www.ijecs.in

International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 6 Issue 4 April 2017, Page No. 21188-21191
Index Copernicus value (2015): 58.10 DOI: 10.18535/ijecs/v6i4.67

Secure Authentication using Image Processing through Visual Cryptography

Mary Jolve. J
[1]Assistant Professor, Department of computer Application,
St. Thomas 'College (Autonomous), Thrissur -680001, Kerala, India
jolvejoyanthikadan@gmail.com

Abstract: ***Authentication is used by a server when the server needs to know exactly who is accessing their information or site. In this process, the user or computer has to prove its identity to the server or client. Usually, authentication by a server entails the use of a user name and password or through cards, retina scans, voice recognition, and fingerprints. An effective method for securely transmitting files, documents and images are found in the field of Visual Cryptography (VC). Visual cryptography method is a cryptographic technique which allows visual information (e.g. printed text, handwritten notes, and images etc.) to be encrypted in such a way that the decryption can be performed by the human visual system (HVS), without the aid of computers. This study focuses on securing a file or document through CAPTCHA images using image processing. The study is to be carried out in two phases where the Phase I would comprise Registration Phase and, Login Phase would be carried out in Phase II.***

Keywords: Visual Cryptography, Image CAPTCHA, Blowfish, Shares

1. Introduction

Internet is being used for several activities like communication, e-commerce, education, and entertainment by great range of user. Today, we use the Internet for almost everything, and for many people it would be impossible to imagine life without it. In today's digital world, information sharing and transfer of file, document etc. has increased exponentially. The threat of an intruder accessing secret document has been a challenging war for the data communication experts. With the rapid growth of Internet facilities and advancement of network topology, multimedia information is transmitted over the Internet conveniently. Various confidential data such as military maps, credit card details, passwords and commercial identification are transmitted over the Internet. The normal way of securing these information like setting username and password has been outdated. The most prominent way of securely transmitting these documents are found in the field of Visual Cryptography (VC).

Visual Cryptography (VC) is a special encryption technique used to encrypt images in such a way that it can be decrypted by the human visual system if the correct key images are matched. It can be used to protect biometric templates in which decryption does not require any complex computations. This technique was introduced by Moni Naor and Adi Shamir and developed it in 1994. They demonstrated a visual secret sharing scheme, where an image was broken up into n shares so that only someone with all n shares could decrypt the image, while any n − 1 shares revealed no information about the original image. Each share was printed on a separate transparency, and decryption was performed by overlaying the shares. When all n shares were overlaid, the original image would appear.

This technique is being used for secretly transfer of images in army, hand written documents, financial documents, text images, internet- voting etc. The image that we use here to encryption is an automated generated CAPTCHA image. CAPTCHAs are challenge puzzles used to determine whether a user is human or not. It is a software program that can generate and grade tests that most humans can pass but current computer programs cannot pass. It stands for Completely Automated Public Turing Test to Tell Computers and Human Apart, and Public means that the code and the data used should be publicly available. For instance, email provider services such as Hotmail and Yahoo provide a CAPTCHA test as a final step of the registration process to stop bots from subscribing and using their resources for spam distribution.

In this research paper 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 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. Once the original CAPTCHA is revealed to the user it can be used as the password. The study is to be carried out in two phases: one is registration phase and the other is login phase.

2. Methodology

Visual Cryptography techniques are considered for security of image in terms of encrypting it with the help of symmetric key, hence if someone access all the shares in unauthorized way, he/she can't decrypt it completely without symmetric key. In the proposed system we use this technique for authentication purpose. It is carried out in two phases:

2.1 Registration Phase

In the registration phase, a key string (password) is asked from the user at the time of registration for the secure file. The key string can be a combination of alphabets and numbers to provide more secure environment. According to the key given by the user this string is concatenated with randomly generated string in the server and an image CAPTCHA is generated**.** By this dynamic generation the theft by camera can be easily avoided**.**

This phase has three main parts: (1) Image CAPTCHA creation, (2) Image CAPTCHA encryption, and (3) Splitting the image.

2.1.1 Image CAPTCHA creation

Image CAPTCHA is automatically generated. It is a text which consists of the characters number or alphanumeric characters in a range of "ABDEFHKLMNPRSTUVWXZabdefgikmnopqrstuvxyz02 3456789". The text is composed of five characters, and each character has its own bending and size value. Characters are split into several parts and each part is given randomly a rotation value in a certain angle domain interval such as: [-1', 1'], [-3', 3'], [-5', 5']. Image parts are also split individually with random width and height values. Rotation in character parts provides confusion in recognizing the exact one.

2.1.2 Image CAPTCHA encryption

In order to encrypt the image CAPTCHA we implement Blowfish algorithm. Bruce Schneier developed Blowfish to be a publicly available cryptographic algorithm with the potential to replace DES. Schneier also encouraged others to evaluate the performance and security of this algorithm. Blowfish is a 64-bit symmetric block cipher that uses a variable-length key from 32 to 448-bits (14 bytes). The algorithm was developed to encrypt 64-bits of plaintext into 64-bits of cipher text efficiently and securely. The elementary operators of Blowfish algorithm include table lookup, addition and XOR to minimize the time required to encrypt and decrypt data on 32-bit processors. The table includes four S- boxes and a P-array.

As with DES, Blowfish incorporates a 16 round Feistel network for encryption and decryption. But during each round of Blowfish, the left and right 32-bits of data are modified unlike DES which only modifies the right 32-bits to become the next round's left 32-bits. Blowfish incorporated a bitwise exclusive-or operation to be performed on the left 32-bits before being modified by the F function or propagated to the right 32-bits for the next round. It also incorporated two exclusive-or operations to be performed after the 16 rounds and a swap operation. This operation is different from the permutation function performed in DES.

Encryption Process:

Data image as a plaintext and the encryption key are two inputs of encryption process. In this case, original image data bit stream is divided into the blocks length of Blowfish algorithm. Image header is excluded to encrypt and the start of the bitmap pixel or array begins right after the header of the file. The byte elements of the array are stored in row order from left to right with each row representing one scan line of the image and the rows of the image are encrypted from top to bottom.

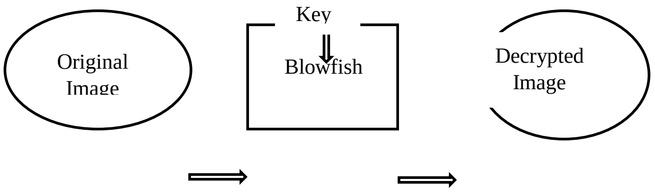

Figure 1: Encryption Process

Decryption Process:

The encrypted image is divided into the same block length of Blowfish algorithm from top to bottom. The first block is entered to the decryption function and the same encryption key is used to decrypt the image but the application of sub keys is reversed. The process of decryption is continued with other blocks of the image from top to bottom.

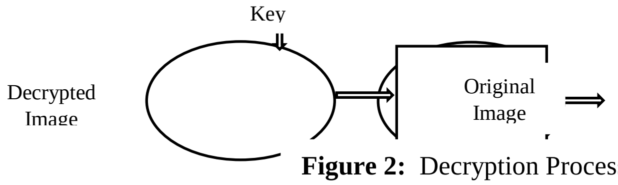

Figure 2: Decryption Process

The basic algorithm for Blowfish is illustrated as follows:

```
Divide image I into two 32-bit halves IL and IR
For i=1 to 16:
IL = IL Pi
IR = F (IL) IR
Swap IL and IR
End for
Swap IL and IR
IR = IR P17
IL = IL P18
Recombine IL and IR
Output I (64-bit data block: cipher text)
```

For decryption, the same process is applied, except that the sub-keys Pi must be supplied in reverse order. The nature of the Feistel network ensures that every half is swapped for the next round.

2.1.3 Splitting the image

The encrypted image has been split into two component images. Each component image has a pair of pixels for every pixel in the original image. These pixel pairs are shaded black or white according to the following rule: if the original image pixel was black, the pixel pairs in the component images must be complementary; randomly shade one ■□, and the other □■. When these complementary pairs are overlapped, they will appear dark gray. On the other hand, if the original image pixel was white, the pixel pairs in the component images must match: both ■□ and both □■. When these matching pairs are overlapped, they will appear light gray. Thus we generate two shares i.e. Share 1and Share 2 and they are shown in the figure below:

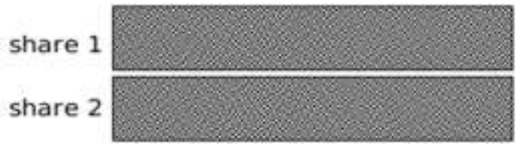

Figure 3: Share generation

However, considered by itself, a component image reveals no information about the original image; it is indistinguishable from a random pattern of ■□ / □■ pairs. So when the two component images are superimposed, the original image appears

Then one of the share is kept with the user and the other share is kept in the server. The user's share and the original image CAPTCHA is 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 because the image CAPTCHA is used as the password later. After the registration, the user can change the key string dynamically when it is needed.

2.2 Login Phase

When the user logs in by entering his confidetial 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. 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

3 Simulation and Result

In this paper we have simulated the image processing part of Encryption and decryption in DOTNET platform. Image CAPTCHA is automatically generated. Firstly we would be obtaining the matrix and pixels of the CAPTCHA & then we would be encrypting the image matrix using blowfish algorithm. . The text in the image will be hidden using a specific key and image hidden with a data is encrypted and decrypted. When the key and the Share 2 images are checked and compared, the file will be downloaded.

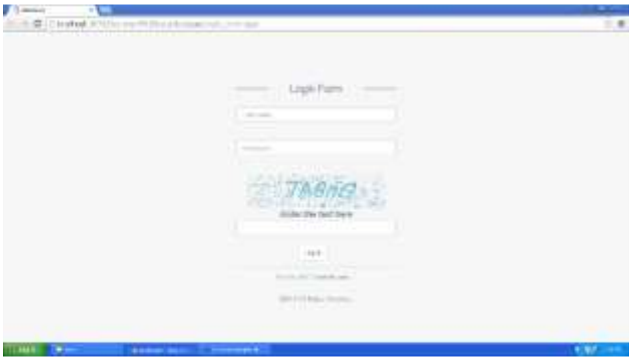

Figure 4: Login Form

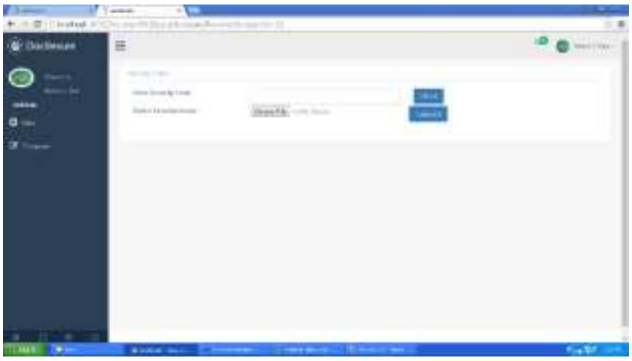

Figure 5: Compare and Check Process

When the secret key and Shares are compared and checked the download button will be visible. When you click the download button the file will be downloaded. If a mismatch is found the button will be hidden and a message box appears in order to check the secret key.

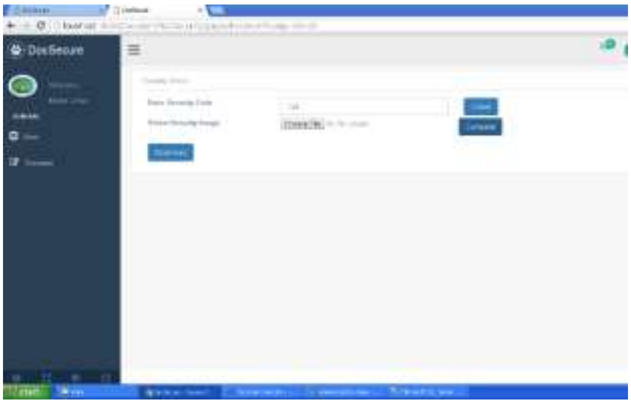

Figure 6: Downloading file form

4 Conclusion

Visual Cryptography is a special kind of cryptographic scheme where the decryption of the Encrypted secret is done by the human vision and not by complex mathematical calculations. Here we implemented image CAPTCHA. In this paper we have proposed two secret sharing visual cryptographic scheme for black and white images in which encryption of the image. This scheme can be extended for colored images and for hiding multiple secrets. Instead of symmetric key, stream cipher can be applied for encrypting image.

One of the reasons for this is the difficulty of use in practice. The shares of visual cryptography are printed on transparencies which need to be superimposed. However, it is not very easy to do precise superposition due to the fine resolution as well as printing noise. Furthermore, many visual cryptography applications need to print shares on paper in which case scanning of the share is necessary. The print and scan process can introduce noise as well which can make the alignment difficult.

5 Acknowledgement

I am extremely grateful to The Deputy Secretary, University Grants Commission, South Western Regional Office, and Bangalore for sanctioning Minor Research Project.

6 Reference

1. Ibrahim Furkan Ince, Ilker Yengin, Yucel Batu Salman, "DESIGNING CAPTCHA ALGORITHM: SPLITTING AND ROTATING THE IMAGES AGAINST OCRs", Int., Conf., IEEE Computer Society, pp. 596-601, 2008

2. Renu Poriye and Dr S. S Tyagi"Secret Sharing Using Visual Cryptography", IJRSCSE, Vol 1, No. 4, pp. 46-2, August 2014,

3. Malyala Sravya Lakshmi and Gadi Lava Raju, "A Comprehensive Study on Visual Cryptography", COMPUSOFT, Int, Vol 3, No. 3, pp. 1065-1069, August-2014

4. Pia Singh and Prof. Karamjeet Singh, "IMAGE ENCRYPTION AND DECRYPTION USING BLOWFISH ALGORITHM IN MATLAB", International Journal of Scientific & Engineering Research, Vol 4, No. 7, pp. 150-154,July-2013.

5. Atul, Kahate, Cryptography and Network Security,(Second Edition 2008)

6. Bruce Schneier. The Blowfish Encryption Algorithm Retrieved October 25, 2008, http:// www. schneier.com/ blowfish.html.

7. Kessler G. C., an Overview of Cryptography”- http://www.garykessler.net/library/crypto.html.28 April 2013.

8. Naor M., Shamir A., Visual cryptography, Advances in Cryptology EUROCRYPT ‟94. Lecture Notes in Computer Science, 1995, pp. 1-12.

9. Singhal, Nidhi and Raina, J P S. “Comparative Analysis Of AES and RC4 Algorithms for Better Utilization”, International Journal of Computer Trends and Technology, ISSN: 2231-280, July to Aug Issue 2011.

10. Jena D., Jena S. K., A Novel Visual Cryptographic Scheme,” IEEE, 2008, pp. 207–211