ISSN 2320-9186

Global Scientific JOURNALS

Secure Mobile Banking Frame Work by Using Cryptography and Steganography Methods.

Tibabu Beza
Lecturer at Adama Science and Technology University
Department of Computer science and Engineering, Adama, Ethiopia
tibabu2010@gmail.com

ABSTRACT

In recent past years, the Internet and Mobile is widely used for communication. The developments in mobile commerce applications make a revolutionary change in the banking services offering anytime, anywhere banking. Today, with the technological advancements in mobile communication and the Internet, the common man's day-to-day requirements are meet at his door step. Mobile banking permits everyone in the country to access the banks for various transactions at their own places.

Communication became easy attention toward Information Security. Data Security is the core issue addressed in the research. The problem with current banking applications is the security shortfall. To solve the current M-Banking security deficit, author proposes the secure mobile banking frame work structure by using Cryptography and Steganography methods. In proposed framework AES Symmetric Cryptography algorithm and LSB of Image Steganography algorithm are used to enhance the current security short fall of M- Banking with minimum cost. In this approach bank encrypted and hidden transaction data in the Image to send it to bank's customer and the customer should decode and decrypt to get the original data.

Keywords: AES, LSB, M-Banking, MMS

INTRODUCTION

1.1. Background

Using the Internet for banking affairs is interested in different aspects. By the use of the Internet, there is no need to go to the bank and to a special branch of the bank and one can manage his bank transactions from any place. There is no problem such as crowded banks and long queues, therefore the customers can save time. It also reduces the customers' expenses. In this system, there is no such problem as closure of the bank after office hours and banking can be done in any hour. On the other hand, mobile phones have advanced during the recent years and as a result of the progress in mobile phones and incorporating difference services in the mobile phones, the banks have started to

ISSN 2320-9186

think of offering banking services on the mobile phone. Some of the reasons for preference of M-Banking over e-banking are [3]: No place restriction, High penetration Coefficient, Fully personalized and Availability.

M-Banking system is one, which provides all daily-banking operations to customer with one click of his mobile handset with supported application. M-Banking system has potential to provide access or delivery of very specific and highly necessary information to customer as given in. Growth in the M-Banking is driven by various facilities like convenience of banking operations, greater reach to consumers and Integration of other m-commerce services with mobile banking.

M-Banking is beneficial to both the customer and the bank. Mobile banking gives opportunity to everybody for easy banking activities sustainably increasing the interaction between user and bank. It has enabled to increase financial access for in rural areas and paved the way for integrating rural people into the mainstream financial system.

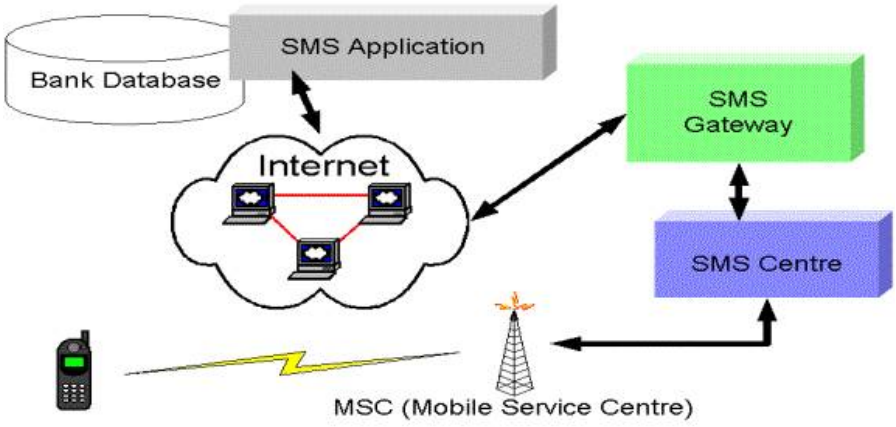
Mobile Banking is being deployed using mobile applications developed on one of the following four channels: such as IVR (Interactive Voice Response), SMS, WAP (Wireless Access Protocol) and Standalone Mobile Application Clients.

1.2. IVR – Interactive Voice Response

Interactive Voice Response service operates through pre-specified numbers that banks advertise to their customers. Customer's make a call at the IVR number and are usually greeted by a stored electronic message followed by a menu of different options. Customers can choose options by pressing the corresponding number in their keypads, and are then read out the corresponding information, mostly using a text to speech program.

1.3. Short Messaging Service Architecture

SMS uses the popular text-messaging standard to enable mobile application based banking. The way this works is that the customer requests for information by sending an SMS containing a service command to a pre-specified number. As figure 1.1 indicates the bank responds with a reply SMS containing the specific information.



ISSN 2320-9186

Sourse: International Journal of Computing Technology and Information Security
Figure 1. 1: SMS Network Architecture.

1.4. WAP – Wireless Access Protocol

WAP uses a concept similar to that used in the Internet banking. Banks maintain WAP sites which customer's access using a WAP compatible browser on their mobile phones. WAP sites offer the familiar form based interface and can implement security quite effectively.

1.5. Standalone Mobile Application Clients

Standalone mobile applications are the ones that hold out the most promise, as they are most suitable to implement complex banking transactions like securities in trading. They can be easily customized according to the user interface complexity Supported by the mobile. In addition, mobile applications enable the implementation of a very secure and reliable channel of communication. [2]

The data transaction through stand alone mobile application clients has led to attract criminal attention. Security concerns are important for both customer and bank. Several challenges of M-Banking that need to be addressed like handset compatibility, security, scalability, reliability. Due to increase the use of mobile handsets for many m-commerce applications, the probability of M-Banking hacking for financial benefits is heavily increased. Current some banks in many countries are sending text SMS directly to the customer handset for basic bank services without any security which can be accessed by any malicious person and can use this information for getting access to customer account [1]. OTA (Over-the-air) mobile data can be hacked in network during transaction of data from bank to customer mobile and vs.

There is a need of secure and cost effective solution, which can be easily provided on all types of handsets. In this thesis work our objective is to propose new security mechanism which is cost effective and secure M-Banking solution by combining the different security algorithms methods. In this thesis work we will present a new security frame work modal to secure M-Banking by using LSB of Steganography and AES of Cryptography methods. The aim of thesis work is to establish a secure communication between the clients and mobile-bank application server in which they can use their mobile phone to securely access their bank accounts, make and receive payments, and check their balance. AES of Cryptography and LSB of Steganography methods are well-known and widely used techniques that manipulate information (message) in order to cipher and hide their existence. These techniques have many applications in computer science and other related fields. They are used to protect military message, emails, credit card information, corporate data, personal file etc.

Cryptography is, traditionally, the study of means of converting information from its normal, comprehensible into an incomprehensible format, rendering it unreadable without secret knowledge, the art of encryption.

Steganography is the art and science of writing hidden message in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message form of security through obscurity. The goal of Steganography is to communicate security in a completely undetectable manner and to avoid drawing suspicion to

ISSN 2320-9186

the transmission of a hidden data. Steganograpy has different terminology which is used in different places. Such as Payload, carrier, Stego-medium, Redundant bit, Steganalyis. Payload is the information which is to be concealed, Carrier file is the media where payload has to be hidden, Stego-medium is the medium in which the information is hidden. Redundant bit is pieces of information inside a file, which can be overwritten or altered without damaging the file. Steganalyis is the process of detecting hidden information from inside of a file.

In this thesis work, we will propose new security model, which is never used before on MMS framework mobile banking by using LSB technique of Image Steganography and AES Encryption methods.

2.1. *Mobile Banking*

Using Internet for banking affairs is interested in different aspects. By the use of the Internet, there is no need to go to the bank and to a special branch of the bank and one can manage his banking works from any places. There is no problem such as crowded banks and long queues, therefore, the customers can save time. It also reduces the customers' expenses. In this system, there is no such problem as closure of the bank after office hours and banking can be done in any hours.

Mobile phones have advanced during the recent years, because of the progress in mobile phones and incorporating difference services in the mobile phones. The banks have started to think of offering banking services on the mobile phone. Mobile banking allows reviewing account history, transferring funds between accounts, making loan payments and checking balances from a cell phone or mobile device with the Internet access. Some of the reasons for preference of M-Banking over E-Banking are- No place restriction, High penetration coefficient, fully personalized and Availability.

Mobile banking has been well received as it increases the convenience of the customers and reduces banking costs. The banking services are divided into two groups of mobile agency services and mobile banking services. Mobile banking services are the same as the conventional banking services and are generally divided into four categories such as: Notifications and alerts, Information, Applications and Transfer:

Notifications and alerts services are offered to inform the customer of the transactions done or to be done with his account. Information is the transactions and statements that sent in specific periods. Customer side sent different inquiry to the service provider regarding his account or a Special transaction. Transfer is the money transferred between different accounts of the customer or payment to third parties.

To implement mobile banking services, an infrastructure server such as WAP (Wireless Application Protocol), i-mode, Palm.Net and so on is needed. [1]. To exchange information with the customer, services such as Short Messaging Service or Multimedia Messaging Service can be used. The issue of security of M-Banking is a source of concern to the users and numerous solutions and systems have been so far presented in order to increase the security of M-Banking.

ISSN 2320-9186

M-Banking system is one, which provides all daily-banking operations to customer with one click of his mobile handset with supported application. M-Banking system has potential to provide access or delivery of very specific and highly necessary information to customer. Growth in the M-Banking is driven by various facilities like convenience of banking operations, greater reach to consumers and integration of other m-commerce services with mobile banking. In M-Banking there is no place restriction, it is highly penetration coefficient as growth of mobile phones are more than computers, it is fully personalized, private increasing transaction and authenticity is 100% available all the time with users. However, there are several challenges that need to be addressed to completely utilize the benefits of the M-Banking like handset compatibility, security, scalability, reliability. Due to increase in use of mobile handsets for many m-commerce applications, Chances of mobile hacking for financial benefits are heavily increased. OTA (Over-the-air) mobile data can be hacked in network path from Bank to customer mobile handset including MPIN, a password use for user identification in M-Banking. Thus, there is a need of secure and cost effective solution, which can be easily provided on all types of handsets. The thesis work is to provide cost effective, secure solution for mobile banking by combining features of AES of Cryptography and LSB of Steganography.

2.2. *Types of Mobile Banking*

Current technology enables three primary methods to access financial data and initiate transactions from a mobile phone: Short message service or multimedia messaging service, mobile web, mobile client applications (Mobile Marketing Association, 2009) and IVR-based Banking. Each offers advantages and challenges for both consumers and bankers.

2.2.1. Short Message Service (SMS)

Message based systems work through text messaging. Short message services include sending text messages to a bank, which receive and interpret the commands sent in the message. The bank returns a text message with the information requested. Typically, these messages are limited to 160 characters. There is also the concern that most SMS systems do not guarantee delivery of the message (Kevin and Justin, 2008). MMS is including text and Image to send and receive from bank and customer. In this thesis we have presented MMS based secure mobile banking with minimum cost using Steganography and Cryptography methods.

2.2.2. Mobile Web

Mobile browsers model is the ability to access the bank's Internet banking website from a cell phone. If user has an IP enabled phones, they can connect to the Internet via their carrier's Internet services or a wireless hotspot. The major advantage of this approach is all the processing is done on a remote server and minimal information is stored on the device. Another advantage is that there is no need to install special software since phones capable of using this technology come with the software installed (Rajneesh & Stephan, 2007).

ISSN 2320-9186

2.2.3. Mobile Client Application

Standalone mobile applications are suitable to implement complex banking transactions like trading in securities. They can be easily customized according to the user interface complexity supported by the mobile. In addition, mobile applications enable the implementation of a very secure and reliable channel of communication.

The client side application architecture requires the user to download the mobile banking software onto their phone. These Java-based systems can be very nice from a customer interaction standpoint, as a bank can offer simple, easy to use applications to provide a variety of services (Riivari, 2005). The real advantage to these applications is that they can be run remotely and only need to connect to the banks systems long enough to get information and execute a transaction thereby lowering the normally high data costs that may be associated with web based applications (Rajnish& Stephan, 2007)

2.2.4. Mobile Banking Based on IVR-Interactive Voice Response

IVR or Interactive Voice Response service operates through pre-specified numbers that banks advertise to their customers. Customer's make a call at the IVR number and are usually greeted by a stored electronic message followed by a menu of different options. Customers can choose options by pressing the corresponding number in their keypads, and are then presented the corresponding information, mostly using a text to speech program. Mobile banking based on IVR has some major limitations that they can be used only for enquiry-based services. In addition, IVR is more expensive as compared to other channels as it involves making a voice call, which is generally more expensive than sending an SMS or making data transfer.

3.2.1. Bank-end Database Server

The bank database server consists of various tables storing customer details pertaining to his/her personal information, account information, transaction information, and message in and out information. Bank database also stores customer confidential information such as PIN, and onetime session key with its corresponding sequence number in encrypted and secure manner. This actual database must be connected to the bank server application. Then the bank server can retrieve, insert values and update the database. Figure 3.1 shows the four components of the proposed architecture of the secure MMS Mobile banking System.

ISSN 2320-9186

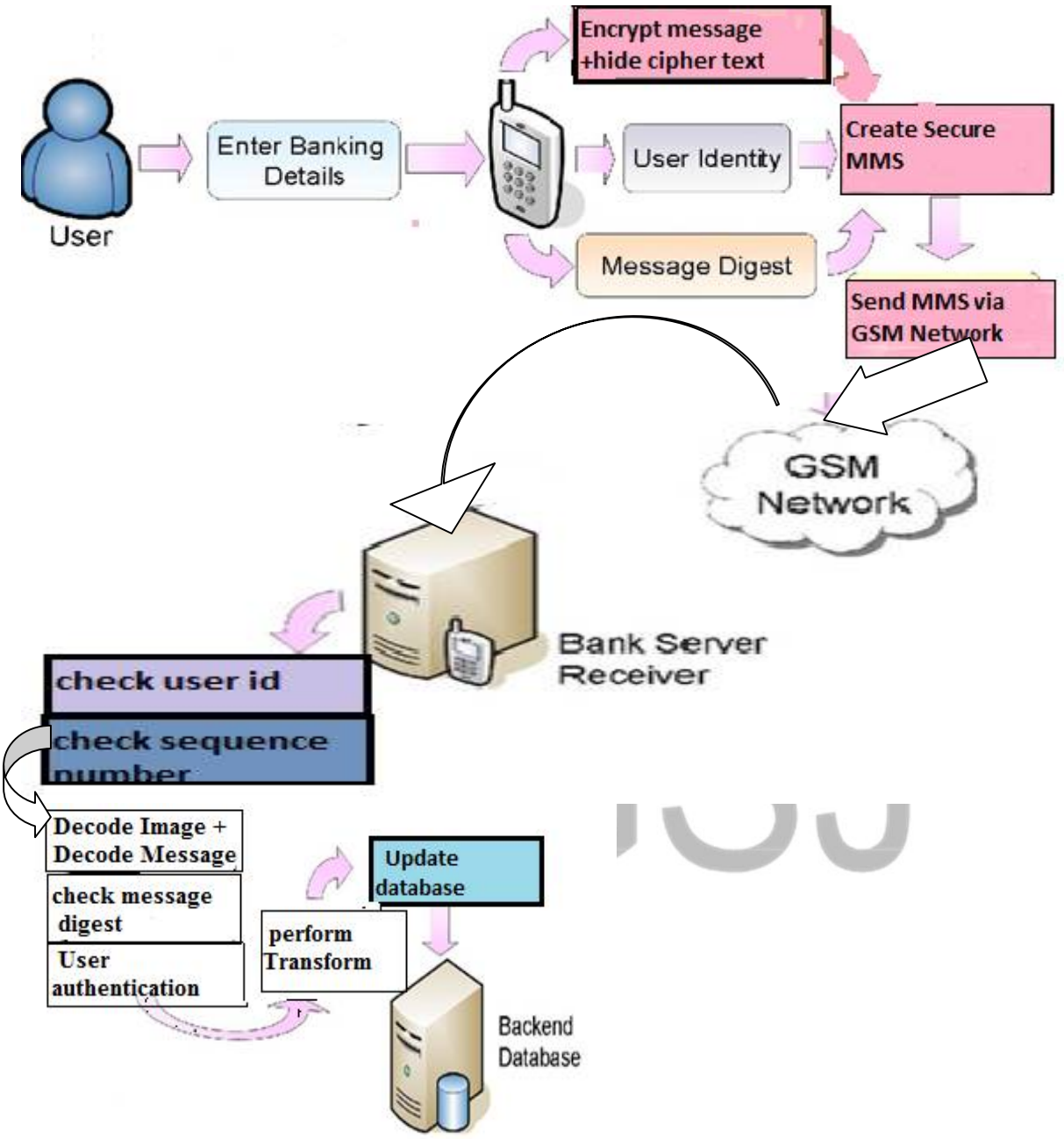


Figure 3. 1 : Sender side Components of Proposed MMS Mobile Banking System

In sender side message should be encryped by using AES and hide by using LSB algorithms before send to reciever Sender can send the Stego Image to reciever via of service provider center. Service provider is the intermidet between sender and reciever to connect them to each other. Reciever should get the Stego Image and then decode Image from securet message and then decrypt the cipher message to get the original message. After reciever get the original message from sender and understand the sender idea, can give the response to sender. the following figure 3.2 show that how customer can receive the response from bank serve

ISSN 2320-9186

3.2.1.1. Security of the Designed Architecture

The major objectives of proposed architecture is to overcome the security limitations of the existing system and other security threats existed due to the open wireless network by designing secure MMS mobile banking channel. The security of the proposed architecture is designed by considering the principles of security services and other security threats through different algorithms and mechanisms. The following section discusses the designed part of the security issues of the proposed architecture.

3.2.2. Combination of Steganography and Cryptography

Those who seek the ultimate in private communication can combine encryption and Steganography. Encrypted data is more difficult to differentiate from naturally occurring phenomena than plain text is in the carrier medium. There are several tools by which we can encrypt data before hiding it in the chosen medium. In some situations, sending an encrypted message will across suspicion while an invisible message will not do so. Both methods can be combined to produce better protection of the message. In case, when the Steganography fails and the message can be detected, it is still of no use as it is encrypted using Cryptography techniques.

Cryptography and Steganography are well known and widely used techniques that manipulate information (messages) in order to cipher or hide their existence respectively. Steganography is the art and science of communicating in a way which hides the existence of the communication. Cryptography scrambles a message so it cannot be understood; the Steganography hides the message so it cannot be seen. In this paper we will focus to use one system, which uses both Cryptography and Steganography for better confidentiality and security in mobile banking. Presently we have very secure methods for both Cryptography and Steganography like AES algorithm of Cryptography and LSB of the Steganography methods are very secure technique. Even if we combine these techniques straight forwardly, there is a chance that the intruder may detect the original message. Therefore, our idea is to apply both of them together with more security levels and to get a very highly secured system for data hiding. This paper mainly focuses on to simulate new system with extra security features where a meaningful piece of text message can be hidden by combining security techniques like Cryptography and Steganography. When data is encrypted and hidden it has much advantage:-

- Hiding data is better than moving it shown and encrypted.
- To hide data in a popular object that will not attract any attention.
- In case the data is extracted, it was encrypted.

But still there is a chance that the intruder can break the code. In our new system instead of applying existing techniques directly we will be using the following approach:-

- Instead of hiding the complete plain text into an Image, we will be hiding the encrypted message.
- In this system to get the original message one should know, along with keys for Cryptography and Steganography methods.

ISSN 2320-9186

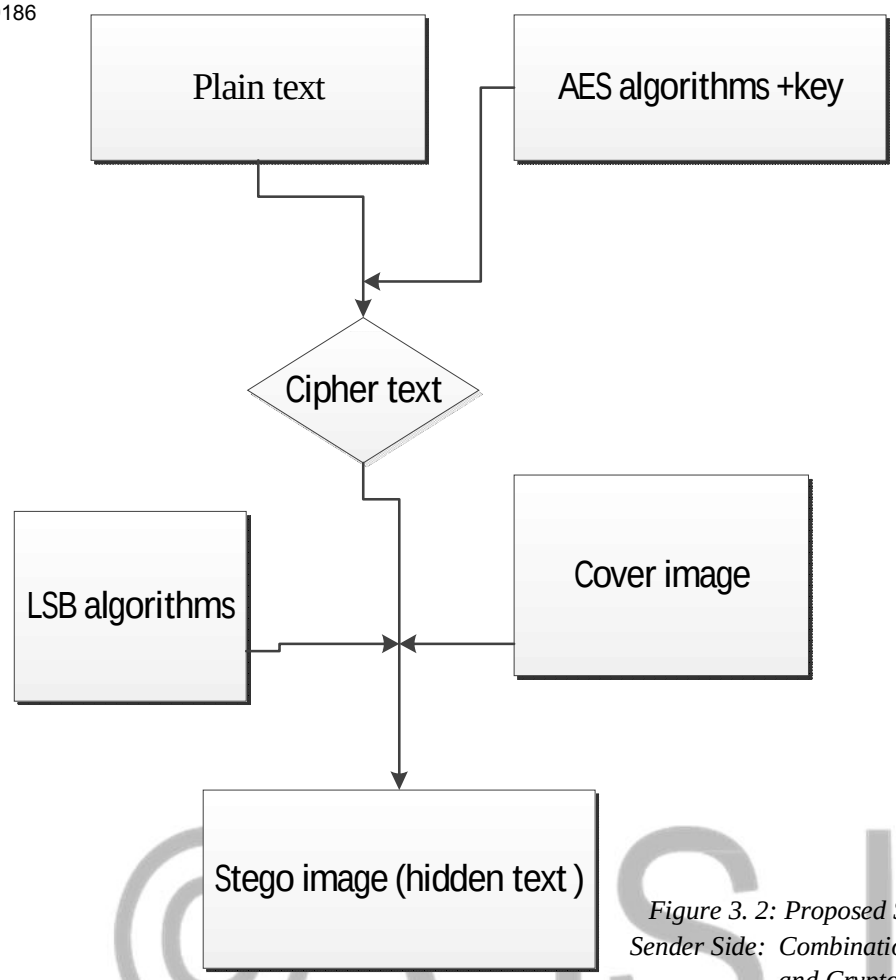


Figure 3. 2: Proposed Security Methods in Sender Side: Combinations of Steganography and Cryptography

Sender Side Encryption and Encoding Proposed security Frame work

Input: Message M, Cover Image C, Key K

Procedure:

Step 1: Original message M is inside a text file.

Step 2: Apply AES algorithm to generate cipher text using key K.

Step 3: Select cover Image from your computer as an input to apply LSB algorithm along with cipher text.

Output: Stego Image S. Send this Stego Image in email to receiver.

Figure 3.3: Sender Side Encryption and Encoding Algorithms

The sender has sent the Stego Image in an email. So the receiver has to use that Stego Image in the decoding process. Receiver will download the Image from email in Google Android. The default location in Google android is /sdcard/ where the downloaded Images Reside. This sdcard provide the storage space in an Android emulator. In Google android at the receiver end, We have used a LSB to decode the hidden message from the Image. Whenever the receiver runs the decoding application, in the first step the Stego Image is feed as an input to the algorithm. The LSB is used in the algorithm. The Image is divided into bit planes. And then the intersection points of the cipher text

ISSN 2320-9186

and the Image is found. The encrypted message will be extracted and then the AES Decryption algorithm is used to decipher the text and to get the plain text. So after all applying these steps the receiver gets the intended message

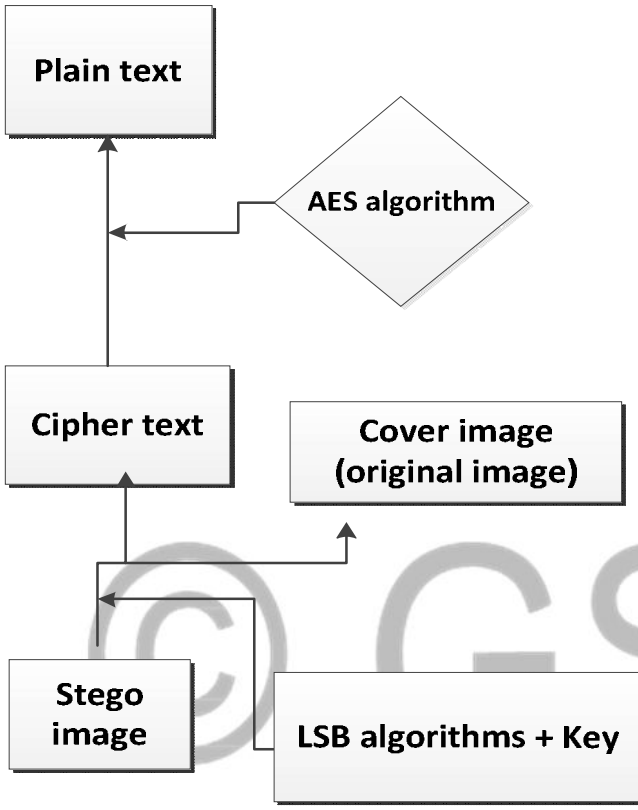


Figure 3. 4: Proposed Security Methods in Receiver Side: Combinations of Steganography and Cryptography.

Receiver Side Decoding and Decrypting Algorithms

Input: Stego Image S, Key *K*.

Procedure:

Step 1: Stego Image is downloaded from email to android emulator's Sdcard.

Step 2: Feed this Image as an input to the LSB algorithms Insertion algorithm to find out the intersection points.

Step 3: Extract the cipher text from the intersection points and feed this as an input to the AES decryption algorithm using key *K*.

Output: Original Message M. Cover Image

Figure 3. 5: Receiver Side Decoding and Decryption Algorithms

ISSN 2320-9186

4.1.1. Implementation of Encryption and hiding

4.1.1.1. Silent Eye Tool

In this thesis work we used the SilentEye for encrypting/ Decrypt text by using AES -128 and hide/unhide or encode/decoding message by using LSB algorithms

We used the tool that contains both LSB and AES algorithms to encrypt and hide secret messag. The SilentEye is a cross-platform application design for an easy use of Steganography, in this case hiding messages into pictures or sounds. It provides a pretty nice interface and an easy integration of new Steganography algorithm and Cryptography process by using a plug-ins system.

Hide information into Images (LSB): JPEG, BMP, BMP, JPG, PNG, TIF, TIFF, and Encrypted data [AES]: AES128 and AES256. Secret message can be hidden in Sinlenteye Tools, it has the Capacity to hide text file or zip compression of message. figure 4.1 indicate that the silent eye tool interface.

Figure 4. 1: Plain Text and Cipher Text.

Table 4. 1: Silent Eye Interface

	SMS message (plain text)	Size of plain text (kb)	Cipher text	Size of cipher text (kb)
1	Name of customer: Aduna Galassa Account number: 0009991 Balance: $20000 Withdrawal: $300 Interest rate: $ 40	**25.5**	6A 3C 69 85 0D E5 B6 92 28 4C 1A E6 E3 29 AE 69 2A 6B 77 1F B0 8F 69 05 CE E4 CB 7F 5D D3 62 0E E4 25 21 D7 30 97 75 57 6D A7 97 F2 1C 6C 76 70 49 B7 52 64 87 55 D9 E6 20 EE 63 F4 79 1E 0D B9 3B 48 1C 87 25 C7 8F 6A 9D 94 23 2B 53 B1 13 88 9A 6A 22 12 B2 AC 82 F1 28 6D 3E 81 1C 90 81 81 87 E3 79 3F B7 9F 79 23 2E 7A 93 19 78 65 C6 41 5D 90 F4 FF 79 24 D9 42 F6 E1 4D 2D 9F 62 99 2C	**25.5**
2	Name of customer: Adane Getu Account number: 011111000 Balance: $3000 Withdrawal: $200 Interest rate: $ 20 Transfer amount: $10	**25.5**	6A 3C 69 85 0D E5 B6 92 28 4C 1A E6 E3 29 AE 69 11 12 96 E4 5D 41 68 9B F9 A7 CF 8C BB 3C 97 16 5B 28 66 28 8F 27 78 84 55 C1 C5 35 D7 6C AC F5 FD 15 57 8A A4 2E B6 28 09 92 8F 57 44 C1 CA C3 26 7C C0 AD 25 4E 20 FF B7 2A AD 09 B1 54 7C 18 63 D0 49 55 E0 59 C7 69 F3 BA 27 B9 6D 1C CE 2E 84 5A 1D B2 CC 1A 4E E3 12 F1 CB 5E 78 9D B7 B4 25 57 92 15 8F 2B DA 7D 17 1B CF E4 9C 6B	**25.52**

ISSN 2320-9186

			72 CF AB 61 4A 2D 10 92 61 B8 6D 78 89 49 4C 71 59 A3	

As table 4.2 indicates that we receive different SMS text. By using SilentEye tool the SMS message encrypted by AES-128 algorithms and the cipher text was hidden in different image size and types. At the end the Stego image was generated which is encrypted and hidden in Image. The following table 4.3 indicate that the cipher text that hidden in different image types and dimensional size.

Table 4. 2: Cipher Text Hidden in Different Image Size and Type.

	SMS message (plain text)	**Size of plain text (kb)**	**Cipher text**	**Size of cipher text (kb)**
	Cipher text	**Size**	**Image size**	**Image type**
1	**6A 3C 69 85 0D E5 B6 92 28 4C 1A E6 E3 29 AE 69 2A 6B 77 1F B0 8F 69 05 CE E4 CB 7F 5D D3 62 0E E4 25 21 D7 30 97 75 57 6D A7 97 F2 1C 6C 76 70 49 B7 52 64 87 55 D9 E6 20 EE 63 F4 79 1E 0D B9 3B 48 1C 87 25 C7 8F 6A 9D 94 23 2B 53 B1 13 88 9A 6A 22 12 B2 AC 82 F1 28 6D 3E 81 1C 90 81 81 87 E3 79 3F B7 9F 79 23 2E 7A 93 19 78 65 C6 41 5D 90 F4 FF 79 24 D9 42 F6 E1 4D 2D 9F 62 99 2C**	**25.5**	**328*308**	**Jpg**
			277*268	**Bmp**
2	**6A 3C 69 85 0D E5 B6 92 28 4C 1A E6 E3 29 AE 69 11 12 96 E4 5D 41 68 9B F9 A7 CF 8C BB 3C 97 16 5B 28 66 28 8F 27 78 84 55 C1 C5 35 D7 6C AC F5 FD 15 57 8A A4 2E B6 28 09 92 8F 57 44 C1 CA C3 26 7C C0 AD 25 4E 20 FF B7 2A AD 09 B1 54 7C 18 63 D0 49 55 E0 59 C7 69 F3 BA 27 B9 6D 1C CE 2E 84 5A 1D B2 CC 1A 4E E3 12 F1 CB 5E 78 9D B7 B4 25 57 92 15 8F 2B DA 7D 17 1B CF E4 9C 6B 72 CF AB 61 4A 2D 10 92 61 B8 6D 78 89 49 4C 71 59 A3**	**25.5**	**400*400**	**25.52**
			1194*943	

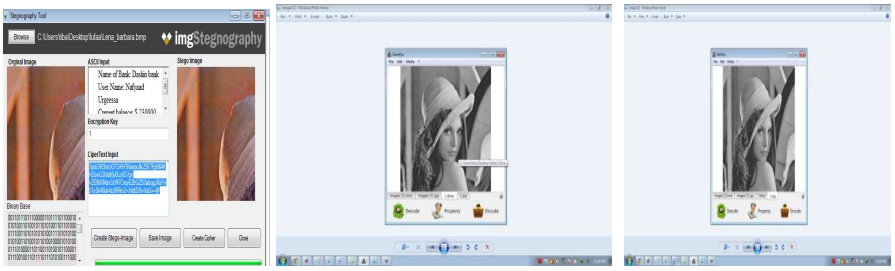
As table 4.3. Indicate during experiment we use two type Images for hiding the cipher text, such as JPG and Bmp types of image. The experiment result of the Original and Stego Image of the above table is list below.

ISSN 2320-9186

Original Stego Original Stego
a) Sara (288*217

Figure 4. 2: Original and Stego Image

As figure 4.2 Indicate the different type of image hide the secret message by using LSB of image steganography. The original and stego image shown side by side on the above.



a) Original Stego a) Original Stego

a) Original Image Stego Image Original Stego Image

Figure 4. 3: Commercial and Dashen Bank Image

The second tests hide the different cipher text in different image. As figure 4.3 above indicate the plain text and cipher text which shown on figure 4.4 below hide in different image.

Original text (plane text)

Name of Bank: Dashin bank
User Name: NafyaadUrgeessa
Current balance: $ 230000
Interest rate $900
Cipher text
Cipher text
7pobSKShsUOTSKHTt6iarou
8kZ5F7FgN64KHZqwG3Ndd0y
0Lo6D7gv+ZE86KMqvSzWFC
nxyEZtrGZDQxbqgJXoPvS1o
Sk46uk4zJMRro2+/hldtDSi+XaQ==@

Stego Image

ISSN 2320-9186

4.1.1.2. Android Emulator

Android provides a whole software stack which includes an operating system, a middle layer and a few inbuilt applications in its emulator. This emulator helps the developer to develop and test his mobile applications on his computer without the use of an actual mobile device. There are a few pre installed applications available in the emulator which can be used from an android application. These preinstalled applications include SMS (Short Message Service), MMS (Multimedia Message Service), alarm clock, calendar, contacts. That is user can activate SMS application from his own application. Also the Android AVD manager provides a better way to change the version of the android system in the emulator, to include sdcard or not in user application, to change the skin of the emulator and lots of other settings. How to configure a new AVD to run a new application on the emulator and lots of other settings. How to configure a new AVD to run a new application on the emulator and how to configure the scared enabled can be seen in Figure 4.5. and Figure 4.6

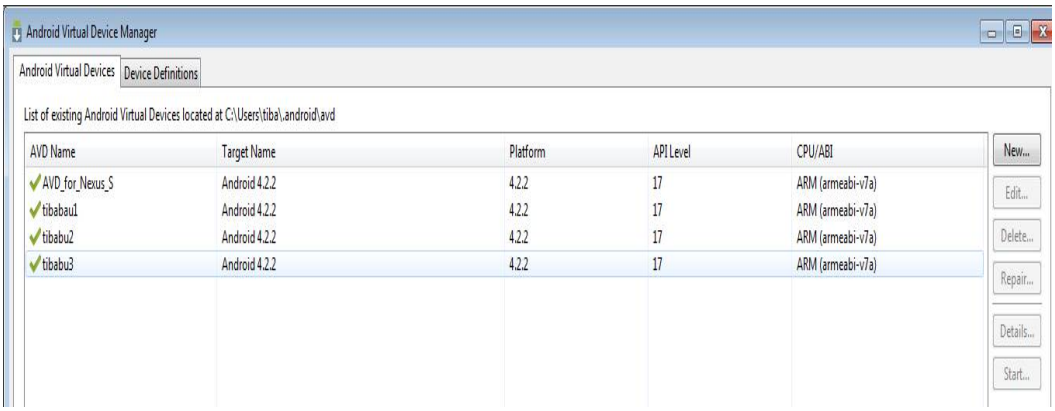


Figure 4. 4: Android SDK and AVD manager.

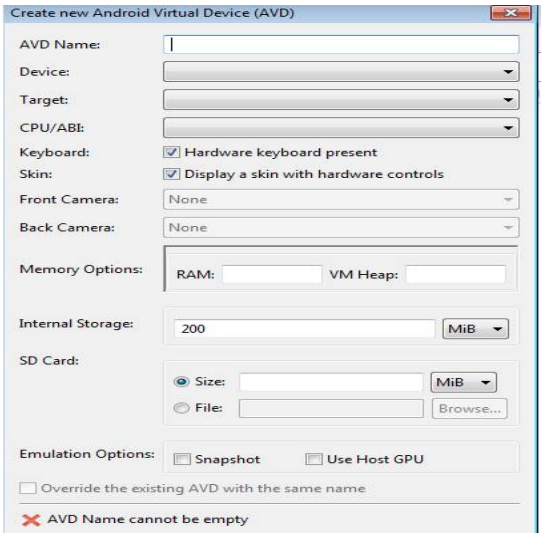


Figure 4. 5: Creating new AVD with SDCARD.

ISSN 2320-9186

The proposed secure mobile framwork, first of all it will recive the plan text from user then it can encrypt the plain text by using AES-128, after that the system can hide the encrypted message by using LSB algorithms methods. Now message encrypted and hidden in Image because we use two different algorithms to secure the system. Incase if one algorithm fail the other algorithms can save the securet message. That is why we are motivated to use mult-security algorithms. After hiding the message the sender can send the Stego Image in email or phone number. The view for how the sender sends the Stego Image in email using the Android emulator is shown in figure 4.8. The sender wants to send email to the receiver attaching the Stego Image in the email. ACTION SEND is used to send email from the emulator. Basically, it tells the Android system that your application wants to send some sort of message. Here Intent is the class provided by android. putExtra() is a method for adding extra data to the message. Here we are adding the receiver's email id, url of Stego Image from sdcard, subject and message body of the email. Emailint.set type sets the type of data the sender wants to send. Here we have used "Image /jpeg" as a type of data send with email as in this Steganography technique the sender will send the Stego Image in the email .

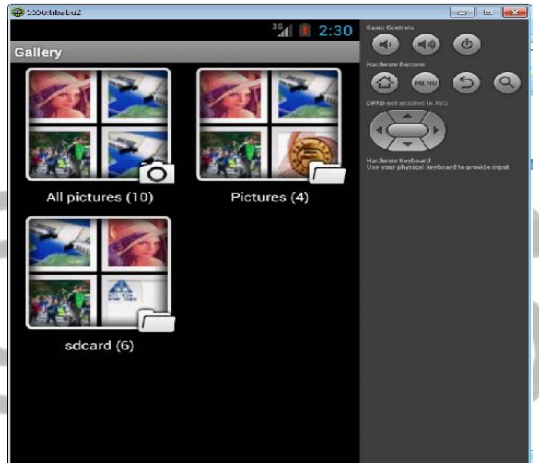


Figure 4. **6***: Androiud Sdk glarry*

4.3.1.1. Simulation Time during Encryption

The time required by the algorithm for processing completely a particular length of data is called the simulation time. It depends on the processor speed, complexity of the algorithm etc. The smallest value of simulation time is desired.

Encryption algorithms have been tested with different text size files. Simulation results are given in Table 4.2 and graph 4.1 for the selected four encryption algorithms. The Main purpose here is to calculate the Encryption speed of each algorithm for different packet sizes. Figure 4.1 shows comparison among SDES, DES, RC2 and AES based on time taken result during encryption. By analyzing the Table 4.4 and graph 4.1, the results that AES has an advantage over other SDES, DES and RC2 in terms of time consumption and. A second point can be noticed here; DES need low time consumption than RC2 and SDES encryption data. The third point is that SDES has low performance in terms of time consumption when compared with RC2, DES and AES. It requires always more time than RC2, AES and DES because of its triple phase encryption characteristics.

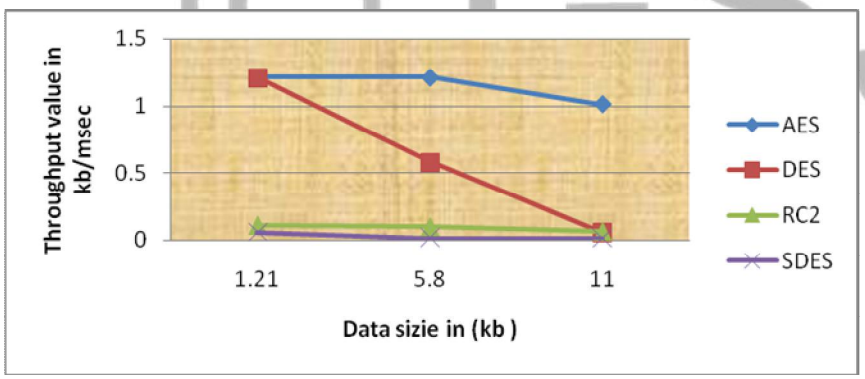
ISSN 2320-9186

Table 4. 3: Time consumption during encryption

		AES	DES	RC2	SDES
	1.1 kb	0	0	0.001	0.002
	5.8 kb	0	0.001001	0.001001	0.04
	11kb	0.001001	0.02001	0.02001	0.08

Graph 4. 1 Time consumption in Millisecond.

4.3.1.2. Power consumption



Graph 4. 2 Power Consumption during Encryption

The throughput of the encryption scheme is calculated by dividing the total plaintext in KB by total encryption time in Millisecond for each algorithm.

Throughput = plain text (kb) /Encryption or Decryption time (sec) ……..... (1)

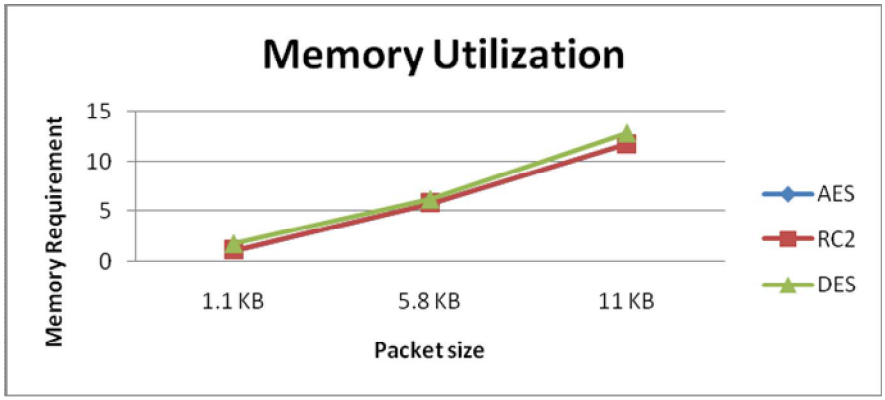
If the throughput value is increased, the power consumption of this encryption technique is decreased. Based on equation (1) we calculate the throughput value. As graph 4.2 indicate the AES power saver than DES, SDES and RC2. The second point is DES is power saves than RC2 and SDES algorithms. The third point is SDES is power consumer than AES, DES and RC2 algorithms.

ISSN 2320-9186

4.3.1.3. Memory required for implementation

Different encryption techniques require different memory size for implementation. This memory requirement depends on the number of operations to be done by the algorithm. It is desirable that the memory required should be as small as possible.

Memory utilization of AES, RC2 and DES algorithms are evaluated here, as the below graph 4.3 and table 4.5 indicate the memory utilization of AES and RC2 are lower than DES. DES needs the higher memory space during encryption and decryption. Low memory consumption is essential to save memory space.

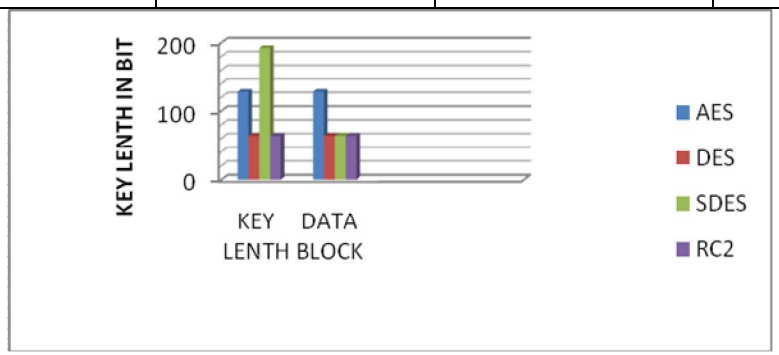


Graph 4. 3 Memory utilization of DEA.AES and RC2

Table 4. 4: Memory utilization of DEA.AES and RC2

4.3.1.4. Security strength

	Algorithms Name		
Packet size	AES	DES	RC2
1.1 KB	1.124 KB	12.08 KB	1.124 KB
5.8 KB	5.863 KB	5.864 KB	5.863 KB
11 KB	11.726 KB	11.728 KB	11.726 KB



Graph 4. 4 key length and Data block Used by AES, DES, and RC2 AND SDES

ISSN 2320-9186

Table 4. 5: Key length and Data block used by AES, DES, RC2 AND SDES

	Name of algorithms			
	AES	DES	RC2	SDES
Key length	128 bit	64 bit	128 bit	192 bit
Data block	128 bit	64 bit	64 bit	64 bit

Security of the data directly depends on the key length and data block of encryption and decryption, higher key length and higher data block will provide higher security. As table 4.6 and graph 4.4 indicate key length of SDES 192 and its data block is 64 bit. AES algorithm key length 128 bit and data block to encrypt and decrypt is 128 bit. RC2 algorithm use 128 bit key length and 64 bit data block. DES algorithms use 64 bit lengths and 64 bit data block to encrypt and decrypt data. Based on key length SDES an algorithm is can provide good security but SDES use 64 bit data block and it is time consuming. Second point is in terms of both key length and data block lengths AES provide good security. And also it is time saver during encryption and decryption. In our proposal we select AES algorithms which is time saver, power saver and providing good security algorithms to secure mobile banking frame work.RC2 algorithms use 128 bit key length but it us only 64 bit data block, so it can provide less security than AES and SDES algorithms. DES algorithms less secure than AES, SDES and RC2 because of its key lengths and data block lengths bit.

4.4. *Analysis Quality of Image*

4.4.1. Mean Squared Error (MSE)

Mean Squared Error is the average squared difference between a reference Image and a distorted Image. It is computed pixel-by-pixel by adding up the squared differences of all the pixels and dividing by the total pixel count. For Images A = {a1 ...aM} and B = {b1 ...bM}, where M is the number of pixel.

$MSE\ (A, B) = 1/M\ (ai - bi)^2$ …… (2)

The squaring of the differences dampens small differences between the 2 pixels but penalize large ones.

4.4.2. Peak Signal-to-Noise Ratio

Peak Signal-to-Noise Ratio is the ratio between the reference signal and the distortion signal in an Image, given in decibels. The higher the PSNR, the closer the distorted Image is to the original. In general, a higher PSNR value should correlate to a higher quality Image.

For Images A = {a1 ... aM}, B = {b1 ... bM}, and MAX equal to the maximum possible pixel value (2^8 - 1 = 255 for 8-bit Image s):

$PSN\ R\ (A, B) = 10\ LOG_{10}\ [MAX^2/MSE\ (A, B)]$…….. (3)

Note that MAX is the maximum possible pixel value of the Image s. For example, if the pixels are represented using 8 bits per sample, then the MAX value is 255. If the Stego Image has a higher PSNR value, then the Stego Image has more quality Image. Table 4.4 shows the PSNR value for four different Image s. The PSNR is calculated using the equation of PSNR in Eq. (3**)**

ISSN 2320-9186

a) Original b) stego c) original d) Stego

Figure 4.10 Student Images and Commercial Imag

The quality of image which found on figure 4.10 and figure 4.11 evaluated. The result of image quality shown on table 4.7. And graph 4.5

a) Original b) Stego c) Original Image d) Stego Image

Figure 4. 7: Dashen Bank and Millennium Image

Table 4. 6: PSNR value of four different Images

Image	PSNR value			Image size
Name of Image	BLUE	GREAN	READ	Dimension
Commercial Bank	31.02	32.619	31.719	440x346
Dashen Bank	16.652	15.196	14.304	300x300
Students image	35.645	35.645	35.645	512 x512
Milinium12345	34.255	35.687	35.348	450 x307

6.1. Conclusion

The biggest advantage that mobile banking offers to banks is that it drastically cuts down the costs of providing service to the customers. Because bank not need more employee in bank and customers not go to bank to receive his /her balance, this can decrease the cost expenditure to employee and transport. It will enable financial institutions to enhance relationships with their customers through more timely, flexible and personalized services.

ISSN 2320-9186

Mobile usage has seen an explosive growth in most of the Asian countries like India, China and Korea. The scale at which Mobile banking has been growing can be measure by looking at the speed by which the number of mobile users has increased in these big Asian economies. In Ethiopia also Dashen Bank and Commercial Bank of Ethiopia use plain text of SMS for mobile banking, which can be easily attacked by unauthorized person. So that mobile banking has the security problem that needs the solution.

In this thesis we proposed approach secured end-to-end communications because it is required that MMS must be secured even from the network operator. The main concept of this proposal is that do the ciphering by using AES algorithm first, and then the hide the cipher text by LSB algorithm.

The proposed mobile banking framework can provide:

- Convenience - perform banking transactions anytime, anywhere with low cost, because the AES algorithms, we used are a memory and power saver algorithm.
- Security – The data can be transfer are encrypted and hidden by single key, this can increase the strength of mobile banking security, because of multiple algorithms used.

REFERENCE:

1. *Mohammad Shirali-Shahrez "Mobile Banking Services in the Bank Area" Sept. 17-20, 2007, Kagawa University, Japan*
2. *Manoj V, " V ,SMS BASED SECURE MOBILE BANKING" International Journal of Engineering and Technology Vol.3 (6), 2011, 472-479*
3. *Mohammad Shirali-Shahreza "Improving Mobile Banking Security Using Steganography" International Conference on Information Technology (ITNG'07) 0-7695-2776-0/07 $20.00 © 2007*
4. *AnupK.Ghosh and Tara M.Swaminatha, "Software Security and Privacy risks in Mobile E-Commerce", Communications of the ACM, Vol.44, Issue 2, pp.51-57, 2010.*
5. *NeeteshSaxena,"Enhancing Ssecurity System of Short Message Service for M-Commerce in GSM ",International Journal of Computer Science & Engineering Technology (IJCSET) ISSN :*
6. *Mary Agoyi, DevrimSeral, "SMS Security: An Asymmetric Encryption Approach", Sixth International Conference on Wireless and Mobile Communications, 2010@IEEE, pp 448-452.*