International Journal of Computer Science and Engineering (IJCSE)
ISSN 2278-9960
Vol. 2, Issue 3, July 2013, 21-26


International Academy of Science, Engineering and Technology
Connecting Researchers; Nurturing Innovations

# ANTI-PHISHING USING VISUAL CRYPTOGRAPHY

**V HEMANTH[1], M SHAREEF[2] & K S RANJITH[3]**

[1,3]Assistant Professor, Department of Computer Science and Engineering, Sree Vidyanikethan Engineering College, Tirupathi, Andhra Pradesh, India

[2]Department of Computer Science and Engineering, Sree Vidyanikethan Engineering College, Tirupathi, Andhra Pradesh, India

## ABSTRACT

Internet plays a vital role in the day to day life of a human. Online transactions made the user to book all kinds of tickets and purchasing things easier. Instead of standing for a long time in a 'Q', the user tries to complete his work online. The main use of online is banking. There are so many types of attacks to misuse the online system. One among them is the Phishing attack. In this paper a solution for phishing attack has been introduced using visual cryptography. This paper mainly concentrates on the online banking system to avoid users not to provide all the information like password, credit card details etc. to an Intruder.

**KEYWORDS:** Image Shares, Phishing Attack, Visual Cryptography

## INTRODUCTION

Phishing (pronounced "Fishing") is one of the major attacks on the online system.

This attack will not hack any server or the website; it just creates a duplicate copy of the website and tries to communicate to confuse the user [1]. This attack mainly concentrates on the design of the website to be same as the original one. By sending the link of the false website to the mail of the user, he tries to click on the given fake link to accesses the website by thinking as the original link of the website. In this attack the intruder tries to get the following details from the user like: Name, Username, Password or PIN, Bank account number, ATM/debit or credit card number, Credit card validation code (CVC) or card verification value (CVV) etc [2].

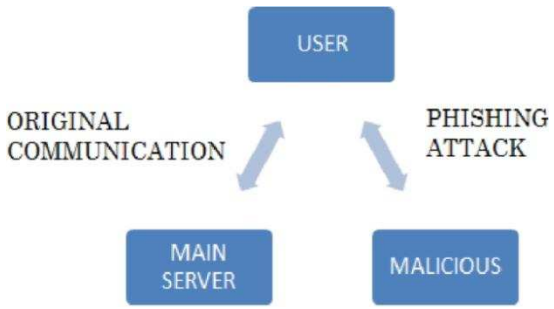


**Figure 1: Phishing Attack**

**Some of the Examples of Phishing Schemes are**

- Sending the fake e-mail message to the banker user, as if the database of the bank has been crashed due to some technical reasons, So they request for the updation of the personal information.
- Fake charities asking to donate money to the poor people and for the old age home for their development etc. By donating the money it will be misused.

**How to Identify Phishing Attacks**

In order to identify the phishing attacks we are explained briefly with some identification schemes.

**How Can I Tell if an E-Mail is Fraud?**

Generally, the phisher become more intelligent, for the user who has no idea about the usage of internet. For the user who doesn't know much about internet can't be able to identify which is original and fake. In order to confuse the user [3].

- **Sending an E-Mail for the Retrieval of Personal Information**

  Most legitimate businesses have a policy that they do not ask you for your personal information through e-mail. Be very suspicious of a message that asks for personal information even if it might look legitimate..

- **Fake Links**

  Here mainly the fake message contains the real company logo's. But if we click on the link which is provided in the web page, it will be diverted towards the phisher's database.

- **URLs that Include the @ Sign**

  In the link given below, the URL will divert you to the page specified after the @ symbol.

  Example: **https://www.woodgrovebank.com@nl.tv/secure_verification.aspx**

The URL location, **nl.tv/secure_verification.aspx**, can be an fake site, remains pervasive and is often protected by national boundaries.

**Phishing Attack Possible through Hyperlinks**

The common characteristics of the hyperlinks in phishing e-mails are listed below:

- The actual link and visual link are not one and the same.
- The attackers often use dotted decimal IP address instead of DNS name.
- Special tricks are used to encode the hyperlinks maliciously.
- The attackers often use fake DNS names that are similar (but not identical) with the target Web site

**Best Practice for Protecting Online Accounts**

- Never respond to the e-mail messages which request for your personal information.
- Never respond to the malicious links.
- Change your passwords weekly or fortnight and use a password which is meaningless.
- Never use e-mails for sending the personal information.
- Make the notes of your transactions.
- Transactions on the Internet Use credit cards.

**Visual Cryptography**

Visual Cryptography (VC) [7][8]is special encryption technique for hiding the visual information(e.g. printed text,

handwritten notes and pictures)by performing encryption, such that encoding the information into shadows/layers/shares, no single layer can give information alone ,To reveal the secret information the user should need more than two shares. By doing this process it will be difficult for a human vision to extract the original data if minimum shares are not available.

**Advantages of VC**

- Simple to implement.
- Decryption algorithm not required (Use a human Visual System). So a person unknown to cryptography can decrypt the message.
- Infinite Computation Power can't predict the message.

In this paper, two shares will be combined to form a new image. In this paper with the help of visual cryptography, the solution for phishing attack can be eradicated. The detail about the proposed technique and the conclusion is described in section 2 and section 3 respectively.

## PROPOSED TECHNIQUE

In this proposed method, it describes how to protect the bank account from the phishing attack. Now a day's so many fake mails regarding 'WON CASH PRICE' please send your bank details to deposit your cash price are send to the e-mail users to miss lead. Not only this some fake mails regarding bank, says that the database has been crashed and ask for updating the personal information to maintain a new database [5].

The user without any regression he/her tries to give the personal information, this information will be sent to the intruder but not to the original bank. So by doing this the user data will be given to an intruder. To avoid this, VC concept have been embedded to protect the bank accounts.

The steps involved in preventing the phishing attacks:

**Step 1:** First user has to apply for online banking and the passwords will be sent through post or for security purpose, user has to collect it from bank personally.

**Step 2:** The user will be provided with two passwords, a) login password and b) Transaction Password along with an image.

**Step 3:** First the user will be logged with the login passwords, after that an image will be displayed which is provided along with the passwords.

**Step 4:** If the image matches with the image provided by the bank then the user has to give his transaction pass word. Otherwise the user should not provide his/her transaction password.

**Step 5:** After finishing the above steps, user has to change both the passwords and the image.

**Step 6:** A set of images of 2 groups which contain five images will be displayed; the user has to select two images each from two groups.

By providing the image the intruder cannot guess the correct image and so the intruder can't be able to get the personal details of the user.

All the above steps have been explained in the below diagram.

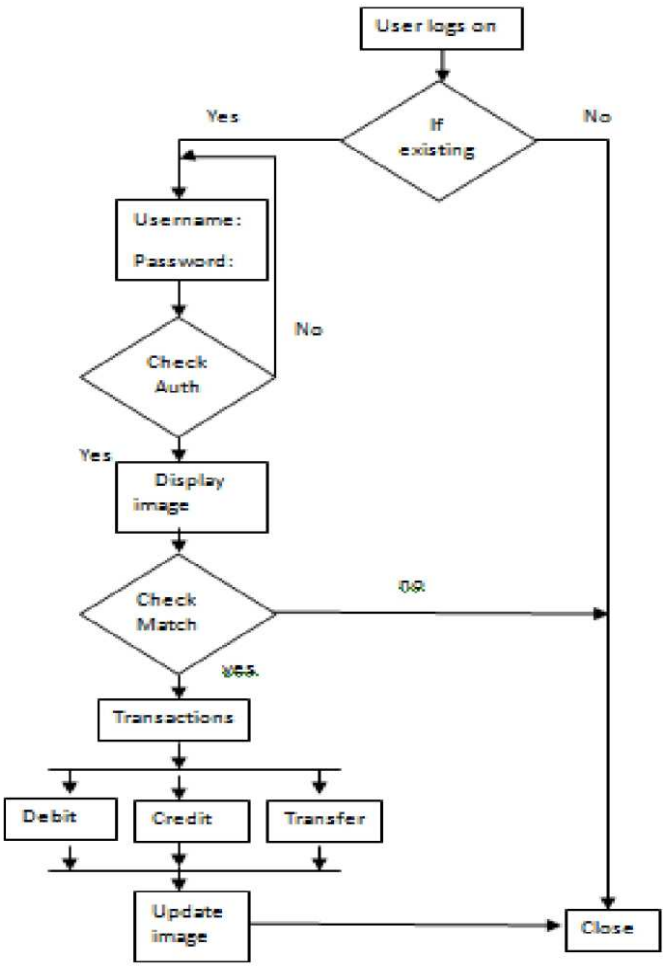


**Figure 2: Flow Chart of Proposed Method**

For each and every transaction if the user tries to generate a new image by combining the two shares, the security will be more. For each and every updation the server will provide the user with a new set of shared images. If the updation is done weekly of a fortnight the level of the security may be reduced. So it is recommended for the user to update the image for each and every login to maintain it security.

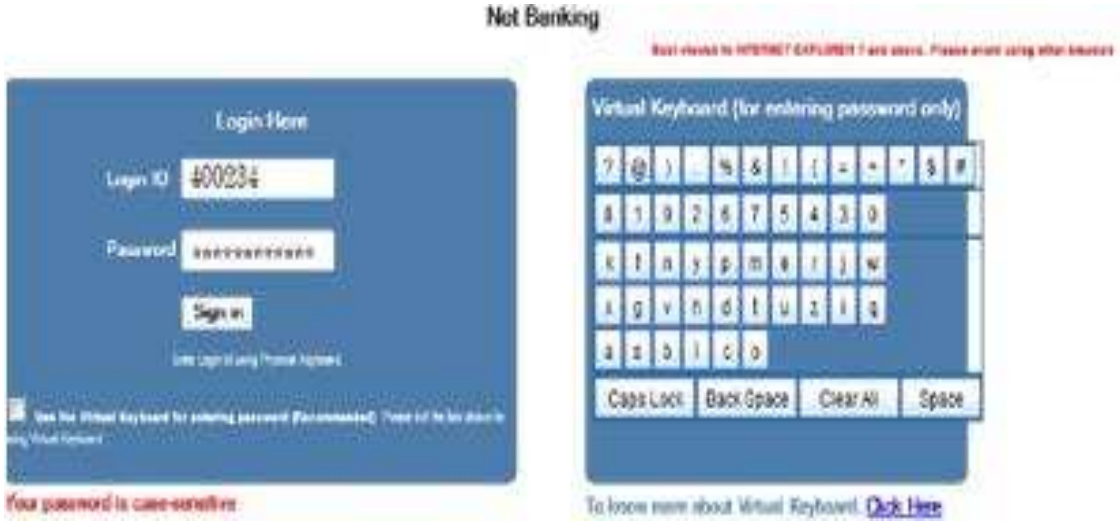


**Figure 3: Login Page**

First the user will be provided with the login ID and the two passwords and an image. With the help of login ID and login password as shown above, the user will be redirected to the next page if the ID and password matches.

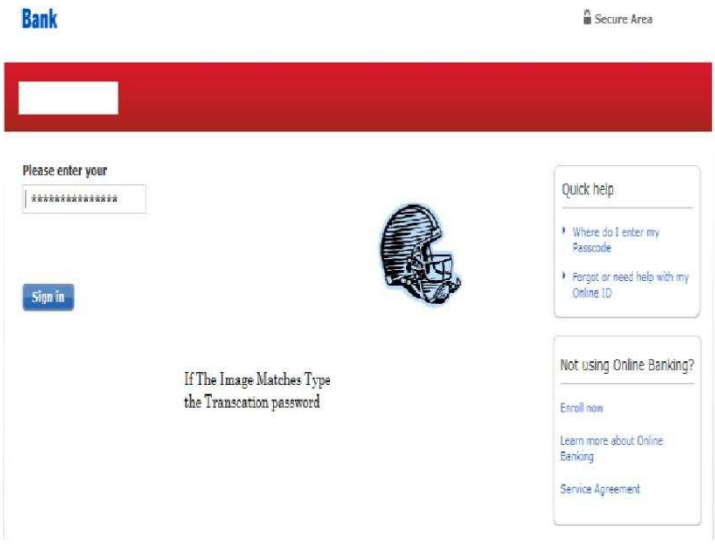


**Figure 4: Image Verification Page**

In the second page the user can see an image and if the image matches with the image provided by the bank, the user has to enter his second password called transaction password, demonstrated with a diagram above.

After login the user has to update his passwords and also has to upload a new image. Now the image updation places a major role. This will be done with the help of visual cryptography [8]. There will be having ten shares which is divided into two groups each of five shares. The selection should be done in such a way that the user has to select two shares one from each group. By combining any two shares an image will be generated, so in this process for each combination gives a different image. For each and every time when user tries to update the image a new image will be generated and the images will never give the previous repeated.

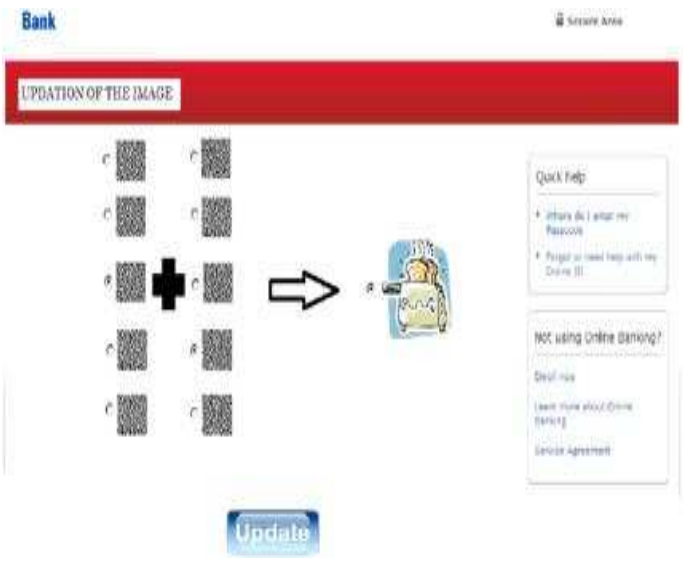


**Figure 5: Updation Page**

## CONCLUSIONS

In this paper the solution for anti phishing with the help of Visual Cryptography (VC) has been demonstrated. With the help of VC the security of the online banking system has been increased to some extent. By implementing the above technique the phishing attack can be eradicated. The security mainly concentrates on the updation of the image. If the user updates his/her image at each login then the security of his/her login will be more secure, if updations is done weekly or fortnight the level of security may vary.

## REFERENCES


1. N.P. Singh. “Online Frauds in Banks with Phishing”. Journal of Internet Banking and Commerce, vol.12, 2009.
2. Juan Chen and Chuanxiong.“Online Detection and Prevention of Phishing Attacks”. IEEE Communications and Networking, NSFC, 2005.
3. Bryan Parno, Cynthia Kuo, and Adrian Perrig. “Phoolproof of Phishing Prevention”. Financial Cryptography and Data Security, Springer, 2006.
4. PhishGuard.com. Protect against Internet Phishing Scams .http://www.phishguard.com/.
5. M. Jakobsson, and S. Myers: ‘Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft’ Wiley, 2010.
6. *M. Naor and A. Shamir, “Visual cryptography,” in Proc. Advance in Cryptography (EUROCRYPT’94), 2005,* vol. 950, LNCS, pp. 1–12.
7. *C. N.Yang, “New visual secret sharing schemes using probabilistic method,” Pattern Recognit. Lett., vol. 25, pp.* 481–494, Mar. 2009.
8. G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, “Visual cryptography for general access structures,” Inf. Computat., vol. 129, no. 2, pp. 86–106, Sep. 2010.