Development of Online Banking System Based on Secure Captcha Image Using Visual Cryptography

Lwin Lwin Oo
University of Computer Studies, Mandalay (UCSM)
Mandalay, Myanmar lwinlwinoo@ucsm.edu.mm

Abstract*— Network Security and privacy are the main expected features in the field of online banking system. Internet banking (online banking) system provides banking services over the internet. It also provides convenience for users and plays a vital role in human lives. Securing online banking system is implemented with captcha image, BPCS steganography and visual cryptography. This system is constructed with registration and login processes between users and administrator of online banking system. Security input password text string is converted into an image by using captcha image generation process because other users are difficult to read not to see. This image is split based on the visual cryptography. The share 2 is hidden into the cover image by using BPCS steganography and sends to the user and the share1 is stored on the database. One time password (OTP) is sent to the user's mobile. This system provides high security for the online banking system.

Keywords— Captcha image, BPCS steganography, *visual cryptography, OTP*

I. INTRODUCTION

In the recent years, Internet has become increasingly popular and used by many people from all over the world. Nowadays, online banking system has become increasingly popular and is widely used in currency. Internet banking (online banking) system provides banking services over the internet such as paying of bills, funds transfer, viewing account statements, etc. It also provides convenience for users and plays a vital role in human lives. It saves time and cost of users and users can access internet banking wherever they are.

As quick as the Internet Banking, the assaults over the online account too increase. And then the threats of online banking fraud have also become a greater concern. Client certainty and devotion to a bank with online managing an account administrations depend significantly on the assurance against managing an account extortion and assault. So, security of internet banking system is a major concern for the financial institutions and their users.

This system is implemented with visual cryptography to make internet banking system more secure and reliable. This system is constructed with registration and login processes between users and administrators of internet banking system. Security texts of the user's personal data and Security text password string are filled in the registration phase. The 'Security text password string' is used as the user input. This input is converted into an image by using captcha image generation process. The captcha image is split into share1 and share 2 based on the visual cryptography. The share 2 is hidden into the uploaded cover image by using BPCS steganography and sends it into user's email account and user must download it .The share1 is kept at server database. In the login process, user login with the stego image. The share2 is extracted from stego image by using BPCS steganography. .Both share1 and share2 are stacked by using Visual Cryptography to reveal the captcha image. Finally, only after verifying the CAPTCHA is correct, One Time Password is sent to user's mobile. The user enters account password and does transaction of the Banking System. This system is implemented by using PHP Programming Language.

II. RELATED WORK

Several methods have been introduced and approaches have been proposed to secure of the online banking. Some of the researchers focused on challenging attacks to discover more secure techniques of the online banking system.

Madhurani B Shiddibhavi, Pundalik Ranjolekar [6] proposed the Detection and Prevention of Data Hacking in Net Banking. This project aimed to achieve the authenticity by visual cryptography technique namely 2 out of 2 scheme technique. The scanned signature image is used as an input to create new bank account. Bank gave one split to user and another will be stored in bank database by using visual cryptography technique. From this technique the secrete data authentication and secure transactions achieved through the online service. This technique applied for photographs and color images.

Aparnaa. K. S, Sathyasundaram. M., Santhi. P. [2] presented Securing Internet Banking with a Two - Shares Visual Cryptography Secret Image. The user who wants to Log-IN must answer a randomly chosen question about the Secret image. This security image used with (2, 2) threshold VCS scheme and CaRP (a CAPTCHA and a graphical password scheme) as a security key for users. Final step used to check whether the website is an authorized website or a phishing website by displaying a Secret Image CAPTCHA. This system prevented Phishing attacker and masquerade attacks.

Shrikant S. Khaire, DR. Sanjay L. Nalbalwar [8] presented Review: Steganography – Bit Plane Complexity Segmentation (BPCS) Technique. This paper focused on basic steganography and various characteristics necessary for data hiding. Implemented a steganography technique had hiding capacity up to 50 – 60%. The secret data was hidden into noise-like region of the vessel image without any deterioration. The original image and the final embedded image appeared to be identical to the human eye.

Madhurani B Shiddibhavi, Pundalik Ranjolekar [6] described Detection and Prevention of Data Hacking in Net Banking Using Visual Cryptography Technique. This paper achieved the authenticity by visual cryptography technique namely 2 out of 2 scheme technique. It takes scanned signature image as an input. Decision of access granted or denied will be confirmed based on comparison of stacked and original image. If both are same then it will be confirmed that the user. The similarity level of signature decided the

acceptation and rejection of user from transaction service. From this technique the secrete data authentication can be achieved and secure transactions can be done through the online service.

III. SYSTEM DESIGN AND IMPLEMENTATION

Online banking system is constructed with registration and login processes. This system is implemented with the combination of steganography and visual cryptography.

In the registration process, the user registers the personal information and security password key string (letter or number) in the online banking which is used as input. Then this security password input is converted into an image by using captcha image generation process. It is stored in the server database during later verification process that occurs at the login process. This captcha image is split into share1 and share2 based on the visual cryptography. The share2 is hidden into the uploaded cover image by using BPCS steganography. Classify each bit-plane block of the cover image is 'simple block' or 'complex block' by using a standard complexity threshold value of each bit-plane block (α_o) = 0.3. We embed the share2 provided by the user into an image of Black and White random pixel combination of background. And then this image sends to user's email and user must download it. The system's administrator stores the share1 into the database for checking the user in login process. Steganography is used again in this system to the confidentiality of the security goal because the share2 hidden into cover image is stored in user as the message. The user needs to save this stego- image because user must log in with this stego- image. This registration process for internet banking system is shown in Figure 1.

In login process, the user must enter with stego image in order to extract share2 from it. The extracted share2 and the share1 from the database are superimposed by using visual cryptography to achieve the authenticity. If administrator (sever) also gets satisfied to display the actual CAPTCHA image the end user. The user must enter secret password key string. Finally, only after verifying the CAPTCHA is reliable, and administrator (sever) sends the OTP message to the user. The user login the system with one time password by using Telerivet mobile Messaging in the final step. This login process for online banking system is shown in Figure.2.

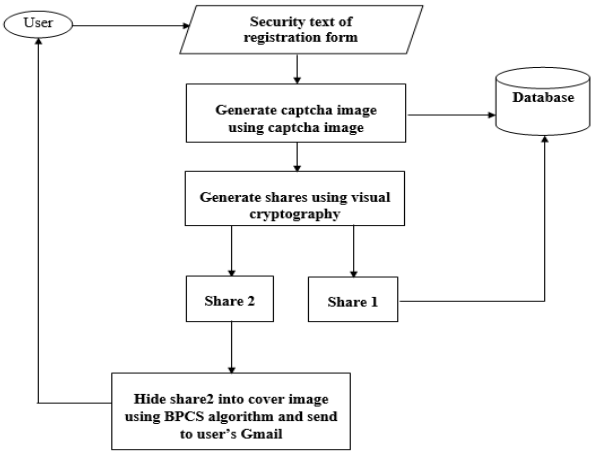

Figure 1. Registration Process for Online Banking System

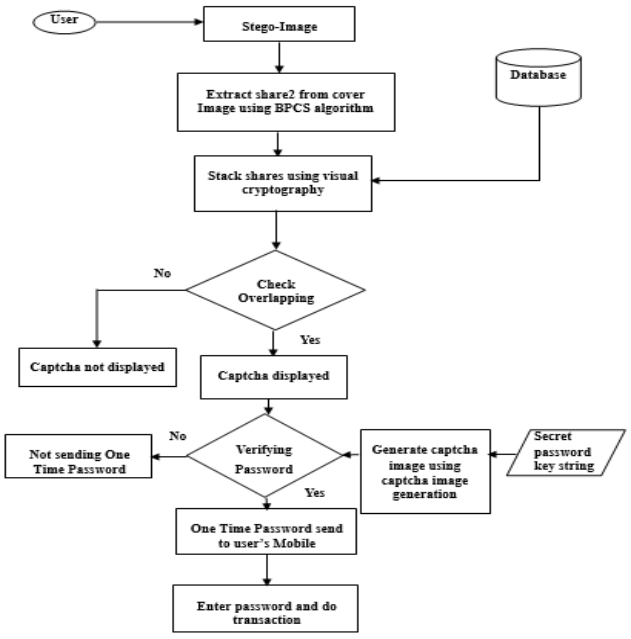

Figure 2. Login Process for Online Banking System

IV. THEORETICAL BACKGROUND

The online banking system has two parts: registration and login processes using with CAPTCHA, Visual cryptography and Bit Plane Complexity Segmentation (BPCS) steganography.

A. CAPTCHA

CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) is a standard security technique used to protect many online services. CAPTCHA is an image consisting of digits or letters and it requires that the user types the digits or letters that are displayed in the captcha image. Types of CAPTCHA are: Text-based Captcha, Image-based Captcha, Audio-based Captcha and Video-based Captcha. Text-based Captcha is the most widely used captcha system to provide higher security in online services. The main advantage of using text-based Captcha is that it can solve the difficulty of remembering passwords because passwords are displayed with a twisted manner in the captcha image. For generating CAPTCHA image, the steps of captcha image are as follows:

Step1: Create a background of desired dimension sufficient to hold the text string (256×64)

Step 2: Define the number of text string which is used as the password (only five characters)

Step 3: Choose the font, font size, font style and font color for the text string

Step 4: Write the text string to the background with the use of TrueType Fonts in PHP, i.e built-in function: imagettftext ($image, $size, $angle,$x, $y, $font, $text)

B. Visual Cryptography

Visual cryptography is a cryptographic technique which allows visual information to be encrypted and one of the best methods to protect the integrity of the data. The visual

cryptography Scheme (VCS) or the secret sharing technique encrypts a secret image by breaking it into two or more share images. It encrypts and decrypts an image without the use of any public or private key. A distinctive feature of VCS is that one can visually decrypt the secret image by superimposing shares without computation. Some important types of threshold Visual Cryptography schemes are: (2, 2) threshold VCS, (2, n) threshold VCS, (n, n) threshold VCS, (k, n) threshold VCS. (2, 2) threshold VCS is a basic threshold scheme of Visual Cryptography. The input is a secret image and the pixels of this image is encrypted into two different (sub pixels) shares. To reveal the output into the secret image, both shares must be overlaid [5]. The steps of (2, 2) threshold VCS are:

Step 1: Take an image as input

Step 2: Create a random binary image of the size equivalent to the input image and it is called share1

Step 3: XOR the share1 with the input image and the result image is share2

C. Bit Plane Complexity Segmentation Steganography

The Kyushu Institute of Technology is the first to propose the Bit Plane Complexity Segmentation (BPCS) steganography. BPCS Steganography is an image based on steganography method and it is based on complexity of image which is used to determine the complex block of the image in order to achieve a better diffusion of the data into the cover image (maximum complexity is 1 and minimum complexity is 0). It performs hiding process at all bit-plane blocks by finding complex block and replaces it with secret data.

Bit Plane Complexity Segmentation (BPCS) is an ancient compression technique used to embed secure data in the images. The main principle of BPCS technique is based on the simple idea that the higher bit planes could also be used for embedding information in noise like regions or complex regions. BPCS Steganography depends on the characteristics of the human vision system (HVS) in which a human not able to see any information in more complex blocks so that secret data is placed into all complex blocks.

The main goal of BPCS Steganography is to make use of a large embedding capacity of image for data hiding without much distortion in the visual appearance of the original image [3]. BPCS Steganography Algorithm:

Step 1: Convert the cover image from Pure Binary Code (PBC) to Canonical Gray Code (CGC).

Step 2: Perform bit plane slicing on cover image

Step 3: Calculate complexity measure 'alpha' (α) for each block of each bit plane of cover image.

Step 4: Segment each Bit-Plane of the cover image into 'informative' and 'complex' regions by using a standard threshold value (α_o) =0.3.

Step 5: If the complexity of each Bit-Plane of the cover image is less than the threshold value (α_o), then conjugate operation is done with the checkerboard pattern in order to make a more complex blocks. If the complexity of each Bit-Plane of the cover image is greater than or equal to the threshold value (α_o), then the secret data can embed in the complex regions of the Bit-Planes of the cover image.

Step 6: Recompose the Bit-Planes back into an image. Resulting embedded image will be called as stego image.

D. Telerivet Mobile Messaging

Telerivet is the first ready-to-use SMS communications platform that works in any country without any need for servers or mobile network integrations. With Telerivet, anyone can easily create, launch and manage an SMS service or interface that runs on any mobile network anywhere in the world. Telerivet Gateway is a free software application from the Telephony subcategory, part of the Communications category. With Telerivet, the user can turn his smartphone into a gateway in four easy steps:

Step 1: Create an account on the Telerivet website

Step 2: Create a project link to the service on the website

Step 3: Download and install Telerivet Gateway app on the smartphone.

Step 4: Link the mobile app to the project on the website.

V. EXPERIMENTAL RESULTS

There are many different methods to measure steganography technique can be determined by comparing cover-image with the stego Image. The various factors are: Robustness, Imperceptibility Bit Error Rate, Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR) Entropy, etc. Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI) are two most commonly used to measure the security level. Both NPCR and UACI are used to test how much difference between cover image and stego-image. NPCR and UACI become two widely used security analyses in the image encryption community for differential attacks. High value of NPCR refers that the change in pixel value has high impact on the appearance of image. UACI is utilized to measure the regular intensity of dissimilarities between the two images. The larger the UACI is, the more resistant to the differential attack the encryption. The NPCR determines the percentage of different pixel numbers between the two images such as original image and encrypted image as follow:

$$D(i,j) = \begin{cases} 1, & P(i,j) \neq C(i,j) \\ 0, & P(i,j) = C(i,j) \end{cases} \quad (1)$$

NPCR is defined by the following formula:

$$NPCR = \frac{\sum_{i=0}^{M-1}\sum_{j=0}^{N-1} D(i,j)}{M \times N} \times 100\% \quad (2)$$

UACI is utilized to measure the regular intensity of dissimilarities between the two images. It is defined by the following formula:

$$UACI = \frac{1}{M \times N}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}\frac{|P(i,j)-C(i,j)|}{255} \times 100 \quad (3)$$

where M×N = dimension of image,

P = cover image,

C = stego image,

D = binary array with the same sizes as original image and stego image.

In this system, stego image is needed to secure because this image sends to user. It is more similar to original (cover) image, the system is more secure. So this system is tested based on fourteen image sizes (pixels) black and white cover image with three different formats (PNG, BMP, JPEG). The fourteen image's pixel sizes are 424×104, 432×112, 440×120, 448×128,456×136, 464×144, 472×152, 480×160,

488×168,496×176, 504×184, 512×192, 520×200 and 528×208. NPCR, UACI, PSNR, MSE and MOS are used to test the performance of the system.

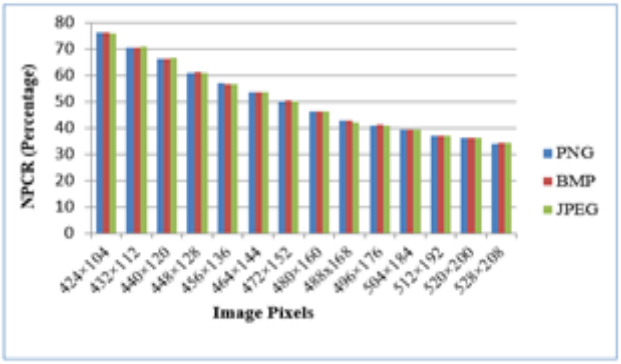

Figure 3. NPCR Values for PNG, BMP and JPEG Image Formats

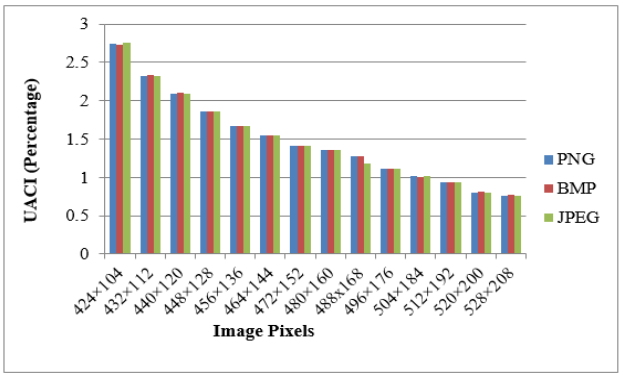

Figure 4. UACI Values for PNG, BMP and JPEG Image Formats

According to the Figure 3 and Figure 4, image's pixel sizes of the images are less, both of NPCR and UACI values are high. The image pixel size 424×104 is the highest NPCR and UACI values and image pixel size 528×208 is the lowest values of NPCR and UACI. The values of NPCR and UACI in the system show that the less value of the image pixel size is, the better the security level.

After testing, PSNR values of 528×208 image size are larger than other image sizes and MSE values of 528×208 image size are smaller than other image sizes. When the image size is large, the value of PSNR is large and that of MSE is small. So, the stego-images for larger pixel sizes are less distortion from the original image.

Table 1 shows the average NPCR, UACI, PSNR and MSE values of fourteen image sizes with PNG, BMP and JPEG image formats.

TABLE I. AVERAGE NPCR, UACI, PSNR AND MSE VALUES FOR THREE IMAGE FORMATS

Image Format	NPCR (%)	UACI (%)	PSNR (dB)	MSE
PNG	50.74	1.49	36.4	16.37
BMP	50.80	1.51	36.42	16.30
JPEG	50.72	1.48	36.41	16.31

According to Table 1, the average NPCR and UACI values of BMP image format is higher than other image formats. The image quality measurement between cover image and stego- image of BMP image format is the maximum PSNR and minimum MSE.

And then the visual quality between original and stego-images depending on own opinion is also tested for three image formats (PNG, BMP, JPEG) with Mean opinion score (MOS) .The MOS is a measure overall visual quality evaluation of the system with a single rational number in the range 1-5, where 1 is the Bad or lowest perceived quality and 5 is the Excellent or highest perceived quality. The following formula is used to calculate MOS:

$$MOS = \frac{\sum_{j=1}^{M}(\frac{\sum_{i=1}^{N} S_{ij}}{N})}{M} \quad (4)$$

where M = number of images,
N = number of persons and
S = score of i^{th} images

TABLE II. MOS SCORES OF 5 PEOPLE FORORIGINAL AND STEGO-IMAGES

Image Type	Person 1	Person 2	Person 3	Person 4	Person 5	Total Scores	MOS values
1.bmp	5	5	5	5	4	24	4.8
2.bmp	4	4	4	4	4	20	4
3.bmp	5	5	5	5	4	24	4.8
4.bmp	4	5	4	4	5	22	4.4
5.png	4	4	4	4	4	20	4
6.png	4	4	4	4	4	20	4
7.png	4	4	4	4	3	19	3.8
8.jpeg	4	4	4	4	4	20	4
9.jpeg	4	4	4	4	4	20	4
10.jpeg	4	4	4	4	4	20	4

According to Table 2, MOS score of this system is good because MOS values are almost 4 for each image of three image formats. The stego- images are the same as the covered images. The system provides confidentiality of the security goals. MOS score of BMP image format is greatest the other image formats. Therefore, this system finds that the BMP image format is better image quality and higher security level than other image formats

VI. CONCLUSION

A role of image steganography and visual cryptography is more and more important in today's multimedia world. The securement based on visual cryptography provides more security than other traditional mechanisms. The Development of Online Banking System is implemented with the three security algorithms and two verifying processes. CAPTCHA is used for displaying and verifying and (2, 2) threshold VCS scheme that involves 2 shares of Security image to achieve the authenticity and to avoid phishing attack. BPCS Steganography is used to for confidentiality. Finally, user enters log in to the banking system with one time password (OTP) from the user's mobile message. So, the attacker can't mishandle the stolen information.

In this system, three image formats (PNG, BMP, JPEG) with fourteen different pixel sizes are tested for measuring encryption quality and image quality. In average, the encryption quality of BMP image format is better than other

image formats and the image quality of the stego-image is near identical to the original image. This system reduces the potential vulnerabilities regarding to the security. Therefore, this online banking system is significantly useful in the growing online fields such as Banking, Financial, Shopping market.

REFERENCES

[1] A. Vinodhini, L. Jani Anbarasi, "Visual Cryptography for Authentication using CAPTCHA", International Journal of Computer and Internet Security, Vol.2, 2010

[2] Aparnaa. K. S, Sathyasundaram. M., Santhi. P, "Securing Internet Banking with a Two - Shares Visual Cryptography Secret Image", International Journal of Engineering Research & Technology (IJERT), Vol. 5 Issue 02, February-2016.

[3] Andysah Putera Utama Siahaan, "High Complexity Bit-Plane Security Enhancements in BPCS Steganography", International Journal of Computer Applications, Volume 148– No.3, August 2016.

[4] "Integer Wavelet Bit-Plane Complexity Segmentation Image Steganography", International Journal of Engineering and Technology, Vol.1, Issue 3, 2015.

[5] Ms. Bhawna Shrivas, Prof. Shweta Yadav, "A survey on Visual Cryptography Techniques and their Applications", International Journal of Computer Science and Information Technology, Vol.6 (2), 2015.

[6] Madhurani B Shiddibhavi, Pundalik Ranjolekar, "Detection and Prevention of Data Hacking in Net Banking Using Visual Cryptography Technique", International Journal of Innovative Research in Computer and Communication Engineering, Vol.4, Issue 6, June 2016.

[7] S. Amier Haider Sha, "Breaking e-Banking CAPTCHAs", National University of Science and Technology, Pakistan.

[8] Shrikant S. Khaire, DR. Sanjay L. Nalbalwar, "Review: Steganography – Bit Plane Complexity Segmentation (BPCS) Technique", International Journal of Engineering Science and Technology Vol. 2(9), 2010.