International Journal of Emerging Technology and Innovative Engineering
IJETIE Volume 1, Issue 11, November 2015 (ISSN: 2394 – 6598)

SECURED INTERNET BANKING USING IMAGE CAPTCHA TECHNIQUE

S. PRIYA[1], M. Malathi[2], G. Jayaseelan[3],
[1]Research Scholar, Bharat University, Chennai
[2]Research Scholar, Annamalai University, Chidambaram
[3]Department of Electronics and Communication Engineering,BCET, Karaikal

ABSTRACT:-Phishing is an attack meant by acquiring user's confidential information from the web. In today's technology the e-commerce, net banking are becoming so common such that identity theft also increasing. To overcome this, Anti-Phishing framework be exposed to avoid such attacks with the help of Visual Cryptographic Scheme. Visual Cryptography is a special encryption technique to hide information in images in such a way that it can be decrypted by the human vision if the correct key image is used. To solve authenticity problem this paper proposes a CAPTCHA based Visual Cryptography scheme to address the authentication issues. A modified multi secret sharing visual cryptographic technique for hiding information in the colored image and respective share be represented as captcha to the user. The secret is processed with image and shares be separated according to the visual cryptographic scheme. Only when the user's share perfectly matches with the original website's share, the hidden information is revealed by the user thus avoids identity theft by the phishers.

Keywords: Phishing, Visual Cryptography, Wiener Filter, Captcha

1.INTRODUCTION

Authenticity of the user is the major issue in today's internet applications such as core banking. Password has been the most used authentication mechanism which is subjected to offline and online dictionary attacks. As technology progresses and as more and more personal data is digitalized, there is more of an emphasis required on data security today than there has ever been. Today hacking of the databases on the internet is unavoidable. If Cryptography is used for secure communications, the sender will distribute one or more random layers in advance to the receiver. Visual cryptography is based on cryptography where n images are encoded in a way that only the human visual system can decrypt the hidden message without any cryptographic computations when all

shares are stacked together. Visual cryptographic technique was proposed by Naor and Shamir. Visual Cryptography technique uses two transparent images. One image contains random pixels and the other image contains the secret information. It is impossible to retrieve the secret information from one of the images. When the random image contains truly random pixels it can be seen as a one-time pad system and will offer unbreakable encryption.

If the sender has a message, he creates a layer 2 for a particular distributed layer 1 and sends it to the receiver. The receiver aligns the two layers and the secret information is revealed, this without the need for an encryption device, a computer or performing calculations by hand. The system is unbreakable, as long as both layers don't fall in the wrong hands. When one of both layers is intercepted it's impossible to retrieve the encrypted information.

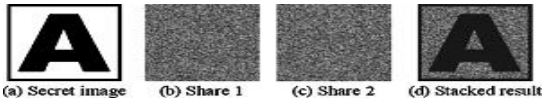


Fig 1 Visual Cryptography of an Image

The Embedded EVCS is constructed by adding random shares of secret image into meaningful covering images. The system will work with color images. With rapid progress in Internet and digital imaging technology, there are more and more ways to easily create, publish, and distribute images. Several secret sharing schemes are said to be information theoretically secure and can be proven to be so, while others give up this unconditional security for improved efficiency while maintaining enough security to be considered as secure as other common cryptographic primitives.

Internet banking portal provides personal banking services that gives you complete control over all your banking demands online. Corporate internet Banking application also provides features to administer and manage non personal accounts online. It is a convenient way to do banking from the comfort of your home or office. Avoid the queue or delays and try our simple and secure Internet Banking facility for an unmatched online banking experience. Online banking is an electronic payment system that enables customers, a financial institution to conduct financial transactions on a website operated by the institution, such as a retail bank, virtual bank, credit union or building society. Online banking is also referred as Internet banking, e-banking, virtual banking and by other terms.To access online banking, a customer would go to the financial institution's secured website, and enter the online banking facility using the customer number and password previously setup. Some financial institutions have set up additional security steps for access to online banking, but there is no consistency to the approach adopted.

Multiple secret sharing has the main advantage of being able to hide more than one secret within a set of shares. This increases the capacity of secret sharing and in some case, the size of the shares remains relatively optimal in terms of data storage and dimensions. This methodology generates a unique CAPTCHA image for users which in turn is divided into two shares. One share is stored in the bank database and the other share is provided to the

customer. Hash code is generated for the customer share and it is stored in the bank database. The customer has to present the share during all of his/her transactions. When the customer presents his share the hash code is generated and compared with the database value. If it matches the shares are stacked to get the original CAPTCHA image which authenticates the user. CAPTCHA images of text should be distorted randomly before being presented to the user. Many implementations of CAPTCHAs use undistorted text, or text with only minor distortions. These implementations are vulnerable to simple automated attacks. Applications of visual cryptographic techniques are Human machine identification by visual cryptography, Visual cryptographic authentication of data matrix, Offline QR code authentication, captcha generation, Multimodal based security authentication, E commerce and Net banking.

2. WIENER FILTER

In signal processing, the **Wiener filter** is a filter used to produce an estimate of a desired or target random process by linear time-invariant filtering of an observed noisy process, assuming known stationary signal and noise spectra, and additive noise. The Wiener filter minimizes the mean square error between the estimated random process and the desired process. The Wiener filter can be used to filter out the noise from the corrupted signal to provide an estimate of the underlying signal of interest.

The Wiener filter is based on a statistical approach and has the following characteristics: Assumption: signal and (additive) noise are stationary linear stochastic processes with known spectral characteristics or known autocorrelation and correlation. Requirement: the filter must be physically realizable/causal (this requirement can be dropped, resulting in a non-causal solution).Performance criterion: minimum mean-square error (MMSE).The Wiener filter problem has solutions for three possible cases: one where a non causal filter is acceptable (requiring an infinite amount of both past and future data), the case where a causal filter is desired (using an infinite amount of past data), and the finite impulse response (FIR) case where a finite amount of past data is used.

3. PHISHING

Phishing is an act of attempt to acquire information such as usernames, passwords, and bank details by masquerading as a trustworthy entity in an electronic communication. A phishing website or message tries to trick the user into revealing personal information by appearing to be from a legitimate source, such as a bank, social network, or even Google. Cyber criminals can use links in emails, tweets, posts and online advertisements to direct you to fake sign-in screens, where they can steal your password .It is becoming increasingly common to tune in to the news or load your favorite news Website and read about yet another Internet e-mail scam. An e-mail scam is a fraudulent e-mail that appears to be from a legitimate Internet address with a justifiable request - usually to verify your personal information or account details. One example would be if you received an e-mail that appears to be from your bank requesting you click a hyperlink in the e-mail and verify your online banking information. Usually there will be a repercussion stated in the e-mail for not following the link, such as "your account will be closed or suspended". The goal of the sender is for you to disclose personal and (or) account related information.

Phishing email will direct the user to visit a website where they are asked to update personal information, such as a password, credit card, social security, or bank account numbers, that the legitimate organization already has. The website however, is bogus and set up only to steal the information the user enters on the page. Spear phishing scams will often appear to be from a company's own human resources or technical support divisions and may ask employees to update their username and passwords. Once hackers get this data they can gain entry into secured networks.

4. ANTI-PHISHING:

Mainly to overcome phishing attacks anti-phishing framework is designed. It is a technological framework that helps prevent unauthorized access to secure and/or sensitive information. Anti-phishing services protect various types of data in diverse ways across a variety of platforms. Anti-phishing service addresses a specific type of attempt to obtain personal or other sensitive information. While anti-phishing services provide tools to help users recognize Web phishing, many anti-phishing service features are responses to efforts to hack a system and steal data. Some anti-phishing tools are available via browsers, through which many phishing attempts occur.

If you supply sensitive information on a website, always ensure that the site is secure. The address of the page should start with "https://" not just "http://" and the Lock icon should be displayed in the browser's status bar. If these indicators are not present, it means that the site is not secure and information you enter on the site is not protected. Fraudulent web forms related to phishing scams are often non-secure sites. Please note, however, that even an apparently secure site may be fraudulent. The fact that a site appears to be secure is not by itself a guarantee that the site is legitimate. However, legitimate sites that require users to supply personal information will always be secure.

5. IDENTIFYING LEGITIMATE WEBSITES

Most websites targeted for phishing are secure websites meaning that SSL with Strong PKI cryptography is used for server authentication, where the website URL is used as identifier. In theory it should be possible for the SSL authentication to be used to confirm the site to the user, and this was SSL design requirement and the Meta of secure browsing. But in practice, this is easy to trick. The superficial flaw is that the browser security user interface (UI) is insufficient to deal with today's strong threats. There are three parts to secure authentication using TLS and certificates: indicating that the connection is in authenticated mode, indicating which site the user is connected to, and indicating which authority says it is this site. All three are necessary for authentication, and need to be confirmed by/to the user.

6. ALGORITHM

The algorithm for binary image (black and white) captcha visual cryptography that creates 2 encrypted images from an original unencrypted image is as follows: First create an image of random pixels the same size and shape as the original image. Next, create a second image the same size and shape as the first, but where a pixel of the original image is the same as the corresponding pixel in the first encrypted image, set the same pixel of the second encrypted image to the opposite color. When a pixel of the original image is different than the corresponding pixel in the first encrypted image, set the same pixel of the second encrypted image to the same color as the corresponding pixel of the first encrypted image. The two apparently random images can now be combined using an exclusive-or (XOR) to re-create the original image.

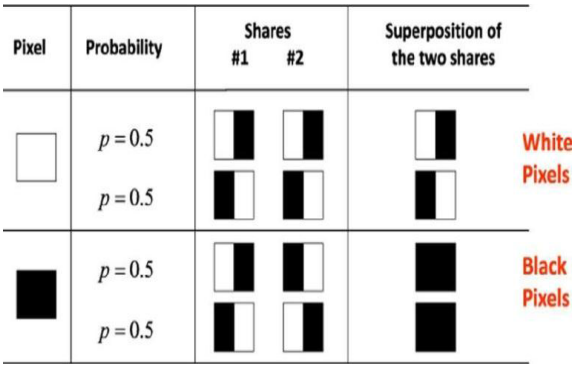


Fig 2 Pixel Expansion Techniques

A pixel is generally thought of as the smallest single component of a digital image. However, the definition is highly context-sensitive. Here the shares are separated with respective pixel expansion. The three phases are involved in the authentication protocol such as Registration, login and Recovery phase

7. REGISTRATION PHASE

In the registration phase, user must provide their personal information with unique phone number. This personal information is stored into the database with the encrypted format and that used for further process. Providing user information user can be register for the application. 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 more secure environment. This one time password are created by using hash algorithm and stored in encrypted format. This string is concatenated with randomly generated string in the server and an image captcha is generated. The image captcha is divided into two shares such that one of the shares is kept with the user and the other share is kept in the server. The user's share and the original image captcha are sent to the user for later verification during 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.

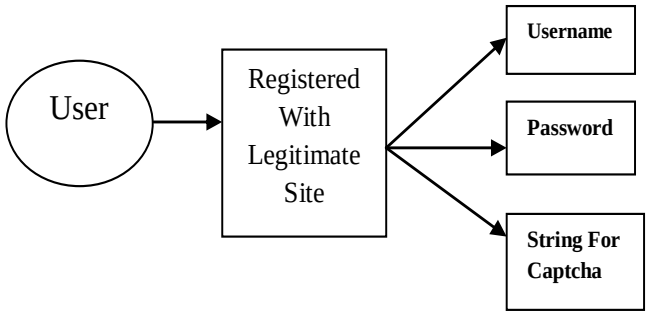


Fig: 3 Registration and Login Phase

LOGIN PHASE: When the user logs in by entering his confidential information for using his account, then first the user is asked to enter his username (user id). Then the user is asked to enter his share which is kept with him. This share is sent to the server where the user's 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 matches with the captcha created at the time of registration.

8. RECOVERY PHASE

In the recovery phase, if user lost his secret share then the protocol is able to recover the user setting for the new captcha. The user needs to provide all the relevant details as a proof that he is the legitimate user access to that particular account.

9. IDENTIFYING THE AUTHORITY

The browser needs to state that the authority is that makes the claim of who the user is connected to. At the simplest level, no authority is stated, and therefore the browser is the authority, as far as the user is concerned. The browser vendors take on this responsibility by controlling a root list of acceptable CAs. This is the current standard practice. The problem with this is that not all certification authorities (CAs) employ equally well or the applicable checking, regardless of attempts by browser vendors to control the quality. Nor do all CAs subscribe to the same model and concept that certificates are only about authenticating ecommerce organizations.

Certificate Manufacturing is the name given to low-value certificates that are delivered on a credit card and an email confirmation; both of these are easily perverted by fraudsters. Hence, a high-value site may be easily spoofed by a valid certificate provided by another CA. This could be because the CA is in another part of the world, and is unfamiliar with high-value ecommerce sites, or it could be that no care is taken at all. As the CA is only charged with protecting its own customers, and not the customers of other CAs, this flaw is inherent in the model. The solution to this is that the browser should show, and the user should be Familiar with, the name of the authority. This presents the CA as a brand, and allows the user to learn the handful of CAs that she is likely to come into contact within her country and her sector. The use of brand is also critical to providing the CA with an incentive to improve their checking, as the user will learn the brand and demand good checking for high-value sites certificates. In that display, the issuing CA is displayed. This was an isolated case, however. There is resistance to CAs being branded on the chrome, resulting in a fallback to the simplest level above; the browser is the user's authority.

10. SYSTEM ARCHITECTURE

In this section we will discuss about the system architecture and implementation which will prevent user sensitive information from phishing attacking websites. Our system architecture is based on the Anti-Phishing image captcha validation scheme using visual cryptography. This technique will prevent our sensitive information from the phishing attack. We are dividing our system implementation into two parts.

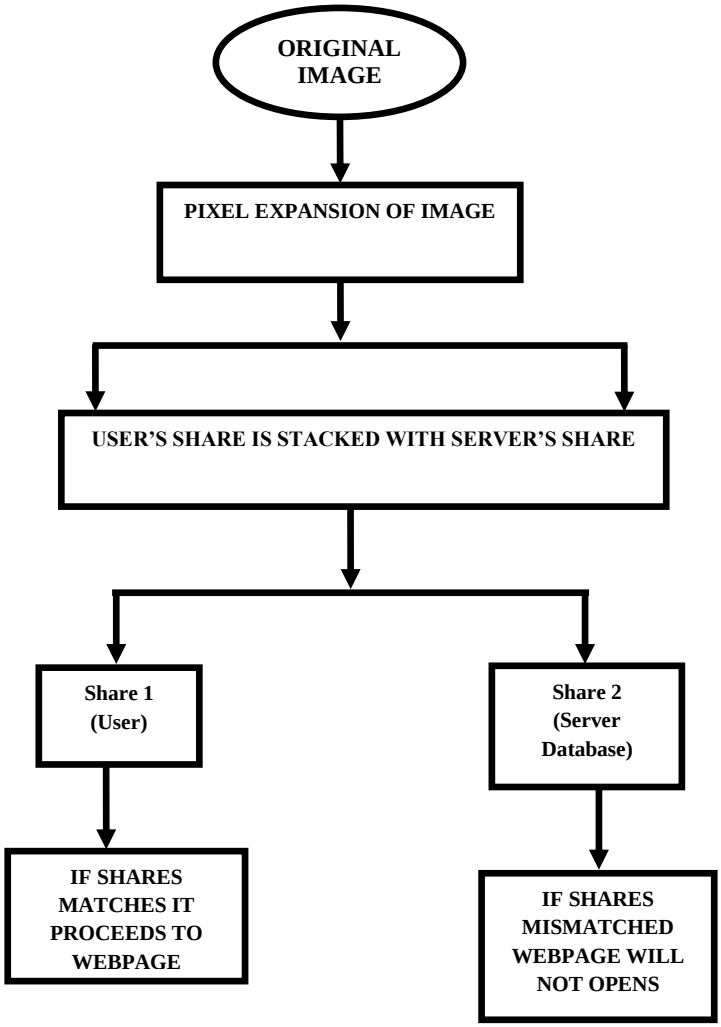


Fig 4: System Architecture

11.IMAGE DEMODULATION

This part is generally implemented at the time of registration of signup process of a site. Here an image which is chosen by a user is uploaded to our anti-phishing mechanism. This image is demodulated using visual cryptography by the method of multi secret sharing scheme. Image is demodulated in such a way that when these two demodulated shares are capable of re-construct the original image. In two demonstrated shares one is stored at the server and one is sent to the user. The original image is also stored at the server side for further verification process.

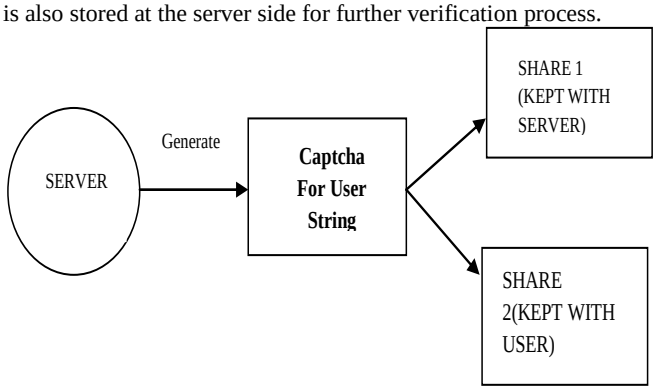


Fig:5 Image Demodulation

12. IMAGE RECONSTRUCTION PHASE

In this part we reconstruct the original image from demodulated shares which are stored at user and server. Based on the user credentials, we get the server side demodulated image. After entering credential user proposed for uploading his image share which is sent him at the time of image demodulated process. By overlapping these user uploaded and server fetched shared image is generated and matched with the uploaded image at beginning then user is authenticated otherwise he is not authenticated.

13.CONCLUSION

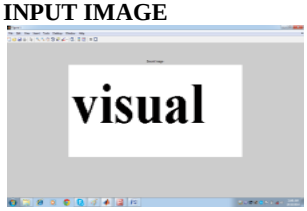
Nowadays phishing attacks are become common due to wide range of design and middle ware technologies. It is hard to detect the hackers who are targeted to user personal information like passwords and account information. In most hacking techniques, phishing is the common technique for crack the user passwords and sensitive information. It can attack globally and capture and store the user's confidential information. By using our proposed method Phishing websites as well as human users can be easily identified. The proposed methodology preserves confidential information of users using 2 layers of security. 1st we demodulate the image into two shares such that again these two shares are capable of regenerate the original image. One share send to user while other will store in the server and original image also stored in server side for further verification process. Second, image re construction. In this we will reconstruct the original image with user share and server share and we compare reconstructed image and original image for fishing detection. If in the case of original image and re constructed images are not matched then site is not authenticated. So, using our proposed method, no machine based user can crack the passwords or other confidential information of the users. This method provides additional security in terms of not letting the intruder log in into the account even when the user knows the username of a particular user.

The proposed methodology is also useful to prevent the attacks of phishing websites on financial web portal, banking portal, online shopping market. This application is just a small step towards tackling the phishing menace an a lot more needs to be done. Some of the features that may be added to this application in order to make it more useful are: The present application is a single user application. Making it a multi user application will enhance its utility. Integrating the application with web browsers will make it more useful. Anti Phishing Working Group (APWG), a pioneer institution formed with the aim to tackle the phishing problem, maintains a black list of sites which are reported upon and confirmed to be phishing sites. Integrating this list with the application so that a passive search of the websites being visited by the user may be carried out and a warning issued in case the site is listed in the black list.

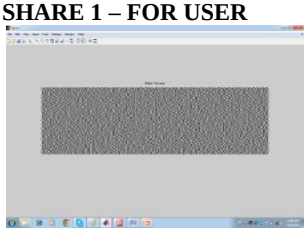
The drawback behind this technique is the contrast of the image is not so clear there may be possibility of irretrievable of information hidden in the captcha. And the pixel expansion in this technique need more space to be occupied in the database.

OUTPUTS:

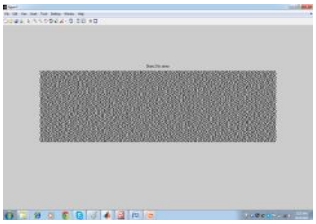
INPUT IMAGE



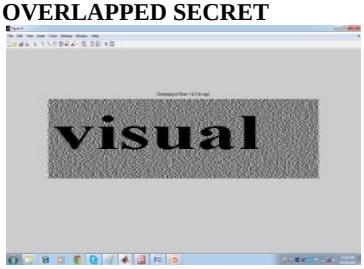
SHARE 1 – FOR USER



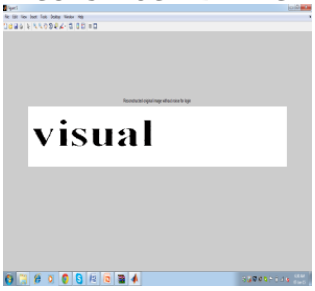
SHARE 2-FOR SERVER



OVERLAPPED SECRET



RECONSTRUCTED IMAGE

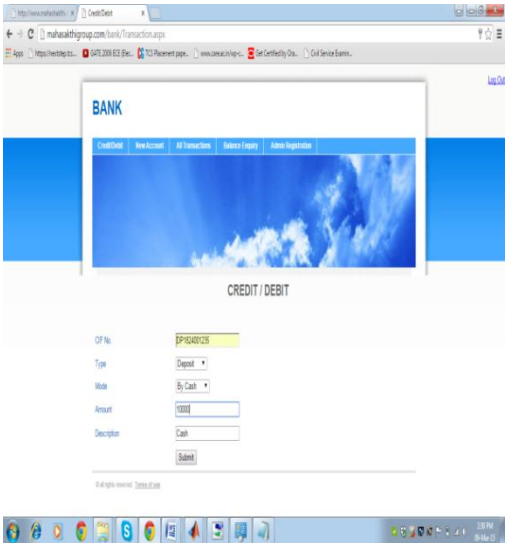


14. REFERENCE ADMIN AND USER DETAILS:

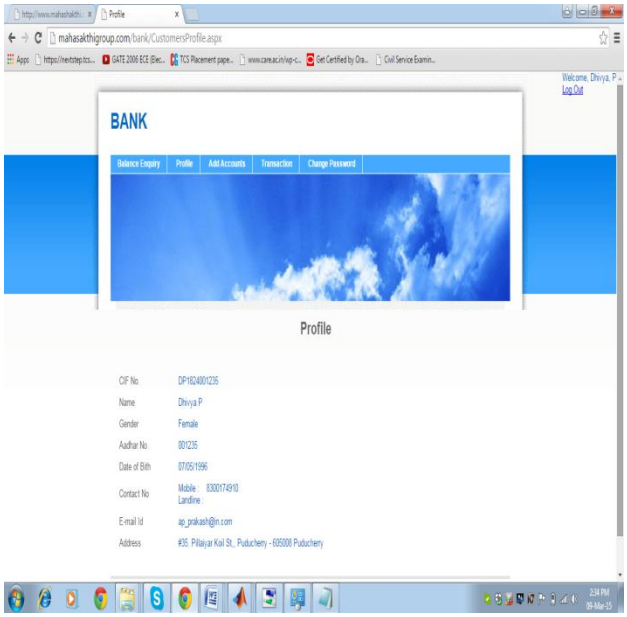
Admin Details
User Name : 9696
PWD : Raj

Customer Details	**Corresponding password**
Cif No :	
DP1824001235	**VmjFJVNQ**
FN1247:5096857415263	**g9gENdfi**
KR1122FC001234	**NULL**
PP105200001234	**XYZ**
RP1749FF001234	**L7aKq5cP**
RR01485968596	**1dWQy5mW**
RR01585968596	**NJBirCcA**
RR01685968596	**qY4xv5Sg**
RR1631:36857496	**WYap3cXH**
SB1935:019685748596	**LTt7OvvP**
SJ1054001235	**XYZ**
SS1946:159685455856	**DohtvgJB**

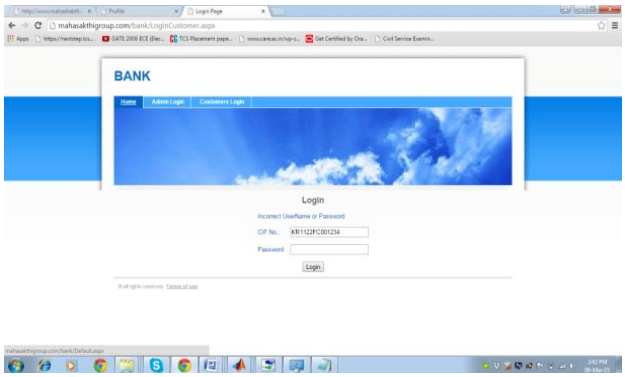
ADMINLOGIN:



CUSTOMER LOGIN:



UNAUTHORIZED LOGIN:



REFERENCES

1.Gaurav Palande , Shekhar Jadhav, Ashutosh Malwade, Vishal Divekar, Prof. S. Baj, "An Enhanced Anti-Phishing Framework Based on Visual Cryptography, International Journal of Emerging Research in Management &Technology ,march 2014

2.Mr.K.A.Aravind,Mr.R.MuthuVenkataKrishnan, Anti-Phishing Framework for Banking Based on Visual Cryptography, International Journal of Computer Science and Mobile Applications, Vol.2 Issue. 1, January- 2014

3.Y.Yesu Jyothi, D.Srinivas, K.Govindaraju, THE SECURED ANTI PHISHING APPROACH USING IMAGE BASED VALIDATION, International Journal of Research in Computer and Communication Technology, Vol 2, Issue 9, September -2013

4.Wei-Qi Yan, Duo Jin, Mohan S Kankanhalli, VISUAL CRYPTOGRAPHY FOR PRINT AND SCAN APPLICATIONS

5.Mary Ruby Star .A.L, T.Venu ,An Anti Phishing Framework For Blocking Service Attacks Using Visual Cryptography, International Journal of Computer Trends and Technology (IJCTT) – volume 4 Issue10 – Oct 2013.

6.Divya James, Mintu Philip,"A Novel Anti Phishing framework based on Visual Cryptography", in Proceedings of Power, Signals, Controls and Computation (EPSCICON), 2012

7.Kulvinder Kaur, 2013 3rd IEEE International Advance Computing Conference (IACC) "Securing Visual Cryptographic Shares using Public Key Encryption".

8.C. M. Hu and W. G. Tzeng, .Cheating Prevention in Visual Cryptography,IEEE Transaction on Image Processing, vol. 16, no. 1, Jan- 2007,pp. 36-45.

9. Horng, G, Chen, T. and Tasi, D.S. Cheating in Visual Cryptography, Designs, Codes and Cryptography, 2006, pp219–236 [1]