International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-4, November 2019

Secret Image Sharing using 2-Pixel Visual Cryptography Encryption

Priyanka Diggavi, R.N.Kulkarni

Abstract: ***Visual Cryptography Scheme (Vcs) Is A Procedure For Encrypting Visual Data Such As Hand-Written Text, Image, Digital Text, Captured Image Etc. In This Scheme, The Shares Are Generated By Scrambling The Pixels Of The Original Image. Further, These Shares Are Sent To Receiver For Decryption At The Receiver End.***
In this paper, we have proposed an automated tool that takes the binary image as an input, and generates initial shares with one pixel encryption algorithm. Further, these initial shares are encrypted using 2-pixel encryption algorithm. The encrypted shares are then sent to the receiver for decryption to obtain the initial shares. The receiver then stacks the shares to get the original image. The proposed work which is presented in the methodology is the extension of VCS algorithm.

Keywords: 2-Pixel Encryption, Encrypted Shares, Initial Shares, One-Pixel Encryption, Visual Cryptography Scheme

I INTRODUCTION

Visual cryptography is proposed by "Naor and Shamir" in 1994. Visual cryptography is a method of encrypting images by creating shares of the original image at the sender side. At the receiver side, decryption is carried out by putting the shares one over the above. The visual cryptography ensures that, there will be no cryptographic complexity while decrypting the images and hence, they termed it as Visual Cryptography Scheme. In this paper, we are proposing an automated encryption tool, which is applied on the input image/text, which in turn generates shares. The obtained shares which are in turn used to combine 2 pixels of same color with the combination of 2 black, white and black, black and white, 2 white. These shares are then processed and then transmitted to the receiver. At the receiver, it uses the received shares, decrypts by applying decryption algorithm, and then get the original shares. The shares are then stacked one above the other to get the original image.

Manuscript published on November 30, 2019.
* Correspondence Author
Priyanka Diggavi*, Master of Technology in comuter networks and engineering, Ballari Institute of Technology and Management, Ballari. Email id : priyankadiggavi@gmail.com
Dr. R.N.Kulkarni, Professor and Head Department of computer science and engineering, Ballari Institute of Technology and Management, Ballari. Email id:rn_kulkarni@rediffmail.com

The proposed algorithm also detects the intruder during the transmission stage if the message/text is not reached to the destination within the stimulated time, sender receives a message that the intruder has been detected. In this paper, the encryption algorithm is a 2-pixel algorithm that provides double security for the document.

II LITERATURE REVIEW

In the paper [1] the authors considered extension of cryptographic pattern, which can decode pictures without any of the cryptographic computation. The system is safe and is easy to implement. They stretched it into a visually different k out of n secret sharing problems, where a user provides a photograph to each one of the n users. Any k of shares can help to decrypt the photograph by stacking them but no k - 1 of them can gain any information about it. In the proposed methodology we have used the basic scheme, 2 out of 2 shares, proposed by these authors.
In the paper [2] authors have suggested a new method named as Anti-phishing structures using visual cryptography in addition to RSA algorithm to resolve the problems of phishing. Using Visual Cryptography Scheme (VCS), image based authentication and the RSA encryption algorithm is applied. Here, Visual cryptography is done by scrambling the original input image into 2 shares, user database contains one share and server database contains another. The original input image can be gained only by stacking k shares. Thus safety of picture can be attained by visual cryptography and RSA algorithm. For the generated shares, RSA algorithm is applied and the shares are sent. As RSA takes big prime numbers, the cryptography computation of the generation may increase. In the proposed methodology we have used the concept of using prime numbers to encrypt the shares.
In the paper [3] the visual cryptography for the images depend upon the RSA algorithm and the ALGamal Algorithms. Plain image is taken and it is separated into 9 blocks. Those blocks are converted to binary numbers. If the size is 64 then it is converted to decimal and even and odd blocks are separated. For even blocks RSA algorithm is applied and for the odd blocks ALGamal encryption algorithm is applied. The 5 shares are generated by the list of odd blocks and the other 4 shares are generated by applying the RSA algorithm to the even blocks. In the proposed methodology conversion of blocks to shares is taken into consideration while implementing the 2-pixel encryption. The paper [4] involves 5 steps for image encryption. First step is image conversion, second step is share generation, third step is share encryption, forth step is share decryption and last step is visual cryptography decryption.

The color image or greyscale is divided into red, blue and green components, halftoning is applied to each component and the visual cryptography (2, 2) scheme is applied to the image. Six shares are generated. These shares are encrypted by image encryption algorithm. At the receiver's side, the scrambled shares are viewed and through decryption original shares are obtained. These shares are stacked together to get the original image.

The scheme of dividing the images into white and black pixels and encrypting the shares with (2, 2) scheme is taken into consideration while proposing this methodology. This paper [5] involves 4 phases of encryption. First phase is generating the shares for the secret image. This also takes (2, scheme where secret image is initially converted to the binary image then each pixel of the original input image is separated into eight sub pixels, in that four pixels in every share by selecting random pixels encoding scheme. The second phase is encrypting the generated share. Key is generated for RSA-encryption algorithm and using public key encryption, the shares are encrypted. In the third phase of the algorithm, the shares are decrypted using RSA at the receiver side. Now, the last phase is visual cryptography decryption, that is, when those shares are obtained and decrypted by the receiver, the shares are then stacked together to get the secret image. The proposed methodology is also based on this paper. But instead of using RSA algorithm, 2-pixel encryption algorithm is introduced.

III PROPOSED METHODOLOGY

In this paper, we have proposed a methodology, which securely transmits the image by generating shares using 2-pixel encryption algorithm. The method is illustrated in Fig – 3.1. At the sender side, the secret image that is to be sent is chosen. The input image is scrambled to produce the initial shares. The one-pixel encryption algorithm is applied to generate the initial shares, share1 and share2. The one-pixel encryption is implemented by substitution algorithm, that is, one pixel of the input image is substituted by four sub-pixels for each shares share1 and share2. These shares are encrypted with 2-pixel encryption algorithm. The 2-pixel encryption is described in the section 3.1. After encrypting the shares using 2-pixel encryption algorithm, the encrypted shares are securely transmitted to the receiver. The receiver then decrypts the shares and obtains the initial shares. The receiver then stacks the shares to get the input image.

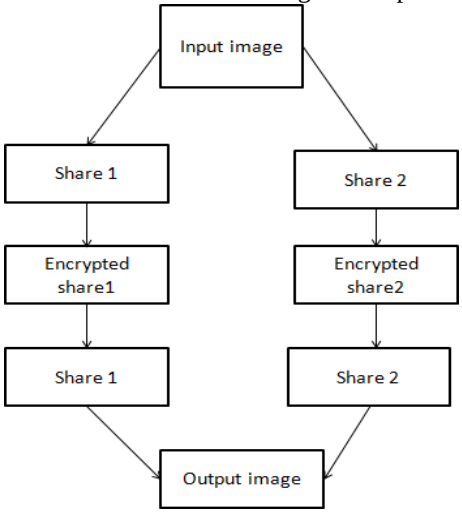

Fig – 3.1: Block diagram of the proposed methodology

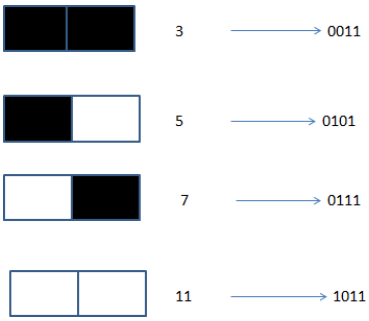

Fig – 3.2: Example values for the 2-pixel encryption patterns.

A . Algorithm: Encryption algorithm for 2-pixel

Input: Generated shares.

Output: Encrypted shares.

1. Begin
2. Read the shares obtained by the previous algorithm (Encryption algorithm for 1-pixel).
3. k←2 // number of shares
4. for k←1 to 2
5. n← number of pixels
6. for i← 0 to n and i+=2
7. do Read 2 pixel
8. pixel 1, pixel 2 ← a prime number // example = 5, as shown in Fig-3.2
9. convert prime number to 4 bit binary number // 5 = 0101
10. read the obtained 4 bit binary digit
11. for j← 0 to 3
12. if bit == 0 // for 5=0101, 0=black and 1=white
13. then set pixel ← black
14. else set pixel ← white
15. Generate the encrypted shares
16. Transmit the encrypted shares
17. End

V RESULTS

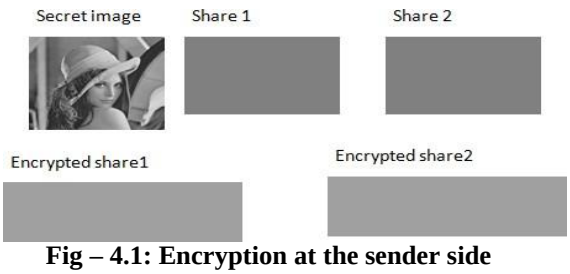

Fig – 4.1: Encryption at the sender side

At the sender side, Secret image is the input image for encryption. Share1 and Share2 are the initial shares generated using one-pixel encryption. Encrypted shares, Encrypted share1 and Encrypted share2, are generated by encrypting the initial shares using 2-pixel encryption algorithm. These encrypted shares are sent to the receiver.

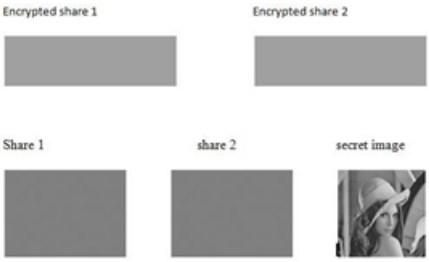

Fig – 4.2: Decryption at the receiver side

At the receiver side, Encrypted share1 and encrypted share2 are decrypted to obtain the initial shares, Share1 and Share2. On stacking of these shares, Secret image is obtained.

V CONCLUSION

In this paper, we have implemented an automated tool, which provides security for sending and receiving sensitive data using VCS. The proposed tool accepts the input either it is text or image and then generates two shares. Further, these shares are encrypted and then converted into the encrypted shares. The encrypted share are then transmitted from source to destination. Finally, at the destination the shares are decrypted and stacked one above the other to get the original image. The tool developed here is tested for its correctness and completeness.

REFERENCES

1. Naor, M. and A. Shamir. Visual cryptography, Advances in cryptology. Eurocrypt '94 Proceeding LNCS, 950:1–12, 1995.
2. Sayali Vaidya, Shreya Zarkar,, Prof. Achal N. Bharambe, ,Arifa Tadvi,Tanashree Chavan International Journal of Engineering Trends and Technology (IJETT) , Anti- Phishing Structure Based On Visual Cryptography and RSA Algorithm – Volume 20 Number 4 – Feb 2015
3. Assist.Prof.Dr. Alaa Kadhim, Rand Mahmoud Mohamed, Visual Cryptography For Image Depend on RSA & AlGamal Algorithms, 2016 Al-Sadeq International Conference on Multidisciplinary in IT and Communication Science and Application(AIC- MITCSA) - IRAQ(9,10)May.
4. SindhuParkavi.S , Sharon.I and Prof. S. Gowri, Visual Cryptography for Color Images to Provid Confidentiality Using Embedded System, Global Journal of Pure and Applied Mathematics. ISSN 0973-1768 Volume 13, Number 6 (2017), pp. 2555-2561
5. Shipra Rathore, Nilmani Verma, A Secure Secret Shares By Novel Visual Cryptography Using Bit Rotation and Blowfish Algorithm, IJESRT, May, 2014.
6. Ateniese, G., Blundo, C., Santis, A. and Stinson, D. Theory. Comput. Sci., Vol. 250, pp. 143-161, 2001.
7. M. Bharathi, R. Charanya, T. Vijayan - Halftone Visual Cryptography & Watermarking (2013).
8. William Stallings, Cryptography and Network Security, Pearson 6th edition and V K Pachghare: Cryptography and Information Security.

AUTHORS PROFILE

Priyanka Diggavi : Master of Technology in comuter networks and engineering in Ballari Institute of Technology and Management, Ballari. Email id : priyankadiggavi@gmail.com

Dr. R.N.Kulkarni. : Professor and Head of the Department, computer science and engineering, Ballari Institute of Technology and Management, Ballari. Email id:rn_kulkarni@rediffmail.com