Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 5.258

IJCSMC, Vol. 5, Issue. 4, April 2016, pg.152 – 158

A X-Or Base Image Encryption And Data Security Through Higher LSB Data Hiding Approach

Anuja R. Yeole[1], Prof. Mahip M. Bartere[2]
[1]Master of Engineering Scholar, Computer Science & Engg., Department
G. H. Raisoni College of Engg and Management, Amravati, India

[2]Guide, Computer Science & Engg., Department
G. H. Raisoni College of Engg and Management, Amravati, India
[1] Anuja.yeole@rediffmail.com; [2] Mahip.bartere@raisoni.net

Abstract: This project proposes double layer encryption and double layer hiding which is supposed to give security to the secret images and the secret data. The project speaks of usage of X- or base visual cryptography and higher LSB data hiding method. Visual cryptography (VC) is a technique that focuses on keeping the content of message secret and not seen by human eye directly. The original motivation of visual cryptography is to secured share secret images in which has no computer formed in this form; however, devices with computational powers are present everywhere (e.g., smart phones). We propose to provide double security and less complexity compared to existing system.

Keywords: visual cryptography, X-or base cryptography, higher LSB data hiding method, image security.

I. INTRODUCTION

The visual cryptography (VC) is a technique where secret images must be encrypted into no. of shares, with each recipient holding one or more shares. Anyone who holds fewer than number of shares they don't read the information which is visible and these are the secret images. Stacking the *n* shares opens to the human to read the image and he will see by his eyes directly. Secret images are of many types which are images, hand printed documents, photographs, and many others. Sharing and delivering secret images is also known as a visual secret sharing (VSS) scheme.

In this paper we will represent the X-OR base for encryption and higher LSB data hiding. These methods are simple to implement and more robust. A X-OR base is a random key so ciphertext does not give any information about the plaintext to the attacker.

II. LITERATURE SURVEY

In 1995: Moni Naor and Adi Shamir propsed a visual cryptography in that consider a new type of cryptographic scheme which can decode concealed images without any cryptographic calculation. This scheme is secure and easy to implement but there is a conventional share are not friendly.

In 2001: Giuseppe Atenies,Carlo Blundob, Alfredo De Santisb, Douglas R. proposed a extended capabilities of visual cryptography to share the secret information but these shares are meaningful shares but this have poor display quality.

In 2004: Jessica Fridrich, Miroslav Goljan, David Soukal proposed a Perturbed Quantization Steganography with Wet Paper Codes they produce a new approach to passive warden steganography. But there is a less security for the perturbed steganography

In 2006: Zhi Zhou, Gonzalo R. Arce, Fellow and Giovanni Di Crescenzo propsed a halftone visual cryptography this paper proposed to achieve visual cryptography via halftoning. This method used in a number of visual secret sharing applications which require high quality visual images such as watermarking, electronic cash. But it has side effects on pixel expansion.

In 2007: Ching-nung Yang And Tse-shih Chen proposed a Extended Visual Secret Sharing Schemes: Improving The Shadow Image Quality in this paper they present a new EVSS scheme by using gray and white subpixel to represent a secret pixel and then gives a clearer shadow images. But it displays low quality images.

In 2011: Feng Liu and Chuan Kun Wu proposed a Embedded extended visual cryptography scheme this paper propose a construction of EVCS which is realized by embedding random shares into a meaningful covering shares and we call it embedded extended visual cryptography. This embedded EVCS has competitive visual quality and it improves a visual quality of the shares. But it has poor display quality of the recovered images.

In 2011: InKoo Kang, Gonzalo R. Arce, Heung-Kyu Lee proposed a color extended visual cryptography using error diffusion. This paper introduces a color visual cryptography encryption method that produces a meaningful color shares via visual information pixel. It is used for color images. But it has poor display quality of the recovered images.

In 2012: Xiaotian Wua, Duanhao Ou, Qiming Lianga, Wei Sun proposed A user-friendly secret image sharing scheme with reversible steganography based on cellular automata. This method uses a two dimensional reversible automata for distorted images. It has low computation cost and pleasing stego images. But this scheme is sensitive when small changes occur means differential attacks against this scheme is useless.

In 2012: Kai-hui lee, pei-ling chiu proposed an extended visual cryptography algorithm for general access structure. This problem solves a existing EVCS scheme. This approach can be used for binary secret images in non-computer aided environment. It is used for modifying the display quality of the cover images. But it reduces the display quality of the recovered images.

In 2012: Cheng Guo, Chin-Chen Chang, Chuan Qin proposed a Multi-threshold Secret Image Sharing Scheme Based on MSP. In this paper multiple secret images can be shared among a group of participants and each secret image is associated with access structure. It can achieve both the high visual quality of the shadow images and high embedding capacity. But these images detected by steganography.

In 2012: Chun-Yuan Hsiao, Hao-Ji Wang proposed a Enhancing Image Quality in Visual Cryptography with Colors. In this paper they use the color model of ateniese et al. to improve the image quality of the reconstructed image of Chiu's image secret sharing scheme. The intuition behind is that a color pixel can be used either as a white or black one, thus solving the problem that the share images do not produce (when stacked) enough black pixels for the reconstructed image in. The technical difficulty of this work is how and where to inject the color pixels so that both the shares and the reconstructed images have high quality.

In 2014: Kai-Hui Lee and Pei-Ling Chiu proposed a Digital Image Sharing by Diverse Image Media. This paper proposes possible ways to hide the noise- like share to reduce the transmission risk problem for the share. This is the first attempt to share images via heterogeneous carriers in VSS scheme. But it has less security and single layer hiding.

In 2015: Sheetal A. Kulkarni and Shubhangi B. Patil proposed a A Robust Encryption Method for Speech Data Hiding in Digital Images for Optimized Security. In this paper the encryption algorithm applied with embedding method is the robust secure method for data hiding.

III. PROPOSED METHODOLOGY

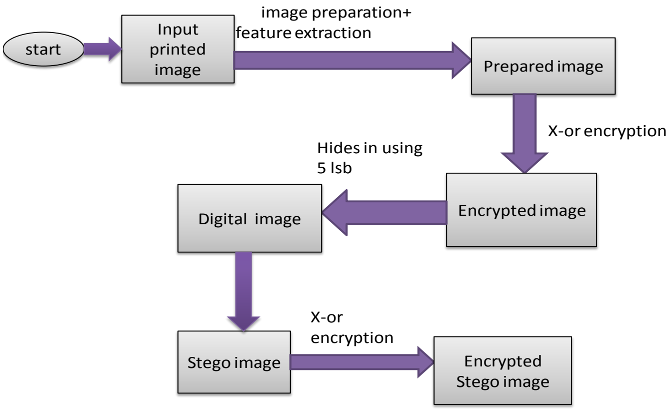

Fig. 3.1 Double Layer Encryption Process

A. Steps for above process

Step1: start
Step2: input an image
Step3: image preparation on input image means unwanted data will be avoided and feature extraction on image
Step4: then get prepared image and in prepared image there is a secret data
Step5: then encrypt the prepared image
Step6: we get encrypted image and in encrypted image there is a secret data
Step7: so encrypted image and secret data will be hides in carrier image
Step8: hence we get new stego image
Step9: again we encrypt the stego image hence we get new encrypted image and in encrypted image there is a secret data.

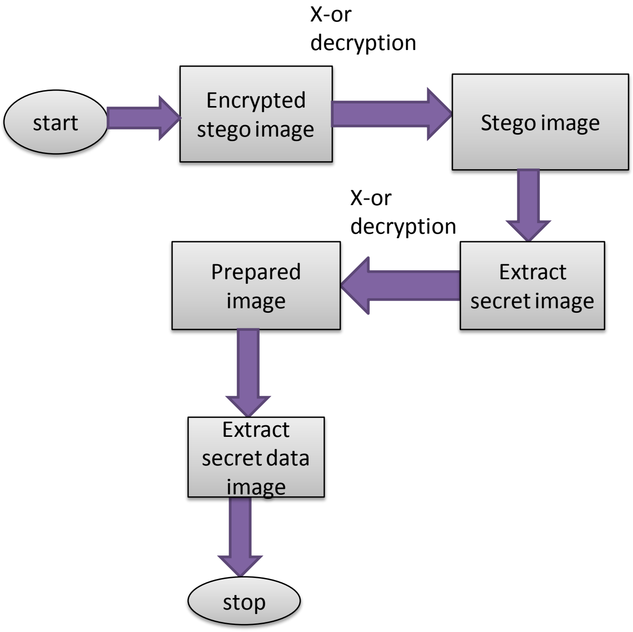

Fig3.2 Double Layer Extraction Process

B. Steps for above figure

Step1: input an encrypted image

Step2: decrypt the image

Step3: hence we get stego image

Step4: extract encrypted image from stego image

Step5: decrypt encrypted image

Step6: hence we get prepared image

Step7: extract secret data from prepared image

Step8: stop

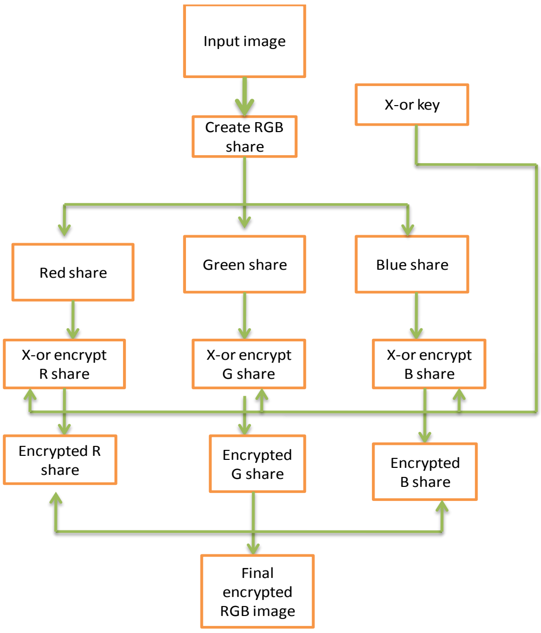

Fig3.3 X-or base encryption process

C. Steps for above process

Step 1**:** An input image will be selected. It must be RGB Image.

Step 2**:** Red, Green and blue channels are distributed from the input image.

Step 3**:** Encrypt each channel using XOR based encryption method using 8 bit random key generated using X-OR key

Step 4: Combine all Red, green and Blue channels to create final encrypted RGB image.

Step 5**:** End.

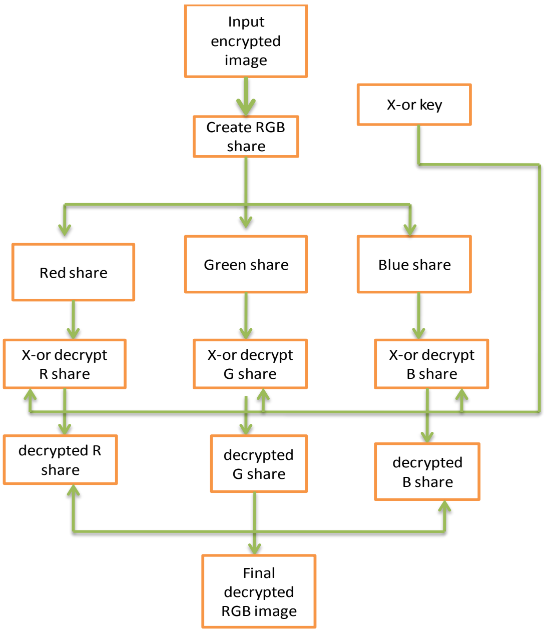

Fig3.4. X-or based decryption process

D. Steps for above process

Step 1: Select an encrypted image.

Step 2: Separate Red, Green and Blue channels from an encrypted Image.

Step 3: Decrypt Red, Green and Blue using XOR based decryption method with random key generated using X-OR key which is used for encryption.

Step 4: combine all decrypted image shares to create final resultant decrypted image.

Step 5: End.

E. Steps for data hiding process

step1: given encrypted image it consist of pixels

step2: pixel consist of RGB channel

Step3: suppose R is 8bit, G is 8bit and B is 8bit

Step4: divide the 8 bit of every RGB channel into groups of (3, 5)

Step5: suppose there is a secret data

Step6: then secret data converted to binary form

step7: then we sample the binary data to 5 groups

Step8: then we replace 5groups of binary data to our given RGB

Step9: hence we get new RGB values

Step10: from this new RGB values we make pixel

Step11: hence we get hided data.

References

[1] M. Naor and A. Shamir, “Visual cryptography,” in Advances in Cryptology, vol. 950. *New York, NY, USA: Springer-Verlag, 1995, pp. 1–12.*

[2] G. Ateniese, C. Blundo, A. D. Santis, and D. R. Stinson, “Extended capabilities for visual cryptography,” *Theoretical Comput. Sci*., vol. 250, nos. 1–2, pp. 143–161, Jan. 2001.

[3] J. Fridrich, M. Goljan, and D. Soukal, “Perturbed quantization steganography with wet paper codes,” *in Proc. Workshop Multimedia Sec.,Magdeburg, Germany*, Sep. 2004, pp. 4–15.

[4] Z. Zhou, G. R. Arce, and G. D. Crescenzo, “Halftone visual cryptography,” *IEEE Trans. Image Process*., vol. 15, no. 8, pp. 2441–2453,Aug. 2006.

[5] C. N. Yang and T. S. Chen, “Extended visual secret sharing schemes: Improving the shadow image quality,” *Int. J. Pattern Recognit. Artif. Intell*., vol. 21, no. 5, pp. 879–898, Aug. 2007.

[6] F. Liu and C. Wu, “Embedded extended visual cryptography schemes,” *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 2, pp. 307–322, Jun. 2011.

[7] I. Kang, G. R. Arce, and H. K. Lee, “Color extended visual cryptography error diffusion*,” IEEE Trans. Image Process*., vol. 20, no. 1,pp. 132–145, Jan. 2011.

[8] C. Guo, C. C. Chang, and C. Qin, “A multi-threshold secret image sharing scheme based on MSP*,” Pattern Recognit. Lett*., vol. 33, no. 12, pp. 1594–1600, Sep. 2012.

[9] Chun-Yuan Hsiao, Hao-Ji Wang, “Enhancing Image Quality in Visual Cryptography with Colors,” 2012 *IEEE, International Conference on Information Security and Intelligence Control (ISIC), Page(s):* 103 – 106, 2012.

[10] X. Wu, D. Ou, Q. Liang, and W. Sun, “A user-friendly secret image sharing scheme with reversible steganography based on cellular automata,” *J. Syst. Softw.*, vol. 85, no. 8, pp. 1852–1863, Aug. 2012.11.

[11] K. H. Lee and P. L. Chiu, “An extended visual cryptography algorithm for general access structures,” *IEEE Trans. Inf. Forensics Security*, vol. 7, no1, pp. 219–229, Feb. 2012.

[12] Kai-Hui Lee and Pei-Ling Chiu, “Digital Image Sharing by Diverse Image Media*,” IEEE Transactions on Information Forensics and Security,* Vol. 9, No. 1, January 2014.

[13] Sheetal A. Kulkarni, A Robust Encryption Method for Speech Data Hiding in Digital Images for Optimized Security, *International Conference on Pervasive Computing (ICPC)*2015