ISSN:0975-9646

Image Based Authentication Using Visual Cryptography and Encryption Algorithm

Shreya Zarkar, Sayali vaidya, Arifa Tadvi, Tanashree Chavan, Prof. Achal Bharambe

Modern Education Society's College Of Engineering Pune
Department of Computer Engineering
Savitribai Phule Pune University
Pune, India

***Abstract*— Now-a-days online attacks have increased to a great extent and the most popular attack among them is phishing. Phishing can be basically defined as one kind of attack in which various attackers acquire the confidential and sensitive information of the victims. Thus, security in such cases should be very high to avoid the online attacks. Phishing steals the confidential information such as password, credit card information, etc which is carried out by fraudsters. So it is very much important for the users to identify the fake website and avoid falling prey to it. In this paper we have proposed a new approach named as "Anti-phishing structure based on visual cryptography and RSA algorithm" to solve the problem of phishing. Here an image based authentication using Visual Cryptography (VC) and the encryption algorithm (RSA) is used. Visual cryptography is mainly done by splitting the original image into two shares one with user database and one with the server database. And the original image can be obtained only by both the shares of the image. This method of image authentication gives 100% result for image size less than 2.5MB. thus security of image can be achieved by visual cryptography and RSA algorithm**

***Keywords*—Phishing, Visual Cryptography, Encryption algorithm, RSA, CAPTCHA, Authentication, Decryption.**

I. INTRODUCTION

Now days, Online transactions are very common and various online attacks are present behind this. Phishing is one kind of attack in which confidential and various attacker can gain sensitive information. Phishing is identified by major attack among all online attacks and new innovative ideas are arising with this. Thus, security in such cases should be very high which cannot be tractable by implementation easiness. Now days most of the applications are only as secure as their underlying system, as a result it is not sure that whether the computer that connected to internet is problem secure or not. Phishing attacks are becoming a problem for online transactions and e- commerce user's. Phishing is form of online identity theft that steals the confidential and sensitive information such as password, credit card information etc. One definition of phishing can be given as "It is a criminal activity using social engineering" Phishing is an attempt by fraudsters to steal your account related information such as User ID, passwords, URN and OTP by sending e-mails which appears to originate from trusted source like Banks, TAX authorities etc. These emails create a sense of urgency for updating account related information.. One of the primary goals of phishing is to acquire the user's information such as username, password, and credit card information. Phishing attacks mainly focus on websites, where attacker carry out fraudulent activities such as financial transactions on behalf of users by forging an email which contains an fake URL that redirects user to fake websites masquerading as an online bank or a government entity. Attacker uses replica of original website that is send to the user, user fills and submits the sensitive and useful information into the website, attacker pulls the information and saves the data for its own illegal use. Following are the references taken into consideration.

A. *The Phishing Guide Understanding & Preventing Phishing Attacks*

The survey focuses on Phishing [1] by Gunter Ollmann. Phishing is the new 21st century crime. The global media runs stories on an almost daily basis covering the latest organization to have their customers targeted and how many victims succumbed to the attack. While the Phishers develop ever more sophisticated attack vectors, businesses flounder to protect their customers' personal data and look to external experts for improving email security. Customers too have become wary of "official" email, and organizations struggle to install confidence in their communications. While various governments and industry groups battle their way in preventing Spam, organizations can in the meantime take a proactive approach in combating the phishing threat. By understanding the tools and techniques used by professional criminals, and analysing flaws in their own perimeter security or applications, organizations can prevent many of the most popular and successful phishing attack vectors. This paper covers the technologies and security flaws Phishers exploit to conduct their attacks, and provides detailed vendor-neutral advice on what organizations can do to prevent future attacks. Security professionals and customers can use this comprehensive analysis to arm themselves against the next phishing scam to reach their in-tray.

B. *Visual Cryptography and Image Security*

The survey focuses on new type of cryptographic scheme [2] which can decode concealed images without any cryptographic computations. The scheme is easy to implement and is perfectly secured. It is extended to variable variant. We extend it into visual variant k out of n secret sharing problem in which the dealer provides transparency to each one of n users. Any k of them can see

image by stacking their transparencies, but any k-1 of them gain no information about it. Secure Server Verification by Using Encryption Algorithm And Visual Cryptography.

C. *Segment Based Visual Cryptography*

The survey focuses on Encryption Algorithm and Visual Cryptography [3] by Bernd Borchert. Bernd Borchert presents 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.

D. *CAPTCHA : Using Hard AI Problems For Security*

The survey focuses on captcha[4] by Luis von Ahn, Manuel Blum, Nicholas J. Hopper, and John Langford. A captcha is a program that can generate and grade tests that: (A) most humans can pass, but (B) current computer programs can't pass. We introduce captcha, an automated test that humans can pass, but current computer programs can't pass: any program that has high success over a captcha can be used to solve an unsolved Artificial Intelligence (AI) problem. We provide several novel constructions of captchas. Since captchas have many applications in practical security, our approach introduces a new class of hard problems that can be exploited for security purposes. Much like research in cryptography has had a positive impact on algorithms for factoring and discrete log, we hope that the use of hard AI problems for security purposes allows us to advance the field of Artificial Intelligence. We introduce two families of AI problems that can be used to construct captchas and we show that solutions to such problems can be used for steganographic communication. Captchas based on these AI problem families, then, imply win-win situation: either the problems remain unsolved or there is away to differentiate humans from computers or the problems are solved and there is a way to communicate covertly on some channels.

E. *A Text-Graphics Character CAPTCHA for Password Authentication*

The survey focuses on Text-Graphics Character (TGC) CAPTCHA, [5] by Matthew Dailey and Chanathip Namprempre. They have proposed a new construct, the Text-Graphics Character (TGC) CAPTCHA, for 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. CAPTCHAs (Completely Automated Public Turing tests to tell Computers and Humans Apart) are currently being used to prevent automated “bots” from registering for email Secure Server Verification by Using Encryption Algorithm And Visual Cryptography. They have also been suggested as a means for preventing dictionary attacks. However, current CAPTCHAs are unsuitable for text-based remote access. Our TGC CAPTCHA
fills this gap. In this paper, we define the TGC CAPTCHA, prove that it is a (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. We believe that the system will not only help improve the security of servers allowing remote terminal access, but also encourage a healthy spirit of competition in the fields of pattern recognition, computer graphics, and psychology. The survey focuses on phishing by Divya James and Mintu Philip. With the advent of internet, various online attacks has been increased and among them the most popular attack is phishing. Phishing is an attempt by an individual or a group to get personal confidential information such as passwords, credit card information from unsuspecting victims for identity theft, financial gain and other fraudulent activities. Fake websites which appear very similar to the original ones are being hosted to achieve this. 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 is implemented. The use of visual cryptography is explored to preserve the privacy of an image captcha by decomposing the original image captcha into two shares (known as sheets) that are stored in separate database servers (one with user and one with server) such that the original image captcha can be revealed only when both are simultaneously available; 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. Using this website cross verifies its identity and proves that it is a genuine website before the end users.

F. *Hashed Based Visual Cryptography Scheme For Image Authentication*

The survey focuses on Hashed Based Visual Cryptography Scheme for image Authentication [6] The proposed hash based visual cryptography scheme for image authentication can overcome the cheating attacks of visual cryptography as proposed by Yang et al. This approach reduces the size of database the process of retrieving and comparing become very fast when compared to retrieving the images from database. This method can be used in biometric fingerprint scanning where the thumb image is captured and shares are generated by using the visual cryptography system. This method can be used to produce the smart cards to the users, which can be used to authenticate the users for providing the services. Using the proposed method the authentication becomes very fast when compared to the previous methods. This approach can be used with all applications of visual cryptography authentication system. We can develop separate authentication device for personal computer, so that every user will have smart card that contains a user share, when the user insert the smart card to that authentication device

user will be authenticated. We hope to develop a full prototype of such method as our future work.

G. *Visual Cryptography and Chaotic Image Encryption for the Security Of Biometric System*

The survey focuses on Protection of biometric data and templates is a crucial issue for the security of biometric systems[7] by Divya James and Mintu Philip. This paper proposes new security architecture for biometric templates using visual cryptography and chaotic image encryption. The use of visual cryptography is explored to preserve the privacy of biometric image by decomposing the original image into two images (known as sheets) such that the original image can be revealed only when both images are simultaneously available; the individual sheet images do not reveal the identity of the original image. The algorithm ensures protection as well as privacy for image using a fast encryption algorithm based on chaotic encryption. Chaos based cryptography is applied on to individual shares. Using this one can cross verify his identity along with the protection and privacy of the image. The comparative analysis of above survey paper is shown in table1:
From comparative analysis we conclude that by using visual cryptography and RSA algorithm anti-phishing can be reduced. The actual content of the paper contains black and white image (i.e. black and white pixels) for cryptography. We can use the same method for colored images as future enhancement.

Table 1

COMPARATIVE ANALYSIS OF LITERATURE SURVEY

Sr. No.	Paper Name	Methodology	Result
1	The Phishing Guide Understanding & Preventing Phishing Attacks	multi-tiered approach(client-side, server-side and enterprise)	66.45%
2	Visual Cryptography	Visual Cryptography(basic)	72.55%
3	Segment-based Visual Cryptography	Visual Cryptography using seven segment display	77.75%
4	CAPTCHA: Using Hard AI Problems For Security	AI problems (Stegnography)	85.30%
5	A Text-Graphics Character CAPTCHA for Password Authentication	Text-Graphics Character Captcha	89.54%
6	Hashed Based Visual Cryptography Scheme For Image Authentication	Visual cryptography	90.15%
7	Visual Cryptography and Chaotic Image Encryption for the Security Of Biometric System	Visual cryptography	91.13%
8	Image Authentication using Visual Cryptography and Encryption algorithm	RSA algorithm & Visual cryptography	94.20%

II. SYSTEM ARCHITECHURE

For phishing detection and prevention, we are proposing a new methodology to detect the phishing website. The proposed approach can be divided into two phases

A. Registration Phase

In the registration phase the most important part is the creation of shares from the image where one share is kept with the user and other share can be kept with the server. If server under test sends some different share then the stacking of shares will create unrecognizable form of image. The stepwise procedure is shown in the figure 1.

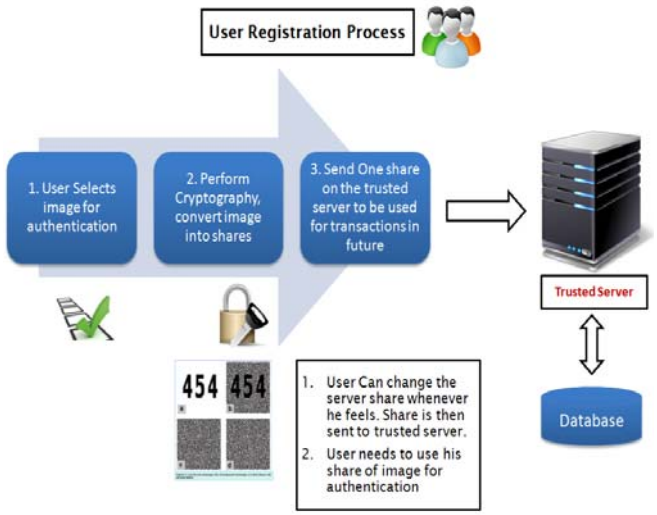


Fig 1: Registration Phase

B. Login Phase

In the login phase the user has to enter the user id and his share of image with the public key. The user id, share of image and public key is sent to the server and they are decrypted using the public and private key of the user. At the server side both the share of images (server share and user share) are stacked together to form the original image. This original image is sent to the user's browser window. Now the user will understand that this is the trusted server and user can enter his further credentials.

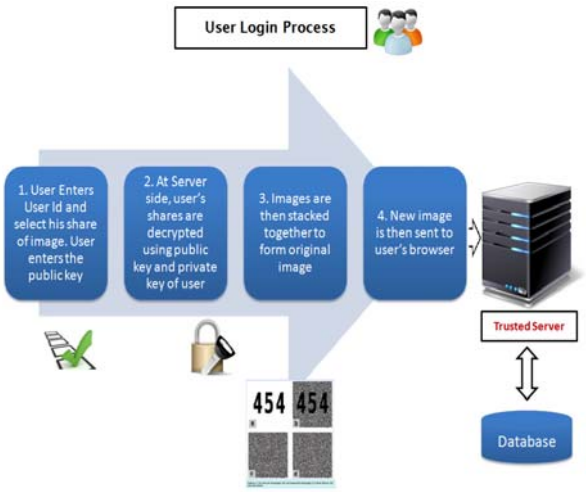


Fig4: Login Phase

III. IMPLEMENTATION

The phishing can be overcome by implementation of RSA algorithm and Visual Cryptography.

A. RSA Algorithm

1. Key Generation

- Select two large prime numbers p, q
- Compute
  n = p ×q
  v = (p-1) × (q-1)
- Select small odd integer k relatively prime to v GCD (k, v) = 1
- Compute d such that
  (d × k)%v = (k × d) %v = 1
- Public key is (k, n)
- Private Key is (d, n)

2. Encryption and Decryption

- Alice and Bob would like to communicate in private
- Alice uses RSA algorithm to generate her public and private keys

-Alice makes key (k, n) publicly available to Bob and anyone else wants to send her private messages

- Bob uses Alice's public key (k, n) to encrypt message M:

-compute E (M) = (Mk) %n
-Bob sends encrypted message E (M) to Alice

- Alice receives E (M) and uses private key (d, n) to decrypt it:

-compute D (M) = (E (M) d) %n
-decrypted message D (M) is original message M

- RSA algorithm for encryption/decryption

-encryption: compute E (M) = (Mk) %n
-decryption: compute D (M) = (E (M) d) %n

With the help of RSA algorithm the public and private keys can be generated and thus used for encryption and decryption.

B. Visual Cryptography Algorithm

Visual Cryptography is encrypting the image into N number of secrete shares. The original image [8] can be obtained only when the user is having N number of secrete shares. when all the shares of images are stacked together the original image is obtained. N-1 shares will not reveal any information about the original image. For the color images the VC can be implemented by converting the values of [9] ARGB (Alpha Red Green Blue) color pixels to CMYK (Cyan Magenta Yellow Key (Black)) color pixels. Share1 will consist of C, M values as 1 and other values as 0. Whereas in share2 Y, K values are 1 and other color values will be 0. C,M (1,1,0,0) will consist of share1 and YK(1,1,0,0) is share2. When both the shares are overlaid the original image will be obtained this process is decryption of two shares to get the original image[10]. Here the encryption and decryption algorithms are stated below.

1. Encryption

- Get color pixel (x,y)
- Each pixel value is of 32 bit, so separate ARGB values from color

```
A = (color>>24) && 0xff;
R = (color>>16) && 0xff;
G= (color>>8) && 0xff;
B = (color>>0) && 0xff;
```

- Convert ARGB values into CMYK values

```
R' = R/255;
G' = G/255;
B' = B/255;
K= 1-max(R',G',B');
C = (1-R'-K)/(1-K);
M = (1-G'-K)/(1-K);
Y = (1-B'-K)/(1-K);
  K= K*255f;
  C= C*255f;
  M=M*255f;
  Y= Y*255f;
  K= K/2f;
  C=C/2f;
  M=M/2f;
   Y= Y/2f;
```

- Create two splits by CMYK values,
  Split-1 =>A and split- 2=>B

A=put pixel(x,y)=>(A,R,G,B)=>(A,C,M,0)
B= put pixel(x,y)=>(A,R,G,B)=>(A,Y,K,0)

2. Decryption

- Get color pixel from image of (x,y) position

```
IntpixA=A.getRGB(i,j);
IntpixB=B.getRGB(I,j);
```

- Calculate (C,M,Y,K) values from split A and B

```
c= (pixA>>16) && 0xff;
m= (pixA>>16) && 0xff;
y= (pixB>>16) && 0xff;
k= (pixB>>16) && 0xff;
```

- Convert CMYK values into ARGB

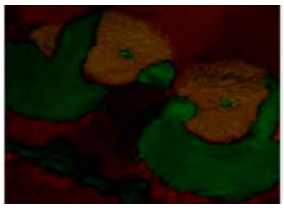
```
c=5*c;
m=5*m;
y=5*y;
k=5*k;
c=c/255f;
m=m/255f;
y=y/255f;
k=k/255f;
    r=255*(1-c)*(1-k);
g=255*(1-m)*(1-k);
b=255*(1-y)*(1-k);
```

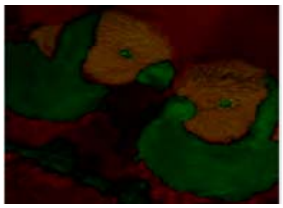
- Create original image from RGB values

Original image=put pixel(x,y)=>(a,r,g,b)=>(A,R,G,B)

IV. RESULTS

With the help of this algorithm visual cryptography is implemented. The image A is divided into two shares A1 and A2. Image A1 will contain the (A, C, M, 0), Y and K components as zero. Whereas share 2 A2 will contain (A, Y, K, 0),C, M components as zero





SHARE A1(A,C,M,0) SHARE A2(A,Y,K,0)

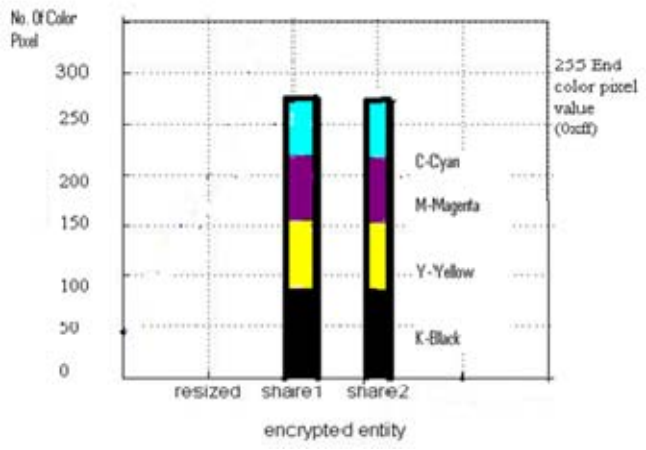
When share A1 and A2 are stacked together with the help of decryption algorithm, original image share A is obtained. This original share is displayed on the user's browser so that user will understand the particular server is genuine and hence user can enter their further credentials.

There are 2 graphs one for encryption & other for decryption.

In the first graph there is colored pixel range on Y axis & shares of the image on X axis. As in the encryption, image is divided into 2 shares so 2 shares are taken on X axis Share1 and Share2. And the maximum value for the colored pixel is 255 which are taken on the Y axis

In the second graph decryption is done. So both the shares are stacked into original image which is represented on x axis. And the maximum value for colored pixel is taken on y axis which is 255.

The system provides 100% result for the images size less than 2.5MB.As the Alfa (A) value increases the size image also increases. If the Alfa value is zero the image is fully transparent it its size is less. If value of Alfa is 100% then image becomes opaque. So the user should select the images whose size is less than 2.5MB to obtain the two shares of the image successfully. If user selects the image whose size is too large then the system might show insufficient heap space error. So to avoid such type of error image should be chosen withy minimum size.



. Figure3: Encrypted graph

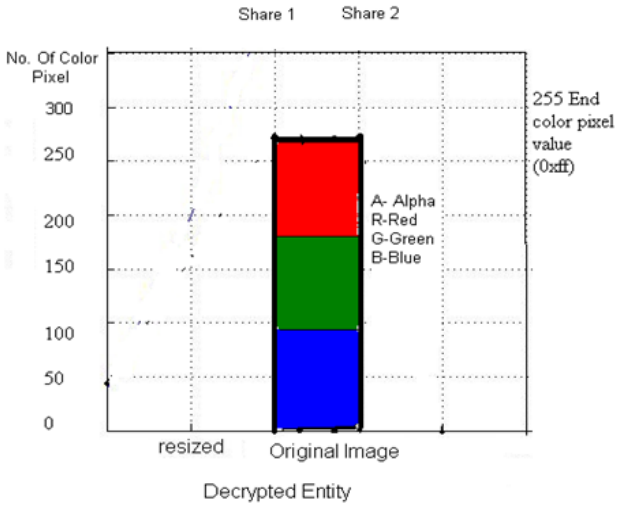


Figure 4: Decrypted graph

V. CONCLUSION

With the huge use of internet phishing attacks are so common because it can attack globally and capture and store the users' confidential information. This information is used by the attackers which are indirectly involved in the phishing process. Phishing is mainly done to gain the access to confidential information. Phishing websites as well as human users can be easily identified using our proposed "Secure Server Verification by using Encryption algorithm and Visual Cryptography". Thus with help of these techniques we can successfully help the users to identify the fake and genuine website.

ACKNOWLEDGMENTS

The authors gratefully acknowledge the contributions of Naor and A.Shamir for their work in the field of visual cryptography.

REFERENCES

[1] Gunter Ollamann, The phishing guide understanding and preventing phishing attacks, 2012.

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

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

[4] Luis von Ahn, CAPTCHA using Hard AI problem for security, Communication ACM, vol. 22, 1979, pp. 612-613.

[5] Matthew Dailey and Chanathip Namprempre, A Text-Graphics Character CAPTCHA for Password Authentication, CRC Press, Boca Raton, FL, 1997.

[6] Yang et al,Hashed Based Visual Cryptography Scheme For Image Aunthentication.

[7] Divya James and Mintu Philip,Visual Cryptography and Chaotic Image Encryption for the Security Of Biometric System.

[8] Komal Khandale, Mrunal Patil, Rohini Tale, Hemavati Tanpure, Data Hiding in color image for Secure Data Transmission with HbyRRBE

[9] Sozan Abdulla "New Visual Cryptography Algorithm For Colored Image" *JOURNAL OF COMPUTING*, vol. 2,ISSUE 4 APRIL 2010, ISSN 2151-9617.

[10] Md. Tanbin Islam Siyam, Kazi Md. Rokibul Alam and Tanveer Al Jami, International Journal of Computer Applications (0975 -8887)