ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 10, October 2015

Steganographic Authentication in Conjunction with Face Recognition for Mobile System

Sharma Davinder Kumar[1], Dumane Sagar Vinayak[2], Dumbre Anup Sanjay[3], Gadalikar Ashok Bhau[4], Sandip A Khate[5]

Department of Information Technology, SPCOE College of Engg Dumbarwadi, Pune, Savitribai Phule Pune University, India[1, 2, 3, 4]

Assistant Professor, Dept of Computer Engg, SPCOE College of Engineering Dumbarwadi, Pune, India[5]

Abstract: In today world Securing data is a challenging issue. Most of data travel through the internet and it becomes difficult to secure data. Today mobile-commerce is a new branch of e-commerce, mobile-banking is main part of m-commerce. But the problem in mobile banking is security how to secure the user information such as username, password etc. The aim is to provide a secure environment in terms of security for transaction. In this paper we focus on authentication in conjunction with face recognition for mobile system. For this we use m-banking. We will make use of steganography to improve the communication channel. Steganography is defined as the invisible communication. There are several types of steganography techniques each have their own strengths and weaknesses.

Keywords: Mobile banking, Mobile commerce, Encryption, Decryption, Network Security.

I. INTRODUCTION

As we know that internet has become integral part of everyone life many people's wants to manage their bank account anywhere, anytime over internet. The user wants to keep their important data secret and safe. Steganography and cryptography are the two basic methods which we can use to share data in safe way. In Cryptography we convert message from readable form to unreadable form or in simple way we can say that we encrypt the message at sender side and decrypt the message at receiver side. In cryptography encryption key is generated which is known to sender and receiver. In cryptography we can't read a message without encryption key or message is not accessible. But in cryptography it's always known to the hacker or intermediate person that the message in encrypted form. The steganography is a word taken form Greek which means, "Covered".

In Steganography technique we used to transmit a secret message from a sender to a receiver in such a way that only receiver can read the existence message no intermediate person can read the message. In steganography we can hide the information in the form of image, text, audio and video. In old time, we protected data by hiding it on the back of wax and writing tables. Steganography is a security technique for long transmission. To hide secret information or data in images, there are number of steganography techniques in which some are easy while other are complex all of them have their strong and weak points. Image steganography Provides security when we are sending file over internet. The network security is becoming more important because the number of user exchange the data over internet. We need to protect the data so that unauthorized user can't access it. Mobile banking generally offered account information, transfer, cards and payments etc.

In this paper we are going present how we can save the secret information from hackers when user is accessing its account over internet.

II. PROPOSED SYSTEM

For implementation of proposed system we must require Mobile device with GPRS camera should enabled in it. User should know the basic knowledge of internet and mobile. Client server application is require for successful communication between the customer and bank. Bank should provide software to client for authentication and transaction purpose. There could be difference in Speed of data transfer which may depend on mobile server. On client side there should not be mobile network problem.

III. RELATED WORK

M-commerce as one of the new branches of E-commerce, M-banking is one of the main part of M-commerce. There are many advantages of m-banking but now day's M-banking is facing security challenges as well. In this paper we are going to presents a method in which how to secure the security of the information requested by users with the use of Steganography method. In this way, instead of directly sending the information it is encrypted first and then hidden in a picture using random bit Steganography method. Then the picture is sent to the server. After receiving the picture the server download the image, decrypts it and decodes to receiver. Then the message is processed on the server to verify user information such as user name and password. Once information is entered, camera is switched ON than the client side and image is captured. Then this image is compared with the database images on successful match user are taken to the menu screen.

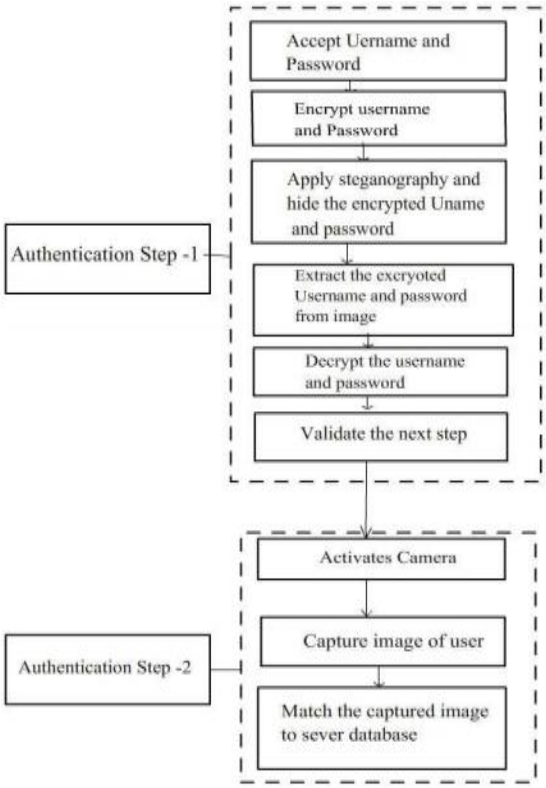
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 10, October 2015

IV.ALGORITHM USED

In this paper, we are using Advanced Encryptions Standard Algorithm (AES) Least Significant Bits (LSB) to hide the information. Advanced Encryptions Standard Algorithm (AES) is a symmetric key algorithm that uses the key size 128, 192 or 256-bits depending upon the number of rounds. In AES each round contain byte substitution, row shift, column mixing and round key addition Advanced Encryptions Standard Algorithm(AES)is a non-feistily cipher that encrypts and decrypts data block. In the least significant bits (LSB) we hide each byte of information in two pixels. In LSB the image is broken into p number of blocks of q number of pixels and a password is given. According to the password, a block is chosen and the important data is hidden in the pixel.

V.SYSTEM ARCHITECTURE



V. IMPLEMENTATION DETAIL

a) Setup
b) User Registration
c) Key Generation
d) Encryption
e) Decryption
f) Face Recognition

VI. ADVANTAGE

a) It is difficult to detect password by unauthorized because password is stored in an Image.
b) It increases the response time of bank server.
c) It provides high security.
d) This application is used to secure the sensitive information of the user.

VII.CONCLUSION

In this paper we have shown drawbacks of existing authentication system. In future, it will provide high security for user to share the important information over internet. Steganography will improve the drawbacks and provides the high security for the user. The proposed system is very secure and at same time mutual authentication can takes place between the user and bank. The future enhancement we can do is speech recognition, thump impression, iris scan, and keystroke.

REFERENCES

[1] Dushyant Goyal and Shiuh-Jeng Wang, Steganographic Authentications in conjunction with Face and Voice Recognition for Mobile Systems.

[2] Priyanka Sahute, Swati Waghamare, Supriya Patil, Ashwini Diwate, " Secure Messaging Using Image Stegnography" International Journal of Modern Trends in Engineering and Research (IJMTER) Volume 02, Issue 03, March - 2015.

[3] Jasleen Kour,Deepankar Verma**, "**Steganography Techniques –A Review Paper" International Journal of Emerging Research in Management &Technology ISSN: 2278-9359 (Volume-3, Issue-5) May 2014.

[4] Anil Kumar, Rohini Sharma**,"** A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique" International Journal of Advanced Research in Computer Science and Software Engineering 3(7),July - 2013, pp. 363-372**.**

[5] Ajit Singh, Swati Malik**, "**Securing Data by Using Cryptography with Steganography" International Journal of Advanced Research in Computer Science and Software Engineering 3(5),May - 2013, pp. 404-409.

[6] Souvik Roy , P. Venkateswaran, "Online Payment System using Steganography Visual Cryptography 978-1-4799-2526-1/14/$31.00 ©2014 IEEE.

[7] Hemalatha S, U Dinesh Acharya, Renuka A, Priya R. Kamath," A Secure Color Image Steganography In Transform Domain" International Journal on Cryptography and Information Security (IJCIS), Vol.3, No.1, March 2013.

BIOGRAPHIES

Sandip A. Kahate B.E. in computer science and engineering from Amravati university**,** M.E.in Wireless Communication and Computing, from Nagpur University and preparation for Ph. D. registration. He is currently working as an Assistant Professor in Computer Engineering Department, Sharadchandra Pawar College of Engineering, At. Post-Otur, Dist-Pune-412409(M.S.), India. He has 10 years of teaching experience. He is author of 1 research paper, with around 10 papers in international journal and 3 in international conference in India and abroad. His areas of interest are Wireless Communication and computing, network security and Ad-Hoc Network.

Gadalikar Ashok Bhau Department of Information Technology, Sharadchandra Pawar college of Engineering, At. Post-Otur, Dist-Pune-412409(M.S.), India. Affiliated to Savitribai Phule Pune University, HSC in 2009, Maharashtra State Board Pune.

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 10, October 2015

Dumane Sagar Vinayak Department of Information Technology, Sharadchandra Pawar college of Engineering At. Post-Otur, Dist-Pune-412409(M.S.), India. Affiliated to Savitribai Phule Pune University, HSC in 2009, Maharashtra State Board Pune.

Dumbre Anup Sanjay Department of Information Technology, Sharadchandra Pawar college of Engineering At. Post-Otur, Dist-Pune-412409(M.S.), India. Affiliated to Savitribai Phule Pune University, Diploma in 2011, Maharashtra State Board of Technical Education Mumbai.

Sharma Davinder Kumar Department of Information Technology, Sharadchandra Pawar college of Engineering At. Post-Otur, Dist-Pune-412409(M.S.), India. Affiliated to Savitribai Phule Pune University, HSC in 2010, Andhra Pradesh State Board Hyderabad.