

Sharing of a Digital Secret Image by Diverse Media for More Security

Tejbir Kaur
M.E. Student ECED,
Thapar University
Patiala

Ajay Kakkar
M.E. Student ECED,
Thapar University
Patiala

ABSTRACT

The efficient algorithms require correct protocols for authentication and key management. It is intended to design the available cryptographic algorithm to achieve more security and this will be done by incorporating visual cryptography. The visual cryptography is an efficient method to share our data in secured manner. Conventional Visual Secret Sharing (VSS) schemes hide secret images in shares that are either printed on transparencies or are encoded and stored in a digital form. Natural visual secret sharing (NVSS) in which various carrier media is used to carry secret images Natural visual secret sharing (NVSS) in which various carrier media is used to carry secret images by a share to protect the secret and the participants during the transmission phase has been proposed. The proposed (n, n) - NVSS scheme shares one digital secret image over $n-1$ arbitrary selected natural images and one noise-like share. The above work have its utility to transfer secret information over web, so that, intruder couldn't detect it. Our aim is to use visual cryptography for transmission of the secret image and to protect the network in order to keep the data confidential. The image is preprocessed, and then feature extraction has been done. The PSNR values of digital and handmade image are 33.04 and 32.93 respectively. In feature extraction process thresholding, binarization and chaos process has been done. The median values of digital and handmade image come out to be 205 and 162 respectively. All the pixels are being arranged with respect to median values. Some more techniques like encryption and pixel swapping has also been used. And at the end, to give our information more security, steganography is used. The PSNR and elapsed time of the images is also been analyzed.

Keywords

NVSS, encryption, image and cryptography.

1. INTRODUCTION

It is a cryptographic technique which allows any visual information like pictures and images to be encrypted in such a way that it can be decrypted only by an authorized user [2]. The used can decrypt the information by the easy method, by sight reading. In visual secret sharing, an image was broken up into n shares so that only person having all the shares could decrypt the image, while if they have less than n shares they revealed no information about the original image [5]. Each share was printed on a separate transparency, and decryption was performed by overlapping the shares as shown in fig.1. This scheme has a disadvantage that is it experiences high transmission risk [1]. So, attacker can guess the secret information. At that point, the new strategy has additionally been produced called expanded visual mystery sharing (EVSS) in which steganography is utilized [3].

2. RELATED WORK

It is a technique in which users are allowed share their data in the secured manner with the help of keys. They worked on secured communication with the help of different methods [1]-[3]. They had also done work on fault attacks against public key cryptography. But at the end, they won't be able to manage the effects of the attack; also it fails to detect a fault if message is zero. Xiang Wang and Ran-Zan Wang worked on so many methods of the conventional visual cryptography like a lossless Tagged Visual Cryptography Scheme, region incrementing visual cryptography (RIVC) [4]-[8]. After studying so many methods, they realised that they should have to minimize the pixel expansion, Because of the contradiction in the quality of shares and the pixel expansion. The quality of share decreased with high value of pixel expansion. Done their work to limit the pixel development [9]- [11]. Ching-Nung Yang proposed a novel strategy in which additional sub-pixels were decreased.

For greater security, steganography is utilized as a part of many examines to hide the information or any data in the QR codes [12]-[16] utilizes steganographic procedure for the information hiding reason. Arooj Nissar had done their work to record the different methodologies that had been proposed for steganalysis in 2007. Abbas Cheddad in 2010 finished up with a few proposals advocates for the object-oriented embedding mechanism.

TEJBIR

(a)Original Share



(b) Secret share 1



(b) Secret share 1

Overlapping Share 1 & 2

TEJBIR

(d) Output image by combining both shares

Fig.1 Example of Visual cryptography

3. PROPOSED SCHEME

The natural shares are used just like hand printed image, landscapes by using these shares. The transmission risk problem is decreased to a certain level.

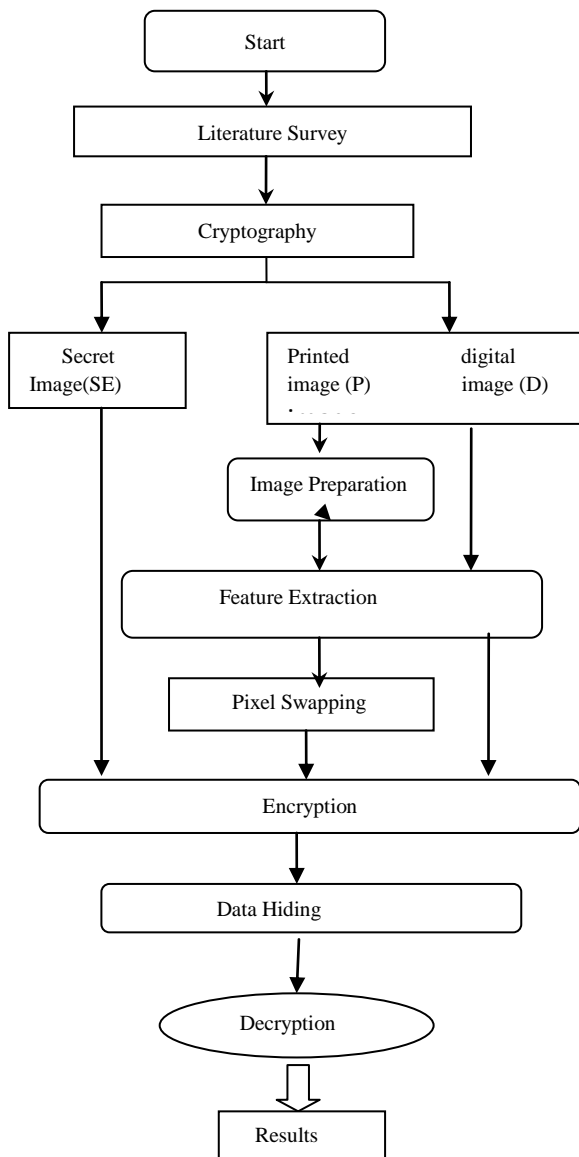


Fig. 2 Proposed Scheme

The security level will be expanded more by transmitting the shares with the help of different medium. So that the unauthorized person cannot get our secret information

Proposed Scheme has been depicted in Fig 2. Initially, three images have been taken of different formats, first is secret image (table 3a), which should be transmitted in secured manner; the second image is the hand-printed image. The handprint image could be any image like Handmade painting or any natural image (table 3g) or any landscape image. Third image is digital image (table 3d). The printed image and the digital image should be of the same size. The process which is used to equalize them is called pre-processing. In Image Pre-processing image will be pre-processed by cropping the input image. Cropping process is performed manually and then stored.

After the pre-processing of the images (table 3j), the Feature Extraction is done by the process called Binarization of the

natural share. Binarization is performed by calculated with respect to the thresholding value of the natural share. The images have been binarized by taking their median value (table1) as a threshold value. With the binarization result the stabilization has been done. Image can be made more secured by applying the feature extraction pixel swapping. And then all three images will be passed through encryption phase. After encryption the data will be done by the technique called steganography. the secret image is been hidden into the other cover image. Then the final image will be shared with the authorised user. Then, after doing the same processes the resultant image will be revealed after decryption.

3.1 Methodology for encryption process

Encryption is a process which uses a finite set of instructions which are only known to sender or receiver to convert original image into encrypted image. These algorithms generally required a set of characters called key. By using the key, we can encrypt and decrypt the secret image.

All the three images in fig 2 are encrypted here. The digital image, the natural one and secret image is also encrypted. The key is needed to encrypt the images; same key is used by the receiver to decrypt the images

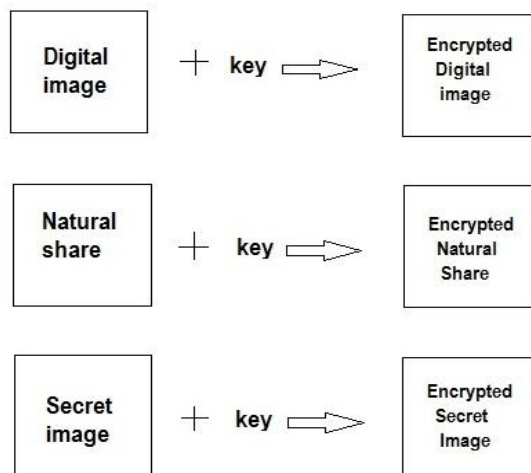


Fig.3 Encryption method

From the above results, three images have been produced. One is the encrypted digital share, encrypted natural share and the secret encrypted share. By applying adding algorithm all the three images are added together to form one share as shown in fig 3. That secret share is then steganographed.

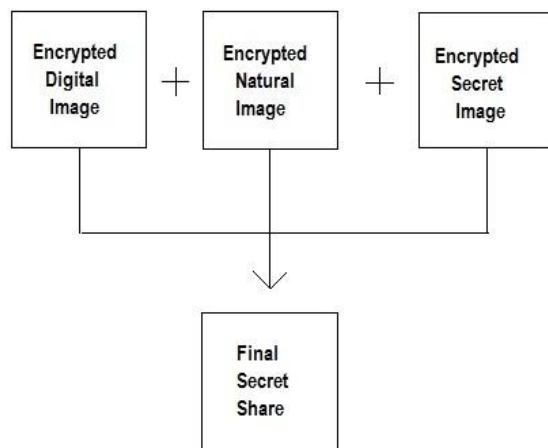


Fig.4 adding of shares

4. RESULTS

As explained in flow chart the printed image is pre-processed by the method of image preparation. In this method, the image captured by smart phone is cropped to size (512*512), so that, it becomes equal to the size of digital image. Feature extraction is done on both digital and cropped image. In feature extraction process there are three steps. 1) Binarization, 2) Stabilization, and 3) Chaos. To get the binarized image, the threshold value is to be set of these images. The threshold value of image is average intensity value of pixels. So, pixel values which are above threshold are set to be 1, and remaining 0. The threshold for digital image of jpg format is 205. And threshold value for cropped image of same format is 162. All the other threshold values are mentioned in the table1:

Table 1. Median values of all images of different formats


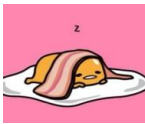




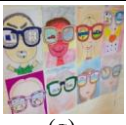





S.No.	Image Format	Thresholding value of Digital Image	Thresholding value of Secret Image
1	JPG	205	162
2	PNG	145	166
3	BMP	194	167







The comparison between the PSNR's of the both digital and natural image is given in the table2 below:

Table 2. Comparison's of PSNR's

	Jpg	png	Bmp
Digital Image	33.04	28.2	33.00
Natural Image	32.93	27.79	33.07

Table 3. Input and Processed Images

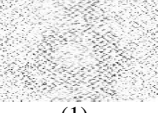

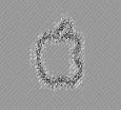
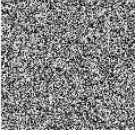
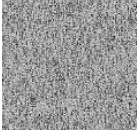

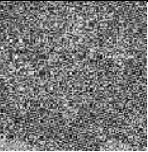
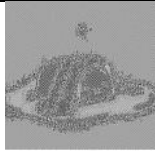
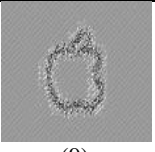
	Image Format		
	JPG	PNG	BMP+
Secret image	 (a)	 (b)	 (c)
Digital image	 (d)	 (e)	 (f)
Original Handmade image	 (g)	 (h)	 (i)
After pre-processing	 (j)	 (k)	 (l)

Binarized digital image	 (m)	 (n)	 (o)
Binarized handmade image	 (p)	 (q)	 (r)

4.1 Encryption

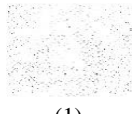





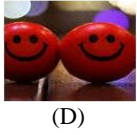


Then after pixel swapping, the encryption has been done on all the images. Pixel swapping is done only on feature extracted image but encryption has been done on digital image, natural image and secret image too. Results of encrypted images of different formats are given below:

Table:3 (1) (2) and (3) are the encrypted digital images ;(4) (5) and (6) are the encrypted natural image; (7) (8) and (9) are the encrypted secret image of jpeg , png and bmp format respectively.

Encrypted Digital image:	 (1)	 (2)	 (3)
Encrypted natural image:	 (4)	 (5)	 (6)
Encrypted Secret image:	 (7)	 (8)	 (9)

After the encryption of all the shares, the adding of images has been done. All the three images are added together to form one final share.

Table 4 Hiding of image by Steganography

Secret Shares	 (1)	 (2)	 (3)
Cover image	 (A)	 (B)	 (C)
Cover image after Steganography	 (D)	 (E)	 (F)

5. CONCLUSION

The proposed a VSS plot, (n, n) - NVSS method, that would be able to share a digital picture utilizing differing image media. The media that incorporate $n-1$ randomly picked images are unaltered in the encryption stage. Consequently, they are absolutely harmless. Contrasted and existing VSS plans, the proposed NVSS plan have less transmission hazard and give the most abnormal amount of ease of use, both for shares and for members. This examination gives four noteworthy commitments. To start with, this is the principal method to share pictures by means of heterogeneous transporters in a VSS conspires. Second, hand-printed pictures for pictures haring plans have been presented effectively. Third, this examination proposes a valuable idea and technique for utilizing unaltered pictures as offers in a VSS method. Fourth, we build up a strategy to store the picture into another picture utilizing steganography procedure.

6. FUTURE ENHANCEMENT

After Decryption prepare has been done, recovered image will be shaped. By contrasting the pixel estimations of secret picture and recovered picture it is found that there will be no pixel expansion or pixel debasement in the recovered picture. There will be no change between secret picture and recovered picture.

7. REFERENCES

- [1] Vercauteren F. (2006). A fault attack on pairing based cryptography, *IEEE transaction on computers*, 55(9), 1075-1080.
- [2] S.V. Kartalopoulos (2006) A primer on cryptography in communications, *IEEE communications magazine* 32(4), 146-151.
- [3] Ma Kun, Liang Han and Wu Kaijie (2012). Homomorphic Property-Based Concurrent Error Detection of RSA: A Countermeasure to Fault Attack, *IEEE Transactions on Computers*, 61(7), 1040-1049.
- [4] Kakkar Ajay, Singh M. L. and Bansal P. K. (2012). Mathematical analysis and Simulation of multiple keys and S-Boxes in a multi-node network for secure Transmission, *International Journal of Computer Mathematics*, 89(16), 2123–2142.
- [5] Wang Xiang, Pei Qingqi and Li Hui (2014). A Lossless Tagged Visual Cryptography Scheme, *IEEE Signal Processing Letters*, 21(7), 853-856.
- [6] Wang Ran-Zan (2009). Region Incrementing Visual Cryptography, *IEEE Signal Processing Letters*, 16(8), 659-662.
- [7] Lee Kai-Hui and Chiu Pei-Ling (2014). Digital Image Sharing by Diverse Image Media, *IEEE Transaction on Information Forensic and Security*, 9(1), 88-98.
- [8] Shyong Jian Shyu and Ming Chiang Chen (2011). Optimum Pixel Expansions for Threshold Visual Secret Sharing Schemes, *IEEE Transactions on Information Forensics and Security*, 6(3), 960-969.
- [9] Liu Feng, Wu Chuankun(2010). Step Construction of Visual Cryptography Schemes, *IEEE Transactions on Information Forensics and Security*, 5(1), 27-38.
- [10] Li Bin (2008). Steganalysis of Multiple-Base Notational System Steganography, *IEEE Signal Processing Letters*, 15, 493-496.
- [11] Zhang Liang and Wang Haili (2009). A High-Capacity Steganography Scheme for JPEG2000 Baseline System, *IEEE transactions on Image Processing*, 18(8), 1797-1803.
- [12] Cheddad Abbas, Condell Joan, Curran Kevin and Mc Kevitt Paul (2010). Digital image steganography: Survey and analysis of current methods, *School of Computing and Intelligent System*, 909(3), 727-752.
- [13] Nissar Arooj (2010). Classification of Steganalysis techniques: A study, Department of Information Technology, *Digital Signal Processing*, 20(6), 1758-1770.
- [14] WangYong (2010). Reliable JPEG steganalysis based on multi-directional correlations, *Department of Applied Mathematics, Information Science and Technology Institute*, 25(8), 577-587.
- [15] Zhou Zhi, Arce Gonzalo R. and Di Crescenzo Giovanni (2006). Halftone Visual Cryptography, *IEEE Transaction on Image Processing*, 15(8), 2441-2453.
- [16] Maninder singh and Dhanwant singh (2015). Energy efficient key management scheme for wireless sensor networks. *International Journal of Research in Information Technology*, 3 (8), 166-173, 2015.