International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-8 Issue-11, September 2019

Secure M-Banking using Steganography

S.Mangayarkarasi, K.Suganya, T.Sree kala

***Abstract*: The overwhelming use of sensible phones and also the extraordinary growth of web users worldwide for all of your wants are necessary currently each day. The security challenges are varied and escalating because of enormous amounts of cash flowing across shoppers and banking establishments. Banks are searching for differing kinds of choices to safeguard users' privacy and to safeguard them against many attacks. During this paper, we have a tendency to target mobile good phone banking by providing identity verification for mobile good phone users, i.e. secret data can be represented as username, password and face recognition. We have a tendency to additionally propose the utilization of varied ways of every which way choosing steganography to enhance the protection of the line for intrusion and hacker detection .**

Keywords: LSB, SLSB, AI-Bit, RGB.

I. INTRODUCTION

Smart phones of the new era area unit terribly powerful will perform all the operations that your notebook computer can do. In each sector and company, technology drives the requirement to grasp dynamical client wants [4]. There's additionally no exception to the money sector. The combination of mobile devices like good phones and tablets into a corporation offers workers the chance to figure a lot of with efficiency. To satisfy all money wants of client banks, good phones and also the net is used a lot of quickly by developing smarter and safer applications. The combination of good phones with applications has additionally diode to a range of security challenges and risks. Despite the benefits of quality, flexibility and hardiness of good phone net use, several banks use standard security mechanisms. Good phones area unit exposed to a range of threats, like notebook computer, that should be countered. It's unlikely that the straightforward implementation of knowledge security standards in server domains with mobile devices is effective for banks and users [1]. Therefore, the amount of security on good phone devices isn't clear from the banking purpose of read [10] [16]. In general, a safety of phone devices is achieved by setting a high level restriction. This reduces the acceptance of users for applications and satisfaction factors [7]. Steganography is a better medium for sending secret message sharing [15].

In this paper three completely different algorithms are presented. The Algorithms are Least Significant Bit , SLSB, and AI-Bit Steganography. Random choice of any LSB formula, SLSB, AI-Bit to send username and countersign to server in encrypted format will increase security. Only 1 key and also the image employed in the steganography (cover image) area unit sent in associate mutually beneficial approach. Supported the key price, the server detects that formula to use to decipher username and countersign. Then the server initiates the request to start out the camera on a mobile device. Employing a camera user, the camera user takes his/her image and sends it and matches the face with the offered information.

II. LSB, SLSB, AI-BIT ALGORITHM

Faster net and with the event of digital signal process, scientific theory and theory of secret writing, steganography has become "digital" [7]. For a laptop, a picture is associate array of numbers representing picture element intensity level. These pixels frame the formation information of the image up to three hundred KB. A typical image size is represented as 640 & 480 pixels and 256 colours. Ordinarily digital pictures square measure in either 24-bit or 8-bit files. The foremost area to cover data is provided by a 24-bit image. All picture element color variations cone from 3 main colours: red, inexperienced and blue. Every primary color is drawn by one byte; 24-bit pictures use a color worth of three bytes per picture element. These 3 bytes square measure positional representation system, decimal and binary values. The background color of the many sites is drawn by a six-digit positional representation system range, 3 pairs representing as red, inexperienced and blue[1]. The white background would have the FFFFFF: 100 percent red (FF), 100 percent inexperienced (FF) and 100 percent blue (FF) worth. Its decimal worth is 255, 255, 255, and its binary worth is 00000000, 10101010, 00001111, three white bytes.

A. LSB Algorithm

The least vital bit (LSB) insertion could be a normally used, with easy embedding data in an exceedingly cowl image [14] approach. A picture of 800=600 pixels will so store a complete quantity of one 440,000 bits or one hundred eighty,000 bytes of embedded knowledge. As an example, a 3-pixel grid of a 24-bit image is often as follows[1];

(10101010 10001010 10100101)
(01100110 00001111 1111000)
(11001100 10000001 01111110)

When the quantity two hundred, that binary illustration is 10101010, is embedded within the least vital bits of this a part of the image, the ensuing grid is as follows

Manuscript published on 30 September 2019.
*Correspondence Author(s)
S.Mangayarkarasi *, Assistant Professor, Department of Computer Science, VISTAS, Chennai. India. Email: mangai.scs@velsuniv.ac.in
K.Suganya, Assistant Professor, Department of Computer Science, VISTAS, Chennai. India. Email: sukka3112@gmail.com
T.Sree kala, Assistant Professor, Department of Computer Science, VISTAS, Chennai. India. Email: sreekala.scs@velsuniv.ac.in

(10111110 10001010 10100101)
(01100110 00001111 1111000)
(11001100 10000001 01111110)

Although the amount was embedded within the 1st eight bytes of the grid, solely the three highlighted bits modified by the embedded message. On average, solely 1/2 the bits in a picture should be modified to hide a secret message with the size. Since every primary color like RGB has 256 doable intensities, the LSB of a peel ends up in little changes in color intensity.. With a happy image, one will even hide the image within the smallest bit, second to smallest, and still not see the distinction. LSB uses BMP pictures in its simplest kind thanks to the employment of lost compression. Sadly, you'd want a really giant cowl image to cover a secret message within a BMP file. Nowadays, 800 & 600 pixels of BMP pictures don't seem to be typically used on the web and will cause suspicion. LSB steganography has so additionally been developed to be employed in alternative image file formats [8, 9].

B. SLSB Algorithm

The SLSB algorithmic program filters the quilt image victimization the default filter with concealing data in areas wherever the speed improves. The e filter is applied to the foremost necessary bits (MSB) of every constituent of the image, going the data decreased to cover. This filter confirms the choice of areas within the image for the smallest amount impact with the inclusion of data that makes it harder to find the existence of hidden messages. The data retrieval is confirmed as a result of the bits used for filtering doesn't seem to be modified, inferring that the filter can choose an equivalent bits throughout the concealment method. It's the foremost economical technique to cover data [8, 9].

C. AI-BIT Steganography

In the primary place, the semi-random pixels altered to inscribe every letter

- Whatever message we wish to enter in a picture, the primary step is to count variety of letters within the message we wish to enter and divide by that range the overall number of rows of pixels within the image.
- Next, take the pixel-wide image range and divide the alphabet by the amount of letters (26). If the image is 780 pixels wide, divide it by twenty six to induce thirty columns per alphabet letter.
- By grouping along these sets of ten rows and thirty columns, we have a tendency to get an element set grid within the image. Each of those sub-grids corresponds to separate message letter cryptography. Row teams correspond to the letter index within the message and column teams correspond with the particular letter cryptography displayed in table one.

III. PROPOSED WORK

A. Training A Information

1. Cr = Nr / NI
2. CC=Nc / Co
3. If Index < N
4. Key = h [m]
5. Value = h[key]

   Row = Cr* index + (AI-Bit)

   Col = Cc * Value + (AI-Bit)

6. Bit = image [Row] [Col] =!Bit

Table 1: Training the information

IMAGE GRID	COLS 0-25	COLS 26-51	COLS 52-77	COLS 78-103	COLS 140-129
Row 10-19	Letter 1=a	Letter 1=b	Letter 1=c	Letter 1=d	Letter 1=e
Row 20-39	Letter 2=a	Letter 2=b	Letter 2=c	Letter 2=d	Letter 2=e
Row 30-49	Letter 3=a	Letter 3=b	Letter 3=c	Letter 3=d	Letter 3=e
Row 40-49	Letter 4=a	Letter 4=b	Letter 4=c	Letter 4=d	Letter 4=e
Row 50-59	Letter 5=a	Letter 5=b	Letter 5=c	Letter 5=d	Letter 5=e
Row 60-69	Letter 6=a	Letter 6=b	Letter 6=c	Letter 6=d	Letter 6=e

B. Retrieving

Even this randomness, as a result of the letter seems within the same order because the bits altered by happening the row within the message. Only decoders grasp that teams match every letter.

Our improvement approach is:

1. Notice the last bits of the primary 3 columns.
2. This variety offers US the precise column variety wherever the bit variance is checked.
3. We will use the previous or next column for embedding bits to extend the payload capability.

C. Golem Software System Stack

Figure1 illustrates the stack of golem software system consisting of a UNIX kernel, a group of golem libraries, an application framework managing golem applications in runtime, and native or third-party applications within the layer of applications.

D. Authentication Mechanism Summary for Banks

The following are the various choices used underneath every of the 3 factors.

Table 2: Security Mechanism summary of Bank

User knows	User possesses	User Is
Username	USB Token	Fingerprint
Password	Smart Card	Palm print
PIN	OTP by	IRIS
Card No.	SMS/token	Voice
CVV2	Swipe cards	Vein pattern
3D Secure/ VbV	Mobile Signature	
Identifiable picture		

E. Security Pitfalls Of Varied Schemes

The server selects the positive identification and sends it to the user, which can be long, random and troublesome for a user UN agency is employed in several systems.

Transmission of login messages via an insecure channel like the net to the authentication server is risky.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

In eventualities like transactions, it's vital to keep up a user ' s privacy as a result of an opponent sniffs within the channel. The communications parties concerned within the authentication method for the analysis of the user's dealings. Losing sensible cards or random range generator is one among the foremost serious issues as a result of a lost card or random range generator will copy a legitimate user. The overall application model is represented in Figure 1.

Information like username And positive identification through an unsecure channel like the net are often extracted by anybody by sniffing the packet.

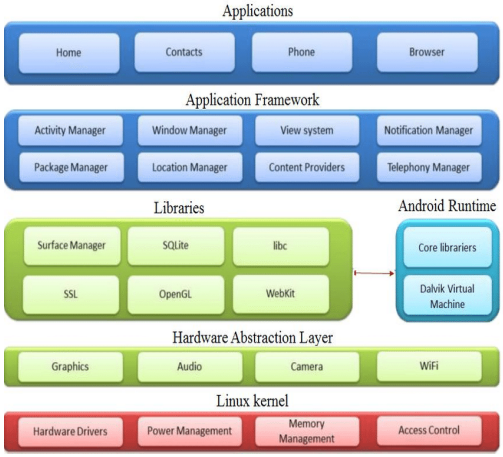

Figure 1: Application Model

F. Proposed Technique for Mobile Banking

In India, leading banks use the secure image to send encrypted image username and secret. Pictures should be hand-picked from a restricted set of pictures hand-picked by the bank. These restricted pictures of an explicit size and backbone square measure hand-picked by the bank.[18]. They embrace username and word within the image and send it via the unsecured network.

Our projected security model, we tend to use mobile purchasers to insert username and word within the mobile image. From Fig1. We tend to additionally choose the random algorithmic rule from any of the steganography algorithms like LSB, SLSB, and AI-Bit.

In order that the entrant or hacker ought to strive all doable algorithmic rules to interrupt notwithstanding he is aware of the algorithm used for cryptography. Second authentication technique, we tend to use the face detection mechanism to attest the user. The careful procedure for victimisation the mobile phone phone for M-banking is shown Figure 2.

Step 1: User login to the golem device mobile consumer application with their user Id and word. This username and word is encrypted in any image from the SD card hand-picked by the user. Mobile consumer encrypts username and word within the image by haphazardly choosing any LSB, SLSB, and AI-Bit algorithms. this can be sent to the server via the unsafe channel.

Step 2: Server aspect is employed to decipher the username and word victimisation the decipherment mechanism accustomed send this image. If the word doesn't match the word on the server aspect, authentication fails if match is found, then step three.

Step 3: If a username and word match is found, then the server sends the request to the mobile consumer to start out the camera instance.

Step 4: Upon beginning the mobile camera, the user clicks on his image and sends it back to the server. The server matches the image to the accessible information with associate degree algorithmic rule for face detection.

Step 5: Match is finished then more operation is started.

Step 6: Logout the M-banking activity and end it

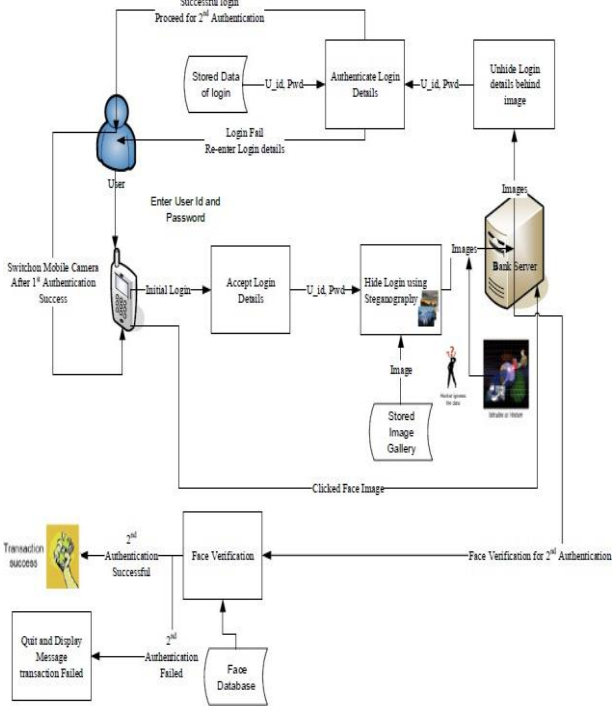

Figure 2: Proposed method for S-Banking

IV. IMPLEMENTATION

The automaton mobile consumer should have a sensible phone with a camera with smart resolution and therefore the ability to browse the web through the Wireless Access Protocol. From Fig2 an infatuated standalone consumer / server design base application is needed for communication between user and bank to be with success complete. However, the bank should offer the user with the mandatory consumer software system or consumer application and therefore the automaton Play Store will be downloaded and put in on the good phone. This application will be used on the automaton package good phone.

A. Experimental Results

The experimental results of various steganographic algorithms are represented in Table 1.

Table 1 : Various Steganographic Algorithms Performance Results

Performance Measures	LSB	SLSB	AI-BIT
MSE	198.10	➢ 198.45	➢ 186.45
SNR	24.06	24.06	24.06
PSNR (MAX=255)	➢ 24.61	24.81	24.81
PSNR (MAX=255.0)	24.61	24.94	24.94

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

The era of mobile banking is not any finish and therefore the planned mechanism for authentication will be extended to mobile looking, that has additionally grownup apace with the introduction of on-line promoting. Comparison Results represented in Figure 3

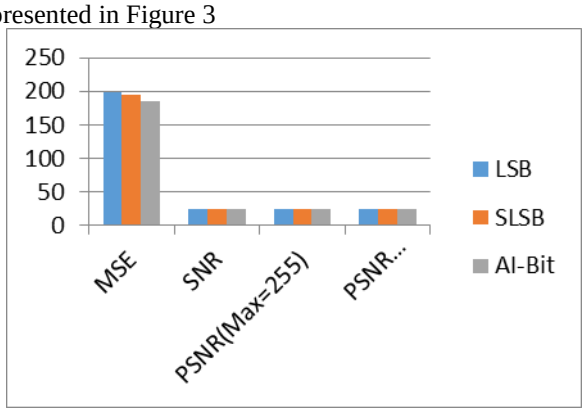

Figure 3: Comparison between Stenographic algorithms

Various organizations like the government and the personal sector will give and promote electronic services via mobile phones. The good phone practicality will be additional extended to totally different locations. Mobile ballot exploitation biometric identification like camera that identifies everyone and may forged their votes remotely. The role of authentication becomes vital all told the on top of applications and our theme is incredibly strong and secure in such eventualities

V. CONCLUSION

In this paper, we tend to mentioned numerous steganography techniques for remote user authentication schemes used for mobile customers. First, we tend to discuss the strategies of steganography wont to increase security. There are several issues known within the mobile banking security mechanism accessible. In this paper we proposed improved script approach supported for biometric with face detection improves all known weakness and strong for the $64000 use of mobile banking. Additionally to providing a much better and safe mechanism, the planned theme will stand up to invented authentication attacks.

REFERENCES

1. Rethink the “Mobile” in Mobile Banking Disruptions and Innovations in Mobile Communications Technology, March 2013.
2. Security for Mobile ATE Applications: Susan Moran Senior Software Engineer, EADS North America Test and Services Irvine, CA: 978-1-4673-0700-0/12/$31.00 ©2012 IEEE.
3. Chang-Lung Tsai Chun- Jung Chen, Deng-Jie Zhuang: “Secure OTP and Biometric Verification Scheme for Mobile Banking”, IEEE. 2012.ISBN 978-1-4673-1956-0. Understanding Android Security: Published bythe IEEE Compute society: 1540- 7993,2009
4. http://www.techotopia.com/index.php/An_Overview_of_the_Android_Architecture.
5. Dushyant Goyal, Shiuh-Jeng Wang, “Steganographic Authentications in conjunction with Face and Voice Recognition for Mobile Systems” , International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 10, October 2015.
6. Neil F. Johnson, Sushil Jajodia ,”Exploring Steganography Seeing the Unseen” ,George Mason University: 0018-9162/98 2008 IEEE.
7. Niels Provos, Peter Honeyman: “Hide and Seek: An Introduction to Steganography”, University of Michigan: 1540-7993, 2003 IEEE.
8. Basel Hasan, Viktor Dmitriyev, Jorge Marx Gómez, Joachim Kurzhöfer, “A Framework along with Guidelines for Designing Secure Mobile Enterprise Applications” , 978-1-4799-3532- 1, IEEE ,2014.
9. Anurag Kumar Jain, Devendra Shanbhag, “Security and Privacy Risks in Mobile Applications” Published by the IEEE Computer Society 1520-9202, 2012 IEEE.
10. Dharmarajan K, M. A. Dorairangaswamy, “Discovering Student E-Learning Preferred Navigation Paths Using Selection Page and Time Preference Algorithm”, International Journal of Engineering and Technologies in Learning (IJET) 12.10(2017):202,211.
11. http://www.sans.edu/research/securitylaboratory/article/2factor-banks
12. http://www.pcworld.com/article/2079620/banks-shouldnt-rely-on-mobile-sms-passcodes-security-firm-says.html
13. Dr. P.Sujatha and Ms. S. Mangayarkarasi, “Data Concealment Approach with Steganography”, International Journal of Applied Engineering Research, Vol.9, No.27, pp. 9697-9700, December 2014.ISSN:0973-4562.
14. http://www.techotopia.com/index.php/An_Overview_of_the_Android_Architecture.
15. https://www.duosecurity.com/blog/the-current-state-of-online-and-mobile-banking-security
16. S.Mangayarkarasi and K.Suganya, “Image Steganography Based Improving M-Security”, International Journal of Management, Technology and Engineering (IJMTE), Volume IX, Issue I, January - 2019, ISSN: 2249-7455. PP : 1000-1006