Defence Science Journal, Vol. 66, No. 6, November 2016, pp. 574-581, DOI : 10.14429/dsj.66.10797

On the Removal of Steganographic Content from Images

Amritha P.P.*, M. Sethumadhavan, and R. Krishnan

TIFAC CORE in Cyber Security, Amrita School of Engineering,
Amrita Vishwa Vidyapeetham, Amrita University, Coimbatore - 641 112 India
**E-mail: pp_amritha@cb.amrita.edu*

ABSTRACT

Steganography is primarily used for the covert transmission of information even though the purpose can be legitimate or malicious. The primary purpose of this work is to build a firewall which will thwart this transmission. This will be achieved by radiometric and geometric operations. These operations will degrade the quality of cover image. However these can be restored to some extent by a deconvolution operation. The finally deconvolved image is subjected to steganalysis to verify the absence of stego content. Experimental results showed that PSNR and SSIM values are between 35 dB - 45 dB and 0.96, respectively which are above the acceptable range. Our method can suppress the stego content to large extent irrespective of embedding algorithm in spatial and transform domain. We verified by using RS steganalysis, difference image histogram and chi-square attack, that 95 per cent of the stego content embedded in the spatial domain was removed by our showering techniques. We also verified that 100 per cent of the stego content was removed in the transform domain with PSNR 30 dB - 45 dB and SSIM between 0.67-0.99. Percentage of stego removed in both domains was measured by using bit error rate and first order Markov feature.

Keywords: Radiometric and geometric operations, PSNR, structure similarity index metric, variational deconvolution, steganalysis, steganography

1. INTRODUCTION

Steganography is an art of covert communication. Historically, steganography has been done in many ways but here we are discussing only digital methods of steganography. In steganography, the secret is hidden within an innocent-looking medium such as text, image, audio or video files. It is not only difficult to detect whether hidden information exists or not, but it is even difficult to extract it without knowledge of the key. This leads to a security concern about prevention of illegal or malicious information transmission through the Internet. There is already some evidence that terrorists used image steganography to transmit their attack plans through websites such as eBay[1]. Hence it is useful to investigate the countermeasures for steganography. Steganalysis is the set of techniques which try to detect the hidden information. The role of the steganalyst can be defined in two ways: passive or active. The passive steganalyst intercepts the cover medium as it is passed through the communication channel, and then tests it to identify whether it contains a secret message or not. An active steganalyst on the other hand, can also modify the secret content so that the integrity of the message is broken. The success of steganalysis depends on the prior information available to him. Steganalysis can also be classified into targeted and universal. Targeted steganalysis can be employed when the steganographic algorithm is known[2]. Universal steganalysis does not assume the knowledge of the algorithm used and hence will employ multiple features so that a variety of known stego algorithms can be analysed. When a new steganographic method is used by a malicious user for communication, the training set used for universal steganalysis will show some false positives.

Our primary motivation in this work is to create a steg-firewall. This firewall will not only prevent objectionable material from coming into a system but can also protect against sensitive information being sent out from the system in the garb of stego. In other words, this could be used to prevent industrial espionage. This calls for the destruction or degradation of the objectionable content without significantly affecting the source or cover image. Even though steganography is used for legitimate purpose; it is also widely used for illegal purposes which include terrorism related activities as well as purveying of pornographic material. Hence there is a need for creating a firewall which can destroy the steganographic content of an otherwise normal and legitimate source. We propose a method to suppress stego content partially or completely while keeping the perceptual quality of the image at an acceptable level. In fact, in most of the cases, Internet security requires only to block harmful information from spreading, rather than knowing what that information is. Hence the goal of our method is different from that of passive or active steganalysis. Despite the similarities between digital watermarking and steganography, not much research has been put into the study of stego removal and analysis on how much secret has been

Received : 31 January 2016, Revised : 30 April 2016
Accepted : 19 July 2016, Online published : 31 October 2016

removed. This paper critically examines the quantum of stego content being removed by incorporating methods similar to that of digital watermarking in addition to targeted and universal steganalysis. On the other hand, if no stego is present in communication, our techniques can still be applied due to the fact that no noticeable disturbances are introduced in the cover image.

A novel combination of various image processing operations for the generic removal of steganographic communication is proposed in this paper. In many of the existing approaches, active steganalysis is done either by applying watermarking attacks or by filtering/denoising method and then quality of the stego free image is measured using peak signal to noise ratio (PSNR). In our approach, after performing operations, we apply image quality enhancement via variational deconvolution[3] on the degraded output image and then final output image undergoes statistical steganalysis to get the percentage of hidden information removed. The performance of the restored image is measured using PSNR and structured similarity index measure (SSIM).

2. BACKGROUND AND RELATED LITERATURE

Techniques have been proposed which aim at the attack on digital watermarking or steganography systems. In this area different attacks and attack suits have been evolved both for images and audio data as cover media. In this section we will give a short overview on how our techniques differ from existing approaches. Westfeld & Pfitzmann[4] mentioned attacks on steganographic systems and mainly focused on digital images as cover media but no comprehensive prevention techniques were described. The first version of the Stirmark attacks[5] was built for image watermarking and steganography algorithms. This applies various signal processing operations on the cover media in order to render the embedded data unusable. Fisk[6], *et al.* looks at the prevention of network steganography by an active warden. The goal of this research has been to stop all steganographic communications at a network firewall. In particular, they concentrated on structured carriers with objectively defined semantics, such as the TCP/IP protocol suite rather than on unstructured carriers such as images that dominate the information hiding literature. Our work differs from[6] by focusing on image data, for which steganalysis is implemented to suppress the stego content and is able to work in real-time.

Sieffert[7], *et al.* explained a framework called stego intrusion detection system. This system sniffs all HTTP traffic, reconstruct any image that are transmitted through the packets, test each image against all known steganalysis algorithms. Al-Naima[8], *et al.* created a firewall using wavelet based denoising technique for destroying stego content in image files. Destruction of secret message was verified by trying to extract secret message after the corresponding operation. Firewall acts as a filter, lets the clean files pass through it. Seven stego algorithms were tested and compared the PSNR of stego image after destruction. Compared to Al-Naima[8], *et al.* authors techniques try to restore the input image to the original cover as close as possible.

Christopher[9], *et al.* introduced a concept to destroy the stego content. Bit deletion and re-encoding of a JPEG is used to destroy the secret. They also used denoising techniques which include two spatial filters, the mean filter and the 5-coefficient Gaussian, three wavelet based methods, VisuShrink, BLS-GSM, the polynomial threshold, and the method of non-local means. These techniques were applied on four common steganography methods: LSB, +/-*k*, Jsteg, and Model based steganography. MSE, Visual Information Fidelity (VIF), SSIM were used to check the quality of the image.

Lafferty[10] explained some destructive scrubbing techniques to remove stego content. In her thesis, filtering based scrubbing method was used which can be applied to both domains. The author introduced a concept of composite scrubber. The effectiveness of scrubbing techniques varies with the image domain utilised for stego embedding. The performance of these scrubbing methods was tested using image quality metrics like MSE, PSNR, WPSNR, SNR. Our work enhances Lafferty[10] by restoring the quality of the image and steganalysis techniques were used to calculate the amount of stego content removed.

Nutzinger[11] performed a real time attack on audio steganography by addition of white noise, sample shifting, variable time delay, and frequency shifting. Independent of the stego algorithm the secret in audio data was removed. These attacks have minimal audio quality degradation, making them usable for different applications. The author has evaluated the quality of stego removed audio using perceptual evaluation of speech quality and mean opinion scale. Qi[12] proposed a novel active steganographic attack called discrete spring transform (DST) to destroy the stego content. This transform was applied on edges of the images extracted using Sobel filter and curve length method to protect against the image quality degradation. DST was applied on spatial and frequency domain and was successful in destroying the hidden data embedded within all mediums.

An overwriting approach was introduced by Ameen and Al-Badrany[13], where random data written again and again over stego images to remove the stego content. Denoising approach using filters and DWT (hard and soft thresholding) approach were also incorporated to remove the stego content. Comparison was made in terms of PSNR for different stego algorithms. They have taken pure cover and different noisy cover like Gaussian, salt and pepper for comparing their results. Our work differs from[13] by using geometrical and radiometric operations to suppress the stego content, increases the quality of the image and calculate the amount of stego content removed by using steganalysis.

Christopher[14,15], *et al.* explained how to estimate clean image from a stego image after applying denoising techniques using the receiver operating characteristic curve[16]. They employed a series of active warden based steganalysis including blind and targeted steganalysis methods and this highlights how clean image estimation is vital to these techniques. Detection performance was measured using higher order statistics and histogram characteristics function[17]. They used bit error rate to check the message after applying denoising techniques and the image quality were measured using VIF and SSIM.

3. PROPOSED SYSTEM

The main objectives of this work are

(i) Develop a Steg-Firewall that will act like a shower which is used before entering a clean room or leaving a secure area. This will suppress the stego content and thus prevent stego images from getting through or sensitive information from going out.
(ii) Examine the effectiveness of showering techniques in suppressing the stego content
(iii) Restore the quality of the degraded image after showering techniques are applied.
(iv) Estimate the percentage of stego content removed.

3.1 Approach

The primary goal of our paper is the obfuscation of stego content which is being passed to the end user. Current network defense mechanisms like firewall and intrusion detection systems will not stop any mails or attachments which contain steganographic content. The proposed Steg-Firewall will modify the incoming images in such a way that hidden information is either destroyed or obfuscated. It will be ensured that this modification affects the cover image only marginally. This process is done in both spatial and frequency domains. Figure 1 shows the architecture of the proposed mechanism. In image processing it is well known that textured and non-textured images are affected differently by low level image processing operations. Since our Steg-Firewall essentially employ low level operations, it was felt necessary that the incoming stego images be divided into textured and non-textured ones. The showering techniques are then applied on the image depending on its type. The showering, while degrading or obfuscating stego content will also have an unintended impact on the cover image, which in turn can lead to marginal degradation. The quality of degraded images is then enhanced using a restoration process. In the final stage, steganalysis is used after the restoration process to estimate the percentage of stego removed. If the output image still contains stego content the filtering process is repeated again on the original input image with a different sequence of operations. Still if it is suspicious we will advise to block that stego image for further use.

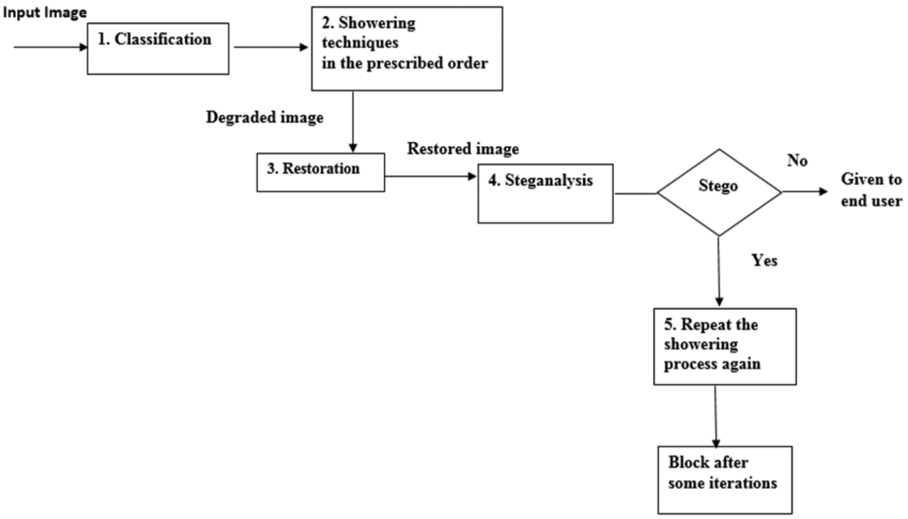


Figure 1. Proposed showering mechanism.

3.2 Proposed Procedure

Classification: Gray-level co-occurrence matrix (GLCM)[18] is used to automatically classify the images into textured and non-textured images. Depending on the type of images it is subjected to showering techniques in different order.

Showering techniques: With multiple types of steganography available, each modifying images in different ways, and embedding data in different places, it should be expected that different embedding methods will require different showering methods. To evaluate the effectiveness of the showering techniques, images with known stego content were used and the impact of these techniques on the removal of the said stego content was deterministically estimated. There are many different ways to approach the showering of steganographic images. Showering can be achieved either using radiometric operations or geometric operations or a combination of the two. The radiometric operations could include Median, Mean, Gaussian and Wiener filters of different window sizes (3, 5, and 7), Wiener restoration, and Wavelet thresholding. The geometric operations include rotation through various angles (1, 2, 3, 4, 5, 10, 15, and 20 degrees). Showering can be done in frequency domain as well. Apart from the filters mentioned above, the five combinational filters used here is summarised in Table 1. So a total of 27 different filters were applied on stego images to remove the stego content.

Table 1. The five different combination filters

Combination filter 1	Gaussian, Median, rotate degree 5
Combination filter 2	Gaussian, Wiener, rotate degree 5, median
Combination filter 3	Gaussian, Median, Wiener, rotate degree 5, Wiener restore
Combination filter 4	Rotate degree 5, Gaussian, Median
Combination filter 5	Median, rotate degree 5, Gaussian

Restoration: Variational deconvolution method is used to restore the quality of the degraded image obtained after applying showering techniques. Suitable kernel has to be selected for different filtering.

Steganalysis: To estimate the amount of stego removed. RS steganalysis[19], Chi-square attack[20], difference image histogram[21] are the three steganalysis methods that have been used to estimate the percentage of stego removed in spatial domain. BER and Markov feature were used to calculate the stego removed in transform domain.

If the steganalysis detects large amount of stego even after applying showering process then the same process has to be repeated by using another sequence of showering operations. If the stego content persists, then the image will be blocked.

The architecture of these processes

consists of two modules:

First module is to suppress the stego content. Irrespective of the steganographic algorithms, destruction techniques are applied on images to suppress the stego/noise and the resultant image is further subjected to different steganalysis techniques to verify that the image is stego free. Statistical steganalysis is integrated to estimate the percentage of stego content being removed. Suppression of stego content is done by applying radiometric and geometric operations. 27 different operations were applied on the image individually and in combination. These processes can suppress stego content in different proportions depending on steganographic algorithm and the domain where we applied the filters.

In the second module, the quality of the image is restored using variational deconvolution[3] so that the showered image approximates the original cover. Even though Wei Fan deconvolution techniques seem to work for all types of filtering, use of particular kernel for different filtering is likely to work better. To restore the quality of rotated images we have to find out a rotation kernel for deconvolution which will be our future work.

3.3 Effectiveness of Showering Process

It is necessary to assess the performance of showering techniques in three different aspects to get an accurate comparison

(i) Image quality metrics.
(ii) Quantity of stego data removed.
(iii) Processor time required to perform showering task.

In this paper we focused on the first two aspects.

Image quality metrics**:** PSNR[10] and SSIM[22] are used to assess the visual quality of the output image.

Metric for calculating the quantity of stego data removed: We use two metrics to calculate the quantity of stego removed at different payload and hence to evaluate performance of our proposed system.

- Bit Error Rate: This metric is designed to capture bit by bit error in the extracted secret message with the original secret image.
- First order Markov feature: This proposed Markov feature set gives percentage of stego content removed. The feature calculation starts by forming the matrix along four directions: horizontal, vertical, diagonal and minor diagonal (further denoted as *H* (*i*, *j*), *V* (*i*, *j*), *D* (*i*, *j*), *MD* (*i*, *j*), respectively).

Let the secret image be $I_1 = [x_{ij}]$ *where* $1 \le i \le M$, $1 \le j \le N$ and the secret image extracted from restored image be $I_2 = [y_{ij}]$ where $1 \le i \le M$, $1 \le j \le N$.

Four matrices are constructed as follows:

$$H(i, j) = [\partial(x_{ij}, y_{ij}) \,\&\&\, \partial(x_{ij+1}, y_{ij+`1})]$$

where $1 \le i \le M$, $1 \le j \le N-1$

$$V(i, j) = [\partial(x_{ij}, y_{ij}) \,\&\&\, \partial(x_{i+1j}, y_{i+1,j})]$$

where $1 \le i \le M-1$, $1 \le j \le N$

$$D(i, j) = [\partial(x_{ij}, y_{ij}) \,\&\&\, \partial(x_{i+1j+1}, y_{i+1j+1})]$$

where $1 \le i \le M-1$, $1 \le j \le N-1$

$$MD(i, j) = [\partial(x_{i+1j}, y_{i+1j}) \,\&\&\, \partial(x_{ij+1}, y_{ij+1})]$$

where $1 \le i \le M-1$, $1 \le j \le N-1$, where && is the logical operator AND.

We define delta function as

$$\partial(x, y) = 0 \quad \begin{cases} if & x = y \\ else & 1 \end{cases}$$

The above matrices will represent the count giving the number of non-equal adjacent pixels from which we can calculate the percentage of stego content removed. This method is found to be more accurate than BER. The above four matrices can be derived from both spatial and transform domains.

4. EXPERIMENTAL RESULTS

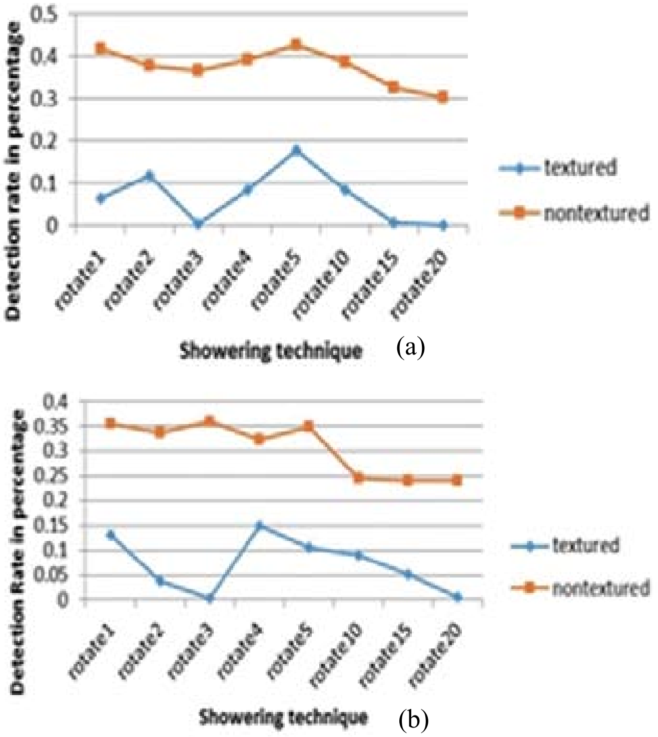
Our database contains 131 textured and non-textured images of size 256 x 256 taken from the USC–SIPI database[23]. All the 131 images were subjected to stego embedding at 1%, 5%, 10%, 30%, 50%, 70%, and 100% of image size using following spatial and transform domain stego algorithms: Random LSB embedding, +/-1 LSB embedding (or LSB matching), Pixel Value Differencing (PVD), OutGuess and Wavelet based steganography.

4.1 Results Obtained for Images Embedded using Spatial Domain Steganography

Initially all spatial domain stego images were subjected to different steganalysis. Only some of these images could give the correct estimate of stego content using these steganalysis methods. Since we are going to use the same steganalysis methods to evaluate the effectiveness of our algorithm, we selected only those images as test images which gave correct result for steganalysis. The showering techniques were applied followed by variational deconvolution. All the output images have been subjected to targeted steganalysis techniques like RS, Difference histogram, Chi-Square attack, PoV's. The size of the payload before and after applying our techniques was calculated. Figure 2 shows that after restoring the quality of rotated stego image of different payloads, the stego content destroyed is almost proportional. The ratio of loss from 100 per cent and 70 per cent is almost constant for each image. *i.e.* when an image loses *x* % for a payload of 100 we can predict how much it will lose for other payloads of 70 to 50. When the payload decreases below 30 we could not get such a pattern. We have noticed that irrespective of embedding rate and type of embedding, rotation above five degree could remove the stego content to a large extent.

In case of median filter the stego content removed is directly proportional to increase in window size. Figure 3 shows the effect of showering using different filters on textured and non-textured images of 100 per cent and 70 per cent payload using Random LSB. We can see from Fig. 3 that by applying median filter, Gaussian filter and combination filter 5 detection rate is low for textured image which implies quantity of stego removed is high. For non-textured images the detection rate is low after applying Wiener filter, combination filter 1, 2, and 3. The result was found to be true irrespective of all payloads. We have applied variational deconvolution method on these images to restore the quality of the source image for further use.

Fan[3], *et al.* explained variational deconvolution has been applied on median filtered images to restore the quality of the



(a)

(b)

Figure 2. The detection rate using RS steganalysis after undergoing various degrees of rotation for textured and non-textured images (a) 100 per cent embedded and (b) 70 per cent embedded using Random LSB.

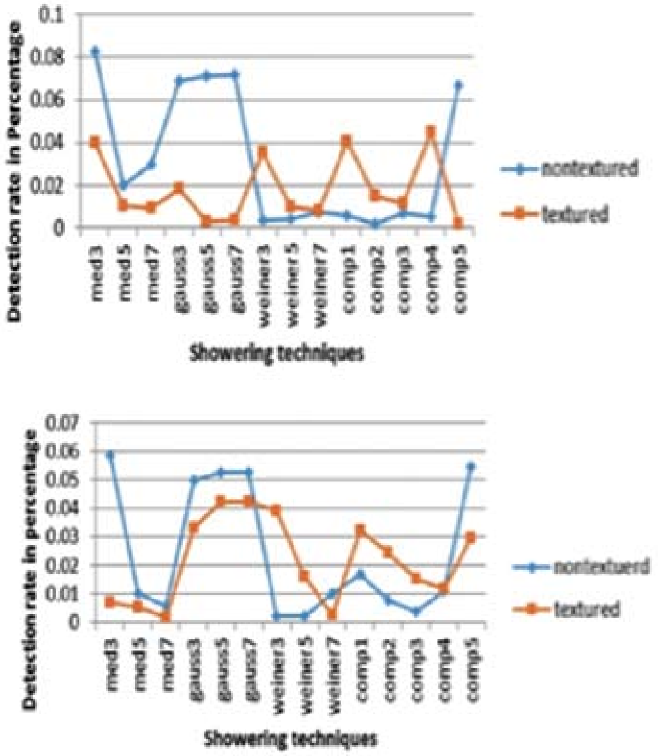


Figure 3. The detection rate using RS steganalysis after undergoing selected showering techniques for textured and non-textured images (a) 100 per cent embedded and (b) 70 per cent embedded using Random LSB.

image after filtering. For restoring the quality of the rotated image, kernel given in^3 did not show any satisfactory result. So we have to find a rotation kernel to increase the quality of images which had undergone geometric distortion. By using Gaussian filter, median filter or wiener filter to destroy the stego content we noticed that these filters not only maintain the PSNR level but also the structural information of the image is preserved which is measured using SSIM. As shown in Fig. 5.

We can observe from Fig. 4 that difference image histogram steganalysis also show same behaviour as RS steganalysis in

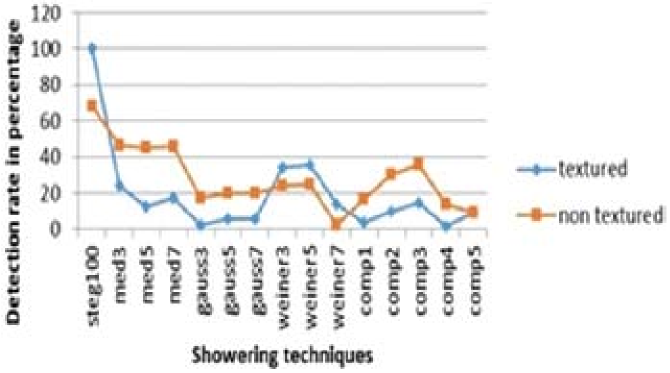
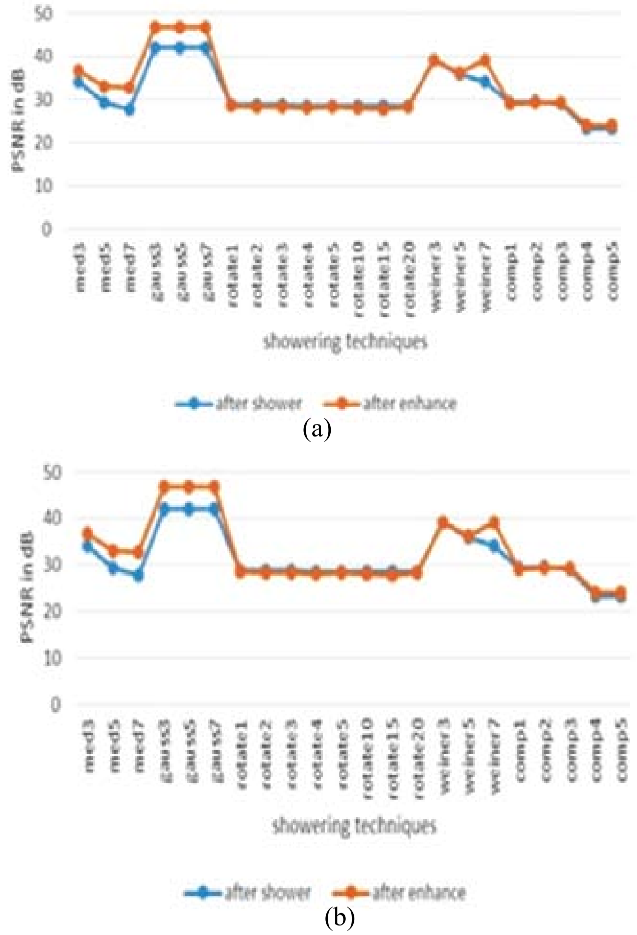


Figure 4. The detection rate using difference image histogram steganalysis for showered image after undergoes different filters for textured and non-textured images.



(a)

(b)

Figure 5. Image quality measured using (a) PSNR and (b) SSIM for evaluating performance of the system.

selecting the showering techniques to destroy stego content *ie*. median and Gaussian is best for textured while Wiener and combination filter 5 are good choices for non-textured images.

Figure 6 shows the detection rate by RS steganalysis obtained after applying showering techniques to 100 per cent embedded stego image created using PVD based Steganography. We found that our technique could suppress the stego content to 92 per cent. Eight percent of the stego content remained in the stego image will not be sufficient to recover the secret message. We have verified the stego content removal against 70%, 50%, 30%, 10%, 5%, and 1% embedded stego images by applying showering process. For all payloads stego content was suppressed to 92 per cent of the stego embedded. In terms of quality, result showed that if we apply median filter, Gaussian filter and wiener filter, the stego content was removed to large extent still preserving the quality of the source image above 30 dB. Even though combination filters could remove stego content to large extent than Gaussian and median filters the image quality was reduced below 30 dB.

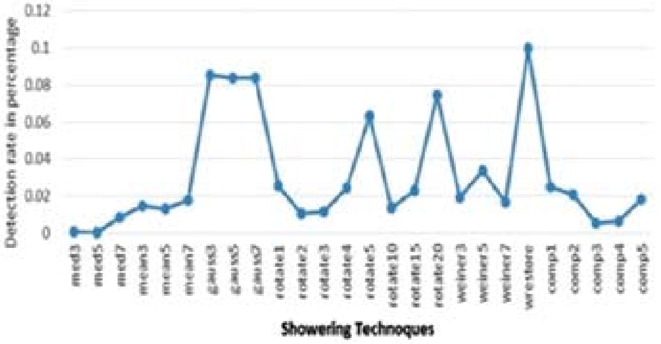


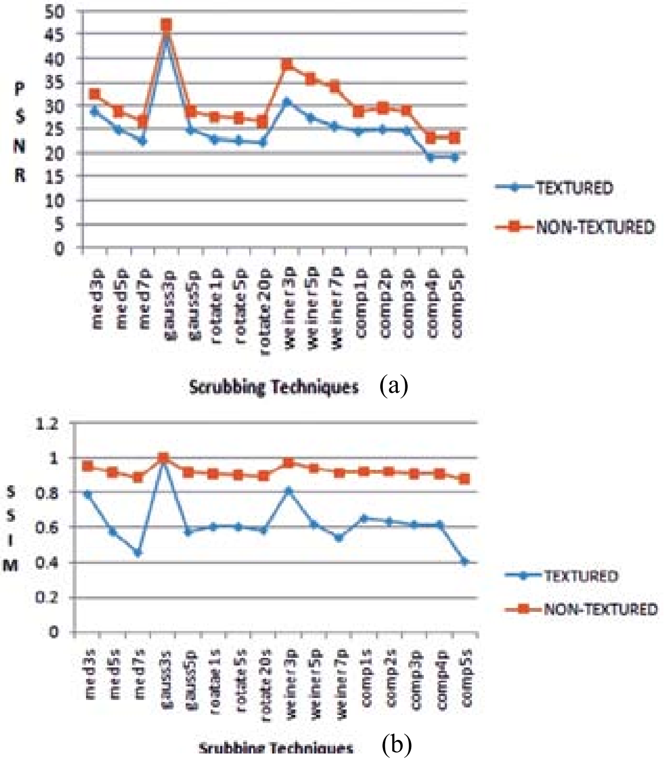
Figure 6. The detection rate using RS steganalysis after undergoing selected showering techniques.

4.2 Results Obtained for Images Embedded using Transform Domain Steganography

Showering techniques were applied on JPEG images with payloads ranging from 10 to 100% of non-zero quantised DCT coefficients. On the degraded image variational deconvolution technique was applied. Then the stego content was tried to be extracted from the DCT coefficients. It was found that the stego content got completely removed. The results obtained are given in Fig. 7. Here Fig. 7(a) and 7(b) are the textured and non-textured stego images obtained using Outguess by embedding the secret image 7(c). On applying Gaussian filter on 7(a) and 7(b) the secret has been completely destroyed. Fig. 7(d) and 7(e) are the restored images after variational deconvolution and Figs. 7(f) and 7(g) are the extracted secret from the nonzero quantised DCT coefficients.

From these results, we can conclude that for textured images, the stego content can be completely suppressed by applying Gaussian and Wiener filters while maintaining the quality of source image above 30 dB; this was not possible with other filters. For non-textured images, Median, Gaussian and Wiener filters gave good results. The results are shown in the Fig. 8 (a) and 8 (b).

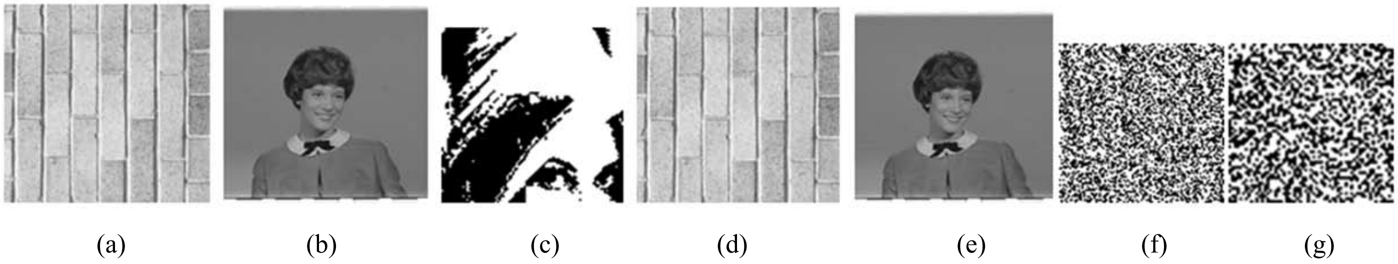
In the case of stego content embedded using wavelet steganography, we have seen that secret message was completely destroyed when we tried to extract it from the wavelet coefficients of the restored image. For textured images, Gaussian and Wiener filter could destroy stego content more by maintaining the PSNR above 35 dB and for non-textured images, Median, Gaussian and Weiner filter were able to destroy the stego content completely with PSNR above 30 dB



(a)

(b)

Figure 8. Quality of the restored image measured using (a) PSNR and (b) SSIM value after the scrubbing technique is applied on stego image.



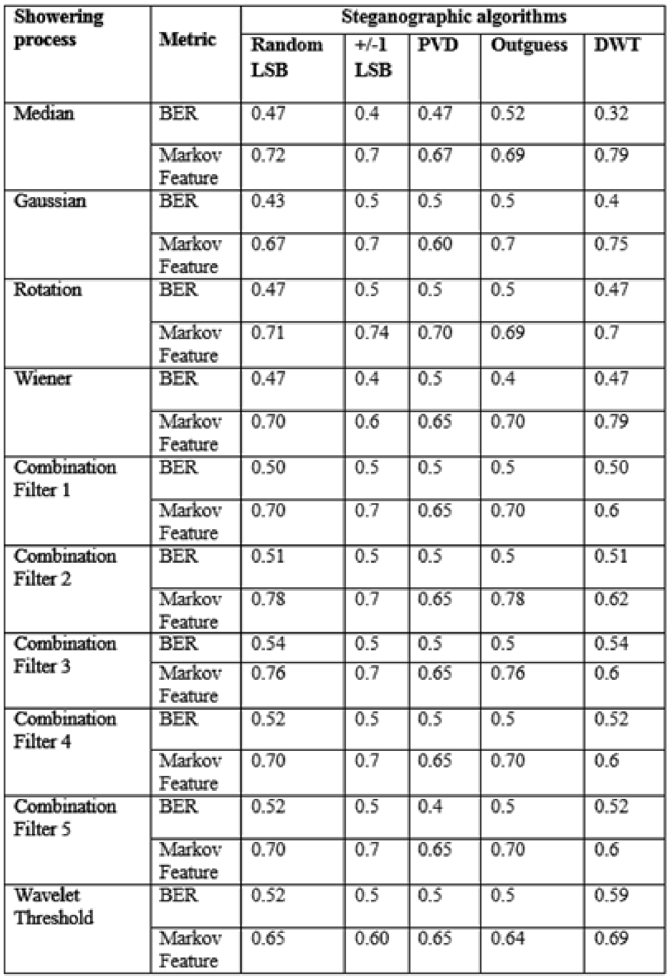
(a) (b) (c) (d) (e) (f) (g)

Figure 7. Textured and non-textured stego images ((a) and (b)), secret (c), the restored images ((d) and (e)) and the extracted secrets ((f) and (g)).

and SSIM was between 0.67-0.99.

A stego image which got embedded in the BMP domain gets transmitted as a JPEG file. The received JPEG file is converted to a BMP format and showering is applied. This effectively removes the stego content. The subsequent conversion of this BMP file into a JPEG format will further contribute to the obfuscation of any residual stego content. BER and First order Markov features are used for calculating the quantity of stego removed from the restored image and the results are presented in Table 2. Among the total of 27 showering operations we have taken, only the ones which destroyed the stego content and whose image quality could be restored are shown in the graph. It can be observed that first order Markov feature is better than BER in terms of measuring the stego removal. Result can be further improved if we use second or third order Markov features.

Table 2. Results of showering process applied on the stego images with message length of 30 K bits



Showering process	Metric	Steganographic algorithms				
		Random LSB	+/-1 LSB	PVD	Outguess	DWT
Median	BER	0.47	0.4	0.47	0.52	0.32
	Markov Feature	0.72	0.7	0.67	0.69	0.79
Gaussian	BER	0.43	0.5	0.5	0.5	0.4
	Markov Feature	0.67	0.7	0.60	0.7	0.75
Rotation	BER	0.47	0.5	0.5	0.5	0.47
	Markov Feature	0.71	0.74	0.70	0.69	0.7
Wiener	BER	0.47	0.4	0.5	0.4	0.47
	Markov Feature	0.70	0.6	0.65	0.70	0.79
Combination Filter 1	BER	0.50	0.5	0.5	0.5	0.50
	Markov Feature	0.70	0.7	0.65	0.70	0.6
Combination Filter 2	BER	0.51	0.5	0.5	0.5	0.51
	Markov Feature	0.78	0.7	0.65	0.78	0.62
Combination Filter 3	BER	0.54	0.5	0.5	0.5	0.54
	Markov Feature	0.76	0.7	0.65	0.76	0.6
Combination Filter 4	BER	0.52	0.5	0.5	0.5	0.52
	Markov Feature	0.70	0.7	0.65	0.70	0.6
Combination Filter 5	BER	0.52	0.5	0.4	0.5	0.52
	Markov Feature	0.70	0.7	0.65	0.70	0.6
Wavelet Threshold	BER	0.52	0.5	0.5	0.5	0.59
	Markov Feature	0.65	0.60	0.65	0.64	0.69

5. CONCLUSIONS AND FUTURE WORK

A combination of showering and restoration techniques applied in sequence provides an effective attack on hidden data, but with varying degrees of success regarding the preservation of the image quality. For textured images with different payloads embedded with spatial domain steganography, good results were attained in removing stego content using Median, Gaussian, combination filter 5 and rotation. On the other hand, Wiener and combination filters 1, 2, 3 and 4 do the same for non-textured images. For images with different payloads embedded in transform domain, Gaussian and Wiener filters were able to destroy stego content completely while preserving the PSNR above 30 dB. Even though other filters could completely remove stego content, they failed in preserving the PSNR above 30 dB. Steganalysis also confirms the performance of our showering techniques in terms of stego removal. We have verified that our techniques work well for all the spatial and transform domain steganographic algorithms. First order Markov feature gave better results than BER. Correlation of image properties with filtering methods and with order dependency of combination filters need to be understood. The extension of the above methods to multimedia needs to be further studied.

REFERENCES

1. Brickell, E.F. &. Odlyzko, A.M. Cryptanalysis: A survey of recent results. *IEEE Proceedings*, 1988, **76**(5), 578-593. doi:10.1109/5.4443
2. Chandramouli, R.; Kharrazi, M. & Memon, N. Image steganography and steganalysis: Concepts and practice. *In* International Workshop on Digital Watermarking. Springer Berlin Heidelberg, 2003, 35-49. doi:10.1007/978-3-540-24624-4_3
3. Fan, W.; Wang, K.; Cayre, F. & Xiong Z. Median filtered image quality enhancement and anti-forensics via variational deconvolution. *In* IEEE Transactions on Information Forensics and Security, 2015, **10**(5), 1076-1091. doi: 10.1109/TIFS.2015.2398362
4. Westfeld, A. & Pfitzmann, A. Attacks on steganographic systems. *In* Information Hiding, Springer Berlin Heidelberg, 2000, 61-76. doi: 10.1007/10719724_5
5. Petitcolas, F.A.; Anderson, R.J. & Kuhn, M.G. Attacks on copyright marking systems. *In* Information Hiding, Springer Berlin Heidelberg, 1998, 218-238. doi: 10.1007/3-540-49380-8_16
6. Fisk, G.; Fisk, M.; Papadopoulos, C. & Neil, J. Eliminating steganography in Internet traffic with active wardens. *In* Information Hiding, Springer Berlin Heidelberg, 2002, pp. 18-35. doi : 10.1007/3-540-36415-3_2
7. Sieffert, M.; Forbes, R.; Green, C.; Popyack, L. & Blake, T. Stego intrusion detection system. *In* Proceedings of the Fourth Digital Forensic Research Workshop, 2004.
8. Al-Naima, F.; Ameen, S.Y. & Al-Saad, A.F. Destroying steganography content in image files. *In* the 5th International Symposium on Communication Systems, Networks and DSP, Greece, 2006.
9. Smith, C.B. & Agaian, S.S. Denoising and the active warden. *In* IEEE International Conference on Systems, Man and Cybernetics, 2007, 3317-3322. doi :10.1109/ICSMC.2007.4413746
10. Lafferty, P. A. Obfuscation and the steganographic active warden model. The Catholic University of America, 2008, PhD Thesis.
11. Nutzinger, M. Real-time attacks on audio steganography. *J. Info. Hiding Multimedia Signal Proc.*, 2012, **3**(1), 47-65.

12. Qilin, Q. A study on countermeasures against steganography: An Active Warden Approach. University of Nebraska, 2013, PhD Thesis.
13. Ameen, S.Y. & Al-Badrany, M.R. Optimal image steganography content destruction techniques. *In* International Conference on Systems, Control, Signal Processing and Informatics, 2013.
14. Smith, C.B. & Agaian, S.S. On noise, steganography, and the active warden. *In* Multimedia Forensics and Security, *Edited by* Li, Chang-Tsun. Information Science Reference, 2008. pp. 139-162.
15. Smith, C.B. & Agaian, S.S. On steganalysis and clean Image Estimation. *In* Multimedia Forensics and Security, *Edited by* Li, Chang-Tsun. Information Science Reference, 2008. pp. 212-243.
16. Egan, J.P. Signal detection theory and ROC analysis. New York: Academic press, 1975.
17. Ker, A.D. Steganalysis of LSB matching in grayscale images. *IEEE Signal Processing Letters*, 2005, **12**(6), 441- 444. doi: 10.1109/LSP.2005.847889
18. Almeida, C.W.; De Souza, R.M. & Candeias, A.L.B. Texture classification based on co-occurrence matrix and self-organizing map. *In* International Conference on, Systems Man and Cybernetics, 2010, pp. 2487-2491. doi: 10.1109/ICSMC.2010.5641934
19. Fridrich, J. & Goljan, M. Practical steganalysis of digital images: state of the art. *In* Electronic Imaging. International Society for Optics and Photonics, 2002, **4**(1), 1-13. doi: 10.1117/12.465263
20. Stanley, C.A. Pairs of values and the chi-squared attack. Iowa State University, 2005. Master's Thesis.
21. Zhang, T. & Ping, X. Reliable detection of LSB steganography based on the difference image histogram. *In* International Journal Acoustics, Speech, and Signal Processing, 2003. doi: 10.1109/ICASSP.2003.1199532
22. Wang, Z.; Simoncelli, E.P. & A.C. Bovik. Multiscale structural similarity for image quality assessment. *In* Signals, Systems and Computers, Asilomar Conference, 2004, 1398-1402. doi: 10.1109/ACSSC.2003.1292216
23. Weber, G. The USC-SIPI Image Database Version 5, USC-SIPI Report #315, 1997.

CONTRIBUTORS

Ms Amritha P.P. received her MTech (Cyber Security) from Amrita University currently pursuing her PhD at Amrita University. Her current research interests include: Steganography and code obfuscation.
In the current study, she performed the literature review, experimental work and analysed the results.

Dr M. Sethumadhavan received his PhD (Number Theory) from Calicut Regional Engineering College. Currently, he is working as a Professor in the Department of Mathematics and Computer Science, Amrita Vishwa Vidyapeetham University, Coimbatore. His current research interests include: Crytography and Boolean functions
In the current study, he contributed in the coordination, provided mathematical analysis and data interpretation.

Dr R. Krishnan received his PhD from IISc, Bangalore. He is currently an Adjunct Professor in Amrita University. His current research interests include: Image processing and remote sensing.
In the current study, he conceived initial idea for the study and contributed in data interpretation.