International Journal of
Emerging Research in Management &Technology
ISSN: 2278-9359 (Volume-4, Issue-2)

Research Article | **February 2015**

Anti phishing using (t, n) Visual Cryptography Scheme For Commerce Bank

Mangala S Wale, Anita Jadhav, Bharati Kale, Ankita Gupta
Computer Department, Pune, Maharashtra,
India

Abstract—

In today's information driven world, online attacks are more active, and one of them is phishing. In phishing attack phishers attempt to fraudulently acquire sensitive information like users id, password, contact details, credit card information etc. by masquerading as a trustworthy person or business in an electronic communications. To solve the problem of phishing we have proposing new technology named as "Anti phishing Using (t, n) Visual Cryptography Scheme (VCS)". This paper proposes (t, n) visual cryptography scheme for Commerce Bank, where image CAPTCHA encoded into n number of shares and the stacking of any t out of n shares revels the secret image. The stacking of t-1 or less than t shares is not able to revels the secret image. Proposed paper also allows a (t, n) VCS with unlimited n shares and provide recovery of share when user lost his/her share where losted share will not reveal any secret image.

Keywords— Image CAPTCHA, Phishing, security, shares, Visual Cryptography Scheme (VCS).

I. INTRODUCTION

Internet has changed the life of human significantly and it has dominated many fields including e-Commerce, e-Healthcare etc. Internet increases the comfort of human life; on the other hand it also increases the need for security measures too. Still they are vulnerable to attacks such as phishing. Phishing is similar to fishing in a lake, but instead of trying to capture fish, phishers attempt to steal sensitive information like online banking password, username, Email id, credit card details from users. Where Anti phishing is a technique used to detect and prevent phishing attack. There are many tools and techniques are available for Anti phishing .There are a variety of methods that can be used to identified a web page as a phishing site ,including whitelists(lists of known safe sites),blacklists(list of known fraudulent sites),heuristics and community ratings. Blacklist is a DNS based anti-phishing approach technique now most commonly used by the browser. Anti Phishing Work Group, Google and other organizations have provided an open blacklist query interface. Internet Explorer7, Netscape Browser8.1, Google Safe Browsing (a feature of the Google Toolbar for Firefox) are important browsers which use blacklists to protect users when they are navigating through phishing sites. Heuristic-based anti-phishing technique is to estimate whether a page has some phishing heuristics characteristics. For example, some heuristics characteristics used by the Spoof Guard toolbar include checking the host name, checking the URL for common spoofing techniques, and checking against previously seen images. If you only use the Heuristic-based technique, the accuracy is not enough.

Visual cryptography (VC) is the simplest and a perfect way to provide the security to the confidential information. Visual Cryptography (VC) for black and white was first formally introduced by Naor and Shamir [1]. In which one secret binary image is cryptographically encoded into n shares of random binary patterns. The n shares are distributed amongst group of n participants, one for each participant. No participants can retrieve any information from his own transparency, but any k or more participants can visually reveal the secret image by polling there transparencies together. The secret cannot be decoded by any k – 1 or less participants, even if higher computational power is available to them. In VC the decryption process requires only human visual system. This property makes visual cryptography especially useful for the low computation load requirement.

In the Existing System, as shown in the Figure 1, when the end user wants to access his confidential information online (in the form of money transfer or payment gateway) by logging into his bank account or secure mail account, the person enters information like username, password, credit card no. etc. on the login page. But quite often, this information can be captured by attackers using phishing techniques (for instance, a phishing website can collect the login information the user enters and redirect him to the original site). There is no such information that cannot be directly obtained from the user at the time of his login input[6].

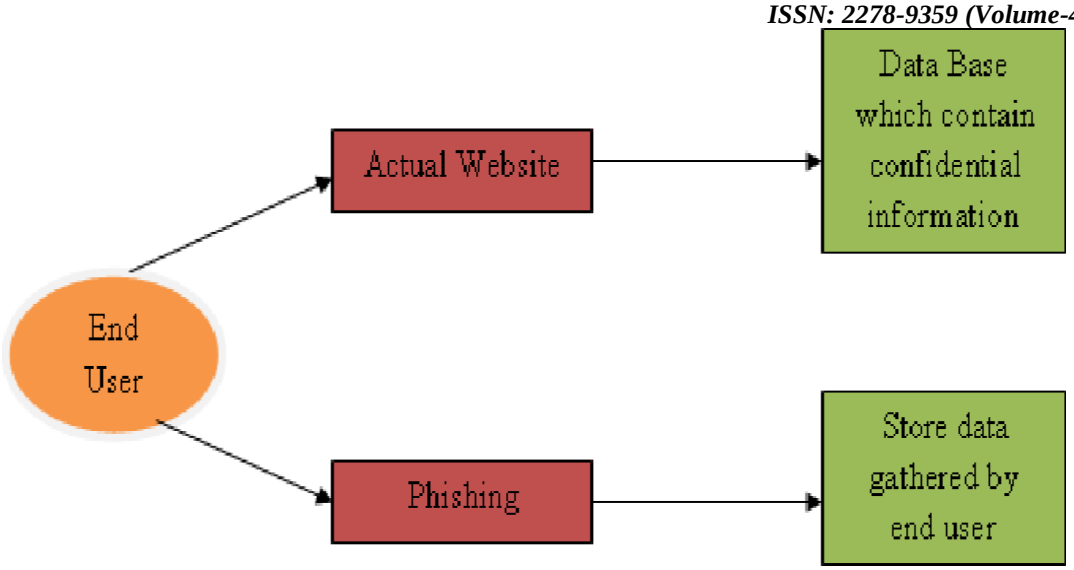


Fig 1: Existing System

Disadvantages of Existing System:

By doing a detailed study about the existing system to avoid phishing attack and the related work that has been done in order to overcome the problem of phishing we have observed the following disadvantages.

1. In the existing system security level leans.
2. It produces security which can be violated by the intruder by various attacks.
3. Complexity in maintaining the tables for user ids and respective passwords.
4. It may undergo the online attacks like phishing by an intruder.
5. Not only leading to online attacks, there might be a chance of misleading the user with false authentication by phishing websites
6. If the confidential information about the user is attacked and known by the intruder it results in lots of loss to the user both financially and personally too.

II. LITERATURE SURVEY

Researchers propose user-based mechanisms to authenticate the server. Auto-mated Challenge Response Method [1] is one such authentication mechanisms, includes challenge generation module from server which in turn interacts with Challenge-Response interface in client and request for response from user. Challenge-Response module in turn will call the get response application which is installed in the client machine. Once the challenge-response is validated user credentials are demanded from client and it is validated by server to proceed the transaction. Automated Challenge-Response Method ensures two way authentication and simplicity. The proposed method also prevents man-in-the middle attacks since the response is obtained from the executable which is called by the browser and third man interruption is impossible. Here instead of getting response from get-response executable it is better to update the get-response executable automatically from bank server when the responses are about to nullify. It gives the concept of Anti phishing technique using various methods. Phishing is a combination of social engineering and technical deception to steal consumers personal identity data and financial account credentials. Even though there are numerous methods reported to avoid Phishing each method has its own limitations. This paper addresses one of the limitations in Transaction Authentication Number method.

Now there are DNS-based anti-phishing approach [2] technique which mainly includes blacklists, heuristic detection, the page similarity assessment. But they do have some shortcomings Blacklist is a DNS based anti-phishing approach technique now most commonly used by the browser. Anti Phishing Work Group, Google and other organizations have provided an open blacklist query interface. Internet Ex-plorer7, Netscape Browser8.1, Google Safe Browsing (a feature of the Google Toolbar for Firefox) are important browsers which use blacklists to protect users when they are navigating through phishing sites. Because every URL in the blacklist has been verified by the administrator, the false alarm probability is very low. However, there are a lot of technical disadvantages. Firstly, the phishing websites we found is a very small proportion, so the failed alarm probability is very high. Secondly, generally to say, the life cycle of a phishing website is only a few days. A website might be shutdown before we found and verified it is a phishing website. Heuristic-based anti-phishing technique is to estimate whether a page has some phishing heuristics characteristics. For example, some heuristics characteristics used by the SpoofGuard [3] toolbar include checking the host name, checking the URL for common spoofing techniques, and checking against previously seen images. If you only use the Heuristic-based technique, the accuracy is not enough. Besides, phishers can use some strategies to avoid such detection rules. The user may be deceived by the phishing website because the phishing website imitates a legitimate website. Its pages are often similar with the legitimate sites. Therefore, some researchers proposed a similarity assessment method to detect

phishing sites. For example, CANTINA [4] is a content similarity based approach to detect phishing websites. First, it calculates the suspicious pages lexical signature using TF-IDF and then feed this lexical signature to a search engine. According to the suspicious pages sort order in the search results we can determine whether it is a phishing site.
Liu Wenyin [5] proposed a page visual similarity assessment method to detect phishing websites, if a web pageis similar to a financial organizations page, but it is not the organizations web page itself, it is considered a phishing sites page. The following technologies used, but they have several drawbacks:
1. Blacklist-based technique with low false alarm probability, but it cannot detect the websites that are not in the blacklist database. Because the life cycle of phishing websites is too short and the establishment of blacklist has a long lag time, the accuracy of the blacklist is not too high.
2. Heuristic-based anti-phishing technique, with a high probability of false and failed alarm, and it is easy for the attacker to use technical means to avoid the heuristic characteristics detection.
3. Similarity assessment based technique is time-consuming. It needs too long time to calculate a pair of pages, so using the method to detect phishing websites on the client terminal is not suitable. And there is low accuracy rate for this method depends on many factors, such as the text, images, and similarity measurement technique. However, this technique (in particular, image similarity identification technique) is not perfect enough yet.

A Novel Anti Phishing Framework Based on Visual Cryptography, 2012, Divya James, Mintu Philip. 2012 [6] Here an image based authentication using Visual Cryptography (vc) is used. The use of visual cryptography is explored to preserve the privacy of image CAPTCHA by decomposing the original image CAPTCHA into two shares that are stored in separate database servers such that the original image CAPTCHA can be revealed only when both are simultaneously available.

Naor and Shamir [7] introduced the visual cryptography scheme (VCS) as a simple and secure way to allow the secret sharing of images without any cryptographic computations. A segment-based visual cryptography suggested by Borchert [8] can be used only to encrypt the messages containing symbols, especially numbers like bank account number, amount etc.A version of Visual Cryptography is presented which is not pixel-based but segment-based. It is used to encrypt messages consisting of symbols which can be represented by a segment display. For example, the decimal digits 0; : : : ; 9 can be represented by the well-known seven-segment display. The advantage of the
segment-based encryption is that it may be easier to adjust the secret images and that the symbols are potentially easier to recognize for the human eye, especially in a transparency-on-screen szenario. The VCS proposed by Wei-Qi Yan et al., [9] can be applied only for printed text or image.The shares of VC printed on transparencies are very difficult to be overlapped with proper alignment even if we ignore the printing errors. A wide variety of applications of visual cryptography would require the printing of the shares on paper like that of documents, checks, tickets or cards.In such cases, scanning of the printed shares is inevitable for restoring the secret. The scanned shares (with printing, handling and scanning errors) have to be superimposed in order to reconstruct the secret image which could be some photo, code or other such important information.

A Text-Graphics Character CAPTCHA for Password Authentication Matthew Dailey Chanathip Namprempre [10] preventing dictionary attacks against password authenticated systems allowing remote access via dumb terminals. Password authentication is commonly used for computer access control. But password authenticated systems are prone to dictionary attacks, in which attackers repeatedly attempt to gain access using the entries in a list of frequently-used passwords. CAPTCHA is (Completely Automated Public Turing tests to tell Computers and Humans Apart) recurrently being used to prevent automated bots from registering for email accounts. They have also been suggested as a means for preventing dictionary attacks. However, current CAPTCHAs are unsuitable for text-based remote access and TGC CAPTCHA fills this gap. In this paper, they define the TGC CAPTCHA, secure CAPTCHA demonstrate its utility in a prototype based on the SSH (Secure Shell) protocol suite, and provide empirical evidence that the test is easy for humans and hard for machines.

New visual secret sharing schemes using probabilistic method, Chung Yang [11] In this paper, they use the frequency of white pixels to show the contrast of the recovered image i.e the frequency of white pixels to let human visual system distinguish between black and white. The scheme have non-expansible shadow size and the same contrast level of the conventional VSS scheme. The term non-expansible means that the sizes of the original image and shadows are the same.we have presented new k; n ProbVSS schemes with non-expansible shadow size based on the probabilistic method.

Yang[11] proposed a probabilistic model of (t, n) VC scheme, and the two cases (2, n) and (n, n) are explicitly constructed to achieve the optimal contrast and also proposed a generalized VC scheme in which the pixel expansion is between the probabilisticmodel of VC scheme and the traditional VC scheme. Sian-Jheng Lin and Wei-Ho Chung A Probabilistic Model of (t, n) Visual Cryptography Scheme With Dynamic Group, 2012 [12] proposed scheme Specifically, an extended VC scheme based on basis matrices and a probabilistic model is proposed. An equation is derived from the fundamental definitions of the (t, n) VC scheme and then the (t, ∞) VC scheme achieving maximal contrast can be designed by using the derived equation.

III. SYSTEM ARCHITECTURE

The system architecture as shown in Fig. 2 where the user register his information in registration module. After the registration, user login to the system to upload the users share and stacking with servers share to identify the original website or phished website by using image CAPTCHA.

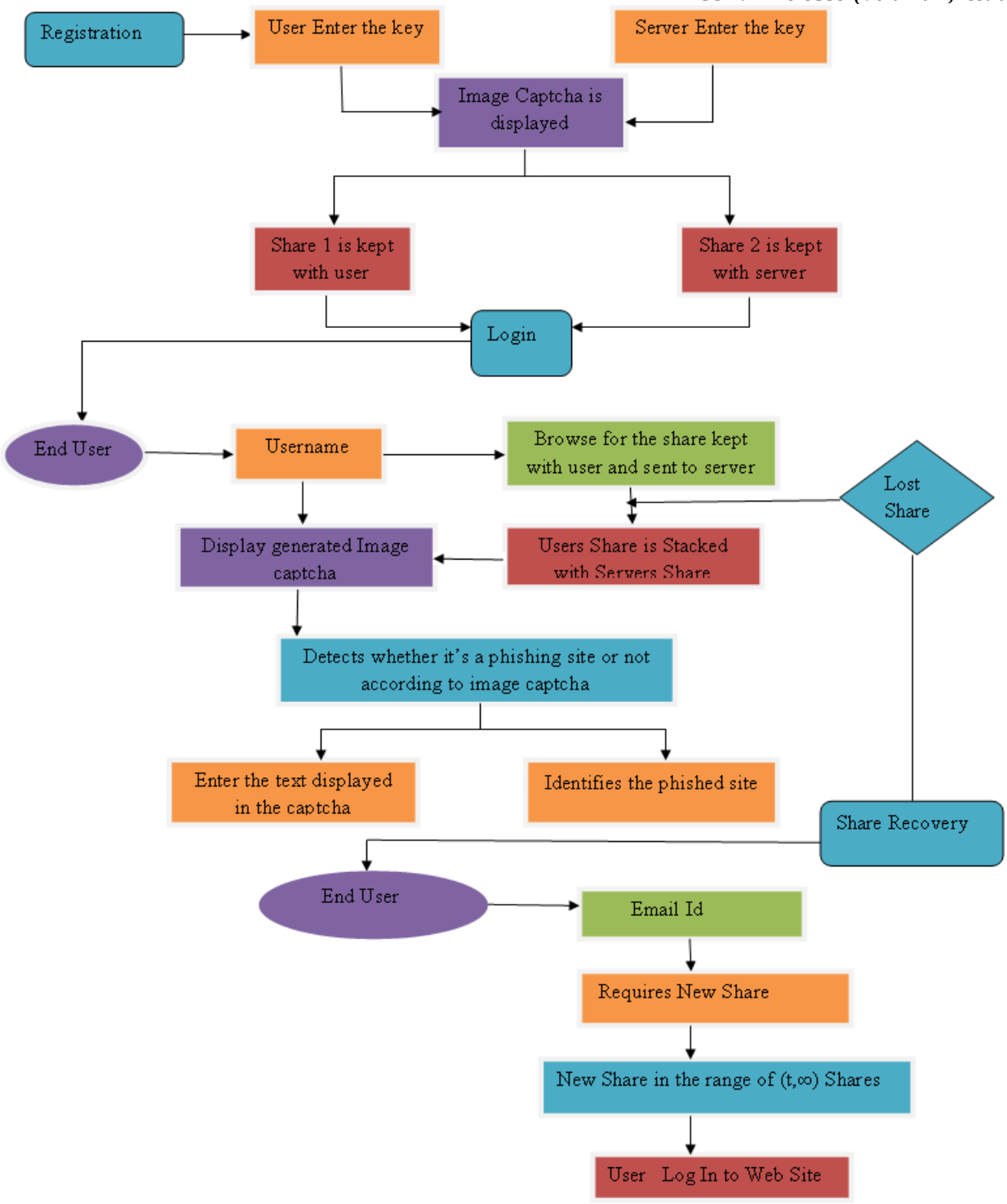


Fig 2.System architecture

IV. PROPOSED SYSTEM

For phishing detection and prevention, we are proposing a new project to detect the phishing website. Our methodology is based on the Anti-Phishing Image CAPTCHA validation scheme using visual cryptography [6]. It prevents password and other confidential information from the phishing websites.

The current project can be divided into three phases:

1. Registration phase
2. Login phase
3. Share recovery phase

A. Registration phase

The authentication technique consists of 3 phases registration phase, login phase and Share recovery phase. In the registration phase, a key string (password) is asked from the user at the time of registration for the secure website. The key string can be a combination of alphabets and numbers to provide a more secure environment. This string is

concatenated with randomly generated string in the server and an image CAPTCHA[19] is generated. The image CAPTCHA is divided into two shares such that one of the shares is kept by the user and the other share is kept in the server. The users share and the original image CAPTCHA are sent to the user for later verification during the login phase. The image CAPTCHA is also stored in the actual database of any confidential website as confidential data. After the registration, the user can change the key string when it is needed. The registration process is depicted in Fig.3.

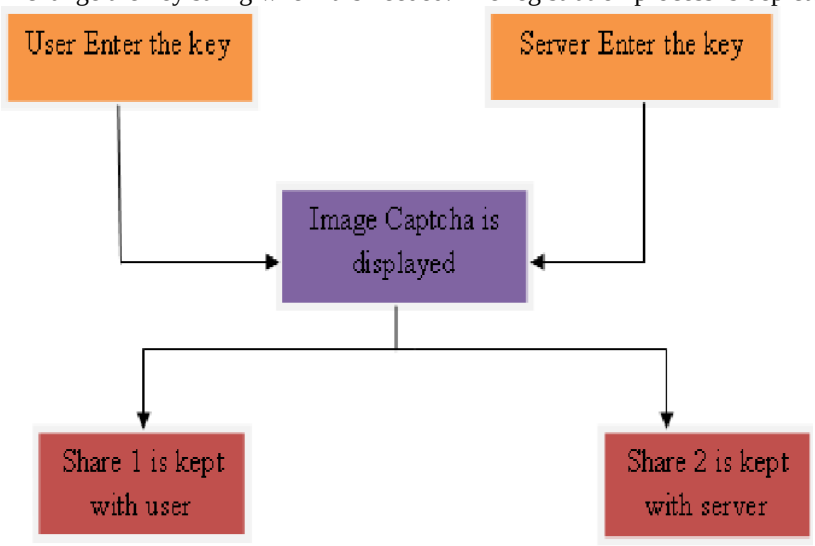


Fig.3: Registration phase

B. Login phase

In the Login phase first the user is prompted for the Email-id. Then the user is asked to enter his share which is kept with him. This share is sent to the server where the users share and share which is stored in the database of the website, for each user, is stacked together to produce the image CAPTCHA. The image CAPTCHA is displayed to the user. Here the end user can check whether the displayed image CAPTCHA [10] matches with the CAPTCHA created at the time of registration. The end user is required to enter the text displayed in the image CAPTCHA. Using the image CAPTCHA generated by stacking two shares one can verify whether the website is genuine or secure web site or a phishing website and can also verify whether the user is a human user or not. Fig 4 can be used to illustrate the login phase.

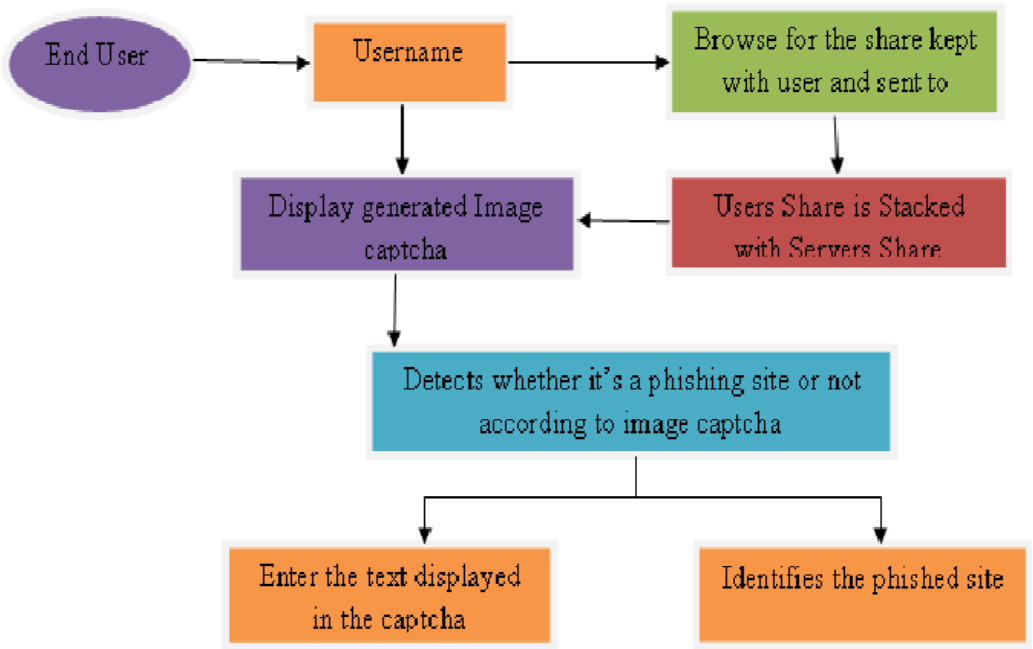


Fig 4: Login phase

C. Share recovery phase

The share recovery phase is used when user lost or corrupts his share. In the registration Phase when the User enters username and try upload his share from the server. If user lost or corrupt his/her share then he request for new share at that time server crosscheck whether the user is authorized or not. The server uses next share algorithm (t, ∞) for generating new share, which is compatible with users share [12].The server generates a new share for the user. Users download new share and process continue with login page is as shown in Fig.5.

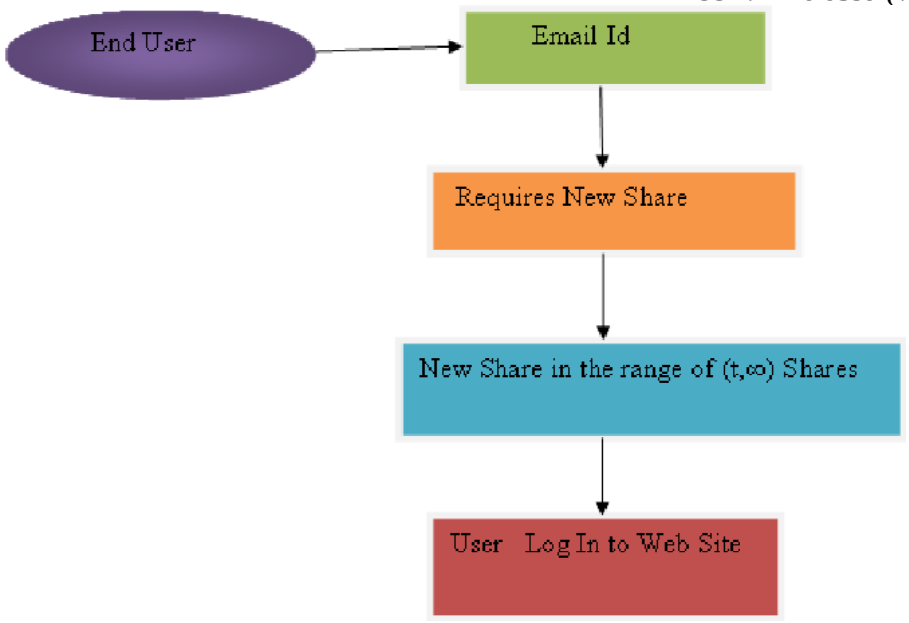
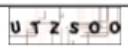
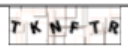
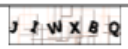


Fig 5: Share recovery phase

V. RESULT AND ANALYSIS

Table 1: Creation and stacking of shares

Case No	Original CAPTCHA	Index table	Server share	Users share	Decrypted CAPTCHA	Total time (in msec.)
1						31
2						47
3						31
4						62
5						47

In the registration phase the most important part is the creation of shares from the image CAPTCHA where one share is kept with the user and other share can be kept with the server. For login, the user needs to enter a valid username in the given field. Then he has to browse his share and process. At the server side the user's share is combined with the share in the server and an image CAPTCHA is generated .The user has to enter the text from the image CAPTCHA and password in the required field in order to login into the website. The entire process is depicted in Table 1 as different Cases. From Case No 1 to 5 illustrates the creation and stacking of shares of two image CAPTCHA's resulting in original CAPTCHA.

VI. CONCLUSION AND FUTURE ENHANCEMENT

Currently phishing attacks are so common because it can attack globally and capture and store the user's confidential information. The project verifies whether the website is a secure website or a phishing website. If website is phishing then it can't display the image CAPTCHA for that specific user. It validates image CAPTCHA and ensure that the site as well as the user is permitted one or not. Table 1 shows different cases for creation and stacking of shares, From Case No 1 to 5 illustrates the creation and stacking of shares of two image CAPTCHA's resulting in original CAPTCHA. So, using image CAPTCHA technique, no machine based user can crack the password or other confidential information of the users. It also prevents intruder's attacks on the users account. This method provides additional security in terms of not letting the intruder log in into the account even when the user knows the user name of a particular user. It is useful to prevent the attacks of phishing websites on financial web portal, banking portal, online shopping market. The project is used for creating new share when user lost his share and is also useful to prevent the attacks of phishing websites on financial web portal, banking portal, online shopping market. We implemented a new (t, ∞) Visual Cryptography algorithm. The algorithm is useful in the sense that if you need one more share, you will get it, no need to perform entire visual cryptography and generation of all shares. Also, execution of algorithm does not need high configuration resources, and it can be easily run with good performance on lower configuration infrastructure.

FUTUTRE ENHANCEMENT

The future work to be carried in the area of improving the quality of resultant image generated after stacking. As work proposed in the current paper, involves black & white shares and image after stacking, in future it can be implemented in RGB color space.

REFERENCES

[1] Thiyagarajan, P. Venkatesan, V.P. Aghila, G. , "Anti-Phishing Technique using Automated Challenge Response Method"', in Proceedings of IEEE- International Conference on Communications and Computational Intelligience, 2010.

[2] Sun Bin, Wen Qiaoyan, Liang Xiaoying, "A DNS based Anti- Phishing Approach", in Proceedings of IEEE-Second International Conference on Networks Security, Wireless Communications and Trusted Computing, 2010.

[3] Nourian, A. Ishtiaq, S. Maheswaran, "CASTLE: A social framework for collaborative antiphishing databases", in Proceedings of IEEE- 5th International Conference on Collaborative Computing:Networking, Applications and Worksharing, 2009.

[4] Sid Stamm, Zulfikar Ramzan, 'Drive-By Pharming", v4861 LNCS,p495-506,2007, Information and Communications Security - 9th International Conference,ICICS 2007, Proceedings.

[5] Anthony Y. Fu, Liu Wenyin,"Detecting Phishing Web Pages with Visual Similarity Assessment Based on Earth Movers Distance (EMD)", October/December 2006.

[6] Divya James, Mintu Philip,"A Novel Anti Phishing Framework Based on Visual Cryptography" 2012.

[7] M. Naor and A. Shamir, V.Venkateswara Reddy , "Visual cryptography", 1995, vol. 950, LNCS, pp. 112.

[8] B. Borchert, "Segment Based Visual Cryptography" WSI Press, Germany, 2007.

[9] W-Q Yan, D. Jin and M. S. Kanakanahalli, "Visual Cryptography for Print and Scan Applications" IEEE Transactions, ISCAS-2004, pp. 572-575.

[10] Matthew Dailey Chanathip Namprempre, "A Text-Graphics Character CAPTCHA for Password Authentication"

[11] C. N. Yang, "New visual secret sharing schemes using probabilistic method", Pattern Recognit. Lett., vol. 25, no. 4, pp. 481494, Mar 2004.

[12] Sian-Jheng Lin and Wei-Ho Chung,"A Probabilistic Model of (t,n) Visual Cryptography Scheme With Dynamic Group", 2012.

