INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH & DEVELOPMENT

ISSN 2278 – 0211 (Online)

Dynamic Collage Steganography on Images

Aswathi P. S.
Student Member IE, CSI, VAST, Thrissur, Kerala, India
Sreedhi Deleepkumar
Student Member IE, CSI, VAST, Thrissur, Kerala, India
Maya Mohanan
Student Member IE, CSI, VAST, Thrissur, Kerala, India
Swathy M.
Student Member IE, CSI, VAST, Thrissur, Kerala, India

Abstract:
Collage steganography, a type of steganographic method, introduced to hide the secret message. This paper presents a new generalized collage steganography, an augmentation of collage steganography, to improve the capacity problem since the limitation of the traditional method is capacity. The secret messages such as text, file, pdf, etc. are converted into a certain bit format and to an object image. Then it is appended into a cover image. So that the other persons will not notice that such data is there. This is the major distinction of this method with the other method of hidden exchange. This file is transferred from sender to receiver in a proper networking channel by using the mail system. A proper cover image is chosen based on an object image. The selected object image and the rotation, translation and scaling factors in the affine transformation are used to append the object image into the cover image. The information is retrieved by using the dynamic method, the sender can encrypt the message and on the other side, the receiver decrypts it. Several steganographic image examples are illustrated. In this paper one such method is shown with high efficiency.

Keywords: *Generalized collage steganography, dynamic algorithm, angular algorithm, embedding capacity, image steganography, embedding data, information hiding, collage, steganography, data hiding*

I. Introduction

Today the internet is one of the tool for human life while being a necessary means of living in many developed countries where it is used for shopping, communicating with other carrying out transaction, etc. Although hidden exchange of information has been an important issue since old times today the age of communication and information (ICT) and especially with the development of the Internet and its use in information systems, the issue of information security has become increasingly important. One of the grounds for discussion in the field of information security is the hidden exchange of information. To this end, various methods such as steganography have been used.

The word “steganography” is a Greek word which means ‘hidden writing’. While implementing this method, the main aim is to hide data in a cover media so that other persons will not notice the existence of such data. This is a major distinction of this method with the other methods of hidden data exchange. For instance, in cryptography methods the individuals receiving the encoded data notice that such secret data exists but they cannot comprehend it. However, in steganography, the individuals will not notice the existence of such data in the sources [1]. In steganography the main goal is the transfer of the hidden data in the cover source and thus its quality should be preserved during the subsequent processes.

Steganography is a data hiding technique used to transmit a cover media with secret information through public channels of communication between a sender and a receiver avoiding perceptually detection from an observer. Possible carriers of secret information are text, audio, image, video, and other files.

This paper proposes dynamic collage steganography, which is a new type of steganographic method.The advantage of this method is that the huge size of text file can also be embedded using this technique. Here the text message is converted into an image format and then it is appended to the cover image. The algorithm used for this process is angular algorithm and it is enhanced by using the dynamic algorithm. Two dimensional images, are selected as cover files in this paper.

1.1. Parameters

1. Embedding capacity: It refers to the aggregate data that can be inserted into the cover-media without deteriorating its integrity.
2. Perceptual transparency: It is necessary that to avoid idea of embedding the data should occur without significant degradation or loss of perceptual quality of the cover media.
3. Robustness: It refers to the ability of embedded data to remain intact if the stego-image undergoes various transformations like rotation, scaling, cropping or compression.
4. Computational complexity: Computational complexity of steganography technique employed for encoding and decoding is another consideration and should be given importance.

Among steganography methods, the most common approach is to use images as the cover media for applying steganography (because the redundancy of information in images is high).Various image steganography methods reported in the literatures can be classified into three major groups: temporal methods, transform domain methods, and fractal methods.

In temporal methods, the data in question are added to quantities of luminosity of pixels in the image.[3].

In transform domain methods, first the image is transferred into another domain. The information is hidden in that domain and finally the image is transferred back to the spatial domain using the related inverse transform. [4].

In fractal methods, blocks of images that contain repeated patterns are selected and the information is embedded in them [5].

1.2. Steganalysis

Steganalysis [4], from an opponent's perspective, is an art of secret communications while avoiding affecting the innocent ones. Its basic requirement is to determine accurately whether a secret message is hidden in the testing medium. Further requirements may include judging the type of the steganography, estimating the rough length of the message, or even extracting the secret message [5]. They try to defeat each other and also develop with each.

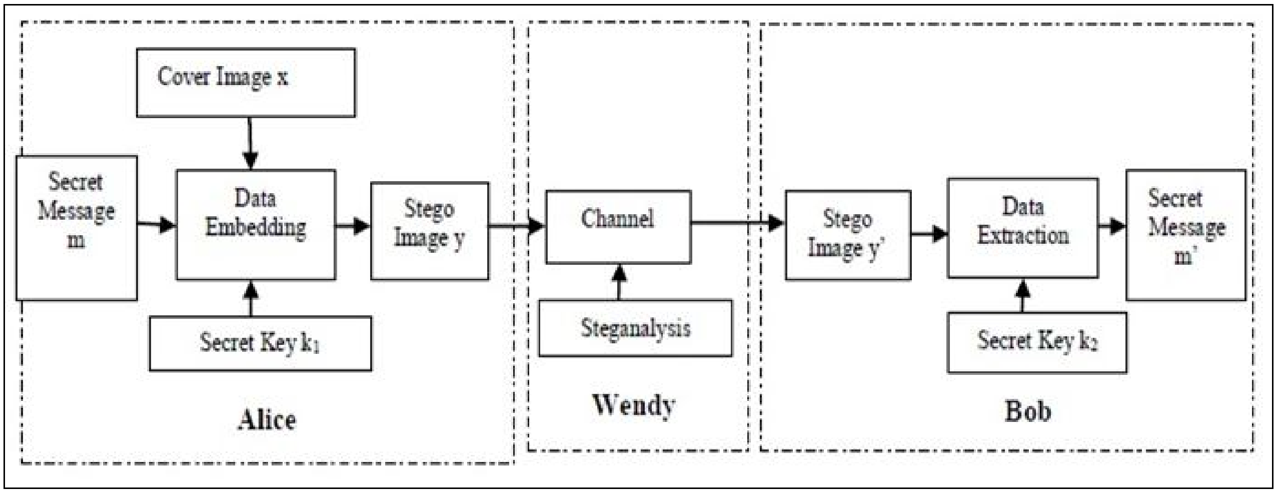

Figure 1: The Model of Steganography and Steganalysis [4]

The organization of the paper is as follows. In Section 2, the original “Collage Steganography” method [12] is described. The hiding phase of the new method is very similar to the original “Collage Steganography” method. Our new proposed method is explained in Section 3. The discussions and methods are mentioned in Section 4. Finally, Section 5 concludes the paper.

2. Original Collage Stegnography

In this method, first a picture is selected as the background image. Then, the images of a number of appropriate objects related to the background are selected. Each of these objects is selected from various types of that object. The figure shown below is an example of the collage steganography.

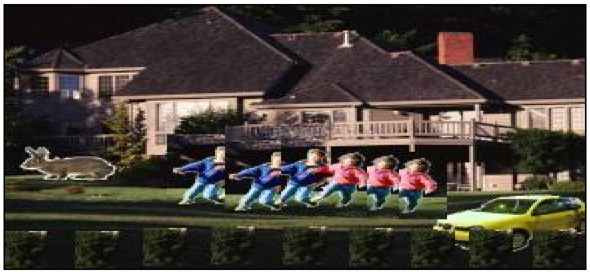

Figure 2

3. Proposed Collage Steganography

Establishing hidden communication is an important subject of discussion. In this project one such method is shown with high efficiency. The major characteristic of these methods is improving the capacity of data that can be sent. While implementing this method, the main purpose is to hide data in a cover media so that other persons will not notice that such data is there. This is a major distinction of this method with the other methods of hidden exchange.

The method of steganography have been mostly applied to images. While the major characteristic of these methods is the change in the structure and features of the images so as not to be identifiable by human users like hackers. Considering that in this method information has been hidden in the appearance of the picture, then by using the present methods of identification of stegano images one cannot identify the steganography images in this method or extract data from them. Here we are representing information in the form of images. Images of a number of relevant objects are put on a scene together in a way that is not noticeable. The information is retrieved via angular algorithm. To improve the capacity we also introduce the dynamic algorithm for the encryption and decryption.

3.1. Image Coordinate Representation

Prior to presenting the generalized collage steganographic method, the image coordinates representation is described as follows. Suppose an image is of the size $M \times N$, which indicates the image has M rows and N columns. The image pixel coordinate is defined as index (x,y), where x indicates the row index and y column index.

3.2. Proposed Encryption:

In our proposed system we have a new method by which the data is totally safe and cannot be tracked by other people who want to misuse the data. Considering that in this method information has been hidden in the appearance of the picture, then by using the present methods of identification of stegano images one cannot identify the steganography images in this method or extract data from them.This information is encrypted using the proposed encryption technique as proposed above to obtain another image which is the object image. Then this image is appended to a cover image. This image is sent to the receiver through the network by using the mail system. Here we use the method of angular encryption and as an enhancement we use the dynamic algorithm for the encryption.

3.3. Proposed Decryption:

The receiver obtains the image, decrypts it to obtain the text an d analyses this text with the cover image to reconstruct the object image. This object image is once again decrypted to obtain the original message. The message is decrypted by the reverse process by using the same angular and dynamic algorithm.

3.4. Block Diagram of Proposed Model

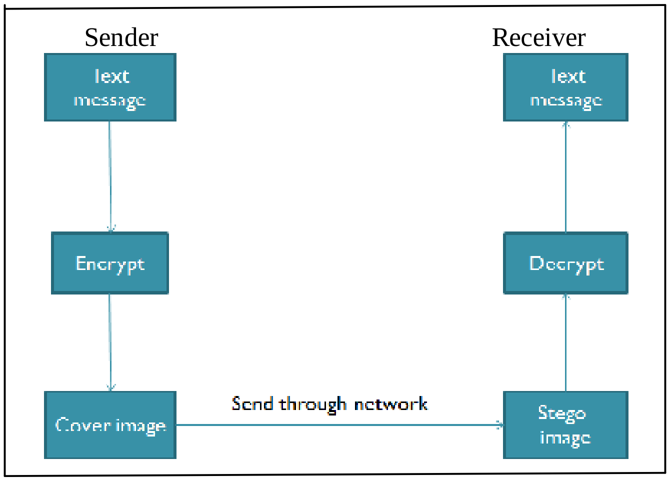

Figure 2: Block Diagram of Proposed Model

3.5. Mail System

The message is transferred from the sender to receive through the system. The system is a normal mail transfer system and additionally it contains the Encryption and Decryption techniques.

4. Discussions

4.1. Angular Encryption

Angular encryption algorithm accepts the confidential message M, a cover image and a random point P(x,y) on the image as input. The three consecutive characters of the messages are embedded in the R,G and B value of a single pixel. Therefore the steps from 2.1 to 2.11 in the algorithm is repeated one by third times the number of characters in the message. The angle θ is computed as the angle between the line P(x,y) C(x,y) and the line from perpendicular to the line P(x,y) C(x,y) to the point C(x,y) as shown in figure1. Hence θ can be computed as cos inverse of (P(x)- C(x)) / d[13].

The value of each of the three consecutive characters are XORed with‘d’ which is the distance between P(x,y) and C(x’,y’) and is then left shifted θ times. Then the resultant three 8-bit values are XORed respectively, with the R,G and B value of a random pixel from the key image and the resultant is set in the cipher image.

4.1.1. Algorithm Angular Encryption

```
•  Input:  Key Image, P(x,y), Secret Message(M)
•  Output:  object Image
1.  Compute n as (length of M) / 3
2.  For i ranging from 0 to n
    2.1. Find the pixel to be set in the cipher as C(x,y)
             Where x = i % (width of key image)
             y = i / (width of key image)
    2.2. Calculate θ = angle between C(x,y)and P(x, y)
    2.3. Calculate d = number of pixels between the
             C(x,y) and P(x, y).
    2.4. Compute ASCII value of the three consecutive characters from position i.
    2.5. XOR the ASCII values with d
    2.6. Shift the resultant 8-bit binary values θ times to the left
    2.7. Compute x1= 13*(i+p(x)+x1) and y1= x1+p(y)
    2.8. If p’(x1,y1) is within the key image get rgb value of the point p’(x1,y1) from the cover image
    2.9. Else set x1= (width of key image) / 3 and get the rgb value
    2.10. XOR the rgb value with the value obtained from step 2.6
    2.11. Set the resultant value in the cipher image
3.  Obtain the complete cipher image
End Angular Encryption
```

4.2. Angular Decryption

The confidential message is retrieved from the image by the angular decryption process. The R, G and B value of the pixels in the cipher image is retrieved and exclusive OR operation is performed with corresponding R, G and B value of the random points on the key image obtained from P(x, y). The 8-bit value obtained is the ASCII value of the text message and by encoding them to character values and combining the plain text is generated [12].

4.2.1. Algorithm Angular Decryption

```
•  Input: Object Image , Key Image, P(x,y)
•  Output: Secret Message(M)
1.  Compute n as width of cipher image
2.  For i ranging from 0 to n
    2.1. Compute x1= 13*(i+p(x)+x1) and
             y1=x1+p(y)
    2.2. If p’(x1,y1) is within the key image get rgb value of the point p’(x1,y1) from the cover image
    2.3. Else set x1= (width of key image) / 3 and get the rgb value
    2.4. Obtain the rgb value of the pixel p’(i, 0) in the cipher image and XOR it with the rgb value obtained from step 2.3
    2.5. Find the point in the key image C(x,y)
             Where x = i % (width of key image)
             y = i / (width of key image)
    2.6. Calculate θ = angle between C (x,y) and P(x, y)
    2.7. Calculate d = number of pixels between the C(x,y) and P(x, y).
    2.8. Right shift the resultant from step 2.4 θ times and XOR each with d
    2.9. The resultant is the ASCII value of the character in the secret message and encode to respective characters
3.  Combine the characters to obtain the complete Message
End Angular Decryption
```

The overall processes at the receiver’s side include the decoding of the secret message from the object image. First the object image is decoded from the image. The resultant text is decrypted to generate the object image. The secret message is then decoded from the image using angular decryption.

4.3. Further Enhancement

The Dynamic Algorithm is used as a further enhancement so unlimited amount of data and even huge files can be encrypted and send to the receiver with the aim to avoid the capacity problem [13].

The algorithm at Sender is represented by the following steps.

1. Convert the carrier image to binary.
2. Divide the secret message into blocks, each block consisting of 16 characters (128 bits).
3. Apply encryption process to convert each plain text block into a cipher text block.
4. Keep all the cipher text blocks together to form the complete cipher text.
5. Transform these cipher text to binary.
6. Embed the cipher text into binary image as per the embedding process discussed, and then we get the stego binary image. Now convert this stego binary image to stego image and then send to receiver.

The algorithm at Receiver is as represented by the following steps.

1. Convert the received image to binary.
2. Retrieve the embedded cipher text bits (two from each pixel) from the stego binary image as per the retrieving process discussed.
3. Keep them together, convert to text and divide into blocks, each 16 characters.
4. Apply decryption process to each cipher text block to get the plain text block.
5. Keep together all the plain text blocks, thus we get the secret message.

5. Conclusion

This paper proposes the dynamic collage steganography, a different method from the existing system. The message is hidden in the cover image itself in the form of an image and its considered as a file. We used angular method and as an enhancement used dynamic algorithm. This file is transferred from sender to receiver in a proper networking channel by using the mail system. The message is retrieved by doing the reverse process for the same that can be done within the mail system. It provides high levels of security.The dynamic method is unique and stronger approach of doing steganography with images.

6. References

1. J.C. Judge, “Steganography: Past, Present, Future,” SANS white paper, November 2001, http://www.sans.org/rr/papers/index.php?id=552.
2. F. Hartung and B. Girod, “Copyright Protection in Video Delivery Networks by Watermarking of Pre-Compressed Video,” in Proc. Of European Conf. on Multimedia Applications, Services and Techniques (ECMAST '97), Springer LNCS, vol. 1242, 1997, pp. 423-436.
3. K. Curran and K. Bailey, “An Evaluation of Image Based Steganography Methods,” International Journal of Digital Evidence, vol. 2, no. 2, Fall 2003, pp. 1-40. [10] N. Provos and P. Honeyman, “Hide and Seek: An Introduction to Steganography,” IEEE Security & Privacy Magazine, vol. 3, no. 1, May/June 2003, pp. 32-44.
4. L.M. Marvel, C.G. Boncelet, and C.T. Retter, “Spread spectrum image steganography,” IEEE Transactions on Image Processing, vol. 8, no. 8, 1999, pp. 1075-1083.
5. M. Shirali-Shahreza and S. Shirali-Shahreza, “Collage Steganography,” in Proc. of the 5th Int. Conf. on Computer and Information Science, 2006, pp. 316-321.
6. R. Chandramouli and N. Memon, “Analysis of LSB based image steganography techniques,” in Proc. of 8th Int. Conf. on Image Processing, 2001, vol. 3, pp.1019-1022.
7. D. Kahn, “The history of steganography,” Proceedings of the First International Workshop on Information Hiding, Lecture Notes in Computer Science, vol. 1174, pp. 1–5, 1996.
8. L. A. Bygrave, “The technologisation of copyright: implications for privacy and related interests,” European Intellectual Property Review, vol. 24, no. 2, pp. 51–57, 2002. Infrastructure for the Cloud
9. N. Cvejic and T. Seppanen, “A wavelet domain LSB Insertion algorithm for high capacity audio steganography,” in Proc. of 10th Digital Signal Processing Workshop and 2nd Signal Processing Education Workshop, 2002, pp. 53-55.
10. R. Crandall, “Some notes on steganography,” http://os.inf.tu-dresden.de/~westfeld/crandall.pdf, 1998
11. Shaveta Mahajan and Arpinder Singh “Methods and Approach for Secure Stegnography”Volume 2, Issue 10, October 2012
12. Sajad Shirali-Shahreza and Mohammad Shirali-Shahreza ,”Advanced Collage Steganography ”Bahria University Journal of Information & Communication Technology Vol. 1, Issue 1, December 2008
13. Mei-Ching Chen, Sos S. Agaian, and C. L. Philip Chen,”Generalized Collage Steganography on Images”,Department of Electrical and Computer Engineering ,University of Texas at San Antonio ,USA