Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 79 (2016) 321 – 327

Procedia Computer Science

7th International Conference on Communication, Computing and Virtualization 2016

Statistical Steganalysis of High Capacity Image Steganography with Cryptography

S.K.Sabnis[a], R.N.Awale[b]

[a]*Asst..Professor. MCT's Rajiv Gandhi Institute of Technology, Mumbai-400053, India.*
[b]*Professor, VJTI, Mumbai-400019, India*

Abstract

Steganalysis of high capacity Wavelet based fusion image steganography with encryption, using Image quality metrics (as a set of features) is proposed. As the first order image statistics using the proposed algorithm are inherently preserved, which is desirable feature of the scheme, improving the security of algorithm against the targeted attacks .In addition comparing the present steganography scheme with two different encryption techniques, on the undetectibility ground, the generalized objective metric like SVD is used as a steganalysis tool. DFrFT encryption is found statistically and visually undetectable achieving the desired robustness though PSNR values are better in DNA encryption

Peer-review under responsibility of the Organizing Committee of ICCCV 2016

Keywords: Steganography; Steganalysis; Image quality metric; robustness; Singular value decomposition; imperceptibility

1. Introduction

Several aspects of the information embedding in images using steganographic techniques are addressed with knowledge of the algorithm/method (which we should always assume), it is very hard to hide messages in an undetectable way. This difficulty increases with the size of the message and the desired robustness of the scheme. Even though we have been able to preserve that first order statistics, while restoration an additional amount of noise gets added to the cover image which can disturb the higher order statistics of the image which are used by the blind attack.

* Corresponding author.
E-mail address: shirish.sabnis6@gmail.com

Peer-review under responsibility of the Organizing Committee of ICCCV 2016
doi:10.1016/j.procs.2016.03.042

1.1 Requirements of Steganography:

Stegaanographic capacity: By steganographic capacity we mean the number of bits that can be embedded given a level of security. This is different from data hiding or watermarking capacity. Specific capacity measures can be computed given detector and steganographic algorithm (Chandramaulli,Memon). Requirements for higher payload and secure communication are often contradictory (shown in Figure 1). Depending on specific application scenarios, a trade off has to be sought.

Robustness: The ability of the embedded data to remain intact if the stego image undergoes transformation due to intelligent stego attacks.

Imperceptibility: It is important when a secret communication occurs between two parties and the fact of a secret communication is kept to be secret.

Security: This refers to eavesdropper's inability to detect the hidden information. In order to avoid raising suspicious of eavesdroppers, while evading the meticulous screening of algorithm detection, the hidden content must be invisible both perceptually and statically.

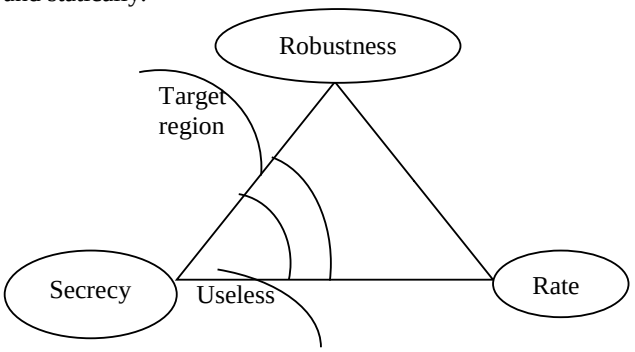


Fig 1: Triangle of peril

Steganography finds application for information security needed to defend against internal/ external hackers, secure commerce, secure bank account, electronic transfers, secure intellectual property, digital rights management, hiding executable multimedia files, covert communication.

2. RELATED WORK

Steganalysis is the process of official counter attack science, has defeated steganographic algorithms whether they are based on the traditional spatial domain or the transform domain. The problem is generally handled with statistical analysis. Stastical undetectibility is one of the main aspects of any steganographic algorithm. Statistical digital signal processing is often used in order to detect data within images. These statistics range from marginal statistics of first and second order in case of targeted attacks and upto ninth order statistics for blind attacks. By exposing the flaws to the algorithm, the user can further improve the algorithm in order to make it more difficult to detect whether or not data is hidden in the images. Steganalysis is achieved through applying different image processing technique eg. image filtering, rotating, cropping, translating etc. More deliberately steganalysis can involve coding a program that examines the stego image structure and measures its statistical properties. From the point of view of steganalyst the attacks are designed to examine a signal and look for statistics which gets distorted due to embedding These statistics range from marginal statistics of First order statistics(histograms)or second order statistics(correlation between pixels, distance, direction)and second order in case of targeted attacks&upto 9^{th} order for blind attacks.

2.1 Visual Attacks:

These methods try to detect the presence of information by visual inspection either by the naked eye or by a computer. The attack is based on guessing the embedding layer of an image (say a bit plane) and then visually inspecting that layer to look for any unusual modification in that layer. These methods use statistics of the image to reveal tiny alterations in the statistical behavior caused by steganographic embedding and hence can successfully detect even small amount of embedding with very high accuracy. These class of attacks are further classified as 'Targeted attacks' or 'Blind attacks' These attacks are designed keeping a particular steganographic algorithm in mind. These attacks are based on the image features which get modified by a particular kind of steganographic embedding.

2.2 Blind Attacks:

The blind approach to steganalysis is similar to the pattern classification problem. The pattern classifier, in our case a Binary Classifier, is trained on a set of training data. The training data comprises of some high order statistics of the transform.

*Classifier***:** As noted earlier, the calculated features vectors obtained from each universal steganalysis techniques are used to train a classifier, which in turn is used to classify between cover and stego images. A number of different classifiers could be employed for this purpose. Two of the techniques more widely used by researchers for universal steganalysis are Fisher's linear discriminate FLD and support vector machines SVMs.

Wavelet Absolute Moment (WAM) Analyzer: It is the most popular Blind Steganalyzer for Spatial Domain Embedding. WAM uses a denoising filter to remove Gaussian noise from images under the assumption that the stego image is an additive mixture of a non-stationary Gaussian signal (the cover image) and a stationary Gaussian signal with a known variance (the noise). The detailed procedure for calculating the WAM features in a gray scale image can be found in [4].

Calibration Based Attacks: The calibration based attacks estimate the cover image statistics by nullifying the impact of embedding in the cover image. They are designed for JPEG domain steganographic schemes. They estimate the cover image statistics by a process termed as Self Calibration. The steganalysis algorithms based on this self calibration process can detect the presence of steganographic noise with almost 100% accuracy even for very low embedding rates. [5].

Farid's wavelet based attack: It is based on the features drawn from the wavelet coefficients of an image. This attack first makes an n level wavelet decomposition of an image and computes four statistics namely Mean, Variance, Skewness and Kurtosis for each set of coefficients yielding a total of 12x (n-1) coefficients. The second set of statistics is based on the errors in an optimal linear predictor of coefficient magnitude. It is from this error that additional statistics i.e. the mean, variance, skewness, and kurtosis are extracted thus forming a 24x (n-1) dimensional feature vector. After extraction of features, a Support Vector Machine (SVM) is used for classification [6].

Image Quality Metrics: Metric arises from the strength parameter of steganography artifacts and not from the variations in the image content.
a)Universal image quality Index: The dynamic range of UQI is[-1,1] ,this index models any distortion as a combination of three factors; loss of correlation, mean distortion and variance distortion. The index is computed using a sliding window approach with a window size of 8x8 leading to a quality map of the image .The overall quality index average of all UQI values in the quality map.[11]

b)Singular value decomposition: SVD Measure is classified in two ways proposed in [12]
Global measure (Numerical measure): It is derived from graphical measure. It computes the global error expressed as a single numerical value depending on the distortion type which is expressed as a Minkowski measure where $\beta=2$

Local measure (Graphical measure): It is a bivariate measure that computes the distance between singular values of the original image block and singular values of the distorted image block.

3. Proposed Work:

Given a cover image c of size (n * m) and payload p of size (2n * 2m).

(i) Robustness against change in image file formats, resizing, filtering etc.

(ii) Steganalysis using IQM i.e. exploiting image quality measures, not as predictors of subjective image quality or algorithmic performance but specifically as a steganalysis tools, that is, as feature in detecting hidden messages.

(iii)In this context of steganalysis, comparision of method with two different encryption schemes is done.

3.1 Choice of IQMs:

IQMs that are sensitive specifically to steganography effects that is, those measures for which the variability in score data can be explained better because of some treatment rather than as random variations.

The rationale arising several quality measures is that different measures respond with different sensitivities to artifacts and distortions. For example, a) Mean square error responds to additive noise b)Spectral phase or mean square HVS weighted error are more sensitive to blur,c)Gradient measures react more to distortions concentrated around edges and textures.

3.2 Encryption techniques:

Comparison of two encryption techniques proposed is given below.

1. Encryption of digital images using Fractional Wavelet Transform (FWT) and random phase masks (RPMs) which is discussed in authors earlier publication[13], the results are shown in Figure 2.
2. Encryption Key Generation Using DNA Sequence, in which generation of encryption key is based on ACGT pair. [15], the results are shown in Figure 3.

3.3 SVD Measure:

We have applied singular value decomposition method as image quality measure to predict the distortion introduced by embedding locally and globally as follows.

a) Graphical measure: Which computes the distance between singular values of original and stego image block of size 8x8 local assessment.

   The equation for the graphical measure is as follows. $D_i = Sqrt[\sum_{i=1}^{n}(Si - Si\ )^2]$

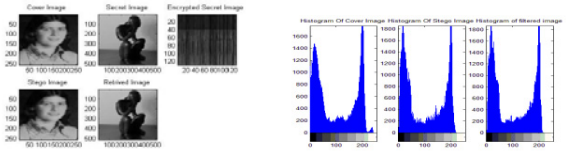
   Si ---Singular value original

   Si^ ---Singular value of stego image

b) Numerical measure: It computes the global error expressed as a single numerical value depending on the distortion type

4. Implementation:

System implemented in Matlab 2010 by taking into account various formats and various sizes of cover and payload image,with their histograms with a common reference is shown below.



. Fig 2:Results Encryption technique 1

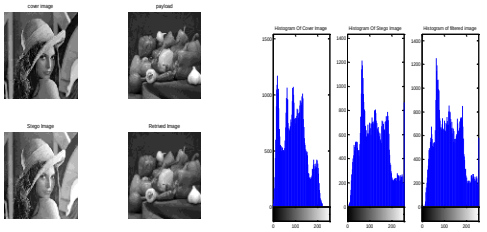


Figure 3:Results Encryption technique 2

4.1 Result Analysis:

The image statistics awareness test was carried out and it was found practically that the generated stego image will be immune to statistical steganalysis for both the techniques with a common reference as shown in figure 2 & 3 above. Among several statistical measures available, we have selected the following IQMS for both the techniques as shown in the Table 1 &2.

Table 1 IQM for technique 1

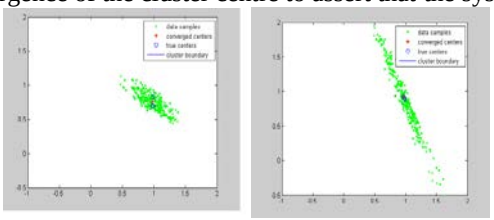
Images	Type	MSE	PSNR	NAE	NCC	UIQI
Catherine africasculpt	JPEG JPEG	0.0017	32.6748	0.060	0.990	0.831
Lena Wpeppers	BMP JPEG	0.0017	33.5501	0.062	0.986	0.704
Cameraman Wpeppers	TIF JPEG	0.002	33.3291	0.051	0.979	0.702

.

Table 2 IQMs for technique 2

Images	Type	MSE	PSNR	NAE	NCC	UIQI
Catherine africasculpt	JPEG JPEG	0.017	65.73	0.282	0.959	0.930
Lena Wpeppers	BMP JPEG	0.018	65.49	0.275	0.986	0.882
Cameraman Wpeppers	TIF JPEG	0.016	65.85	0.225	0.980	0.904

Cluster of the IQMs i.e. Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR)
Normalized cross correlation (NCC),Normalized absolute error (NAE),Universal image quality index(UIQI) are plotted showing the trend of convergence of the cluster centre to assert that the systems are statistically immune.



Cluster IQM 1 *Cluster IQM 2*

Fig 4

SVD based measure: Distortion maps (graphical measure) in both cases with a block size 8 results in more detailed distortion maps leading to higher correlation with subjective evaluation. The graphical measure does not require a simplified model of the HVS, hence they do not have any assumptions concerning the viewing distance and the distortion type.

a) b)

Fig 5 a)Distortion map for tech1 b)Distortion map for tech2

5. Conclusion:.

As the scheme inherently preserves the first order statistics. Because information hiding techniques are often based on the visual masking effect of human visual system, it is not suitable to use only PSNR to evaluate the stego- image degradation. Hence we investigate statistical detectibility using image quality metrics. We seek IQMs that are sensitive specifically to steganography effects.In this context comparison of two encryption techniques, is presented. The most reasonable method for evaluating subjective quality by observation. The SVD measure offers that perspective. From the distortion maps of graphical measure percentage distortion is more in technique 1 but one can, not detect any message on the basis of type of distortion hence the embedding system is immune statistically and perceptually.

References

1. N. Provos and P. Honey man. "Hide and Seek: An Introduction to Steganography", IEEE: Security and Privacy, vol. 1, pp. 32-44, 2003.
2. H S Majunatha Reddy, and K B Raja , "HIGH CAPACITY AND SECURITY STEGANOGRAPHY USING DISCRETE WAVELET TRANSFORM " , International Journal of Computer Science and Security (IJCSS), Volume (3): Issue (6)
3. S. K. Muttoo and Sushil Kumar,"Image Steganogaraphy based on Complex Double Dual Tree Wavelet Transform",2010 International Conference on Multimedia Information Networking and Security.
4. Souvik Bhattacharyya and Gautam Sanyal,"Data Hiding in Images in Discrete Wavelet Domain Using PMM",International Journal of Electrical and Computer Engineering 5:6 2010
5. Amitava Nag, Sushanta Biswas, Debasree Sarkar and Partha Pratim Sarkar, "A Novel Technique for Image Steganography Based on DWT and Human Encoding" ,International Journal of Computer Science and Security, (IJCSS), Volume (4): Issue (6)
6. S. K. Muttoo and Sushil Kumar, "Robust Source Coding Steganographic Technique Using Wavelet Transforms",BVICAM's International Journal of Information Technology Bharati Vidyapeeth's Institute of Computer Applications and Management, New Delhi
7. Qingzhong Liu,Andrew H. Sung and Mengyu Qiao,"Improved Detection and Evaluation for JPEG Steganalysis",MM'09, October 19 - 24, 2009, Beijing, China. Copyright 2009 ACM 978-1-60558-608-3/09/10
8. Jessica Fridrich,"Feature-Based Steganalysis for JPEG Images and its Implications for Future Design of Steganographic Schemes,"Dept. of Electrical Engineering,SUNNY Binghamton, Binghamton, NY 13902-6000, USA.

9. R.Amirtharajan,R. Akila and P.Deepikachowdavarapu,"A Comparative Analysis of Image Steganography,"International Journal of Computer Applications (0975 -8887) Volume 2 - No.3, May 2010.
10. K.Sumathy 1, R.Tamilselvi "Comparison of Encryption Levels for Image Security Using Various Transforms" International Conference on Information and Network TechnologyIACSIT Press, Singapore IPCSIT vol.4 (2011).
11. Z. Wang and A. Bovik, "A universal image quality index," IEEE Signal Process. Lett., vol. 9, no. 3, pp. 81–84, Mar. 2002.
12. Aleksandr Shnayderman, Alexander Gusev, and Ahmet M. Eskicioglu"An SVD-Based Grayscale Image Quality Measure for Local and Global Assessment " IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 15, NO. 2, FEBRUARY 2006.
13. S.K.Sabnis,R.N.Awale"A High Capacity And Security Enhancement Image Steganography With Effective Encryption" International Journal Ascent Publications ISSN 0975-7074, Vol. 4, No. IV (October 2012), pp. 235-249.
14. Sapna Sasidharan and Deepu Sleeba Philip,"A FAST PARTIAL IMAGE ENCRYPTION SCHEME WITH WAVELET TRANSFORM AND RC4,"International Journal of Advances in Engineering and Technology, Sept 2011. IJAET ISSN: 2231-1963.
15. Ismail Amir Ismail, Mohammed Amin, and Hossam Diab,"A Digital Image Encryption Algorithm Based A Composition of Two Chaotic Logistic Maps" ,International Journal of Network Security, Vol.11, No.1, PP.1-10, July 2010.
16. Ozaktas H M, Barshan B, Mendlovic D, et al. "Convolution, filtering, and multiplexing in fractional Fourier domains and their relationship to chirp and wavelet transform". J Opt Soc Amer A, 1994, 11: 547-559.
17. Ismail Avcibas,Nasir Memon Bulent Sankur 'Steganalysis Using Image Quality Metrics' IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 12, NO. 2, FEBRUARY 2003.
18. Chunhua Chen,Yun Q Shi,wen Chen,Guorong Xuan " Statstical moment based universal steganalysis using JPEG 2-D Array and 2-D characteristic function" IEEE ICIP.