, Vol. 18, no. 4, pp. 509-516, 2009.
[11] W. J. Chen, C. C. Chang and T. H. N. Le, High Payload Steganography Mechanism Using Hybrid Edge Detector, Expert Systems with Applications (ESWA 2010), vol. 37, pp. 3292-3301, 2010, April.
[12] V. M. Viswanatham, J. Manikonda, A Novel Technique for Embedding Data in Spatial Domain, International Journal on Computer Science and Engineering, vol. 2, 2010.
[13] S. Yu, Y. Hu and J. Zhou, "Content-based watermarking scheme for image authentication," in Proc. of the 8th International Conference on Control, Automation, Robotics and Vision, pp. 1083-1087, Kunming, China, 2004.
[14] J. Fridrich, M. Goljan, Protection of Digital Images Self Embedding, Symposium on Content Security and Data Hiding in Digital Media, New Jersey Institute of Technology, New York, NJ, USA, 1999.
[15] A. Swaminathan, Y. M. Wu, Robust and secure image hashing, IEEE Transactions on Information Forensics and Security, vol. 1, no. 2, pp. 215-229, 2006.