E-Banking Security using Cryptography, Steganography and Data Mining

Namrata Devadiga
Student of Computer Engineering
K. J. Somaiya COE
Vidyavihar

Harshad Kothari
Student of Computer Engineering
K. J. Somaiya COE
Vidyavihar

Hardik Jain
Student of Computer Engineering
K. J. Somaiya COE
Vidyavihar

Smita Sankhe
Assistant Professor of
Computer Engineering
K. J. Somaiya COE
Vidyavihar

ABSTRACT

The growth of E-Banking has led to an ease of access and 24-hour banking facility for one and all. However, this has led to a rise in e-banking fraud which is a growing problem affecting users around the world. As card is becoming the most prevailing mode of payment for online as well as regular purchase, fraud related with it is also increasing. The drastic upsurge of online banking fraud can be seen as an integrative misuse of social, cyber and physical resources [1]. Thus, the proposed system uses cryptography and steganography technology along with various data mining techniques in order to effectively secure the e-banking process and prevent online fraud.

Keywords

E-Banking, Online Banking Fraud, Cryptography, Steganography, Data Mining.

1. INTRODUCTION

The progress of using card as one of the main modes of payment in the recent times has led to sophistication of the online banking process specifically to provide a safe and secure transaction. These refinements in the banking process have however had no impact on the skyrocketing frauds related to it. In this situation of advanced online fraud there is very restricted information available to differentiate sincere customer actions from fraud [1]. Thus, in such an exceptionally sparse and imbalanced data environment, making prompt and effective detection has become extremely necessary and perplexing [1].Hackers are becoming increasingly proficient and carrying out major security attacks like Spoofing, Phishing, Pharming and Keystroke Capturing. The current online E-Banking system aims at providing a highly secure system by encryption of data during transactions; however with the advancement of technology the means to crack these security measures has also intensified. The suggested system thus, strives for providing an extremely safe online banking experience by using both cryptography and steganography for fraud prevention and a data mining technique for fraud detection.

2. EXISTING SYSTEM

The existing system for online banking requires the user to enter his/her card details directly in the payment gateway of an online website. This information is encrypted using a high end key and these coded details are then forwarded to the bank server over the internet. However even though the way of encryption of the data and the algorithms used promise high level of security they are yet hacked by professional hackers. This is primarily because the data is just encrypted using a key and hacking this key is not a difficult task for professional hackers. Apart from encrypting the user details using a key there is no further mechanism to hide such significant data from the hackers. To add an additional feature of security a One Time Password is sent to the registered phone number associated with the card. This is to ensure that person using the card is a genuine customer and not a fake user. However, the generation of OTP is not done on specific international sites and due to network issues in some cases. In such situations, the user may then have to use his master key to complete the transaction. The major drawback of using the master key is that then there is no OTP generation for that particular transaction. So, if the master key is hacked the card can be used for multiple fraudulent transactions.

Once the control has been transferred to the server side user specific inspection is done to check for any discrepancies in the usual transaction pattern. In case there is a change in the sequence of usage like a sudden variation in the transaction amount or location of the user then the existing system suspects it to be a fraudulent transaction and immediately notifies the user with a call. In case it is not a con the execution of transaction is continued normally else the transaction is blocked instantaneously in order to avoid the improper usage of a user’s card.

However, the main drawback of the existing system is that it fails to prevent the hacking of the user card details in the very first place. The newly planned system thus overcomes this drawback by not only encrypting the user details but also storing these details in an image by using steganography. Steganography has a very significant plus over cryptography which is that the intended secret message to be transmitted over a network does not garner any attention to itself as an item of examination [2].

Thus the system carries out the transaction using this image making hacking of details much more difficult thereby adding an additional level of security as compared to the existing system. Along with fraud prevention the system also focuses on fraud detection by carrying out data mining on the server side in order to determine any kind of change in user spending pattern and transaction location further safe guarding the online banking procedure.

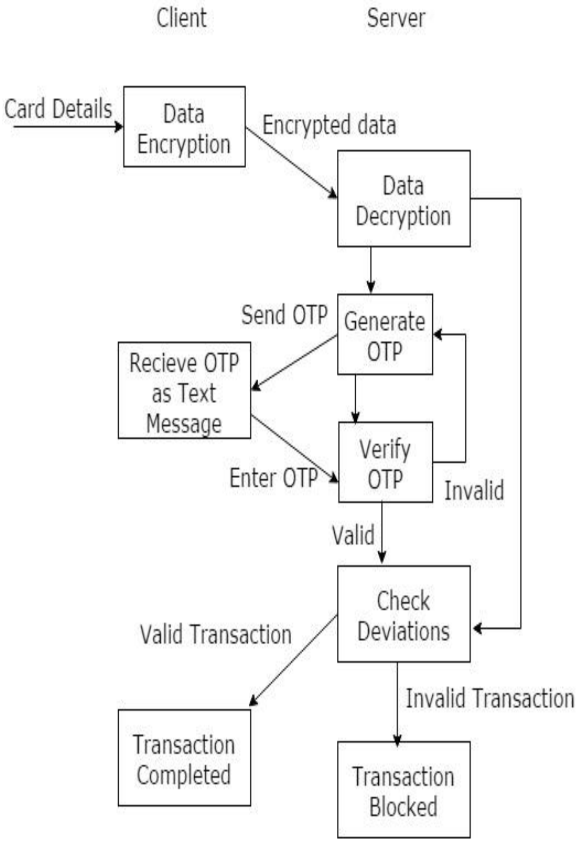


Fig. 1 Existing System

3. PROPOSED SYSTEM

The proposed system deals with fraud prevention and detection by using cryptography for encrypting user card details, steganography for storing these encrypted details in an image which is mainly used for carrying out the transaction and finally data mining for detecting major deviations in the user's transaction pattern and accordingly blocking or completing the transaction. The three main modules of the proposed system are thus, data encryption, image steganography and data mining.

3.1 Data Encryption

This module of the system deals with fraud prevention. The user enters his card details in an android application of the system. Along with these card details the location of the user device as well as the current date and time is extracted.

The card details, user location in terms of latitude and longitude and the current date and time are then encrypted using the AES encryption algorithm [8]. The key used for encryption in the AES algorithm used above is further encrypted using the RSA algorithm [9]. This provides two layers of security by using cryptography itself and thus makes the online transaction process more guarded. (Refer Fig. 2)

3.2 Image Steganography

This encrypted data from the previous module is now embedded in a carrier image selected by the user by applying the F5 algorithm [10]. The use of steganography here mainly ensures that user details are not only transferred over a network securely but also protected from unwanted attention from the hackers. Steganography technique embeds data in an image in such a way that no difference can be seen between the actual image and an image which contains data [3]. This feature is very useful when an image in being transferred over the internet as the hackers will have no idea that the image contains confidential data and even if they do get to know extracting the data from this image will be a task much tougher than breaking the key of an encrypted code (Refer figure 2).

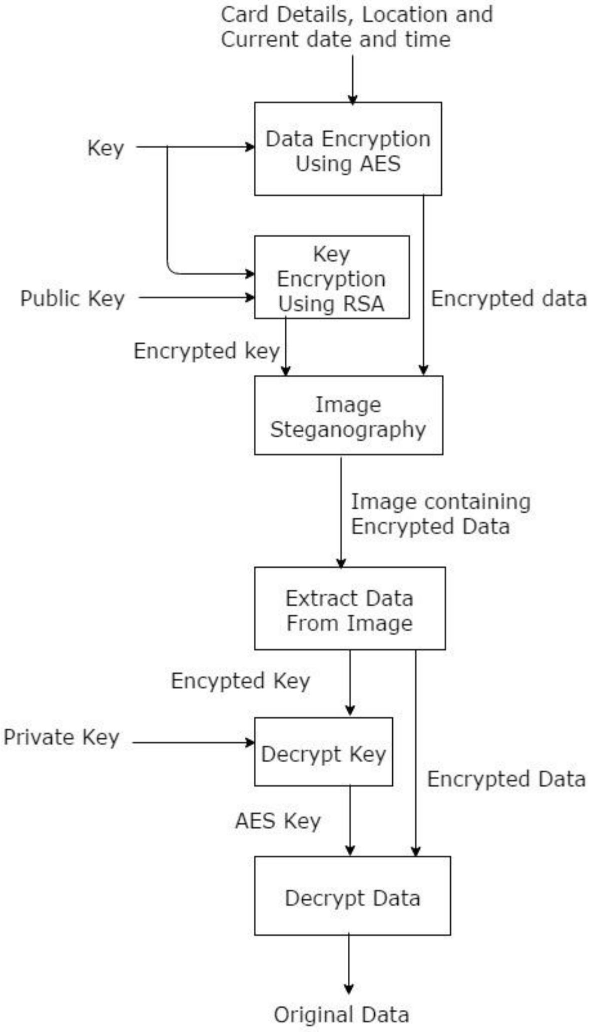


Fig. 2 Encryption and Steganography

3.3 Validation and Data Mining

This module of the suggested system deals with data mining of user's previous transactions in order to detect frauds. This is implemented using DBSCAN Clustering algorithm [7]. As soon as a transaction takes place first the image age is checked. This is done by checking the time and date details which is a part of the encrypted data sent in the image. If the image is older than five minutes then the user is notified to create a new image for carrying out the transaction. Then the user's card details are validated. Once this is done the transaction amount is checked and compared to previous transaction amounts in order to ensure no fraudulent behavior.

Lastly data mining is performed on the user data based on the user location. Using the latitude and longitude of user location clusters are formed of all previous locations. If user transaction has taken place in a location which falls within a cluster then the transaction is considered to be legitimate. However, if the location varies majorly then the transaction is considered to be fraudulent and necessary action is taken to block the transaction. (Refer Fig. 3)

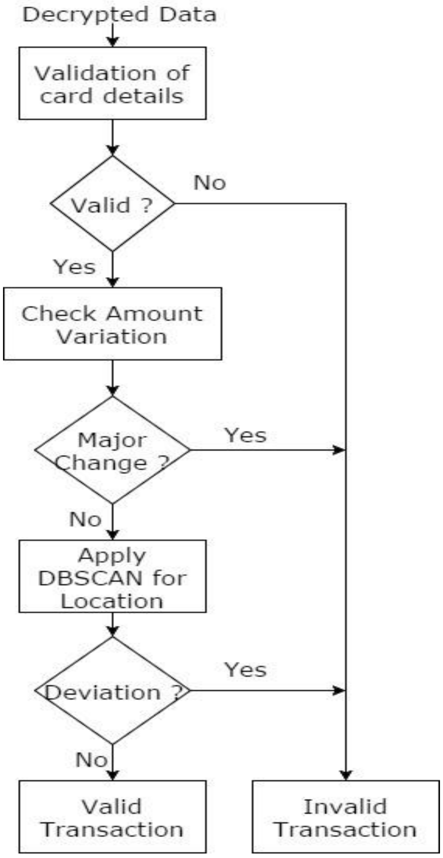


Fig. 3 Validation and Data Mining

4. WORKING OF PROPOSED SYSTEM

E-Banking Security is a project that aims at providing a secure e-banking system to all end users. The user enters his/her card details in the android application of our system before carrying out any transaction. Along with the card details the user location is also detected in terms of latitude and longitude along with current date and time. All this data is then encrypted using AES algorithm [8] and this encrypted data is then embedded in an image using F5 steganography algorithm [10]. This image is used by the user for carrying out the respective transaction thus, ensuring that user details are securely transmitted over a network.

At the server end once the image is received firstly the time of image creation is checked. In case the difference between the time of creation of image and the time of transaction exceeds a period of 5 minutes the user is immediately notified that particular image cannot be used for transaction and the user has to create another image to continue with the payment.

After this first step the encrypted user details then extracted from the given image. This data is decrypted using the AES decryption algorithm [8]. After decryption of data the first task done is validation of user card details wherein the card number, cvv, expiry date and name is verified.

After validation the amount of the user transaction is then compared to the amount of all previous transactions carried out by the user. This is done by finding an average spending amount for a particular user (Refer Fig. 4). In case the amount being spent in the current transaction varies majorly from the average amount spent then the transaction is considered to be a fraudulent one.

Lastly the location of the user is checked for any variation. The latitude and longitude of the current transaction and of all the previous transactions are clustered using data mining algorithm DBSCAN [7]. This data mining technique ensures that if any transaction location differs on a large scale from the usual locations then that transaction is considered to be an illicit one and marked as a noise point.

In case a transaction is found to be a fraudulent transaction then necessary action is taken to prevent the completion of the same. Either the user is called by the bank executive to confirm whether the transaction is a legitimate transaction or a One Time Password may also be generated to confirm the identity of the user carrying out the payment.

Thus, the suggested system ensures that both fraud prevention and fraud detection is done effectively. Securing the E-Banking process has been the main motivation of our system. With the exponential increase in hacking and various other unlawful activities every additional level of security is a boon for the E-Banking system and the users.

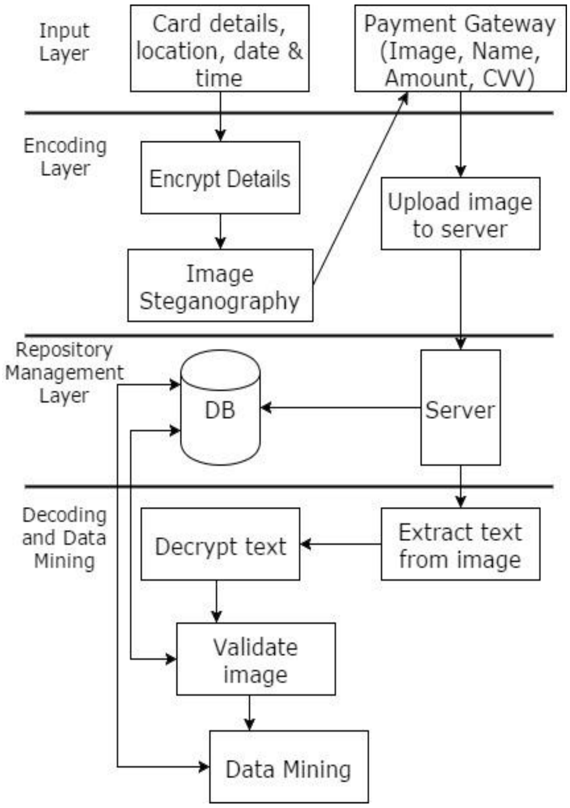


Fig. 4 System Architecture

5. RESULTS

The time taken by F5 algorithm [10] to embed data in an image varies with the resolution of the carrier image (Refer Table I). The table contains outputs of the tests we have conducted by embedding a block of data into images having different resolutions. The minimum time observed was of 2 seconds when an image of resolution 80x80 pixels was used and maximum observed time taken by the algorithm was 2 minutes and 27seconds for an image of resolution 4608x2592 pixels. As seen below as the resolution of an image increases the time for embedding the data in the image also increases. Thus efficiency of the system is highest when the image has smaller resolution and this efficiency decreases as resolution increases.

Table 1. Time taken for steganography of image for particular resolution

Resolution (pixels)	Time (Minutes:Seconds)
80x80	00:02
275x183	00:07
461x551	00:30
1280x1280	00:38
2576x1932	01:54
4608x2592	02:27

In order to test the image generated by the F5 algorithm a standard measuring technique called PSNR (Peak signal to noise ratio) has been used [5]. The following formula has been used for calculating PSNR value of the image (Refer Equation 1).

$$\text{PSNR} = 10.\log10\left(\frac{MAX^{\,2}}{MSE}\right) \quad - (1)$$

Where

$$\text{MSE} = \frac{1}{MN}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}(C(x,y) - S(x,y))^2 \quad - (2)$$

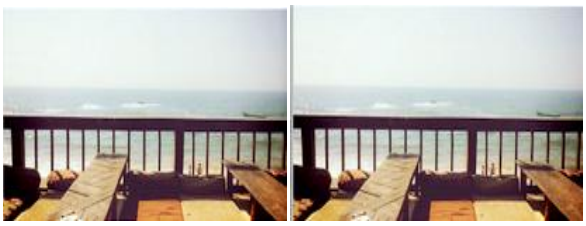
and MAX is the maximum possible pixel value for the images [6].

The original image C has a size of M x M and the image generated by steganography S has a size of N x N. Both the images have pixel values (x,y) from 0 to M-1 and 0 to N-1 respectively (Refer Equation 2) .

Table 2 demonstrates the PSNR values obtained after testing images with different resolutions. It is known that higher the PSNR value higher is the quality of an image [6]. The PSNR values of images generated by F5 algorithm usually ranges between 42 and 47 [11]. On testing the various images generated by the system using the PSNR formula (Refer Equation 1) one can came to the conclusion that the system has succeeded in providing satisfactory image quality after steganography.

Table 2. PSNR and MSE values for different images

Image Resolution	MSE	PSNR
634x470	3.9321	42.2186
720x1080	1.5026	46.3963
864x864	2.5936	44.0258
1080x1848	1.3601	46.8290
1080x1920	3.1690	43.1555



(a) **(b)**

Fig. 5 (a) Original Image (b) Image after steganograph

Based on the images above (Refer Fig. 5) one can settle that both the original image and the image created after steganography look alike. This means that there is little but no distortion i.e. distortion which is not visible to the naked human eye in the image created by our system. Thus the system succeeds in creating an object which is safe from being doubted for containing crucial data by any potential hacker [6].

In order to determine the efficiency and accuracy of the data mining module of the system tests were conducted using 2 datasets [4]. The first data set consists of randomly generated data points using random function of mathematics. The second dataset is the actual dataset used in the project which includes data points whose latitude and longitude matches various locations in India.

The clusters formed in dataset containing the randomly generated points always managed to identify the noise points correctly (Refer Fig. 6). For every case that the algorithm was run for this randomly generated dataset the results were always fitting. The above test is done on a dataset of size 93 randomly generated points.

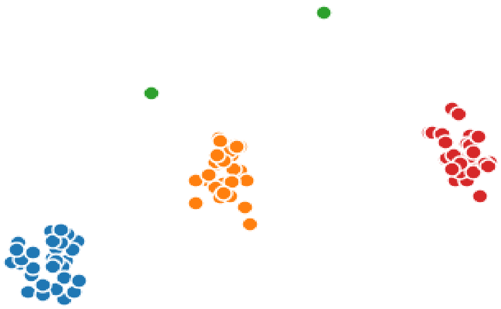


Fig. 6 Test on random generated data

Now on testing the algorithm on the actual dataset of 500 points (Refer Fig. 7) it is seen that not only are the required noise points identified correctly but also the new cluster formation takes place once the noise points in a specific area crosses the required minimum. On testing the algorithm for all borderline cases such as expired image, wrong card details, variation in amount of transaction and major deviation in location it has been found that the system works perfectly for all cases.

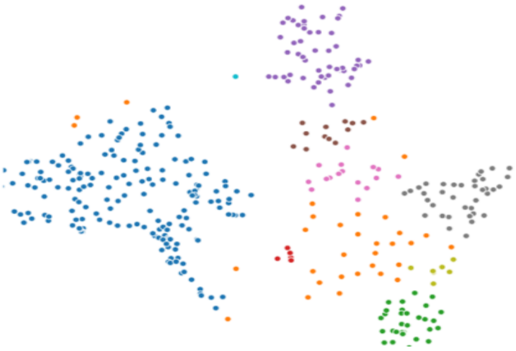


Fig. 7 Test on actual dataset

6. CONCLUSION

Based on the analysis done one can come to a conclusion that the system has been successfully implemented and provides a secure E-Banking experience for every user. The system provides a strong mechanism to prevent online frauds by using cryptography and steganography on the client side. On the server side of the system Data mining ensures fraud detection. Based on all the tests conducted on the image generated by steganography one can deduce that the image satisfies all the necessary criteria in terms of quality and efficiency. The testing done on the data mining module with two different datasets ensures that all the normal and extreme cases are satisfactorily handled by the algorithm. The main aim of the system was to deliver a safe and protected online banking experience and on the basis of the analysis and testing conducted one can reckon that it has been efficaciously achieved.

7. REFERENCES

[1] Wei Wei, Jinjiu Li, Longbing, Cao, YumingOu, Jiahang Chen, “Effective detection of sophisticated online banking fraud on extremely imbalanced data”, World Wide Web, July 2013, Vol. 16, Issue 4, pp 449–475.

[2] S. Srilakshmi, “Dual Stegnography Scheme For Secure Data Communication Using Finite State Machine”, International Journal of Advanced Research in Computer Science, Vol. 5, No. 4, April 2014.

[3] Arshia Azam, Rumana Firdous, F. Asma Begum, “High Security Image Steganography Using RSA Algorithm”, Journal of Innovation in Electronics and Communication, Vol 4, July-Dec ’14.

[4] Shimei Wang, Yun Liu, Bo Shen, “MDBSCAN: Multi-level Density Based Spatial Clustering of Applications with Noise”, KMO '16, July 25-28, 2016 ACM, Hagen, Germany.

[5] Naitik P Kamdar, Dipesh G. Kamdar, Dharmesh N. khandhar, “Performance Evaluation of LSB based Steganography for optimization of PSNR and MSE”, Journal of Information, Knowledge and Research in Electronics and Communication Engineering, Vol – 02, Issue – 02.

[6] Rosziati Ibrahim, Teoh Suk Kuan, “Steganography Algorithm to Hide Secret Message inside an Image”, Computer Technology and Application 2, pp.102-108, 2011.

[7] Iyer Aurobind Venkatkumar, Sanatkumar Jayantibhai Kondhol Shardaben, “Comparative study of Data Mining Clustering algorithms”, 2016 IEEE International Conference on Data Science and Engineering.

[8] Bawna Bhat, Abdul Wahid Ali, Apurva Gupta, “DES and AES Performance Evaluation”, International Conference on Computing, Communication and Automation.

[9] S. Anandakumar, “Image Cryptography Using RSA Algorithm in Network Security”, International Journal of Computer Science & Engineering Technology, Vol 5, Issue 9, September 2015.

[10] Andreas Westfeld, “F5—A Steganographic Algorithm High Capacity Despite Better Steganalysis”, I. S. Moskowitz (Ed.): IH 2001, LNCS 2137, pp. 289–302, 2001.

[11] Ali Akbar Hashemi, Navid Daryasafar, “Improving the F5 Steganography Method through Shrinkage Mapping”, International Journal of Scientific & Engineering Research Volume 3, Issue 6, June-2012.