Volume 6, Issue 9, September 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

XOR Technique for Digital Image Steganalysis

Balkar Singh
Ph.D Scholar, CSE Department, Thapar University,
Patiala, Punjab, India

Abstract— In the recent years a number of method was developed to secure the digital media during its transmission through a unreliable channel .Today is a modern life everyone want to use internet technology to transmit his / her data. But internet is not considering a reliable channel. Anyone can hack our data during its transmission. We need to secure our data during transmission time if anyone hack our data then he/she is not able to read or modify our data. So we try to send our data in a secure manner by using different type of technique. At the sender site technique like steganography can be used to hide our data in the digital medium and at the receiver side steganalysis technique is used to abstract the hidden data. Our proposed technique help a steganalysis to check cover medium have a data or not.

Keywords— Steganography, Steganalysis, MSE, PSNR, Digital Data.

I. INTRODUCTION

In this paper we presented a steganalysis technique which is developed using statistical properties of digital image. During the hidden process statistical properties like entropy, Peak Signal to Noise Ratio (PSNR) Mean Square Error (MSE) changed when data is hidden in the cover image. The cover image has data or not can be detected by using these properties.

Types of technique used to secure digital data:-

1.1 Steganography
1.2 Cryptography
1.3 Watermarking

Steganography: - This technique is used to hide the secret data in the cover image. The word steganography is derived from Greek words which mean Covered Writing. The main purpose of steganography is to hide the secret message by embedding it into carrier medium.

Cryptography: - This technique is used to secure the digital data during its transmission through unreliable channel. In this technique actually value is changed into another form. So that if any one hack our data than he / she is not able to find what is the actually value of the data.

Watermarking:- This technique is used for ownership and to protect our digital image from tampering. Like organization uses their logo for their ownership so that no one can blame for their data.

II. STEGANALYSIS AND ITS TYPE

Steganalysis: It is the process to decide if an image or other medium contains the hidden message. It is a way of distinguishing between a cover-object and stego-object. A steganalyst may be passive or active.

2.1 A steganalyst is known as passive if his/her aim to detect the presence of a message. He/she may try to find out the embedding method used to hide the messages in the code medium.

2.2 An active steganalyst tries to estimate the hidden message by him/her.

III. STEGANALYSIS TECHNIQUE

Steganalysis Techniques: - There are two types of steganalysis as given below:

Universal Steganalysis Technique: - It attempts to detect the presence of embedded message independent of the embedded algorithm. This is also known as Blind Steganalysis Technique.

Embedded Algorithm Based Steganalysis Technique: - This approach takes the advantage of particular algorithmic detail of the embedding algorithm.

IV. STATISTICAL AND QUALITY PARAMETERS

In this section, we have discussed the image measure parameters which are used in the development steganalysis techniques.

Mean Square Error (*MSE*): It measures the average of the square of the error. The error is the amount by which value implied by the estimator differ from the quantity to be estimated. The difference occurs because of randomness or because the estimator does not account for information that could produce a more accurate estimate. It is the second moment (about the origin) of the error.

MSE for two images *A* and *B*, each of size $x \times y$, is defined as:

$$MSE = \sum_{m=1}^{x} \sum_{n=1}^{y} \frac{(A_{mn} - B_{mn})^2}{x \times y}$$

where A_{mn} is the pixel of reconstructed image *A* and B_{mn} is the pixel of original image *B*, x and y are the height and width of the images, respectively.

Peak Signal–to-Noise Ratio (*PSNR*): It is used in the comparison between an original image and a coded/decoded image. It is measured in decibels (*dB*).The syntax for *PSNR* is given by

$$PSNR = 10 \log_{10} \frac{(2^B - 1)^2}{MSE}$$

where *B* is the bit depth of the image and *MSE* is the mean square error.

V. PROPOSED TECHNIQUE AND RESULTS

XOR: It is a logical operation that implements an exclusive or, that is, a true output (1) results if one, and only one, of the inputs to the gate is true (1). If both inputs are false (0) and both are true (1), a false output (0) results. Its behavior is summarized in the truth table as given below:

Table: Truth table of XOR.

INPUT		OUTPUT
A	B	A XOR B
0	0	0
0	1	1
1	0	1
1	1	0

***XOR* Based Steganalysis Approach:**

a) Read the cover image.
b) Read the suspicious image.
c) Convert the both image into bit stream
d) Find the sum of *XOR* between cover image and suspicious image's *LSB.*
e) If sum is greater than 0 then image is stego.
f) Else image is cover.

Table 1:-

Image name	***PSNR* (in *dB*)**	**XOR**	
		Flag	**Time(sec)**
IMG 1	61.50	1	0.8438
IMG 2	60.84	1	0.7813
IMG 3	61.58	1	0.7813
IMG 4	61.08	1	0.8125
IMG 5	52.80	1	0.9688
IMG 6	61.10	1	0.8125
IMG 7	62.46	1	0.8750
IMG 8	60.95	1	0.8750
IMG 9	60.92	1	0.8750
IMG 10	60.54	1	0.8750
IMG 11	60.63	1	0.9063
IMG 12	60.77	1	0.8594
IMG 13	60.55	1	1.2969
IMG 14	60.58	1	0.8750
IMG 15	60.35	1	0.9375
IMG 16	60.91	1	0.9063
IMG 17	61.77	1	0.7969
IMG 18	63.63	1	0.9375
IMG 19	63.19	1	0.9531
IMG 20	62.61	1	1.2500
IMG 21	47.66	1	0.8594

IMG 22	63.48	1	1.1094
IMG 23	53.34	1	1.0781
IMG 24	52.95	1	0.9219
IMG 25	55.39	1	1.3125
IMG 26	53.26	1	0.9688
IMG 27	55.39	1	0.9219
IMG 28	56.27	1	0.9063
IMG 29	64.26	1	0.7969
IMG 30	55.49	1	0.9219
IMG 31	54.56	1	1.4688
IMG 32	55.85	1	1.1563
IMG 33	59.37	1	0.8906
IMG 34	46.32	1	0.9219
IMG 35	46.82	1	1.0000
IMG 36	47.33	1	0.9844
IMG 37	47.89	1	0.9063
IMG 38	54.55	1	1.3906
IMG 39	55.34	1	1.4844
IMG 40	55.42	1	1.2969
IMG 41	51.28	1	1.1719
IMG 42	48.22	1	0.8594
IMG 43	47.63	1	1.0000
IMG 44	50.52	0	1.4531
IMG 45	51.27	0	1.4688
IMG 46	55.26	1	0.8906
IMG 47	51.92	1	1.1875
IMG 48	51.92	1	0.7813
IMG 49	48.66	1	0.9063
IMG 50	47.79	1	1.0938
IMG 51	47.79	1	1.4844
IMG52	46.00	1	1.2969
IMG 53	61.58	1	1.0781
IMG 54	60.87	1	0.9531
IMG 55	60.87	1	1.2031
IMG 56	60.82	1	1.2656
IMG57	61.02	1	1.2031
IMG 58	60.88	1	1.4688
IMG 59	60.95	1	1.4844
IMG 60	60.92	1	1.1094
IMG 61	60.79	1	0.8281
IMG 62	60.88	1	0.8906
IMG 63	60.71	1	1.1563
IMG 64	60.97	1	0.9063
IMG 65	61.69	1	0.7813
IMG 66	63.14	1	0.9688
IMG 67	60.79	1	0.7656
IMG 68	61.71	1	0.7813
IMG 69	61.80	1	0.7656
IMG 70	60.73	1	1.0000
IMG 71	60.54	1	0.8594
IMG 72	61.66	1	0.8125
IMG 73	61.67	0	1.3281
IMG 74	61.75	1	0.9219

IMG 75	61.98	1	1.0625
IMG 76	61.98	1	1.1094
IMG 77	61.09	1	1.0938
IMG 78	61.90	1	1.1094
IMG 79	48.94	0	1.0938
IMG 80	47.06	1	0.9844
IMG 81	48.93	1	1.0156
IMG 82	47.83	1	1.0625
IMG 83	48.87	1	1.0469
IMG 84	49.10	0	1.3906
IMG 85	50.61	1	1.4844
IMG 86	49.82	1	0.9688
IMG 87	49.17	1	0.9844
IMG 88	49.34	1	1.0156
IMG 89	49.26	0	1.0000
IMG 90	49.12	1	1.3594
IMG 91	49.26	0	1.3125
IMG 92	59.37	1	1.0313
IMG 93	56.52	1	0.7969
IMG 94	55.82	1	0.8906
IMG 95	54.77	1	0.8906
IMG 96	56.86	1	0.9844
IMG 97	55.34	1	0.9844
IMG 98	55.49	1	0.9844
IMG 99	54.00	1	0.8750
IMG 100	55.37	1	0.7813

Table 1 shows the result after applying the technique on hundred images. Time execution as well as PSNR is given in the table. Flag value is used to calculate the how much our technique successful works or not.

VI. CONCLUSIONS

The results show that it is a very good technique for image steganalysis. Proposed technique takes very less time in execution. The result is more than 90 % of the proposed technique and almost it tells that the cover image have a secret data or not.

REFERENCES

[1] G. J. Simmons, “The Prisoners’ Problem and The Subliminal Channel,” In Proceedings of Advances in Cryptology, pp. 51-67, 1983.

[2] E.T. Lin and E. T. Delp, “A Review of Data Hiding in Digital Images,” In Proceedings of the Image Processing, Image Quality, Image Capture Systems Conference, pp. 274-278, 1999.

[3] A. Westfeld and A. Pfitzmann, "Attacks on Steganographic Systems," In Proceedings of Lecture Notes in Computer Science, Vol. 1768, pp. 61−75., 2000

[4] N. Provos, “Defending Against Statistical Steganalysis,” In Proceedings of 10th USENIX Security Synposium, 2001.

[5] I. Avcibas, N. Menon, and B. Sankur, “Image Steganalysis with Binary Similarity Measures,” In Proceedings of ICIP, 2002.

[6] S. Lyu, and H. Farid, “Detecting Hidden Messages Using Higher Order Statistics and Support Vector Machines,” In Proceedins of Lecture Notes in Computer Science: 5th International Workshop on Information Hiding, Vol. 2578, 2002.

[7] I. Avcibas, N. Menon, and B. Sankur, “Steganalysis Using Image Quality Metrics”, In Proceedings of IEEE Transactions on Image Processing, Vol. 12, No. 2, pp. 221-229, 2003.

[8] M. U. Celik, G. Sharma and A. Tekalp, “ Universal Image Steganalysis Using Rate Distortion Curves,” In Proceedings of IST/SPIE’s 16th Annual Symposium on Electronics Imaging Science and Technology, 2004.

[9] M. Kharrazi, H. T. Sencar, and N. Menon, "Benchmarking Steganographic and Steganalysis Techniques," In Proceedings of IST/SPIE's 17th Annual Symposium on Electronic Imaging Science and Technology, 2005.

[10] A. G. H. Chamorro, A. E. Trujillo, J. L. Hernandez, M. N. Miyatake, H. P. Meana, "A Methodology of Steganaysis for Images," In Proceedings of International Conference on Electrical, Communications, and Computers", pp. 102-106, 2009.

[11] A. S. Hashemi, M. M. Ghazi, S. Ghaemmaghami, H. S. Zadeh, "Universal Steganalysis Based on Local Prediction Error in Wavelet Domain," In Proceedings of Seventh International Conference on Intelligent Information Hiding and Multimedia Signal Processing, pp. 165-168, 2011.

[12] S. Verma, S. Sood and S.K. Ranade, "Relevance of Steganalysis Using DIH on LSB Steganography," International Journal Advanced Research in Computer Science and Software Engineering, Vol. 4, No. 2, pp. 835-838, 2014.

