# A Robust Steganography Algorithm Based on Curvelet Transform

Hadi Gharavi
Computer and Information Technology Department
Sadjad University of Technology
Mashhad,Iran
Email: h.gharavi123@sadjad.ac.ir

Boshra Rajaei
Computer and Information Technology Department
Sadjad University of Technology
Mashhad,Iran
Email: b.rajaei@sadjad.ac.ir

***Abstract*—Steganography is a latin word for ”covert writing”. In the past two decades, steganography is widely used for hiding secret information in digital media, e.g. image, audio and text. There are two main categories of steganographic methods. The ones that hide information in the original domain and those which employ a transform representation of input cover media. In this paper, images are used as cover. It has been empirically proved that on average, transform-based algorithms provide higher security and robustness comparing to their equivalent spatial domain counterparts; The proposed steganographic algorithm utilizes features from the curvelet transform for hiding message and has been tested curvelet security and robustness benchmarks, that due to the 2D nature of its asymmetric kernels, has potential of tolerate online robustness attacks which has been confirmed experimentally.**

***Index Terms*—Steganography, Curvelet transform, Robustness,wavelet**

## I. Introduction

Information hiding is the science of sending and embedding secret information using a cover media. Unlike cryptography where everyone can see the encrypted secret message, steganography hides secret message in other objects known as cover object in a way that nothing can be percepted [1]. In this techniques both the cover and the secret message can be text, image, audio or video. Information hiding includes two main categories; watermarking and steganography [2]. Watermarking algorithms emphasize on robustness of the embedded information while in steganography, security is of main concern [3]. A system is called robust if the embedded information cannot be altered without making drastic changes to the stego-object(the cover image after embedding secret information). Security is provided when an eavesdropper does not doubt existence of secret message. Capacity refers to the maximum amount of information that may be embedded in a cover imperceptibly. Robustness and security are two different aspects of steganography which have trade off with each other [4].

Steganography schemes work in spatial or transform domains. In spatial domain, secret message is embedded by directly manipulating cover object values. These methods are computationally simple but less robust against operation attack [5]. In transform domain, the cover object is converted to a transform space such as discrete fourier transform (DFT), discrete wavelet transform (DWT), discrete curvelet transform (DCT) and etc [6]. Then, secret message is embedded by modifying the transform coefficients. For example, The authors in [2] used spatial domain to hide data based on DES cryptography using S-box mapping and a secret key which is shared between sender and receiver. In transform domain, Rekik et al. use wavelet and fourier transforms to embed secret audio message in speech audio signals [7]. Al-Ataby et al. [3] proposed high capacity image steganography based on curvelet transform with acceptable security but regardless to robustness of embedded data. Furthermore, S.Edward Jero et al. [8] used curvelet transform to embed patient data into ECG signal but similar to [3], robustness has been ignored.

In this paper we employ discrete curvelet transform (DCT) for robust hiding a secret message in a normal color image while preserving security. The rest of paper is organized as follows: Section II introduces background concepts necessary for understanding proposed method. In Section III, curvelet-based steganography algorithm is explained. In Section IV, using some real world images the performance of the steganography algorithm is shown. Finally the paper is concluded in Section V along with our future research trends.

## II. Background Material

### A. The Curvelet Transform

The curvelet transform is a multiscale directional transform that allows an almost optimal non-adaptive sparse representation of 2D objects with elongated edges to overcome inherent limitations of traditional multiscale representations such as wavelets [9]. For input Cartesian arrays of the form$f[t_1, t_2], 0 \leq t_1, t_2 < n$, curvelet coefficients can be expressed as fallow:

$$c^D(j,l,k) := \sum_{0 \leq t_1,t_2 < n} f[t_1,t_2]\,\overline{\varphi^D_{(j,l,k)}[t_1,t_2]} \qquad (1)$$

where $j$,$l$ and $k$ are scale, orientation and translation parameter, respectively and $\varphi^D_{i,j,k}$ indicate a digital curvelet kernel. This conversion has redundancy so that the redundancy of curvelet transform is about 2.8 when wavelets are chosen at the finest scale, and 7.2 otherwise. For a detailed description of the transform, the interested reader may refer to [10]. Fast discrete curvelet transform (FDCT) is implemented using

978-1-5386-4916-9/18/$31.00 ©2018 IEEE

two approach. The first is based on unequally-spaced fast Fourier transform (FDCT-USFFT) and the second is the FDCT based on frequency wrapping of specially selected Fourier samples (FDCT-FW) [10]. We used package CurveLab FDCT-FW implementation for curvelet transform.

### B. $YC_b$ $C_r$ Color Space

Because of extensive use of social networks, image is the most popular cover object to embed secret message. Color images can be represented in various spaces such as RGB (red, green, blue), HSV (hue, saturation, value), YC$_b$C$_r$ (luminance, chrominance), etc. The human visual is more sensitive to little changes in luminance comparing to chrominance [11]. In order to protect invisibility, YC$_b$C$_r$ color model is employed because it separates luminance and chrominance. Conversion from RGB to YC$_b$C$_r$ is possible using the following transformation [12].

$$\begin{bmatrix} Y \\ C_b \\ C_r \end{bmatrix} = \begin{bmatrix} 0.299 & 0.587 & 0.114 \\ -0.169 & -0.331 & 0.500 \\ 0.500 & -0.419 & -0.081 \end{bmatrix} \begin{bmatrix} R \\ G \\ B \end{bmatrix} \tag{2}$$

where Y is luminance, C$_b$ and $C_r$ are difference blue and red chromatic components, respectively.

## III. THE PROPOSED METHOD

Our proposed steganography approach is divided to four fundamental parts. First is a offline processing to select cover. Then, discrete curvelet transform applied to the YC$_b$C$_r$ selected cover and secret messages embed in a pre-determined scale. Finally, at receiver side, the information is extracted from stego-image.

### A. Cover Selection

In steganography, cover statistics play a major role in security degree of algorithm. Because human visual system is less sensitive to changes in regions with dense texture, images with high details is more suitable to hide the information. This will improve imperceptibility of final stego image. In our work, local variance is used as a measure of level of details in candidate image. Algorithm 1 describes cover selection step:

```
Algorithm 1: How to select cover
  Input: normal images
  Output: suitable cover images
  Divide a cover image into $8 \times 8$ non-overlapping blocks
  for all blocks $b$ do
      $r \leftarrow v(b)$
      if $r > \alpha$ then
          $n \leftarrow n + 1$
  if $n > \beta$ then
      select image $\leftarrow 1$
```

In this algorithm, the value of $n$ is a counter and $r$ is normalized variance with fallowing formula rule.

$$r = 1 - \frac{1}{1 + v} \tag{3}$$

Also, $0 < \alpha < 1$ is a predefined variance threshold and $\beta$ is a threshold on lower bound number of dense blocks. These parameters have significant impact on enhancing the imperceptibility of the selected images. As $\alpha$ tend to 1, this similarity between block pixels increases. As the number $\beta$ becomes larger, image have more dense texture. Hence, selected image is more suitable as a cover object.

### B. Scale Selection

Curvelet is a multiscale transform in which the scales are being represented in the form of concentric squares in Fig.1. Smaller squares indicate low frequency and vice versa. Regarding security considerations, the human visual system is less sensitive to high frequencies. In contrast, low frequencies is suitable for robustness embedding. Therefor, we decide to choose middle scales for hiding secret bits.

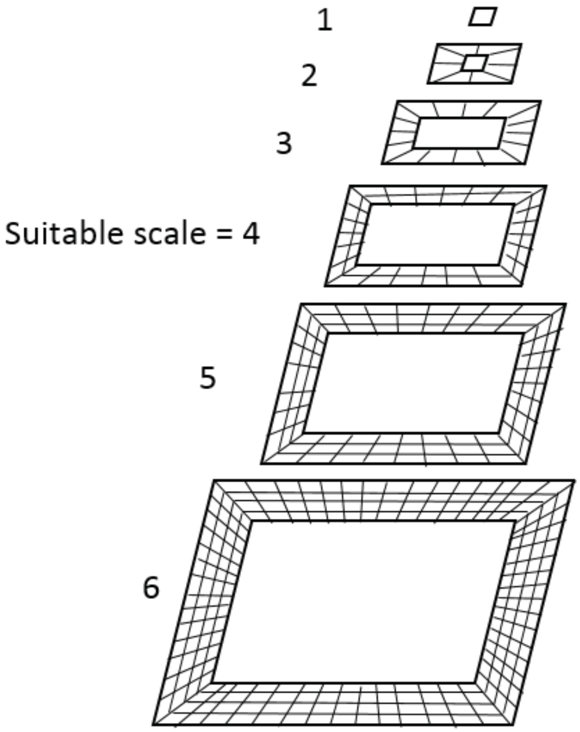


Fig. 1: Different scales of curvelet transform and the selected scale

### C. Embedding Procedure

After converting RGB images to YC$_b$C$_r$, secret message bits are embedded using the curvelet coefficients. Modifying a curvelet coefficient has impact on its neighborhood. Thus, it destroy the already hidden information. In order to embed secret bits, message is converted to a binary vector, $m$. To select embedding location, coefficients are first divided into $4 \times 4$ non-overlapping blocks as it has been shown in Fig.2. Block selection is based on a private key $k$ which is vector of natural numbers that are generated by a pre-shared seed between the receiver and sender. Finally, a pair of secret bits are embedded as following equation:

$$C'_{B^k_{ij}}(c,r) = \begin{cases} C_{B^k_{ij}}(2,2)+\delta & \text{if } m(l,l+1)=00 \\ C_{B^k_{ij}}(2,3)+\delta & \text{if } m(l,l+1)=01 \\ C_{B^k_{ij}}(3,2)+\delta & \text{if } m(l,l+1)=10 \\ C_{B^k_{ij}}(3,3)+\delta & \text{if } m(l,l+1)=11 \end{cases} \tag{4}$$

where $C'$ is the coefficient after embedding two bits of message in $C$ coefficient and $\delta$ is embedding strength factor. By increasing $\delta$, the impact of changing coefficients on embedded bit will be reduced. Also, $i$,$j$ indicates the block coordinate $B$ in the sub-band.

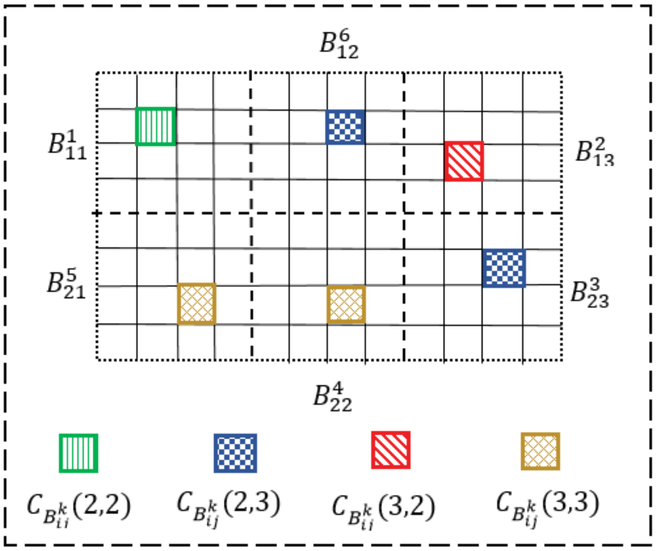


Fig. 2: Sample of secret bits embedding locations for a stream of 001001111101

### D. Extraction Procedure

The extraction procedure is composed of the following four steps:

**Step 1**: Convert the RGB stego image to YC$_b$C$_r$.

**Step 2**: Calculate curvelet transform of C$_b$ and C$_r$ components.

**Step 3**: Divide coefficients into $4 \times 4$ non-overlapping blocks.

**Step 4**: Extract the secret bits from blocks based on a private key using the following equation:

$$m(l,l+1) = \\ \begin{cases} 00 & C'_{B^k_{ij}}(2,2) > C'_{B^k_{ij}}(2,3), C'_{B^k_{ij}}(3,2), C'_{B^k_{ij}}(3,3) \\ 01 & C'_{B^k_{ij}}(2,3) > C'_{B^k_{ij}}(2,2), C'_{B^k_{ij}}(3,2), C'_{B^k_{ij}}(3,3) \\ 10 & C'_{B^k_{ij}}(3,2) > C'_{B^k_{ij}}(2,2), C'_{B^k_{ij}}(2,3), C'_{B^k_{ij}}(3,3) \\ 11 & C'_{B^k_{ij}}(3,3) > C'_{B^k_{ij}}(2,2), C'_{B^k_{ij}}(2,3), C'_{B^k_{ij}}(3,2) \end{cases} \tag{5}$$

where $m$ indicates message bits which are extracted in pair.

## IV. Experimental Results

### A. Security Evaluation

In order to examine the security performance of proposed scheme, it should be capable of embeding data imperceptibly not only to human visual system, but also to computer analysis. At first step, we use a dataset of 300 real-world $768 \times 1024$ color images with free credits from different websites over the internet. To select cover images using Algorithm 1, we set $\alpha$ and $\beta$ parameters to $0.997$ and $8.5 \times 10^2$,respectively. These parameters are chosen empirically so that one-third of the images are remain as cover image which some of the selected covers is shown in Fig.3. In this process, by selecting the more detailed images, imperceptibly will be increased. So we will obtain higher security on the stego image. Peak signal to noise ratio (PSNR) and mean square error (MSE) are two metrics to measure similarity between original cover and final stego image [13]. PSNR and MSE for an $M \times N$ image are defined as:

$$PSNR = 20\log_{10}\frac{255}{\sqrt{MSE}} \tag{6}$$

$$MSE = \sum_{i=1}^{M}\sum_{j=1}^{N}\frac{(f(i,j)-f'(i,j))^2}{M \times N} \tag{7}$$

where $f$ and $f'$ are cover and stego images,respectively. Another similarity measurement is relative entropy (Kullback-Leibler divergence) which is calculated as follow [14]:

$$D(P_c \parallel P_s) = \sum_{v \in V} P_c(v)\log_2\frac{P_c(v)}{P_s(v)} \tag{8}$$

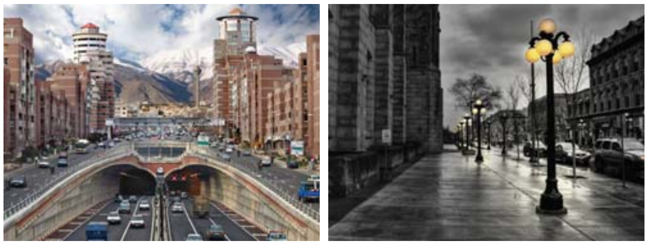
where $p_c$ and $p_s$ indicate cover and stego probability distributions and $v \in V\{0,1,2,\ldots,255\}$ is the pixel value image. Table I represent imperceptibly performance of the proposed algorithm while hiding message of length $10^4$ bits and Fig.4 shows two sample stego images.

TABLE I: Effect of $\delta$ parameter on security averaged over 100 selected covers

| embed parameter($\delta$) | PSNR | KL | MSE | BER |
|---|---|---|---|---|
| $\delta = 50$ | 42.89 | 0.011 | 3.36 | 0.09 |
| $\delta = 60$ | 41.55 | 0.012 | 4.58 | 0.07 |
| $\delta = 70$ | 39.33 | 0.015 | 7.67 | 0.05 |
| $\delta = 100$ | 37.53 | 0.018 | 11.62 | 0.03 |
| $\delta = 120$ | 36.03 | 0.022 | 16.41 | 0.02 |
| $\delta = 150$ | 34.18 | 0.028 | 25.15 | 0.01 |

(a) Tehran (b) Street (c) Fruit

Fig. 3: Sample normal cover images. a and b) Selected images. c) Rejected image



(a) PSNR=35.8 , $\delta$=120 (b) PSNR=35.7 , $\delta$=120

Fig. 4: Stego images after embedding $10^4$ bits

A steganographic scheme is broken not only when the secret message is extracted but also the stego image is detected by steganalysis. Steganalysis is another metric of security evaluation. It tries to break steganography schemes by analysing statistical features of stego image. It is a classification problem that classifies input image as either stego or non-stego using computer analysis. A lot of these methods are done by extracting features from the input image. Both ensemble classifiers (EC) [15], and extreme learning machine (ELM) [16] are designed to analyze jpeg images and are employed to evaluate detection accuracy of proposed scheme in table II. As is evident in this table, only ensemble classifier have more accuracy in stego detection. Due to given the emphasis on robustness in this paper , these results are acceptable.

TABLE II: Detection accuracy of stego images

| Steganalysis | Feature Dim | Hidden Neurons | Accuracy **(%)** |
|---|---|---|---|
| $ELM$[16] | 805 | 100 | 56 |
| $EC$[15] | 548 | – | 76 |

### B. Robustness Evaluation

In order to measure robustness, we apply several attacks such as JPEG2k compression, Gaussian noise and etc. Bit error rate(BER) is an objective robustness metric. BER is the ratio between the incorrectly extracted bits after attack and the original bits. This metric expresses the percentage of data loss [8].

$$BER = \frac{number\ of\ Bit\ Retrieved\ Incorrectly}{Total\ number\ of\ Bits} \times 100 \qquad (9)$$

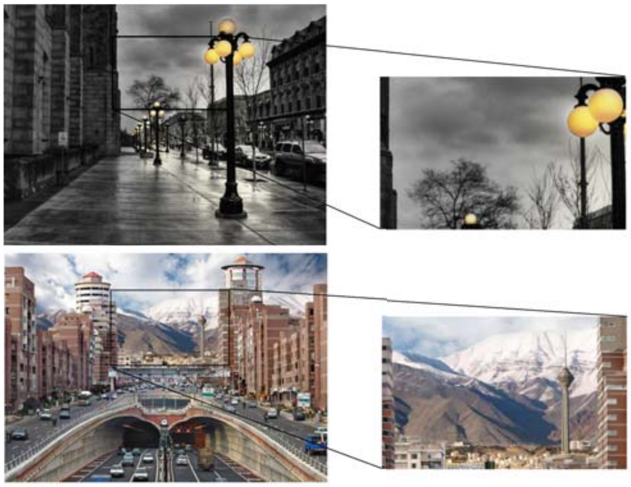
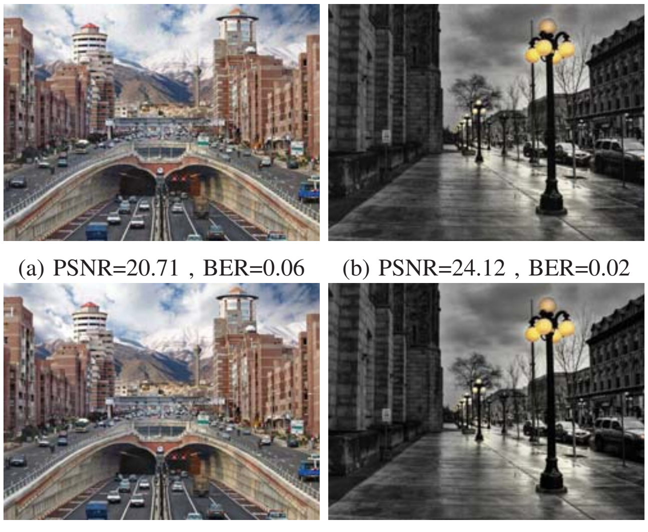


Fig. 5: Enlarged region stego images from Fig.4

Fig.6 shows BER with respect to signal to noise ratio from Gaussian noise over Street and Tehran sample images.



(a) PSNR=20.71 , BER=0.06 (b) PSNR=24.12 , BER=0.02

(c) PSNR=29.41 , BER=0.15 (d) PSNR=31.54 , BER=0.05

Fig. 6: Stego images after a,b) gaussian noise (SNR=15); c,d) JPEG2k compression(bpp=0.8)

TABLE III: Robustness study of the proposed method using different online attacks

| Attacks | PSNR | | KL | | BER | |
|---|---|---|---|---|---|---|
| | proposed | Singh et al [6] | proposed | Singh et al [6] | proposed | Singh et al [6] |
| JPEG2k (bpp =0.5) | 30.01 | 29.52 | 0.034 | 0.039 | 0.22 | 0.29 |
| JPEG2k (bpp =0.7) | 31.49 | 30.24 | 0.026 | 0.029 | 0.13 | 0.15 |
| JPEG2k (bpp =0.8) | 32.15 | 31.10 | 0.021 | 0.027 | 0.10 | 0.12 |
| JPEG2k (bpp =0.1) | 33.35 | 32.19 | 0.016 | 0.018 | 0.06 | 0.08 |
| Gaussian noise (SNR= 15) | 22.73 | 23.43 | 0.089 | 0.081 | 0.08 | 0.07 |
| Low-pass filter(win= 3) | 37.93 | 36.89 | 0.008 | 0.007 | 0.02 | 0.02 |
| Laplacian filter(alpha= 0.7) | 22.41 | 23.04 | 0.081 | 0.078 | 0.02 | 0.02 |

Table III shows BER of our proposed steganography method in comparison singh et al [6]. Both methods under different image processing attacks and embedding $10^4$ secret bits. The results are averaged over 60 achieved stego image.In addition, Fig.7 studies robustness of the proposed method under Gaussian noise attack with different SNRs using two sample covers. Obviously, the algorithm tolerate well noises as strong to 20 in SNR term. This is a significant result since online attacks aim to degrading an image in a level not being perceptible . Hence strong noises that may degrade an innocent cover image, are not of interest here.

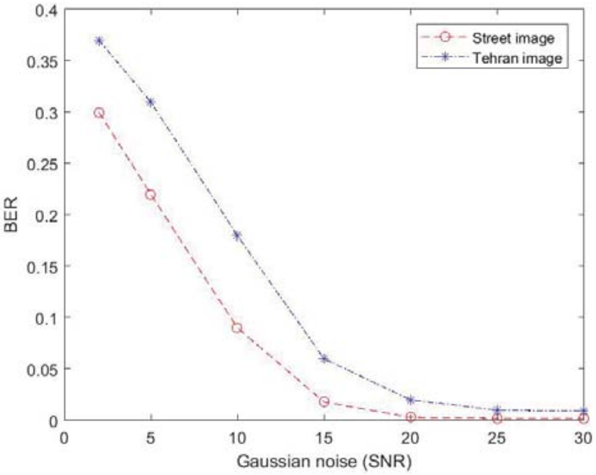


Fig. 7: Bit error rate under Gaussian noise attack

## V. Conclusion

In steganogrphy, there are three main success factors: security, robustness and capacity. In this paper a steganographic algorithm was presented that while preserving robustness at an acceptable level, improve highest security and capacity. To do this, curvelet coefficients of middle frequencies are employed. It has been shown that the proposed method outperform its similar wavelet-based algorithm. As our future research direction we aim to study curvelet power in steganalysis application and also provide double steganography methods by employing middle frequency curvelet coefficients and high frequency wavelet coefficients to hide information in two privacy levels.

## References

[1] H. M. Reddy and K. B. Raja, “High capacity and security steganography using discrete wavelet transform,” *International Journal of Computer Science and Security(IJCSS)*, vol. 3, pp. 462–472, 2009.

[2] Z. Zhao, Z.-M. L. H. Luo, and J.-S. Pan, “Reversible data hiding based on multilevel histogram modification and sequential recovery,” *AEU - International Journal of Electronics and Communications*, vol. 65, pp. 814–826.

[3] A. A. Al-Ataby and F. M. Al-Naima, “High capacity image steganography based on curvelet transform,” in *Developments in E-systems Engineering*, 2011.

[4] S. Katzenbeisser and F. A. P. Petitcolas, *Information hiding techniques for steganography and digital watermarking*. Artech house, 2000.

[5] M. S. Subhedar and V. H. Mankar, “Current status and key issues in image steganography: A survey,” *Computer Science Review*, vol. 13-14, pp. 95–113, 2014.

[6] S. Singh and T. J. Siddiqui, “Robust image steganography technique based on redundant discrete wavelet transform,” in *Power, Control and Embedded Systems (ICPCES)*, 2011.

[7] S. Rekik, D. Guerchi, S.-A. Selouani, and H. Hamam, “Speech steganography using wavelet and fourier transforms,” *EURASIP Journal on Audio, Speech, and Music Processing*, 2012.

[8] S. E. Jero, P. Ramu, and S. Ramakrishnan, “Ecg steganography using curvelet transform,” *Biomedical Signal Processing and Control*, vol. 22, pp. 161–169, 2015.

[9] J. Ma and G. Plonka, “The curvelet transform,” *IEEE Signal Processing Magazine*, vol. 27, pp. 118–133, 2010.

[10] E. Candès, L. Demanet, D. Donoho, and L. Ying, “Fast discrete curvelet transforms,” *Multiscale Model. Simul*, vol. 5, pp. 861–899, 2006.

[11] U. D. A. Hemalatha S and R. A, “Wavelet transform based steganography technique to hide audio signals in image,” *Procedia Computer Science*, vol. 47, pp. 272–281, 2015.

[12] oge marques, *Practical Image and Video Processing Using MATLAB*. WILEY-IEEE, 2011.

[13] Q. Huynh-Thu and M. Ghanbar, “Scope of validity of psnr in image/video qualityassessment, electron,” *Electronic Lett.*, vol. 44, pp. 800–801, 2008.

[14] C. Cachin, “An information-theoretic model for steganography,” *Information and Computation*, vol. 192, pp. 41–56, 2004.

[15] Jan Kodovský and Jessica Fridrich, “Ensemble Classifiers for Steganalysis of Digital Media,” *IEEE Transactions on Information Forensics and Security*, vol. 7, pp. 432–444, 2011

[16] Veenu Bhasin and Punam Bedi, “Steganalysis for JPEG Images Using Extreme Learning Machine,” in *IEEE International Conference on Systems, Man, and Cybernetics*, 2011.