Enhancing Stego Image Security Using Visual Cryptography and Biometrics

Ayyappadas K.1, Manusankar C.2, and Balasankar C.3

1Dept. of IT, MEA Engineering College, Perinthalmanna, India
Email: ayyappadask@gmail.com
2Dept. of CSE, Ilahia College of Engineering and Technology, Muvattupuzha, India
Email: manusankarc@gmail.com
3Freelance Developer cum Student Dept. of CSE Adi Shankara Institute of Engineering and Technology, Kalady, India
Email: balu.balasankar@gmail.com

Abstract— The main idea of this paper is to apply the Biometric template Encryption (encryption using biometric template) along with Visual cryptography to secure our valuable stego images. In the proposed scheme visual cryptography is applied to the stego image to get the image divided into parts and each part is encrypted using users biometric template and generate the biometrically encrypted visual cryptographic shear (BEVS) image to provide an extra layer of authentication to the users and send through the communication channel. The original image is available only when each BVES image is decrypted by the users biometric template and each part do not reveal any information about the original image. The original stego image can be viewed only when each image are simultaneously available.

Index Terms— Visual cryptography, Biometrics, Secure, Stego Image, Authentication

I. INTRODUCTION

Visual cryptography (VC) was invented by Naor and Shamir [2] in 1995. Visual cryptography allow secret sharing of images without any cryptographic computations. In this paper visual cryptography is used. K-out-of-n visual cryptography scheme is used which is denoted by (k,n)VCS. The steganography is not new today. In fact several examples from the times of ancient Greece are available. Steganography differs from Cryptography in the sense that where cryptography focuses on keeping the contents of a message secret, steganography focuses on keeping the existence of a message secret. A block diagram of a generic image stenographic system is given in Figure 1. A message is embedded in a digital image (cover image) through an embedding algorithm, with the help of a secret key. stego image is transmitted over a channel to the receiver where it is processed by the extraction algorithm using the secret key. The most common and simplest image embedding method is the least significant bit (LSB) insertion. The LSB insertion embeds the message in the least significant bit of some selected pixels of the cover image. Rao Y. et al[7]. gives an analysis of lsb based steganography techniques. The embedding capacity of LSB method can be increased by using two or more least significant bits. At the same time, not only the risk of making the embedded message statistically detectable increases but also the image fidelity degrades. Hence a variable-sized LSB embedding scheme is presented in , in which the number of LSBs used for message embedding /extracting depends on the local characteristics of the pixel. The advantages of LSB-based method are easy to implement.

II. RELATED WORK

Sharing Single Secret Naor and Shamir’s[2] proposed encoding scheme to share a binary image into two shares Share1 and Share2. If pixel is white one of the above two rows of Table 1 is chosen to generate Share1 and Share2. Similarly if pixel is black one of the below two rows of Table 1 is chosen to generate Share1 and Share2. Here each share pixel p is encoded into two white and two black pixels each share alone gives no clue about the pixel p whether it is white or black[1]. Secret image is shown only when both shares are superimposed. In image based steganography methods. The most common and simplest image embedding method is the least significant bit (LSB) insertion. The LSB insertion embeds the message in the least significant bit of some selected pixels of the cover image. Rao Y. et al[7]. gives an analysis of LSB based steganography techniques. The embedding capacity of LSB method can be increased by using two or more least significant bits. At the same time, not only the risk of making the embedded message statistically detectable increases but also the image fidelity degrades. Hence a variable-sized LSB embedding scheme is presented in , in which the number of LSBs used for message embedding /extracting depends on the local characteristics of the pixel. The advantages of LSB-based method are easy to implement.

<table>
<thead>
<tr>
<th>Pixel</th>
<th>Probability</th>
<th>Share1</th>
<th>Share2</th>
<th>Share1 + Share2</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>50%</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>50%</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>50%</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>50%</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
III. PROPOSED SYSTEM

In order to enhance the authentication of the stego images, visual cryptography technique and encryption of the images using users biometric template are applied. To ensure that proper person is accessing the message. The secret image is initially assigned. Then the shares are generated. The system architecture of the proposed system is shown in figure 2. The secret image is initially assigned. Then the shares are generated. Next shares after encrypting it with the biometric features of the user are stored. Next the stored shares were decrypted and then all the shares is stacked to reveal all the secrets. This work explores the possibility of using visual cryptography for imparting privacy to biometric templates. During the enrollment process, the private data is sent to a trusted third-party entity. Once the trusted entity receives it, the data is decomposed into images and the original data is discarded. The decomposed components are then transmitted and stored in two different database servers such that the identity of the private data is not revealed. During the authentication process, the trusted entity sends a request to each server and the corresponding Share is transmitted to it. Share are superimposed in order to reconstruct the private image thereby avoiding any complicated decryption and decoding computations that are used in watermarking, steganography, or cryptosystem approaches. Once the matching score is computed, the reconstructed image is discarded. Further, cooperation between the two servers is essential in order to reconstruct the original. Since the spatial arrangement of the pixels in these images varies from block to block, it is impossible to recover the original template without accessing the shares. The XOR operator is used to superimpose the two noisy images and fully recover the original template. It is observed that the reconstructed images are similar to the original private image. The shares are stored after encrypting it with the biometric features of the user, gives the bevs image. Then the bevs image is sent through the communication channel. At the receiver end, the stored shares are decrypted and then all the shares are stacked to reveal all the secrets. Figure 2 represents the block diagram for securing the stegno image.

CONCLUSIONS AND FUTURE WORK

In this paper a method is proposed to enhance the authentication of stego image, visual cryptography and biometric template are used, to ensure that the person who is accessing the image is an authorized one. If he is an authorized person then the system reveals the bevs image. The system is more complicated, but provides more security and authentication. And using other type of visual cryptography meaningful share is generated which also can be applied. The biometric templates are also vulnerable to theft so more secured templates are needed for encryption and decryption. This work explores the possibility of using visual cryptography and biometrics for imparting privacy. The study on the effect of various parameters and on the matching performance suggests that there is indeed a relation between the quality of the reconstructed secret and these parameters. Finally, demonstrate the difficulty of exposing the identity of the secret image by using only one of the Share. Increasing the pixel expansion factor can lead to an increase in the storage requirements for the Share. In the recent literature there have been some efforts to develop a VCS without pixel expansion, for generating Share that are not random noisy images. Thus, more work is necessary to handle this problem. Future work involves enhancing the capabilities of the proposed architecture to handle peer–peer network to store the encrypted Share.
REFERENCES


Ayyappadas K. is presently a Faculty at Department of Information Technology, MEA Engineering College, Perumthalmanna, Kerala, India. He completed his M.E. degree in Computer Science and Engineering from Anna University of technology Coimbatore in 2011 and his B.Tech degree from MG University in 2008. His research interest includes Web Services, Network Security and Web Technology. He is a Cisco Certified Network Associate and a member of CSI.

Manusankar.C is presently a Faculty at Department of Computer Science & Engineering, Ilahia College of Engineering and Technology, Muvattupuzha, Kerala, India. He completed his M.E. degree in Computer Science and Engineering from Anna University of technology Coimbatore in 2011 and his B.Tech degree from MG University in 2008. Before joining PG Study in the year of 2009, he was a Technical Support Executive at the virus removal wing of Sutherland Global Services, Cochin, Kerala, India. He has completed the MCSA, CCNA and CISE courses and currently doing Certified Ethical Hacker Course (CeH). His research interest includes Computer Security, Network Security, Computer Networks and Bio Informatics. He is a member of Computer society of India. He has published more than 12 articles in International/ National Journals/Conferences.