Statistical Deformity in Steganogrpahy and its Overcomings

Parth Kaushik, Dr Kamaldeep Joshi, Jyoti Pandey, Tanu Garg

Abstract

Data Protection is important now days but most pivotal is to protect the medium through which data can be transfer from one point to another. To work upon it many different techniques are designed and implemented one of the techniques is Steganography . Steganography originates from greek word which means covered writing / or concealing information with other non secret text [Wikipedia]. Later on research different sub techniques of Steganography presented like Image, Audio, Text, Video etc. which uses different embedding mechanism to embed secret data in secure medium to prevent it from intruder. The first process tries to overcome the Targeted Steganalytic Attacks. This paper discusses Statistical properties of Steganography. Whenever message embed in a medium its properties changes and the resulted stego image will not be same as parent image . The work mainly revolve around first order statistics based targeted attacks. This paper proposes algorithm which can preserve image after embedding.

1. Introduction -

Information is everything and to transfer it over the internet it has become a top priority for many organization .Most of the times information hiding present negative effect when concerned to personal privacy. Threat to communication is very much whether in business, education or corporate sector. People trying to stole the medium of communication and provide secret conversation to their business rivals which result in data loss ,Moreover main threat to communication occurred when this medium used to transfer viruses such as Trojan which ultimately destroy privacy. Thus there is emerging need of technique which mainly protect the medium without revealing the contents of message and technique is called Steganography. Main goal behind it is to ensure privacy without any data loss and Steganography works on a principal by maximizing embedding and minimizing discernible rate.

The Art of data hiding is prevailing from ancient era. We all have seen famous example of King Herodotus sending messages by shaving head of his most trusted servant. Similar but different techniques can be seen from Indian context in period of Mahabharata. When queen draupadi swayamvar was conducted and each king sent a script in which message was encrypted through invisible ink and it only come into existence when they provide steam to that manuscript .Information hiding techniques are prevailing from many years but all of them are of different nature, each techniques depends on the context . But later working on all these techniques it was found that it is difficult to differentiate them without any common parameter .Now days, Steganography play a pivotal role and on further research it was found that choosing image as cover medium for secured communication is best because when message is embedded to image around 10k replicas of image created which become difficult for intruder to find correct image.

2. Steganography Statistical Attacks

2.1 Targeted Attacks

Every time when data embedded in image its features changes which allow intruders to detect the image and perform attack over it to stole relevant information .These attacks are developed in such manner that minute changes in stego image can be detected .Various types of targeted attacks are follows as-:

1. **Histogram Analysis:** Histgram is graphical representation of values in x-y coordinates system and these are effectively used in presenting image to find pecularieties.The main concerned about images here is to protect their stastical properties .It was analyzed that inside cover medium /images .No of odd pixels != No of even pixels while in case of stego image its vice versa followed.Based on it chi square test sugges 2 hypothesis i,e Null Hypo :either the image contains secret data ,H1 : Image doesnot contains secret embeded data.To choose which hypothesis will work it depends on confidence values"C". Elaborating discussion about histogram analysis can be found in [37].
2. **Sample Pair Assay**: This type of analysis is responsible of detecting random bits embedded in images. It is so accurate that it can easily measure the length of the message even if it is too minute relative to the image. Principle behind this techniques is that it uses four subset of image pixels (P,Q,R,S) whose number changes with rate of embedding (Fig 1) and such changes inform the user that bits are unevenly scattered . A assay of this technique can be found in[34].

2.2 Blind Attacks

These attacks follow the same phenomena as pattern classification problem. In blind attacks, the binary classifiers are trained on a set of order statistics data of the transform domain. On the basis of it, classifier will able to identify between embedded and nonembedded images. This technique tries to essay the cover medium statistics from stego image by minimizing the rate of embedding secret data inside the image. This phenomenon is also called as 'Cover medium prediction". Various attacks involved in these techniques are defined as as-:

1. **Wavelet Moment Analysis (WAM):** It is one of the most popular steganalyzer which filter noise from images considering that images are a mixture of diverse noises i.e. additive of Gaussian and non-Gaussian signals.
2. **Calibration Based Attacks:**

   These attacks estimate the statistical property of image i.e. it mainly identifies the noise with almost 100 % accuracy. This process works by decompressing to stego picture into JPEG domain by cropping 4*4 rows and column and then recompressing.Thus this process produces a calibrated image with features similar to the original image. The process use cropping of 4 pixels because when we recompress 8*8 grid one unable to saw the previous JPEG and thus the resulting DCT coefficient will not affect the DCT domain.
3. **Steganalysis Attack(Frequency domain attack)**

Factual imperceptibility is one of the fundamental parts of any steganographic calculation. To keep up measurable imperceptibility, the steganographic methods are composed with the point of limiting the antiquities presented in the cover motion by the inserting system. The primary accentuation is for the most part on limiting the commotion included by installing while at the same time expanding the payload.

This is a critical thought in the plan of installing calculations since the commotion included impacts the measurable properties of a medium. As of now said already, the calculation which rolls out less implanting improvements or includes less added substance commotion, for the most part, gives preferable security over the calculation which rolls out generally more improvements or includes higher added substance commotion .

From the perspective of the steganalyst, the assaults are intended to look at a flag and search for measurements which get contorted because of installing. These measurements run from minimal measurements of the first and second request if there should arise an occurrence of focused attacks [34, 38, and 39] and up to ninth request insights for daze assaults [40]. Thus, with a specific end goal to overcome these steganalytic assaults, there has been a move from the previously mentioned.

3 Methodology

Statistically invisible is one of the main aspects of any steganographic algorithm.To maintain the invisibility different techniques are designed and implemented such that secret message can be embedded in the cover medium. In order to save it from intruder principle must maintain to minimize artefacts.e noise by increasing the payload. Also from a different research point of view, it was proposed that algorithm which adds less noise provides better security than others [33].

According to steganalyst different attacks are designed to examine cover as well as its properties.They can be range from first-order statistics to second order statistics in case of targeted attacks.

Thus this chapter presents the preserving techniques for marginal statistics of an image in 3.1 and in 3.2 new algorithms is designed which preserves first order statistics. In 3.3 new methods is proposed to implement algorithm 3.2 in the realm.

This paper is mainly revolved around steganalysis and different research papers are reviewed and proposed. As the internet is spreading day by day and it becomes less secure and which directly make secret communication permeable.

3.1.1 Pixel Swapping

The idea behind pixel swapping was to insert data in such a way that the histogram of the image remains imperturbable. Here simple but effective algorithm was proposed called to be “Pixel Swap” which inserts

secret bits into cover image without any modifications to the original image histogram. The principle behind is to consider a pair of pixels such that their

difference is within a fixed threshold value. Let suppose to insert value 0, first, we have to check (if the first pixel >second pixel) or not, if so swapping of values will be done. In similar pattern pixel value, 1 can be inserted.

3.1(a) Algorithm for Pixel Swapping

I/P: Cover Medium (IMG) (I)

I/P Arguments: **Msg Stream** (*), **Threshold** (&), Pseudo **Key** (S)

Output: Embedded Image Is

1. (p1, p2) = Randomize (I, S) // p1, p2 are pixels of image

2. If | p1-p2| < = &

{

Proceed to step 3

Else return to: 1

3. If * (i) = 0

{

If p1 > = p2

Swap (p1, p2) // Swap function

i= i + 1 //increment of 1

Else i = i + 1

Go back to: 1

}}

Else go to step 4.

4. If *(i) = 1

If p1 < = p2

{

Swap (p1, p2)

I = I + 1

Else i = i + 1

Go back to: 1

}

Else to: 1.}

The process revolves around random (I, m) function which generates random pixels (p1, p2) by using secret key S. Once these pixels used by it cannot be reused further. After, it function swap called: Swap (p1, p2) which interchanges according to rule in lemma 1. Extraction of the above involves an inverse process of the above lemma. On analysis of PS algorithm, it was found that this algo by default preserves the values of bins.Thus it able to protect the image from the first order statistics attacks. The noise included should be restricted as long as f(x) is kept little. We tried the calculation at f (x)=2 and f(x)=5 i.e. viably we are introducing changes to the Least Significant Planes of the pixel gray level yet without disturbing the receptacle estimation of the two gray level qualities.

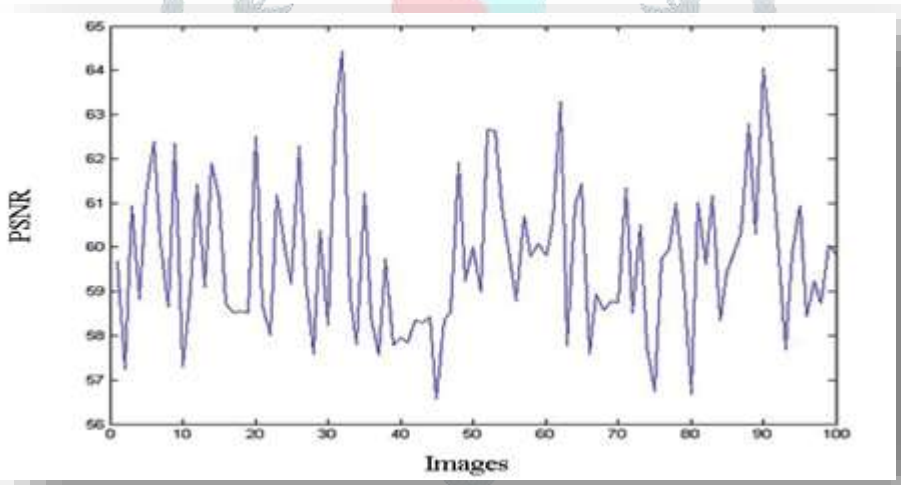

Fig 3.1 (i) PSNR for& =2

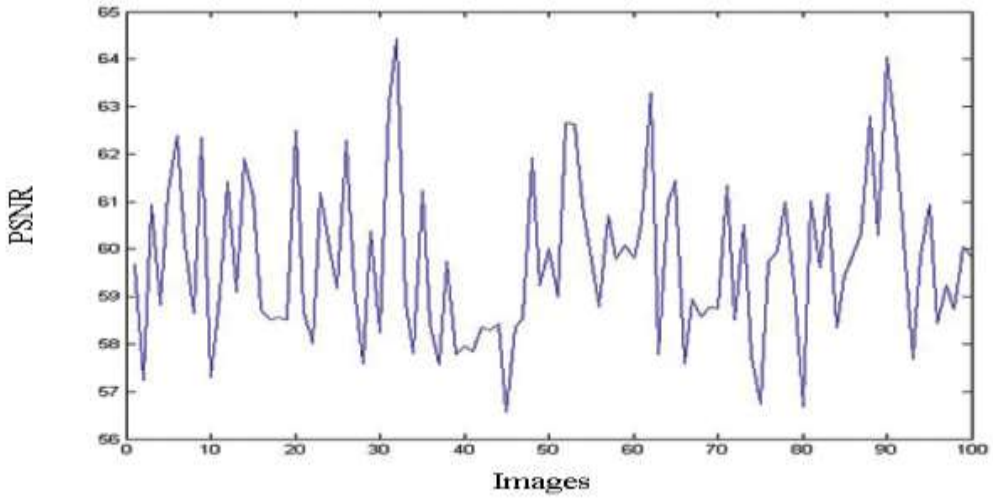

Fig 3.2(ii) PSNR for& =5

Fig 3.2: PSNR for the different values of &

3.2 Statistical Restoration

This technique as the name suggests Restoration which converts histogram of stego image into the histogram of the cover medium after successfully embedding of secret bits. As mentioned in the 1st picture. These restoration techniques will only give a better result if the cover medium would as close to a Gaussian distribution. It tries to overcome the drawback and provide a better result for the recreation of image histogram for non-Gaussian distribution as well

The histogram h (m) of a gray level scale image Im with range (0.....n) can be represented as discrete f(x) where h(rk) pk/p , where rk is the kth gray level. Pk can be defined as no of pixels with gray value = rk and p is the total no of pixels in the image (Im). Now histogram h(m) can also be represented as h(m) = {h(ro), h(r2), h(r3).....h(rn-1)} for simply h(m) = {h(ro), h(r2), h(r3).....h(n-1)}.

3.2(a)Statistical Restoration Algorithm

Algorithm: (SRA)

I/P: Cover Pic (I)

Arguments: Matrix (#), new Matrix ($)

S // No of pixels with gray value i

O/P: Stego Image (Is)

Begin

for all s> #(b, c) do

{

1. s = #(b, c)

2. If s> 0, s number of pixels with gray value i from the set of pixels used for compensation are changed to gray value j for full compensation.
Else k pixels with gray value j from the set of pixels used for compensation are changed to gray value i for full compensation

3. Compensation Vector (^) will be modified to reflect the pixel changes [29]

$$\hat{}(a) = \begin{cases} \hat{}(a) - s & \text{if } \hat{}(a) > s \\ 0 & \text{if } \hat{}(a) <= s \end{cases}$$

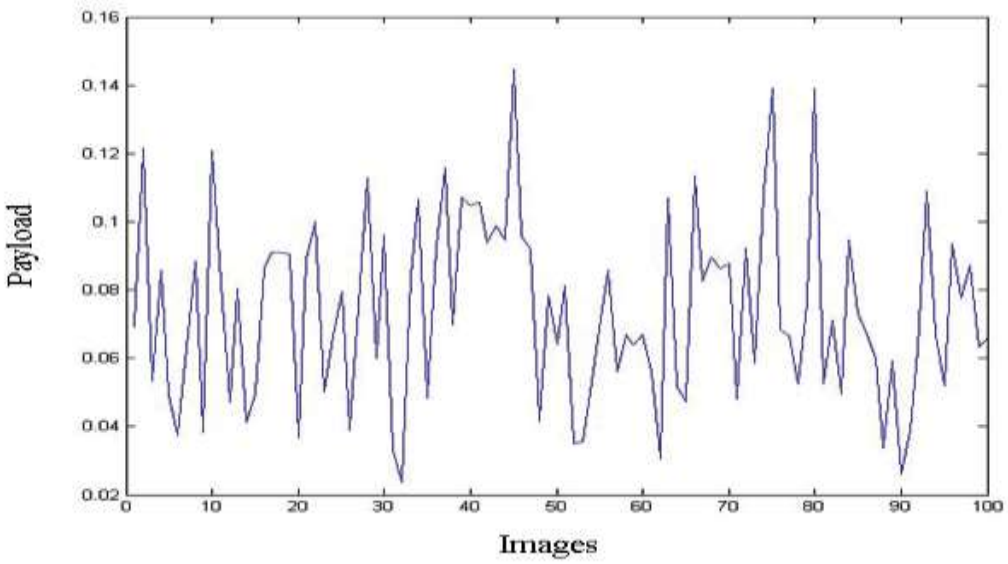

Fig 3.3(i) Max embedding rate for &=2

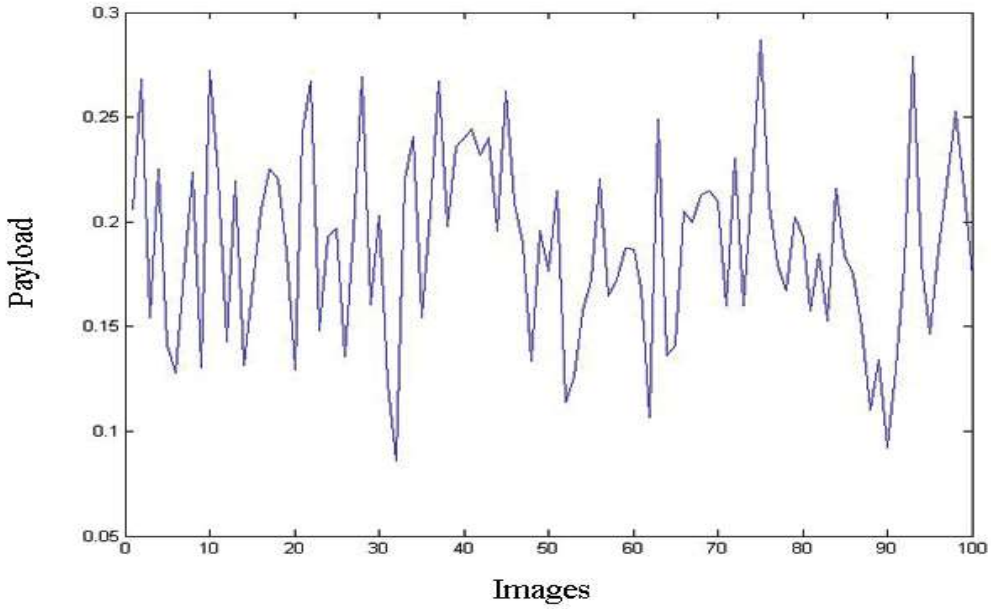

Fig 3.4 (ii) Max embedding rate at &=5

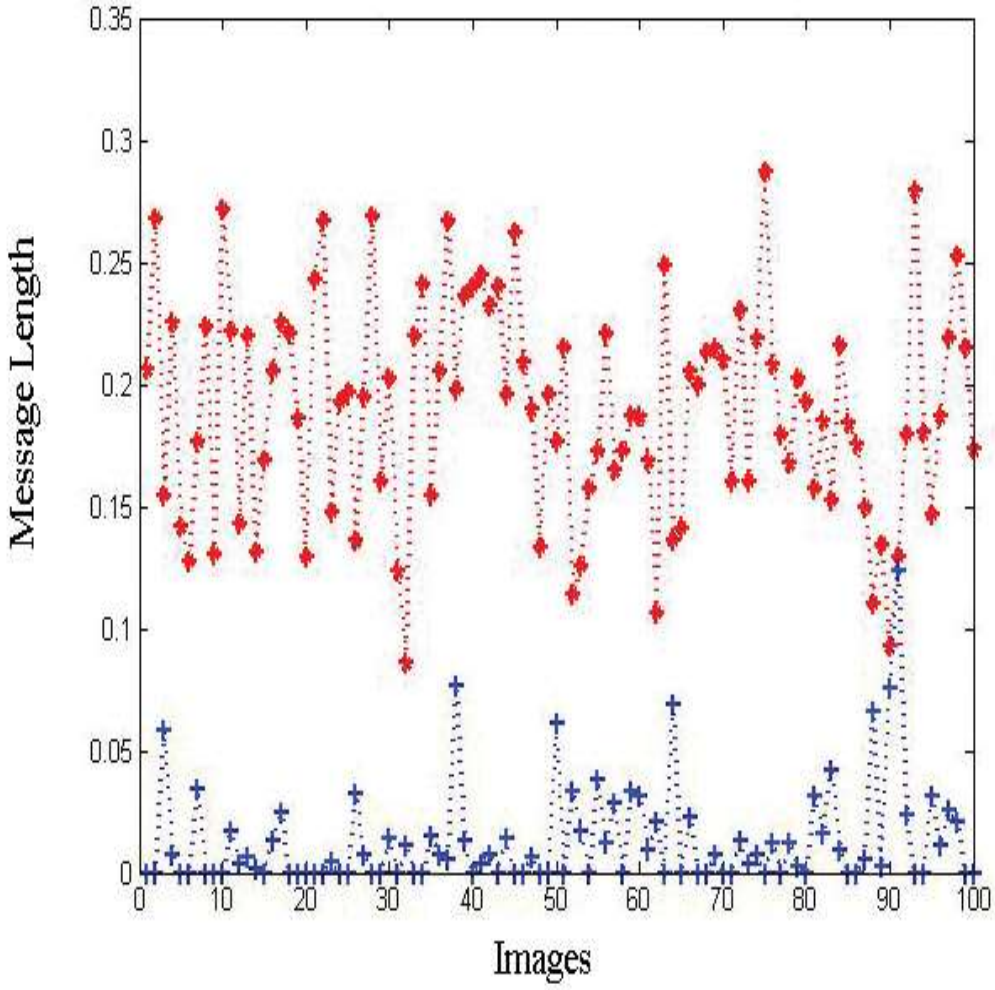

Fig 3.5: PS algorithm against Sample Pair Assault for &= 5. Red Plot:

Now representing the histogram of stego image h^m as h^(m) = {h^(0), h^(1), h^(2), h^(3)..... h^(n) . Later pixel of image categorized into 2 streams Embedding and Restoration. In embedding process kept record of Meta data about pixels recorder maintain all the details regarding amount of pixel change. After this, we integrate the histogram with the pixels from the Restoration technique using the meta data kept such that original histogram of the cover can be restored.

4 Conclusion

Paper is organized around statistical attacks in steganography which means when any message embed in image its properties changes and it become vulnerable to attacks by an intruder. Further, we analyze two kinds of attacks mainly visual and blind attacks.Which can be defined on their respective properties. To save the statistical property of image after embedding we follow first order statistics to find out how secure is our

image. We also developed 2 Algorithms especially pixel swapping and statistical restoration after that we compare these algorithms results through the author Solanki proposed scheme and it was found out our algorithm provides more security to the image . First algorithm was developed to preserve the first order statistics while embedding secret message inside the cover image. It can be seen that this technique maintain the quality of stego image by maintain acceptable quality. Another algorithm was developed to explicitly restore the properties of the image after data insertion inside the image. It was construct that under specified constraints algorithm provide the optimal solution. But it was later observed that although restoration technique can resist targeted attack but it breach the security concerns against blind attacks i.e. restoration process act as a source of noise in the cover signal which can later be captured during extraction of the image.

To overcome this new approach was found i.e. calibration based blind attacks, they disturbs the estimation of attack on further study it was predicted that "Stego population remain statistically closer to the cover population & the difference between these two cannot be observed." Thus algorithm performance is optimal in breaking the calibration based blind attacks

Future Directions

Over the span of this work, some extensive future work will be done in future. Right off the bat, it was watched that a large portion of the steganography inquire about till date has been towards outlining calculation which produce stego pictures which are as near the cover as could be expected under the circumstances. Every one of the calculations examines the conduct of the cover picture while overlooking the message bit stream. It might be conceivable to plan some encoding capacities, which given a cover picture and an implanting calculation can change the message stream with the end goal that it turns out to be more appropriate for inserting than the first piece stream. This sort of steganography can be valuable even in the "Active Warden Framework" of steganography on the grounds that initially the altered message stream.

5.References :

[1] N. F. Johnson, and S. Jajodia, "Steganography: Seeing the Unseen", IEEE Computer,

Feb. 1998,pp. 26-34.

[2] J. Mielikainen,"LSB Matching Revisited", IEEE Signal Processing Letters , vol. 13, no.

5, May 2006, pp. 285 - 287 .

[3] A. Ker,"Steganalysis of Embedding in Two Least-Significant Bits", IEEE Trans. on InformationForensics and Security, vol. 2, no. 1, March 2007, pp. 46-54.

[4] X. Zhang , and S. Wang, "Steganography using multiple-base notational system and humanvision sensitivity, IEEE Signal Processing Letters, vol. 12, Issue 1, Jan. 2005, pp.67-70.

[5] D.C. Wu, and W.H. Tsai, "A Steganographic method for images by pixel-value differencing",Pattern Recognition Letters, vol. 24, Jan. 2003, pp. 1613–1626.

[6] H.C. Wu, N.I. Wu, C.S. Tsai, and M.S. Hwang, "Image steganographic scheme based on pixel-value differencing and LSB replacement methods", IEE Proc. Vision, Image and Signal Processing, vol. 152, Oct. 2005, pp. 611-615.

[7] R. Crandall, "Some Notes on Steganography", Posted on Steganography Mailing List, 1998.

[8] A. Sur, P. Goel, and J. Mukhopadhyay, "A Spatial Domain Steganographic Scheme forReducing Embedding Noise", in Proc. 3rd International Symposium Communications,Control and Signal Processing (ISCCSP 2008), St. Julians, Malta, 12-14 March, pp. 10241028.56

[9] A. Sur, P. Goel, and J. Mukhopadhyay, "A SDS based Steganographic scheme for reducingEmbedding Noise", 15th International Conference on Advanced Computing and Communication,(ADCOM-2007), Guwahati, India, 18-21 Dec., pp. 771-775.

[10] I.J. Cox, J. Kilian, F.T. Leighton, T. Shamoon, "A Secure, Robust Watermark for Multimedia", in Proc. of the 1st Int. Workshop on Information Hiding, Cambridge, U.K, 30thMay - 1 June 1996 ,pp. 185-206.

[11] E. Koch, and J. Zhao, "Towards Robust and Hidden Image Copyright Labeling", in Proc.IEEE Workshop on Nonlinear Signal and Image Processing, Halkidiki, Greece, June.1995, pp. 452-455.

[12] I. Avcibas, N. Memon, and B. Sankur, "Steganalysis using Image Quality Metrics", IEEETrans. on Image Processing, vol. 12, Feb 2003, pp. 221-229.

[13] H. Farid, and L. Siwei, "Detecting Hidden Messages Using Higher-Order Statistics andSupport Vector Machines", in Proc. 5th Int. Workshop on Information Hiding, Noordwijkerhout,The Netherlands, 7-9 Oct. 2002, pp. 340-354.

[14] J. Fridrich, "Feature-Based Steganalysis for JPEG Images and its Implications for FutureDesign of Steganographic Schemes", in Proc. 6th Int. Workshop on Information Hiding,Toronto, Canada, 23-25 May 2004, pp. 67-81.

[15] K. Solanki, A. Sarkar, and B.S. Manjunath, "YASS: Yet Another Steganographic Scheme that Resists Blind Steganalysis", in Proc. 9th Int. Workshop on Information Hiding, Saint Malo, Brittany, France,11-13 June 2007, pp. 16-31.

[16] J. Wang , J. Li, and G. Wiederhold, "SIMPLicity : Semantics-sensitive integrated matching for picture Libraries", IEEE Trans. on Pattern Analysis and Machine Intelligence, vol.23, no. 9, Sept. 2001, pp. 947-963.

[17] A.Westfeld, "High capacity despite better steganalysis (F5 - a steganographic algorithm)",in Proc. 4th Int. Workshop on Information Hiding, Pittsburgh, PA, USA, pp. 289-302, 25-27 April 2001.

[18] N. Provos, "Defending against statistical steganalysis", in Proc. 10th USENIX SecuritySymposium, vol. 10, pp. 24-24, Washington DC, 2001.57

[19] P. Sallee, "Model-based steganography", in Proc. 2nd International Workshop on DigitalWatermarking, Seoul, Korea, pp. 154-167, 20-20 Oct. 2003.

[20] J. Fridrich, M. Goljan, P. Lisonek, and D. Soukal, "Writing on wet paper", IEEE Trans.

on Signal Processing, Special Issue on Media Security, vol. 53, Oct. 2005, pp. 3923-3935.

[21] K. Solanki , K. Sullivan, U. Madhow, and B.S. Manjunath, and S. Chandrasekaran, "Statisticalrestoration for robust and secure steganography", in Proc. IEEE Int. Conf. on ImageProcessing, Genova, Italy, vol. 2, 11-14 Sep. 2005, pp. 1118-1121.

[22] K. Solanki, K. Sullivan, U. Madhow, B.S. Manjunath, and S. Chandrasekaran, "Probably secure steganography: Achieving zero K-L divergence using statistical restoration", inProc. IEEE Int. Conf. on Image Processing, Atlanta, GA, USA, 8-11 Oct. 2006, pp. 125-128.

[23] K. Solanki, N. Jacobsen, U. Madhow, B.S. Manjunath, and S. Chandrasekaran, "Robust

image-adaptive data hiding based on erasure and error correction", IEEE Trans. on Image

Processing, vol. 13, no. 12, Dec. 2004, pp. 1627-1639.

[24] M. Kharrazi, H.T. Sencar, and N. Memon, "Cover selection for steganographicembedding",in Proc. Int. Conf. Image Processing. Atlanta, GA, USA, pp. 117-120, 8-11 Oct., 2006.

[25] X.G. Xia, C.G. Boncelet, and G.R. Arce, "A multiresolution watermark for digital images",IEEE Int. Conf. on Image Processing, Washington, DC, USA, 26-29 Oct. 1997.

[26] A. Sarkar, K. Solanki, and B.S. Manjunath, "Further Study on YASS: Steganography

Based on Randomized Embedding to Resist Blind Steganalysis", in Proc. SPIE - Security,

Steganography, and Watermarking of Multimedia Contents X, San Jose, California,

vol. 6819, pp. 681917-681917-11 , Jan. 2008.

[27] S. Hetzl, and P. Mutzel, "A graph theoretic approach to steganography", in Proc. 9th IFIPInt. Conf. on Communications and Multimedia Security, Salzburg, Austria, pp. 119-128,19-21 Sep. 2005.

[28] T. Pevny , and J. Fridrich, "Merging Markov and DCT features for multi-class JPEG steganalysis",in Proc. SPIE, Electronic Imaging, Security, Steganography, and Watermarkingof Multimedia Contents IX, San Jose, CA, vol. 6505 , Jan 2007, pp. 03-04.58

[29] R.A. Johnson, "Miller & Freund's Probability and Statistics for Engineers", Prentice Hallof India Pvt. Ltd., New Delhi, 2003.

[30] C. Chen, Y.Q. Shi, W. Chen, and G. Xuan, "Statistical moments based universal steganalysisusing JPEG-2D array and 2-D characteristic function", in Proc. Int. Conf. on ImageProcessing, Atlanta, GA, USA, 8-11 Oct., 2006, pp. 105-108.

[31] R.O. Duda, P.E. Hart, and D.G. Stork, "Pattern Classification", John Wiley & Sons Inc., New York, 2000.

[32] H. Farid, "http://www.cs.dartmouth.edu/farid/research/steg.m" (Code for generating

Wavelet-based feature vectors for steganalysis.)

[33] J. Fridrich, and D. Soukal, "Matrix Embedding for Large Payloads", IEEE Trans. on InformationForensics and Security, vol. 1, Sept. 2006, pp. 390-395.

[34] S. Dumitrescu, X. Wu, and N. Memon, "On steganalysis of random lsb embedding in

Continuous-toneimages",in Proc. IEEE International Conference on Image Processing,

Rochester, New York., September 2002.

[35] J. Fridrich, T. Pevny, and J. Kodovsky, "Statistically Undetectable JPEG Steganography: Dead Ends, Challenges, and Opportunities", in Proc. ACM Multimedia and SecurityWorkshop,Dallas, TX, 20-21 Sept. 2007, pp. 3-14.

[36] R Tzschoppe, R. Buml and J J. Eggers, "Histogram Modifications with Minimum MSE Distortion", Technical Report, December 18, 2001, Erlangen, Germany.

[37] R Chandramouli , M Kharrazi and N Memon, "Image Steganography and Steganalysis:

Concepts and Practices", in Proc. 2nd Int. Workshop on Digital Watermarking, Seoul,

Korea, 20-22 Oct. 2003, pp. 35-49.

[38] J. Fridrich, M. Goljan and R. Dui, "Reliable Detection of LSB steganography in Color andGrayscale Images",in Proc. ACM Workshop on Multimedia and Security, Ottawa, CA, 5thOct. 2001, pp. 27-30.

[39] A.D. Ker, "Steganalysis of LSB matching in grayscale images", IEEE Signal Processing Letters, vol. 12,pp. 441–444, June 2005.59

[40] J. Fridrich, M. Goljan, and T. Holotyak, "New Blind Steganalysis and its Implications", inProc. SPIE Security, Steganography, and Watermarking of Multimedia Contents VIII, vol. 6072, pp. 607201, Jan. 2006

[41] J. J. Eggers, R. Bauml, and B. Girod, "A communications approach to image steganography",in Proc. SPIE Security and Watermarking of Multimedia Contents IV, vol. 4675, pp.26-37, April 2002.

[42] J. Fridrich, M. Goljan, and D. Hogea,"Steganalysis of JPEG Images: Breaking the F5 Algorithm",in Proc. 5th International Workshop on Information Hiding, Noordwijkerhout,

The Netherlands, 79 Oct. 2002, pp. 310 - 323.

[43] J. Harmsen, and W. Pearlman, “Steganalysis of additive noise modelable information hiding”,in Proc. Security andWatermarking of Multimedia Contents V, vol. 5020, June 2003,pp. 131-142.