A Bit-Level Alteration Approach in Image Steganography

Niloy Roy
Email: niloy.roy@tu-ilmenau.de
Technische Universität Ilmenau

Introduction

Steganography deals with concealing data into digital RGB images.

The hiding techniques maintain the secrecy of the data while encryption ensures it’s integrity against intruders.

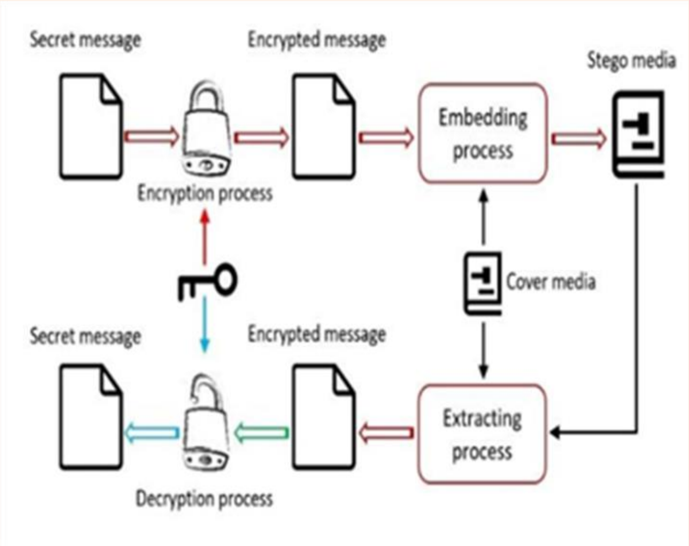


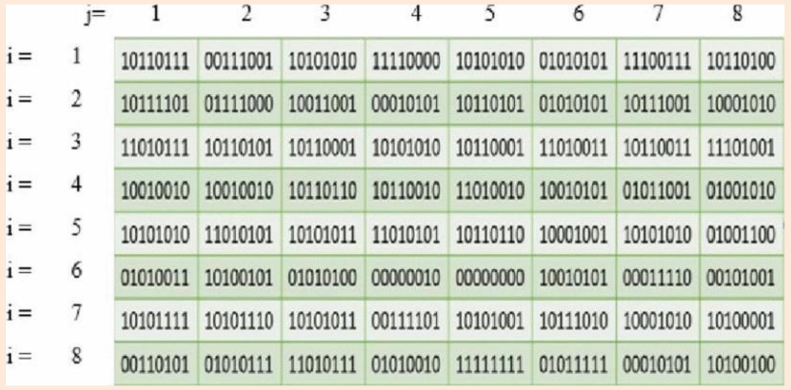
Figure 1: Basic combination diagram for steganography and cryptography from [1]

This work describes the development and assesment of one such steganography technique for providing increased confidentiality with less computational cost.

Hiding Technique

For encryption: AES-128 algorithm

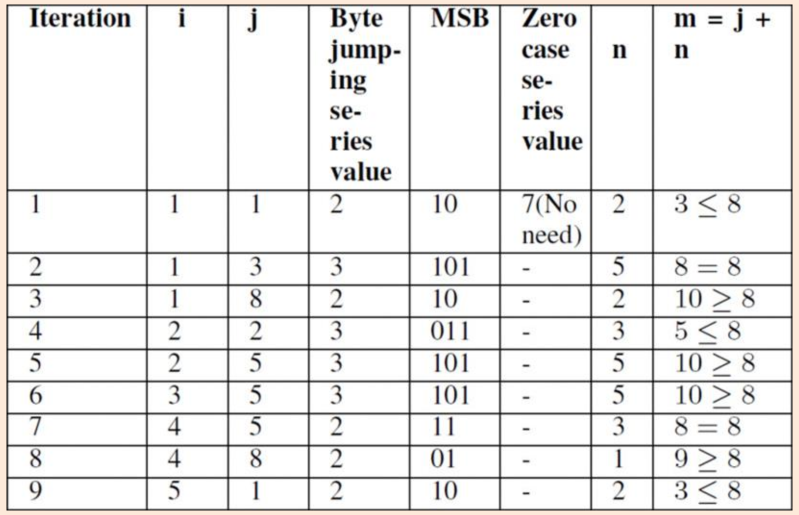
For hiding: A variant based on LSB technique



j=	1	2	3	4	5	6	7	8
i = 1	10110111	00111001	10101010	11110000	10101010	01010101	11100111	10110100
i = 2	10111101	01111000	10011001	00010101	10110101	01010101	10111001	10001010
i = 3	11010111	10110101	10110001	10101010	10110001	11010011	10110011	11101001
i = 4	10010010	10010010	10110110	10110010	11010010	10010101	01011001	01001010
i = 5	10101010	11010101	10101011	11010101	10110110	10001001	10101010	01001100
i = 6	01010011	10100101	01010100	00000010	00000000	10010101	00011110	00101001
i = 7	10101111	10101110	10101011	00111101	10101001	10111010	10001010	10100001
i = 8	00110101	01010111	11010111	01010010	11111111	01011111	00010101	10100100

Figure 2: Byte array of an 8 by 8 image [2]

Two sets of pseudo-random natural numbers and the most significant bits (MSB) of the pixel being traversed are used to find out the bits to be altered.



Iteration	i	j	Byte jumping series value	MSB	Zero case series value	n	m = j + n
1	1	1	2	10	7(No need)	2	$3 \leq 8$
2	1	3	3	101	-	5	$8 = 8$
3	1	8	2	10	-	2	$10 \geq 8$
4	2	2	3	011	-	3	$5 \leq 8$
5	2	5	3	101	-	5	$10 \geq 8$
6	3	5	3	101	-	5	$10 \geq 8$
7	4	5	2	11	-	3	$8 = 8$
8	4	8	2	01	-	1	$9 \geq 8$
9	5	1	2	10	-	2	$3 \leq 8$

Figure 3: Iteration to hide the cipher bit stream [2]

Byte jumping series: [2 3 2 3 3 3 2 2]
Zero case series: [7 3 5 4 2 6 1]

Results

The tool showed lower Mean Square Error and higher signal to noise ratio.

Tool Name	Output file type	Output file size	MSE value	PSNR value
ZSteg	.bmp/.tiff	473 KB	0.00042	81.911
OpenStego	.bmp	70.3 FB	0.01244	67.184
QuickStego	.bmp	147 KB	0.03177	63.111

Table 1: MSE and PSNR of different tools. OpenStego , QuickStego data from [3]

However, the payload capacity is only 1.6%.

- Beneficial in terms of detectability but expensive from a space complexity point of view.

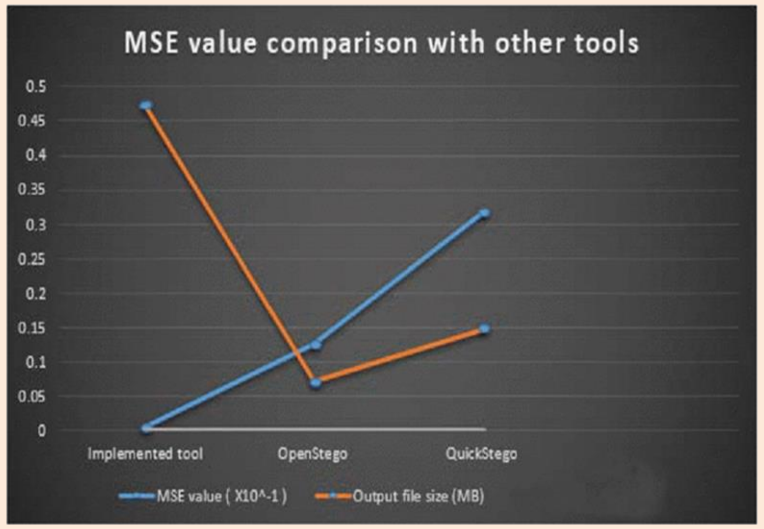


Figure 4: X axis for output file size and Y axis for MSE values . [2]

Conclusion and Future Work

Prime contribution: Minimizing detectability in RGB image steganography.

Future work:

1. To improve the payload capacity,
2. To make the tool compatible with image formats like JPEG, PNG etc.

References

[1]Sarjiyus, Omega & Baha, Benson & Garba, Etemi. (2021). Enhanced Security Framework for Internet Banking Services. Journal of Information Technology and Computing. 2. 9-29. 10.48185/jitc.v2i1.162.

[2] Z. Sultana, F. Jannat, S. S. Saumik, N. Roy, N. K. Datta and M. N.Islam,”A new approach to hide data in color image using LSB steganography technique, ” Proceedings of the 3rd International Conference on Electrical Information and Communication Technology (EICT), Khulna, pp.1–6, 2017.

[3] V, V. and Sebastian, S., “Comparative Study Of Steganography Tools.” in International Journal of Innovations & Advancement in Computer Science IJIACS, ISSN 2347 - 8616, Volume 2, Issue2, February 2015.