Selective Region based Invisible Water Marking using Asymmetric Key Encryption

Somenath Nag Choudhury*

CSE Department, RCC Institute of Information TechnologyKolkata – 700015, West Bengal, India; Somenath.nc@gmail.com

Abstract

This introduces an approach, to deal with invisible water marking, by interactively selecting the appropriate threshold values each time to choose the desired area to embed the watermark, the informative image and encrypting the complete embedded image using a well-known asymmetric key cryptographic algorithm, RSA, with a static encryption table generated by choosing two large enough prime numbers, that satisfy the need required for this purpose.

Keywords: Decryption, Embedding, Encryption, Steganography, Threshold

1. Introduction

Image steganography, is one of the most interesting aspect and subject of concern while dealing with exchange of information (either in forms of data or image). It is always desired to have a method for appropriate embedding and extraction of that information's, taking into consideration the important factors commonly known as capacity, robustness and security[1,2]. Instead of making the decision of selecting the area by the program, it would be better if it is the user who could be able to choose the region by providing the threshold values, aware of the fact that host image is of type gray. It is then required to encrypt the information by using a suitable encryption algorithm to generate the cipher text. For that an inbuilt table containing the probable cipher text values generated from sufficiently large and carefully chosen key values will easily solve the problem. As the area being selected during the run time, it is also desired to embed the information of the selected region into the host image in order to accurate extraction of the embedded information. For the simplicity of the algorithm, embedding is done by modifying the Least Significant Bits (LSB) of the host image.

2. Literature Review

To match with the current pace of imaging technologies and devices that produces high definition images, image steganography nowadays can be correctly termed as digital image steganography[3].

**Author for correspondence*

Before one insert the desired information, he/she needs to take care of some important factors related to correct embedding. These are: 1) The maximum size of the file that could be inserted within a known fixed size cover file-capacity or capacity of the cover image and it depends on the number of secret bits can be stored per cover image pixel, 2) The sensitive data should be secure enough so that it becomes prone to any disturbance caused by outside attack - robustness and could be achieved by using any of the typical cryptographic algorithms with proper selection of key/s, 3) The embedding should be smooth enough so that it becomes difficult to make any difference in the Peak Signal to Noise Ratio (PSNR) values between the cover image and the generated stego image-imperceptibility[1,2].

The two important domains of image steganography are: 1) One that deals with the space or region of the data where it originally exist in the cover image and directly interacting with them without making any changes in their original position/location–spatial domain image steganography, it includes LSB (Least Significant Bit), PVD (Pixel Value Differencing), RPE (Random Pixel Embedding), EBE (Edge Based Data Embedding) and 2) One that deals with transformation of the cover image first by using any of the DFT (Discrete Fourier Transformation), DCT (Discrete Cosine Transformation), or DWT (Discrete Wavelet Transformation) and then interacting with the data in the space–transform domain or frequency domain image steganography[1,4,10].

3. Proposed Method

3.1 Cover Image and Water Image to Cipher Image

Step 1: Reading and resizing the RGB host image into 256 × 256.

Step 2: Converting the resized Host image to its equivalent Gray scale image.

Step 3: Reading the Water image and resize it by 32 × 32 (A factor of 256 × 256).

Step 4: Converting the Water image into black and white image.

Step 5: Taking the min and max threshold values for the pixels and a threshold value for the region.

Step 6: Search until the required/desired area being found with appropriate threshold values. If a failure occurs user may continue or stop the search process, as they wish.

Step 7: If the area is found, then keeping track of the North-West and South-East points of the area.

Step 8: Embedding the water image into cover image in the desired area by converting each data to its 8 bit equivalent binary.

Step 9: Embedding the locations as the last data.

Step 10: Encrypting the entire embedded image by using the alternative key values from the encryption table.

3.2 Cipher Image to Cover Image and Water Image

Step 1: Decrypting the cipher image to embedded image by using alternative key values from the decryption table.

Step 2: Process the last data to have the information of the location or region.

Step 3: Extracting the data and segregating into cover image and water image.

4. Experimental Results

4.1 Encryption Process

Figure 1. Cover image.

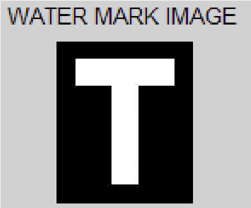


Figure 2. Watermark image.

Figure 3. Resize watermark image.

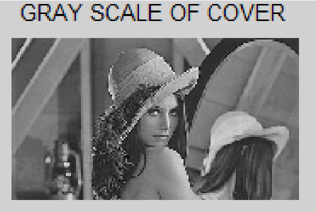


Figure 4. Gray of cover image.

Figure 5. Resized gray of cover

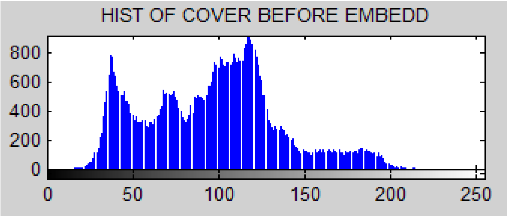


Figure 6. Histogram of cover image before embed.

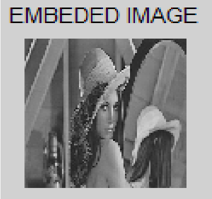


Figure 7. Embeded cover image.

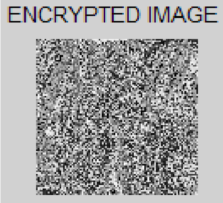


Figure 8. Encrypted cover image.

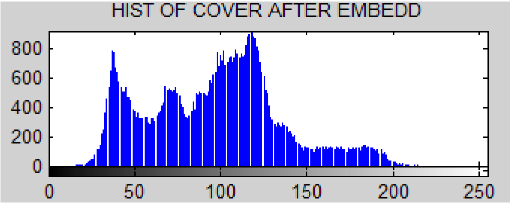


Figure 9. Histogram of cover image after embed.

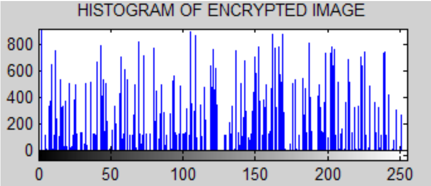


Figure 10. Histogram of encrypted image.

4.2 Decryption Process

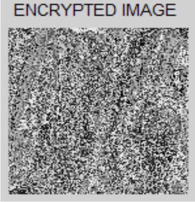


Figure 11. Encrypted image.

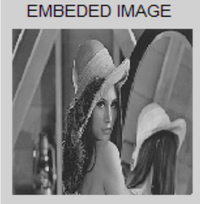


Figure 12. Embeded image.

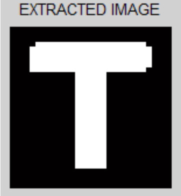


Figure 13. Extracted image.

5. Validation

The three basic needs of image steganography has been achieved successfully. The capacity need is achieved by proper resizing both the cover image and water image, such that the size of the water becomes a factor of the size of cover. Image is imperceptible enough to predict any embedding is done as being observed in the histogram analysis before and after the embedding. Also to make sure it becomes prone to any outside attack, a cryptographic algorithm has been used to make the data secure enough.

6. Performance Aspects

6.1 Capacity

Table 1. Capacity analysis of cover image

Cover size	Water size	Embedding Ratio	Result
256*256	32*32	1:1	Success
256*256	16*16	1:1	Success
256*256	32*16	1:1	Success
256*256	16*32	1:1	Success

6.2 Imperceptibility

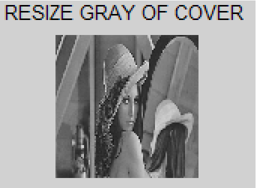


Figure 14. Before embed.

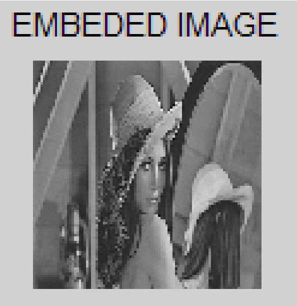


Figure 15. After embed.

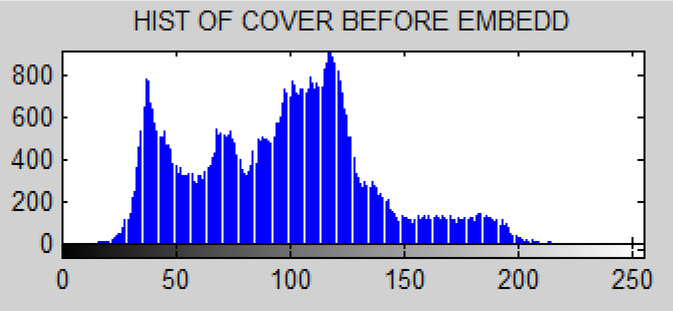


Figure 16. Histogram of cover image before embed.

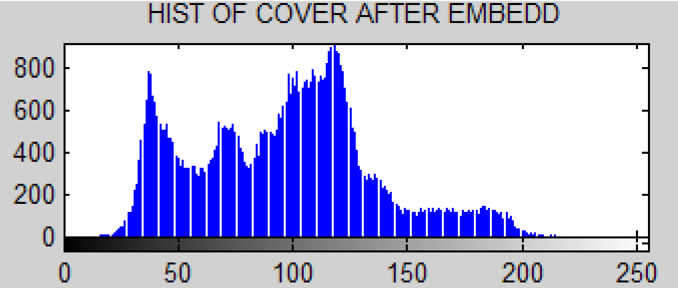
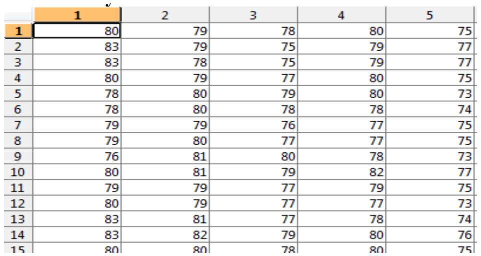


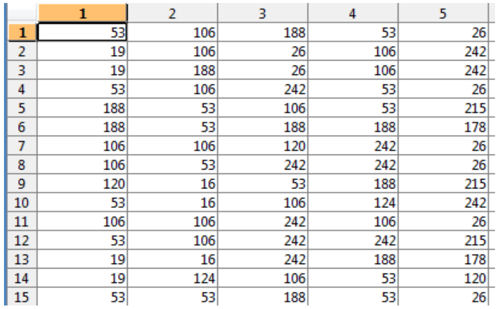
Figure 17. Histogram of cover image after embed.

6.3 Security



	1	2	3	4	5
1	80	79	78	80	75
2	83	79	75	79	77
3	83	78	75	79	77
4	80	79	77	80	75
5	78	80	79	80	73
6	78	80	78	78	74
7	79	79	76	77	75
8	79	80	77	77	75
9	76	81	80	78	73
10	80	81	79	82	77
11	79	79	77	79	75
12	80	79	77	77	73
13	83	81	77	78	74
14	83	82	79	80	76
15	80	80	78	80	75

Figure 18. Embeded image data before encryption.



	1	2	3	4	5
1	53	106	188	53	26
2	19	106	26	106	242
3	19	188	26	106	242
4	53	106	242	53	26
5	188	53	106	53	215
6	188	53	188	188	178
7	106	106	120	242	26
8	106	53	242	242	26
9	120	16	53	188	215
10	53	16	106	124	242
11	106	106	242	106	26
12	53	106	242	242	215
13	19	16	242	188	178
14	19	124	106	53	120
15	53	53	188	53	26

Figure 19. Embeded image data after encryption.

6.4 Thresholds

Table 2. Different applied threshold values

Min value	Max value	Area %	Result
80	120	80	Success
60	80	70	Success
90	130	50	Success
100	150	60	Success
120	160	40	Success

6.5 Run Time

Table 3. Total run time

Run no.	Time (sec)	Result
Run 1	30	Completed
Run 2	28	Completed
Run 3	31	Completed
Run 4	33	Completed
Run 5	29	Completed

6.6 Time Complexity

The running time of the proposed procedure is O (n*m) where ‘n’ and ‘m’ are the dimensions of the cover image.

6.7 Ease of Use

User will have the freedom to choose the threshold values and on successful searching of region user will have the information about the region and on failure it will ask for fresh values. Thus user satisfaction is achieved.

7. Conclusion

Secure data hiding is always been a challenging task in the field of image steganography. In this new approach a simple embedding technique has been introduced with LSB modification of the bits. Experimental results reveal that this algorithm correctly searches the region based on the threshold values provided by the user and properly performs the invisible water marking operation. It also guarantees the security and non-predictability of the data being inserted. The simplicity of the algorithm and ease of use can make its application in variety of different areas of image steganography.

8. Future Scope

Expectations and demands create their own challenges. To cope up with different applications, this approach could be a helping hand to try out with different types and size of images, embedding through modified techniques, make it protected from noises in the channel and use of filters to make it clean at the senders and receivers end respectively, dynamic creation of the encryption and decryption table with a better and proper exchange of key policy.

9. References

1. Khan I, Gupta S, Singh S. A new data hiding approach in images for secret data communication with steganography. International Journal of Computer Application (0975-8887). 2016 Feb; 135(13):9–14.
2. Devi M, Sharma N. Improved detection of least significant bit steganography algorithms in color and gray scale images. Proceedings of 2014 RAECS UIET; Punjab University Chandigarh. 2014 Mar. p. 6–8.
3. Goswami S, Goswami J, Mehra R. An efficient algorithm of steganography using JPEG colored image. IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE-2014); Jaipur. 2014 May 9-11. p. 1–5.
4. Alam S, Kumar V, Siddiqui WA, Ahmed M. Key dependent image steganography using edge detection. Fourth International Conference on Advance Computing and Communication Technologies. IEEE-ICACCT; Rohtak. 2014 Feb 8-9. p. 85–8.
5. Singla D, Juneja M. An analysis of edge based image steganography techniques in spatial domain. Proceedings of RAECS UIET; Punjab University Chandigarh. 2014 Mar 6-8. p. 1–5

6. Kamaldeep. Image steganography techniques in spatial domain, their parameters and analytical techniques: A review article. IJAIR. 2013; 2(5):85–92.
7. Hussain M, Hussain M. A survey of image steganography techniques. International Journal of Advanced Science and Technology. 2013; 54:113–23.
8. Hamid N, Yahya A, Ahmad RB, Nejim D, Kannon L. Steganography in image files: A survey. Australian Journal of Basic and Applied Sciences. 2013; 7(1):35–55.
9. Gangwar A, Srivastava V. Improved RGB-LSB steganography using secret key. International Journal of Computer Trends and Technology. 2013; 4(2):85–9.
10. Gutta RS, Chincholkar YD, Lahane PU. Steganography for two and three LSBs using extended substitution algorithm. ICTAT Journal on Communication Technology. 2013; 4(1):685–90.
11. Ashwin S, Ramesh J, Kumar SA, Gunavathi K. Novel and secure encoding and hiding techniques using image steganography: A survey. Emerging Trends in Electrical Engineering and Energy Management (ICETEEEM); Chennai. 2012 Dec 13-15. p. 171–7.