Volume 4, Issue 12, December 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Proposal to Secure Visual Cryptographic Shares of Secret Image using RSA

Siddaram Shetty*, Minu P. Abraham
Dept. of Computer Science and Engg,
NMAMIT, Nitte, India

Abstract— A Visual Cryptography is one of the secure techniques that can be used to encrypt a secret document or image by breaking down to shares. In the technique of Visual Cryptography, anyone can visually recover or decode the original image (i.e. secret image) by overlapping the shares without any computation; this property made the Visual Cryptography distinctive from existing traditional secure methods. In order to take the advantage of this, the third party can recover the secret image if the shares of secret image are passing in sequence over a network. This paper presents an approach to encrypt a generated image share of Visual Cryptography using Public key Encryption. We used RSA algorithm in order to provide the double security of the document. Hence, shares of secret image are not exist in their actual form for third parties (those who try to create fake shares) to make alteration. The proposed scheme provides shares that are more secure and robust against number of attacks. This scheme also provides strong security for the handwritten text, documents and images that exists in the public network.

Keywords— Visual Cryptography, Encryption, Decryption, VC Shares, Information Security

I. INTRODUCTION

In recent years, information sharing and transfer has been increased rapidly. Hence, there is threat of third party accessing secret information has been an ever existing concern for the data communication experts. With the rapid advancement of network topology, multimedia information is transmitted over the Internet conveniently. Many confidential data items such as military maps and commercial identification are sent over the internet. While using secret documents (images, text etc.) for sending over the network, the issue to be taken into consideration is the security, since there is a chance of stealing the secret information by the hackers due to weak link in the public network. In order to deal with the security issue of secret images, we need to develop an appropriate secure algorithm by which we can secure our data over the internet. With the help of Visual Cryptography, the system visual information can be secure over the internet.

Our proposed method combines the advantages of both Visual Cryptography and Public Key Cryptography. This proposed method improves the issue of security shares of Visual Cryptography by encrypting with Public Key Cryptography [10], which provides much security for the transfer of secret information in form of images, printed text and hand written material.

Visual Cryptography (VC) is one of the encryption techniques that is used to encrypt secret images in such a way that it can be decrypted by the human visual system if the correct key images are used. The technique was first proposed by Moni Naor and Adi Shamir [2] in 1994. According to them Visual Cryptography is a technique of encrypting a secret image into shares such that stacking a sufficient shares of secret image reveals the original image. Shares are usually binary images presented in transparencies. Unlike existing traditional cryptographic methods, Visual Cryptography needs no complicated computation for recovering the secret image. The method of decryption involves simply stacking the shares and view the original (secret) image that appears on the stacked shares. The technique Visual Cryptography is being used for secret transfer of images in military, hand written documents, text images etc.

The shares of Visual Cryptography exist in their normal form during transmission in sequence over the network. However, directly third party cannot predict the secret information with only single share, but there is a chance of recovering the secret image if hackers are able to collect all the shares that are passing in sequence over the network. Thus to get out of this, we need to improve the security of shares. Due to same reason we have used both Public Key Cryptography and Visual Cryptography so that even if hackers are able to get all the shares but they cannot retrieve the original secret without the access of private key.

II. APPLICATIONS OF VISUAL CRYPTOGRAPHY

There are many applications incorporated with the Visual Cryptography Scheme. Two main applications are discussed in this section.

A. Electronic-Balloting System:

Dilemma et al [3] proposed a secret - Ballot Receipts system that is based on (2, 2) binary VCS. It generates an encrypted receipt to every voter which allows them to verify the election outcome even if all election computers and records were

compromised. At the polling station, the voter will get a double - layer receipt that prints his/her voting decision. Then the voter will be asked or allowed to give one of the layers to the poll worker who will destroy it immediately with a paper shredder. Then the remaining another layer will now become unreadable.

B. Encrypting Financial Documents:

The VCS principle can also be applied in transmitting confidential financial documents over Inter net. Visual Cryptography can be used to encode the original document with a specified (k, n) Visual Cryptography Scheme, then send each of the encoded n shares separately through Emails or FAX to the recipient. The process of decoding only involves bitwise OR operation on all shares in the specified directory, and no need of extra effort of cryptographic computation. Any third party who intercepts only m of n shares where m < k will not be able to gain any information about the financial document.

III. RELATED WORK

A large number of researches have been carried out in this area to increase the security & visual quality of the secret image. Some of them are listed here:

Néelima Guntupalli et al [4] presented survey on various Schemes of Visual Cryptography and established the conceptual knowledge about Visual Cryptography.

Debashish Jena, **Sanjay Kumar Jena** [5] implemented Data Hiding using Conjugate Ordered Dithering (DHCOD) algorithm for generating the shares. A dithered halftone image generated by the cover image was the first share. For second share, some noise was added to the secret image and converted it to the binary image after that using share 1 and binary image they generated the second share. The original image (secret image) has been recovered with the simple AND operation of share 1 and share 2. Share generation process is made complicated by this method.

Padhmavati, P. Nirmal Kumar, **M. A. Dorai Rangaswamy** [6] generated shares first by Visual Cryptography VC (2, 2) scheme. Then both shares were embedded into the cover images with the help of watermarking. For reveal of secret image, the extraction process was used to extract the shares from the embedded images. At the end both shares were overlapped to reveal the secret image. Two cover images have been used to hide the shares which require extra memory space.

Wei-Qi-Yan, Duo Jin, Mohan S Kankanhalli [7] suggested a solution for superimposition of two shares. Some alignment marks are used in Walsh transform domain. It is always beneficial to use the scheme developed by this author, because in VC decryption stacking of two shares is mandatory and without exact alignment retrieval is not possible.

Vaibhav Choudhary et al [8] discussed an Improved Pixel Sieve Method for Visual Cryptography used an additional sieve to generate shares. In this scheme Secret is hidden properly using this scheme but efficiency of this scheme cannot be evaluated as decryption algorithm and the results of retrieval have not been shown in the paper.

IV. PROPOSED SCHEME

The proposed scheme generates the shares of Visual Cryptography using basic Visual Cryptography model and then encrypt both shares using RSA algorithm of Public Key Cryptography, in order to secure the secret shares and shares must be protected from the vicious opponent who may try to alter the bit sequences to form the fake shares. During the phase of decryption, secret shares are extracted by RSA decryption algorithm & stacked to reveal the secret image. The methodology of proposed scheme is given below [1].

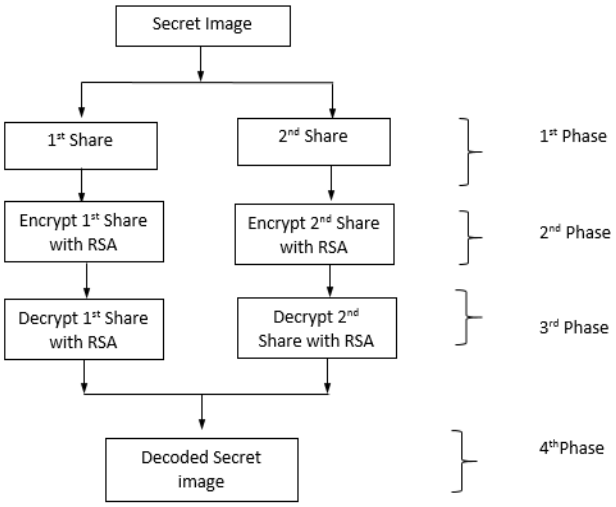

Fig: Methodology of the Proposed Scheme

A. 1st Phase Generating the Shares of Secret Image: In this phase implementation of Visual Cryptography is done. It involves the creation of shares from secret image using Visual Cryptography (2, 2) scheme. Very first the secret image is taken and is converted to a binary image then every pixel in the secret image is divided into eight sub pixels, four pixels in each share by selecting the pixel encoding scheme in a random manner.

B. *2nd Phase Encrypting the generated Shares:* This is the second phase of proposed approach which will encrypt shares that are generated in the first phase. The algorithm RSA is used to encrypt the shares. First we have generated the key for RSA and then we perform the encryption. Thus, encrypted shares are the result of 2nd phase.

C. 3rd Phase *Decrypting the Shares using RSA:* The process of decrypting the shares takes place at destination side. Using RSA decryption algorithm, we again convert the encrypted shares into their actual form, which were encrypted at the sender side

D. 4th Phase Visual Cryptography decryption: In the last phase, the process of Visual Cryptographic decryption is performed. Here by applying the binary XOR operation, on both decrypted shares, we are going to recover the original secret image.

Characteristics of Visual Cryptography
Following are some of the advantages of Visual Cryptography
(1). Complete Security
(2). Because of the binary property, it has robust method against the loss of compression and distortion.
(3). No need of Computer for decryption.

Weakness of Visual Cryptography
(1). The resolution of the restored secret image is lower than the original secret image

V. CONCLUSION AND FUTURE SCOPE

Providing security to the confidential data shared in day to day life is an important issue in real life. Visual cryptographic scheme, which can decrypt secrete images without any cryptographic computations. The proposed scheme is perfectly secure and very easy to implement with low computation cost. In our proposed scheme, first the secret image is taken and then it is divided into shares after converting it into binary image, then the shares of binary image are encrypted and decrypted using RSA algorithm, because of this even if the third party or intruder, once getting all the shares, he/she can't get back the original secret image without availability of the private key. We can notice that there are many possible extensions exist as the visual quality & size of retrieved image. We can use following as some of the future extensions.

1. We can use colour image in place of binary image and then generate the shares using Visual Cryptography method.
2. Encrypted shares can compressed in order to reduce the bandwidth requirement.

We can implement this type of system in various fields like in Military, Defence, and other places where the confidentially of data should be must.

REFERENCES

[1] Kulvinder Kaur, 2013 3rd IEEE International Advance Computing Conference (IACC) "Securing Visual Cryptographic Shares using Public Key Encryption".
[2] M. Naor and A. Shamir "Visual Cryptography". Advances in Cryptology EUROCRYPT '94. Lecture Notes in Computer Science, (950):1–12, 1995.
[3] D Chaum, Secret-ballot receipts: True voter-verifiable elections, IEEE Security and Privacy, 2004, 38-47.
[4] Neelima. Guntupalli et al, "An Introduction to Different Types of Visual Cryptography Schemes", *International Journal of Science and Advanced Technology* (ISSN 2221-8386), Volume 1 No 7 September 2011, PP 198- 205.
[5] D. Jena and S. Jena "A Novel Visual Cryptography Scheme". 978- 07695- 3516-6/08 © 2008 IEEE DOI 10.1109/ICACC.2009.109.
[6] B. Padhmavati, P. Nirmal Kumar, M. A. Dorai Rangaswamy "A Novel Scheme for Mutual Authentication and Cheating Prevention in Visual Cryptography Using Image Processing". Department of Computer Science & Engineering, Easwari Engineering College, Chennai, DOI: 02, ACS.2010.01.264, 2010 *ACEEE*.
[7] Wei-Qi Yan, Duo Jin, Mohan S Kankanhalli "Visual Cryptography for print and scan applications" School of Computing, National University of Singapore, Singapore 117543
[8] Vaibhav Choudhary "An Improved Pixel Sieve Method for Visual Cryptography" *International Journal of Computer Applications*, (0975 – 8887) Volume 12– No.9, January 2011.
[9] Ms. Kirti Mhamunkar "Securing White and Black Image Using Visual Cryptographic Shares" International Journal for Research in Advent Technology, Volume 2, Issue 1, Jan 2014.
[10] Behrouz A. Forouzon, "Cryptography & Network Security" 4th Edition

