Invisible Digital Watermarking Through Encryption

Samir Kumar Bandyopadhyay
Dept. of Computer Sc. & Engg,
University of Calcutta
92 A.P.C. Road, Kolkata – 700009,
India

Tuhin Utsab Paul
Dept. of Computer Sc. & Engg,
University of Calcutta,
92 A.P.C. Road, Kolkata-700009,
India

Avishek Raychoudhury
Dept. of Computer Sc. & Engg,
University of Calcutta
92 A.P.C. Road, Kolkata-700009,
India

ABSTRACT
Technique for hiding the data of images has been proposed in this paper. At the source, hidden (target image) is encoded within another image (cover image). Firstly, the cover image and the target image can be adjusted by resize function. Secondly, only the final encrypted image i.e. cover image and target image is sent over the network. This image is finally decoded at the receiver end. Received results are encouraging from practical point of view.

Keywords
Data, image, Hiding, Security, Encryption

1. INTRODUCTION
Invisible digital watermarks are a new technology which could solve the "problem" of enforcing the copyright of content transmitted across shared networks. They allow a copyright holder to insert a hidden message (invisible watermark) within images, moving pictures, sound files, and even raw text. Furthermore, the author can monitor traffic on the shared network for the presence of his or her watermark via network system. Because this method conceals both the content of the message (cryptography) and the presence of the message (steganography) an invisible watermark is very difficult to remove. Thereby, this technology could greatly strengthen the enforcement of copyright law on the Internet.

Data hiding is defined as the process by which a message or image is imperceptibly embedded into a host or cover to get a composite signal. Generally, in encryption, the actual information is not maintained in its original format and thereby it is converted into an alternative equivalent multimedia file like image, video or audio, which in turn is being hidden within another object. This apparent message is sent through the network to the recipient, where the actual message is separated from it.

In this paper, our first consideration is that of embedding information into image, which could survive attacks on the network. Next, digital embedding technique is proposed for hiding an image into another image in such a way that the quality of the recovered image improves significantly.

In most of the algorithms designed based on the principle of data hiding, requires the sending original cover image along with the encoded cover image to the receiver. This approach makes the designed algorithm weaker as it conveys some idea of data hiding to the sender. But our method only the encrypted image will be sent to the receiver.

The design of this technique is based on extensive analysis of the data-hiding process.

2. PREVIOUS WORKS
Miroslav Dobsicek [1] has developed method where the content is encrypted with one key and can be decrypted with several other keys, the relative entropy between encrypt and one specific decrypt key

Yusuk Lim, Changsheng Xu and David Dagan Feng, 2001, developed the web based authentication system. In case of watermark embedding system, it is installed in the server as application software that any authorized user, who has access to server, can generate watermarked image. The distribution can use any kind of network transmission such as FTP, email etc. Once image is distributed to externally, client can access to authentication web page to get verification of image [2].

Min Wu and Bede Liu, June 2003, proposed [3] a new method which manipulates "flappable" pixels to enforce specific block based relationship in order to embed a significant amount of data without causing noticeable artifacts. The hidden data can then be extracted without using the original image and can also be accurately extracted after high quality printing and scanning with the help of a few registration marks.

In 2007, Nameer N. EL-Emam proposed data security using LSB insertion steganographic method. In this approach, high security layers have been proposed through three layers to make it difficult to break through the encryption of the input data and confuse steganalysis too [4]. Rehab H. Alwan, Fadhil J. Kadhim, and Ahmad T. Al- Taani, 2005, have explained a method with three main steps. First, the edge of the image is detected using Sobel mask filters. Second, the least significant bit LSB of each pixel is used. Finally, a gray level connectivity is applied using a fuzzy approach and the ASCII code is used for information hiding. The prior bit of the LSB represents the edged image after gray level connectivity, and the remaining six bits represent the original image with very little difference in contrast. The given method embeds three images in one image and includes, as a special case of data embedding, information hiding, identifying and authenticating text embedded within the digital images [5].

Prof S. K. Bandyopadhyay, Debnath Bhattacharyya, Swarnendu Mukherjee, Debashis Ganguly, Poulami Das in 2008 has proposed a heuristic approach to hide huge amount of data using LSB steganography technique. The resultant stego-image was distortion less. Also, they have given much emphasis on space complexity of the data hiding technique [6].

G. Sahoo and R. K. Tiwari in 2008 proposed method works on more than one image using the concept of file hybridization. This particular method implements the cryptographic technique to embed two information files using steganography and due to this reason they have used a stego key for the embedding process [7]. In fact, the embedding of high-entropy data (often due to encryption) changes the histogram of colour frequencies in a predictable way. So, in order to obtain more security in our prescribed method, we have embedded an entire image behind another image of twice the size of target image for a remarkable change in the final image.

3. PROPOSED WORK

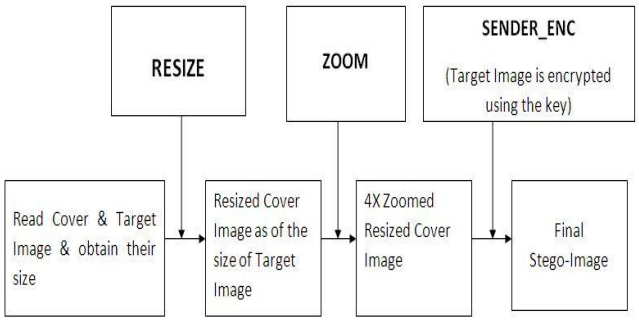
Algorithms are basically implemented over normal bitmap image file, but it should be clarified that the same scheme can be extended to operate over other file formats also. The image file, which is to be hidden, is here referred as Target Image and the image behind which it is to be hidden is termed as Cover Image. The selection of neither the Target Image nor the Cover Image is constrained by any size limit.

The Cover Image is zoomed twice of its original size using row-column duplication scheme ie, say a pixel (x,y) is duplicated in {(x', y'), (x'+1,y'), (x',y'+1), (x'+1,y'+1)}. In next attempt, the entire Target Image will be hidden in the Cover Image starting from the first byte position of the Cover Image.

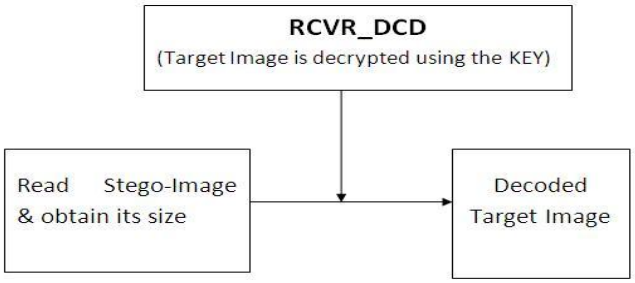
The method for encryption can be personalized, i.e., can be selected according to the user needs. But, the authors specifically suggests this specialized scheme, proposed in this paper, as because here the information are no longer being merged or masked with another and instead of that keeping the pixel values of the Target Image as an encrypted information in the carrier, i.e., the Cover Image is altered to obtain resultant image which is taken as Final Image. Thus no essence of the actual information is retrained in the Final Image, whereas in usual methods of the mostly done bitwise merging; the information belongs in encrypted way directly merged into final object obtained.

The stated Algorithm has got five distinct divisions: a. main function for each of the sender and receiver end which calls next sections; b. to resize the Cover Image in the size of the Target Image. c. to zoom the Cover Image in twice the size of the Target Image d. Encryption; e. Decryption.

SENDER END APPROACH



RECIEVER END APPROACH



3.1 Algorithms

3.1.1 SNDR_MAIN (Target Image, Cover Image)

This is the main function in our algorithm. This function will also be used in the sender side and will call other modules of our algorithm.

Input: This function will take Target Image and Cover Image as input.

Output: It will output the encoded stego-image.

3.1.2 RESIZE (PICTURE, SIZE)

This function is used in the algorithm to resize an image to obtain an image of the desired size from the input image.

Input: This function will take the image, which has to be resized along with the desired image size, which is to be obtained after resizing.

Output: This function outputs an image of desired size.

3.1.3 ZOOM (PICTURE, SIZE)

This function is used in the algorithm to zoom an image to obtain an image of the double size of the input image using row-column duplication technique.

Input: This function will take the image, which has to be zoomed along with the desired image size, which is to be obtained after zooming.

Output: This function outputs an image of desired size.

3.1.4 SNDR_ENC (PICTURE_1, PICTURE_2)

This function is used in the algorithm to encrypt an image with the help of another image to obtain an encrypted image.

Input: This function will take the cover image (PICTURE_1) [Resized and Zoomed 4x] in which another image will be hidden i.e. the target image (PICTURE_2).

Output: This function will output the stego-image as the final image.

3.1.5 RCVR_MAIN (STEGOIMAGE)

This is the main function in our algorithm. This function will be used in the receiver side and will call other modules of our algorithm.

Input: This function will take StegoImage as input.

Output: It will output the decoded Image.

3.1.6 RCVR_DCD (PICTURE_1)

This function is used in the algorithm to decrypt an image with the help of a key to obtain the final image.

Input: This function will take the StegoImage (PICTURE_1) in which another image is hidden.

Output: This function will output the TargetImage as the final image.

4. TEST RESULT

4.1 Complexity analysis of the stated algorithm

In case of space complexity at the sender end, for cover image dimension mXn, after the zooming operation, the size becomes 2mX2n. So, for storing this zoomed image, space required=2m*2n=4mn,which is O(mn).The target image is then encrypted and stored in this zoomed image, which does not alter the space complexity.

In the receiver end the decryption algorithm performs image scan in row wise order and generate the target image. Thus the time complexity order becomes O(mn).

In case of space complexity at the receiver end, if the received image size is mXn, then the FinalImage is (m/2Xn/2). So, for storing the FinalImage space required=(m/2)*(n/2)=mn/4,which is O(mn).

4.2 Test Results

Sender End:

Figure 1 :Cover Image (300x280)

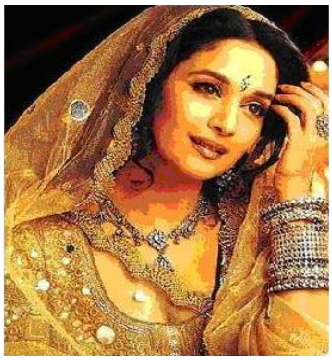


Figure 2: Targe Image(513x420)

Figure 3: Stego Image (1026x840)

Receiver end:

Figure 4: Final Image (513x420)

5. CONCLUSION

The main advantage of our algorithm is that the final image can be derived only from the StegoImage. The original cover image is not needed for decoding the stego image. This provides less network transmission overhead as well as less scope of suspicion for the network intruder. Moreover this algorithm is free from size constrains i.e. it performs well on any size of the cover image or target image. The fourth pixel value of every quadrant of the stego image is free and using LSB modification can use it for transmission of additional data or DCT based method or any other method.

6. REFERENCES

[1] Dobsicek, M., Extended steganographic system. In: 8th Intl. Student Conf. on Electrical Engineering, FEE CTU 2004, Poster 04.

[2] Yusuk Lim, Changsheng Xu and David Dagan Feng, “Web based Image Authentication Using Invisible Fragile Watermark”, 2001, Pan-Sydney Area Workshop on Visual Information Processing (VIP2001), Sydney, Australia, Page(s): 31 - 34

[3] Min Wu, Member, IEEE, and Bede Liu, Fellow, IEEE, “Data Hiding in Binary Image for Authentication and Annotation”, IEEE Trans. Image Processing, volume 6, Issue 4, Aug. 2004 Page(s): 528 - 538

[4] Nameer N. EL-Emam "Hiding a large amount of data with high security using steganography algorithm", Journal of Computer Science. April 2007, Page(s): 223 – 232

[5] Rehab H. Alwan, Fadhil J. Kadhim, and Ahmad T. Al-Taani, “Data Embedding Based on Better Use of Bits in Image Pixels”, International Journal of Signal Processing Vol 2, No. 2, 2005, Page(s): 104 - 107

[6] S.K.Bandyopadhyay, Debnath Bhattacharyya, Swarnendu Mukherjee, Debashis Ganguly, PoulumiDas, "A Secure Scheme for Image Transformation", August 2008, IEEE SNPD, Page(s): 490 – 493

[7] G. Sahoo, R. K. Tiwari, "Designing an Embedded Algorithm for Data Hiding using Steganographic.