INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH & DEVELOPMENT

ISSN 2278 – 0211 (Online)

(N, 1) Secret Sharing

Tejal M. Tillu
Department of Computer Engineering, K. J. Somaiya College of Engineering, Mumbai, India
Preeti R. More
Department of Computer Engineering, K. J. Somaiya College of Engineering, Mumbai, India

Abstract:
In this, paper we propose a novel approach of (N,1) Secret Sharing. This approach aims to embed secret data in images based on Steganography with color images. The cover image is the one behind which the text data is hidden. There are 'N' such cover images and one stego image. The stego image is the last image or 'N+1' image. We present the approach for embedding the secret data as well as extracting this data on the receiver side. The cover images are colored images that would be sent to the receiver side through a secured channel. The sender will send the last image i.e. stego image or N+1 image through the unsecured channel to the receiver. The receiving end would require all the N cover images in sequence and the +1 stego image to retrieve the entire secret data.

1. Introduction

Data security is the practice of keeping data protected from corruption and unauthorized access. The focus behind data security is to ensure privacy while protecting personal or corporate data. Privacy of data is the ability of an individual or group to seclude the information and reveal it selectively. But there is a threat to the privacy of data while sharing. The hackers are likely to intrude the data on the path between sender and receiver. There are many problems arising due to illicit interception of data. To prevent the data from being intruded, an approach for keeping the data secured is necessary. Steganography is one of the method`s that is capable of hiding the secret data in a host medium and conveys the hidden data. More importantly, it conceals the existence of embedded data and in the best case; a third party cannot recognize that both parties are communicating in a secure manner. Among the different kinds of digital media, digital imagery is most widely used data type for information hiding.

2. Image based Steganography

Image based Steganography allows textual data to be hidden behind image. In an image-based hiding system, the original image used to embed secret data is called the cover image. The intended recipient can then extract the secret data from the cover image. In the business world image steganography can be used to hide a secret chemical formula or plans for a new invention. It can also be used for corporate espionage by sending out trade secrets without anyone at the company knowing about it. Image based Steganography can also be used to keep private digital information protected for number of purposes such as secret data hiding, copyright protection, data authentication, ensuring authenticated data availability for academic usage, monitoring of data piracy, ownership identification, providing confidentiality and integrity enhancement.

3. Problem with Image Steganography

The hidden data behind an image should make a visually imperceptible change to the cover image when viewed at that image level for any unintended recipient. In order to achieve this imperceptibility, the image-based hiding systems must provide high visual quality of a cover image. This requirement creates a conflict between two performance objectives. First, the sending party has to apply the least modification to a cover image to provide high embedding efficiency. Conversely, one has to embed the maximum amount of secret data to the cover image to provide high capacity. Therefore, an acceptable compromise between high embedding efficiency and high embedding payload must be made by users, depending on their different desires. Recently, many steganography schemes have been developed. Likewise, many researchers have also been interested in compromising such schemes by detecting the secret data. As the steganalysis systems have been developed, the conventional image-based hiding schemes have not been sufficient to achieve the imperceptibility of the stego image.

4. Proposed Approach

A remedy to this problem has been proposed as the concept of (N,1) secret sharing. It takes input data from the user and hides it behind 'N' images called the cover images. The N number of cover images depends upon the size of the data. At the sender side the input data is divided into N chunks. The size of each chunk is such that embedding it behind the cover image would not affect the image quality. The N chunks are embedded behind 'N' cover images. These cover images are sent to the receiver over the secured channel. The channel is made secured as the N images travel through different nodes. The intruder will have to know the different paths through which the data is being transmitted to get access to all N images. This protects the data from intrusion and makes the channel secured. The sender is asked to enter a password after uploading the input data file to be transferred. This password acts as a key. The last image which is plus 1 stego image, contains the key, the order of the N images and the code of how the data is encrypted behind each cover image. The order is necessary to re-arrange the N images at receiver side to decrypt the hidden message. This stego image is generated using the hash key algorithm. The stego image would be sent via an unsecured media such as internet. The system would allow user to enter any size of text data. This would eliminate the previous problem of data size limitation. Also the computation of embedding data behind each image is reduced. The resultant N cover images are of high quality which prevents them from being detected of having hidden data.

5. Working of System (Implementation)

The presented approach allows the user to embed their secret textual information in images in a way that can be invisible and does not degrade or affect the quality of the original image. This system provides an efficient way for secure transfer of information.

5.1. Input textual data

Input the text file containing the data which user wants to send over to the intended recipient. The input text file is read by our system and is divided into N number of chunks.

5.2. Input Images

The system contains an image repository consisting of high quality images. Depending on the number of chunks created, the value of N is decided. N numbers of images are retrieved from the repository. When the data is encrypted behind images they are called as cover images.

5.3. Encoding data behind images

Each chunk of textual data is encrypted behind one of the N images. After the encryption is complete the sender is asked to enter a password. This password acts as a key and is necessary at the receiving end to decrypt the data.

5.4. Stego Image

The stego image contains important information such as the sequence of N cover images. Also the stego image contains the algorithm for decryption of data.

5.5. Transmission of (N, 1)

The N cover images are transmitted over the network over to the receiving end. On the path of transmission, each cover image is transmitted via a different node of the network. This reduces the imperceptibility of data. The +1 stego image is transmitted to the receiving end over un-secured medium such as internet.

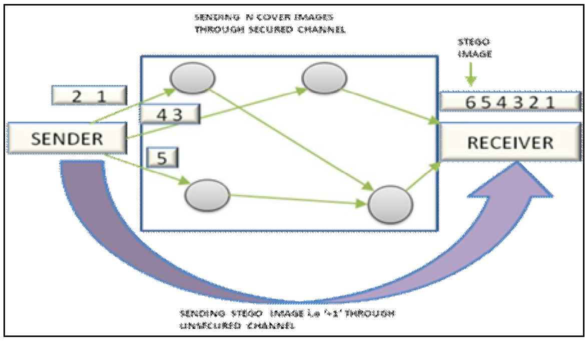

Figure 1

5.6. Decoding of data behind images

To recover the secret data, the receiver needs all N cover images and the +1 Stego image along with the key. The receiver must have these three vital parts to decode the data. The user is asked to enter the password which is the key. On entering the correct key, the application executes and the data is decoded. The resultant secret data is stored in a new textual file on the receiver`s machine.

Any two machines on the network can play the role of a sender and a receiver.

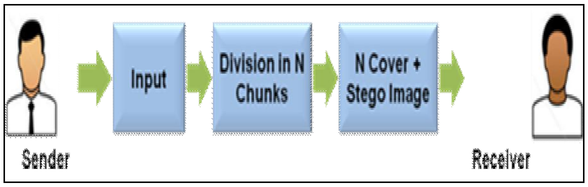

Figure 2

6. Experiments

The experiments conducted show the following outputs. These are the resultant images using different encryption approaches.

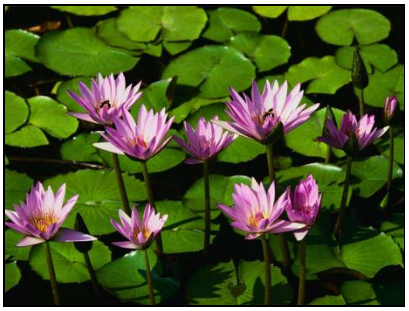

Figure 3: Original Image

- The quality of the image gets degraded when moderate amount of data is encrypted behind image using the older approach.

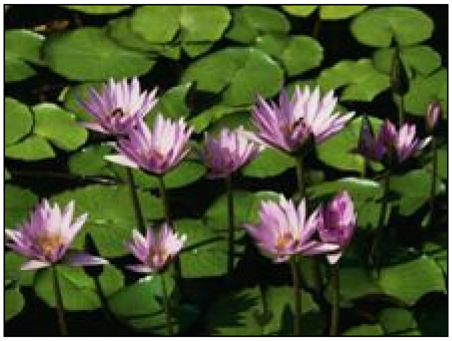

Figure 4: Steganography behind single image with moderate data

- The image gets distorted when the amount of input data is bulky.

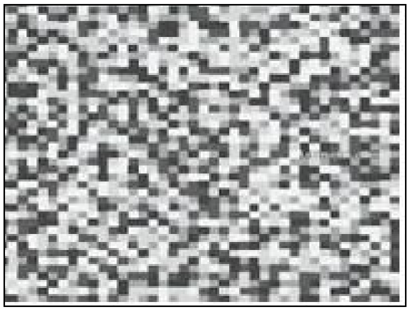

Figure 5: Steganography behind single image with bulky data

- The quality of the original image is maintained with the (N, 1) approach.

Figure 6: Image with encrypted data using (N,1) approach

7. Advantages

This approach has many advantages over existing schemes.

- It requires least modification of the original image, resulting in the required high quality of the cover image.
- It allows us to fully utilize all available original image pixels to hide the secret data. This feature provides high embedding payload.
- The conversion process does not require high computational overhead.
- Finally, the successful interception of the cover image does not provide any clue of the secret data, because the extraction of secure data is possible only when a party has all N cover images and one stego image in a correct order.

8. Conclusion

Data privacy or information privacy is the relationship between collection and dissemination of data, technology, the public expectation of privacy, and the legal issues. Our system fulfills the expectancy of all such fields. The target users of the proposed system are those who want to make their information secure or protect their work form other or illegal use. The data fed as an input by the user is getting embedded into the image. The quality of the image is maintained to be high resolution preventing it from being suspected of containing data. The retrieval of the message from the images is successful at the receiving side.

9. References

1. A Hash-Based Approach for Color Image Steganography.(Rubata Riasat, Imran Sarwar Bajwa, M. Zaman Ale 978-1-61284-941-6/11/$26.00 ©2011 IEEE)
   (N. 1) Secret Sharing Approach Based on Steganography with Gray Digital Images. (Jinsuk Baek, Cheonshik Kim, Paul S. Fisher, and Hongyang Chao 978-1-4244-5849-3/10/$26.00 ©2010 IEEE)
2. Secured Secret Color Image Sharing With Steganography. (L.Jani Anbarasi, S.Kannan ISBN: 978-1-4673-1601-9/12/$31.00 ©2012 IEEE)