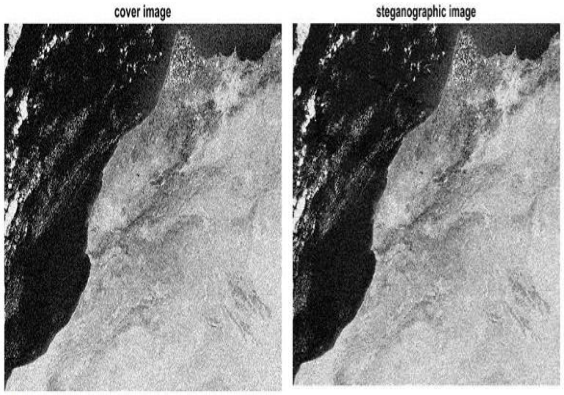
ATM Detail Security using Image Steganography and Cryptographic Encryption Technique

Mannmay Mukesh Vinze[1], Jeevan Danve[2], Manish Bharti[3], Mohandas Pawar[4]
[1,2,3,4]*Computer Engineering, MIT ADT University, Pune*

Abstract **- In this digital world Automated Teller Machines (ATM) are extensively used worldwide. Banks are highly focused upon ensuring user security. Security of user`s financial assets is one of the most important asset since ancient times to the modern world. The number of online transactions have increased over the years. This increased number of digital transactions have attracted the hackers to steal users data as well as money. Over the years cyber-attacks have become modernized in order to and capable to crack traditional passwords. This study introduces image stenographic algorithm based upon cryptography and stenography in order to ensure the authenticity of the user. The proposed algorithm makes use of cipher text, stenographer image is placed at bank end. Image from. Cipher text or hash values are distributed between customer and banking end. When a user requests a financial transaction, hash values of both ends are compared and dynamic key is generated each time. In this way a unique key is generated each time for transaction.**

INTRODUCTION

Stenographic technique finds its extensive application in information and data security. The term stenography means "covered writing." In Digital world, stenography means covering the secrete information like user financial and account credentials in order to avoid detection and tracking. The covering content is called stego-medium, that claims to be the data itself but it actually covers the original data over the network. This exposed stego-medium file avoids attention towards the original content. Stenographic approaches are widely used in digital world in order to secure data over the network. Stenography plays the role of data security in combination with Cryptography [1]. First all stenography translates the information/data into encrypted content and then this encrypted content is embedded with cover medium. In this way cryptography and stenographic techniques perform their role to add confidentiality and authenticity. Both of these techniques work differently, cryptography encrypts the message by altering the message structure. In contrast to cryptography which focuses on keeping the message secret while the existence of secret message may tempt the attacker whereas Steganography hides a message as well as the very existence of secret information. Cryptography ensures privacy of message and structure of the message alter whereas steganography ensures the secrecy of message and the structure of message does not alter [2]. Steganography may use in conjunction with cryptography by concealing the existence of the ciphered text so that the information is more secure. The following images were used by Bhallamudi S. (2015) in order to explain the difference between the image used as cover and stego-image. Visually there seems to be no difference. But Stego-image includes the sensitive information that must be secured from illegal access [12].



There are number of media file formats that can be used as cover media for stenography. The type of stenography depends upon the media file used as cover media, e.g. audio, video or image file. Image stenography allows dealing with human visual system and embed the data into image format. This study investigates image stenography based encryption techniques in combination with cryptography, in order to secure transaction information of ATM users. The

methodology proposed in this study first encrypts the user data using RSA algorithm followed by the selection of image file as a cover. As a result a stego-image will be generated and shared among the user and bank end.

LITERATURE REVIEW

Guo and Le measured the quality factors of images regarding transmission of data based upon quantization tables and permutation techniques. The authors encrypted the message using Vernam cipher followed by embedding through Lease Significant Byte (LSB) technique and then combined the cryptography algorithm into it [3]. According to another research made by Seethalakshmi et al, the best points to hide or encrypt sensitive data into images. Petal and Meena also made an effort to superimpose cryptography and stenography. First of all picture selection is done pseudo randomly and then LSB of pictures if shuffled with MSB of picture [4]. Abood worked on embedding of cryptography and stenography. Encryption and decryption parts are done using RC4 cipher stream and steganalysis is done with RGB pixel shuffling. Number of authors proposed different strategies for hiding images based upon quantum technology [5]. First one of them recommends to hide the image into another image. Second strategy used water-marked Grey colored image to embed into carrier image. Qo et al, also proposed a different strategy in order to hide data in image format that is based upon matrix coding [9].

PROBLEM STATEMENT

This is the era of science and technology and people all around the world use ATM machines for making financial transaction. Hackers are interested to hack these financial transaction for stealing data as well as money. There is a strong need to investigate the encryption of user data in order to make sure the security of sensitive financial data. In this way user`s personal as well as financial data can be secured.

METHODOLOGIES

There are number of approaches being used for embedding data encryption through cryptography and stenography. In this study RSA algorithm is used for cryptography along with image stenography.

RSA Algorithm is extensively used for cryptography. It is based upon two type of keys, public key and private key. Two random prime numbers are chosen (p and q) and their random products are used to generate public as well as private keys. Public key includes two values modulus and exponents, while private key only includes private exponent. The following figure depicts the generation and implementation of simple RSA algorithm fir data security purpose [13].

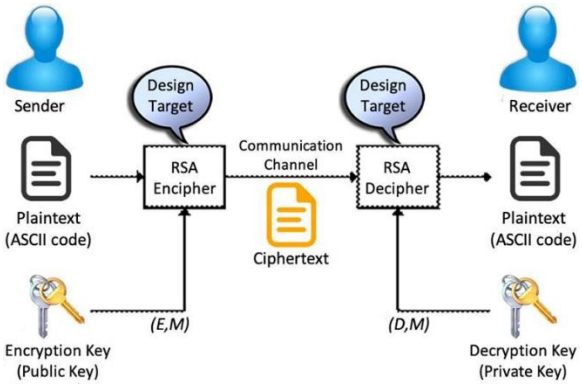


Image Stenography makes use of cover image in order to mask sensitive data. An image consist of pixels and each pixels is sub-divided into bits. Image data is stored in the form of bit sequence in the memory. A particular bit sequence represents the combination of RGB. Minor modifications in this bit sequence can encapsulate sensitive data into bit sequence of the original image. Different image formats like JPEG (Joint Photographic Experts Group) or GIF (Graphical Interchange Format) can be used for data encapsulation. But this study is focused upon securing ATM based information into JPEG images.

First of all the cipher text is generated after aforementioned RSA algorithm and then hidden into the .jpeg image file. Cipher text is mostly appended at the end of image bits and then exposed to network for transmission of data.

RMI Architecture is the most important part in order to implement this ATM user data security technique. RMI stands for Remote Method Invocation, that allows the network security programmers to introduce a distributed algorithm into the system. This algorithm creates a relationship between client and server. Server creates an object or model and makes it accessible from client end. Server in our case is bank`s server and client is ATM machine. ATM machine has a reference identification for a particular objects and calls that server with the help of that reference. In order to ensure a secure and successful connection ATM and

server objects are connected remotely on the basis of remote reference and Transport layer of network model. The overall RMI architecture is implemented in following steps; compilation of source code at both ends (server and ATM), generation of objects, installation, start RMI, start server and then start client.

PROPOSED TECHNIQUE

The module that ensures the security of ATM users` data, plays its role in two phases;

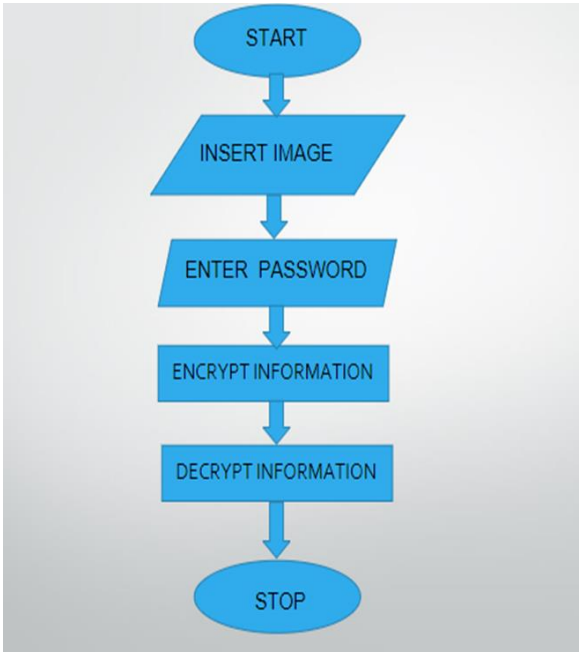
- Data Embedding
- User Authentication

The first phase, data embedding makes use of an image file to embed customer`s data into an image file. Before embedding this data is encrypted into cipher text (using RSA algorithm)and then embedded using LSB algorithm. Embedding includes appended the carrier image file bits with least significant bits of sensitive data file. As a result sensitive data gets merged into the image bits and image files still seems to be same, due to human visual limitations. Mostly the banking customer`s sensitive information includes account number, customer name, customer address, username, ATM pin, mobile number, etc. If a hackers gets access to any of these information he/she can be able to manipulate this data for financial gains. With the passage of time, hackers are using advanced and dynamic methods to access illegal information. In situation technologists and network security administrators also introduce advanced and refined methods to ensure data security against cyber-attacks. After the completion of embedding process, a hashing function generates a hash against the stego-medium file. Whenever a user comes to ATM machines following steps are performed;

Encryption (at ATM machine) includes selecting the sensitive data entered by the user, encrypting that content with RSA algorithm, selecting an image as cover medium, read header and footer of the selected image file, append image footer by adding cipher key generated as a result of RSA algorithm application, establish connection between ATM and bank server, sends stego-image to an IP address. This IP address refers to the bank server.

The following section is termed as User Authentication phase. In simple words this phase makes sure the credentials received from the ATM machine, entered by the user match the credentials of that particular user previously saved in bank database. This phase includes comparison between hash values received from the ATM machines and previously stored reference value for that user. Decryption (at Bank Server) is completed in following steps; receive the stego-image file and then read its herder and footer. Separate the cipher text from footer after comparing it with original image footer. Decode the cipher text by generating private key according to previously defined RSA algorithm, the same was used for encryption at ATM machine. If the values are same allow the user to perform financial transaction.

It should be noted here that RSA key plays very important role in order to ensure the security of sensitive data. The privacy and security of stenography and cryptography work relies upon RSA key. Bigger the size of RSA key, higher is the security of sensitive data. In this proposed mechanism we have used RSA algorithm that generates public and private keys from random prime numbers. These prime numbers are used to find modulus and size of RSA keys is directly related with number of bits used for the generation of modulus. In our implementation we have used 2048 bit key.



Overall ATM machine activity starts by establishing a link between ATM and bank server. After that, the algorithm implemented at bank end is used to generate cipher text from the data entered by the user. This cipher text is embedded into image file and stego-image is then sent over the network. This stego-image

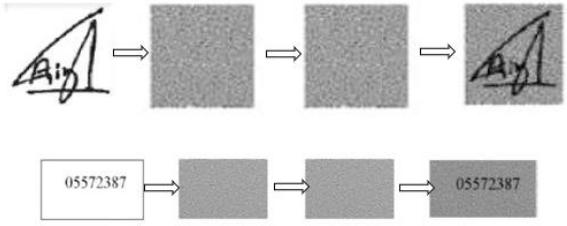
is decoded at the bank end. The overall process can visualized from the figure. The ATM machine algorithms are responsible to find a suitable image and then hide the information in it. The client end is also responsible to ensure that has code is sent only after making IP address of the bank server is identified and confirmed. After the receiving hash code or encrypted stego-image from the client-end, server perform decryption process and separates out the original sensitive information. User authentication is the main phase of this process, this is done at Bank server according to values stored in its database.

DATA-FLOW MECHANISM

As mentioned previously we aim to ensure the security of sensitive data of ATM machine user. For this purpose we embed this data into an image file before sending it to server. Additionally we add another process of cryptography that adds an additional layer of security into the overall process. Cryptography provides bits of cipher text that are appended into footer bits of the selected image and then sent to the server. This modified or stego-image claims to be the data itself but in actual it resides the data in itself in encrypted format. It should be noted here that stego-image seems to be the original image, there seems to be no change in visuals of the original image after embedding the data. So the hackers or any any person illegal accessing that image will conceive it to be a random image. On the other hand the receiver, Bank server receive the .jpeg image file and compares its bit sequence with originally stored parent image file and extracts the bit sequence of the cipher text. This cipher text is then decoded into the original sensitive information provided by the user.

RESULTS AND DISCUSSION

A number of researches recommend to user two factor authentication at ATM machines. PIN is first verified from the server send from the ATM machines. The server generates a random key that is again tested and verified at server end. This key or code is sent to registered mobile device and user enters it from ATM machines. Server matches this code with the code sent to that user`s device. After confirmation server allows the user to perform financial activity. Simple and easy to implement algorithms avoid over loading the client, server or network on one hand and keep the system responsive all the time. The images chosen for embedding are random, there is no need to use a particular image for this purpose. This approach vanishes the need of scanning for image generation process. However if hacker or any unauthorized person gets access to this image or image data, he/she can`t access the sensitive data. This image only includes a hash value. And only bank server knows where the hash value resides in the image bits and how to decode that hash value to get a particular users data. So no data or information is leaked or reveled to any third party trying to access that information illegally. This system is not only able to secure users data but also makes the overall process fast and error free. The following images represent how the actual image is encoded and decoded using cryptography followed by stenographic algorithms. Following images includes two different types of data, first one is signature and second one is digit, that can be pin or password or anything digital value. These original values are embedded into cover image, the third image shows stego-image that becomes after encoding the and fourth image is retrieved at server after decoding.



CONCLUSION AND FUTURE HORIZON

As the time passes human lifestyle is becoming more and more digital. Computer and internet is serving the mankind in number of ways. People do a lot of sale-purchase activities online. This huge financial activity welcomes cyber-attacks. In order to secure online and ATM based financial activities network security administrators investigate and launch more secure and practical mechanisms to secure bank infrastructure against cyber-thefts. This study investigated a similar mechanism that allows ATM machine user to communicate with bank server securely and easily over the network. Proposed algorithm uses encryption of sensitive data using RSA algorithm followed by embedding into .jpeg files. Then these .jpeg files are send over the network. As a result of combined

utilization of cryptography and stenography, we are able to misguide the hacker with a random image files that seems to contain no data in itself. Hackers are not attracted towards this random image file as it seem to contain no sensitive information. As a result they leave it undisturbed. In this proposed mechanism cryptography works to secure the original data by encoded it and stenography in combination with cryptography resides that encoded information and claims to have nothing in stego-image file. So only intended receiver knows the type and contents of information loaded on stego-image file. Receiver of bank server decodes this stego-image and and compares the hash values. In future we can make use of other image formats like GIF, etc for this embedding process in addition to audio or video files. Video files can help to transfer when huge amount of sensitive data needs to be embedded and transferred over the network.

REFERENCES

[1] Moorthy H, Rama. (2020). Steganographic And Visual Cryptographic Approach For Authentication Of Bank Users Using ATM Cards.

[2] Chandra, Sourabh & Paira, Smita. (2019). SECURE TRANSMISSION OF DATA USING IMAGE STEGANOGRAPHY. ICTACT Journal on Image and Video Processing. 10. 10.21917/ijivp.2019.0291.

[3] Jing-Ming Guo and Thanh Nam Le, "Secret Communication using JPEG Double Compression", IEEE Signal Processing Letters, Vol. 17, No. 10, pp. 879-882, 2010.

[4] Kamaldeep Joshi and Rajkumar Yadav, "A New LSB-S Image Steganography Method Blend with Cryptography for Secret Communication", Proceedings of 3rd International Conference on Image Processing, pp. 86-90, 2015.

[5] K.S. Seethalakshmi, B.A. Usha and K.N. Sangeetha, "Security Enhancement in Image Steganography using Neural Networks and Visual Cryptography", Proceedings of International Conference on Computational Systems and Information Systems for Sustainable Solutions, pp. 396-403, 2016.

[6] Nikhil Patel and Shweta Meena, "LSB Based Image Steganography using Dynamic Key Cryptography", Proceedings of International Conference on Emerging Trends in Communication Technologies, pp. 448-457, 2016.

[7] May H. Abood, "An Efficient Image Cryptography using Hash-LSB Steganography with RC4 and Pixel Shuffling Encryption Algorithms", Proceedings of Annual Conference on New Trends in Information and Communications Technology Applications, pp. 86-90, 2017.

[8] A.A. El-Latif, B. Abd El Atty, M.S. Hossain, M.D. A. Rahman, A. Alamri and B.B. Gupta, "Efficient Quantum Information Hiding for Remote Medical Image Sharing", IEEE Access, Vol. 6, pp. 21075-21083, 2018.

[9] Z. Qu, Z. Cheng and X. Wang, "Matrix Coding-Based Quantum Image Steganography Algorithm", IEEE Access, Vol. 7, pp. 35684-35698, 2019.

[10] Abdullah, Ako & Hama Aziz, Roza. (2016). New Approaches to Encrypt and Decrypt Data in Image using Cryptography and Steganography Algorithm. International Journal of Computer Applications. 143. 11-17. 10.5120/ijca2016910143.

[11] R, Poornima & R.J, Iswarya. (2013). An Overview of Digital Image Steganography. International Journal of Computer Science & Engineering Survey. 4. 23-31. 10.5121/ijcses.2013.4102.

[12] Bhallamudi, Savitha. (2015). Image Steganography. 10.13140/RG.2.2.21323.18727.

[13] Bodur, Hüseyin & Kara, Resul. (2015). Secure SMS Encryption Using RSA Encryption Algorithm on Android Message Application.