Secure Server Verification using Visual Cryptography and RSA Algorithm

Shabbir Hussain[1], Mufazzal Hussain[2], Ganesh Thakur[3]
[123]Computer Science Department, G. H. Raisoni Institute of Engineering and Technology, Pune, India

Abstract: In the era of the internet, various online attacks have been increased and among them the most popular attack is phishing. Phishing is an attempt to thieve personal confidential information such as passwords, credit card information etc. from unsuspecting victims for identity theft, financial gain and other fraudulent activities. In this paper we have proposed a new approach named as "Secure Server Verification by Using RSA Algorithm and Visual Cryptography" to solve the problem of phishing. The Visual Cryptography Scheme is a secure method that encrypts a secret document or image by breaking it into shares. A distinctive property of Visual Cryptography Scheme is that one can visually decode the secret image by superimposing shares without computation. By taking the advantage of this property, third person can easily retrieve the secret image if shares are passing in sequence over the network. The project presents an approach for encrypting visual cryptographically generated image shares using Public Key Encryption. RSA algorithm is used for providing the double security of secret document. Thus secret share are not available in their actual form for any alteration by the adversaries who try to create fake shares. The scheme provides more secure secret shares that are robust against a number of attacks & the system provides a strong security for the handwritten text, images and printed documents over the public network.

Keywords*:* **Phishing, Visual Cryptography, RSA Algorithm, Security.**

PROBLEM DEFINITION

Phishers can fake the URL that appears in the address field at the top of user’s browser window and redirect him to another web site with the intention of performing fraud.
Fraudsters send e-mails with a link to a spoofed website asking you to update or confirm account related information. This is done with the intention of obtaining sensitive account related information like your Internet Banking User ID, Password, PIN, credit card / debit card / bank account number, card verification value (CVV) number, etc

INTRODUCTION

Online transactions are nowadays become very common and there are various attacks present behind this. In these types of various attacks, phishing is identified as a major security threat and new innovative ideas are arising with this in each second so preventive mechanisms should also be so effective .Thus the security in these cases be very high and should not be easily tractable with implementation easiness[2].
Today, most applications are only as secure as their underlying system. Since the design and technology of middleware has improved steadily, 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. The question is how to handle applications that require a high level of security.

Phishing is a form of online identity theft that aims to steal sensitive information such as online banking passwords and credit card information from users. 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” [3]. The conduct of identity theft with this acquired sensitive information has also become easier with the use of technology and identity theft can be described as “a crime in which the impostor obtains key pieces of information such as Social Security and driver's license numbers and uses them for his or her own gain”. So here introduces a new method which can be used as a safe way against phishing which is named as "Secure Server Verification using Visual Cryptography and RSA algorithm". As the name describes, in this approach website cross verifies its own identity and proves that it is a genuine website (to use bank transaction, E-commerce and online booking system etc.) before the end users and make the both the sides of the system secure as well as an authenticated one.

VISUAL CRYPTOGRAPHY

One of the best known techniques to protect data is cryptography. It is the art of sending and receiving encrypted messages that can be decrypted only by the sender or the receiver. Encryption and decryption are accomplished by using mathematical algorithms in such a way that no one but the intended recipient can decrypt and read the message.
Naor and Shamir [4] introduced the visual cryptography scheme (VCS) as a simple and secure way to allow the secret sharing of images without any cryptographic computations. An image is composition of pixels. The shared secret is an image composed of black and white pixels. Let each pixel be stored in d bits. Then 2d gray-leveled image can be shown by using a set of pixels. A recursive VC method proposed by Monoth et al., [5] is computationally complex as the encoded shares are further encoded into number of sub-shares recursively. Similarly a technique proposed by Kim et al., [6] also suffers from computational complexity, though it avoids dithering of the pixels. Most of the previous research work on VC focused on improving two parameters: pixel expansion and contrast [7], [8]. In these cases all participants will not present false or fake shares during the phase of recovering the secret image. Thus, the image shown on the stacking of shares is considered as the real secrete image.
VCS is a cryptographic technique that allows for the encryption of visual information such that decryption can be performed using the human visual system. We can achieve this by one of the following access structure schemes. [9][10]:

1. (2, 2)- Threshold VCS scheme- This is a simplest threshold scheme that takes a secret message and encrypts it in two different shares that reveal the secret image when they are overlaid.

2. (n, n) -Threshold VCS scheme-This scheme encrypts the secret image to n shares such that when all n of the shares are combined will the secret image is revealed.
3. (k, n) Threshold VCS scheme- This scheme encrypts the secret image to n shares such that when any group of at least k shares are overlaid the secret image will be revealed.

In the case of (2, 2) VCS, each pixel P in the original image is encrypted into two sub pixels called shares. Figure.1 denotes the shares of a white pixel and a black pixel. Note that the choice of shares for a white and black pixel is randomly determined (there are two choices available for each pixel). Neither share provides any clue about the original pixel since different pixels in the secret image will be encrypted using independent random choices. When the two shares are superimposed, the value of the original pixel P can be determined. If P is a black pixel, we get two black sub pixels; if it is a white pixel, we get one black sub pixel and one white sub pixel.

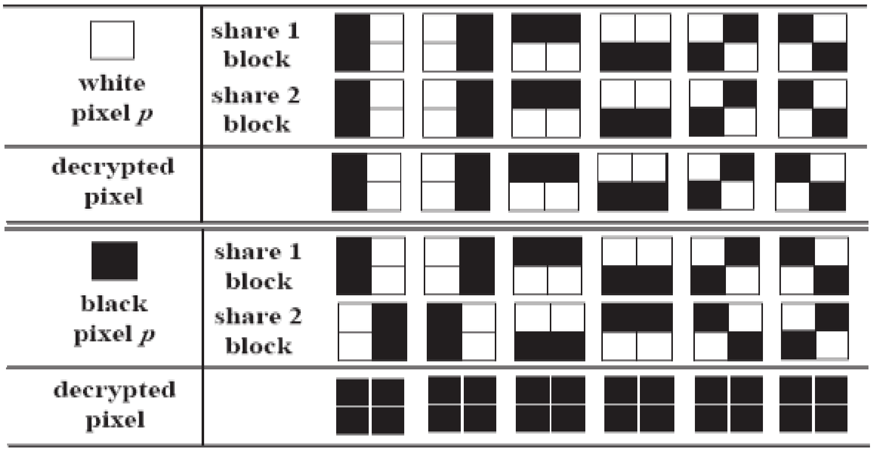

Fig 1: 2-out-of-2 VCS scheme with 2 sub pixel construction.

In the case of (2, 2) VCS, each pixel P in the original image is encrypted into two sub pixels called shares. Fig.1 denotes the shares of a white pixel and a black pixel. Note that the choice of shares for a white and black pixel is randomly determined (there are two choices available for each pixel). Neither share provides any clue about the original pixel since different pixels in the secret image will be encrypted using independent random choices. When the two shares are superimposed, the value of the original pixel P can be determined. If P is a black pixel, we get two black sub pixels; if it is a white pixel, we get one black sub pixel and one white sub pixel. [1]
Naor & Shamir [2] describe that many extension from his basic work can be possible. Further he extends his work with following suggestions: Use partially filled circles to represent grey values. It is mention below. In the following Figure.

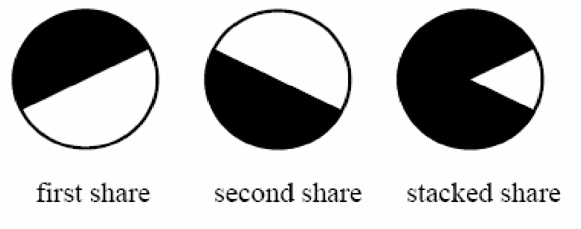

Fig 2: Extended VC scheme

Image Scaling Algorithm

Scaling of image is one frequently used task in any decent image processing software. Even if you say you don't, the software does. Ever zoomed your image for a closer look? Or used that convenient thumbnail preview? It all happens there, regardless of what you may be thinking. The principle in image scaling is to have a reference image and using this image as the base to construct a new scaled image. The constructed image will be smaller, larger, or equal in size depending on the scaling ratio. When enlarging an image, we are actually introducing empty spaces in the original base picture. From the image below, an image with dimension (w1 = 4, h1 = 4) is to be enlarged to (w2 = 8, h2 = 8). The black pixels represent empty spaces where interpolation is needed, and the complete picture is the result of nearest neighbor interpolation.

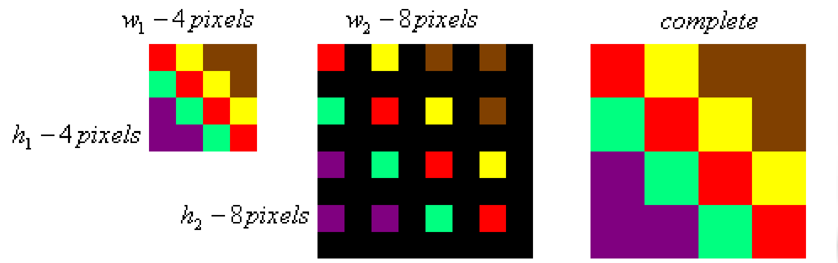

Fig 3: Image Scaling Algorithm

Scaling algorithm is to find appropriate spot to put the empty spaces inside the original image, and to fill all those spaces with livelier colors. For the nearest neighbor technique, the empty spaces will be replaced with the nearest neighboring pixel, hence the name. This results in a sharp but jaggy image, and if the enlarge scale is two; it would seems each pixel has doubled in size. Shrinking, in the other hand involves reduction of pixels and it means lost of irrecoverable information. In this case scaling algorithm is to find the right pixels to throw away. Good scaling algorithm is one that can do up and down scaling without introducing too many conditions (the ifs) in its implementation code, even better if there is none. Nearest neighbor is a no if, up down scaling algorithm. What information it needs are both the horizontal and vertical ratios between the original image and the (to be) scaled image. Consider again the diagram above, w1 and h1 are the width and height of an image, whereas w2 and h2 are the width and height when enlarged (or shrinked). Calculating the ratio for both horizontal and vertical plane is given by, of course the not equal to zero is a condition, and will eventually be translated as ifs in coding implementation. However, to be fair no algorithm is needed if one intends to shrink image to zero size, who the hell wants to do that?
Once ratio has been calculated prepare a buffer, or array, or whatever that can store information for the to be constructed image. The size should be enough to store w2*h2 of pixels.

RSA ALGORITHM

The RSA algorithm was publicly described in 1978 by Ron Rivest, Adi Shamir, and Leonard Adleman at MIT; the letters RSA are the initials of their surnames, it is an algorithm for public-key cryptography. It is the first algorithm known to be suitable for signing as well as encryption, and was one of the first great advances in public key cryptography. RSA is widely used in electronic commerce protocols, and is believed to be secure given sufficiently long keys and the use of up-to-date implementations.

Among the various public key cryptography algorithms, the RSA cryptosystem is the best known, most versatile, and widely used public key cryptosystem today.

Key Generation Algorithm

The RSA algorithm involves three steps: key generation, encryption and decryption.

Key generation

RSA involves a public key and a private key. The public key can be known to everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted using the private key. The keys for the RSA algorithm are generated the following way:

1. Choose two distinct prime numbers p and q.

For security purposes, the integer p and integer q should be chosen at random, and should be of similar bit-length.

2. Compute $n = pq$.
n is used as the modulus for both the public and private keys

3. Compute $\varphi(n) = (p - 1)(q - 1)$, where φ is Euler's totient function.

4. Choose an integer e such that $1 < e < \varphi(n)$ and greatest common divisor of $(e, \varphi(n)) = 1$; i.e., e and $\varphi(n)$ are co-prime.
e is released as the public key exponent.
e having a short bit-length and small Hamming weight results in more efficient encryption.

5. Determine d as:
i.e., d is the multiplicative inverse of e mod $\varphi(n)$.
This is more clearly stated as solve for d given $(de) = 1 \bmod \varphi(n)$
d is kept as the private key exponent.

By construction, $d*e= 1 \bmod \varphi(n)$. The public key consists of the modulus n and the public (or encryption) exponent e. The private key consists of the modulus n and the private (or decryption) exponent d which must be kept secret. (p, q, and $\varphi(n)$ must also be kept secret because they can be used to calculate d.)

Encryption

Sender A does the following:-

• Obtains the recipient B's public key (n, e).

• Represents the plaintext message as a positive integer m such that

Computes the cipher text.

• Sends the cipher text c to B.

Decryption

Recipient B does the following:

- Alice can recover from by using her private key exponent via computing

- Extracts the plaintext from the integer representative m.

CURRENT METHODOLOGY

We often do online transactions like mobile recharge, online shopping from websites which are registered to the bank. When the end user wants to access his confidential information online (in the form of money transfer or payment gateway) by logging into his bank account or secure mail account, the person enters information like username, password, credit card no. etc. on the login page. But quite often, this information can be captured by attackers using phishing techniques (for instance, a phishing website can collect the login information the user enters and redirect him to the original site). There is no such information that cannot be directly obtained from the user at the time of his login input.

PROPOSED METHODOLOGY

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

This methodology is divided into two phases:

Registration phase
In the registration phase, user selects a random image. Then using cryptography convert the image into shares on the client side. Send one share to the server for future use and other remains with the user. User can change the share stored on server at any time in case he feels the share is compromised. The trusted server stores unique shares for every user.

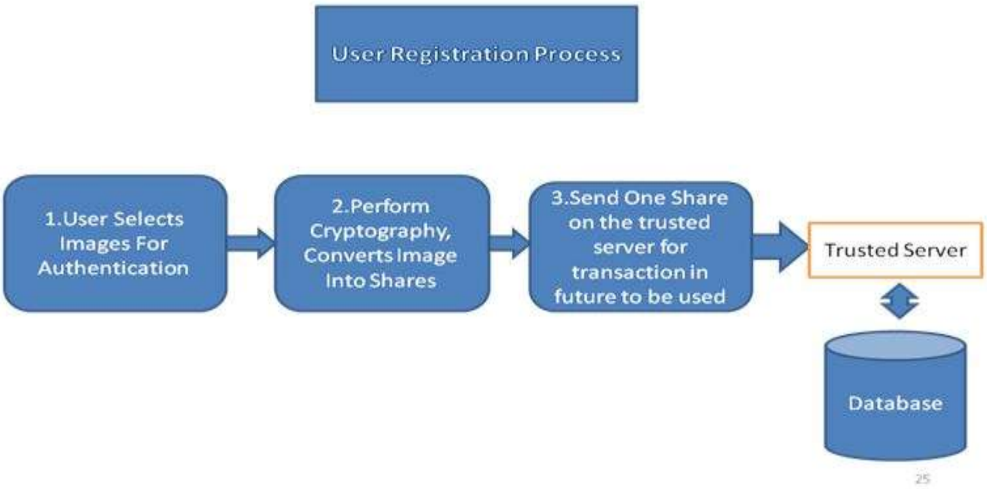
User Registration Process
1.User Selects Images For Authentication
2.Perform Cryptography, Converts Image Into Shares
3.Send One Share on the trusted server for transaction in future to be used
Trusted Server
Database
25

Fig 4: Registration 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). Create random public key and private key on the client side using cryptography .Then send the key to trusted server. Using public key encrypt the share2 on the server side. If it is a trusted server then the public key and the encrypted share2 is send to user. Then at client-side it is decrypted using private key. The user's share and the share received from the server under test are stacked together to produce the image. If image obtained is original then the server under test is verified secure or the website is not phishing else it is a phishing site.

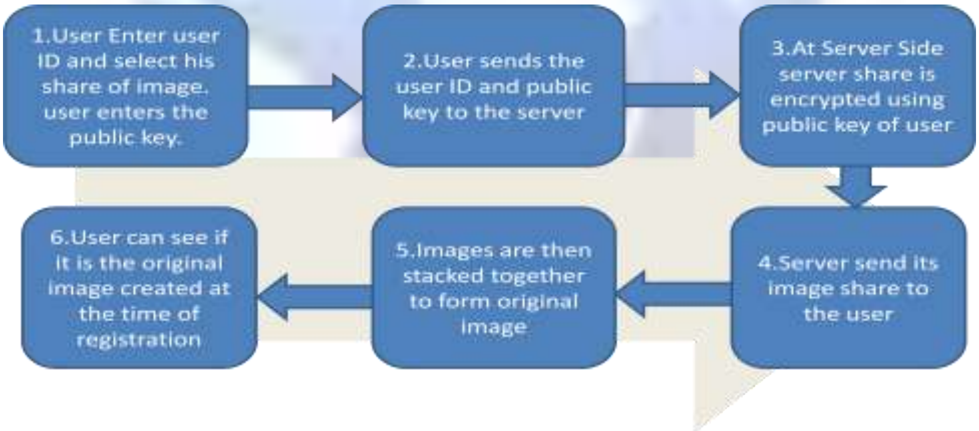
1.User Enter user ID and select his share of image. user enters the public key.
2.User sends the user ID and public key to the server
3.At Server Side server share is encrypted using public key of user
4.Server send its image share to the user
5.Images are then stacked together to form original image
6.User can see if it is the original image created at the time of registration

Fig 5: Login Phase

IMPLEMENTATION AND ANALYSIS

The proposed methodology is implemented using J2EE (Servlets as a Server side technology). Figure 5 shows the result of creation and stacking of shares.

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.

In previous research of Anti-phishing technique [2], as captcha is generated on server side, client can't change it, in order to provide security. However, in mentioned approach it is possible for client to change image when needed. Also RSA public crypto-system is more secure.

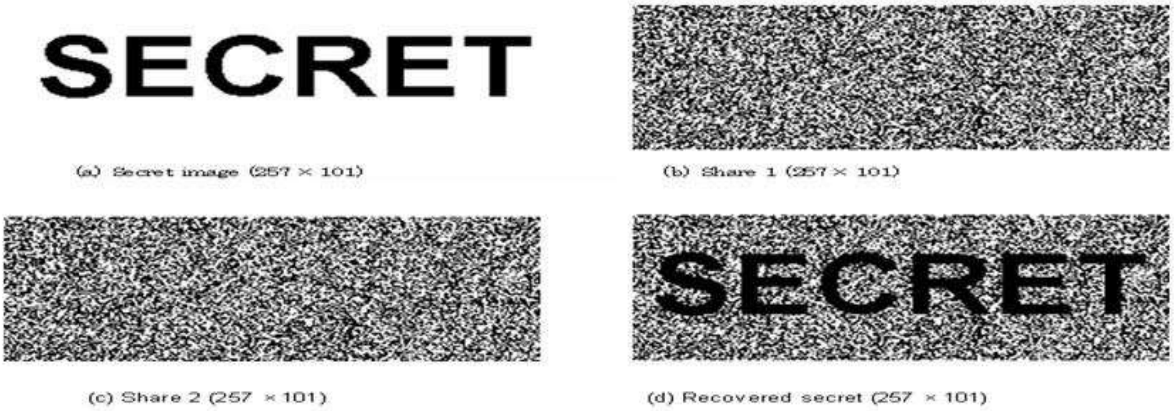
SECRET
(a) Secret image (257 × 101)
(b) Share 1 (257 × 101)
(c) Share 2 (257 × 101)
(d) Recovered secret (257 × 101)
SECRET

Fig 6: Result of a size invariant (2, 2) scheme

CONCLUSION

As implementation is done using RSA, decryption is not possible without private key. Thus this approach can be used in any online transaction, it is secure and provides authentication.

REFERENCES

[1]. IJERT paper for Secure Server Verification using RSA algorithm and Visual Cryptography, vol-2, issue-4, April 2013.
[2]. Ollmann G., the Phishing Guide Understanding & Preventing Phishing Attacks, NGS Software Insight Security Research.
[3]. Divya James, Mintu Philip, A Novel Anti Phishing framework based on Visual Cryptography, in Proceedings of IEEE International Conference on Information Technology, 2012.
[4]. M. Naor and A. Shamir, Visual cryptography, in Proc. EUROCRYPT, 1994, pp. 1–12.
[5]. T. Monoth and A. P. Babu, .Recursive Visual Cryptography Using Random Basis Column Pixel Expansion, in Proceedings of IEEE International Conference on Information Technology, 2007, pp. 41-43.
[6]. H. J. Kim, V. Sachnev, S. J. Choi and S. Xiang. An Innocuous Visual Cryptography Scheme, in Proceedings of IEEE-8th International Workshop on Image Analysis for Multimedia Interactive Services, 2007.
[7]. C. Blundo and A. De Santis, .On the contrast in Visual Cryptography Schemes, in Journal on Cryptography, vol. 12, 1999, pp. 261-289.
[8]. P. A. Eisen and D. R. Stinson, .Threshold Visual Cryptography with specified Whiteness Levels of Reconstructed Pixels, Designs, Codes, Cryptography, vol. 25, no. 1, 2002, pp. 15-61.
[9]. E. R. Verheul and H. C. A. Van Tilborg, .Constructions and Properties of k out of n Visual Secret Sharing Schemes. Designs, Codes, Cryptography, vol. 11, no. 2, 1997, pp. 179-196.
[10].Ching-Nung Yang, Senior Member, IEEE, Hsiang-Wen Shih, Chih-Cheng Wu, and Lein Harn, “k Out of n Region Incrementing Scheme in Visual Cryptography”, vol. 22, no. 5 MAY 2012.