Stepping Up Internet Banking Security Using Dynamic Pattern Based Image Steganography

P. Thiyagarajan, G. Aghila, and V. Prasanna Venkatesan

CDBR-SSE Lab Department of Computer Science,
Pondicherry University, Puducherry 605 014
thiyagu.phd@gmail.com, aghilaa@gmail.com,
prasanna_v@yahoo.com

Abstract. In the world of E-Commerce internet banking is one of the indispensable applications. Security issues are to be addressed critically in internet banking applications and it directly influences the comfort. Even though the existing mechanisms ensure security the hackers succeed in breaking these mechanisms. In this regard to step up the internet banking security a new layer called 'Stego Layer' is introduced which in turn uses Dynamic Pattern Based Image Steganography (DPIS) algorithm. Stego-layer will be present in both client and server for embedding and extracting the message. The proposed method is compared with other popular encryption algorithms in practice.

Keywords: Image Steganography, Session Hijacking, AES, Internet Banking Security, Dynamic Key Management, Pixel Intensity.

1 Introduction

Information is Wealth, is a profoundly known statement. This goes inherent in all the aspects of business. With information serving a critical role in an organisation, preserving it becomes the most challenging activity. This paper presents a method to enhance the security of data which is transmitted between client and server. This deals with the step-wise transition of data and suggests a mechanism to cover the information from the intruders. The security is guaranteed by the inclusion of a stego layer in the client and server side. The functionality of the layer is that the information to be exchanged between the banking parties is hidden in an image before being transmitted.

2 Internet Banking

Internet banking, otherwise called anywhere anytime banking, has become an indispensable tool in the modern banking arena. With the help of internet banking, one can access any information regarding their account and transactions, any time of the day. One can regularly monitor the account as well as keep track of financial transactions, which can be of immense help in detecting any fraudulent transaction. In the world of internet money transaction between accounts take place in fraction of seconds. The main issue of the internet banking analysed in the survey conducted by

A. Abraham et al. (Eds.): ACC 2011, Part IV, CCIS 193, pp. 98–112, 2011.

online banking association in the year 2002 [9] is security. Security is a crucial requirement of an E-Commerce system [6] due to the fact that the sensitive financial information that these systems transmit travel over un-trusted networks where it is essentially a fair game for anyone with local or even remote access to fetch the confidential data in any part of the path followed.

3 Threats in Internet Banking

Internet has become parts of life some way or the other without which individual can’t survive. With almost all processes automated, the processing time has become almost negligible which is directly proportional to the efficiency of the system as a whole. Christos K.Dimitriadis et.al [5] in analysing the security of internet banking classified the attacks broadly in to four categories. They are

- Phishing
- Injection of commands
- User credentials guessing
- Use of known authenticated session by attacker.

The following section explains the sample attacks which are relevant to our work and falls in above categories.

A. Man in the middle attack

Man in the middle attack falls under the Injection of commands category [5]. In this attack, attackers intrude into an existing connection to interrupt the exchanged data and inject false information. It involves eavesdropping on a connection, intruding into a connection, intercepting messages, and selectively modifying data. Such attacks are usually selected by hackers against public-key cryptosystems. Quite often in such cases, the victim parties are made to believe that they remain safe in communicating with each other.

B. Session hijacking

Session hijacking falls under the use of known authenticated session by attacker category [5]. Session hijacking is the act of taking control of a user session after successfully obtaining or generating an authentication session ID. In Session hijacking attacker seizes the control of a legitimate user's Web application session using brute forced or reverse-engineered session IDs while that session is in progress.

C. Man in the browser attack

Man in the browser attack falls under the user credentials compromise category [5]. This “Man in the browser attack” takes place only in computer memory. It takes place before Secure Socket Layer (SSL) encoding. When a user's PC is infected, the malicious code is triggered as the user visits an online bank website. This attack retrieves authentication information, such as logins and passwords, entered on a legitimate bank site. The retrieved personal data is sent directly to an FTP site where it is stored.

4 Existing Techniques for Handling Attacks in Internet

Financial institutions offering Internet-banking should have reliable and secure methods for transactions. In this section some of the security mechanisms from literature have been discussed.

Plossl et.al [10] addresses authentication and phishing issues by proposing a visual cryptography mechanism. According to their proposal the client is supplied with challenge-response list. When the client carries a transaction, he has to scan the list to find the response that corresponds to the challenge provided by the bank.

Hiltgen et.al [8] in his paper targets Man in the middle attack by Short-time password solutions based on a password generating hardware token which are available from various manufacturers such as RSA Security, Active Card or VeriSign. The RSA's SecureID solution is the most prominent example. It consists of a small device including a LCD display and one button the user can press to initiate the calculation of the next short-time password.

Geeta et.al [7] in her paper enhances the security level of Mobile banking using Steganography. In this method pixels are chosen according to the key generated and secret message bits are embedded at constant rate in the chosen pixel. This method does not ensure that significant color do not suffer from data embedding and bits are embedded sequentially in all selected pixels which may pave way for steganalyst to easily crack the method.

AES is the most commonly used encryption algorithm [11] for high end security applications. Recently it has been proven by cryptographers that the AES is breakable [1]. The survey clearly points out the need for a technique which ensures for secured transactions in internet banking. In this work the 'stego-layer' method has been evaluated and compared with Advanced Encryption Standard (AES) against important security parameters. The proposed method also provides solution for Man in the middle attack and Session hijacking.

5 Proposed Method Using Dynamic Pattern Image Steganography Algorithm

In proposed method a new layer called 'stego-layer' was introduced both in client and server side. Any critical data passing to and from the client and server will pass through the 'stego-layer'. The 'stego-layer' uses Dynamic Pattern based Image Steganography algorithm for embedding and extracting message which is explained in this section.

Steganography is the art of hiding secret information in media such as image, audio and video [4]. The purpose of steganography is to conceal the existence of the secret information in any given medium. It is known that Internet banking is based on Client-Server architecture. The proposed stego-layer was introduced in both client and server sides for embedding and extracting process. Figure 1 shows the architecture of the proposed stego-layer method.

In stego-layer embedding and extracting was done by the Dynamic Pattern Based Image Steganography (DPIS) algorithm. The idea behind DPIS technique is that significant color channels should not suffer from data embedding while the insignificant color channel can be used for data embedding. Figure 2 and Figure 3 depicts the embedding and extracting process of DPIS algorithm.

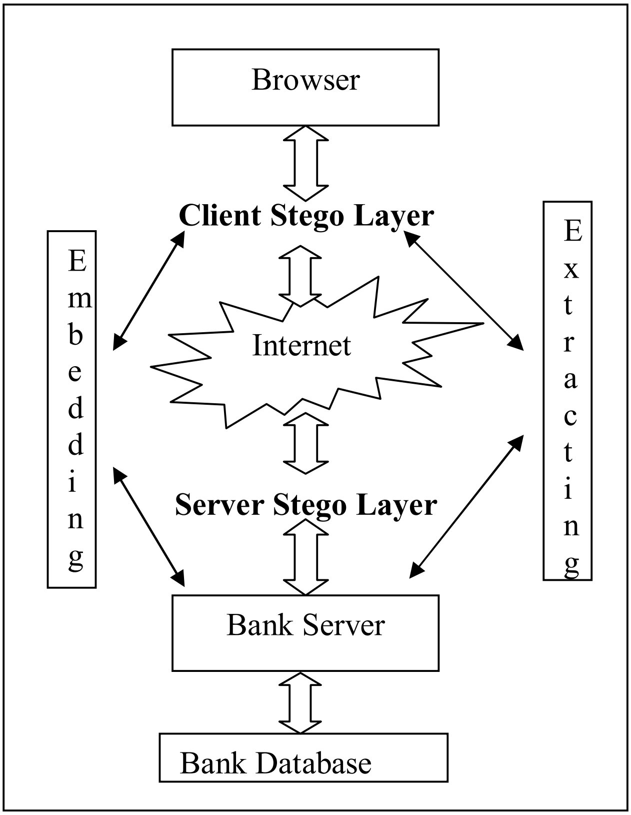


Fig. 1. Architecture of proposed Stego-layer Method

If the indicator chosen is lowest color channel then the pixel is exempted from data embedding else if the indicator chosen is not the lowest color channel then choose the lowest value channel apart from the indicator channel for data embedding.

Embedding Part

```
Generate Indicator Sequence of any length
Get the Cover image
Get the Secret message to be embedded
  For 1 to last _row
      For 1 to last_col
             Fix the Indicator Channel
             If (Indicator channel is lowest)
                    Skip
             Else
                 Find the lowest channel
               Embed the secret message
               bits
                 Mark the bits embedded in
               3rd channel
             End if
     End For
 End For
```

Extracting Part

```
Get the Indicator Sequence from embedding part
Get the Stego-Image
For 1 to last _row
  For 1 to last_col
       While (Entire bits not extracted = true)
             Find the Indicator channel
            If (Indicator channel is lowest)
                 Skip
               Else
                 Find the data channel
                 Extract the bits   embedded
             End if
       End While
   End For
 End For
```

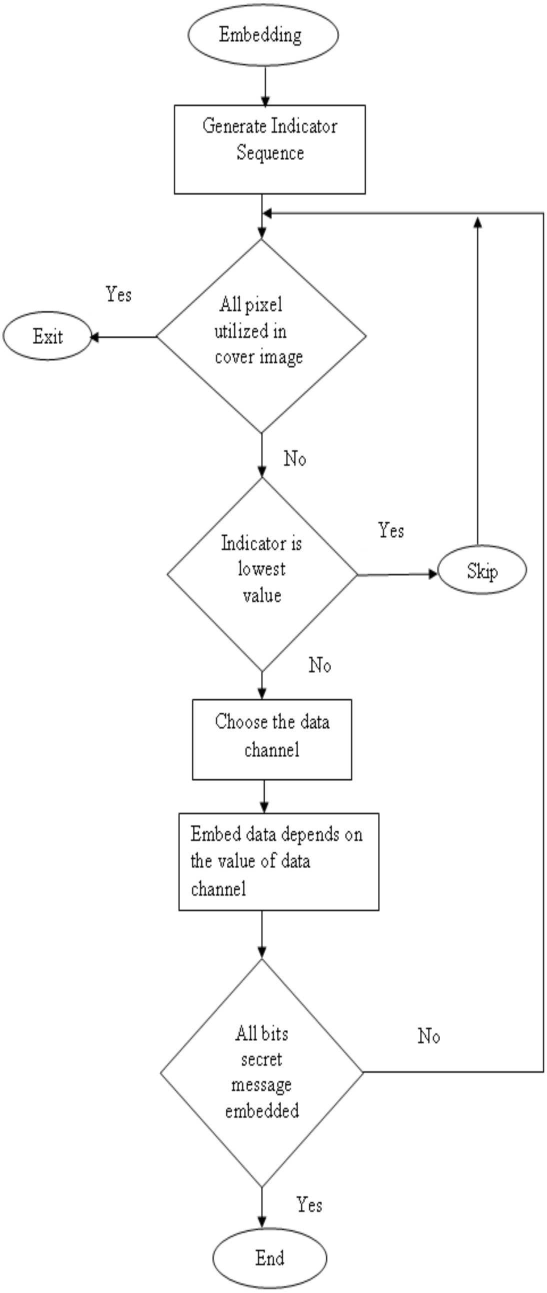

Embedding
Generate Indicator Sequence
All pixel utilized in cover image
Yes
Exit
No
Indicator is lowest value
Yes
Skip
No
Choose the data channel
Embed data depends on the value of data channel
All bits secret message embedded
No
Yes
End

Fig. 2. Flow chart for Steps followed in Client Stego Layer

The above steps completely describe the embedding and extracting process.

Criteria for choosing number of bits to be embedded in data channel

Experiments have been conducted to find almost how many least significant bits can be changed in pixel such that the color doesn't vary from the original color and the results have been used in DPIS technique. DPIS technique has been tested on different image category such as portrait, flower, nature, toys etc. Figure 4 and figure 5 shows the Cover and Stego images generated through DPIS technique.

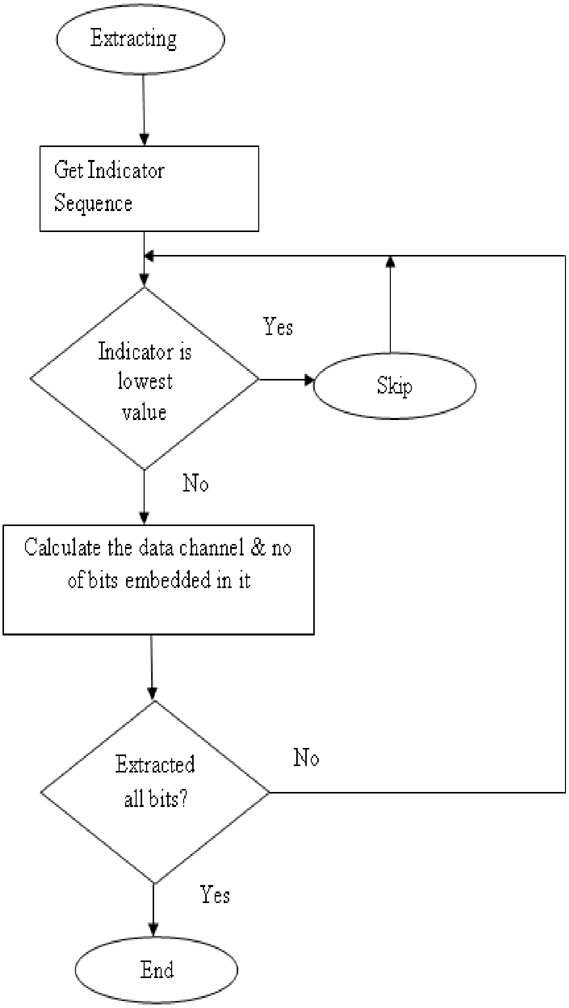

Extracting
Get Indicator Sequence
Indicator is lowest value
Yes
Skip
No
Calculate the data channel & no of bits embedded in it
Extracted all bits?
No
Yes
End

Fig. 3. Flow chart for Steps followed in Server Stego Layer

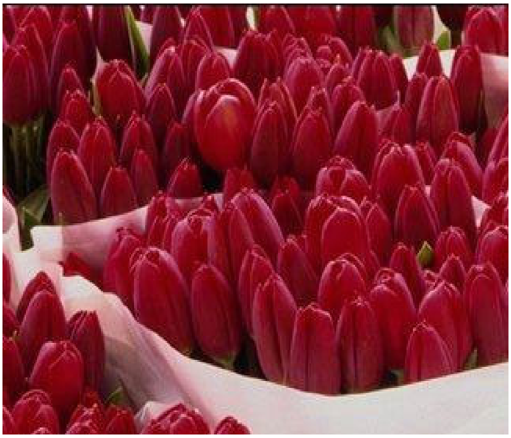
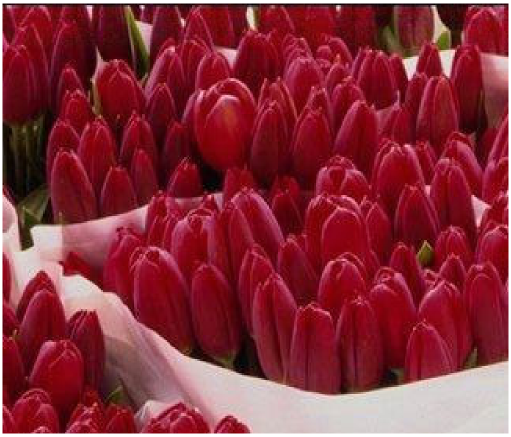


Image Size: 323 x 429, No of pixels: 138567

Fig. 4. Cover Image



Pixel used for embedding: 4714, Secret Message size: 2113

Fig. 5. Stego- Image

Proposed method is moulded so as to ensure the preservation of the data between destinations which comprises of a bank and a customer, or vice versa. This work deals with the step-wise transition of data from internet to bank server and suggests a mechanism to cover the information from the intruders. This superlative degree of security is guaranteed by the inclusion of a stego layer into the network. As the client visit the banking website he is made to enter his customer id. This customer-id is validated and key (Indicator Sequence) for the transaction is issued from the bank server to the client. Client will have to use this key for any further transaction to server. Key for the particular customer is changed by the bank server at regular intervals of time to enhance the system security. The functionality of the layer is to hide the information sent between the communicating parties in an image before being transferred.

The prototype implementation of proposed method is done in Visual Basic 6 (VB 6). DPIS algorithm was implemented in MATLAB and its executable is invoked in VB. The sample implementation screenshots are shown in figure 9, figure 10 and figure 11 which depict the internet banking login screen for embedding and extracting user credentials in to an image. Once the user submits his username and password, the data is passed to stego layer. In stego-layer, DPIS embedding algorithm is invoked and it embeds the user credentials using the key allocated for that particular user in to the image called stego-image. Thus each customer has dynamic key and the allocated key will be changed after certain period of time to strengthen the security.

The stego-image is passed to bank server through the internet. Once it reaches the server stego layer, the embedded message is decrypted using the symmetric key by DPIS algorithm. The decrypted user credentials are extracted to a file and it is validated in the bank server.

6 Behavior of Common Attacks in the Stego-Layer Method

There are many attacks in the literature survey for internet applications [5]. In this section the behaviour of common attacks in proposed ‘Stego-layer’ method has been analysed experimentally. The most common attacks are

- Brute force
- Extracting data from all pixels
- Extracting same number of bits from data channels

Brute force attack on Indicator sequence: Brute force attacks for Stego-layer method [3] [5] involves in trying all possible keys until valid key is found. In dynamic pattern based image steganography technique, indicator channel contains the information where the data are stored. Intruder may try the brute force attack on indicator sequence until meaningful message is traced. In all experiments length of indicator sequence is greater or equal to 20 so number of distinct patterns generated is very high. For example if the indicator length is 20 the number of distinct patterns generated is *7, 748, 40,978* and it is difficult to break by brute force attack.

Fig. 6. Stego-image generated by DPIS algorithm

The secret message shown in the Table 1 has been embedded in the cover medium by DPIS technique and the obtained stegoimage is shown Figure 6. Brute force attack has been applied on the indicator sequence for extracting message from the stego image.

Table 1. Embedded message and extracted message with wrong pixel indicator

Embedded Secret Message in cover medium	PondicherryUniversity Computer Science Dept
Secret message obtained by wrong indicator sequence	QibP(97u2q◀ ├ <↑ <]← 4]nD ǀ:8*│ ─ ~v&N-F┤ KKe┐ W;'

The above experiment depicts that even if one value in the indicator sequence is incorrect, embedded secret message cannot be extracted.

Extracting data from all the pixels sequentially: In Stego-layer method data are not embedded in all the pixels sequentially. Some pixels in the sequence are missed in order to strengthen the algorithm. The Table 2 shows the result of extracting data from all the pixels from stegoimage shown in Figure 7.

Fig. 7. Stego-image generated by DPIS algorithm

The embedded message in the image cannot be extracted without the key. Since the Key is known only by the communicating parties the Stego-layer method prevents Man in the middle attack and Session Hijacking.

Table 2. Embedded Message and Extracted Message from all the pixels in the Stego Image

Embedded Secret Message in cover medium	PondicherryUniversity Computer Science Dept
Secret message obtained by extracting bits from all pixels in stego image	T+*m*□-&#tKK`w0 -xy

Extracting same number of bits from all pixels: In the Stego-layer technique the number of bits embedded in each pixel varies and it is decided during the run time. Experiments were conducted for extracting same number of bits from all the pixels in the stegoimage generated by DPIS technique. The Table 3 shows the result of extracting same number of bits from all the pixels from stegoimage which is shown in Figure 8.

Fig. 8. Stego-image generated by DPIS algorithm

Table 3. Embedded message and message extracted with uniform number of bits from pixels in the stego image

<table>
<tr><td>Embedded Secret Message in cover medium</td><td>Pondicherry University Computer Science Dept</td></tr>
<tr><td>Secret message from stego image obtained by extracting 2 bits from all data channels</td><td>Sj Lc;G;? Cq chT =Y { w@SO` =o `4' h | *Hf#</td></tr>
</table>

6.1 Detection of Tampered Stego Images

In Stego-layer method, provision has been provided to check whether the stego image has been modified by any intruder [2] [5]. Before decrypting the embedded message the stegoimage is checked for any change done by intruder. If stegoimage is not tampered then the extraction part will be executed.

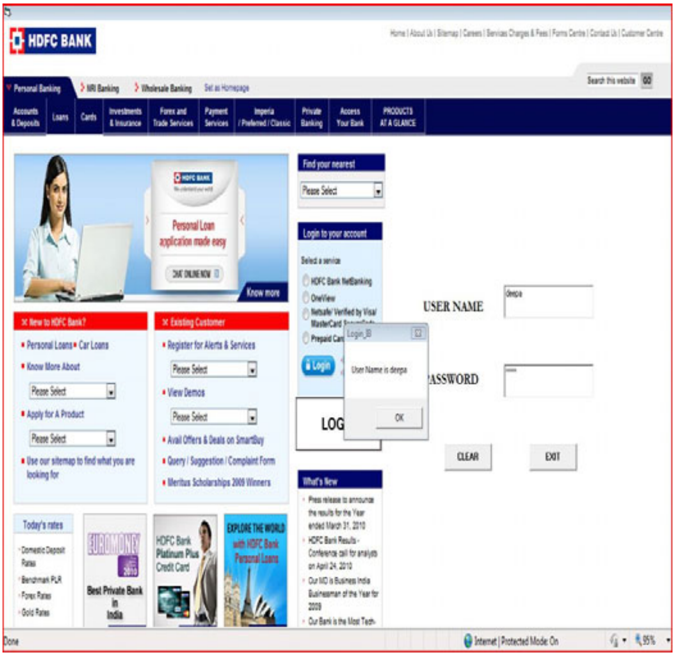
This has been achieved in the DPIS technique by user id. Since user id has been known by both client and server, hash value of user id is stored in predetermined pixel of the image. Before extracting, the particular pixel which contains the hash value of the user id will be checked in order to make sure that the image has not been modified by the intruder. Thus Man in the browser attack has been detected using Stego-layer method.

7 Comparison of Stego-Layer Method with Existing Standard Cryptographic Algorithm

There are numerous mechanisms reported for strengthening internet banking in the literature. For each efficient methods proposed for security an equal intelligent method for breaking the security has been developed by the hackers. In table 4 the proposed stego-layer method is compared with Advanced Encryption Standard (AES) algorithm against functional and non-functional parameters.

Table 4: Comparison of Stego-Layer method with Advanced Encryption Standard algorithm (+++ - Good ++++ - Very Good)

Type	Parameters	AES Algorithm	Stego-layer method
Non functional parameters	Performance	+++	++++
	Efficiency	+++	+++
	Time need to decipher a message	+++	++++
Functional Parameters	Key length	Static and vary with 3 different key length	Dynamic
	Identification of tampered message at receiver's side	No	Yes
	Covertness in message transmission	No	Yes

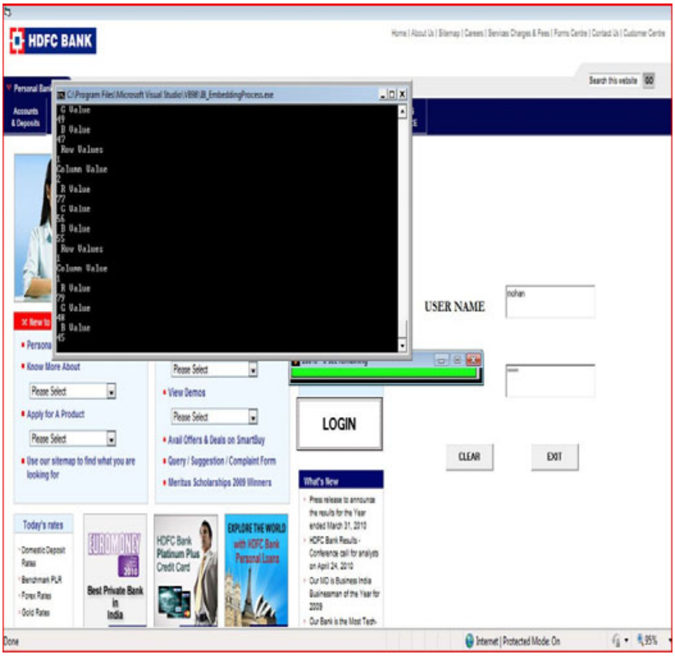


Login_B

User Name is deepa

USER NAME deepa

Fig. 9. Bank login Screen

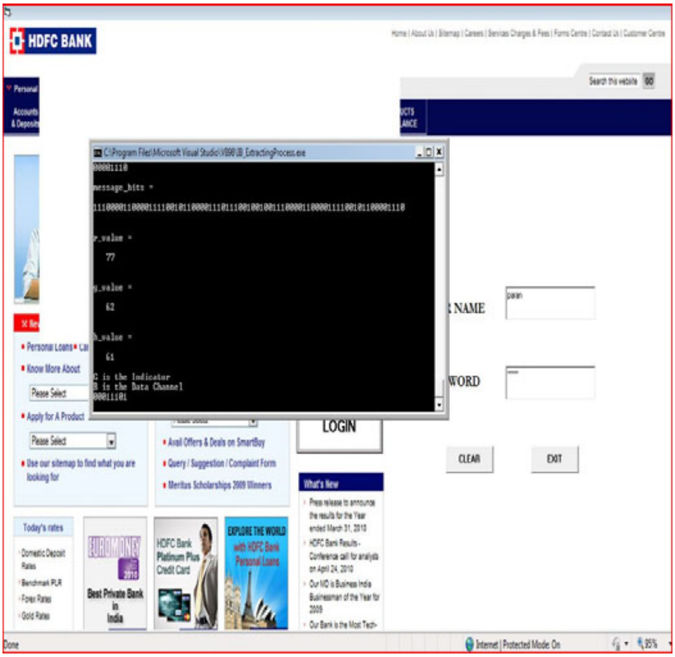

HDFC BANK
Home | About Us | Sitemap | Careers | Services Charges & Fees | Forms Centre | Contact Us | Customer Centre
Know More About
Apply for A Product
View Demos
Today's rates
What's New
USER NAME
LOGIN
CLEAR
EXIT
Done
Internet | Protected Mode: On

C:\Program Files\Microsoft Visual Studio\VB98\IB_EmbeddingProcess.exe

```
 G Value
49
 B Value
47
 Row Values
1
Column Value
2
 R Value
77
 G Value
56
 B Value
55
 Row Values
1
Column Value
1
 R Value
79
 G Value
48
 B Value
45
```

USER NAME mohan

Fig. 10. Embedding user credentials in to an image at client side



HDFC BANK
Personal
Accounts & Deposits
C:\Program Files\Microsoft Visual Studio\VB98\B_ExtractingProcess.exe
NAME
WORD
LOGIN
CLEAR
EXIT
Personal Loans
Know More About
Please Select
Apply for A Product
Use our sitemap to find what you are looking for
Avail Offers & Deals on SmartBuy
Query / Suggestion / Complaint Form
Meritus Scholarships 2009 Winners
What's New
Today's rates
EUROMONEY
Best Private Bank in India
HDFC Bank Platinum Plus Credit Card
EXPLORE THE WORLD with HDFC Bank Personal Loans
Done
Internet | Protected Mode: On

```
00001110

message_bits =

1110000110000111100101100001110111001001001110000110000111100101100001110


r_value =

   77


g_value =

   62


b_value =

   61

G is the Indicator
B is the Data Channel
00011101
```

Fig. 11. Extracting user credentials from stego-image at server side

8 Conclusion

In this ‘stego-layer’ method a new security mechanism was introduced for internet banking using Dynamic Pattern Image Steganography algorithm. The proposed method has been compared with existing algorithm against functional and non-functional parameters. Regular attacks were experimented on the proposed method and from the results it is obvious that attack results in vain. Further work will focus on choosing appropriate image size so as to ensure it will not be an overload in the network and to compare the proposed method with other different algorithms for efficiency.

Acknowledgement

This research, CDBR Smart and Secure Environment, was sponsored by National Technical Research Organisation (NTRO) and their support is greatly acknowledged. I would also like to thank Mr.M.R.Parandama and Ms.S.Deepa for their support in implementation.

References

[1] Biryukov, A., Dunkelman, O., Keller, N., Khovratovich, D., Shamir, A.: Key Recovery Attacks of Practical Complexity on AES Variants With Up To 10 Rounds (2009)

[2] Anderson, R.J., Petitcolas, F.A.P.: On limits of steganography. IEEE Journals of Selected Areas in Communications (May 1998)

[3] Westfeld, A., Pfitzmann, A.: Attacks on Steganographic Systems. In: Proceedings of the Third International Workshop on Information Hiding, September 29-October 01, pp. 61–76 (1999)

[4] Bailey, K., Curran, K.: An Evaluation of Image Based Steganography Methods. Multimedia Tools & Applications 30(1), 55–88 (2006)

[5] Dimitriadis, C.K.: Analyzing the Security of Internet Banking Authentication Mechanisms. Information Systems Control Journal 3 (2007)

[6] Oghenerukeyb, E.A., et al.: Customers Perception of Security Indicators in Online Banking Sites in Nigeria. Journal of Internet Banking and Commerce (April 2009)

[7] Navale, G.S., Joshi, S.S., Deshmukh, A.A.: M-banking Security a futuristic improved Security approach. International Journal of Computer Science Issues 7(1,2) (January 2010)

[8] Hiltgen, A., Kramp, T., Weigold, T.: Secure Internet Banking Authentication. IEEE Security and Privacy 4(2) (2006)

[9] Mishra, A. K.: Internet Banking in India-Part I, `http://www.banknetindia.com/banking/ibkg.htm`

[10] Plössl, K., Federrath, H., Nowey, T.: Protection Mechanisms Against Phishing Attacks. In: Katsikas, S.K., López, J., Pernul, G. (eds.) TrustBus 2005. LNCS, vol. 3592, pp. 20–29. Springer, Heidelberg (2005)

[11] Seleborg, S.: About AES – Advanced Encryption Standard (2007), `http://www.axantum.com/axcrypt/etc/About-AES.pdf`