MOBILE BANKING TRANSACTION SECURITY USING STEGANOGRAPHY

Ashish Deo *

Pravin Choudhary *

Kiran Kulkarni *

Anshu Sethi *

ABSTRACT

With the help of modern information communication technology, mobile banking, as a new type of financial services carrier, can provide efficient and effective financial services for clients. Compare with Internet banking, mobile banking is more secure and user friendly. The implementation of wireless communication technologies may result in more complicated information security problems. Based on the principles of information security, this paper presented issues of information security of mobile banking and discussed the security protection measures such as: Encryption technology, identity authentication and digital signature.

This paper presents general information about steganography, the art of data hiding. The paper provides an overview of steganography, general forms of steganography, specific steganographic methods, and recent developments in the field.

Keywords: *Information Security, Encryption Technology, Steganalysis, Data Hiding, Data Security, Data Embedding, Stego-Objects.*

* PVPIT, Computer Engineering, University of Pune, India.

I. INTRODUCTION

The aim of this work is to provide a secure environment in terms of security for transaction in banking applications. In order to improve security we are making use of "Steganography" technique in a way that is never used before.

II. NEED OF THIS TECHNOLOGY

Mobile communication is very easily susceptible to Piracy or Information Theft. Various viruses n Trojans can be used to destroy the security and safety of our personal data. Electronic data can be attacked by attackers or hackers in various ways. Worms like Jokey redirect your active transaction to hackers account. Fake Banking servers can be used to obtain personal details. Phishing attacks are very common threat to security. Data stealing Trojans are used to transmit data to hackers.

III. IDENTIFICATION OF NEED

Task of enhancing security include construction of formula for both data encryption and also for hiding pattern. Server should not process any fake request hence concept of custom "Session id" and "Request id" is introduced. Implementation of such a security constraints in banking sector not only help to serve customer in better way but also make customer confident and satisfy.

Instead of making use of some previous techniques of Steganography, such as LSB method which are easy to detect, it uses two mathematical formulae. To make use of Steganography appropriate image format should be selected such as loss less image formats.

IV. SCOPE

Art and science of communicating in a way that hides the existence of a message, signal or pattern imposed on content

- persistent under transmission
- not encryption
- original image/file is intact
- not fingerprinting
- fingerprinting leaves separate file describing contents

Task of enhancing security include construction of formula for both data encryption and also for hiding pattern. Server should not process any fake request hence concept of custom "Session id" and "Request id" is introduced. Implementation of such a security constraints in banking sector not only help to serve customer in better way but also make customer confident and satisfy.

V. WORKING

1. First, the client registers a key, then selects the session's encryption algorithm, and encrypts the request message. After that, it signs digital signature on the message, and then encrypts the session key using the server's public key. Finally the client attaches a time-stamp to the message and sends the message to the server after secure processing.

2. After receiving the client's message, the server decrypts the session key using its private key, then decrypts the request message using the session key. According to the key's information of the client, the server obtains the client's public key and examines the signature's validity. Then the server encrypts the response message using the session key, signs digital signature on it, and attaches a time-stamp. Finally it sends the message to the client.

3. After receiving the response message, the client decrypts it, and then examines the signature's validity. Then the client encrypts the request message using the session key, signs digital signature on it, and attaches a time-stamp. Finally the message is sent to the server.

4. The server examines the validity of the Session ID and signature. If valid, encrypts the response message using the session key, signs digital signature on it, and attaches a time-stamp. Finally it sends the message to the client.

Algorithm Used:

First of all, steganography program uses a form of basic LSB altering. This form of steganography is believed to be weak and easily breakable, but selected to use it for two main reasons:

1. It is simple so that numerous experiments related to it can be done.
2. & to strengthen this weak technique by adding more randomness.

The method itself does still encode data by flipping LSBs, but by adding randomness to images and to how data is encoded, we can make the cover images and stego-images seem more similar. There are several types of "randomness" that we can employ in our application. First of all, the exact pixels altered to encode each letter are semi-random. When embedding a message within an image, the first step is to count the number of letters in the message and divide the total number of rows of pixels in the image by that number. For example, if the image is 1000 pixels tall and we want to embed a message 100 letters in length, divide 1000 by 100 to get 10 rows per letter. This is the number of rows of pixels that could be associated with each letter.

Next, take the number of pixels the image is wide and divide by the number of letters in the alphabet (26). So if the image is 780 pixels wide, divide by 26 to get 30 columns per letter of the alphabet.

By grouping these sets of (10 in the example) rows and (30 in the example) columns together, we get a grid of sets of pixels within the image. Each of these subgrids corresponds to an encoding of a different letter of the message. The groups of rows correspond to the index of the letter in the message (e.g., first letter, second letter, etc.) and the groups of columns correspond to the actual letter encoded. So, for example, to encode the third letter as the letter "b" look at the third set of rows (rows 20-29 in our example) and the second set of columns (columns 26-51 in our example). Now to actually encode that the third letter in the message is "b", take a random bit from this sub grid (from rows 20-20 and columns 26-51 in our example) and flip it. See table 1 below for a visual representation of how sub grids map to different letters in the message for part of the image.

Image Grid	Cols 0-25	Cols 26-51	Cols 52-77	Cols 78-103	Cols 104-129
Row 0-9	Letter 1=a	Letter 1=b	Letter 1=c	Letter 1=d	Letter 1=e
Row 10-19	Letter 2=a	Letter 2=b	Letter 2=c	Letter 2=d	Letter 2=e
Row 20-29	Letter 3=a	Letter 3=b	Letter 3=c	Letter 3=d	Letter 3=e
Row 30-39	Letter 4=a	Letter 4=b	Letter 4=c	Letter 4=d	Letter 4=e
Row 40-49	Letter 5=a	Letter 5=b	Letter 5=c	Letter 5=d	Letter 5=e
Row 50-59	Letter 6=a	Letter 6=b	Letter 6=c	Letter 6=d	Letter 6=e

Now someone decoding the message by comparing the altered image against the original can easily determine the message even with this randomness since the letters appear in the message in the same order we find altered bits going down the rows and the decoder knows which groups of columns correspond to each letter. However, with the added randomness, it may be more difficult for someone who lacks the original image to detect something is wrong with the bit patterns of the modified image.

Additionally, by spreading the letters out across all the rows of the image, we reduce the chances of steganalysis detecting something wrong with a small portion of the image. This method does have a rather low data capacity (at most the number of rows of the image), but this also increases its strength against steganalysis since there are fewer alterations to be detected. In addition to the randomness built directly into the data embedding, my program offers options for adding random noise to the image before embedding data into it. The noise is added by selecting random pixels and flipping their LSB before the secret data is even embedded (and then using this altered cover as the new cover). The hope here is to create a cover with a bit pattern that is random in such a way that it is then difficult to tell covers apart from stego-objects, that is, covers that might seem themselves like stego-objects and thus confuse steganalysis tactics.

Taking this added randomness even one step further & implemented the ability for my program to generate its own random images to be used for covers. A fully random image presents no patterns in its least significant bits, and so it is (nearly) impossible to reliably detect alterations in bit patterns caused by my steganography method since there are no patterns to begin with. The problem with this is that the complete lack of a pattern in the cover image may itself arouse suspicion of an outside observer, as would the fact that communicators are sending images to one another that are composed of entirely random pixels. As a counter to this, we modified our random image generator to generate images with pixels that are similar to those surrounding them. The result is a fairly random image that still displays visual patterns and thus could potentially pass as a form of modern art, which is less suspicious than a fully random image.

The goal of all of this is to generate both covers and stego-objects that are statistically very similar. We found overall that it is very possible to generate cover/stego pairs that are almost identical statistically, thus making it nearly impossible for steganalysis to identify a single image as either cover or stego. Not every random image will have this property, but due to the nature of randomness, as large number are expected to.

Future work on this application could include refining the random image generator, exploring different ways to add randomness to images and to the embedding of messages within images, and altering images in other (perhaps larger) ways, such as flipping or shifting pixels.

VI. CONCLUSION

Improved M-Banking Security allows user to operate there bank account with the help of mobile like never before. It helps both bank & user to keep their data safe & safe banking. It makes easy to perform various transactions in secured manner. Every year many user face problem related to security of their account and causing loss of valuable information and money too which can be prevented to some extent using combination of various techniques as explained in this short article.

ACKNOWLEDGEMENT

When the compilation of paper comes to an end, the time comes to acknowledge all persons who have made its success possible. It gives us immense pleasure to express our gratitude to each individual associated directly or indirectly with the successful completion of the paper. I would like to take this opportunity to specially thank our guide, Prof. Sandeep Kadam of Computer Department, PVPIT Bavdhan, Pune, for vesting trust in us.

REFERENCES

1. R. J. Anderson, F. A. P. Petitcolas, "On the limits of the steganography," IEEE Journal Selected Areas in Communications, Vol. 16, No. 4, pp. 474-481, May 1998.
2. Hiding a Large Amount of Data with High Security Using Steganography Algorithm (Nameer N. EL-Emam , Jordan)
3. Steganography and Steganalysis (J.R. Krenn, January 2004)
   a. Image Steganography and Steganalysis
4. A Study of Steganography and The Art Of Hiding Information (Alain C. Brainos II, East Carolina University).
5. Steganography FAQ (Aelphaeis Mangarae [Zone-H.Org], March 18th 2006
6. L. Ehsan, F. Edrisi, Digital Steganography using DCT, MS Thesis, IRIB University, Tehran, Iran, 2002.
7. "Steganograpy", http://en.wikipedia.org/wiki/Steganography, Wikipedia page on steganography, includes links to many other sources.
8. Bergmair, Richard and Stefan Katzenbeisser. Content-Aware Steganography: About Lazy Prisoners and Narrow-Minded Wardens. 8th International Workshop, IH 2006, Alexandria, VA, USA, July 2006, Revised Selected Papers, Springer, 2006, p. 107-123.
9. Adee, Sally. Spy vs. Spy, August 2008,http://www.spectrum.ieee.org/aug08/659 3
10. Chakinala, R.C. et al. Steganographic Communications in Ordered Channels. 8th Inter-

national Workshop, IH 2006, Alexandria, VA, USA, July 2006, Revised Selected Papers, Springer, 2006, p. 42-57.