DATABASE SECURITY USING CYBER SECURITY

Aashita Chhabra
Assistant Professor
DSPSR, Rohini
New Delhi, India

Abstract

A new approach has been shown, implemented for providing security in an organization for the long term goal. Primarily steganography techniques have been used (including email authentication) to enhance the security of data in one organization. Suppose we want to send the message "Please withdraw 5$ from my account" which we want to keep confidential. So for that firstly we apply encryption technique then we apply Steganography using LSB substitution method. Now that file is to be sent through an e-mail to other person in an organization. In order to receive that file receiver must be aware of the password security which is already applied by the sender.It has been done to provide more authentication to the data. Further if some data is at someone else inbox and being an admin, we want to retrieve that data, it can be done by using this technique.

Keywords: Steganography, Least Significant Bit, Cryptography, IMAP, SMTP

Introduction

This module generates the user interface through which a user browses the image file and can play and stops the image file. This GUI contains different fields such as text area for entering message and buttons for encryption and decryption. During encryption, image file will be created and in this image file. LSB of the each byte will be replaced by the encrypted data which is generated by the combination of the encryption key and the plain text i.e., the original message. Then this image file will be sent to the recipient. At recipient side this encrypted data will be extracted from each LSB and performs decryption operation on it and gives original information. During encryption, image file will be created and in this image file. LSB of the each byte will be replaced by the encrypted data which is generated by the combination of the encryption key (Password) and the plain text i.e., the original message. Then this image file will be sent to the recipient. At recipient side this encrypted data will be extracted from each LSB and performs decryption operation on it and gives original information. Using IMAP, we'll try to retrieve emails containing stegano images as attachments from Gmail server. Using SMTP, we'll send stegano images to recipients.

Problem Literature

If a person sends sensitive information over the insecure channels of the system then there may be a chance of hacking it, they can alter the information and sends it over the net. (Example: Military persons sending sensitive information over the net. This problem has been solved by the proposed system. In the proposed system the above problem has been solved by embedding the

data into the image file. Then this image file will be passed over the net, even if hacker hacks it, can be able to see only an image file. At the destination side this data will be encrypted from image file and performs decryption to get original message.
It is desktop application so only one user can use it that who has the computer. User has to browse the image file using the GUI which is provided by this application. User enters the data in the data into text box and gives encryption key to encrypt the data. During decryption time again user has to give the decrypted key to get the plain text.

The Proposed Method

The technique of providing security to data has been given using some USE –CASE diagram to get the idea about our implementation. We have Visual C# .NET builds on a strong C++ heritage. Immediately familiar to C++ and Java developers, C# is a modern and intuitive object-oriented programming language that offers significant improvements, including a unified type system, "unsafe" code for maximum developer control, and powerful new language constructs easily understood by most developers. Developers can take advantage of an innovative component-oriented language with inherent support for properties, indexers, delegates, versioning, operator overloading, and custom attributes. With XML comments, C# developers can produce useful source code documentation. An advanced inheritance model enables developers to reuse their code from within any programming language that supports .NET
We have used LSB hiding technique hide the secret message directly in the least two significant bits in the image pixels, hence that affect the image resolution, which reduces the image quality and make the image easy to attack. As well as this method is already has been attacked and broken. Therefore a new technique that able to make the secret message more secure and enhance the quality of the image is proposed. The proposed method hides the secret message based on searching about the identical values between the secret messages and image pixels

The Proposed Hiding Algorithm.
Inputs: RGB image, secret message and the password.
Output: Stego image.
Begin

scan the image row by row and encode it in binary. encode the
secret message in binary.
check the size of the image and the size of the secret message. start sub-
iteration 1:

choose one pixel of the image randomly
divide the image into three parts (Red, Green and Blue parts)
hide two by two bits of the secret message in each part of the pixel by searching about the identical.

if the identical is satisfied then set the image with the new values. otherwise
hide in the two least significant bits and set the
image with the new values
save the location of the hiding bits in binary table. end sub-
iteration 1.
set the image with the new values and save it.
End

Some of the methods have been shown below

1. Encryption

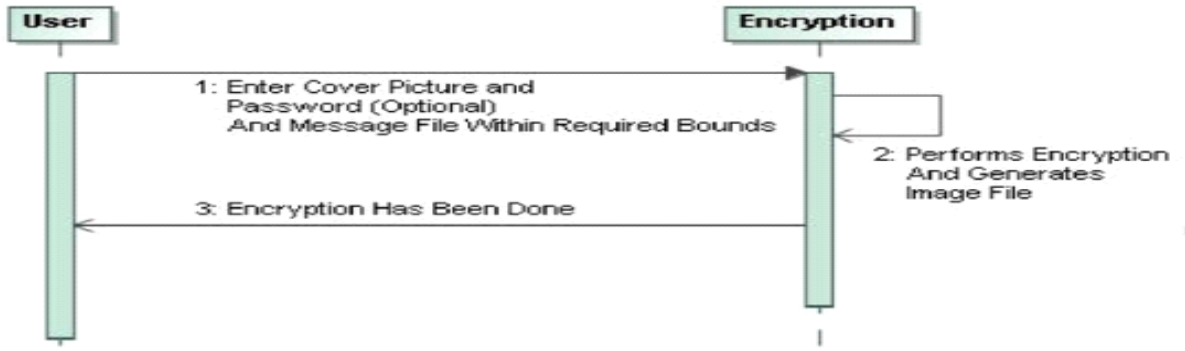

Figure – 1

2. Decryption

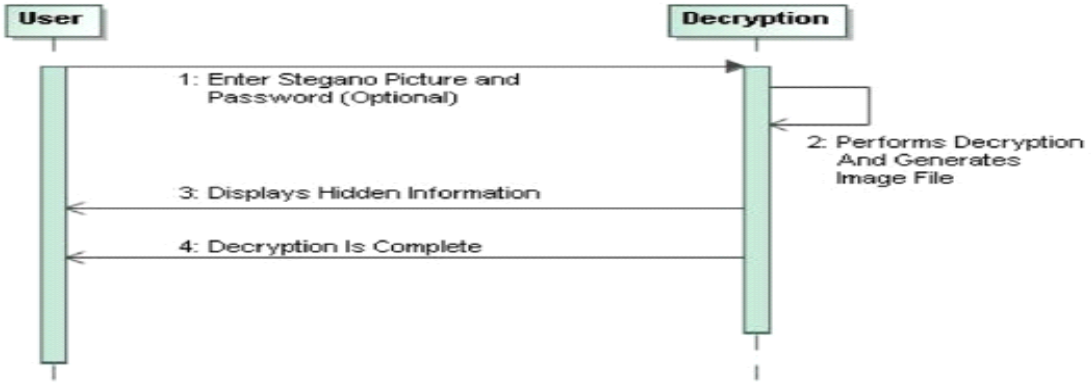

Figure – 2

3. Email Application (IMAP)

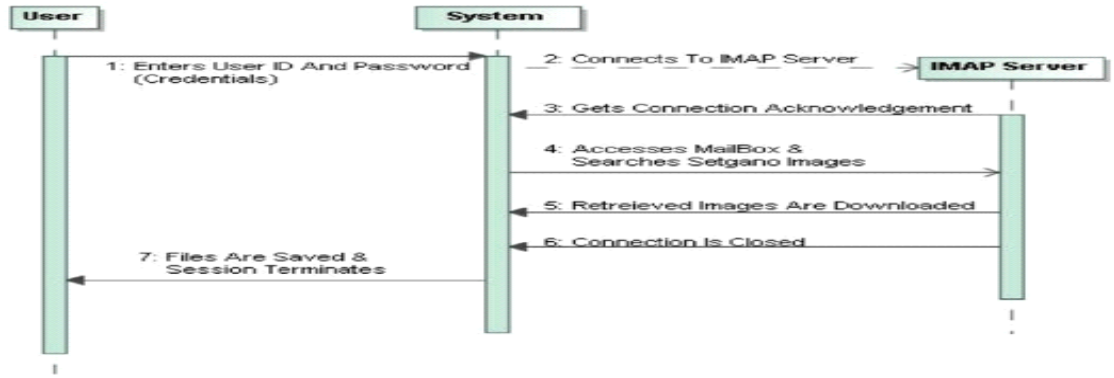

Figure - 3

4. Email Application (SMTP)

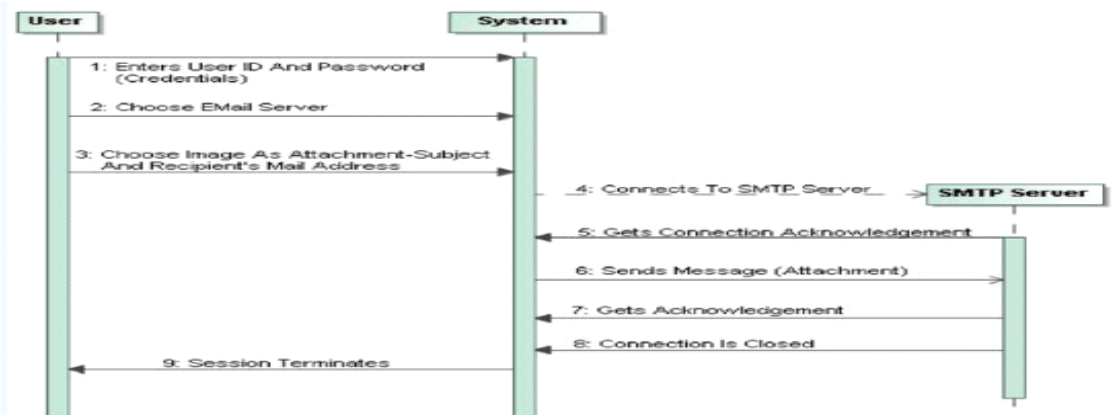

Figure - 4

Conclusion

Here are some of the results which will take place during implementation of this technique .User can select “Encrypt File” and “Decrypt File” from the given option to perform operation. When user selects larger files then an error will be shown “File Size Is Too Large”. So the user is expected to select files within the limits as given in the window. Entering Message to be encoded with the help of password-Once user has added message to be hidden behind the image file he would have to select image by going in the “File-Open Image” option. Decoding image by entering password to fetch original hidden message-To decode message from image file user has to enter password after selecting image in which message was hidden. User would have to click on “Decode” button to fetch the message. Message retrieved after inserting password-User would be able to retrieve message after providing required image file and password. Displays When User Sends Images-User has the option to send mail from Gmail, yahoo or Hotmail and then provide credentials. After that user can add attachment or file which they want to send and

add message to the same. Confirmation message while email is being sent-Once the email has been sent, user will get a confirmation message. Downloading encrypted message from mail-User can download images which have already been sent by again logging with the same email id as used earlier and click on "Download Stegan Images" option. Images would be downloaded and details would be visible at bottom of the image as shown. User would get message once the files are downloaded. User can click on "Help" menu to get any type of information regarding steganography Hence this method will allow you to provide high core security be applying many techniques in a single interface .

References

- B. Dunbar. A detailed look at Steganographic Techniques and their use in an Open-Systems Environment, Sans Institute, 1(2002).
- C. Christian. An Information-Theoretic Model for Steganography, Proceedings of 2nd Workshop on Information Hiding, MIT Laboratory for Computer Science. 1998.
- H. Wu, H. Wang, C. Tsai and C. Wang, Reversible image steganographic scheme via predictive coding. 1 (2010), ISSN: 01419382, 35-43.
- J, Corporation, Steganography. http://www.webopedia.com/ TERM/S/steganography.html. 2005.
- M. D. Swanson, B. Zhu and A. H. Tewfik, Robust Data Hiding for Images, IEEE Digital Signal Processing Workshop, University of Minnesota, September 1996 (37-40).
- N Ghoshal, J K Mandal .A steganographic scheme for colour image authentication (SSCIA), Recent Trends in Information Technology ICRTIT 2011 International Conference on (2011), 826-831.
- N. Johnson, Survey of Steganography Software, Technical Report, January 2002.
- N. Johnson, Digital Watermarking and Steganography: Fundamentals and Techniques , The Computer Journal. (2009)
- P. Fabien, J. Ross. Anderson, and Markus G. Kuhn. "Information Hiding – A Survey." Proceedings of the IEEE, 87:7. 1062-1078. 1999.
- Spam Mimic." http://www.spammimic.com.
- W, Peter. Disappearing Cryptography: Information Hiding: Steganography & Watermarking (second edition). San Francisco: Morgan Kaufmann. 3(1992) 192-213.