ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

A Secure Visual Cryptography Scheme for Sharing Secret Image using RSA

Siddaram Shetty[1], Minu P Abraham[2]

PG Scholar, Dept. of CSE, NMAMIT, Nitte, Udupi, Karnataka, India[1]

Asst. Professor, Dept. of CSE, NMAMIT, Nitte, Udupi, Karnataka, India[2]

ABSTRACT: Visual Cryptography is one of the techniques that can be used for securing image-based secrets. The scheme Visual Cryptography is used to encrypt a secret image or document by breaking into shares. In order to take the advantage of this property, 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 generated image shares 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 documents, handwritten-text, images etc. that exists in the public network.

KEYWORDS: Visual Cryptography, Encryption, Decryption, Information Security, VC Shares.

I. INTRODUCTION

Now days, information sharing and transfer have been increased rapidly. Therefore, there is threat from third party or unauthorized party accessing secret information has been an ever existing concern for the data communication experts. With the rapid advancement in the network topology, multimedia information can be transmitted over the Internet conveniently. Many secure and confidential data items like military maps and commercial identifications are sent over the internet. While using secret documents (images, text etc.) for sending over the network, the security issue is to be taken into consideration, 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 are in need of 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 securely sent over the internet.

The proposed scheme combines the advantages of both Visual Cryptography as well as Public Key Cryptography. This scheme enhances the security of VC shares by encrypting with Public Key Cryptography [10], which provides the strong security to 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, when compared to existing traditional cryptographic methods, Visual Cryptography needs no complicated computation for recovering the secret image. The decryption method is to 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.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

Application of VCS

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

1) **Electronic-Balloting System**: Secret-Ballot Receipts system are one 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 receive a double-layer receipt that prints his/her voting decision. The voter will be asked to give one of the layers to the poll worker who will destroy it immediately with a paper shredder. The remaining one layer will now become unreadable [3].

2) **Encrypting Financial Documents**: The VCS principle can also be applied in transmitting confidential financial documents over Internet. Visual Cryptography is an example of this type of system being proposed. Visual Cryptography can encode the original drawing document with a specified (k, n) VCS, then send each of the encoded n shares separately through Emails or FAX to the recipient. The decoding only requires bitwise OR operation on all shares in the specified directory, and needs no extra effort of cryptographic computation. Any malicious attacker who intercepts only m of n shares where $m < k$ will not be able to gain any information about the financial document.

II. RELATED WORK

Various researches have been carried out in this area to increase the security & visual quality of the secret image. Some of them are as follows:

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.

B. 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.

Yogesh Bani, Dr. B.Majhi, Ram S. Mangrulkar [9] proposed a novel approach for Visual Cryptography using Data Hiding by Conjugate Error Diffusion watermarking technique. Two shares have been generated and then embed into the cover image x with the help of watermarking. Secret and cover images have been revealed after overlapping shares. Cover image consume extra storage space. Intruder can attack on the shares to reveal the secret, which causes disturbance in the pixels of original image and the receiver will not get the actual secret. At the receiver end.

.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

III. PROPOSED ALGORITHM

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].

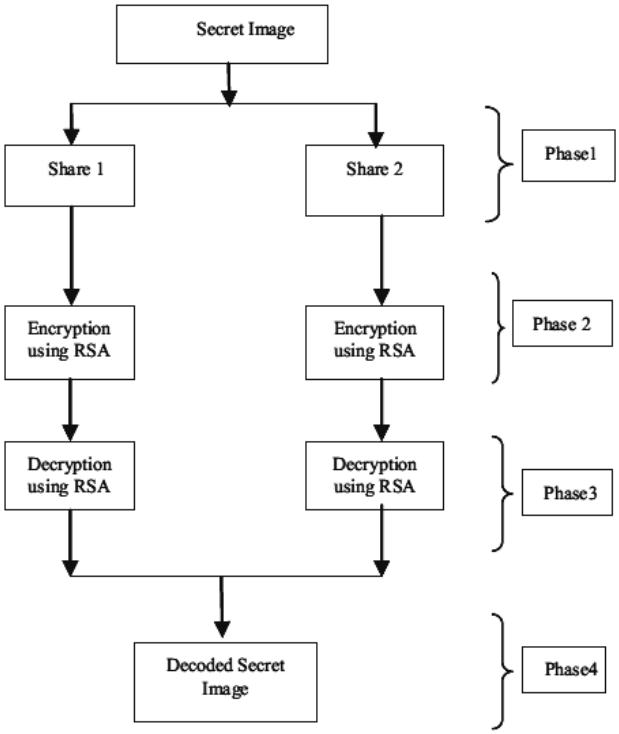


Fig: 3.1: Methodology of the Proposed Scheme

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 random pixel encoding scheme out of three given in Fig 3.2.

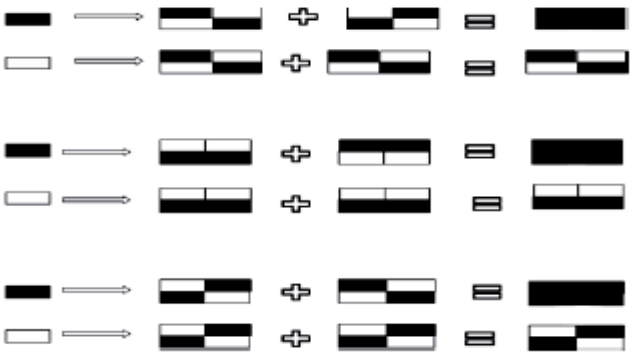


Fig: 3.2: Pixel encoding schemes

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

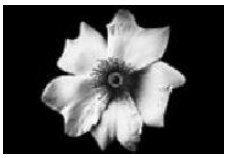
B 2nd Phase Encrypting the generated Shares:This is the second phase of our proposed approach where we will encrypt the shares that are generated in the first phase. The RSA algorithm is taken to encrypt the shares. First we have generated the key for RSA and then we perform the encryption using public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

C3rd 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. Here, for decrypting the shares.

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 get back the original secret image.

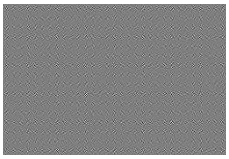
IV. RESULTS AND ANALYSIS

To test the proposed scheme a small software application is written in java. This application contains minimum tools to test the proposed scheme. The experiments have been run in Windows XP on a Compaq laptop with Intel Dual Core 1.5 GHz processor.
In order to test the performance of this proposed scheme, a number of experiments have been carried out by varying the image size, types.But every time secret image is retrieved with good visual quality. Results of some experiments are shown in Fig.4.1, Fig.4.2.All the images have been resized to fit into the paper.



A. Binary Input Image1

B.Image1_Share1



C.Image1_Share2

D.Image1_Encrypted_Share1

E.Image1_Encrypted_Share1

F.Image1_Decrypted_Share1

G.Image1_Decrypted_Share2

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

H. Recovered Image from Decrypted Shares

Fig 4.1 Experiment 1

A. Colour Input Image2

B.Image2_Share1

C.Image2_Share2

D.Image2_Encrypted_Share1

E.Image2_Encrypted_Share2

F.Image2_Decrypted_Share1

G.Image2_Decrypted_Share2

H. Recovered Image from Decrypted Shares

Fig 4.2 Experiment-2

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

These experiments have been conducted by taking secret images (both of type black and white and colour image) of different sizes as an input shown by 'A' in Fig.4.1, 4.2. 'B' &'C' show share1 & share2 of the secret image generated by the Visual Cryptographic encryption phase. 'D' &'E' show the encrypted share1 & encrypted share2. These are the results of second phase, in which the Visual Cryptographic shares have been encrypted using RSA algorithm. 'F' &'G' show the decrypted share1 & decrypted share2 which are decrypted by using RSA decryption algorithm. These are the results of 4th phase. And lastly,'H' shows the original secret image revealed by overlapping the decrypted share1 and decrypted share2. The Visual Cryptographic decryption is used to retrieve this secret image.

Advantages of our proposed scheme:
1. Complete Security for the secret images or documents.
2. Because of the binary property, it has robust method against
the loss of compression and distortion.
3. No need of complex computation for decryption.

V. CONCLUSION AND FUTURE SCOPE

Providing much security to the secret data that is shared in day to day life is one of the important issues in real life. In the scheme of Visual cryptography, we can decrypt the secret images without need of cryptographic computations. The proposed scheme is more secure and it is very easy to implement with low computation cost. In this proposed scheme, Very first the secret image is taken and then it is divided into shares after converting it into binary image, next the shares of binary image are encrypted and decrypted by using RSA algorithm, because of this even if the unauthorized person, once getting all the shares, he/she can't get back the original secret image without availability of the private key. We can implement this type of system in various fields like Military, Defence, and other places where the confidentiality of the data is must. . We can notice that there are many future extensions exist as the visual quality and size of the retrieved image.

It has been observed that there are many possible enhancements and extensions exist as the visual quality & size of revealed image. The major areas of future scope are:

1. Compression of encrypted shares to reduce bandwidth requirement.
2.Shares of Color image can be generated by using VC (2, 3) scheme and VC (2, 4) scheme in order to make the shares more un readable.

REFERENCES

[1] Kulvinder Kaur "Securing Visual Cryptographic Shares using Public Key Encryption", 2013 3rd IEEE International Advance Computing Conference (IACC).
[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]Y. Bani, Dr. B. Majhi and R. S. Mangrulkar, 2008. A Novel Approach for Visual Cryptography Using a Watermarking Technique. In *Proceedings of2nd National Conference, IndiaCom 2008*.
[10] Behrouz A. Forouzon, "Cryptography & Network Security" 4th Edition