Issue 9 vol 3 ISSN: 2321-8134

IJFEAT

INTERNATIONAL JOURNAL FOR ENGINEERING APPLICATIONS AND TECHNOLOGY

IMAGE STEGANOGRAPHY FOR IMPROVING SECURITY AUTHENTICATION SYSTEM

Jitendra H. Saturwar[1], Sanyukta V. Pachkawade[2], Rushikesh A. Vyas[3], Avadhut A. Mendhe[4]

[1]*Associate Professor, Dept of CSE* , J.D.I.E.T, Yavatmal, Maharashtra, India, **jsaturwar@gmail.com**
[2]*Student, Dept of CSE*, J.D.I.E.T, Yavatmal, Maharashtra, India, **sanyukta18196@gmail.com**
[3]*Student, Dept of CSE, J.D.I.E.T, Yavatmal, Maharashtra, India,* ***rishikeshvyas7@gmail.com***
[4]*Student, Dept of CSE, J.D.I.E.T, Yavatmal, Maharashtra, India,* ***avadhut8633@gmail.com***

Abstract

Authentication provides security to any system. In this digital world, confidential information on the mobile platforms has challenging task for the specialists. One of the authentication techniques is a textual password based. Texual password uses authentication system for providing security in system. If user tends to choose some meaningful word from dictionary then it is easy to crack or by using the brute force attack, it makes textual passwords vulnerable to dictionary and easy to break. To overcome this drawbacks, a new authenticate technique is proposed in order to provide for more security authentication system. The textual password will be hidden in an image using image-steganography technique. Steganography is used to hide secret information in some harmless carrier. The most basic and important image steganography technique is Least Significant Bit (LSB) embedding technique. Data can be hidden in the least significant bits of the cover image. So the human eye would be unable to notice the hidden image in the cover file. LSB steganography is combined with AES cryptography to hide textual password, in order to provide high level security on authentication system that run on mobile platform.

Index Terms:- *Authentication; Least Significant Bit (LSB); cryptography; Advanced Encryption Standard (AES); digital signatures; Android.*

---------- *** ----------

1. INTRODUCTION

Digital technology has changed people's daily activities, having a major impact by using information in all spheres of its existence. After rapid growth of the Internet, Mobile Networks and Social Media, nowadays the development of more security and high performance Authentication System on mobile devices are increase dramatically. Newly developed technologies make easier and cheaper access, processing, storing and transmitting of information. In this ever changing and evolving environment, establishing secure communication on Authentication System. It is an important target for researchers to secure Authentication System within certain authentication techniques. Textual password based is a one of the authentication techniques. In this the textual password commonly follows an encryption algorithm to provide security. This techniques has some limitations and drawbacks. Users tend to choose meaningful words from dictionaries, which make textual passwords easy to break and vulnerable to dictionary or brute force attacks. To overcome the drawbacks, a new authenticate technique is proposed in order to provide for more security authentication system using cryptography and steganography techniques[1].

Information confidentiality, integrity and authenticity can be ensured by implemented steganography and cryptography. Steganography hides the secret information in different carriers in such a way it becomes difficult to detect. Cryptography uses encryption to scramble the secret information. Commonly the carriers are media files (like images, audio, video) or other supports like communications protocols; an example is network steganography . It contents some embedded bits, which are inserted to it by the process of steganography. Both technologies have their limitations and this is why most of the specialists sustain that a good solution for securing the digital information is to combine the two techniques . All information stored in encrypted manner.

2. PROPOSED WORK

Image steganography which has drawn attention of researchers because of its applicability in today's digitalized world. There are many applications in this direction mainly developed on computers running different operation systems. Regarding Android for mobile phones, there are few reliable projects on steganography. An approach in steganography that drawn our attention is a project SmartSteg, an application Android based that uses LSB steganography. Different with the most of the applications that exist on Android smart phones, these apps can embeds the hidden information in entire files [2].

Other approach uses Android based apps LSB steganography with AES encryption to hide a short text message in an image and then share that message via the Multimedia Messaging Service (MMS)[6].

MoBiSis is an application that implements a steganographic algorithm . It is able to send the image that covers the secret message via the Multimedia Messaging Service (MMS). The cover image can be retrieved from the device's message inbox. The disadvantage of this application is the size of the cover image with the secret message embedded which must be less than 30 Kb [4].

Similar applications with MoBiSiS having the same limitations which are MobiStego and Pixelknot both available on Google Play. It is worthwhile to mention that the aforesaid works still focusing on theoretical grounds of information hiding. Nevertheless, how to employ stegano-Image under Android for practical applications

2.1 Steganography :

In steganography the data are hidden in a cover image so that other persons will not notice that such data is there. Steganography can also be defined as a technology of hiding messages inside some harmless carriers to shelter the communication so that the outsiders may not discover the existence of information in the carrier. Steganography is mainly applied to media such as text, images, video clips, music and sound. This is using Secret Key Steganography. As shown in Figure 2.1, Secret key Steganography is another process of Steganography which uses the same procedure other than using secure keys. It uses the individual key for embedding the data into the object that is similar to symmetric key. For decryption, it uses the same key which is used for encryption. This type of Steganography provides better security compared to pure Steganography. The main problem of using this type of steganography system is sharing the secret key. If the attacker knows the key, it will be easy to decrypt and also access original information .

Fig-2.1.Secret Key Steganography

2.2 Least Significant Bit(LSB) :

The most basic but important image Steganographic Technique is Least Significant Bit embedding technique. This technique can be used for hiding images in 24-bit, 8-bit or gray scale format. In this, least significant bit of each pixel is replaced with secret message bit until message end. Data can be hidden in the least significant bits of the cover image and the human eye would be unable to notice the hidden image in the cover file. When using a 24-bit image we can store 3 bit in each pixel by changing a bit of each if the red, green and blue color components[1].

An 800 x 600 pixel image can store 1,4400,00 bits or 180,000 bytes of embedded data. For example a 24 bit can be as follows:

Pixel 1: (10110101 01101100 10101101)
Pixel 2: (10110110 11001101 00111110)
Pixel 3: (10110101 01100011 10001110)

The number 150 which binary representation is 10010110. This get embedded into the least significant bits of this part of the image, the resulting grid as follows:

Pixel 1: (10110101 01101100 1010110**0**)
Pixel 2: (1011011**1** 1100110**0** 0011111**1**)
Pixel 3: (1011010**1** 0110001**0** 10001110)

Although the number is embedded into the first 8 bytes of the grid, only the 5 bold underlined bits need to be changed according to the embedded message. In LSB Technique, consecutive bytes of the image data from the first byte to the end of the message are used to embed the information. But this approach is very easy to detect. A more secure system can be in which the sender and receiver share a secret key that specifies only certain pixels to be changed. Even if the intruder suspects that LSB steganography has been used, there is no way of knowing which pixels to target without the secret key. On an average, only half of the bits in an image will need to be modified to hide a secret message using the maximum cover size. There are 256 possible intensities of each primary color, so, changing the LSB of a pixel results in small changes in the intensity of the colors. These changes cannot be perceived by the human eye, thus the message is successfully hidden. If the message is hidden even in the second to least significant as well as in least significant bit then too no difference is seen in the image. In its simplest form, LSB makes use of BMP images, since they use lossless compression.

2.3 Authentication System :

Basically all authentication techniques are working on two types of scheme.

2.3.1 Recall Base:

Textual can be considered as an example of recall based Scheme. To secure system, the user creates a password for a system. Strong Textual Password can secure a system at certain level but it is difficult to memorize.

2.3.2 Recognition Base:

In Recognition base scheme user is required to identify and recognize his/her password which was created by him/her. Biometrics authentication includes fingerprint, palm prints, face recognition, voice recognition, retina recantation etc. Problem with graphical password is shoulder surfing attack. Biometrics base authentication technique is also part of recognition scheme. In biometrics technique record or replay attack as well as hill climbing attack is also possible. In Token base authentication there is possibility of fraud, loss, and theft. Textual password is best example for knowledge base technique.

2.4 LSB-AES Encryption :

The aim of this study is to hide the data over an image with Least Significant Bit steganographic algorithm and before hiding in an image, it performs AES encryption on it. Then using that stegano-image as a digital key to login password in an Authentication System on Android mobile device with MySQL database. To store the user data on database this application is using MySQL database which the structure as shown below:

TABLE I. TABLE DATA STRUCTURES

No.	Fields Name	Data Type	Size	Information References
1	username	varchar	1000	Primary Key
2	password	varchar	1000	-
3	email	varchar	1000	-

During interchanging data well formatted and structured data is required. JSON parsing is good and well structured, light weight and easy to parse. Usually most of the application requires to interchange data from server. Hence, this application using Android JSON parsing to interchanging data from MySQL database. JSON is an acronym for JavaScript Object Notation, a lightweight text - based open standard designed for human - readable data interchange.

Derived from the JavaScript scripting language for representing simple data structures and associative arrays is called as objects. The official Internet media type for JSON is application/ json. The JSON

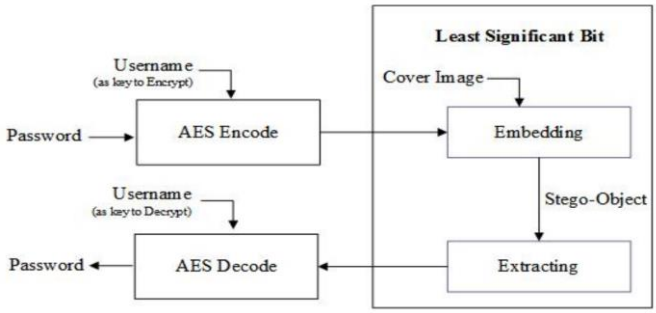

Fig-2.2. LSB-AES Encryption Data Hiding Pattern

format is often used for serializing and transmitting structured data over a network connection.The data hiding patterns using the Least Significant Bit steganographic technique in this project can be explained using this simple block diagram as shown inFigure 2.2. There are 2 process algorithm in this Secure Authentication System application:

2.4.1 Sign Up - Embedding Password Algorithm:

These algorithms are used to hide the user password and a secret message into the image, so the user will no longer need to write down their password, just by simply choose key images that had been embedded as a replacement password. First user choose a username and password that will be used and an image file as a carrier media to hide secret message. The result of this process is an image embedded of the secret password, username and secret message corresponding made by the user. Figure 2.3 represents the activity diagram for embedding password algorithm[1].

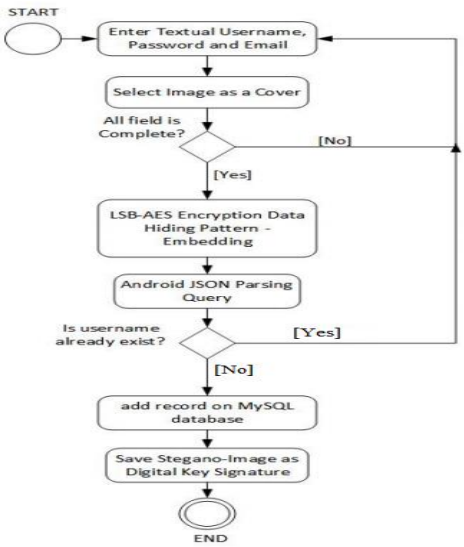

Fig-2.3. Embedding Password Algorithm

2.4.2 Sign In – Extracting Password Algorithm:

These algorithms are used to reveal the user password and a secret message by extracting the secret image. Then this Android application would be searching the username, password and a secret message in database using Android JSON Parsing to retrieve data from MySQL Database. As the outcome of this process if there is found a match combination of username, password and secret message, then the

status "access granted" will be given. Figure 2.4 represents the activity diagram for extracting password algorithm.

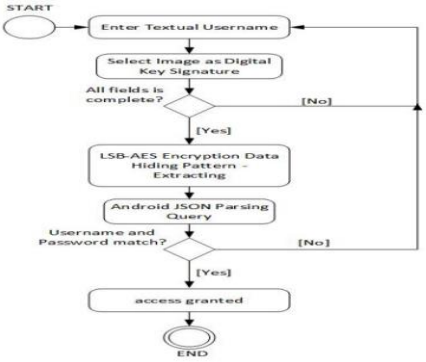

Fig-2.4. Extracting Password Algorithm

3. RESULTS

3.1 Mean Square Error (MSE):

Mean Square Error is the measurement of average of the square of errors. Mean Square Error is the cumulative squared error between the stego and the original image. The error indicates the distortion in an image. MSE can be calculated by using the following 2-D mathematically equation:

$$MSE = \left(\frac{1}{2}\right)^2 \sum_{i=1}^{M} \sum_{j=1}^{N} X_{ij} - Y_{ij} \quad \text{--(1)}$$

Where, X_{ij} = The value of pixel in cover image

Y_{ij} = The value of pixel in stego image

N = Size of image

3.2 Peak Signal to Noise Ratio (PSNR) :

PSNR is a measure of the peak error. Peak Signal to Noise Ratio is the ratio of the square of the peak value the signal could have to the noise variance as shown in (2).

$$PSNR = 10 \log \frac{255^2}{MSE} db \quad \text{---(2)}$$

This is one of the major quality parameter of stego-image, There are a lot of agreement and dis-agreement on the benchmark value, however, a processed image visual perceptibility to the human eyes has been observed to have a PSNR greater than 30 dB [10-13]. The larger the PSNR, the better is the image quality, or the higher the value of PSNR the better the superiority of the signal ahead of noise. MSE and PSNR values of an image are between original image and stego image.

3.3 Calculation on Result:

Evaluation parameters are used Peak Signal to noise Ratio (PSNR), Mean Square Error (MSE). Both will used as performance parameters to measure the quality of image and Time Elapsed to encode and decode data. Signal-to-noise ratio, in image processing, is where the numerator as the square of the peak value of the signal and the denominator equals the noise variance. The error metrics can be used to compare the various image de-noising techniques are the Mean Square Error (MSE) and the Peak Signal to Noise Ratio (PSNR).

4. CONCLUSION

Stegano-image to login password in an Authentication System mechanism is more secure and reliable compared other textual authentication mechanism. By using stegano-image, it can make any systems more secure and it will give beneficial for applications which in cooperate world, government sector and in personal use. The algorithm eliminates a brute force attack. All data and critical information such as passwords are stored in encrypted manner and embedded in a cover image so it's difficult for brute force attack to crack it. Finally the stegano-image security authentication system provides high level security to the system which contains more important data, especially in mobile computing environment.

ACKNOWLEDGEMENT

Apart from our own , the success of this paper depends largely on the encouragement and guidelines of many others. I am especially thankful to our guide Prof. J. H. Saturwar who has provided guidance, expertise and encouragement.

REFERENCES

[1]. Teddy Mantoro, Didit Dwi Permadi and Adamu Abubakar, "Stegano-Image as a Digital Signature to Improve Security Authentication System in Mobile Computing", International Conference on Informatics and Computing (ICIC), 2016.

[2]. B. B. Zaidan, A.A.Zaidan, A. K. Al-Frajat and H. A. Jalab, On the Diffference between Hiding Information and Cryptography techniques: An Overview, Journal of Applied Sciences, 10(15):1650-1655,2010.

[3]. D. Bucerzan, C. Ratiu, M.J. Monolescu "SmartSteg: A New Android Based Steganography Application" International Journal Computer Communication October 2013.

[4]. I. Rosziati, L. C. Kee, MoBiSiS: An Android-based Application for Sending Stego Image through MMS, ICCGI 2012 : The Seventh International Multi-Conference on Computing in the Global Information Technology,115-120,2012.

[5]. R. Rayarikar, S. Upadhyay, P. Pimpale, "SMS Encryption using AES Algorithm on Android", International Journal of Computer Applications (0975 – 8887) Volume 50- No.19, July 2012.

[6]. Kutter, Martin, and Fabien AP Petitcolas. "Fair benchmark for image watermarking systems." In Electronic Imaging'99, pp. 226-239. International Society for Optics and Photonics, 1999.