ISSN XXXX XXXX © 2018 IJESC

Research Article Volume 8 Issue No.5

Digital Image Steganalysis by Statistical Approach

Tanu Kumari[1], Kuldeep Singh[2]
M.Tech Student[1], Assistant Professor[2]
Department of Computer Science and Engineering
Delhi College of Technology and Management, India

Abstract:
In this modern era, the communication over the network increases day by day. So, the security of data is the main issue now a days. For this security purpose we use steganalysis for securing our data from the attackers. In this paper, we present digital image steganalysis by using statistical approach. The statistical properties of digital image like correlation, variance, entropy, MSE (Mean Square Error), PSNR (Peak Signal to Noise Ratio) are changed because of the secret information hidden in the digital image. To detect whether there is any secret information is present or not, we have used these statistical measures. By using the statistical approach, to check the performance of the proposed methods of steganography, we enquired into the intrinsic detectability of various generally used steganography technique.

Keywords: Statistical Approaches, Image, steganalysis.

I. INTRODUCTION

The technique of hiding secret data within a cover object is called as steganography. These cover object can be audio, video, images and text files. In this technique the multimedia carrier i.e. images, audio, video and text files are used for securing the data. Steganography is the Greek word. The meaning of this word is covered writing. By using this technique the information is hiding by embedding into the multimedia object. It has been widely used for hiding the data from the criminals. In this technique the sender hides the secret information by embed it into the cover object by applying steganographic algorithm. In the network security cryptography is also used to hiding the data from the attackers but it is totally different from the steganography but the main purpose of both is that no one can decipher the hidden data. The dissemination of the tools of steganography has made the demand for strong means to recognize the secret information. If the attacker don't have the secret key then he cannot access the hidden data.We consider that the attacker knows the algorithm, in cryptography[4]. In the steganography, stegnalysis is the process which decides whether the hidden message is present in an image or not. It differentiates the cover image and the stegoimage. A steganalyst is a person who has skill to find messages which are hidden by steganography. Steganalyst can be of two types. Either he can be active or passive.

- The staganalyst is called as active if he/her tries to find out the messages by the estimation.
- A passive staganalyst can detect the presence if hidden data. Passive staganalyst can detect the method of data hiding.

1.1 Measures of Steganalysis: To identify that a suspected medium is embedded with secret data or not, is the main goal of steganalysis. There are four possible situations to steganalyze the suspected medium, which are as following:

- False positive (*FP*): A cover medium is wrongly classified as stego.
- 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.

During the setganalysis process, at least one of above the condition will occur [33].

1.2 Techniques ofsSteganalysis [23]: Steganalysis techniques are of two types which are as given below:

1.2.1 Embedded Algorithm Based Steganalysis Technique: The advantage of particular algorithmic detail of the embedding algorithm is taken by this approach.

1.2.2 Universal Steganalysis Technique: To detect the presence of embedded message independent of the embedded algorithm, this technique is applied. This technique is also called as Blind Steganalysis Technique.

1.3 Statistical and Quality Parameters: The image measure parameters have discussed in this section. In the development steganalysis technique, these parameters are used.

1.3.1 Variance: It measures how far a set of numbers is spread out. If the expected value of a random variable X is (mean) $\mu = E[X]$, then the variance of X is given by the following equation:
Variance $(X) = E[(X-\mu)^2]$
That is, the expected value of the squared difference between the variable's realization and the variable's mean is the variance.

1.3.2 Mean Square Error (*MSE*): The average of the square of the error is measured by MSE. The amount by which value implied by the estimator differ from the quantity to be estimated, is known as the error. Due to the randomness or the estimator does not account for information that could produce a more accurate estimate, the difference occurred.
MSE for two images *A* and *B*, each of size $x \times y$, is given by:

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

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.

1.3.3 Peak Signal–to-Noise Ratio (*PSNR*): When there is a comparison between an original image and a coded/decoded

image, the PSNR is used. 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.

II. PRELIMINARY STUDY

Farid [12] proposed the information hiding techniques that have become more sophisticated and widespread. The detection of hidden messages has become more difficult, when the data carriers are high-resolution digital images. In this paper, the author proposed a new approach for the detection of hidden messages in the images. A wavelet like decomposition ˙to build high order statistical models of natural images are used, in this approach. To discriminate between untouched and adulterated images, a fisher linear discriminate analysis is used. Westfeld *et al.* [5] analyzed a powerful statistical attack which can be applied to any of the steganography technique. In this technique, a set of Pair of Values *(PoVs*) are used to detect the presence of secret message. In this paper, the author describes the fact that during message embedding process, any steganographic technique changes the frequency of pair of value. In the detection of the stego-images which are generated from detection of steganography algorithms, this method was effective. Westfeld*et al.* [6] described that there is various steganographic systems which are weak without against visual and statistical attacks. Without these weakness systems offer only a relatively small capacity for the steganographic messages. There is an F5 algorithm which is recently developed withstand visual and statistical attacks and it offers a large capacity of steganography. To improve the efficiency of the message embedding F5 implements the matrix encoding. It reduces the changes. Avcibas *et al.* [10] described a scheme which is based on LSB detection. This LSB detection scheme uses the binary similarity between the 7^{th} bit plane and 8^{th} bit plane. LSB hiding disrupted the natural correlation between the bit planes. On a per image basis this scheme does not auto-calibrate.

Problem Statement: Steganalysis is the technique which is used to extract, identify the message to be hidden in the various sourced of media. These media sources which used to hide the secret information can be images, text, audio, and video. As compare to generic steganalysis the scheme works better. But during message embedding process does not well change the frequency of pair of value. In the detection of stego-images, this method is very effective.Westfeld [6] described that there is various steganographic systems which are weak without against visual and statistical attacks. Without these weakness systems offer only a relatively small capacity for the steganographic messages. There is an F5 algorithm which is recently developed withstands visual and statistical attacks and it offers a large capacity of steganography. To improve the efficiency of the message embedding F5 implements the matrix encoding. It reduces the changes. After the preliminary study, we analyzed that using some mathematical formula, there is a need to do statistical analyses of digital images and develop the approach to detect the data.

III. RELATED WORK

Variance Based Steganalysis Approach:

1) Analyze the covert object.
2) Analyze the object that we want to send.
3) Calculate the variance between both object row wise.
4) Calculate the variance between both object column wise.
5) Calculate the difference of the variance between both object.
6) Draw a bar graph between variance of both object.
7) Count the number of rows and number of columns in which bar graph is not override.
8) Calculate 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.

Table .1. Variance based stegnalysis approach applied on hundred images

Image name	***PSNR* (in *dB*)**	**Variance**	
		Flag	**Time(sec)**
C1	60.84	1	0.1406
C2	61.50	1	0.1406
C3	61.08	1	0.1563
C4	61.58	1	0.1563
C5	61.10	0	0.1875
C6	52.80	0	0.1406
C7	60.95	1	0.1406
C8	62.45	1	0.1406
C9	60.92	0	0.1406
C10	60.54	1	0.1719
C11	60.77	1	0.1406
C12	60.63	1	0.1094
C13	60.55	0	0.1250
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	64.26	0	0.1406
C29	56.27	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	47.33	0	0.1406
C36	46.82	0	0.1250
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	47.63	0	0.1406
C43	48.22	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	60.95	0	0.1406
C59	60.88	0	0.1250
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
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	0.1406
C76	61.98	0	0.1563

C77	61.90	0	0.1563
C78	61.09	0	0.1406
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	49.12	0	0.1719
C90	49.26	0	0.1406
C91	49.26	0	0.1563
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	55.49	0	0.1250
C98	55.34	0	0.1563
C99	54.00	0	0.1563
C100	55.37	0	0.1406

The above Table shows the hundred images and their PSNR with corresponding Stego object. Flag 0 shows that there is no data in the image and flag 1 shows some hidden data in the image. The proposed approach take minimum time (0.148937 seconds on an average) but show only 18 images has hidden data. The proliferation of steganographic tools has created a demand for powerful means to detect hidden data.

IV. CONCLUSION

In this paper, the main attention is to develop a steganography technique by using statistical properties of an image to hide the data in to the covert image. Here, we also enquired the inherent detectability of the data hiding techniques which are commonly used. In the study of steganalysis, our proposed approach providing the satisfying result but still there is some problems in it for solving. We also conclude the future research directions in this field to hide the data. And we also believe that it will enhance the study of stealthy transmission of an interception of the data to be hidden. For the future,in order to achieve the blind steganalysis of the images and videos of various formats, the statistical properties will be further investigated.

V. REFERENCES

[1]. T. M. Cover, and J. A. Thomas, “Elements of Information Theory,” Wiley, 1991.

[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]. R. C. Gonzalez, R. E. Woods and S. L. Eddins, “Digital Image Processing Using MATLAB,” 5th Edition, Pearson, 2009.

[4]. L. Marvel, C. G. Boncelet Jr., C. T. Retter, “Spread Spectrum Image Steganography,” In Proceedings of IEEE Transactions on Image Processing, Vol. 8, No. 8, pp. 1075-1083, 1999.

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

[6]. A. Westfeld, “High Capacity Despite Better Steganalysis (F5- S Steganographic Algorithm),” In Proceedings of Lecture Notes in Computer Science: 4th International Workshop on Information Hiding, Vol. 2137, pp. 289-302, 2001.

[7]. B. Chen, and G. Wornell, “Quantization Index Modulation: A Class of Provably Good Methods for Digital Watermarking and Information Theory and Information Embedding,” In Proceedings of IEEE Transactions on Information Theory, Vol. 47, No. 4, pp. 1423-1443, 2001.

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

[9]. J. Fridrich, M. Goljan, and R. Du. “Detecting LSB Steganography in Color and Grayscale Images,” In Proceedings of Magazine of IEEE Multimedia, Special Issue on Security, Vol. 8, pp. 22-28, 2001.

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

[11]. 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.

[12]. H. Farid, "Detecting Hidden Messages Using Higher Order Statistical Models," In Proceedings of the IEEE International Conference on Image Processing, Vol. 2, pp. 905-908, 2002.

[13]. 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. 221229, 2003.

[14]. J. J. Harmsen, and W.A Pearlman, "Steganalysis of Additive Noise Modelable Information Hiding," In Proceedings of IST/SPIE's 15th Annual Symposium on Electronic Imaging Science and Technology, 2003.

[15]. P. Sallee, "Model Based Methods for Steganography," In Proceedings of Seconds International Workshop on Digital Watermaking, pp. 154-167, 2003.

[16]. 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.

[17]. S. Dumitrescu, X. Wu, and Z. Wang, "Detection of LSB Steganography viaSample Pair Analysis," In Proceedings of IEEE Transactions on Signal Processing, Vol. 51, No. 7, pp. 1995-2007, 2003.

[18]. S. Lyu, and H. Farid, "Steganalysis Using Color Wavelet Statistics and One Class Support Vector Machines," In Proceedings of IST/SPIE's 16th Annual Symposium on Electronic Imaging Science and Technology, 2004.

[19]. Y. Wang and P. Moulin, "Steganalysis of Block Structured Stegotext," In Proceedings of IST/SPIE's 16th Annual Symposium on Electronic Imaging Science and Technology, 2004.

[20]. P. Moulin, and Y. Wang, "New Results on Steganographic Capacity," In Proceedings of Conference on Information Sciences and Systems, 2004.

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

[22]. P. Sallee, "Model Based Methods for Steganography and Steganalysis", In Proceedings of International Journal of Image and Graphics, Vol. 5, No. 1, pp. 167190, 2005.

[23]. H. Farid, S. Lyu, "Steganalysis Using Higher-Order Image Statistics," In Proceedings of IEEE Transactions on Information Forensics and Security, Vol. 1, No. 1, pp. 1-10, 2006.

[24]. K. Sullivan, U. Madhow, S. Chandrasekran, B.S. Manjunath, "Steganalysis for Markov Cover Data With Applications to Images," In Proceedings of IEEE Transactions on Information Forensics and Security, Vol. 1, No. 2, pp. 275-287, 2006.

[25]. S. Bera, M. Sharma, "Steganalysis of Real Time Image by Statistical Attacks," In Proceedings of International Journal of Engineering Science and Technology, Vol. 2, No.9, 2010

[26]. A. D. Ker, "Steganalysis of Embedding in Two Least-Significant Bits," In Proceedings of IEEE Transactions on Information Forensics and Security, Vol. 2, No. 1, pp. 46-54, 2007.

[27]. H. Cai, S. S. Agaian, "JPEG Steganalysis Using Color Correlation and Training On Clean Images Only," In Proceedings of the Seventh International Conference on Machine Learning and Cybernetics, pp. 3710-3713, 2008.

[28]. 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.

[29]. A. G. H. Chamorro, M. N. Miyatake, "A New Methodology of Image Steganalysis Including for JPEG Steganography," In Proceedings of Electronics, Robotics, and Automotive Mechanics Conference, pp. 434438, 2010.

[30]. V. Singhal, D. Yadav, D. K. Bandil, "Steganography and Steganalysis: Review," In Proceedings of International Journal of Electronics and Computer Science Engineering, Vol. 1, pp. 399-405, 2011.

[31]. H. B. Kekre, A. A. Athawale, S. A. Patki, "Steganalysis of LSB Embedded Images Using Gray Level Co-Occurrence Matrix," In Proceedings of International Journal of Image Processing, Vol. 5, No. 1, pp. 36-45, 2011.

[32]. 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.

[33]. B. Li, J. He, J. Huang, Y. Q. Shi, "A Survey on Image Steganography and Steganalysis," In proceedings of Journal of Information Hiding and Multimedia Signal Processing, Vol. 2, No. 2, 2011.