Anti Phishing Website Using Visual Cryptography

Manasi Ashokrao Deshmukh[1], Prof. R. W. Deshpande[2]

Department of Computer Engineering, Siddhant College of Engineering, Pune, India[1]

Department of Computer Engineering, Siddhant College of Engineering, Pune, India[2]

ABSTRACT: We are having numeral of networks and personal accounts in our day to day life, and there is some sort of easy authentication techniques is used. Now days each and every single application which uses security includes authentication process having username and password. Phishing is an effort by an personality or a group to burgle personal confidenial in turn such as passwords, credit card information etc from unsuspecting victims for identity theft, monetary gain and other fraudulent activities. In this paper we have proposed a new approach named as "A Novel Anti-phishing framework based on visual cryptography" to solve the problem of phishing. Here, an image based confirmation, by means of Visual Cryptography (VC) is worn. According to this approach, user registration contains the captcha image as password and the image is splits into two parts using K-N sharing algorithm. For the purpose of user authentication user is sent one share (part of image) and it contains the watermark text for matching purpose and other part of image is on server side. We need to secure Website Authentication process. Here is many approaches present there for cryptographic mechanism but not for website authentication. Though our system has proposed an approach provides authentication of website by using OTP on mobile number. If OTP is matched then only the bank system starts. Bank system has the functionality of Account Creation, Transaction and Report.

KEYWORDS: Steganography, AES Cryptography, watermarking, DCT, K-N Sharing

I. INTRODUCTION

In present days people used to prefer e-commerce, online booking system, online banking system etc. So there are many chances to gain the confidential information by attacker. Attacker can gain the confidential credentials with phishing technique and it is the illegal activity which can perform with different social engineering technique.

Definition of phishing [1] state that When the attacker uses someones secret in-formation for illegal purpose. Communication channels such as websites, e-mails and to and for e-commerce, online banking instant messaging service is provided by the attacker to stole the secret information of the user. In this case to avoid this type of attack service provider must provide authentication process with user name and password. Phishing [1] is an attempt by an individual or a group to thieve personal confidential information. In phishing individual or group of thieve can get credentials of user like password, credit card details from unsuspecting victims. phishing attacks can be committed through fraud emails, or spam, written to appear as if they have been sent by banks or other organizations with the intent of getting sensitive information like ATM pin, user name, accounts, passwords or credit card details. So introduces new approach named as "A Anti Phishing Framework which is based on visual Cryptography to solve phishing problems. According to this approach website proves that it is a genuine website or not by cross verifying its own identity.

Here an image based authentication using visual cryptography is used. Visual cryptography is mostly used to keep the privacy of image captcha [2][3] by creating two shares of the original image captcha which are stored in separate database servers when both image captchas are revealed then only we can get the original image; the single share of image cannot prove the identity of the original image captcha. Once the original image captcha is revealed to user it can be used as password. In this approach password image is generated for every login attempt and it will be downloaded from email which has been used for registration. Every time the image generated is unique. For security purposes every application provides user authentication. From ancient days secret data or code is used for hiding and living security to information. In user authentication the process which we have to pass through is username and password.

Authentication process divided into Token based authentication, Biometric based authentication and Knowledge based authentication. Most of the web application provides knowledge based authentication which include alphanumeric password as well as graphical password. In todays changing world when we are having number of networks and personal account some sort of easy authentication method is needed.

Phishing is an effort by an personality or a group to burgle personal con denial in turn such as passwords, credit card information etc from unsuspecting victims for identity theft, racial gain and other fraudulent activities. In this paper we have proposed a new approach named as "A Novel Anti- phishing framework based on visual cryptography" to solve the problem of phishing. Here a picture based verification using Visual Cryptography (vc) is worn. 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[2]; the individual sheet images do not reveal the identity of the original image captcha. Once the original image captcha is revealed to the user it can be used as the password. In this approach we provide image based authentication, password image is generated for every login attempt and it will be downloaded from the email which has been used for registration. Every time the image generated is unique.

II. RELATED WORK

There are various types of attacks but phishing is identified as major threat in security. So prevention mechanism will effective to stop it, which can be cover by creating Anti-phishing web interaction which avoid lack of security in this digital world. For phishing recognition and avoidance, we are proposing a novel methodology to sense the phishing website. Our methodology is based on the Anti-Phishing Image Captcha validation scheme using visual cryptography. It prevents pass-word and other confidential information from the phishing websites. The projected approach is able to be separated into two phases: 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 contains the watermark text for matching purpose. If image match is found, then next step is OTP sending on to mobile number.

Phishing is a form of online identity theft. Phishing webpages are forged web-pages created by malicious people that aim to steal sensitive information such as online banking passwords and credit card information. This system presents an approach for detecting and preventing phishing attacks on online banking portal. This proposed system is used for Banking application where information sequrity is most important thing , using this techniques like Visual Cryptography and Image based authentication one can avoid phishing attacks on websites, so the websites consists of important data related to customers can use this system for antiphishing.

III. LITERATURE SURVEY

M. Noar and A. Shamir, \Visual cryptography". EUROCRYPT, 1994.[1]

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 can be used only to en-crypt 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 scenario.

The VCS proposed by Wei-Qi Yan et al., can be applied only for printed text or image.The shares of VC printed on transparencies are very difficult to be over-lapped with proper alignment even if we ignore the printing errors. A wide variety of applications of visual.

Divya James and Mintu Philips “A Novel Anti Phishing Framework Based On Visual Cryptography”. International Conference @2012 IEEE[2]

In this paper we have proposed a new approach named as "A Novel Anti-phishing framework based on visual cryptography "to solve the problem of phishing, 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.

Vimal Kumar and Rakesh Kumar, Detection of Phishing Attack Using Visual Cryptography in Ad hoc Network". International ICCSP conference @2015 IEEE.[3]

This paper provides a novel anti-phishing approach based on visual cryptogra-phy. According to this approach a user generates two shares of an image using (2, 2) visual cryptography scheme. Client stores the first share of this image and second share is uploaded to the website at the time of user registration. After this, web-site asks for some other information like second share of the image, user name, and password. These credentials of a particular user can change once per login. During each login phase, a user verifies the legitimacy of a website by getting secret infor-mation with the help of stacking both shares. There are many existing approaches based on cryptographic technique but they all suffer from False Positive notification. However, proposed approach does not suffer from False Positive (FP) notification and outperforms all existing approachesIn the future work, proposed scheme is based on centralized approach, centralized server can be problematic when attacker will attack on the server to get the user information. So this problem can be reduced with the help of distributed sever approach.

Barnali Gupta Banik and Samir Kumar Bandyopadhyay International Conference on Intellience and Communication Networks@2015 IEEE.[4]

In this paper a new technique of Image Steganography has been proposed which is using Lorenz Chaotic Encryption to encrypt the secret message, 3 level Discrete Wavelet Transform to hide encrypted data and visual cryptography to share stego image in secret communication. In this paper a new method of steganography has been proposed which is using chaotic encryption to encrypt secret image and visual cryptography for secret sharing of stego image. In this paper author concluded that that this is an efficient way of secret sharing in Image Steganography. This method is effective where privacy and security of secret message is much important rather than the quality of retrieved secret message.

Sruthy K Joseph, Ramesh R "Random Grid based Visual Cryptography using a common share". Conference on Computing and Network Communications (CoCoNet'15), Dec. 16-19, 2015, Trivandrum, India[5]

In this paper author discusses a visual cryptography scheme using random grids, where it uses a common share to transmit n binary secrets. The binary secret image is divided into two share images (random grids) as in (2, 2) visual cryptography scheme. In this paper author used n+1 share images to transmit n secrets and the extra share is common to all n secrets. Since RG is used it creates shares without pixel expansion. This scheme can be viewed as a modified scheme of (2, 2) random grid based visual cryptography.

IV. PROPOSED SYSTEM MODEL

In this system, there are exist 2 phases:

1 USER REGISTRATION PHASE

Bank which provide online banking. In this phase user registration is done with the help of Visual Cryptography Algorithm. While registration of user with visual cryptography user is provided by the random images that server have. Among these images user select one image for visual cryptography. The selected image need to remember by the user which is needed in future. After the selection of image Visual Cryptography algorithm is applied on that image. Output of this phase will give two shares. Out of which first share goes under the process of phase two. And second share will recorded to server side with user id and original image Second the OTP will generate on user mob. For authentication on the user credential which will also help for strong security.

2 DETECTION OF PHISHING SITE

When user goes for a transaction, user need to upload the share one[1][2][4]. After uploading, server will request for private key. User need to provide private key as-signed during registration (in phase two). Now server is with share one and private key. Then server identify the user from that key. Now server stacks its share two with users share one by Visual Cryptography. A new image is formed from these two images. Server will check that image with the original one while user also checks formed image with original image selected in phase one. If formed image is identical as original picture then precede further operation and if it is not phishing is detect and user can terminates the transaction without any loss of confidentinal data.

A. *The system will execute using below procedure:*

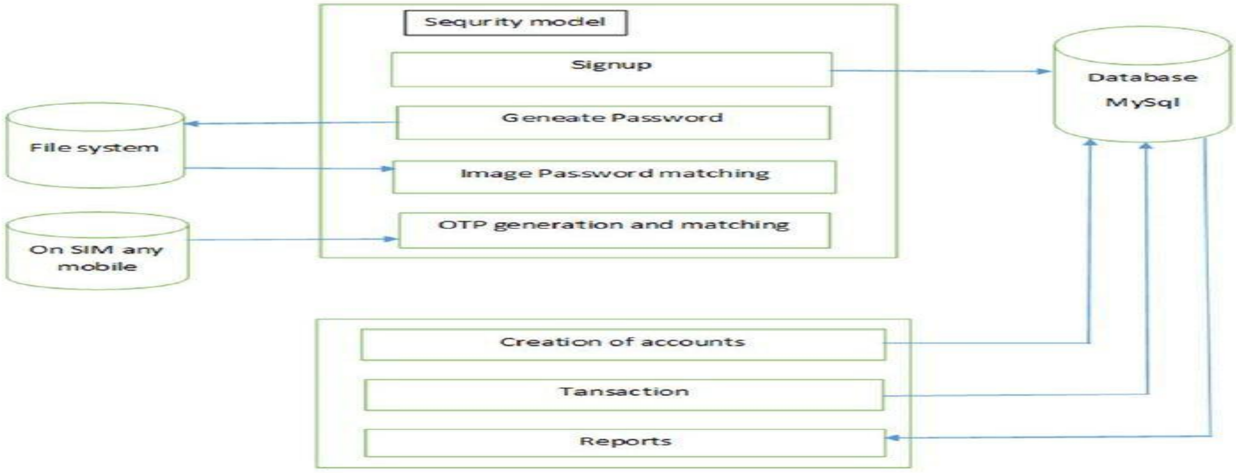


Fig1. Proposed System Architecture

Phase 1 To do any online transaction one need to register to any banks which provide online banking. In this phase user registration is done with the help of Visual Cryptography Algorithm.

Phase 2 While registration of user with visual cryptography user is provided by the randomimages that server have. Among these images user select one image for visual cryptography. The selected image required to remember by the system user which is needed to use for further execution. After the selection of image algorithm is applied on that image, the algorithm is visual cryptography. Output of this phase will give two shares using k-n sharing algorithm. Out of which first share goes under the process of phase two. And second share will recorded to server side with user id and original image.

Phase 3 APPLY THE ENCRYPTION ALGORITHM: Now user completed the phase one. Now need to proceed with secure approach by giving share one to user. And after that ,to the encrypted image private key will be assigned. And stored it(private key) to server side. By this phase server can be easily identified.

Phase 4 DETECTION OF PHISHING SITE: Whenever user goes for a trans-action; every time he need to upload the share one. After uploading the share, server will request for private key. User need to enter private key assigned dur-ing registration (in phase two). Now server is having both the private key and share one. Every time server will identify the authenticated user from private key. Now server upload its share two and stacks both the shares of the image by Visual Cryptography. From these two images , new image is formed. Server will check that image with the original image while user also checks formed image with original image selected in phase one. If both images (that is formed and original) are same then user will proceed further transaction and if it is not phishing is detected.

B. *Keyword Points:*

Steganography :

It is the practice of conceal a video, image, message, or file within another video, image, message, or file. In digital steganography, electronic connections may contain steganographic coding within of a transport layer, such the same as a document file, image file, protocol or program.

Digital watermarking Algorithm :

Internet is being a popular way to transfer the digital information from one place to another. In the mean time of the transmission, illegal copies of the original data can be made to make changes or to interchange the information. It can be difficult to difference between the original information and its copy as no security is provided to the data. Digital Watermarking technique is used to identify whether the data is duplicate or original. It provides the ownership and secures it from illicit copies. Digital watermarking is a method of embedding several data in the digital information to validate authenticity, rights of the data. The digital information can be in the form of image, video, audio, or text, etc. The digital information in which the watermark [6] to be embedded is known as the host. The watermark can be a logo or any useful information which proves the ownership of the data. Digital watermarking has different applications such the same as copyright security, authentication, copse communication, broadcast monitoring, source tracking, etc. Digital watermarking can be visible or invisible. In visible watermarking the watermark to be embedded in the host is purely visible to the users. Whether within the case of undetectable watermarking the pattern otherwise the watermark is in the hidden format that means the watermark is not perceptible to the users of the data. This type of watermarking useful in the covert communication between the people Watermarking" is the process of hiding digital information in a carrier signal; It is prominently used for tracing copyright infringements and for banknote authentication. Requirements and design of watermarking techniques are impacted by the different types of content in two major ways : imperceptibility and robustness requirements.

Digital watermarking may be used for a wide range of applications, such as:

1. Copyright protection
2. Source tracking
3. Broadcast monitoring
4. Video authentication
5. Software crippling on screencasting programs, to encourage users to pur-chase the full version to remove it.

AES 128 bit Encryption Decryption algorithm : The Advanced Encryp-tion Standard or AES is a symmetric block cipher used by the U.S. government to protect classified information and is implemented in software and hardware throughout the world to encrypt sensitive data.

The features of AES are as follows :

- Symmetric key symmetric block cipher
- 128-bit data, 128/192/256-bit keys
- Stronger and faster than Triple-DES
- Provide full specification and design details
- Software implementable in C and Java.

K-N sharing algorithm:

Step I: The original image (Iw h), number of shares to be divided (n) and number of shares needed (k) to recover the original picture are taken as in input

Step II: The number of sequences (ns) of (n-k+1) number of 1's and (k-1) num-bers of 0"s i.e. nCk-1 is calculated. Subsequently the sequences S_q1; S_q2; :$S_q$ns are constructed.

Step III: Let the shares of I denoted by S1, S2,, Sn, each of size w X h. Shares are generated using the following logic.

i. Initialize all the bit positions of St by 0, for 1 t n
ii. if (ith bit value of Ienc is 1) Generate a random number r in the range 1 to ns. Perform OR between the ith bit of Sj share (where 1 tj n) with the jth bit of the sequence Sqr, (1 r ns).

C. *Mathematical Module*

System Specification:

S= fS, s, X, Y, T, NDD, CP U_{count}g, f_{main}, f_{friend}, memory shared, DD.

S (system):- Is our proposed system which includes following tuple.

s (initial state at time T) :-GUI of AntiFishins website using visual Cryp-tography. The GUI provides space to enter a query/input for user.
X (input to system) :- Input Query. The user has to first enter the query. The query may be ambiguous or not. The query also represents what user wants to search.
Y (output of system):- List of AntiFishins website with all details. User has to enter a query into AntiFishins website then AntiFishins website generates a result which contains relevant and irrelevant AntiFishins reports and their details.
T (No. of steps to be performed):- These are the total number of steps required to process a query and generates results.
f_{main}(main algorithm) :- It contains Process P. Process P contains Input ,Output and subordinates functions. It shows how the query will be processed into different modules and how the results are generated.
DD (deterministic data):- It contains Database data. Here we have consid-ered OLD i.e. Hazard records contains the users crime with the criteria rules which contains number of ambiguous queries. Such queries are user for showing results. Hence, OLD is our DD.
NDD (non-deterministic data):- No. of input queries. In our system, user can enter numbers of queries so that we cannot judge how many queries user enters into single session. Hence, Number of Input queries are our NDD.
f_{friend} :- IE, UR, VC. i n our system,are the friend functions of the main func-tions. Since we will be using both the functions, both are included in riend function. IE is Information Extraction which is used for extracting information on browser. VC is based on the password that is image is converted into pass-word using vidual cryptography the data for submitting the data to the server. UR is based on the Users information stored on to the Database.
Memory shared: - Database. Database will store information like list of Users and its registration details and numbers users details. Since it is the only memory shared in our system, we have included it in the memory shared.
CPU_{count}: - In our system, we require 1 CPU for server and minimum 1 CPU for client. Hence, CPUcount is 2

Subordinate Functions:

Identify the processes as P.

S= fI; O; P; ::::::::g

P = fUR; IE; V Cg

Where,

UR is User Registration IE is Information Extraction. VC is Visual cryptography.

UR= f U, SUBMIT, MESSAGESg

Where,

U=input Query using the information

SUBMIT = f1, 2, 3,.........., n

MESSAGES is output of UR which is Status Messages.

IE= fCP, NLP Techniques, Infog

Where,

CP is input which is filter information to IE, NLP is use for transforming all the letters to lowercases, stemming and removing stop word.

Algorithm1:

```
Step 1: Accept a Query (Q).
Step 2: Get Data from from.
Step 3: call UR function
Step 2.1: Get U as Input to UR.
Step 2.2 : SUBMIT data
Step 2.5 : Output as MESSAGE.
Step 4: call to IE Function
Step 4.1 : Get CP as Input .
Step 4.2 :Call Function NLP
Step 4.3: Process NLP as Removing Stop Word.
Step 4.4 : Get Relevant Information
Step5: Display Result.
Step 6: Stop.
```

VC = fCP; Submit; V isualCryptography; MESSAGEg

Where,

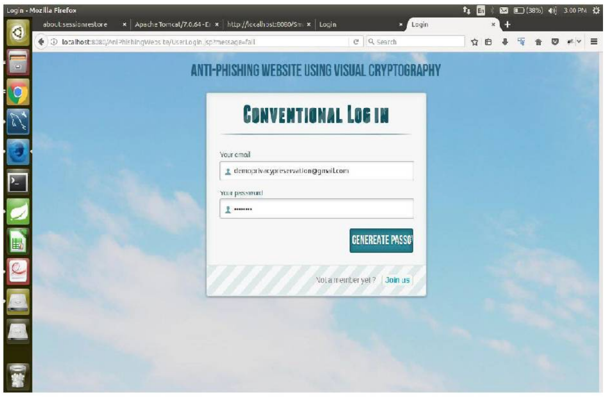
CP is input which is lter information to VC SUBMIT = f1; 2; 3; ; ng

Visual Cryptoraphy is function for creating the image as password. MESSAGES is output of UR which is Status Messages.

Algorithm2:

```
Step 1: Accept a Query (Q).
Step 2: Get Data from from.
Step 3: call to CR Function
Step 3.1 : Get CP as Input .
Step 3.2 : Call Function Submit
Step 3.3 : Call Visual Cryptography for image stegnography.
Step 3.4: process submit function for storing the data onto the server.
Step 3.5 : Output as Messages
Step4: Display Result.
Step 5: Stop.
```

V. Simulation Results



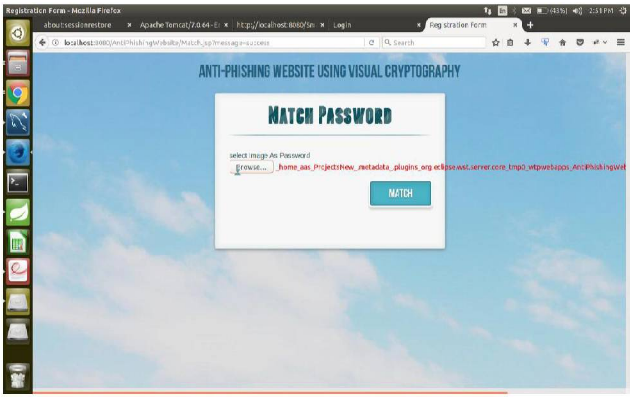
ANTI-PHISHING WEBSITE USING VISUAL CRYPTOGRAPHY

CONVENTIONAL LOG IN

Your email: demoprivacypreservation@gmail.com

Your password: ••••••••

Fig.2. Login Page



ANTI-PHISHING WEBSITE USING VISUAL CRYPTOGRAPHY

MATCH PASSWORD

select image As Password

_home_aas_ProjectsNew_.metadata_.plugins_org.eclipse.wst.server.core_tmp0_wtpwebapps_AntiPhishingWeb

Fig. 3. Match Image as Password

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 7, July 2017

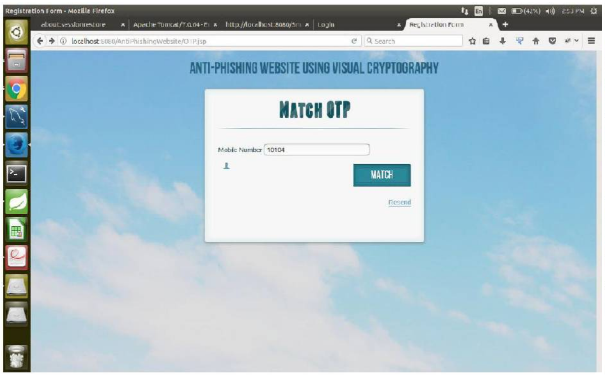
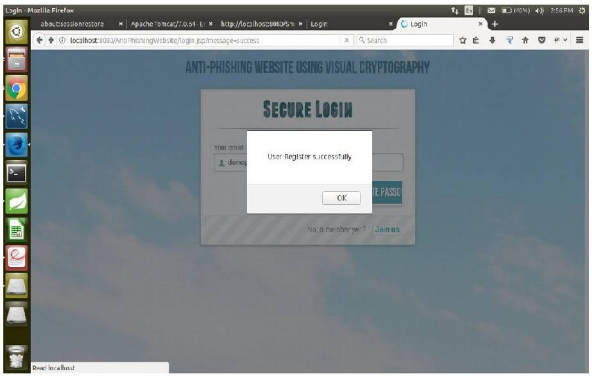

Registration Form - Mozilla Firefox
localhost:8080/AntiPhishingWebsite/OTP.jsp
ANTI-PHISHING WEBSITE USING VISUAL CRYPTOGRAPHY
MATCH OTP
Mobile Number 10104
MATCH
Resend

Fig. 4. One Time Password


Login - Mozilla Firefox
localhost:8080/AntiPhishingWebsite/login.jsp?message=success
ANTI-PHISHING WEBSITE USING VISUAL CRYPTOGRAPHY
SECURE LOGIN
Your email
OK
Not a member yet ? Join us

User Register successfully

Fig 5. Login Successfully

Implemented paper perform this system in witch we get output in the form of Homepage i.e to log in to main bank account system. Here we perform security approach with the help of captch image. First result widow fig2, shows that the login page.

Second windows fig3, shown prescribed to attach or upload image to check password match and send OTP on mobile of user who wants to login.

This third widow fig4 shows page for OTP fill. After it, it is correct then user loged in successfully.

Final Window fig5, is here after successfully Login the page and come to Bank Account Sction.

VI. CONCLUSION AND FUTURE WORK

Phishing attack is more common in today's world because when it attacks it can capture and store user data information. Attackers use that data information wrongly and user gets loss their money and suffers from financial Problem. The proposed methodology can help to identify the phishing websites using Anti-phishing website using visual cryptography, which preserves confidential information of user using different layers of security. Using vi-sual cryptography two shares of the images are generated first share goes under the process of detection of phishing site and second share will record to server side with user id and original image during this OTP will generate on user mobile when user goes for a transaction user need to upload the share one. After uploading, server will request for private key. User need to provide private key. Now server stacks its share two with user share one by visual cryptography. A new image is formed from these two images. Server will check that image with original one while user also checks formed image with original image selected in phase one. While checking if created picture is exact same as original one then only we can precede onwards otherwise if it is not match then phishing is captured and user session terminated transaction with no any loss of secure data. So it becomes strong security.

FUTURE WORK

Essentially, since to complete the transaction user should have the encrypted part of image that is share one, means at the time of each transaction user is going to upload a image. To overcome such a problem we can provide alternating system to user by storing user share to server database only. And at the time of any transaction user will select one image given by the application server to user.

REFERENCES

1. M. Noar and A. Shamir, \Visual cryptography". EUROCRYPT, 1994.
2. Divya James and Mintu Philips, A Novel Anti Phishing Framework Based On Visual Cryptography". International Conference @2012 IEEE
3. Vimal Kumar and Rakesh Kumar, Detection of Phishing Attack Using Vi-sual Cryptography in Ad hoc Network". International ICCSP conference @2015 IEEE.
4. Barnali Gupta Banik and Samir Kumar Bandyopadhyay International Confer-ence on Intellience and Communication Networks@2015 IEEE.
5. Sruthy K Joseph, Ramesh R "Random Grid based Visual Cryptography using a common share". Conference on Computing and Network Communications (CoCoNet'15), Dec. 16-19, 2015, Trivandrum, India.

6. Mr.A.Duraisamy, Mr. M. Sathiyamoorthy, Mr. S. Chandrasekar, \Protection Of Privacy In Visual Cryptography Scheme Using Error Di usion Technique", IJCSN, Vol 2, Issue 2, April 2013 ISSN (Online) : 2277-5420
7. Anushree Suklabaidya, G. Sahoo, \Visual Cryptographic Applications", IJCSE, Vol. 5 No. 06 Jun 2013, ISSN : 0975-3397
8. Sharma and Rao, \Visual Cryptography authentication for Data Matrix Code", International Journal of Computer Science and Telecommunications , Volume 2, Issue 8, November 2011
9. P.S. Revenkar, AnisaAnjum, W .Z. Gandhare, Secure Iris Authentication Using Visual Cryptography", IJCSIS, Vol. 7, No.3, 2010, ISSN 1947-5500
10. Vinodhini and Ambarasi proposed a method for authentication based on Visual Cryptography using CAPTCHA. CAPTCHA stands for Completely Automated Public Turing test to tell Computers and Humans Apart.
11. Mounika Reddy. M, MadhuraVani.B, \A Novel Anti Phishing Framework Based On Visual Cryptography", IJARCCE,Vol. 2, Issue 9, September 2013 ISSN (On-line) : 2278-1021
12. Jing Dong proposed biometric watermarking for protecting biometric data and templates in biometric systems.
13. L. N. Pande, Niraj Shukla, Visual Cryptography Schemes Using Compressed Random Shares", International Journal Of Advance Research In Computer Sci-ence And Management Studies, Volume 1, Issue 4, September 2013, ISSN: 2321-7782 (Online)
14. Young-Chang Hou , Zen-Yu Quan, Progressive Visual Cryptography With Un-expanded Shares", IEEE Transactions On Circuits And Systems For Video Tech-nology, Vol. 21, No. 11, November 2011
15. Verheul and Van Tilborg proposed Colored secret images can be shared with the concept of arcs to construct a colored VCS.