International Journal of Security and Its Applications
Vol.9, No.2 (2015), pp.179-188
http://dx.doi.org/10.14257/ijsia.2015.9.2.17

Secure Password Transmission for Web Applications over Internet using Cryptography and Image Steganography

Mehdi Hussain[1,2], Ainuddin Wahid Abdul Wahab[1,], Ishrat Batool[3] and Muhammad Arif [1]

[1]*Faculty of Computer Science and Information Technology, University of Malaya 50603 Kuala Lumpur, Malaysia*
[2]*School of Electrical Engineering and Computer Science, National University of Sciences and Technology, Islamabad Pakistan*
[3]*Foundation University, Rawalpindi Campus, Pakistan*
[1]*mehdi141@siswa.um.edu.my,* [2]*ainuddin@um.edu.my,*
[3]*ib4941@gmail.com,* [4]*arifmuhammad36@siswa.um.edu.my*

Abstract

The significance of digital information security has been enhanced due to the boost of internet communication. Providing security for server client communication over the internet is a critical issue due to open world digital eavesdroppers. Generally, password authentication is required for establishing a connection between server and client environment. The client password is verified by the server ends to establish a valid connection. Successful password verification initiates the client and server to perform further secured request and response mechanisms. The problem of password authentication over insecure networks presents in many application areas, such as web login, remote logins of computer networks. Hence the significance of confidential password transmission over insecure internet becomes the necessity of secure authentication. In this paper, we proposed a secure password transmission over the internet for authentication of server/client environment using encryption and image steganography. Client password is first encrypted and embedded in an image using steganographic algorithm at client side and transmitted over unsecured network to the web server. On the other side server extract safely password from image steganography decoding algorithm, decrypt and verified it's with SQL database server. In case if the intruder steals the image over network he/she will be unable to decode the password from the image. The prototype of the proposed method is implemented using JavaScript, Html, and ASP.net for verification purpose.

Keywords: *Secure password transmission; secure authentication using Image; Steganography and Cryptography; Password over unsecure network*

1. Introduction

Due to the internet availability and growth in the last decade, it opened the door of many research domains one of them is information security. Information security is playing a vital role in many sectors such as banks, private, government corporate data, hospitals and e-commerce data over the internet. Generally all of the above communications are dealt in server client environment. Providing security for server client authentication over the internet is a critical issue due to open world digital eavesdroppers.

Generally, a client server environment is a model of computing of a distributed application structure that partitions tasks or workloads between the providers of a resource or service, called servers, and service requesters, called clients. One of the best forms of the client server model is the internet. Internet includes many types of application such as Websites, Web servers, FTP clients and servers, and DNS. Where the client is known as a

ISSN: 1738-9976 IJSIA

web browser such as internet explorer and chrome are typically used as a client to interact with websites which resides on internet servers. Generally this interaction requires an authentication of client and server environment.

Password authentication is one of the simplest and the most convenient authentication mechanisms over insecure networks. It provides the legal users to use the resources of the remote systems. Many Internet applications are based on password authentication, for example, remote login, government organizations, private corporations, database management systems and cloud storage servers systems. However, the current Internet environment is vulnerable to various attacks such as replay attack, guessing attack, modification attack, and stolen verifier attack. Therefore, a number of researchers have proposed several password authentication schemes for secure login of legal users.

In today's research major challenge is implementing a good authentication scheme which should maintain the equilibrium between security, integrity and availability. Also provides rich usability functionalities on an authentication scheme is a necessity in modern unsecured network contexts.

In this paper, we propose a novel method of secure password transmission over internet for authentication using cryptography with image steganography. Password on the client web browser is first encrypted and embedded in an image using steganography method, secondly transferred over an insecure network (internet) to the server machine. For experimental results, this encryption and embedding procedure is implemented in JavaScript of the client browser end. On the other side server receives that image and extracts the encrypted password from stego-image and decrypt the message and verified with its backend SQL database server. Section II discussed the background of Steganography and Cryptography. Section III discussed the Literature review and motivation. Section IV consists of the proposed model. Section V detailed discussion strength and limitation of the proposed model.

2. Background

2.1. Steganography

Steganography word is originated from Greek words Steganós (covered), and Graptos (writing) which literally means "cover writing" [1]. Generally steganography is known as "invisible" communication. Steganography means to conceal messages existence in another medium (audio, video, image, communication).

Steganography means is not to modify the structure or layout of the secret message, but hides it inside a cover-object (carrier object) [2]. After hiding process cover object and stego-object (carrying hidden information object) are similar. So, steganography (hiding information) and cryptography (protecting information) are totally different from one another. Due to invisibility or hidden factor, it is difficult to recover information without known procedure in steganography. Detecting procedure of steganography known as Steganoanalysis.

2.1.1. Image Steganography Terminologies

Image steganography terminologies are as follows:

- Cover-Image: Original image which is used as a carrier for hidden information.
- Message: Actual information which is used to hide into images. Message could be a plain text or some other image.
- Stego-Image: After embedding message into a cover image is known as stego-image.

- Stego-Key: A key is used for embedding or extracting the messages and stego- from cover-images images.

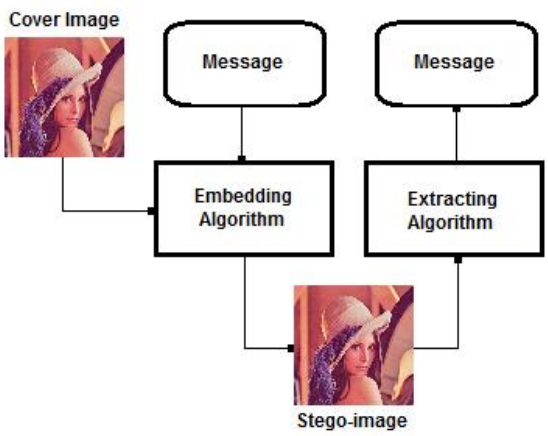

Figure 1. Basic Image Steganography Diagram

Generally image steganography is method of information hiding into cover-image and generates a stego-image. This stego-image then sent to the other party by a known medium, where the third party does not know that this stego-image has hidden message. After receiving stego-image hidden message can simply be extracted with or without stego-key (depending on embedding algorithm) by the receiving end. Basic diagram of image steganography is shown in Figure-1 without stego-key, where embedding algorithm required a cover image with message for embedding procedure. Output of embedding algorithm is a stego-image which simply sent to extract algorithm, where extracted algorithms can unhide the message from stego-image.

2.1.2. Basic LSB example of Steganography

The least significant bit (in other words, the 1st bit) of some or all of the bytes inside an image is changed with a bit of the secret message. For example a grid for 3 pixels of an 8-bit image can be shown as follows with its binary representation:

45 28 220
(00101101 00011100 11011100)

If the secret number 5, which binary representation is 101, is embedded into the least significant bits of this part of the image, the resulting grid is as follows:

45 28 221
(00101101 00011100 11011101)

Although the number 5 was embedded into the 3 pixel bytes of the image, only the 3 underlined bits needed to be changed according to the embedded message.

There are many latest image steganography algorithms such as object based embedding; Pixel value differencing, hiding data considering visual quality of image or etc. are as follows [3, 4, 5, and 6]. But in our scheme we adopted a low computation complexity simple

LSB [1] steganography algorithm due to real time JavaScript code running in web browser at client end.

2.2. Cryptography

Generally protection of sensitive information is achieved through encryption. Cryptography is a science of secret writing. It is an ancient art. The word cryptography derives from the ancient Greek (kryptos and graphein) word that means hidden writing [7]. It transforms the appearance of original message without changing its information content.

2.2.1. Cryptography Terminologies

- Plaintext: Message or actual data to encrypt.
- Ciphertext: Comes to different representation of plaintext, unintelligible form of plain text.
- Encryption: Algorithm, which convert the plaintext to ciphertext.
- Decryption: It transforms the ciphertext to the plaintext format.
- Key: Secret key (numerical value or alpha numeric or alpha only) is used in encryption and decryption of data.

Therefore, cryptography is used to encrypt and decrypt data. It conceals and retrieves information with a given secret key. Figure-2 shows the basic diagram of cryptography model. It consists of two broader classifications; symmetric and asymmetric.

2.2.2. Private or Symmetric-Key Cryptography

It is also known as symmetric key cryptography. In symmetric key cryptography, both the sender and the receiver have the same secret key. Single key is used for encryption and decryption by sender and receiver end. Figure-2 shows the Secret key cryptography.

2.2.3. Asymmetric-Key Cryptography

It is also known as asymmetric encryption; it uses two keys one for encryption and second for decryption. In public key cryptography, both keys work in pairs of public and private keys. Sender uses the public or known key of receiver to encrypt the message and receiver decrypt the message with his/her private or secret key.

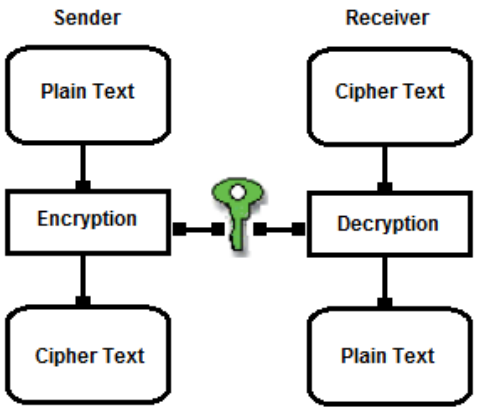

Figure 2. Basic Cryptography Diagram

3. Literature Review

Generally, there are many different proposed methods available, which used image steganography for authentication but for different purposes. In [8] authors proposed a model where GPS location information is embedded in the GPS image to prove the identity of GPS location with GPS image itself. This embedding GPS location proves the authenticity of GPS image. Similarly, in [9] authors proposed a personal biometric information embedding in images for authentication of online shopping system using image steganography.

For securing the internet traffic for different application purposes there are numerous services such as Secure Socket Layer (SSL), Secure Electronic Transaction (SET), and Visa Payer Authentication Service (3D Secure). Most popular internet standard SSL plays a vital role in web data communication. This SSL protocol used to provide secure access to websites. It often used a combination of public key and private key technology. This private key encryption (also called symmetric encryption) is faster, but public key (also called asymmetric encryption) provides more secure authentication. So this SSL is designed to take the advantages of both public and private encryption methods. Different Internet browser is known by Microsoft. Google, Mozilla and other provide the support of SSL, and also most web server software, such as IIS and Apache also provides the support of it.

Basic internal working of SSL is based on digital certificates. There are two types of digital certificates, one for the client end and other for the server end. Generally server and client verify their identities before establishing a connection for future communication. This identity verification process used their digital certificates. This process is commonly referred to as mutual authentication.

Further advantages and limitation of the above security transaction/transmission authentication protocol are discussed in [10, 11, 12, and 13]. Following major strategic points demands to explore a new way of secure communication method.

- The above SSL, SET, 3D Secure traffic transmission itself shows their existence identity over network.
- For achieving secure communication they required maintenance of digital certificates.
- Extra initial handshake communication required over unsecure network.
- Ideal service provider likes less traffic, because want to entertain as much as requests of different clients and servers.
- Intruder can identify its traffic over unsecure network for investigation.
- May need special software to be installed in the customer machine.

This SSL only cryptographic solution is not fully ideal for secure authentication due to above reasons. To the best of our knowledge, there is no such system to transmit the password for authentication using image steganography for web authentication. We need to develop a new secure password based authentication system for unsecured network to consider the above deficiencies.

4. Proposed Model

In this section, we proposed a secure password transmission over untrusted network using password encryption and then embedding into images using steganographic algorithm. Generally when user interested to login to the server for accessing its resources, then user

name and password are required by server to verify the authentication of legitimate user. Algorithm is as follows.

Step 1: Fetch the user name and password from client page.

Step 2: Run the JavaScript callback code against Login button.

a) Encrypt the password characters as 'EncPass'.

b) Load the *.bmp image (64x64) into JavaScript array buffer.

c) Apply and embed the 'EncPass' data using basic LSB steganographic algorithm on loaded image data buffer knows as 'StegImg'.

d) Apply the base64 encoding on StegImg and 'StegBase64' data produced.

Step 3: Add the 'StegBase64' as an image data into html request form tag for server.

/* after successfully receiving the requested form data from client */

Step 4: Server fetch the 'StegBase64' data from requested form data.

Step 5: Decode 'StegBase64' data using ASP.net, and resultant 'StegImg' retrieved.

Step 6: Extract 'EncPass' data from 'StegImg' after applying the basic LSB steganographic algorithm.

Step 7: Decrypt the 'EncPass' and get the actual password.

Step 8: Search actual password with username into SQL database server for verification.

Step 9: If password and username matched then client consider as legitimate user for login otherwise rejected the request.

Example code.

```
<script src="…/secureAuthentication.js"></script>
<script>
   <!- User password with key is encrypted by CryptoJS library -->
    var EncPass     = CryptoJS.AES.encrypt("Password", Key);

   <!- LoadImgBuffer function load the temporary buffer for processing-->
    var CoverImg    = LoadImgBuffer();

   <!-  Apply LSB embedding for testing the framework  -->
    var StegImg     = SteganoJS.Embedd.LSB(CoverImg, EncPass, NULL);
```



```
    <!- Encode the stegImg data into base64 for sending regular image in
          image tag of form data. -->
     var StegBase64  = base64EncArr(StegImg);


    <!- Update the src buffer of image tag. -->


    UpdatetheSrcImgBuffer(StegBase64);
</script>
```

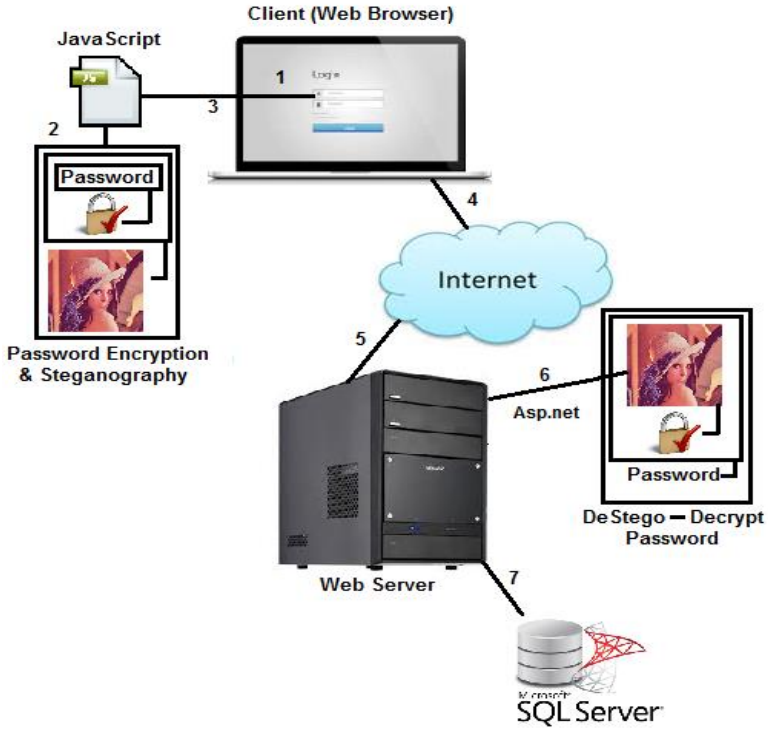

Figure 3. General Flow of Proposed Method

5. Dissuasion

Figure-3 shows the complete flow of requests and responses between client and server ends are depicted. In our case, user enters its user name and password into the client browser, a JavaScript code run on client machine to encrypt password characters [14], secondly prepare the image buffer (BMP 64x64 size) into the memory and then embed the encrypted password into image data using basic LSB method [15]. After embedding the data into images from JavaScript call back function further encode it into the base64 data format. This base64 data further sent to the server end as a regular image tag.

On the other side server retrieves the request from the client end. It fetches the image tag data (in base64 format) for further processing. This base64 encoded data decoded by base64 decoder using ASP.net on the server end. Apply the de-stego algorithm on image data and extract the encrypted password, secondly that encrypted password further decrypted and finally retrieve the actual password. This actual password is further used to match with SQL Database server for verification purpose against its user name. If actual password matched with the user name database then server generates the response signal to the client as a legitimate user otherwise forbade for further processing.

According to the proposed model, we notice the computation complexity is quite high due to image data manipulation for both client and server ends, but the security level is high due to multi-layer secure method over untrusting networks. In case, if any intruder monitors or fetches the request and responses of communication between server-client he/she are unable to find the password for authentication due to image steganography and further encryption of the password. Server and client already synchronized by encryption and steganographic algorithms before handshaking.

5.1. Advantages of Proposed method

Advantages of proposed methods are as follows to considering the transmission of password over unsecure network.

- Proposed method provides protection against current attacks to retrieve password over network.
- Secure the user password over untrusted network.
- Authentication information would be hidden in innocent carrier.
- Intruder would be unable to identify the actual data for attack.
- Minimum initial handshaking required for ideal service provider context.
- Take the steganography advantage in authentication.
- If incase intruder identify the traffic data but unable to extract the authentication information due to steganography with encryption.
- No need of extra software installation on client machine.

6. Conclusion

In the proposed method, we design a secure password transmission for authentication of web application over unsecured internet using encryption with image steganography. To achieve experiments results, for sending and securing passwords, used encryption and steganography algorithms in JavaScript at the client end. On the receiving end (the server side) also implemented above algorithm in ASP.Net, which further extracts the password from stego-image and verifies it with the SQL database server. The main target of the proposed scheme is to secure the password for authentication in server/client environment in multi-layer security such as encryption, and further encrypted password embedded in image using steganography. In case, if the intruder steals the image over network he will still not be able to decode the password from the image file. The computation complexity for both client and server ends is increased due to image data manipulation, but proposed scheme provides much security over conventional methods. Future work investigation is two folded. First to send all web page critical information in embedded images over an insecure network. Secondly, we will investigate in future, to design a random image selection usage strategy for communication in the server client.

Acknowledgements

I would like to thank the National University of Science and Technology (NUST) of Pakistan for supporting and funding research under Faculty Development Program 2014.

References

[1] Anderson, R. J. Stretching the limits of Steganography, in Information Hiding, Springer Lecture Notes in Computer Science, Vol. 1174, (**1996**), pp. 39-48.

[2] Mehdi Hussain and Mureed Hussain, A Survey of Image Steganography Techniques, International Journal of Advanced Science and Technology Vol. 54, May (**2013**).
[3] W. Luo, F. Huang, J. Huang, Edge adaptive image steganography based on LSB matching revisited, IEEE Transactions on Information Forensics and Security 5 (2) (**2010**) 201–214.
[4] Hussain, M. Hussain, M, Pixel intensity based high capacity data embedding method, IEEE International Conference Information and Emerging Technologies (ICIET), Pakistan, June (**2010**).
[5] Hussain, M. and Hussain, M, Embedding data in edge boundaries with high PSNR, Proceedings of 7th International Conference on Emerging Technologies (ICET 2011), pp.1-6, Sept (**2011**).
[6] Mehdi Hussain, M. Hussain, Information hiding using edge boundaries of objects, International journal of security and application, (**2011**).
[7] S. William, Cryptography and Network Security: Principles and Practice, 2nd edition, Prentice-Hall, Inc., (**1999**).
[8] Mei-Yi Wu , Chuan-Chi Hsu , Jia-Hong Lee, A GeoTagging Scheme Using Image Steganography and GPS Information Authentication , Proceedings of the 2009 Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, p.1245-1248, September 12-14, (**2009**).
[9] A. Ihmaidi, Hussam Ud-DIN, Ahmad Al-Jaber, and Amjad Hudaib. Securing Online Shopping using Biometric Personal Authentication and Steganography. Conference on Information and Communication Technologies. IEEE, (**2006**).
[10] Jewson R., E-payments: Credit Cards on the Internet, Aconite White paper, Oct (**2001**).
[11] Anderson R., Security Engineering A Guide to Building Dependable Distributed Systems. WILEY Computer Publishing, (**2001**).
[12] Wolrath C., Secure Electronic Transaction: a market survey and a test implementation of SET technology, Master Thesis, UPPSALA University. (**1998**).
[13] Visa International,. 3-D Secure Introduction, Visa International Service Association, (**2002**).
[14] Open source JavaScript library for encryption, https://code.google.com/p/crypto-js/downloads/detail?name=CryptoJS%20v3.1.2.zip
[15] Open source JavaScript image steganography, http://www.peter-eigenschink.at/projects/steganographyjs/

Authors

Mehdi Hussain received his BS degree in Computer Science from The Islamia University Bahawalpur, Pakistan in 2005. He obtained his MS degree in Computer Science from SZABIST Islamabad 2011 Pakistan. He has 8 years working experience in a renewed Software House (Streaming Networks (private)). He recently selected as funded scholar at National University of Science and Technology (NUST) under faculty development program 2014. Presently he is research scholar at University of Malaya, Malaysia. Research interests are multimedia security, steganography. He can be reached at *mehdi141@hotmail.com*.

Ainuddin Wahid Bin Abdul Wahab received his BCompSc and MCompSc degree from University of Malaya, Malaysia. He obtained his Doctoral Degree (PhD), from SURREY UNIVERSITY, SURREY, UK (Multimedia Network). He is Senior Lecturer in Department of Computer System & Technology, Faculty of Computer Science & Information Technology University of Malaya Malaysia. His research interests are Security Services Sn: Digital Forensic, Steganography, Network Security.Public Key Infrastructure and Biometrics (Information Hiding, Digital Forensic). He can be reached at ainuddin@um.edu.my.

Muhammad Arif is a PhD student at Faculty of CS and IT, University of Malaya. Currently he is working on Medical image Processing. His research interests include image processing, E learning, Artificial intelligence and data mining. He joined UM as a Bright Spark Scholar in September 2013 for the period of 3 years. Before this he completed masters and bachelor degrees in Pakistan. He received his BS degree in Computer Science from University of Sargodha, Pakistan in 2011. He obtained his MS degree in Computer Science from COMSATS Islamabad 2013 Pakistan.