ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 8, August 2016

Variance Method for Digital Image Steganalysis

Balkar Singh

Ph.D Scholar, Dept. of CSE, Thapar University, Patiala, Punjab, India

ABSTRACT: In this paper we presented steganalysis techniques which are developed using statistical properties of an image. When secret data is hidden in an image, the statistical properties like variance, correlation, entropy, (Peak Signal to Noise Ratio) *PSNR*, and (Mean Square Error) *MSE* are changed due to the hidden secret data. We have used these quantitative measures to detect whether any secret data is present in the image or not. Using a statistical approach, we investigated the inherent detectability of several commonly used steganography techniques to check the performance of proposed steganalysis approaches.

KEYWORDS: Variance, PSNR, Steganography, Steganalysis

I. INTRODUCTION

In modern life, everything depends on technical i.e for data transmission internet is used. Data is transferred through unreliable channel. So we need to apply algorithm to secure our data. If anyone hack our data then he/she is not able to edit or miss use our data. There are number of techniques can be used to secure our data during its transmission through unreliable channel.
Steganography.
Watermarking.
Cryptography.
Steganography:- It is the technique to hide secret message within the cover message like audio, video and text files. The word steganogrpahy is derived from the greek word which mean covered image.
Watermarking:- This technique is used for ownership and copy right protection. For example, it used in dollar and Indian rupees as well as company use for their logo.
Cryptography:- This technique is also used for security purpose during digital data transmission through unreliable channel. In this technique data is encrypted by using different algorithm i.e. ABCD is encrypted ZYXW. So only the sender knows what is method is used to encrypt data. If anyone hack this data it is so difficult to decrypt the data in the real form.

II. LITERATURE SURVEY

Westfeld *et al.* [7] introduced a powerful statistical attack that can be applied to any steganography technique in which a set of Pairs of Values (*PoVs*) are used to detect the presence of secret message. Authors exploited the fact that any steganographic techniques change the frequency of pair of value during message embedding process. This method was effective in detecting Stego-images generated from variety of steganography algorithms. Westfeld [8] analyzed that many steganographic systems are weak against visual and statistical attacks. Systems without these weaknesses offer only a relatively small capacity for steganographic messages. The newly developed algorithm *F5* withstands visual and statistical attacks, yet it still offers a large steganographic capacity. *F5* implements matrix encoding to improve the efficiency of embedding. Thus it reduces the number of necessary changes. *F5* employs permutative straddling to uniformly spread out the changes over the whole steganogram. Avcibas *et al.* [12] proposed *LSB* detection scheme by using binary similarity between the 7^{th} bit plane and 8^{th} bit plane. It is assumed that there is a natural correlation between the bit planes that is disrupted by the *LSB* hiding. This scheme does not auto-calibrate on a per image basis and instead calibrate on a training set of cover and stego images. The scheme works better than a generic steganalysis scheme, but not as well state of the art *LSB* steganalysis. Farid [14] analyzed that techniques for information hiding have become increasingly more sophisticated and widespread. With high-resolution digital images as carriers, detecting

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 8, August 2016

hidden messages has become considerably more difficult. This paper describes a new approach to detecting hidden messages in images. The approach uses a wavelet-like decomposition to build high-order statistical models of natural images. A Fisher linear discriminate analysis is then used to discriminate between untouched and adulterated images.

III. STEGANALYSIS AND ITS TYPES

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.

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

2.1 Criteria for Steganalysis: The main goal of a steganalysis is to identify whether or not a suspected medium is embedded with secret data, in others words, to determine the testing medium belongs to the cover or stego class. If a certain steganalytic method is used to steganalyze a suspicious medium, there are four possible resultant situations.

- True positive (*TP*): A stego image medium is correctly classified as stego.
- False negative (*FN*): A stego image medium is wrongly classified as cover.
- True negative (*TN*): A cover medium is correctly classified as cover.
- False positive (*FP*): A cover medium is wrongly classified as stego.

2.2 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

Statistical and Quality Parameters: In this section, we have discussed the image measure parameters which are used in the development steganalysis techniques.

3.1 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.

3.2 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.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 8, August 2016

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.

V. PROPOSED TECHNIQUE

Variance: It is a measure of how far a set of numbers is spread out. If a random variable *X* has the expected value (mean) $\mu = E[X]$, then the variance of *X* is given by equation

$$\text{Variance}(X) = E[(X-\mu)^2]$$

That is, the variance is the expected value of the squared difference between the variable's realization and the variable's mean.

Variance Based Steganalysis Approach:

a) Read the cover image.
b) Read the suspicious image.
c) Find the variance between both images row wise.
d) Find the variance between both images column wise.
e) Find the difference of the variance between both images.
f) Draw a histogram between variance of both images.
g) Count the number of rows and number of columns in which histogram is not override.
h) Find the percentage of the pixel that has been changed with the total number of pixels.
If percentage is greater than 1, then image is stego
Else image is cover.

VI. RESULTS

We applied the proposed technique on one hundred image i.e. image name from c1 to c100. The table no. 1 shows the time execution taken by the technique to complete the process. PSNR of every image is also calculated and given in the table 1.

Table 1:-Approach applied on Hundred images

Image Name	PSNR(dB)	Variance	
		Flag	Time
C1	61.50	1	0.1406
C2	60.84	1	0.1406
C3	61.58	1	0.1563
C4	61.08	1	0.1563
C5	52.80	0	0.1406
C6	61.10	0	0.1875
C7	62.46	1	0.1406
C8	60.95	1	0.1406
C9	60.92	0	0.1406
C10	60.54	1	0.1719
C11	60.63	1	0.1094
C12	60.77	1	0.1406
C13	60.55	0	0.1250

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 8, August 2016

C14	60.58	1	0.1406
C15	60.35	1	0.1406
C16	60.91	0	0.1250
C17	61.77	0	0.1250
C18	63.63	0	0.1563
C19	63.19	0	0.1563
C20	62.61	0	0.1563
C21	47.66	0	0.1563
C22	63.48	0	0.1563
C23	53.34	0	0.1563
C24	52.95	0	0.1250
C25	55.39	0	0.1406
C26	53.26	0	0.1406
C27	55.39	0	0.1875
C28	56.27	0	0.1406
C29	64.26	0	0.1406
C30	55.49	0	0.1406
C31	54.56	0	0.1719
C32	55.85	0	0.1250
C33	59.37	0	0.1563
C34	46.32	1	0.1406
C35	46.82	0	0.1250
C36	47.33	0	0.1406
C37	47.89	1	0.1406
C38	54.55	0	0.1406
C39	55.34	0	0.1250
C40	55.42	0	0.1563
C41	51.28	0	0.1563
C42	48.22	0	0.1406
C43	47.63	0	0.1406
C44	50.52	0	0.1563
C45	51.27	1	0.1719
C46	55.26	0	0.1406
C47	51.92	0	0.1563
C48	51.92	0	0.1406
C49	48.66	1	0.1406
C50	47.79	0	0.1563
C51	47.79	0	0.1563
C52	46.00	0	0.1563
C53	61.58	0	0.1875
C54	60.87	0	0.1406
C55	60.87	0	0.1406
C56	60.82	0	0.1719
C57	61.02	0	0.1563
C58	60.88	0	0.1250
C59	60.95	0	0.1406
C60	60.92	0	0.1406
C61	60.79	1	0.1719
C62	60.88	0	0.1563
C63	60.71	0	0.1563
C64	60.97	0	0.1563

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 8, August 2016

C65	61.69	0	0.1719
C66	63.14	0	0.1406
C67	60.79	0	0.1563
C68	61.71	0	0.1406
C69	61.80	0	0.1563
C70	60.73	0	0.1406
C71	60.54	1	0.1563
C72	61.66	0	0.1719
C73	61.67	0	0.1406
C74	61.75	0	0.1563
C75	61.98	0	0.15563
C76	61.98	0	0.1406
C77	61.09	0	0.1406
C78	61.90	0	0.1563
C79	48.94	1	0.1563
C80	47.06	0	0.1250
C81	48.93	0	0.1406
C82	47.83	0	0.1406
C83	48.87	0	0.1563
C84	49.10	0	0.1406
C85	50.61	0	0.1406
C86	49.82	0	0.1406
C87	49.17	0	0.1904
C88	49.34	0	0.1875
C89	49.26	0	0.1563
C90	49.12	0	0.1719
C91	49.26	0	0.1406
C92	59.37	0	0.1563
C93	56.52	0	0.1250
C94	55.82	0	0.1563
C95	54.77	0	0.1719
C96	56.86	0	0.1406
C97	55.34	0	0.1563
C98	55.49	0	0.1250
C99	54.00	0	0.1563
C100	55.37	0	0.1406

Table 1 shows the hundred images and their PSNR with corresponding Stego. Flag 0 shows the image has no data in the image and flag 1 show there is some hidden data in the image.

VII. CONCLUSION

The primary focus of this paper is to develop the steganalysis technique techniques using statistical properties of an image. Using a statistical approach, we investigated the inherent detectability of several commonly used data hiding techniques.

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.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 8, August 2016

[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.