Security Enhancement using Data Hiding in Images (E-Banking)

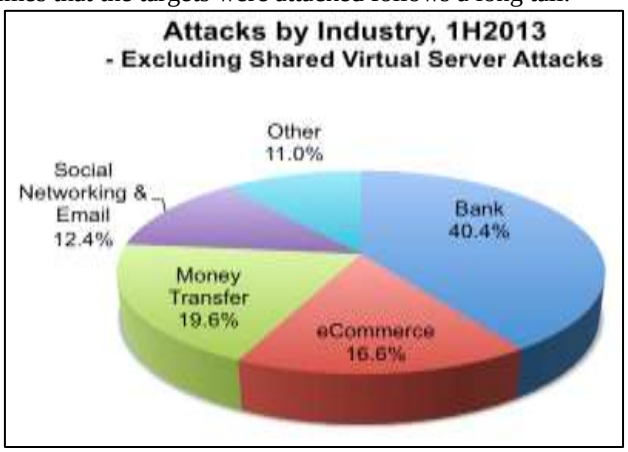
Nehal Rathod[1] Ankita Savardekar[2] S.P. Khachne[3]
[1,2]Student [3]Professor
[1,2,3]Rajiv Gandhi Institute of Technology, Mumbai

Abstract— E-Banking appeared when banks planned to capture more customer base and geographical region at the cost of minimal Human intervention. Nowadays this is one of the most important sources for performing bank related operations online. When you will register for Online banking you will get login Id which is generated by system and is Unique across all the registered users of that bank. The most important goal of security enhancement using data hiding in image is to hide messages within the image so the intended receiver of the image get the data of his interest in the form of the image so even if this image fall in wrong hand chances are less that person receiving the image get to know that some data is hidden in the image. This kind of technology is very useful in case of increasing security of the secure system. Through hiding a secret message inside the Image, a simple image is taken as carrier to carry the data to be hidden in it. Once Image is obtained, data that needs to be hidden is taken from user and is placed between the data bytes of actual image such that receiver of the image may consider it as normal image but when supply this image to decoder, can extract the hidden message within it in its entirety.

Key words: LSB (Least Significant Bit), E-Banking, BPCS

I. INTRODUCTION

It is banking website that lets you perform operation online at your convenience 24X7, 365 Days of year. It is kind of web site that makes user e banking experience more pleasant and secure by providing two factor Authentication that minimizes the chances of Unauthorized access to users account by way of Phishing.As mentioned in the need of project, the problem was to find a way in which the end user can gain the benefits of all the software applications without having to buy them or install them at their workstations. In other words, the problem was to develop a web architecture where the software applications can be considered as 'Software Solutions' and that too at low cost.We counted 720 unique target institutions during the period, up significantly from the 611found in 2H2012. The number of times that the targets were attacked follows a long tail.



- PayPal was the most-targeted institution (13,498 attacks, or 18.3% of the total),
- followed by Taobao.com (6,605 attacks, or 9%).
- The top 80 targets were attacked 100 or more times each in the period.
- Half of the targets were attacked one to three times during the period.[3]

A. *Two-Factor Authentication*

Two-factor authentication adds a second level of authentication to an account log-in. When you have to enter only your username and one password, that's considered a single-factor authentication. 2FA requires the user to have two out of three types of credentials before being able to access an account.

B. *Three-Factor Authentication*

A password is one of the only three known means of authenticating the identity of an individual (FIPS 145). Authorities today agree that effective authentication of a person's identity requires a combination of at least two of the three independent means of authentication, or factors

1) Something known: a memorized "Secret" word, phrase, number, code, or fact known only to an individual (and the entity to whom he/she is identifying him/herself).
2) Something possessed: a discrete "Token" which strongly resists counterfeiting, such as a signet ring, a key, a badge, a wax seal, a credit card with a holograph, etc.
3) Something one is, or a measurement of the individual: a characteristic "Biometric" such as a fingerprint, signature, voiceprint, picture, retinal pattern, DNA, etc[4].

II. PROPOSED SYSTEM

A. *System Overview*

- The Proposed System makes the Security level high on the E-Banking sites. It disables the unauthorised user to get access to the authorised user account account with 3 layers of Security provided.
- The First layer which is the simple login page having user login ID and password field to be filled.The user with correct password and ID is allowed to proceed further with Second layer of authentication which is nothing but it sends the Secondary Password which keeps Changing all the time to all users through the Process of Stegnography.
- Now the Second layer includes Stegnography process which means hiding the text in images and that image is mailed to the user as a Security phase.The user needs to download that Image and paste the path of that image as the Secondary Password. The Password is now automatically abstracted from the Image and if matched

with the user, he/she is allowed to enter the Third layer of Authentication.

- The Third layer of Authentication the user is sent a confirmation of his/her Password that is, OTP-ONE TIME PASSWORD is generated for that particular user for his authenticate user Verification. It is sent via sms to the user. This Password is now entered by the user on the last authenticating login screen. If the Password is matched than the user can successfully enter the E-Banking site account where he can be able to check his balance,transfer money and carry out all his banking transactions related to E-Banking.
- As a bank we are used to thinking about security. The growth of the Internet has offered greater flexibility for us all, but it also brings new risks that must be guarded against.
  1) Steps of Security Used
  2) Multi layer logon verification
  3) Transaction verification
  4) 128 bit Secure Socket Layer (SSL) Encryption

III. ALGORITHMS

A. LSB (Least Significant Bit)

Least significant bit (LSB) insertion is a common and simple approach to embed information in an image file. In this method the LSB of a byte is replaced with an M‟s bit. This technique works good for image steganography. To the human eye the stego image will look identical to the carrier image.. For hiding information inside the images, the LSB (Least Significant Byte) method is usually used. To a computer an image file is simply a file that shows different colors and intensities of light on different areas of an image. The best type of image file to hide information inside is a 24 Bit BMP (Bitmap) image. When an image is of high quality and resolution it is a easier to hide information inside image. Although 24 Bit images are best for hiding information due to their size. Some people may choose 8 Bit BMP‟s or possibly another image format such as GIF . The reason being is that posting of large images on the internet may arouse suspicion. The least significant bit i.e. the eighth bit is used to change to a bit of the secret message. When using a 24-bit image, one can store 3 bits in each pixel by changing a bit of each of the red, green and blue color components. Suppose that we have three adjacent pixels (9 bytes) with the RGB encoding .[1]

10010101 00001101 11001001
10010110 00001111 11001011
10011111 00010000 11001011

When the number 300, can be which binary representation is 100101100 embedded into the least significant bits of this part of the image. If we overlay these 9 bits over the LSB of the 9 bytes above we get the following (where bits in bold have been changed)

10010101 00001100 11001000
10010111 00001110 11001011
10011111 00010000 11001010

Here the number 300 was embedded into the grid, only the 5 bits needed to be changed according to the embedded message. On average, only half of the bits in an image will need to be modified to hide a secret message using the maximum cover size.

The simple algorithm for OPA explains the procedure of hiding thesample text in an image.[4]

1) Select a cover image of size M*N as an input.
2) The message to be hidden is embedded in RGB component only of an image.
3) Use a pixel selection filter to obtain the best areas to hide information in the cover image to obtain a better rate. The filter is applied to Least Significant Bit (LSB) of every pixel to hide information, leaving most significant bits (MSB).
4) After that Message is hidden using Bit Replacement method.

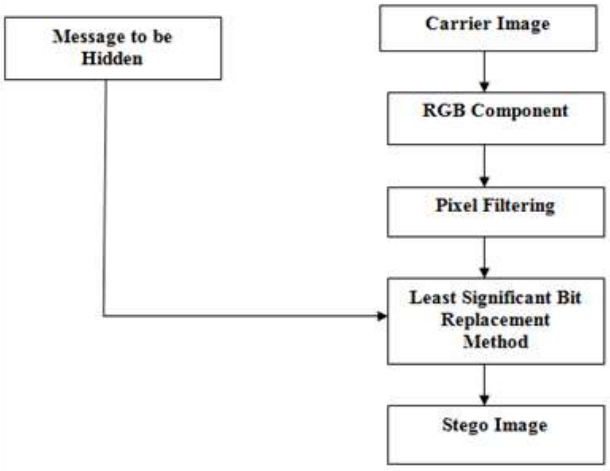


Fig. 8: Block diagram for LSB algorithm

B. BPCS (Bit Plane Complexity Segmentation)

BPCS steganography was introduced by Eiji Kawaguchi and Richard O. Eason, to overcome the short comings of traditional steganographic techniques such as Least Significant Bit (LSB) technique, Transform embedding technique, Perceptual masking technique. Previously steganographic techniques have limited information-hiding capacity.50–60% Data can be hidden after implementation of this paper . This technique is called Bit Plane Complexity Segmentation (BPCS) Steganography. BPCS steganography makes use of important characteristic that of human vision. In BPCS, the vessel image is divided into ―informative region‖ and ―noise-like region‖ and the secret data is hidden in noise blocks of vessel image without degrading image quality. In LSB technique, data is hidden in last four bits i.e. only in the 4 LSB bits. But in BPCS technique, data is hidden in MSB planes along with the LSB planes provided secret data is hidden in complex region.[2-9]

C. The Merits of BPCS-Steganography are as follows. 1)

The information hiding capacity of a true color image is around 50%. 2) A sharpening operation on the dummy image increases the embedding capacity quite a bit. 3) Randomization of the secret data by a compression operation makes the embedded data more intangible. 4) Customization of a BPCS - Steganography program for each user is easy. It further protects against eavesdropping on the embedded information 5) It is most secured technique and provides high security.[4]

D. Hiding and Extracting Data

We start off by converting a sample 8-bit grayscale image into CGC (Canonical Gray Coding) form. CGC allows us to

manipulate each bit plane without affecting the other bits that represent each grayscale value. 8x8 pixel blocks are segmented within the image and each of the bits (8 bits per pixel) in CGC form will have their own corresponding 8x8 plane. Visually, this would be like slicing the 8x8 planes into 8 8x8 black and white bit planes (see CGC diagram). Each bit plane will be measured for complexity, which is determined by the number of borders (transitions between black and white in each pixel plane) present in an 8x8 bit plane versus the maximum borders possible. If a region is complex enough, we will embed our data into the cover image, which is broken up into appropriately sized 8x8 blocks for each bit plane. If the data to embed (8x8 blocks at a time) in the cover file is statistically complex, it can be embedded into the complex blocks of the image. If not, we will conjugate (exclusive or) the data with a checkerboard pattern (the most complex pattern possible) to ensure complexity. There will be a conjugation bit in each plane that will show whether the data was conjugated with a checkerboard pattern. This technically gets rid of 1 bit of embedding capacity per 8x8 region giving 63 bits to embed per 8x8 bit plane.

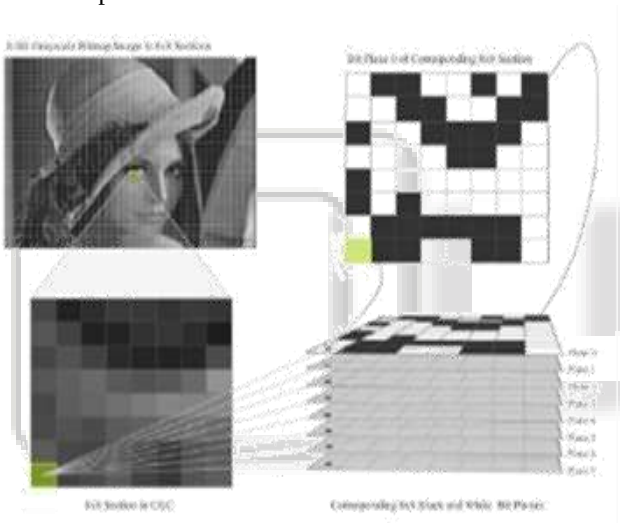


Fig. 3: CGC Diagram

Once the data has been embedded, the image is converted back into the original format from CGC and saved. Extraction is basically the same as embedding, except if a bit plane is determined to be complex, it will then look at the conjugation bit and extract the data accordingly. Because the embedded data in the complex regions has to be complex, the complex regions before and after embedding data will remain complex. Color is basically the same process. However, it will have 3 8-bit grayscale values that represent each color, thus giving approximately three times the file size and three times the embedding capacity (to its corresponding grayscale version). A subtle other difference is that the color file has a slightly different file structure that does not contain a palette for the pixel values.[3]

IV. Conclusion and Future Scope

The LSB modification technique provides an easy way to embed information in images, but the data can be easily decoded. The proposed scheme used in our project makes use of three factor authentication which thereby enhances the security of the system. Certainly the time complexity of the overall process increases but at the same time the security achieved at this cost is well worth it. This cryptographic scheme can be used for other steganographic techniques.

References

[1] Shailender Gupta, Ankur Goyal, Bharat Bhushan "Information Hiding Using Least Significant Bit Steganography and Cryptography" Published Online June 2012 in MECS DOI: 10.5815/ijmecs.2012.06.04
[2] Pranita P. Khairnar, Prof. V. S. Ubale "Steganography Using BPCS technology "International Journal of Engineering and Science Vol.3, Issue 2 (May 2013).
[3] Rosziati Ibrahim and Teoh Suk Kuan Faculty of Computer Science and Information Technology, University Tun Hussein On"Stegnography Algorithm to Hide Secret Message Inside an Image"February 25, 2011.
[4] Clair, Bryan, "Steganography: How to Send a Secret Message", 8 Nov. 2008 www.strangehorizons.com/2001/20011008/steganography.html.
[5] "Cryptography and Network Security: principles and practices", William Stallings, pearsons education, first Indian reprint 2003.
[6] IEEE paper on Review: Steganography – Bit Plane Complexity Segmentation (BPCS) Technique IJEST Vol. 2(9), 2010.

