www.ijecs.in
International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 5 Issue 10 Oct. 2016, Page No. 18392-18394

Visual Crypto-Steganography in Images

Pranav Swaminathan, Tejas Dani, Ronak Bhatia, Shubhankur Jain, Paulami Shah
Computer Engineering Department
MPSTME, NMIMS Mumbai, India
pranavswaminathan.nmims@gmail.com
Computer Engineering Department
MPSTME, NMIMS Mumbai, India
tejasdani.nmims@gmail.com
Computer Engineering Department
MPSTME, NMIMS
Mumbai, India
ronakbhatia1.nmims@gmail.com
Computer Engineering Department
MPSTME, NMIMS Mumbai, India
shubhankur.nmims@gmail.com
Assistant Professor
Computer Engineering Department
MPSTME, NMIMS Mumbai, India
paulami.shah@nmims.edu

***Abstract*— The advent of modern technology has provided us with a platform to exchange information on a massive scale. There is always a threat of intercepting this confidential information which ultimately calls for some sort of security measure to allow uninterrupted flow of information from the sender to the receiver. Already devised methods like cryptography and steganography have been referred to as the flag bearers in this field. Cryptography is a process where a person changes the meaning of the original data by converting it into a cipher text. And steganography, on the other hand helps in hiding the cipher text or plain text in a medium thereby obscuring its existence. Both these methods are tested methods of providing security. In today's information age, information sharing and transfer has increased exponentially. The concern around making secret information completely threat free has been a daunting problem for the experts. Cryptography combined with steganography can certainly be used to overcome this threat. The two methods of cryptography and steganography when combined help in achieving significant levels of data security thereby proving to be a better method than these processes being used as standalone ones for transmitting data over an insecure channel which is susceptible to intrusion. One of the most secure forms of steganography is Visual Steganography which is implemented commonly in image files. There might be some changes in the colour frequency of the image when the data text is embedded which would become very obvious to the person seeing it. In order to overcome the conspicuous behaviour of the image, we propose layers of data protection where the data text will first be converted to an unreadable cipher followed by embedding the cipher into an image file in an encrypted format which will then be divided into shares to achieve another layer of security. Hence, the concept of cryptography and steganography both are used to provide two layers of security followed by visual cryptography scheme to divide the image into shares for it to be transmitted over a network channel.**

***Keywords*— Visual Cryptography, Steganography, cipher text, key, shares, VCS**

A. Abbreviations and Acronyms

TABLE I
ABBREVIATIONS AND DESCRIPTION

Abbreviation	Description
AES	Advanced Encryption Standard
LSB	Least Significant Bit
VCS	Visual Cryptography Scheme
EVCS	Extended Visual Cryptography Scheme
PNG	Portable Network Graphics
JPEG	Joint Photographic Experts Group

I. INTRODUCTION

After doing a comparative study of various encryption algorithms, we decided to use AES encryption algorithm in order to encrypt the text thereby providing the first layer of security. The US National Institute of Standards and Technology approves the use of AES with 192 or 256 bit keys for encryption which is a feature of being able to incorporate large blocks of texts [6]. Below are the steps about how the

DOI: 10.18535/ijecs/v5i10.29

different levels of security are achieved in order for a successful transmission to happen without the loss of information.

A. *Encryption Phase*

In this phase, the original data to be encrypted is given as input by the user. The text information inserted by the user in the text area provided is called the original data (confidential data) [1]. The encryption algorithm used is AES (Advanced Encryption Standard).

Fig.1. Encryption Phase

B. *Encoding Phase*

In the encoding phase, the encrypted data which is obtained is written into a suitable image. After getting the result of the previous phase in the text area, the data will be encoded into an image which the user will select from a list of images available to him. When the image file of the extension .png or .jpg is selected [1], it is first loaded and the image is converted into a byte representation. The modification of the image is facilitated by the obtained byte representation. The cryptic or the cipher data is also converted into the byte format. Bit by bit, the cipher data is added to the image byte array at its least significant bit using bit-wise operations [2]. The image in which the cipher text is stored is called as the stego image.

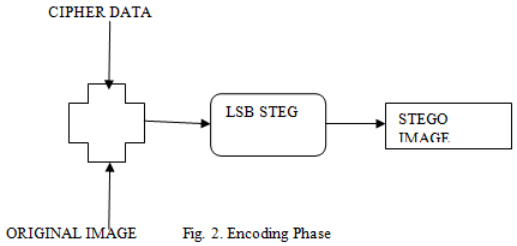

Fig. 2. Encoding Phase

C. *Decoding Phase*

In the decoding phase, the encrypted data is retrieved from the stego image. This is done by inversing the encoding process which was used before at the sender side [1].

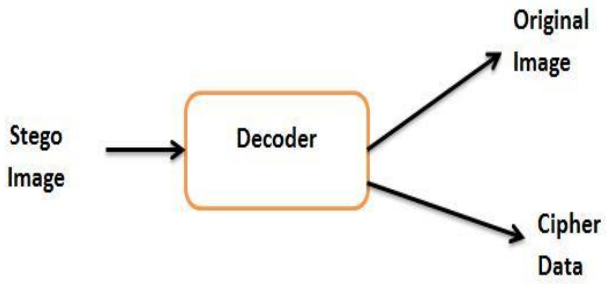

Fig.3. Decoding Phase

D. *Decryption Phase*

In the decryption phase, the cipher data is converted into the original data. The algorithm which is used in the method of encrypting the original data uses the same encryption key while decrypting the data to give back the. AES algorithm uses the same secret key (encryption key) in the inverse manner as well which was used during encryption too [3]. Finally, the original text will be displayed.

Fig.4. Decryption Phase

Although, at times, it might be cumbersome to safely pass around the key from one person to another, there is another additional advanced method which provides one more layer of security and is known as Visual Cryptography Scheme (VCS) [7].

E. *Visual Cryptography Scheme (VCS)*

A visual cryptography scheme (VCS) is a sharing scheme which secretly allows the encoding of an image into shares which can be distributed to participants. A major reason for using this scheme is that it requires no prerequisites for cryptography. A visual cryptography scheme (VCS) consists of meaningful shares. Here, the method is construction of a VCS which is realized by embedding random shares into meaningful covering shares [7]. They provide competitive visual quality compared to other forms of cryptographic schemes.
Purpose of the VCS is that it takes a secret image as input, and outputs shares that satisfy two conditions:
1) The secret image can be recovered by any number of qualified subset of shares.
2) Apart from the size of the secret image, any forbidden shares subset cannot retrieve any information of the secret image.

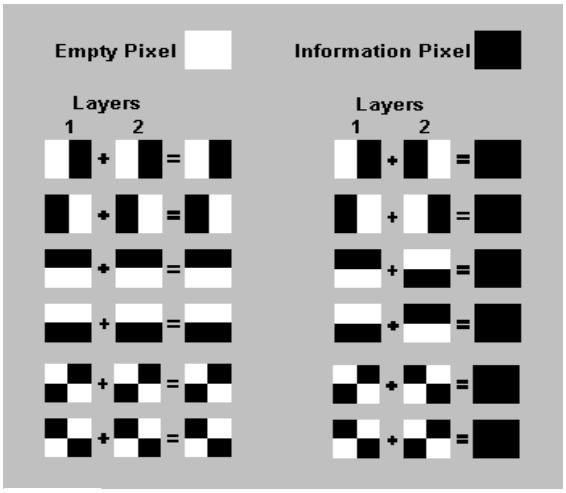

Fig.5. Explanation of expansion of pixels

The above figure shows states that the layers of the divided pixel can assume. If the pixel is divided into 4 parts, we can obtain 6 states as shown above. Pixel states of layer 1 might be in a given state and pixel state of layer 2 may have one of two states: identical or inverted to the pixel of layer 1.

DOI: 10.18535/ijecs/v5i10.29

1) If the pixel of layer 2 is identical to layer 1, the over layer pixel will be half black and half white.
2) If the pixels of layer 1 and 2 are inverted or opposite, then we will have a completely black one.

II. SIMULATION RESULTS AND ADVANTAGES OF PROPOSED SYSTEM

VCS is flexible as it allows the existence of two trade-offs amidst the visual quality and the pixel expansion of the shares and also between the visual quality of the shares and the secret image expansion of the pixels [5]. Due to this flexibility, the dealer has the freedom to choose proper parameters for different applications.

With VCS adding an extra layer of security for successful transmission of confidential information, the stego image itself can be broken down into shares and passed through any medium. Even if one share is intercepted by a hacker, it won't make sense to him at all as the entire information is revealed only when all the shares are overlapped. Following is our simulation result where an image contains cipher text embedded inside it using AES algorithm, thereby making it the stego image [7]. This stego image is then divided into 5 shares. Note how the stego image is obtained only when all the 5 shares are overlapped.

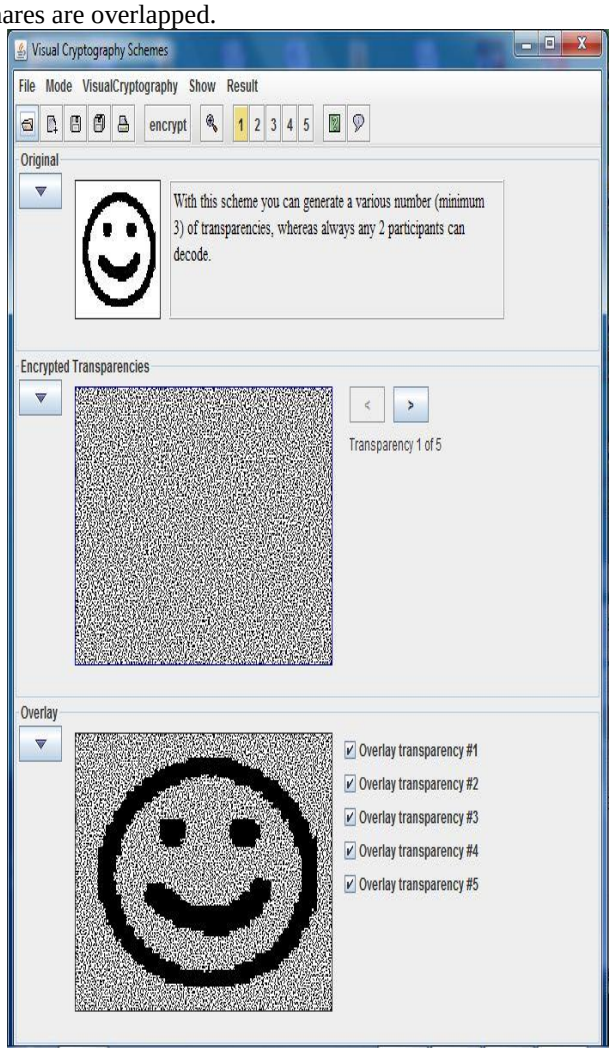

Fig.6. 5 out of 5 transparencies overlap

This is a lossless technique where the exact information is recreated just as it was when it was encrypted. Note here that the possession of just one share will lead the interceptor to no information thereby safeguarding the integrity of the information and staying in line with the rules of security.

III. CONCLUSION AND FUTURE SCOPE

This visual cryptography steganography in images can be extended onto application software which could be meticulously used for the purpose of any type of image formats to hide any type of file inside them. The main advantage of this application will be in supporting any type of pictures without needing to convert the image to bitmap. Steganography, like cryptography, will play an intensifying role in the future of safe and secure communication in the world of digital media. Security of web applications can be raised by prompting the user to provide the secret key after which the password can be compared with the image files using the key. The proposed system has discussed implementation of securely using least significant bit manipulation based steganography that uses the AES algorithm.

VCS is an unbreakable method to hide a highly confidential message. Without the receiver possessing all the shares of the divided image, it will be plain black and white image for him. Also, it is useful in places where people have less knowledge of encryption and decryption like in army fronts or on military assignments [8].

The three layers of security should be sufficient enough to transmit messages in a contaminated network channel.

ACKNOWLEDGMENT

For this project, we would like to thank our families for their continuous support and faith in us.

REFERENCES

[1] Goel, M. K., & Jain, D. N. (2012). A Novel Visual Cryptographic Steganography Technique. *International Journal Of Computer, Electronics and Electrical Engineering*.

[2] Goel, M. K., & Jain, D. N. (2012). A RSA- DWT BASED VISUAL CRYPTOGRAPHIC STEGANOGRPHY TECHNIQUE. *International Journal Of Advanced Research In Computer Science And Electronics Engineering*, 95-99.

[3] Gupta, R., Jain, A., & Singh, G. (2012). Combine use of Steganography and Visual Cryptography for Secured Data hiding in Computer Forensics . *International Journal of Computer Science and Information Technologies*, 4366 - 4370 .

[4] Juneja, M., Sandhu, P. S., & Walia, E. (2009). Application of LSB Based Steganographic Technique for 8-bit Color Images . *International Journal of Computer, Electrical, Automation, Control and Information Engineering*.

[5] Marwaha, P., & Marwaha, P. (2010). Visual cryptographic steganography in images. *Computing Communication and Networking Technologies (ICCCNT)*.

[6] Pahal, R., & Kumar, V. (2013). Efficient Implementation of AES. *International Journal of Advanced Research in*.

[7] Prema, G., & Natarajan, S. (2013). Steganography using Genetic Algorithm along with Visual Cryptography for wireless network application. *Information Communication and Embedded Systems (ICICES)*.

[8] TechRepublic. (2012). Integrating Steganography Using Genetic Algorithm and Visual Cryptography for Robust Encryption in Computer Forensics. *International Journal of Electronics and Computer Science Engineering*.