Steganography Technique to Prevent Data Loss by Using Boolean Functions

Satya Ranjan Dash, Alo Sen, Sk. Sarif Hassan, Rahul Roy, Chinmaya Misra and Kamakhya Narain Singh

Abstract Steganalysis technique embedded the secret message, so we have to conceal the very important data. Our main objective is undetectability, robustness and capacity of the hidden data. Existing image steganography techniques used various methods to hide data in a perfect manner. We used many Boolean functions to achieve a data (image)-hiding method or image steganography without loss of any information. Also, the data can be hidden and unhidden efficiently through the Boolean functions. Our experiments and corresponding outcome deliver that it is more secured than the existing approaches of steganography.

Keywords Image steganography · Boolean function · Data hiding
Human visual system · Pixel value differencing

S. R. Dash (✉) · A. Sen · C. Misra · K. N. Singh
School of Computer Application, Kalinga Institute of Industrial Technology, Deemed To Be University, Bhubaneswar, India
e-mail: sdashfca@kiit.ac.in

A. Sen
e-mail: alosen10@gmail.com

C. Misra
e-mail: cmisra@yahoo.com

K. N. Singh
e-mail: kamakhya.vbhcu@gmail.com

Sk. Sarif Hassan
Department of Mathematics, University of Petroleum and Energy Studies, Uttarakhand, India
e-mail: sarimif@gmail.com

R. Roy
Applied Electronics and Instrumentation, Asansol Engineering College, Asansol, India

S. S. Dash et al. (eds.), *Artificial Intelligence and Evolutionary Computations in Engineering Systems*, Advances in Intelligent Systems and Computing 668,
https://doi.org/10.1007/978-981-10-7868-2_26

1 Introduction

Steganography is known as "invisible" medium. It means to cover up communication reality in another medium. Image steganography is the most popular technique to hide image, video, etc. It has been developed spatial domain method through which image pixel can be vague with same bits. Image can say many things what human can see with human visual system (HVS). Steganography is not a new word; from ancient ages, people were sending the secret message or information in various formats which is coming under ancient steganography. Secret message is sent through various techniques like secret letter in each word or secret word in each sentence, sometime with the different sizes of grasses which indicate different meaning.

Nowadays we are using digital steganography, as modern era has Internet and digital signal processing due to which now become digital, and here, we are using different kinds of steganography techniques like image-based steganography. Embedded hidden message is also possible in video, audio file also. We also have different kinds of steganography algorithm to embed the message. We also are using DNA cryptography to hide and unhide the data [1].

Steganography is important due to its secret communication over the Internet. In image steganography, secret communication can be sent by embedding text message into cover image, thus generating stega-image [2]. We have different kinds of steganography techniques depending on the suitability described in Fig. 1.

Different steganography measures are

- Capacity—where maximum data we can embedded into the image.
- Perceptual transparency—where subsequent information hiding into cover page, perceptual quality will be converted into stego-image.
- Robustness—where after embedding, data should stay together into stego-image goes into some alteration such as cropping, filtering etc.
- Computation complexity—where cost is computationally evaluate for embedding and extracting a hidden message.

There are different steganography techniques, and all the techniques have their pros and cons. One of these techniques is masking and filtering. In this technique, we

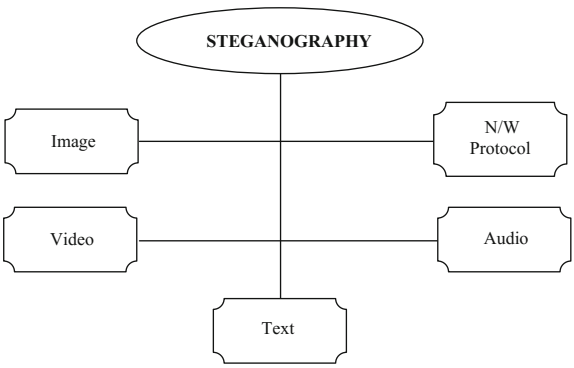


Fig. 1 Types of steganography

embedded information in added important areas than now hiding into the noise level, but the problem is that it can be applied into only grey scale images and limited to 24 bits. Steganography is employed in various useful applications.

The performance of steganography can be calculated from various factors, and the most important factor is the undetectability of data from an unseen communication. Further connected procedures are the steganographic capability, which is the most information that can carefully entrenched in a work lacking statistically assessable objects [3], and toughness, which refers to how well the steganographic classification resists the image out of hidden data.

2 Related Work

Steganography can be used any digital media comparing to watermarking, and encryption. In steganography, the keys are optional but in case of encryption it is necessary. At least two unless self-embedded files are required, but in case of encryption and steganography, the detection method is blind, but in case of watermarking, it is usually informative. The objective of steganography is to secret communication, but it protects the data in case of encryption. Steganography is very ancient except its digital version. The LSB-based image steganography embeds the undisclosed in the least significant bits of pixel values of the cover image (CVR). The idea of LSB embedding is easy. Also, pixel value differencing (PVD) is another technique to hide data and embedded the secret message. Transform domain technique [4] is more difficult but better than spatial domain method. It conceal information in areas of the picture that are fewer uncovered to density, cropping and processing along with many other techniques. It is also used to the stego objects [5–7] like images, audio, and video as well as file structures, and html pages. Most favourable pixel correction development is used to improve stego-image value obtained by effortless LSB replacement method. To make sure that the adaptive amount k of LSBs remains unaffected after pixel adaptation, the LSBs figure is computed by the high-order bits [8].

There are various steganography methods or techniques like in binary file techniques watermark can be embedded by making some changes in binary code, and in text technique, which is used in document to embed information inside a document we can simply alter some of its characteristics and updated thing can not visible to the human eye. We can also used wavelets to encode the whole image, sound techniques and video steganography techniques for the secret communication [9]. Al-Ataby and Al-Naima [10] had developed a customized image steganography procedure based on wavelet transform. The developed technique assures high level of security. It compresses the data with increase in the capacity or payload of the steganography process. However, this technique can produce high computational overhead. Al-Shatnawi [11] proposed an image steganography method which hides the undisclosed communication on probing about the similar kinds of bits among the secret message and the pixel value [12].

Table 1 Fifteen projection operators

	F0	F1	F2	F3	F4	F5	F6	F7	F8	F9	F10	F11	F12	F13	F14	F15
0,0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
0,1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
1,0	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
1,1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1

3 Proposed Work

We have aimed to create a secure data hiding technique through which we can have 100% recovery of data, meaning that we can hide the data without any loss of information and unhide the data successfully. There is always any i and j which will be treated as projection operators. We have created projection operators based on Boolean function. Table 1 illustrates the Boolean functions.

We have illustrated the data hiding algorithm as follows.

3.1 Proposed Algorithm

3.1.1 Data Hiding Method

Step 1: Read the image and calculate the size of the image.
Step 2: Get two pixels of region of interest (ROI) of square area, namely A and B by generating random pixel values. The size of A and B should be $n * n$ matrix.
Step 3: Convert the rgb image to binary image.
Step 4: For $i = 1$ to n
For $j = 1$ to n
Calculate C_i such that $C_i = A$ op B, where op is a projection operator.
Step 5: Check the values of C_i with the values of A and B, respectively, to find whether they are same or not.
Step 6: Finally, we will be getting an image with shuffled region of interest (ROI).

4 Experimental Results

We have used MATLAB for our experiment. We have taken an image in Fig. 2 having size 252 * 256. Then we have chosen two random ROI and get two cropped image Fig. 3 having size 100 * 100. Figures 4 and 6 define the corresponding

Fig. 2 Color image of 252 * 256 size

Fig. 3 First cropped image of size 100 * 100

Fig. 4 Binary image of first cropped image

binary images of Figs. 3 and 5 respectively. Thus, we are getting the pixel of region of interest (ROI) for square area, namely *A* (Fig. 4) and *B* (Fig. 6) matrices.

We have applied projection operator upon *A* and *B* which create *C* having size 100 * 100. The operation is as follows:

C [*i*] [*j*] = *A* [*i*] [*j*] F_0 to F_{15} *B* [*i*] [*j*] (Totally, 15 Boolean functions have been projected upon *A* and *B* and produced 15 different matrix). Then, each new matrix has been checked with *A* and *B* for equality, and finally, we are getting an image with shuffled region of interest (ROI).

The above experiment is based on only one sample report. We have done 500 times execution of same program to generate different matrices *A* and *B*, so that we can find out those projection operator for which most of the shuffled region of interest (ROI) will be similar to corresponding *A* and *B* matrices. Hence, data hiding

Fig. 5 Second cropped image of size 100 * 100

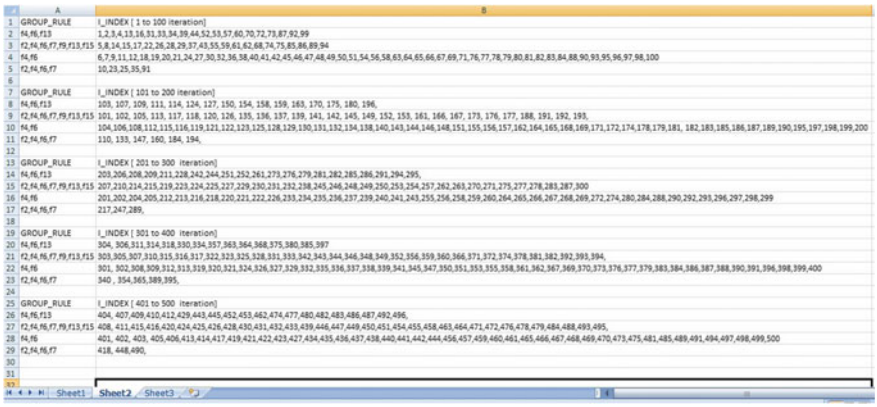
Fig. 6 Binary image of second cropped image

will be more efficient with 100% preservation of data by those 15 projection Boolean functions.

5 Analysis

- Figure 7 illustrates those Boolean functions which are common in most of the iterations among total 500 iterations.
- According to the priority from Fig. 7, the Boolean functions are as follows:
- F_4 and F_6: mostly found within 101–200 iterations, where the resultant shuffled ROI was matched with either *A* or *B* matrix.
- F_2,F_4,F_6,F_7,F_9,F_{13},F_{15}: mostly found within 301–500 iterations, where the resultant shuffled ROI was matched with either *A* or *B* matrix.
- F_2,F_4,F_6,F_7: mostly found within 101–200 iterations, where the resultant shuffled ROI was matched with either *A* or *B* matrix.
- F_0,F_1,F_3,F_5,F_8,F_{10},F_{11},F_{12},F_{14}: not found in any of the iterations.

So, the Boolean functions with the higher priority can be efficiently used for 100% data recovery while unhiding the image without no information loss.



	A	B
1	GROUP_RULE	I_INDEX [1 to 100 iteration]
2	f4,f6,f13	1,2,3,4,13,16,31,33,34,39,44,52,53,57,60,70,72,73,87,92,99
3	f2,f4,f6,f7,f9,f13,f15	5,8,14,15,17,22,26,28,29,37,43,55,59,61,62,68,74,75,85,86,89,94
4	f4,f6	6,7,9,11,12,18,19,20,21,24,27,30,32,36,38,40,41,42,45,46,47,48,49,50,51,54,56,58,63,64,65,66,67,69,71,76,77,78,79,80,81,82,83,84,88,90,93,95,96,97,98,100
5	f2,f4,f6,f7	10,23,25,35,91
6		
7	GROUP_RULE	I_INDEX [101 to 200 iteration]
8	f4,f6,f13	103, 107, 109, 111, 114, 124, 127, 150, 154, 158, 159, 163, 170, 175, 180, 196,
9	f2,f4,f6,f7,f9,f13,f15	101, 102, 105, 113, 117, 118, 120, 126, 135, 136, 137, 139, 141, 142, 145, 149, 152, 153, 161, 166, 167, 173, 176, 177, 188, 191, 192, 193,
10	f4,f6	104,106,108,112,115,116,119,121,122,123,125,128,129,130,131,132,134,138,140,143,144,146,148,151,155,156,157,162,164,165,168,169,171,172,174,178,179,181, 182,183,185,186,187,189,190,195,197,198,199,200
11	f2,f4,f6,f7	110, 133, 147, 160, 184, 194,
12		
13	GROUP_RULE	I_INDEX [201 to 300 iteration]
14	f4,f6,f13	203,206,208,209,211,228,242,244,251,252,261,273,276,279,281,282,285,286,291,294,295,
15	f2,f4,f6,f7,f9,f13,f15	207,210,214,215,219,223,224,225,227,229,230,231,232,238,245,246,248,249,250,253,254,257,262,263,270,271,275,277,278,283,287,300
16	f4,f6	201,202,204,205,212,213,216,218,220,221,222,226,233,234,235,236,237,239,240,241,243,255,258,258,259,260,264,265,266,267,268,269,272,274,280,284,288,290,292,293,296,297,298,299
17	f2,f4,f6,f7	217,247,289,
18		
19	GROUP_RULE	I_INDEX [301 to 400 iteration]
20	f4,f6,f13	304, 306,311,314,318,330,334,357,363,364,368,375,380,385,397
21	f2,f4,f6,f7,f9,f13,f15	303,305,307,310,315,316,317,322,323,325,328,331,333,342,343,344,346,348,349,352,356,359,360,366,371,372,374,378,381,382,392,393,394,
22	f4,f6	301, 302,308,309,312,313,319,320,321,324,326,327,329,332,335,336,337,338,339,341,345,347,350,351,353,355,358,361,362,367,369,370,373,376,377,379,383,384,386,387,388,390,391,396,398,399,400
23	f2,f4,f6,f7	340 , 354,365,389,395,
24		
25	GROUP_RULE	I_INDEX [401 to 500 iteration]
26	f4,f6,f13	404, 407,409,410,412,429,443,445,452,453,462,474,477,480,482,483,486,487,492,496,
27	f2,f4,f6,f7,f9,f13,f15	408, 411,415,416,420,424,425,426,428,430,431,432,433,439,446,447,449,450,451,454,455,458,463,464,471,472,476,478,479,484,488,493,495,
28	f4,f6	401, 402, 403, 405,406,413,414,417,419,421,422,423,427,434,435,436,437,438,440,441,442,444,456,457,459,460,461,465,466,467,468,469,470,473,475,481,485,489,491,494,497,498,499,500
29	f2,f4,f6,f7	418, 448,490,
30		
31		
32		

Sheet1 Sheet2 Sheet3

Fig. 7 Boolean functions of iterations

6 Conclusion

In this paper, a novel steganography technique was offered, implemented and analysed by using 15 Boolean functions. We have successfully hidden the image by using these functions. We have taken randomly two ROIs of same $n * n$ matrix from the whole image. Our data hiding method has used 15 boolean functions to accomplish 100% recovery of data, it means we can embedded maximum data into the image and unhide it successfully without loss of any information. We had not illustrated the unhiding methodology, but in the invert process, we can unhide the data efficiently. According to analysis, some Boolean functions got no priority over others. We will try to focus on those operators for better distribution.

References

1. A. Aieh, et al., Deoxyribonucleic acid (DNA) for a shared secret key cryptosystem with Diffie hellman key sharing technique. in *Computer, Communication, Control and Information Technology (C3IT), 2015 Third International Conference on*. IEEE, 2015
2. M. Hussain, M. Hussain, A Survey of Image Steganography Techniques. Inter. J. Adv. Sci. Tech. **54**, 113–124 (2013)
3. I. Cox et al., *Digital watermarking and steganography* (Morgan Kaufmann, Burlington, 2007)
4. S. Katzenbeisser, F. Petitcolas, *Information Hiding Techniques for Steganography and Digital Watermarking* (Artech house, Norwood, 2000)
5. H.S.M. Reddy, K.B. Raja, High capacity and security steganography using discrete wavelet transform. Int. J. Comput. Sci. Secur. (IJCSS) **3**(6), 462 (2009)
6. S. Katzenbeisser, F. Petitcolas, *Information Hiding Techniques for Steganography and Digital Watermarking* (Artech house, Norwood, 2000)
7. P. Kruus et al., A survey of steganography techniques for image files. Adv. Secur. Res. J. **5** (1), 41–52 (2003).

8. H. Yang, X. Sun, G. Sun, A high-capacity image data hiding scheme using adaptive LSB substitution. Radioengineering **18**(4), 509–516 (2009)
9. S. Channalli, J. Ajay, Steganography an Art of Hiding Data. *arXiv preprint* arXiv:0912.2319 (2009)
10. A. Al-Ataby, F. Al-Naima, A modified high capacity image steganography technique based on wavelet transform. Int. Arab J. Inf. Technol. **7**(4), 6 (2008)
11. A.M. Al-Shatnawi, A new method in image steganography with improved image quality. Appl. Math. Sci. **6**(79), 3907–3915 (2012)
12. K.B. Raja, et al., A secure image steganography using LSB, DCT and compression techniques on raw images. in *Intelligent Sensing and Information Processing, 2005. ICISIP 2005. Third International Conference on*. IEEE, 2005