

Visual Cryptography Security Innovation for Image Sharing Secretly

Dr.N.Kalyana Sundaram¹, Dr.R.Ahila², Harini R³, Jenifer S⁴, Mr. Murugan⁵

Department of Information Technology, New Prince Shri Bhavani College of Engineering and Technology, Chennai, India^{1,3}

Department of Computer Science and Engineering, New Prince Shri Bhavani College of Engineering and Technology, Chennai, India^{2,4}

Vee Eee Technologies, Chennai, India⁵

ABSTRACT: Visual Cryptography is one of the methods that can be utilized for getting image-based privileged insights. The plan Visual Cryptography is utilized to scramble a mystery image or document by breaking into shares. To exploit this property, the outsider can recuperate the mystery image on the off chance that the portions of mystery image are ignoring in grouping an organization. This paper presents a way to deal with scramble created image portions of Visual Cryptography utilizing Public key Encryption. We involved RSA algorithm to give the twofold security of the document. Consequently, portions of mystery image are not exist in their genuine structure for outsiders (the people who attempt to make counterfeit offers) to make modification. The proposed plot gives shares that are safer and vigorous against number of assaults. This conspire likewise gives solid security to the documents, transcribed text, images and so on that exists in the public organization.

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.

II. LITERATURE REVIEW

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 embedded into the cover image x with the help of watermarking. Secret and cover images have been revealed after overlapping shares. Cover image consumes 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.

III. METHODOLOGY

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].

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.

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.

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.

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.

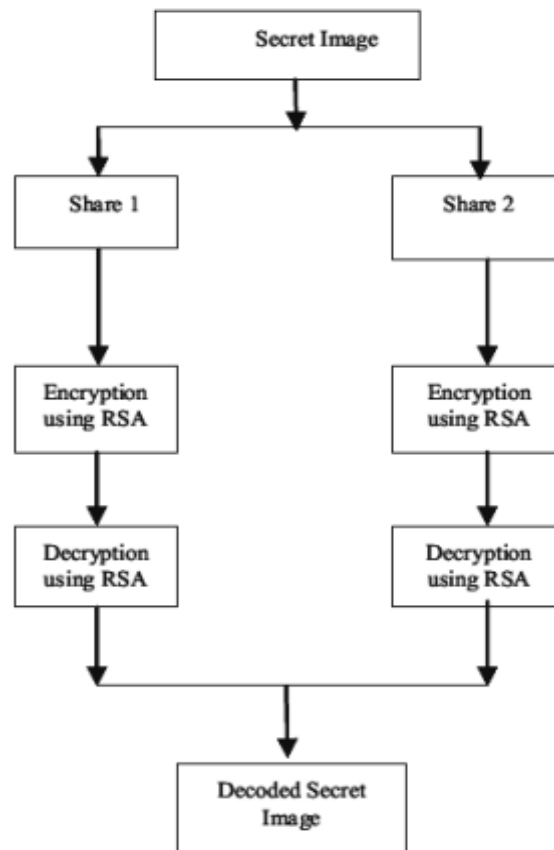


Figure.1 Proposed Methodology

IV. RESULTS AND DISCUSSION

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.

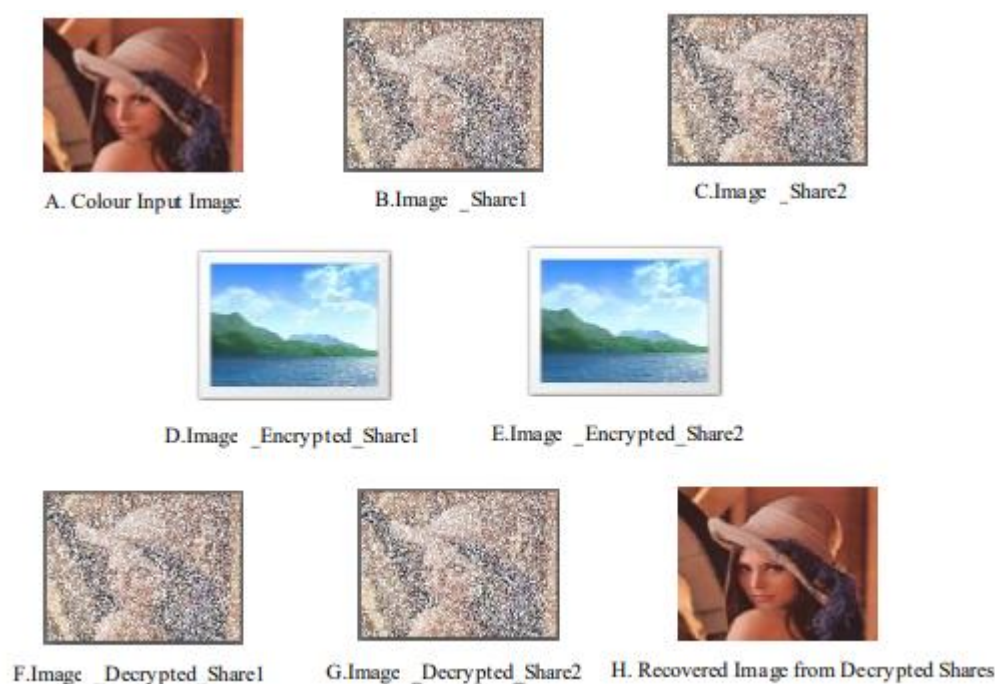


Figure.2 Experimental Results

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. CONCLUSIONS

Giving a lot of safety to the restricted information that is partaken in everyday life is one of the significant issues, all things considered. In the plan of Visual cryptography, we can decode the mystery images without need of cryptographic calculations. The proposed scheme is safer and it is exceptionally simple to execute with low calculation cost. In this proposed plot, Very first the mystery image is taken and afterward it is isolated into shares subsequent to changing over it into twofold image, next the portions of double image are scrambled and unscrambled by utilizing RSA algorithm, as a result of this regardless of whether the unapproved individual, once getting every one of the offers, he/she can't get back the first mystery image without accessibility of the private key. We can execute this sort of framework in different fields like Military, Defense, and different spots where the secrecy of the data is must. . We can see that there are numerous future augmentations exist as the visual quality and size of the recovered image.

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 of 2nd National Conference, IndiaCom 2008.
10. Behrouz A. Forouzan, “Cryptography & Network Security” 4th Edition.
11. J.Sasidevi, R.Sugumar, Fuzzy C-means Clustering and Elliptic Curve Cryptography using privacy preserving in cloud, International Journal of Business Intelligence and Data Mining, Volume 15, Issue 3, pp.273-287, July 2019.