Randomized Embedding Scheme Based on DCT Coefficients for Image Steganography

Ajit Danti
JNN College of Engineering, Shimoga, Karnataka, India

Preethi Acharya
JNN College of Engineering, Shimoga, Karnataka, India

ABSTRACT
Main goal of steganography is to communicate securely in a completely undetectable manner. It is an art of hiding secret data in an innocently looking dummy container. In the Steganographic process, communication is masked to make the hidden message not discernible to the observer. Hidden message may be textual or image. In this paper, a novel image steganography method based on randomized bit embedding is presented. Firstly the Discrete Cosine Transform (DCT) of the cover image is obtained. Then the stego image is constructed by hiding the given secrete message image in Least Significant Bit of the cover image in random locations based on threshold. DCT coefficients determine the randomized pixel locations for hiding to resist blind steganalysis methods such as self calibration process by cropping some pixels to estimate the cover image features. Blind steganalysis schemes can be guessed easily hence the proposed technique is more practically applicable. Quality of the stego image is analyzed by tradeoff between no of bits used for embedding. Efficacy of the proposed method is illustrated by exhaustive experimental results and comparisons.

General Terms
Security, Bit embedding, Hiding.

Keywords
Steganography, DCT (Discrete Cosine Transform), Image hiding, Randomization

1. INTRODUCTION
Steganography refers to the science of "invisible" communication. In the field of secure communication, Steganography, the art of communicating without revealing its existence, as well as *cryptography*, the art of concealing the meaning of a message, have a rich history. Information hiding is an interesting technology which includes watermarking and steganography etc. Steganography hides secret data in a dummy container. This container may be a digital still image, audio file, or video file. Steganography provides good security in itself and when combined with encryption becomes an extremely powerful security tool. In steganography, unlike other forms of communications, one's awareness of the underlying communication between the sender and receiver defeats the whole purpose. Therefore, the first requirement of a steganographic system is its undetectability. In other words, a steganographic system is considered to be insecure, if the third person is able to differentiate between cover image and stego image.

Steganography would provide an ultimate guarantee of authentication that no other security tool may ensure. S. Miaou et al. (2000) present an LSB embedding technique for electronic patient records based on bi-polar multiple-base data hiding. A pixel value difference between an original image and its JPEG version is taken to be a number conversion base. Nirinjan and Anand (1998) and Li et al. (2007) also discuss patient data concealment in digital images.

JPEG is arguably the most popular format for storing, presenting, and exchanging images. It is not surprising that steganography in the JPEG format, and its converse problem of steganalysis of JPEG images to find ones with hidden data, have received considerable attention from researchers over the past decade. There are many approaches and software available for JPEG steganography, which include OutGuess (Provos, N. 2001), StegHide (Hetz et. al, 2005), model-based steganography (Sallee P, 2004), perturbed quantization (Fridrich J. et., al, 2004), F5 (Westfeld A., 2001), and statistical restoration (Solanki K. et., al, 2005 and 2006).

There have been various approaches in defining and evaluating the security of a steganographic system. Zollner et al. (1998) were among the first to address the undetectability aspect of steganographical systems. They provide an analysis to show that information theoretically secure steganography is possible if embedding operation has a random nature and the embedded message is independent from both the cover-image and stego-image. These conditions, however, ensure undetectability against an attacker who knows the stego- image but has no information available about the indeterministic embedding operation. That is, attacker has no access to the statistics, distribution, or conditional distribution of the cover- image.

One of the earliest methods to discuss digital steganography is credited to Kurak and McHugh (1992), who proposed a method which resembles embedding into the 4 LSBs (least significant bits). They examined image downgrading and contamination which is known as image-based steganography.

Many steganalysis schemes (Wang, Y. et., al, 2003 and Pevny, T. et., al, 2006 and 2007) have been able to successfully detect the above steganographic techniques that match marginal statistics or models. They exploit the fact that higher order statistics get modified by data hiding using these stego methods. It is known that, the higher order statistics, in general, are difficult to match, model, or restore. Recently, blind steganalysis algorithms (Pevny, T. et., al, 2006 ,2007 and Avcibas, I. et., al, 2002 and Lyu, S. et., al, 1974 and Harmsen, J.J. et., al, 2003 and Shi, Y.Q. et., al, 2007 and Dabeer, O. et., al, 2004) have been proposed that employ supervised learning to distinguish between the plain cover and stego images, and also identify the particular hiding algorithm used for steganography. These techniques bank on the fact that there are some image *features*

that are modified during the embedding process which can be used as an input to the learning machine.

The DCT transforms a signal or image from the spatial domain to the frequency domain. It separates the image into parts (or spectral sub-bands) of differing importance (with respect to the image's visual quality). It can separate the image into High, Middle and Low frequency components. In order to avoid inducing significant perceptual distortion in the image, most methods avoid hiding in DCT coefficients whose value is 0. To detect the presence of data embedded in this manner, steganalysis algorithms exploit the fact that the DCT coefficient histogram gets modified when hiding random information bits. Hence recently proposed steganographic approaches attempt to match as closely as possible, the original DCT histogram or its model. Westfield's F5 (2001) algorithm increases, decreases, or keeps unchanged the coefficient value based on the data bit to be hidden, so as to better match the host statistics. Provos's OutGuess (2001) was the first attempt in explicitly matching the DCT histogram. Sallee P (2004) proposed a model based approach for steganography, wherein the DCT coefficients were modified to hide data such that they follow an underlying model. Fridrich et al's (2004) perturbed quantization attempts to resemble the statistics of a double-compressed image. Statistical restoration method proposed by Solanki et al (2005), can match the DCT histograms exactly, thus providing provable security so long as only the marginal statistics are used by the steganalyst.

In spite of the absence of good universal models, recent steganalysis algorithms have been very successful by using a *self-calibration* method to approximate the statistics of the original cover (Pevny and Fridrich, 2007, and Dabeer et al., 2004). The calibration method typically used for JPEG steganography is quite simple; a few pixel rows and/or columns are cropped from the image so as to desynchronize it from the original JPEG grid and the resulting image is compressed again, which forms a good approximation of the cover image. The results reported in Pevny and Fridrich (2007), the most recent multi-class JPEG steganalysis method that employs such self-calibration, are close to perfect: the steganalyst can determine one out of 6 stego algorithms employed for hiding with a detection accuracy of more than 95% in most cases, even at low embedding rates.

In this paper, randomized steganographic scheme is presented, this method devised for secure and active steganography that can effectively resist blind steganalysis methods. The proposed technique is based on simple idea of hiding data in random locations in an image which makes self calibration process difficult. Proposed approach is robust and untraceable for many of the embedding algorithms, such as OutGuess (Provos, N. 2001) and StegHide (Hetz et al, 2005) (are detectable due to absence of randomization). Least Significant Bit (LSB) insertion is a common approach to embedding information in an image. Taking advantage of the way the human eye perceives images, this technique involves replacing the N least significant bits of each pixel of a container or cover image with the data of a hidden message image. Blind statistical steganalysis schemes use a supervised learning technique on *features* derived from plain cover as well as stego signals. This class of methods has been very successful in detecting steganographic methods available today. For example, detection results presented in (Pevny, T. et., all, 2007) and also our own experiments indicate that popular JPEG steganographic schemes such as OutGuess (Provos, N. 2001), StegHide (Hetz et al, 2005) , model-based steganography (Sallee P, 2004), and 1D statistical restoration schemes (Solanki K. et., al, 2005 and 2006) can be successfully detected. Self-calibration mechanism is used by the blind steganalysis schemes to estimate the statistics of the cover image from the stego image. For JPEG steganography, this is typically achieved by decompressing the stego image to the spatial domain followed by cropping the image by a few pixels on each side and compressing the image again using the same compression parameters.

2. PROPOSED APPROACH

Steganographic technique consists of an embedding algorithm and a detector function as shown in Fig 1. The embedding algorithm is used to hide secret messages inside a cover (or carrier) document within its steganographic capacity. Steganographic capacity refers to the maximum amount (rate) of information that can be embedded into a cover- image and then can be reliably recovered from the stego-image (or a distorted version), under the constraints of undetectability, perceptual intactness and robustness, depending on whether attacker is active or passive. Compared to data hiding systems, stegosystems have the added core requirement of undetectability. Therefore, the steganographic embedding operation needs to preserve the statistical properties of the cover- image, in addition to its perceptual quality. On the other hand, if attacker suspects of a covert communication but cannot reliably make a decision, he may choose to modify the stego-image before delivering it.

The embedding process is usually protected by a keyword so that only those who posses the secret keyword can access the hidden message. The detector function is applied to the carrier and returns the hidden secret message. For secure covert communication, it is important that by injecting a secret message into a carrier document no *detectable changes* are introduced. The main goal is to not raise suspicion and avoid introducing statistically detectable modifications into the carrier document.

2.1 Randomized Embedding

In this section, we present a steganography scheme that embeds secrete message image in the least significant bits of randomly chosen locations. Proposed algorithm hides the secret message in least significant bits of the pixels at random positions in the cover image. If the message is simply hidden in least significant bits of the consecutive pixels, hackers can easily extract the bits by trial and error to get the original hidden message image. This randomization is expected to increase the security of the system and makes guessing difficult. Commonly used randomization in selecting the pixels are - selecting all even pixels for hiding, selecting all odd pixels for hiding or select 10^{th}, 20^{th} ……100^{th} pixels etc. These are obviously good but chances of guessing are more. The randomization approach proposed in this paper places itself far from these guesses.

In the proposed method Discrete Cosine Transform (DCT) is applied to the given cover image to get the DCT coefficients. The pixels having the DCT coefficients lower than the threshold value are only considered for embedding the secrete message image. The threshold value is empirically determined from the set of cover images. In our experiments, threshold is set to zero

for illustration. The pixels in the cover image satisfying the threshold condition are not in consecutive locations instead pixel locations are random throughout the cover image. These random pixels are called *potential pixels*.

This randomization can easily resist any blind steganalysis methods. Once the *potential pixels* are found, message image can be easily embedded. In embedding process, 5 most significant bits of each pixel of message image is hidden at the 5 least significant bits of the *potential pixels* in one-to-one correspondence.

2.2 Recovery of original Message Image

Recovery process needs stego image and the key which is shared between sender and the receiver. The key contains locations of *potential pixels*. At the receiver end, based on the key we can find the locations of the potential pixels of the stego image in which message image is hidden. Then extract 5 least significant bits from each pixel in those locations, which gives the hidden message image. The detailed algorithm is given below.

2.3 Stego Algorithm:

1. Select a suitable cover image to hide the given message image such that the size of the cover image should satisfy the following condition

$n>2m$	[1]

where n is the number of pixels in the cover image, m is the number of pixels in the message image.

2. Compute the 2D DCT coefficients for each pixel of the cover image using the equation,

$$DCT_{ij} = \alpha_i \alpha_j \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} C_{mn} \cos \frac{\pi(2m+1)i}{2M} \cos \frac{\pi(2n+1)j}{2N}, \quad 0 \le i \le M-1, \quad 0 \le j \le N-1 \qquad [2]$$

Where,

$$\alpha_i = \begin{cases} 1/\sqrt{M}, & i = 0 \\ \sqrt{2/M}, & 1 \le i \le M-1 \end{cases} \qquad \alpha_j = \begin{cases} 1/\sqrt{N}, & j = 0 \\ \sqrt{2/N}, & 1 \le j \le N-1 \end{cases}$$

Where DCT denote discrete cosine transformation image C denote the Cover image

3. Determine the random locations of the *potential pixels* whose DCT coefficient is less than threshold *t*. (For better illustrations we have used *t=0*)

4. Construct a key vector consist of total number of *potential pixels* for hiding message image and their locations.

5. Replace 5 least significant bits of *potential pixels* of cover image with 5 most significant bits of message image to get *stego image*.

2.4 Recovery Algorithm

1. Transmit the key vector constructed by the above stego algorithm to the receiver by the secured channel.
2. Transmit the stego image to the receiver over the network.
3. Recover the *potential pixels* from the received stego image using the locations determined by the key vector.
4. Extract the 5 least significant bits of each potential pixel of the stego image to get the hidden message image.

3. EXPERIMENTAL RESULTS

We conduct a comprehensive set of experiments and present the results demonstrating the applicability of the presented approach. First, the results for the embedding capacity are presented for some standard sample images as given below.

3.1 Embedding Scheme:

In Table 1 we list the number of locations available in different standard images based on different threshold values (*t*). Threshold is defined based on the DCT values. First we should find the 2D DCT for the given cover image then based on the predefined threshold find the total number of locations available. Consider the number of locations of the potential pixels just enough to accommodate all pixels of message image to be hidden.

Threshold *t* is determined empirically based on given set of cover images. In our experiments we use threshold value as zero for illustration. Experimental results are shown in Fig. 4, Fig. 5, Fig. 6 & Fig.7.

Threshold	No of Pixels Locations in the cover image			
	Cover1	Cover2	Cover3	Cover4
t<0	19900	19800	20000	20000
t<1	22300	22900	21200	21500
3<t<200	13200	12000	16400	15400
5<t<300	10000	8800	14400	13000

Table.1 Number of locations available to hide the message image.

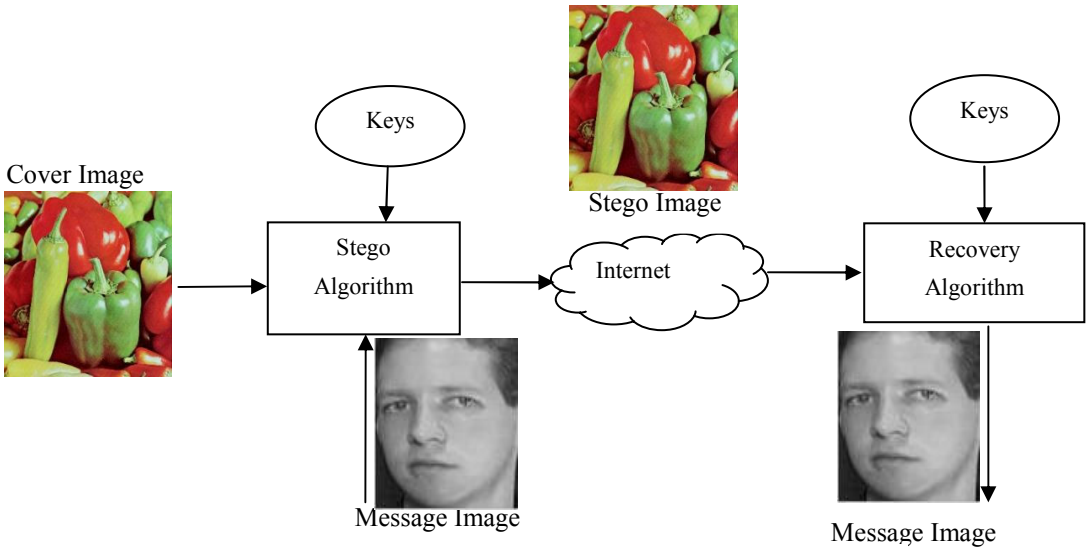


Fig.1 Block Diagram of the Proposed Approach

Fig.2 Sample Cover Images: Cover1, Cover2, Cover3 and Cover4

Fig.3. Sample Message Images: Message1, Message2 and Message3 and Message4

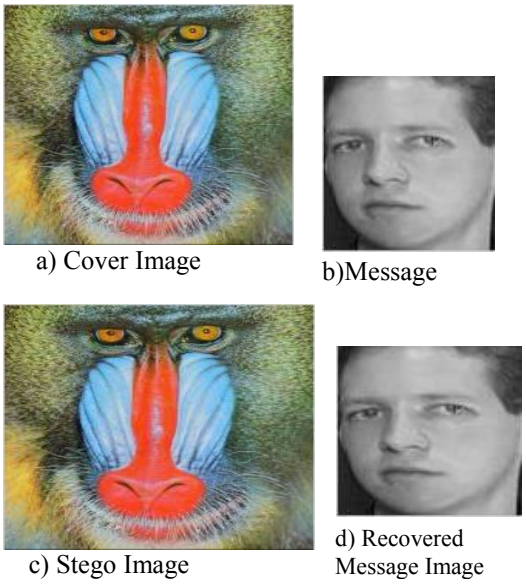


Fig.4 The stego image is constructed by hiding a message image in the cover image.

Fig. 5) The stego image is constructed by hiding a message image in the cover image.

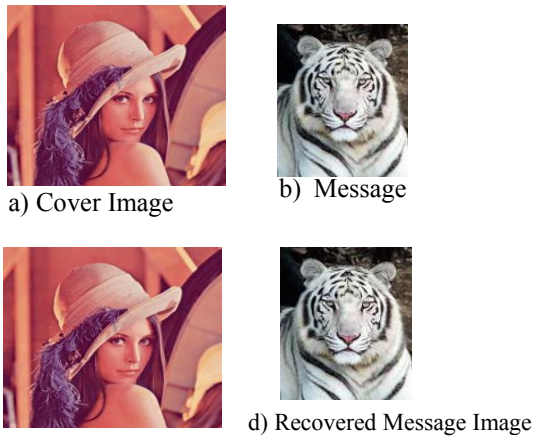


Fig.6 The stego image is constructed by hiding the message image in the cover image.

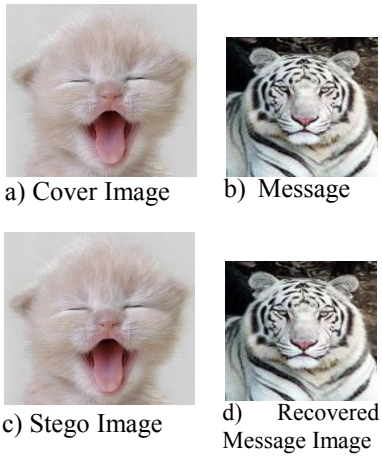


Fig.7 The stego image is constructed by hiding the message image in the cover image.

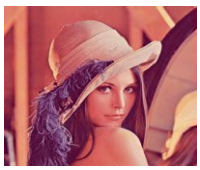
Bits	Different message images			
	Message1	Message2	Message3	Message4
3	e=0.1872	0.1376	0.2106	0.1506
4	e=0.0890	0.0955	0.1828	0.1018
5	e=0.0420	0.0822	0.1743	0.0868
6	e=0.0186	0.0785	0.1723	0.0837

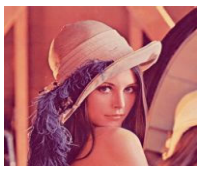
Table 2. Errors in recovered message image using varying number of bits for embedding


a) Cover Image


b) Message Image

Stego Images


c) 3 bit embedding (error e=0.1872)


d) 4 bit embedding (error e= 0.0890)


e) 5 bit embedding (error e= 0.0420)


f) 6 bit embedding (error e=0.0186)

Fig. 8 Experimental results showing the stego image constructed by varying number of bits embedding and errors.

4. STEGO ERROR ANALYSIS

The efficiency of the proposed method is measured by the difference error between the message image and the recovered message image using the equation 3. Efficiency of the sample extracted message images are determined based on error and number of bits used. Table 2 shows the errors obtained with varying number of bits for embedding.

$$error\ e = \frac{\sqrt{\sum_{j=1}^{M_c}\sum_{i=1}^{M_{rr}}(x(i,j)-y(i,j))^2}}{rxc} \quad [3]$$

Where,

x: Given message image

y: Extracted message image

r: Number of rows in message image

c: Number of columns in message image

In the Fig.8, sample experimental results are shown by varying the number of bits for embedding message image in the given cover image. Error increases with the less number of bits used. Similarly error decreases with more number of bits used in the embedding process. Higher error introduces more distortion in the stego image. In this paper, 5 bits are used for embedding for better stego mage analysis by tradeoff between no of bits and the minimum error. Hence use of more number of bits for hiding message in the cover image results in minimum errors in the stego image but the stego image looks suspicious which may attract the attention of the hackers. This may leads to failure of the whole purpose. Errors can be minimized by trade off between optimum number of bits for hiding and error to get the innocent stego image.

In the Fig 9, stego image errors are plotted against the number of bits used for embedding to demonstrate the relation between bits and the error in the stego image.

5. CONCLUSIONS

In this paper a new steganographic technique is proposed for embedding images in the least significant bits, supported for JPEG and BMP image formats. This technique embeds MSBs (5-Most significant bits) of the message image in the LSBs (5-Least significant bits) of the cover image based on the randomly selected locations determined by DCT coefficients and a predetermined threshold. The randomization that we apply based on threshold makes this scheme more stronger and secured. The proposed scheme can resist blind steganalysis schemes effectively.

The proposed method is experimented and efficacy of the approach is demonstrated. Stego images are analyzed by varying the number of bits for embedding with their efficiency and errors. In the future, the security of the proposed scheme can be further improved by employing compression and encryption techniques. Randomization can be further enhanced by probabilistic weighted bits for embedding the message image.

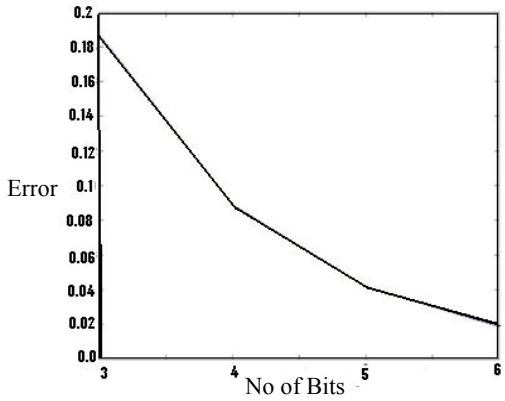


Fig. 9 Errors with respect to varying no of bits used for embedding

6. ACKNOWLEDGMENTS

The authors are thankful to Dr. P. Nagabushan, Dr. P. S. Hiremath, Dr. B. V. Dhandra & Dr. Mallikarjun Hangarge for their constant support and encouragement during this work.

7. REFERENCES

[1] Avcibas, I., Sankur, B., Memon, N.: Image steganalysis with binary similarity measures. In: Proc. ICIP, pp. 645–648 (2002)

[2] C. Kurak and J. McHugh, a cautionary note on image downgrading, in:Proceedings of the IEEE 8th Annual Computer Security Applications Conference, 30 Nov-4 Dec, 1992, pp. 153-159.

[3] Dabeer, O., Sullivan, K., Madhow, U., Chandrasekaran, S., Manjunath, B.: Detection of hiding in the least significant bit. IEEE Transactions on Signal Processing, Supplement on Secure Media I 52, 3046–3058 (2004)

[4] Fridrich, J., Goljan, M., Lison˘ek, P., Soukal, D.: Writing on wet paper. In: ACM Workshop on Multimedia and security, Magdeburg, Germany (2004)

[5] Harmsen, J.J., Pearlman, W.A.: Steganalysis of additive noise modelable information hiding. In: Proc. of SPIE, pp. 131–142 (2003)

[6] Hetzl, S., Mutzel, P.: A graph theoretic approach to steganography. In: 9th IFIP TC-6 TC-11 International Conference, Communications and Multimedia Security, Salzburg, Austria, vol. 3677, pp. 119–128 (2005)

[7] Lyu, S., Farid, H.: Detecting hidden messages using higher-order statistics and support vector machines. In: Ershov, A.P., Nepomniaschy, V.A. (eds.) International Symposium on Theoretical Programming. LNCS, vol. 5, Springer, Heidelberg (1974)

[8] Pevny, T., Fridrich, J.: Multi-class blind steganalysis for JPEG images. In: Proc. of SPIE, San Jose, CA (2006)

[9] Pevny, T., Fridrich, J.: Merging Markov and DCT features for multi-class JPEG steganalysis. In: Proc. of SPIE, San Jose, CA (2007)

[10] Provos, N.: Defending against statistical steganalysis. In: 10th USENIX Security Symposium, Washington DC, USA (2001) of the IEEE 22nd Annual EMBS International Conference, July 23-28, 2000, Chicago, USA, pp. 280-283.

[11] S. Miaou, C. Hsu, Y. Tsai and H. Chao, A secure data hiding technique with heterogeneous data-combining capability for electronic patient records, in: Proceedin

[12] Sallee, P.: Model-based steganography. In: Kalker, T., Cox, I., Ro, Y.M. (eds.) IWDW 2003. LNCS, vol. 2939, pp. 154–167. Springer, Heidelberg (2004)

[13] Shi, Y.Q., Chen, C., Chen, W.: A Markov process based approach to effective attacking JPEG steganography. In: Leilich, H.-O. (ed.) GI-NTG Fachtagung Struktur und Betrieb von Rechensystemen. LNCS, Springer, Heidelberg (1974)

[14] Solanki, K., Sullivan, K., Madhow, U., Manjunath, B.S., Chandrasekaran, S.: Statistical restoration for robust and secure steganography. In: Proc. ICIP, Genova, Italy, pp. II 1118–1121 (2005)

[15] Solanki, K., Sullivan, K., Madhow, U., Manjunath, B.S., Chandrasekaran, S.: Probably secure steganography: Achieving zero K-L divergence using statistical restoration. In: Proc. ICIP, Atlanta, GA, USA, pp. 125–128 (2006)

[16] U. C. Nirinjan and D. Anand, Watermarking medical images with patient information, in:Proceeding of the 20th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, Hong Kong, China, 29 Oct-1 Nov, 1998, pp. 703-706.

[17] Wang, Y., Moulin, P.: Steganalysis of block-DCT image steganography. In: IEEE workshop on Statistical Signal Processing, IEEE Computer Society Press, Los Alamitos (2003)

[18] Westfeld, A.: High capacity despite better steganalysis (F5 - a steganographic algorithm). In: Moskowitz, I.S. (ed.) Information Hiding. LNCS, vol. 2137, pp. 289–302. pringer, Heidelberg (2001)

[19] Y. Li, C. Li and Wei, Protection of mammograms using blind steganography and watermarking, in: Proceeding of the IEEE International Symposium on Information Assurance and security , 2007, pp. 496-499.

[20] Zollner, H. Federrah, H. Klimant, A. Pfitzman, R. Piotraschke, A. Westfeld, G. Wicke, and G. Wolf. Modelling the security of steganographic systems, 2nd Information Hiding Workshop, pp.345{355, april 1998.