Hybrid Steganography using Visual Cryptography and LSB Encryption Method

Gokul.M
Final Year – M.Tech - CVIP
Amrita Vishwa Vidhyapeetham University
Coimbatore

Umeshbabu R
Final Year – M.Tech - CVIP
Amrita Vishwa Vidhyapeetham University
Coimbatore

Shriram K Vasudevan
Technical Manager – Learning and Development
Amrita Vishwa Vidhyapeetham University
Coimbatore

Deepak Karthik
Final Year – M.Tech - CVIP
Amrita Vishwa Vidhyapeetham University
Coimbatore

ABSTRACT

The biggest threat in the data transfer is through any medium is, the chance for it being hacked. Any information, these days are hackable. So utmost care has to be taken for any communication to be done, in particular, if confidential. The so claimed most sheltered data have also been hacked nowadays. The digital watermarking is a widely used method for information hiding to authenticate as well as secure the content in an image. This paper describes a hybrid watermarking technique to embed a secret message into an image using visual cryptography and SLSB(Selected Least Significant Bit) encryption techniques. This paper becomes very special in few aspects, all of them are explained in a detailed way in the chapters.

Keywords

Information Hiding, SLSB (Selected Least Significant Bit), Visual Cryptography.

1.Introduction

The paper is so well organized as follows starting with and navigates in the order:

- Introduction
- Proposed methodology
- Encryption and Decryption process
- Results

A digital watermarking technique is defined as embedding invisible data for securing and authentication purpose. The watermarking techniques can be broadly classified into two categories breakable watermarking and robust watermarking. This could become very handy in case of confidential information that has to be sent from a source to the destination. The information itself, say I LOVE INDIA can be embedded in an image and can be sent across through medium. And since it is embedded in the image, it becomes un identifiable and at the same time, secured. Most importantly, the image that we are embedding the information with will not be altered much. That is, an intruder or hacker would not find a much of difference between the message less image and message embedded image. Another notable point in this project is, it is a key less encryption that we do. If it has a key, it has also to be transferred along with the information, which literally is a pain and if the key gets hacked, it will further create panic. So, to avoid all these confusions, Steganography [6][7]is proposed and implementation details are covered well in this paper.

2. Proposed Methodology

Here first the encryption part is discussed and the decryption is paid attention then.

Encryption

Step 1: The secret text message is written in an image . This image is given as input to the share generation algorithm.

Step 2: The share generation algorithm results in two shared images.

Step 3: The share images along with the, chosen cover image is given as input to the LSB bit encryption method .

Step 4: The result of the LSB bit encryption method is just the cover image with minor artifacts .

Decryption

Step 1: The input for LSB bit extraction is the steganographed image.

Step 2: The result of the LSB extraction algorithm is the 2 share images retrieved.

Step 3:The share images are given as input to the share combining algorithm.

Step4 :The resulting output of the share combining algorithm is an image with the retrieved secret message .

3. Encryption and decryption process

Visual Cryptography

The visual cryptographic method [1][4][11] is applied here. At first, the original image is binarised to keep the pixel values as either 0 or 1, this is considered for simplicity of LSB bit encryption [3][2][8]. Next the secret message image is scrambled where share 1 is created by taking the odd positioned bits of the secret image and the share 2 is generated using the even positioned bits of the secret image .

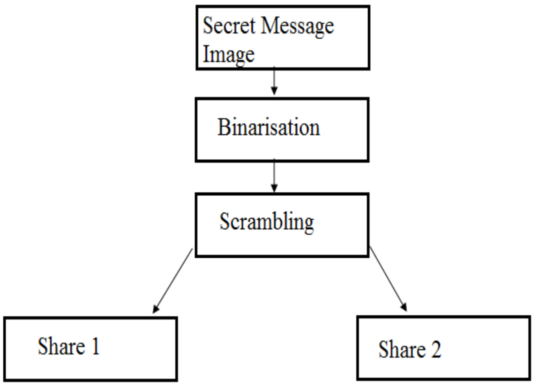


Figure 1: Share generation process

SLSB bit encryption

The share 1 and share 2 is embedded into the cover image by first choosing the image plane where it can be embedded .The plane choosing is performed by taking the average of pixel values of a particular position and the pixel value of a the plane which is greater is chosen as the LSB encryption pixel .The LSB bit of this pixel value is replaced by the MSB bits of the shares. The last pixel of the image is replaced with a number, this number signifies the position of the shares .The number 1 signifies that first share is encrypted in the upper half of the image and the second half of the image with share2. The number 2 signifies that the first share to be encrypted is share 2 and the next half of the image with share 1. Similarly the numbers 3 and 4 signifies as the share to be used in the left half of the image and the right half of the image. This number is changed each time the encryption is performed.

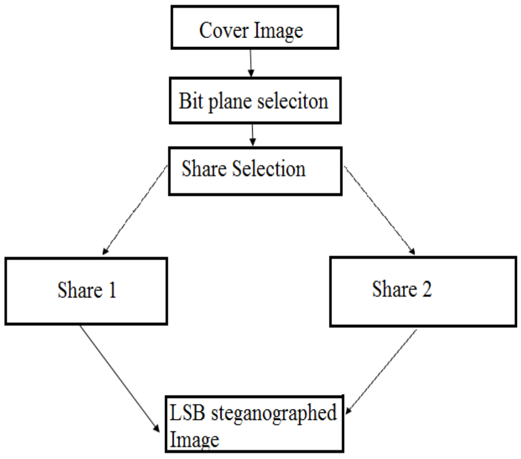


Figure 2: LSB bit encryption process

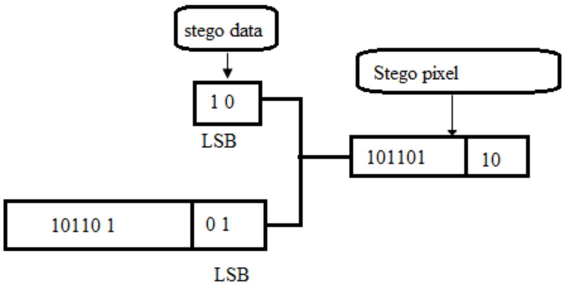


Figure 3 :LSB bit replacement

Decryption Process

LSB Extraction

The LSB bits of the steganographed image is extracted at first .Then the last pixel value LSB number is identified to the share positions .

The LSB bits of other pixels are arranged according the number identified .The share 1 and share 2 are generated using this LSB extraction.

Decryption of visual cryptography

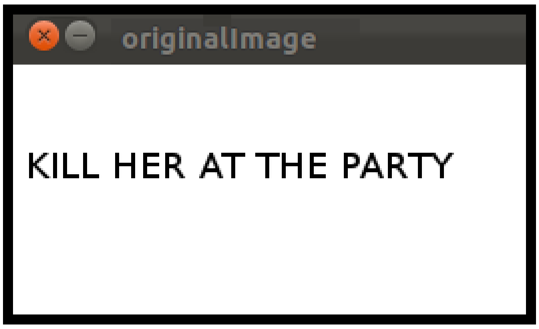
The obtained shares from the LSB extraction is fed as input to the visual decryption process [4] .Here the shares are combined by alternating the pixels from each share to generate the secret message image.

4. Results

The secret message image size of 268x127 was used for the encryption process. The image is as shown in figure 4 .The shares of size 536x127 was generated using the visual cryptographic method as described in the methodology. Figure 5 and 6 illustrates the generated share 1 and share 2 respectively.

The cover image used was of size 536 x 254. Figure 7 shows the cover image used. The resulting steganographed image was of the same size of the cover image, but the quality of the image slightly varies when compared to the original image. The decrypted image from the steganographed image, results with the secret message in a slightly scrambled form of size 536x127. Figure 9 illustrates the decrypted image.

The attacks and the amount of sustainability in terms of correlation percentage is listed in the table 1 along with the other existing methods and its comparison graph is shown in figure 10.



KILL HER AT THE PARTY

Figure 4: Secret message image .

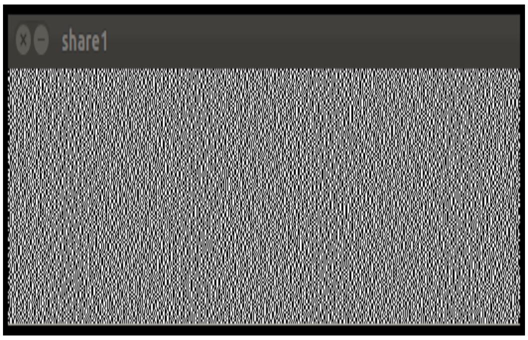


Figure 5: Generated share 1.

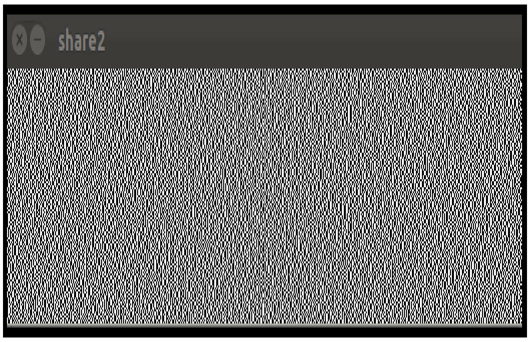


Figure 6: Generated share 2.

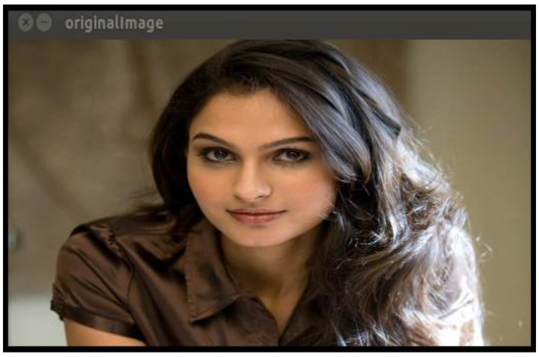


Figure 7 : Cover image

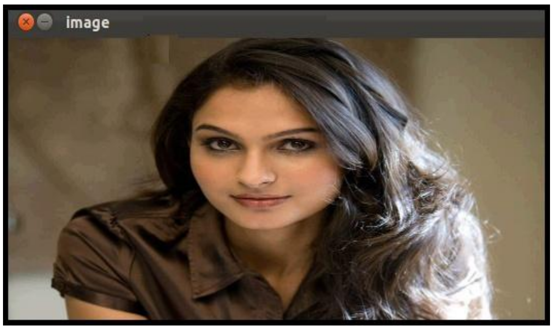
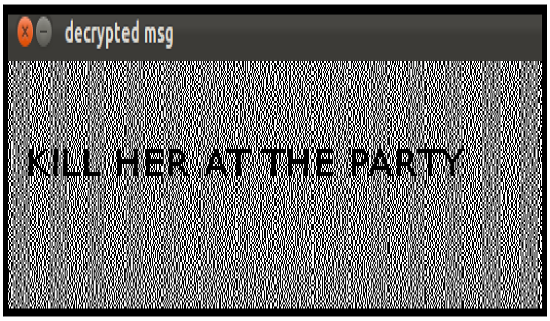


Figure 8 : Steganographed image.



KILL HER AT THE PARTY

Figure 9: Decrypted image .

TABLE 1: Verification and comparison results

	CORRELATION PERCENTAGE	
Attack	Halftone visual cryptography	Proposed method
No Attack	99.75	98.3
Salt and pepper noise	98.62	-
Sharpening	98.34	92
Blurring	97.48	87.2
Averaging filter	98.52	92
Jpeg compression	98.33	97
Flipping	98.67	99

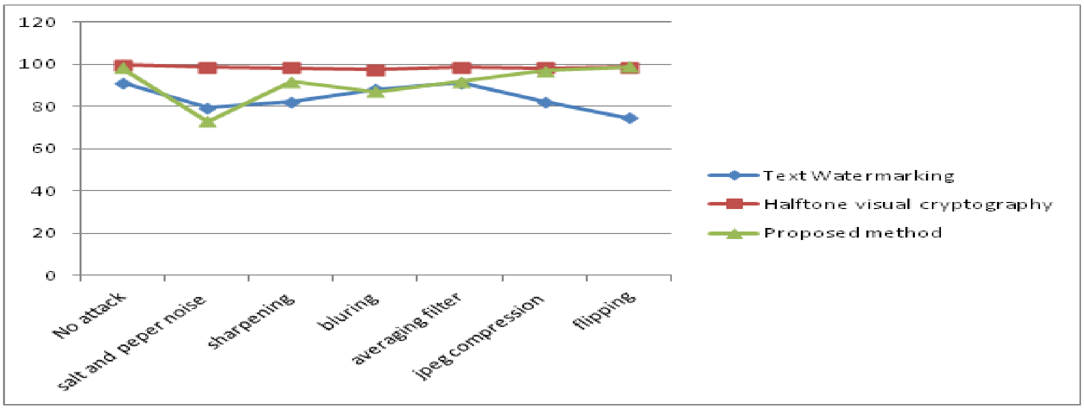


Figure 10. Comparison chart

5. Conclusion

Here, after all the analysis was done we are concluding with 3 points:

1. The image size and the quality of the cover image is retained up to 90% of the original cover image.
2. The secret message is highly secure. Unless the algorithm is known by the intruder the decryption is highly impossible.
3. The pattern of the encryption of the shares changes every time when the encryption function is called, this makes the system more robust.

The future scope of this work is to apply a DCT based compression on the secret image and store only the dominant values in the cover image for further security. Also The LSB bit encryption algorithm can be replaced with a more complicated method. This system can be analyzed and compared based on their performance and fidelity with the current proposed system.

6. ACKNOWLEDGEMENT

We wish to thank the almighty for giving us power and knowledge. We thank Amrita University for giving us consistent support and encouragement throughout this project. Also we would like to thank Prof.P.N.Kumar for his valuable advices and guidance.

7. REFERENCES

[1] Naor, M. and Shamir, A. “Visual cryptography, Advances in Cryptology - EUROCRYPT '94”, 1995.

[2] Hartung, F. and Kutter, M ,”Multimedia Watermarking Techniques, Proc. of IEEE, Tutorial, Survey , and Special Issue on Data Hiding & Security”, pp.1079-1107,1999

[3] Roque, J.J. and Minguet, J.M., “SLSB: Improving the Steganographic Algorithm LSB”, The 7th International Workshop on Security in Information Systems (WOSIS2009), Milan, Italy, Pp.1-11, 2009.

[4] D.Mathivadhani, C.Meena” Digital Watermarking and Information Hiding Using Wavelets, SLSB and Visual Cryptography Method" 2010 IEEE

[5] Sharp, T. “An implementation of key-based digital signal steganography.” Proc. 4th International Workshop on Information Hiding. Springer LNCS, Vol. 2137, Pp.13-26, 2001.

[6] Yuan Tai Hsu ,Long Wen Chang ,“A new Construction algorithm of Visual cryptography for gray level images” , 2006,IEEE

[7] G.Karthigai Selvi ,Leon Mariadhasan and K.LShunmuganthan “Steganography Using Edge Adaptive Image” International Conference on Computing,Electronics and Electrical Technologies 2012,IEEE

[8] Weiqi Luo ,member ,IEEE Fangjun Huang member, IEEE, and Jiwu Huang ,senior member ,IEEE, “Edge Adaptive Image Steganography based on LSB matching Revisited” ,IEEE transations on information forensics and security ,vol.5, no.2 , June 2010.

[9] Piyush Marwaha, Paresh Marwaha , “Visual cryptographic Steganography in images”,2nd International conference on Computing ,Communication and Networking Technologies ,2010.

[10] Ujwala B.S,Chetan K.R ,“An efficient DCT based pringerprinting scheme for thwarting collision attacks”,IEEE 2010

[11] Bhandare Shital, Jhade Manoj, Jadhav Angarika,“An improved approach for extended visual cryptography scheme for color images”,2011,International journal of computer applications.

[12] Vaibhav Choudhary,Pravin kumar,Kishore Kumar,D.S.Singh, “An improved pixel sieve method for visual cryptography”,2011,vol.12,no.9, International journal of computer applications.

[13] Jaishri Chourasia, M.B. Potdar,Abdul Jhummarwala,Keyur Parmar, “Halftone image watermarking based on visual cryptography”,2012,vol.41,no.20, International journal of computer applications.

[14] Chunlin Song, Sud Sudirman and Madjid Merabti, “Robust Digital image watermarking using Region Adaptive embedding technique”,IEEE, pp. 378-382, 2010.

[15] Y-C Hou, P-M Chen, “An asymmetric Watermarking scheme based on Visual cryptography”,In Proceedings of ICSP, vol.2,pp.992-995, (2000).