A Novel Anti Phishing Framework Based On Visual Cryptography

Bhagyesh Mali, Akshay Kadam, Akshay Hande, Prof. P.B.Lad

Abstract— Computer and network security is one of the most Crucial areas today. With so many attacks happening on all kinds of computer systems and networks, it is imperative that the subject be understood by students who are going to be the IT professionals of the future. Phishing is the attempt to obtain sensitive information such as usernames, passwords, and credit card details (and money), often for malicious reasons, by disguising as a trustworthy entity in an electronic communication. "A Novel Anti-phishing framework based on visual cryptography" to solve the problem of phishing. The use of visual cryptography is showed to protect the privacy of image captcha by dividing the original image captcha into two parts (shares). That image shares are stored in separate database servers such that the original image captcha can be exposed only when both are simultaneously available. Once the image captcha parts are match then user can use whole image as password.

Index Terms— Phishing, Visual cryptography, Image Captcha, Security

1 INTRODUCTION

Now a days Online transactions become more popular because of fast life no one want to wait for withdraw money from ATM but their are various attacks are present behind this online transactions so that security becomes the major concern. Their are various types of attack in this phishing is one of the attack and new innovation ideas are arising with this in each second so preventing mechanism should also be so effective. Thus the security in this case be very high and should not be traceable very easily.

Today all are trying to keep their app as secure as possible. Since the design and technology of middleware has improved, their detection is a difficult problem. As a result, it is nearly impossible to be sure whether a computer that is connected to the internet can be considered trustworthy and secure or not. Phishing scams are also becoming a problem for online banking and e-commerce users. Phishing is an type of attack which steal the sensitive information from internet this sensitive information's are credit card information, internet banking password One definition of phishing is given as"it is a criminal activity using social engineering techniques. Phishers attempt to fraudulently acquire sensitive information, such as passwords and credit card details, by masquerading as a trustworthy person or business in an electronic communication".

Another comprehensive definition of phishing states that it is "the act of sending an email to a user falsely claiming to be an established legitimate enterprise into an attempt to scam the user into surrendering private information that will be used for identity theft".

- *Bhagyesh Mali is currently pursuing bachelors degree program in information technology in mumbai University, India E-mail: bhagyeshmali5@gmail.com*
- *Akshay Kadam is currently pursuing bachelors degree program in information technology in mumbai University, India.Email: ak8990227@gmail.com*
- *Akshay Hande is currently pursuing bachelors degree program in information technology in mumbai University, India.Email: handeakshay28@gmail.com*
- *Prof. P.B.Lad is currently working in degree college (Konkan Gyanpeeth college of Engineering) in information technology branch in mumbai University, India.Email: poonam.lad23@gmail.com*

1.1 Objective

The prime objective of this project is to ensure the security of information (in this case image) transformation by creating image shares.

The four objectives are:

1. Confidentiality (the information cannot be understood by anyone for whom it was unintended)
2. Integrity (the information cannot be altered in storage or transit between sender and intended receiver without the alteration being detected)
3. Non-repudiation (the creator/sender of the information cannot deny at a later stage his or her intentions in the creation or transmission of the information)
4. Authentication (the sender and receiver can confirm each other's identity and the origin/destination of the information). Because system Recommend the best alternate product.

1.2 Purpose

Today, various people utilize the distinctive applications to image data transfer. By far most of the people use their images for various customers using the social application. The attack on these social applications can copy or hack the important data. For better usage of these applications, users are using it on their mobiles, tablets, etc. The protection against the hacking attacks on those web or available is plans, there exist distinctive data security framework for multimedia data. These present security frameworks are either using encryption or steganography, or the combination of both. There is diverse securable image encryption that can be especially for protection against the unauthorized access.

1.3 Scope

Visual cryptography technique is used to make the data secure. Here the original data is divided into a number of shares which are sent through different communication channels from sender to receiver. Therefore the intruder has less chance to get the whole information. But still it is not so secured. This can be made more secure by introducing a symmetric key for both encryption and decryption process. Using the key, the image is first encrypted then divided into a number of shares. If the intruder gets k number of shares s/he can not be able to decrypt it if the key is not known to his/her. For key, a combination of character or number can be used.

2 LITERATURE SURVEY

The related approaches for phishing detection system are email based approach, blacklist approach, visual clue based approach information flow based approach, layout similarity based approach and website feature based approach. In the existing system of phishing detection there is also an approach where the visual cryptography is used. In this approach when the user first registers at the bank server, then at the time of registration itself an image is selected which is divided into two shares. One share of image is stored at the bank server and user gets another share which he keeps with him. When the user wants to initiate the transaction with merchant server he sends his UID code to the merchant server. Merchant server then sends his sys Id & password along with user's UID to the bank server. When bank server gets this request he first verifies if the merchant is registered merchant. If so, he fetches the share of image associated with the specific UID code. And sends it to the merchant server which then sends it to the user. When user gets the share of image he combines it with his share. If user gets the original image which was selected at the time of registration, then he gets to know that the merchant is authenticated, and the user can now precede the transaction. Visual cryptography technique was introduced by Naor and Shamir in 1994 as an alternative for conventional cryptography.They demonstrated a visual secret sharing plan, where a picture was separated into n imparts so that just somebody to all n shares could decode the picture, while any n 1 shares uncovered no data about the first original image. Each share was printed on a separate transparency, and decryption was performed by overlaying the shares. At the point when all n shares were overlaid, the first picture would show up. There are a few speculations of the fundamental plan including k-out-of-n visual cryptography. Rijimen displayed another 2-out-of-2 VC plot by applying the thought of shading mixture. When two transparencies superimposed on one another with distinctive colours, they lead to raise third blended shading. In 2002, Nakajima predicted a new method of extended visual cryptography. This method is for regular images which are used to produce meaningful binary shares .This system works by taking three pictures as an input and generates two images which correspond to two of the three input pictures.The third picture is recreated by printing the two share pictures onto transparencies and stacking them together. By and large, visual cryptography experiences the deterioration of the image quality. In this also describes the method to improve the quality of the output image. Binary visual cryptography scheme is proposed Hou et al. in the year 2004, which is applied to gray level images, that a gray level image is transformed into halftone images. The method that uses the density of the net dots to simulate the gray level is called Halftone and transforms an image with gray level into a binary image before processing. Halftone visual cryptography is proposed by the Zhi Zhou et al. In 2006 which produce meaningful and good high quality halftone shares, the generated halftone shares contain the visual information.

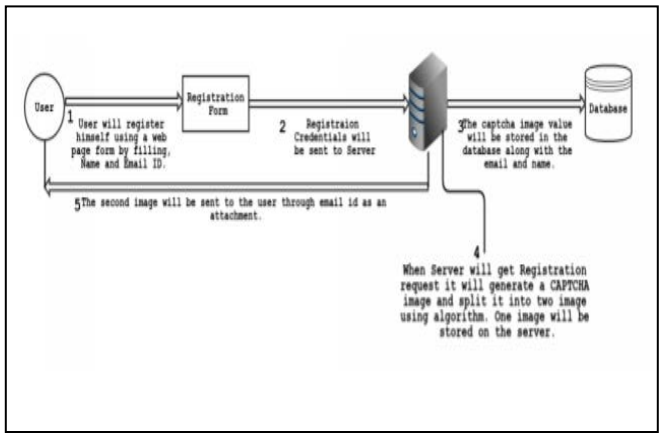
3 METHODOLOGY

3.1 SYSTEM DESIGN

Basic Modules:- The proposed approach can be divided into two phases:

3.1.1. REGISTRATION PHASE:

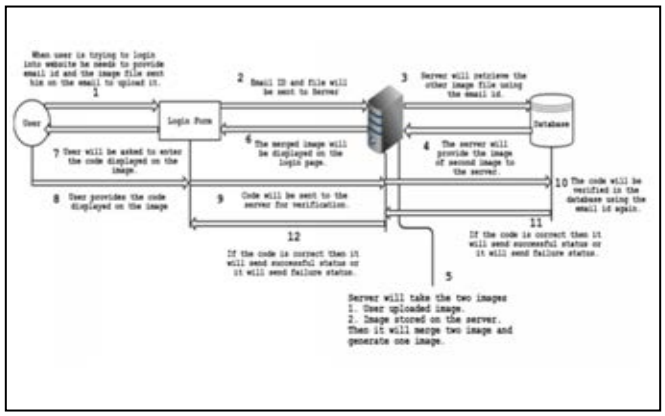
In the registration phase, a key string (password) is asked from the user at the time of registration for the scure website. The key string can be a combination of alphabets and numbers to provide more secure environment. This string is concatenated with randomly generated string in the server and an 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.



3.1.2. LOGIN PHASE:

In the Login phase first the user is prompted for the username (user id).The useris 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

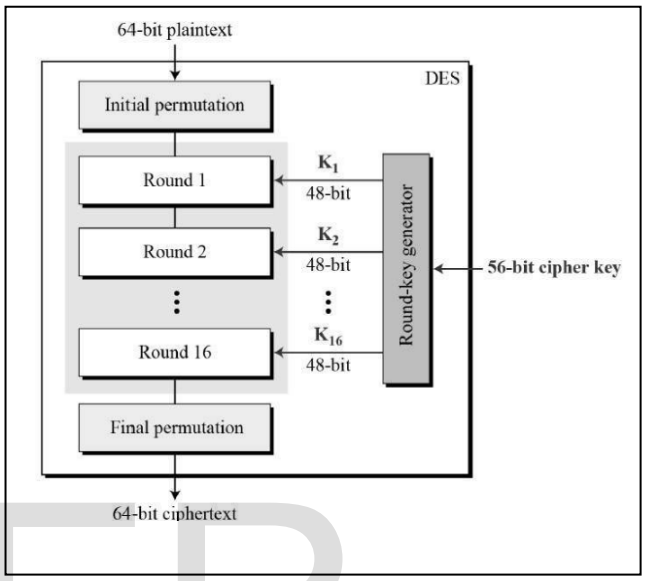
user, is stacked together to produce the image captcha. The image captcha is displayed to the user .Here the end user can check whether the displayed image captcha matches with the captcha created at the time of registration. The end user is required to enter the text displayed in the image captcha and this can serve the purpose of password and using this, the user can log in into the website. Using the username and image captcha generated by stacking two shares one can verify whether the website is genuine/secure website or a phishing website and can also verify whether the user is human user or not.Figure.below can be used to illustrate the login phase.



3.2 Algorithm Design

DES Algorithm

The Data Encryption Standard (DES) is a symmetric-key block cipher published by the National Institute of Standards and Technology (NIST).DES is an implementation of a Feistel Cipher. It uses 16 round Feistel structure. The block size is 64-bit. Though, key length is 64-bit, DES has an effective key length of 56 bits, since 8 of the 64 bits of the key are not used by the encryption algorithm (function as check bits only).

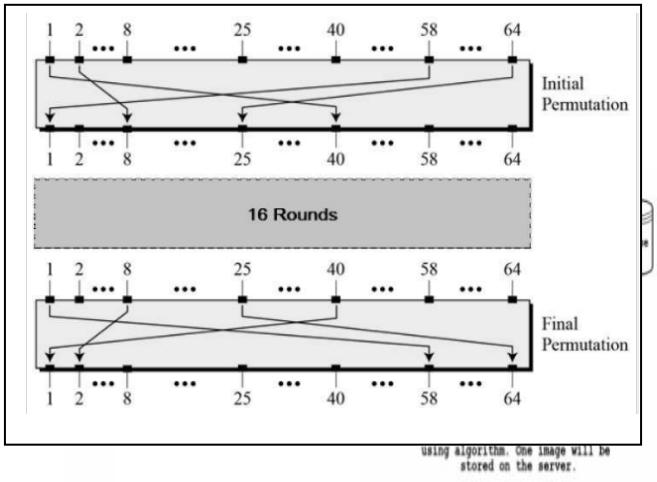


Since DES is based on the Feistel Cipher, all that is required to specify DES is −

- Round function
- Key schedule
- Any additional processing − Initial and final permutation

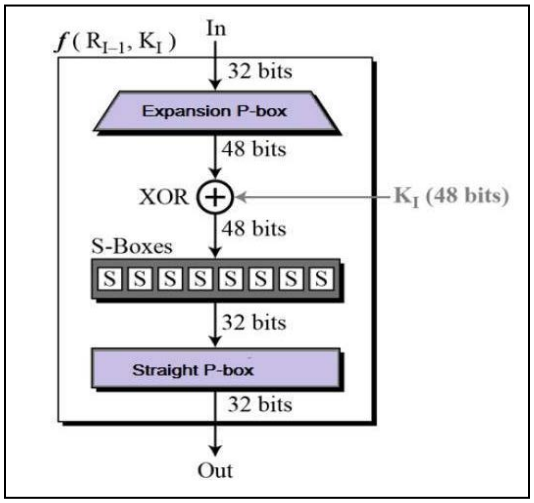
Initial and Final Permutation

The initial and final permutations are straight Permutation boxes (P-boxes) that are inverses of each other. They have no cryptography significance in DES. The initial and final permutations are shown as follows

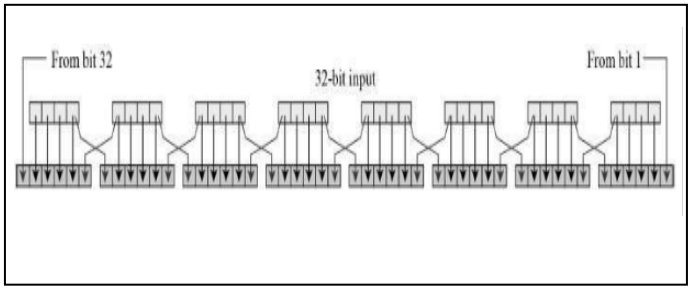


Round Function

The heart of this cipher is the DES function, f. The DES function applies a 48-bit key to the rightmost 32 bits to produce a 32-bit output.



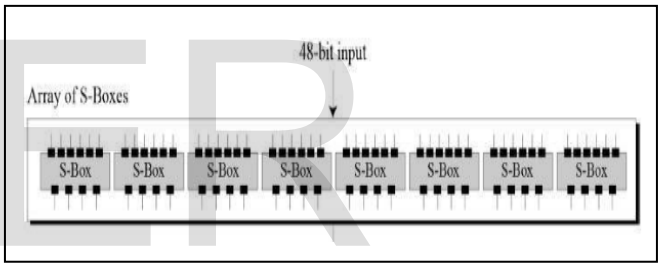
Expansion Permutation Box − since right input is 32-bit and round key is a 48-bit, we first need to expand right input to 48 bits. Permutation logic is graphically depicted in the following illustration



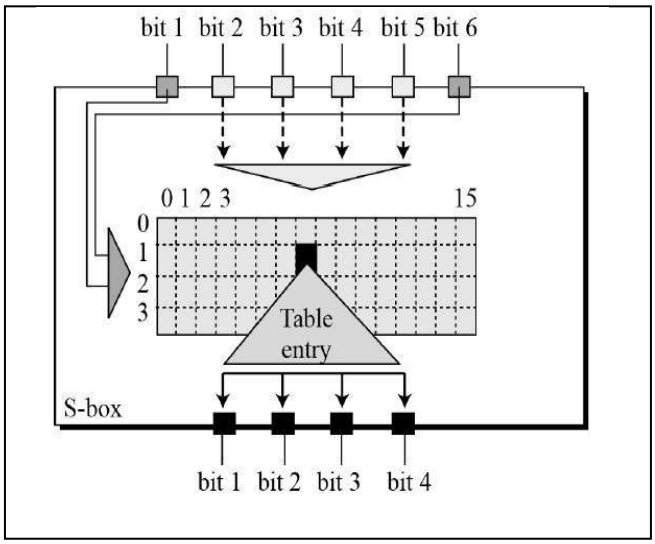
The graphically depicted permutation logic is generally described as table in DES specification illustrated as shown

32	01	02	03	04	05
04	05	06	07	08	09
08	09	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	31	31	32	01

- **XOR (Whitener).** − After the expansion permutation, DES does XOR operation on the expanded right section and the round key. The round key is used only in this operation.
- **Substitution Boxes.** − The S-boxes c2arry out the real mixing (confusion). DES uses 8 S-boxes, each with a 6-bit input and a 4-bit output. Refer the following illustration



The S-box rule is illustrated below



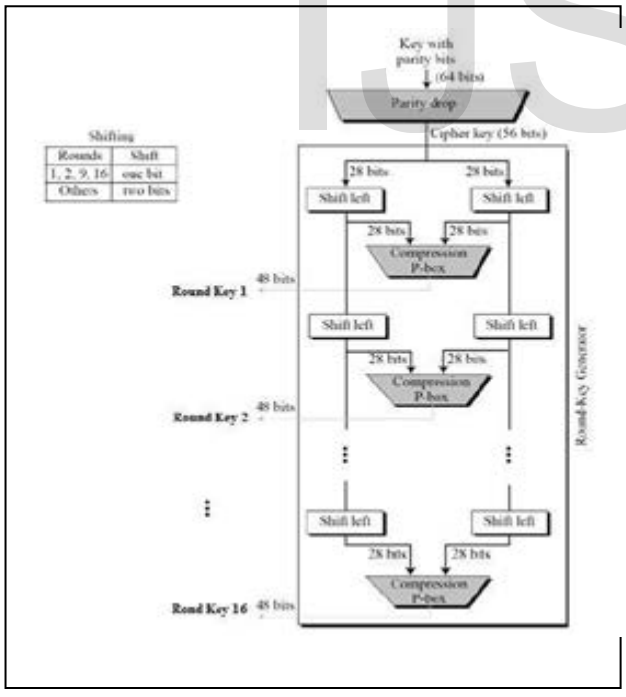
- There are a total of eight S-box tables. The output of all eight s-boxes is then combined in to 32 bit section.

Straight Permutation − The 32 bit output of S-boxes is then subjected to the straight permutation with rule shown in the following illustration

16	07	20	21	29	12	28	17
01	15	23	26	05	18	31	10
02	08	24	14	32	27	03	09
19	13	30	06	22	11	04	25

Key Generation

The round-key generator creates sixteen 48-bit keys out of a 56-bit cipher key. The process of key generation is depicted in the following illustration



4 RESULT

4.1 User interface

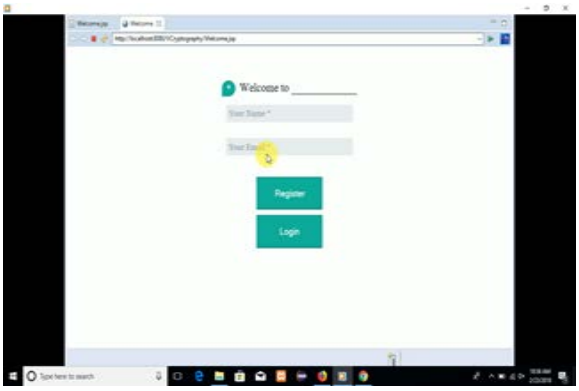


Fig.User Registration Phase

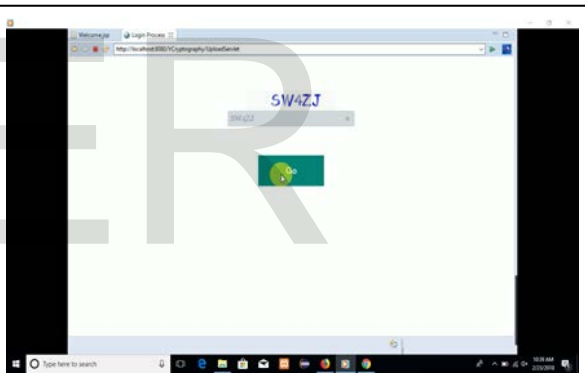


Fig.After successful matching of two shares

4 CONCLUSION

Currently phishing attacks are so common because it can attack globally and capture and store the user's' confidential information. This information is used by the attackers which are indirectly involved in the phishing process. Phishing websites as well as human users can be easily identified using our proposed "Anti-phishing framework based on Visual Cryptography".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.

REFERENCES

[1] Monoth and A. P. Babu, ."Recursive Visual Cryptography Using Random Basis Column Pixel Expansion". in Proceedings of IEEE International Conference on Information Technology, 2007

[2] B.Persis Urbana Ivy,Purshotam Mandiwa,Mukesh Kumar.,"A Modified RSA Cryptosystem Based on 'n' prime number" International Journal of Enginerring And Computer Science ISSN:2319-7242,Nov2012

[3] Divya James and Mintu Philip," A NOVEL ANTI PHISHING FRAMEWORK BASED ON VISUAL CRYPTOGRAPHY "International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.1, January 2012

[4] M. Naor and A. Shamir, "Visual cryptography," in Proc. EUROCRYPT, 1994, pp. 1–12

[5] 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.