Sumeet Kaur et al. International Journal of Recent Research Aspects ISSN: 2349-7688, Vol. 5, Issue 1, March 2018, pp.6-11

Estimating the Effect of Noises over an Efficient Image Steganography Algorithm Based on Intensity and Path Adaptation

Sumeet Kaur[1], Savina Bansal[2], R.K. Bansal[3]

[1]Research Scholar, PTU.
[2,3]Maharaja Ranjit Singh State Technical University, Bathinda
Corresponding author: Sumeet Kaur, email: purbasumeet@yahoo.co.in

Abstract-**T Steganography techniques as proposed by different researchers have varying degrees of performance abilities. An efficient steganography technique is suggested in this paper that aims at eliminating the drawbacks of widely used LSB and PVD methods. Proposed approach is simpler to implement and based on intensity adaptive range table to decide the no of bits for a pixel of selected image for embedding secret message and also involve the selection of a unique traversing path randomly. From experimental results, it is found that the proposed technique offers better embedding capacity, imperceptibility and value of various statistical parameters like PSNR, RMSE, and SSIM show that stego images generated are resistant against statistical and visual analysis. Further different types of noises have been added randomly to generated stego object. Results shows that even in presence of noise there is possibility of recovering secret message to a sufficient extent that proves efficiency and feasibility of proposed techniques.**

Keywords— **Secret Information, Security, Steganalysis, Steganography, Cover Object, Stego Object**

I. Introduction

As need to communicate secretly over the public internet is continually growing, use of steganography to support secret communication is also increasing. Steganography is a branch of information security that deals with embedding secret information in digital media called cover object or stego object. A lot of research work, books and articles have been published and large variety of software tools has been developed for steganography. Govt. agencies of different countries especially U.S. has also shown interest in using steganography for security purposes. Realizing need and potential benefits, governments of different countries are moving towards e-governance. One of the important features of e-governance is transfer of personal and secret information over the internet. To protect information from security threats is one of the top priorities. Steganography can provide higher level of protection and security to digital media that is communicated over public networks. Steganography techniques has vast number of applications in different fields like military, forensic, medical sciences, books, software, music & film industry, and various other areas crucial for maintaining integrity, authenticity, copyright defense, illicit use recognition, sharing and communication of digital media over public networks.

Both steganography and cryptography techniques are used for security reasons but they have different objectives. Cryptography scrambles text and transforms it into non readable form. Cryptography enciphers text and also attracts interest of hackers but steganography hides very existence of secret information into cover object. Till now encryption techniques are widely used security techniques. Governments and private companies are paying huge amount of money and time for designing of secure cryptosystems but these techniques are not adequate and applicable in all areas. Further strength of these techniques depends on length of keys. With advancement of technology, key length goes on increasing and hence putting a question mark on use and strength of these techniques. At International Cryptology Conference, MD5 and other encryption systems, which are widely used, were proved untrustworthy [1]

Other data hiding techniques related to steganography are fingerprinting and watermarking. Watermarking generates watermarked signal into cover multimedia to secure owner authenticity on digital medium and primarily concerned on security of embedded secret information rather than capacity. Separate mark in the digital medium is provided to different customers as concealed number, so as to enable owner of digital medium to recognize those, who break their authorization agreement. Important difference between fingerprint and watermarking is that fingerprint is exceptional with every copy of digital object but watermark embedded is similar with every copy of digital object.

An efficient steganography technique must have large data hiding capacity, good quality of visual and statistical characteristics [2]. The primary goal of steganography techniques is to enhance data hiding capacity and to minimize identification of generated stego object against security attacks. Secondary goal of a steganography technique is to avoid retrieval of embedded secrets from the stego object.

Steganography techniques are divided into spatial domain and transform domain types. Spatial domain techniques generally use bitwise operation based on intensity of pixels and noise. In spatial domain category pixel are selected based on physical position and intensity value of pixel. Transform domain techniques transform the image to frequency domain using various methods such as DCT, DFT, DWT, etc and then message is embedded. Embedding in spatial domain schemes provides higher capacity; contrary to the frequency domain scheme which shows more strength against attacks like compression and filtering noise etc.

Steganalysis is process of detecting, embedding and then reading (and or destroying) hidden secret information. Steganography leaves some detectable traces and also changes properties of original cover object. Steganalysis is not only used by attacker for illegally detecting hidden information but also used to check strength of a steganography algorithm. LSB techniques are widely used and also provide high capacity. Various LSB based steganography tools are available over internet. Sufficient work has be done towards steganalysis of LSB based techniques[3],[4],[5],[6], [7], [8], [9]. There are large no of steganalysis tools like higher-level statistical tests, Chi-Square Statistical test, Steg Spy1, ANOVA test, Steg Detect2 etc.

II. Review and analysis of some of existing techniques

Here study, review and analysis of some of the commonly used existing techniques are made. Literature from some of most commonly used LSB and PVD techniques are considered to get more insight about existing steganography techniques.

LSB techniques (LSB): LSB is one of the simplest and commonly used methods for data embedding. Different versions of LSB techniques are: Least Significant Bit Replacement (LSBR), Least Significant Bit Matching (LSBM), Least Significant Bit Matching Revisited (LSBMR) etc.

Least Significant Bit Replacement (LSBR): In LSBR technique, least significant bits of cover image pixels are replaced by secret message bits hence only lowest bit plane of cover object is changed and highest bit plane remains same. In some improved versions of LSBs before embedding some traversing order is generated by PRNG and in some other LSB schemes first secret data is encrypted before embedding[10]. These schemes are simple and easy to implement and provide high data embedding capacity. However, these schemes are very easy to attack as some detectable asymmetry is introduced like using LSBR even pixel values are increased by one or left unmodified but odd values are left unmodified or decremented by one. There are various Steganalysis algorithms which can detect hidden message with LSBR even at very low data hiding capacity [2] like chi square attack [3], sample pair analysis[6], general framework for structural Steganalysis [9], [11], RS Steganalysis [5].

Least Significant Bit Matching (LSBM): In this technique, least significant bits of pixels of cover object are matched with bits to be embedded, if LSB of cover pixels are not matched with corresponding message bit then cover pixel will be randomly added or subtracted by one, Therefore LSBM technique is also called + - embedding LSB [19]. LSBM is secure as compared to LSBR and it avoids asymmetric distortion introduced by LSBR, thus Steganalysis techniques which are used to detect LSBR are not applicable to LSBM. From study of stego object created by LSBM, it was found that there is change in another statistical property that is stego image histogram contains few higher frequencies as compare to cover object. To detect such artifact a steganalyzer has been designed based on Histogram characteristic function using center of mass[12]. Several steganalysis techniques have been designed for LSBM [12], [13], [14], [15], [16], [17], [18].

LSB Matching Revisited (LSBMR): In LSBR and LSBM each pixel is considered independent, but LSBMR takes two pixels for embedding as a group. The LSB of one pixel is used to carry the first bit; odd-even relationship of two pixel values is used to carry the other secret bit. LSBMR avoid limitations of both LSBR and LSBM like asymmetry introduced in LSB plane by LSBR and also makes detection difficult against Steganalysis attacks [2]. It provides very high capacity but on the negative side, LSB techniques have very low imperceptibility, low security and vulnerability to various attacks. In most of the LSB techniques, all pixels are treated equal and tolerate same amount of distortion but this is not true for images with larger smoother and/or regular regions [19].

Pixel Value Differencing Techniques (PVD): Pixel value differencing schemes has high capacity and good imperceptibility because PVD schemes use characteristics of human visual sensitivity. Original PVD techniques suffer from attacks like histogram analysis, although pseudo random bits are selected for embedding. Here cover image is divided into smaller blocks, each block is rotated by a random degree [19]. Then resulting image is divided into non overlapping blocks with three pixels each and central pixel is used for data hiding. Here number of hiding bits depends on difference of intensities among pixels to preserve statistical properties and to defeat steganalysis, same sort order of pixels and first edge regions are used adaptively while preserving smoother regions.

Non Adaptive and Adaptive PVD Methods: In this technique, position of pixels selected for embedding depends only on PRNG without considering important parameters like length of secret message and content of image. Number of pixels selected for embedding are adapted and selected based on various features like texture, flat/smooth regions. It leads more secure and fewer detectable visual distortions in stego objects [19].

Adaptive PVDs are more secure and improved version of normal and non adaptive PVDs, based on characteristics of human visual systems like sharper regions/ high intensity regions/ edge region provide better hiding capacity with robustness than smoother regions. PVD techniques provide high level of imperceptibility as compared to LSB techniques with same level of hiding capacity. But PVD techniques do not preserve statistical characteristics even at very low capacity (10% embedding)[19]. On negative side of PVD techniques is that the histogram analysis of stego images shows presence of secret data [20].

III. Motivation For Work

Before From literature survey and analysis of PVD based techniques certain reasons for weak points of PVDs techniques were traced out like PVD based techniques do not take full advantage of edge information [4]. Only vertical edges and fixed traversing order (generally raster scan order) are used which lead to easy detection by steganalysis. There are undesirable effects in histogram of stego image due to non adaptive quantization of pixel difference. After embedding, sort order of pixel is also changed that lead to statistical changes in stego images. In most of the existing PVD techniques, position of pixel for embedding is decided by certain secret key and hence embedding in smoother/flat regions are there rather than selecting edge or sharper regions first. Our eyes are less sensitive to regions in an image where brightness is very high or low. Highly textured regions can tolerate more changes like sharp/edge regions but it is sensitive to even slight changes in smooth regions. These properties of human visual system can be exploited while designing more secure steganography algorithms. Different types of images have different embedding capacity. Adaptive schemes are more secure. Hiding data by considering message length as well as nature of contents of image like first hiding in edge regions then in smooth regions can be made more secure and robust [19]. Cover selection is also one of the major issues [21].

These reasons have provided the base for research to design more robust and efficient steganography algorithms like: Imperceptibility can be improved by embedding in busy areas rather than smooth areas [20]. Security of an embedding algorithm can be improved by defeating against steganalysis based on histogram analysis techniques. To ensure feasibility and efficiency of a embedding scheme different types of noises are considered and implemented[22][23][24].

IV. PROPOSED WORK

Proposed embedding scheme is based on image steganography. It is an adaptive approach. To improve imperceptibility and visual quality of stego image, bits selected for embedding the secret message are adapted. Large no of bits are used from cover image with high intensity and less no of bits are selected from pixels having low intensity. This also tends to eliminate some of the drawbacks in commonly used LSB and PVD techniques. A unique concept of selecting and implementing different types of paths randomly for traversing the given cover image for embedding secret bits has also been added that will defeat various steganalysis attacks. Different types of noises have been added randomly to stego object and their effect is checked to prove feasibility of proposed technique over noisy channels.

(A) Embedding Algorithm: Following steps are considered as part of embedding algorithm:

(1) Convert secret message to be embedded in the cover image in binary form and certain transformations are made to secret text before embedding to provide additional layer of security to increase robustness and defeat steganalysis attacks accordingly. A key K1 is exchanged between sender and receiver.

(2) After scrambling original text data is converted into equivalent ASCII code and then binary code is generated.

(3) An adaptable intensity-range-table is designed. Here 8-bit gray scale images are considered having intensity in the range $0 \leq 255$. Set of rules used to design range table and making technique adaptable are as follows:

   i. Pixels with intensity value falling in range say $0 \leq 192$ one bit of is used to hide of secret data
   ii. Pixels with intensity value falling in range say $193 \leq 223$ two bits are used to hide of secret data
   iii. Pixels with intensity value falling in range say $224 \leq 239$ three bits are used to hide of secret data
   iv. Pixels with intensity value falling in range say $240 \leq 255$ four bits are used to hide of secret data

(4) Different scan pattern are considered, implemented and a particular one is selected randomly at a time to traverse an image. Depending on number of paths considered at sender side, a code is assigned to the path and an n-bit key say K2 and a seed value are exchanged accordingly.

(5) Above mentioned steps are repeated until all pixels are embedded in the selected cover object.

(6) Different types of noises are implemented and their effect is checked over proposed work.

(B) Extracting Algorithm: At the receiving side extracting algorithm is used to recover secret bits from the stego object. Following steps are taken for it:

(1) From seed value, key K2 and traversing path for stego object is recognized.

(2) From intensity range table, position of pixels and number of bits of secret data embedded in particular pixels are identified and extracted accordingly and recovered.

(3) Above mentioned steps are repeated until all pixels of cover image are traced out and secret message bits are recovered from the given stego object.

(4) Using Key K1, generated array of recovered bits is unscrambled.

(5) Binary data in above said array is changed back into ASCII form to get data in character form.

V. RESULTS AND ANALYSIS

For any Steganography algorithm desirable parameters are capacity, imperceptibility and robustness but it is very hard to achieve all these parameters because there is trade-off between parameters.

a) Capacity: Capacity is defined as amount of hidden data that we can embed and latter on can be retrieved without any distortion in cover object.

b) Imperceptibility: There should be no visual and statistical distortion between cover and stego object.

c) Robustness: A steganography algorithm is said to be robust if it can tolerate any attack or different transformations like scaling, rotation, compression etc.

d) Security: Embedded information should not be removable even after detection.

To check hiding capacity, imperceptibility and robustness of proposed technique various experiments are performed with test images.

(A) Visual analysis: Visual analysis is made to find out distortions in stego object after embedding secret message in cover image with benchmark gray scale images like Lena, Baboon and Lady. Results with bench mark gray scale image of Lena, Baboon and Lady are as follows:

(i) Lena (ii) 90608bt (iii) baboon

(iv) 90608bt (v) Lady (vi) 90608bt

Fig 1: (i), (iii), (v) show cover objects of 'Lena', 'Baboon' and 'Lady' respectively. (ii), (iv) and (v) are corresponding stego objects with different data hiding capacities.

Visual analysis of cover objects and stego objects show that there is no visual degradation in stego objects even at very high data embedding capacities that proves efficiency and robustness of proposed technique.

(B) Robustness Analysis: Robustness of proposed technique is verified from statistical analysis.

(i) Statistical Analysis: For performance analysis of proposed scheme certain statistical parameters like Peak Signal to Noise Ratio (PSNR), Root Mean Square Error (RMSE) and Structural Content Metric (S) are computed.

Table 1: Implementation of Various Statistical Parameters with Proposed Technique

*Size (512*512)*	*Capacity*	*Peak Signal to Noise Ratio (PSNR)*	*Root Mean Square Error (RMSE)*
Lena Image (tif)	119147	62.5486	0.0362
	90608	63.7308	0.0275
	87990	63.8640	0.0267
	87626	63.8857	0.0266
	87472	63.8914	0.0265
	87388	63.8951	0.0265
	87304	63.9001	0.0265
Baboon Gray scale image (tif)	119147	62.7139	0.0348
	90608	63.9126	0.0264
	87990	64.0464	0.0256
	87626	64.0626	0.0255
	87472	64.0704	0.0255
	87388	64.0769	0.0254
	87304	64.0808	0.0254
Lady Gray scale image (gif)	119147	62.3119	0.0382
	90608	63.4344	0.0295
	87990	63.5454	0.0287
	87626	63.5627	0.0286
	87472	63.5685	0.0286
	87388	63.5708	0.0286
	87304	63.5737	0.0286

Illustration: Various experiments are performed using benchmark images and different statistical parameters are computed. From experiment observations it is clear that the proposed technique has high embedding capacity, very high value of peak signal to noise ratio, very low value of root mean square error and value of structural metric constants are obtained as desired which prove that proposed technique is an efficient embedding technique.

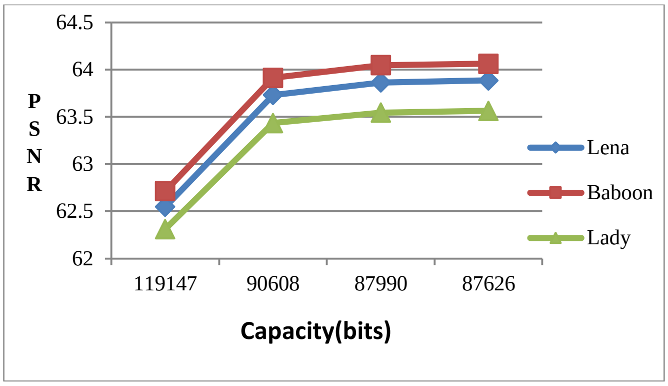

Fig 2: Relationship between Capacity and Peak Signal to Noise Ratio

Illustration: Above chart shows relationship between sizes of hidden secret message in a cover object with peak signal to noise ratio. From chart it is clear that as size of embedded secret message increases, peak signal to ratio decreases.

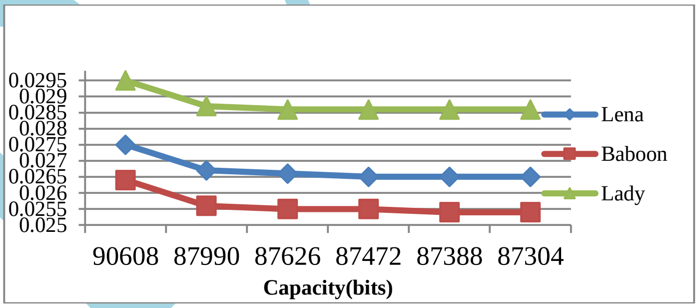

Fig 3: Relationship between Capacity and Root Mean Square Error

Illustration: From above graphical representation it is clear that even for same embedding capacity different images show different values of root mean square error, from experiments it is clear that 'Baboon' image shows lowest value of root mean square error, these observations show that efficiency of a given embedding technique not only depends upon embedding logic but also on other important factors like intensities of pixels of given cover image, texture, number and types of edges etc available in selected image as a cover object.

(ii) Implementation of Various Noises with Proposed Technique: Different types of noises are considered and added randomly. After implementation their effect is checked on proposed scheme to show efficiency of the technique:

Table 2: Implementation of Various Noises with Proposed Technique

Image Type - Lena(512*512)							
Noise Type	*Path Type*	*Embedding capacity (in bits)*	*PSNR*	*RMSE*	*S*	*M*	*P=%M*
Salt σ=0.02	olumn	119147	62.7139	0.0348	1.0001	58363	48.984
		87472	64.0704	0.0255	1	43301	49.5027

		86968	64.0984	0.0253	1	43071	49.5251
		90608	63.9126	0.0264	1	44737	49.3742
		87990	64.0464	0.0256	1	43558	49.5034
		87626	64.0626	0.0255	1	43384	49.5104
		87472	64.0704	0.0255	1	43301	49.5027
		87388	64.0769	0.0254	1	43269	49.5137
		87304	64.0808	0.0254	1	43225	49.5109
Gaussian σ=0.02	Row wise	86884	64.1043	0.0253	1	43627	50.2129
		90608	63.9126	0.0264	1	45316	50.0132
		87990	64.0464	0.0256	1	44028	50.037
		87626	64.0626	0.0255	1	43905	50.105
		87472	64.0704	0.0255	1	43670	49.9245
Gaussian σ=0.02	Column wise	87304	64.0808	0.0254	1	43817	50.189
		90608	63.9126	0.0264	1	45130	49.808
		87990	64.0464	0.0256	1	44070	50.0852
		87626	64.0626	0.0255	1	43999	50.2123
		87472	64.0704	0.0255	1	43756	50.0229
		87388	64.0769	0.0254	1	43788	50.1076
		87304	64.0808	0.0254	1	43582	49.919
		87990	63.8658	0.0267	1	43739	49.7091
		87626	63.8814	0.0266	1	43210	49.3118
		87472	63.8901	0.0266	1	43313	49.5164
		87388	63.8939	0.0265	1	43446	49.7162
		87304	63.8951	0.0265	1	43063	49.3253
Speckle σ=0.02	Row wise	86884	64.1043	0.0253	1	43522	50.0921
		87990	64.0464	0.0256	1	44010	50.017
		87626	64.0626	0.0255	1	43863	50.0571
		87472	64.0704	0.0255	1	43716	49.9771
		87388	64.0769	0.0254	1	43714	50.0229
		87304	64.0808	0.0254	1	43732	50.0916
		87052	64.0945	0.0253	1	43606	50.0919

Illustration: Purpose of randomly selecting different scan paths is to defeat steganalysis and to make technique more secure and robust, further effect of different noises over stego image is also checked to show reliability of proposed technique. Noises are added randomly to the entire stego image. Although different paths and different type of noises are added while embedding secret in cover image even then there is approximately same effect is observed that is clear from parameters M and P. Very low value of RMSE, very high value of PSNR and a perfect value for structural metric constants are achieved in results computed from different experiments with benchmark images that shows efficiency and feasibility of proposed scheme.

VI. CONCLUSIONS

Steganography is one of the reliable security options. It can be a valuable tool for confidentiality of secret information over internet but one has to cautiously select a suitable cover medium with required file format, compression and particular embedding logic according to the need of application. Steganography has applications in various fields and can be used in combination with cryptography to doubly protect the secret message. Like other technologies it has certain limitations, so there is also need to understand steganalysis to use it for the well being of community.

From study and analysis of existing steganography techniques it is observed that if a technique provides high payload capacity, it may be less robust and vice versa. LSB techniques and PVD techniques are widely used approaches in spatial domain but both approaches have major concern over data embedding capacity rather than security, only few works has been done to acquire security in spatial domain. Proposed technique not only provides high embedding capacity but also support imperceptibility and robustness to a good extent. Results from statistical and visual analysis show that after embedding cover object and stego objects are similar, there is no distortion in stego object even at very high capacity and desirable values of other statistical parameters are also achieved.

REFERENCES

1. Wang, X., Feng, D. Lai, X., Yu, H., Collisions for Hash Functions MD4, MD5, HAVAL-128 and RIPEMD. Cryptology ePrint Archive, Report 2004/1999,(2004)
2. X. Zhang and S. Wang, “Steganography using multiple-base notational system and human vision sensitivity,” IEEE Signal Process. Lett., vol. 12, no. 1, pp. 67–70, Jan. (2005)
3. Westfield and A. Pfitzmann, “Attacks on Steganographic Systems,” Lecture Notes in Computer Science, vol. 1768, Springer-Verlag, Berlin, , pp. 61-75(2000)
4. N.Provos, “Defending Against Statistical Steganalysis”, 10th USENIX Security Symposium, Washington, DC, (2001)
5. J. Fridrich, M. Goljan, and R. Du, “Detecting LSB steganography in color, and gray-scale images,” IEEE Multimedia, vol. 8, no. 4, pp. 22–28, Oct. (2001)
6. Sorina Dumitrescu, Xiaolin Wu, and Zhe Wang, “Detection of LSB Steganography via Sample Pair Analysis”, IEEE Transactions on Signal Processing, VOL.51, NO.7, July (2003)
7. Andrew D. Ker, “Quantative evaluation of pairs and rs Steganalysis”, In Delp III, E.J., Wong, P.W., eds.: Security, Steganography, and Watermarking of Multimedia Contents VI. Volume 5306 of Proc. SPIE, pp.83–97,(2004)
8. Xinpeng Zhang, Shuozhong Wang, "Vulnerability of pixel-value differencing steganography to histogram analysis and modification for enhanced security, Pattern Recognition Letters 25, 331–339, Elsevier, (2004)
9. A. D. Ker, “Steganalysis of LSB matching in grayscale images,” IEEE Signal Process. Lett., vol. 12, no. 6, pp. 441–444, Jun. (2005)
10. W. Luo , F. Huang and J. Huang “Edge Adaptive Image Steganography Based on LSB Matching Revisited", IEEE Transaction On Information Forensics And Security, vol. 5, no. 2, pp.201 -214, June,(2010)
11. J. Harmsen and W. Pearlman, “Steganalysis of additive-noise modelable information hiding,” Proc. SPIE Electronic Imaging, vol. 5020, pp. 131–142, (2003)
12. J.Fridrich, M.Goljan, D.Soukal, “Higher-order statistical Steganalysis of palette images”, In Delp III, E.J., Wong, P.W., eds.: Security and Watermarking of Multimedia Contents V. Volume 5020 of Proc. SPIE. pp.178–190, (2003)
13. Andrew D. Ker, “Improved Detection of LSB Steganography in Grayscale Images”, Proc. The 6th Information Hiding workshop Vol 3200 of Springer LNCS, pp. 97-115, (2004)
14. X. Li, T. Zeng, and B. Yang, “Detecting LSB matching by applying calibration technique for difference image,” in Proc. 10th ACM Workshop on Multimedia and Security, Oxford, U.K, pp. 133–138., (2008)
15. F. Huang, B. Li, and J. Huang, “Attack LSB matching steganography by counting alteration rate of the number of neighborhood gray levels,” in Proc. IEEE Int. Conf. Image Processing, Oct. 16–19, vol. 1, pp. 401–404, (2007)

16. X. Zhang and S. Wang, "Steganography using multiple-base notational system and human vision sensitivity," IEEE Signal Process. Lett., vol. 12, no. 1, pp. 67–70, Jan. (2005)
17. B. Li, J. Huang, and Y. Q. Shi, "Textural features based universal Steganalysis," Proc. SPIE on Security, Forensics, Steganography and Watermarking of Multimedia, vol. 6819, p. 681912, (2008)
18. M. Goljan, J. Fridrich, and T. Holotyak, "New blind steganalysis and its implications," Proc. SPIE on Security, Forensics, Steganography and Watermarking of Multimedia, vol. 6072, pp. 1–13,(2006)
19. Weiqi Luo, Fangjun Huang and Jiwu Huang, "A more Secure Steganography based on Adaptive pixel-value Differencing Scheme", Multimedia Tools and Applications Vol. 52, No. 2-3, pp. 407-430, (2011)
20. El-Alfy, El-Sayed M., and Azzat A. Al-Sadi. "Pixel— Value Differencing Steganography: Attacks and Improvements." ICCIT. 2012.
21. Kharrazi, Mehdi, Husrev T. Sencar, and Nasir Memon. "Cover selection for steganographic embedding." Image Processing, 2006 IEEE International Conference on. IEEE, 2006
22. Zhang, Lei, et al. "Two-stage image denoising by principal component analysis with local pixel grouping." Pattern Recognition 43.4 (2010): 1531-1549
23. Luisier, Florian, Thierry Blu, and Michael Unser. "Image denoising in mixed Poisson–Gaussian noise." IEEE Transactions on Image Processing 20.3 (2011): 696-708.
24. Richards, Mark A. Fundamentals of radar signal processing. Tata McGraw-Hill Education, 2005.