Secured M-Banking using Steganography and IMEI number of mobile phone

Mr. Ashish.R
5th sem,Dept of CSE
PES Institute of Technology
Bangalore-85
E-mail:ashishreddy_19@yahoo.com

Mr. Bhargava Pejakala Kakrannaya
5th sem,Dept of CSE
PES Institute of Technology
Bangalore-85
E-mail:pejakalabhargava@gmail.com

ABSTRACT

Nowadays m-banking (mobile banking) is widely used in many banks. M-Banking has changed the dimension of the current banking trend. But there are few problems associated with this too. One of the main issues in m-banking services is the security of the systems.

For solving the above problem, we proposed a method in this paper. By this method we send secure banking messages for intended customer's mobile phone using the concept of IMEI number and Steganography. In this method the information is hidden in an SMS picture message using steganographic tools and is sent to the customer .The tool on customer's side extracts the IMEI code from the SMS picture message and compares it with the user's mobile phone IMEI code. If it matches then the information hidden in the other part of the picture message is retrieved using the same tool. This concept can be implemented in J2ME (Java 2 Micro Edition) language which is the most widely used language for mobile softwares.

KEYWORDS :

Steganography, IMEI, SMS, SMSC, M-Banking, Picture messages.

INTRODUCTION:

After expansion of the use of mobile phones and advancements in mobile communication, mobile phone companies decided to add some extra features to their mobile phones in order to attract more customers. One of the first services offered on the mobile phones was the short message service (SMS). SMS is the transfer and exchange of short text messages between mobile phones. On the other hand, because of advancing mobile phones during the recent years, the banks have started to think of offering banking services on the mobile phone.

Some of the reasons for offering these services are as follows:

1) No place restriction : In m- banking, one can do banking transactions from any place in the world.
2) Fully personalized : Mobile phones are strictly private and are used only by their owners. Therefore it increases the possibility of user authentication.

Availability : Most of the people keep user stored

mobile phones at their side, both indoors and outdoors, and therefore, the customer can be served at any moment.

Advantages of SMS are :

- We can send messages even when network is busy.
- SMS costs very less.
- We can send and receive messages while making phone calls.

In general, the mobile banking has been well received as it increases the convenience of the customers and reduces banking costs.

To exchange information with the customer, services such as Short Message Service (SMS) or Multimedia Messaging Service (MMS) can be used. SMS is defined in accordance with standard of GSM digital mobile phones

According to GSM03.40, the length of message exchanged is maximum 160 characters stored in 140 bytes based on the data saving method under the standards. These messages can be a mixture of letters and numbers and even non-text binary form. With the use of the same binary messages, pictures can be also sent which names picture message. Of course these pictures are only in two colors and of a low quality. Exchange of SMS is done indirect and through an SMS agent (SMSC). SMSC is a network element in the mobile telephone network which delivers SMS messages. When a user sends a text message to another user their, the message gets in the SMSC, which delivers it to the destination when they are accessible.

Steganography is the science of ***hiding*** information, highlighted in recent years, chiefly aimed to hide data within a cover media so that other individuals fail to realize their existence. The word steganography is derived from the Greek words "***stegos***" meaning "cover" and "***grafia***" meaning "writing" defining it as "covered writing". There is a major distinction of this method with the other methods of hidden exchange of data because, for example, in the method of cryptography, individuals see the encoded data and notice that such data exists but they cannot comprehend it.

However, in steganography, individuals will not notice at all that data exists in the sources. Most steganography jobs have been performed on images, video clips, text, music and sound. It has been implemented on varying systems such as computers and mobile phones. Almost all digital file formats can be used for steganography, but the formats that are more suitable are those with a high degree of redundancy. Redundancy can be defined as the bits of an object that provide accuracy far greater than necessary for the object's use and display . The redundant bits of an object are those bits that can be altered without the alteration being detected easily. Image and audio files especially comply with this requirement, while research has also uncovered other file formats that can be used for information hiding.

Categories of file formats that can be used for Steganography are

- Text
- Images
- Audio/Video
- Protocol

EXISTING PROBLEMS:

One of the services offered in mobile banking is sending notifications and alerts as well as the information requested by the customer. These services can be provided through SMS. While sending SMS, the messages can be sniffed on the way and stored by a hacker. This is very important especially in cases when important and sensitive messages are to be sent. So effective means of security for these kind of confidential messages is required. Even though the customer information can be sent by an email, or through the telephone, it is still insecure. If it is said through the mobile phone, it can be stolen easily by tracing the voices. Moreover authenticating the phone caller is a difficult task. And mail account can be easily hacked too. And also its very inconvenience for the customer to travel all the way to the bank to get the required information.

SUGGESTED METHOD:

In this paper a new method for sending the required confidential alerts, notifications or information requested by the customer is proposed. In this method the data (Information + IMEI number of the customer mobile) is hidden in a SMS picture message using steganography and is sent to the user.

Suggested method consists of following parts:

1) Generating data in hidden format through SMS picture message according to user mobile phone IMEI code.
2) Sending it to the customer.
3) Getting the SMS picture message and first extracting the IMEI number present in hidden format.
4)If the IMEI number matches with that of the phone,then extract the hidden customer data and convert it into user readable format.
5) If it doesn't matches then it is made sure that hidden data is not extracted.

The first part is executed by a stego-software, which is run by the software producer. The third, fourth and fifth parts are done by user software, which is wanted to extract the data.
The IMEI number is a 15-digit number which is unique for every mobile phone and it is used to recognize the GSM/DCS/PCS mobile phones in network services. This number has various usages such as the recognition of the stolen mobile phones.

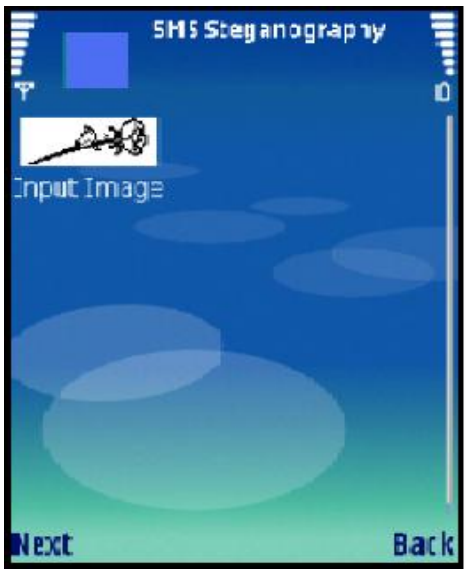
Just key in *#06# on your cellular phone and it will display its IMEI number in most phones.Since the beginning of 2003, its format is NNXXXXYY-ZZZZZZ-A. The first 8 digits (NNXXXXYY) are the verification code of the respective country. The next six digits (ZZZZZZ) are the serial number of the mobile phone and the last one digit is a control-related number.

It is possible to identify the mobile phone brand using IMEI number where in bank database needs to have the same and also its duty of the customer to report the bank his new IMEI number when he changes his mobile phone. Therefore when the bank receives a request from a customer, it can detect the brand of mobile phone and sends the prepared SMS picture message in a proper format which is compatible with the customer mobile phone. For instance if customer is using NOKIA mobile phone then picture message has to be in OTA format.

Firstly, by using the method of steganography in the SMS, the data is hidden in an SMS picture message. Briefly speaking, in this method, in order to hide information in an SMS picture message, the picture is divided into smaller blocks. If changing the pixels of the block is not noticeable, a pixel of the block is changed and, thus, information is hidden in the picture.

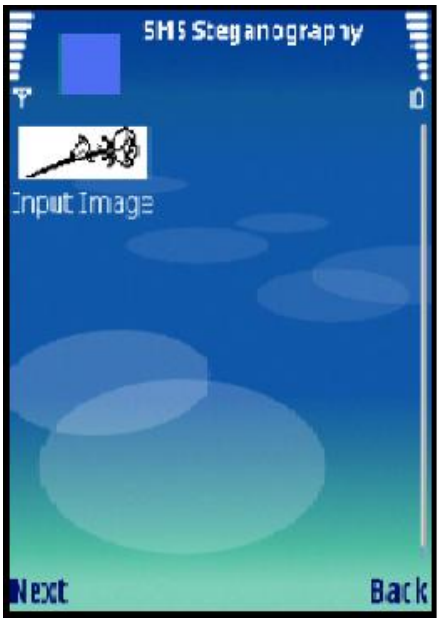
Secondly, the SMS picture message is sent to the user. Finally the user software gets the SMS and extracts the data (i.e first it extracts the IMEI number from the picture message and checks it with phone's IMEI. If it matches then it extracts the information which is in coded format in the picture message. If any mismatch occurs then hidden data is not extracted) from it.

The information to be sent to the customer is being prepared by the bank system. After receiving this information the program sends the SMS picture message and repeats this action until the entire information is stored in the form of picture messages, making sure everytime the IMEI number of the customer mobile phone is included in the picture message in hidden format.



A screenshot of sender program

SMS picture message produced by the sender program in which data is hidden.



A screenshot of receiver program

SMS picture message received by the customer which contains the data in hidden format.

ADVANTAGES

Some advantages of our method are as follow:

1) If the SMS picture message is stolen, the data is remained secure and hidden,

because for extracting the data from SMS picture message, IMEI code in picture message should match with that of the mobile phone.

2) Steganography methods are usually carried out on colour or grayscale pictures and little work has been done on steganography in two-colour pictures. Therefore, using the existing two-colour pictures in SMS messages for steganography is less noticeable.

countries; therefore the suggested method can be implemented in many countries especially

3) Each day millions of SMS messages are exchanged throughout the world. Therefore, steganography in SMS picture messages has attracted less attention and it is hardly likely to identify pictures containing hidden information.

4) Costs of SMS message especially compared to services such as the WAP is very low. Therefore, benefitting from this method for hidden sending data is very cost-effective.

5) The mobile phone is a public facility and most individuals have mobile phones. On the other hand, the SMS is a popular service. Therefore, our proposed method covers many users.

6) Because of not using sophisticated technologies, this method can be implemented on simple mobile phones as well and there is no need to use advanced mobile phones.

7) All mobile phones, even black and white models and old-fashioned ones are capable to send and receive SMS so this method covers a lot of users.

CONCLUSION

In this paper, with the application of Steganography, a new method is proposed for sending alerts, notifications or information requested by the customer through SMS picture messages(M-Banking).

Steganography is a relatively new method in secret exchange of information. Therefore, the possibility of disclosure and extraction of its information especially in mobile phone systems is much lower. SMS service is available in many

developed countries.

Because of the low costs of this method respect to using SMS, it can be used in poor regions as well. Also the MMS(Multimedia Messaging Service) messages can be used for establishing hidden communication, but this service needs more resources such as advanced mobile phones and network services that support MMS, and also this service is need more costs than SMS service. Many mobile phones support Java language, and approximately all mobile phones can transfer SMS messages, so this method can be implemented on wide range of mobile phones.

This method is not limited to M-banking. For example this method can also be used for sending mobile software activation code, defence where in secret information can be exchanged.