ISSN No. 0976-5697

Volume 6, No. 5, May - June 2015

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

An Overview of Image Steganographic Techniques

Archana.O.Vyas
Deptt. Of Electronics and Tele-Communication Engg.,
G. H. Raisoni College Of Engineering and Management,
Amravati, India

Dr. Sanjay.V. Dudul
Deptt. Of Applied Electronics,
Sant Gadge Baba Amravati University,
Amravati, India

Abstract: Steganography is the art of hiding information in ways that prevent the detection of hidden messages. Steganography, derived from Greek, literally means "Covered writing". It includes a vast array of secret communication methods that conceal the message's very existence. These methods include invisible inks, microdots, character arrangement, digital signatures, covert channels, and spread spectrum communications. Steganographic applications only require the flexibility to alter cover object in order to be able to embed the hidden information. For this reason any type of digital object can be potentially used as a cover object. For example, images, audio, streaming data, software or natural language text have been used as cover objects. The secrecy lies in the design of neural algorithm. The neural algorithm that has been chosen to train the secret data bits and selected image bits, which has to be transacted through a secured channel between the source and destination. This makes the steganography process that hides the data in a more efficient manner. The neural algorithm is designed with respect to the input patterns. The main advantage of this proposal is that the secret data is not transmitted as it is. The added advantage is that the cipher text generated depends on the design of neural algorithm. Different algorithms are available for digital image steganography both in the spatial and transform domain like LSB substitution, OPAP, Pixel indicator technique, F5 etc.

Keywords: Steganography; Cover Object; Security; LSB substitution; F5; OPAP; PIT

I. INTRODUCTION

In the recent times, the need for digital communication has increased dramatically and as a result the internet has essentially become the most effective and fast media for digital communication. At the same time, data over the internet has become susceptible to copyright infringement, eavesdropping, hacking etc. and thereby necessitating secret and reliable communication.

Digital media is the most preferred source for transfer of information and communication now days. With the growth and access of internet to everyone, it became easier and possible to copy and to distribute the digital information illegally [1]. Digitally transferred data can be copied without any loss of content and quality as well, which is a serious problem to the security, authenticity and copyright to the owner of the data [2][3]. Maintaining secrecy of data has become an important issue and steganography offers a very reliable solution for such problems. Steganography is an art and science of embedding secret message into cover medium. In steganography, secret message is embedded in an appropriate carrier object that may be image, video, sound or other file to be transmitted over internet and embedding is parameterized by a key that makes difficult even, to detect the presence of data and further to find a key to access it. Once cover object is embedded, it is known as a stego object [3]. Steganography is complementary to cryptography, where it aims at hiding the existence of a message rather than making the message illegible through encryption. Thus, Steganography might be useful for secret communication in countries and regions where public use of cryptography is prohibited or restricted [4].

Recent developments in digital communications have made it possible to use intelligent methods for secret communication. One such method is image hiding, where a secret image is hidden in a host or cover image. The modified host image that contains the secret image is referred to as hybrid (stego) image.

There are numerous methods for hiding a secret image in a host image. Mainly, they can be divided into methods that embed the secret image into the host image in spatial domain and those that use transform domain. For spatial domain methods, the simplest methods are those that modify the least significant bits of pixels in the host image. The benefits of these methods are their simplicity, but they are weak in resisting simple attacks such as compression etc. In these methods, the capacity of embedding a secret image is limited and an increase in capacity severely affects the visual quality of hybrid image. Image hiding techniques that are implemented in transform domain have made it possible to take advantage of features in human visual system. These methods are more robust with regard to compression and some transforms, because they focus on the same features of image as compression techniques do.

Recently, images have been very popular choice as a cover medium primarily, because of their redundancy in representation and pervasiveness in applications in daily life. Over the years, many algorithms for hiding the data in images have been reported and developing newer algorithms (techniques or methods) are a topic of current research.

A. Steganographic notions:

The goal of steganography is to embed a message M in a cover object C in a covert manner, such that the presence of the embedded M in the resulting stego object S cannot be discovered by anyone except the intended recipient. All image steganography systems, irrespective of the algorithms by which they are implemented, follow the terms mentioned below.

a. ***Image:*** An image C denotes a discrete function assigning a colour vector $c(x, y)$ to every pixel (x, y) [5].

b. ***Cover Image****:* The cover image is the carrier of the hidden message. A cover is generally chosen in a manner that it appears most ordinary and innocuous and does not arouse suspicion as such [4].

c. ***Stego Image****:* The cover image with a secret message concealed within it is known as the stego image. It is used at the recipient side for extracting the hidden message [4].

d. ***Stego Key:*** Stego key is a key to embed data in a cover and extract data from the stego medium. It may be a number generated via a pseudo-random number generator [1] or can just be a password for decoding the embedding location.

e. ***Embedding Domain****:* The Embedding domain refers to the cover medium characteristics that are exploited in embedding message into it. It may be spatial domain, when direct modification of the constituent elements of the cover is modified (e.g. pixels in an image) or it can be the frequency domain or transform domain if mathematical transformations are carried on the medium before embedding [4].

B. Evaluation parameters for a steganography algorithm:

The main objectives for any steganography algorithm are capacity, undetectability and robustness [5]. Although it is difficult for a steganography algorithm to possess all the characteristics at the same time, because there is generally trade-offs among these characteristics.

a. ***Capacity:*** The amount of data to be embedded in cover medium and can retrieved later successfully without significantly changing the cover medium [6].

b. ***Undetectability:*** There should be no visual difference between cover and stego object i.e. embedded message should not be visible to human eye [6].

c. ***Robustness:*** A stego system is said to be robust, if it can sustain any attack and if it undergoes transformation such as scaling, rotation, filtering and lossy compression etc. It should remain intact [6].

d. ***Security:*** An embedding algorithm is said to be secure, if the embedded information could not be removed after detection by the attacker. It relies on the knowledge about the embedded algorithm and secret key [6].

e. ***Embedding rate:*** It is generally specified in absolute measurement, such that the size of the secret message or in relative measurement called data embedding rate given mostly in bits per non zero DCT pixel coefficient (BPNPC) and bits per pixel (BPP).

f. ***Imperceptibility or Fidelity****:* Stego images are expected not to have any significant visual artifacts under the same level of security and capacity. Higher fidelity of stego images implies better imperceptibility [4].

g. ***Type of images supported****:* As Images are available in a large number of formats, it is important to understand which type of images are suitable for the steganographic algorithm of various types. Images primarily use lossy or lossless compression mechanism and the properties of images affect the steganographic methods applicable to those images [4].

h. ***Time complexity:*** Steganographic algorithm varies according to the domain of embedding. In simpler systems, the embedding job is less time consuming but may not be as secure as some other more complicated systems offering better performance. Nevertheless, time complexity of an algorithm is important for judging the applicability of algorithm for embedding into large images and also their implementation is low resource system such as mobile devices etc. [4].

The rest of this paper is organized as follows:

Section II briefs various image steganography methods and difference between spatial domain and transform domain techniques. Section III explains various evaluation parameters, mathematically. Section IV elaborates the scope of research and limitations noticed so far in the reported research work in the field of steganography. Finally, section V describes the concluding part.

II. STEGANOGRAPHY METHODS

Steganography algorithms may differ from each other depending upon type of cover objects used, type of domain (spatial or transform domain), type of file format or compression used and type of embedding method used to modify the cover object etc. and can be classified accordingly as shown in Figure 1.

A. Image steganography:

Different types of cover objects like text, image, audio or video files can be used to hide the secret data. Image steganography is the most popular form of steganography. Here, secret message is embedded into an image as noise, which is almost impossible to detect by human eyes. Data hiding in still image imposes certain challenges to cope up with human visual systems (HVS). Still images are further subject to various operations like ranging from simple to nonlinear transformation such as cropping, blurring, filtering and lossy compression etc. and data hiding method should be resistant to these types of transformations [7]. In the recent times, there have been quite a large number of research activities in the field of image steganography. Many algorithms have been developed over the existing LSB methods and also in the transform techniques. Several algorithms are reported in literature. The algorithms are primarily classified into two major parts based on whether the pixels of the image are modified directly or some mathematical transform is applied on the images before embedding. The former techniques are called spatial domain techniques, while the latter are the transform domain techniques [4].

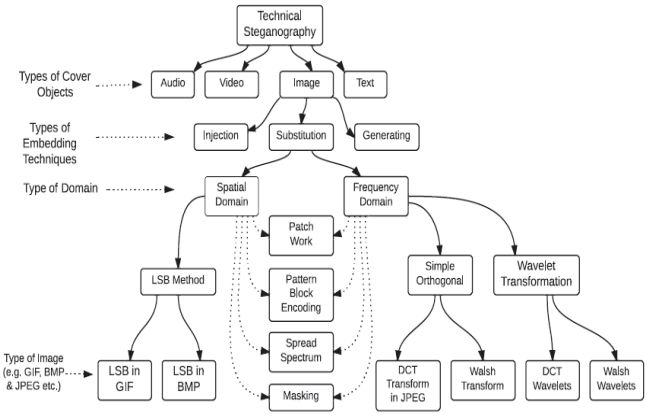


Figure 1- Classification of various image steganography techniques [6].

B. Steganography based on domain type:

Based upon domain type, spatial domain and transform domain techniques are commonly used steganography techniques.

a. Spatial Domain Techniques:

Spatial domain techniques include bitwise manipulation of intensity of pixels and noise manipulation. There are various approaches to embed data in spatial domain. Most commonly used and simple techniques for spatial domain are Least Significant Bit (LSB) Methods [6].

a) Direct least significant bit substitution:

LSB substitution forms one of the most conventional techniques of hiding considerably large secret message without introducing many visible distortions [8]. It works by replacing the LSBs of randomly selected or sequential pixels in an image.

The following operation describes the embedding of the LSB substitution algorithm.

$$Y_i = 2[X_i/2] + m_i \quad (1)$$

where *mi*, *Xi* and *Yi* denote the *ith* message bit, value of the selected pixel before embedding and value of the modified pixel after embedding respectively [4]. The biggest advantage of the LSB substitution method is the simplicity. LSB substitution affects pixels by ±1, if it can be assumed in general sense that the distortion produced by the mechanism is perceptually transparent in the passive warden [7] context. However, LSB substitution falls an easy prey to statistical attacks and image processing activities like compression cropping etc. In fact, embedding in LSB causes PoVs (Pair of Values) in the image to flatten out with respect to each other which makes LSB embedding more susceptible to steganalysis [3].

b) Optimal Pixel Adjustment Procedure (OPAP):

Originally proposed by Chi-Kwon Chan and L.M Cheng, the OPAP scheme was developed as an improvement over the LSB based algorithm and described in [9]. The OPAP scheme modifies the embedded bits in order to improve the overall visibility of the stego image. The adjustment is done on the basis of the pixel differences between original pixel Pi and the pixel Pi´ of the stego-image. If the difference is δi, then depending on it, pixel modification is done on the pixels before the embedded pixel so as to minimize the difference between the original pixel and the embedded stego pixel. The algorithm is tested for grey scale images and provides good overall imperceptibility. OPAP has been tested to provide high PSNR values (55.96 and 56.71) for standard test images Baboon and Lena [10].

c) Pixel Indicator Technique (PIT) [11]:

Pixel Indicator Technique is basically a modification over the conventional LSB insertion method of embedding and is primarily devoted to enhancing the security of the existing LSB scheme. PIT was designed to work on 24-bit/pixel RGB images. The algorithm uses two LSB of one colour channel to mark the existence of data in the other two. The size of the secret data serves as the key for choosing the selection channel. The indicator channel and the embedding channel are ordered in the way: RGB, RBG, GBR, GRB, BRG, and BGR. The algorithm produces extremely low visual distortion when the embedding rate is less than 3 bits and has low susceptibility to histogram and visual attacks at this rate. Thus, the maximum recommendable embedding rate for the PIT is less than 3 bits/ colour channel.

d) Pixel Value Differencing:

In the Pixel Value Differencing or PVD scheme [12], number of insertion bits in PVD depends on whether the pixel is an edge or a smooth area [8]. Human Visual System is sensitive to subtle changes in the smooth areas as compared to the edges. This is primarily because the difference between pixels in the smooth areas is much less as compared to that between the edge pixels and embedding in edge pixels causes less visual distortion. Few implementations of the PVD scheme may be found in [13, 14]. PVD does not cause much visual distortion and neither it is directly susceptible to the histogram attack as the LSB substitution. It is however susceptible to histogram analysis of the differences of the pixel pairs andχ2-attack [15].

e) Selected LSB algorithm:

The SLSB proposed in [16] embeds into single colour components of the pixels. It does not necessarily embed into the LSBs only but selects the colour plane and the modifiable bits of the colour plane in such a manner that will produce the minimum distortion. It falls in the category of the filtering algorithms as it applies a sample pair analysis filter before embedding to ensure that only the best candidate pixels are selected for embedding. It can embed at a rate of more than 1 bit per pixels. This, however might lead to variation of the degree of randomness of the pixels of the image and thereby makes it susceptible to statistical attacks when used for high degree of embedding [1].

b. Transform Domain Techniques:

a) JSteg:

The JSteg algorithm is acclaimed as the first commercially available steganographic tool for JPEG images [15]. The algorithm applies Discrete Cosine Transform to the image blocks and embeds the data in to LSBs of the DCT coefficients, sequentially. The sequential embedding and absence of any secret key makes the algorithm susceptible to eavesdropping as only knowledge of the embedding procedure is sufficient to decode the hidden message. Moreover, JSteg is easily steg-analyzed using the χ2-attack. Also, as the algorithm uses the DCT, it is extremely necessary to treat the DCT coefficients with sensitive care and intelligence in order to prevent the algorithm from leaving significant statistical signatures [17].

b) OutGuess:

This algorithm was an improvement of the existing JSteg algorithm. The OutGuess uses a PRNG (Pseudo Random Number Generator) to randomize the pixels in which the embedding is to be made. It also does not embed into DCT coefficients with values 0 and 1 as because they form a Pair of Value when their LSB changes and there are no ways of distinguishing between a zero DCT coefficient and a steganographic zero. The algorithm, after embedding, modifies the unchanged DCT coefficients to preserve the histogram of the original image. Thus, OutGuess is immune to attacks like the visual attack, histogram attack and the χ2-attack. The steganalyzing algorithm for OutGuess utilizes the fact that as OutGuess uses LSB embedding of the DCT

coefficients and that it makes random changes to the quantized coefficients, the spatial discontinuity at the border of each8×8block will increase.

c) F5:

The F5 algorithm was proposed as a steganographic technique that allows higher capacity of embedding and better security at the same time [16]. The F5 differs from most other steganographic algorithm in the fact that it does not overwrite LSBs of DCT coefficients/pixels rather it increments/decrement the value of the DC coefficients depending on need. The algorithm takes into consideration that flipping the LSBs either at the pixel level or at the DC coefficient level alters the statistical properties of the image and can serve as a means to steg-analyze the algorithm. F5 uses permutative straddling and matrix encoding to scatter the embedding effect and to embed data, respectively. F5 is the first implementation of the matrix encoding method proposed in [18]. F5 embeds at a rate of 3.8 bits per change and is secure against most statistical attacks like the histogram attack, the χ2-attack, blockiness detection etc. Moreover, it has a high embedding capacity. However, F5 remained a challenging algorithm to break until Fridrichet al. steganalyzed F5 by estimating the original histogram of the cover image from the stego image [19]. It is accomplished by decompressing the stego-image to spatial domain, cropping it by 4 pixels in both directions and recompressing using the same quality factor as the stego image.

d) Singular Value Decomposition (SVD) transform based method (RHISSVD):

The SVD based steganographic method proposed in [20] transforms the image into singular values and then embeds into them. Singular Values correspond to the luminance in the image and minor changes in them do not cause perceptible distortions in the image. The experimental results show that the method has a high PSNR value beyond the perceptible range for RGB images with compression quality ≤60 %. It has an average embedding capacity of 0.44bits per singular value coefficient for an image with compression quality 50%.Comparison between spatial domain & transform domain technique can be based upon various criteria like robustness, payload capacity, complexity of technique as shown in Table 1.

Table1. Comparison between spatial domain techniques and transform domain techniques [6].

Criteria	**Spatial Domain Techniques**	**Transform Domain or frequency domain Techniques**
Embedding Process	In spatial domain Steganography methods, secret messages are embedded by manipulation of pixel values i.e. intensity of pixel values.	Transform domain techniques, first convert image from spatial domain to frequency domain and
Robustness Against Attacks	Data embedding in the spatial domain is more robust to geometrical attacks, such as cropping and down sampling.	Data embedding in the frequency domain usually has more robustness to signal processing attacks, such as addition of noise, compression and low pass filtering [14].
Capacity	Data embedding in spatial domain category provides higher capacity.	Data embedding capacity is lower as Compared to transform domain
Complexity	Spatial domain Techniques are quite simpler.	These techniques are complex.
Examples	Commonly used techniques for spatial domain are LSB techniques.	Masking and filtering techniques are more commonly used with frequency domain

III. PERFORMANCE PARAMETERS

The effectiveness of a steganographic technique can be evaluated based on the following performance parameters.

a. Detectability: Let, Pc and Ps be probability distributions of the cover image and the stego-image, respectively. Then the detectability *D (Pc||Ps)* is given by

$$D\,(P_C||P_S) = \int P_C \log\,(P_C / P_S) \qquad (2)$$

Thus, for a completely secure stego system, *D=0* and if *D*≤€, then it is €-secure. A steganographic system is said to be undetectable or secure if no statistical tests can distinguish between the cover and the stego-image [21].

b. Peak signal to noise ratio (PSNR): Peak signal to noise ratio should be as high as possible. It is given in dB units and mathematically calculated as follows.

$$PSNR = 10\,\log_{10}(\frac{255^2}{MSE})dB \qquad (3)$$

Where, *MSE* denotes mean square error and is given by

$$MSE = \frac{1}{m*n}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}(X_{ij} - Y_{ij})^2 \qquad (4)$$

Where $m*n$ represents the size of each image i.e. *X*-Cover image and *Y*- stego image.

c. Embedding Rate: The rate at which the secret message can be embedded in the cover image is called embedding rate. It is generally given in the absolute measurement such that the size of the secret message or in the relative measurement. It is defined as the bits of the secret message embedded per pixel of the cover image and is the ratio of the

number of embedded bits to the number of pixels in an image.

$$EmbeddingRate = \frac{(bitsofsecret\ message\ embedded)}{(No.\ ofPixels\ ofCoverImage)} \quad (5)$$

Its unit is BPP (bits per pixel) or BPNPC (bits per nonzero DCT coefficients).

IV. SCOPE OF FURTHER RESEARCH

The literature survey provides details of how algorithms have evolved over time with respect to the nature of the cover image and the respective domain. In addition, preceding sections also highlight some characteristics that are extremely necessary for good steganographic system. Incorporating all of these features into a single system is itself a matter of significant research. However, in the light of information gathered hitherto, some of the possibilities of future scope in the field of digital image steganography are listed below.

a. ***Mathematically relating the security and capacity:*** Security and capacity tradeoff are important issues in steganography. There has not been much theoretical exploration in relating security and capacity parameter mathematically [4].

b. ***Development of algorithm based on objects in images:*** As the steganalysis techniques are getting stronger, eventually most steganography algorithms are falling prey to them. There is a trend in developing algorithm which targets selective parts of image for embedding. These algorithms are called object oriented steganography. The main concept of these algorithms is to identify areas in image also known as region of interest ROI where the embedding will cause the minimum distortion [4].

c. ***Improving the steganographic algorithms:*** It has been observed that all steganographic algorithms, be that in special domain or transform domain (frequency domain), ultimately change statistical properties of images and as a result of which they fall prey to statistical steganalysis technique. Thus, it is evident that there still remains ample scope for research in developing algorithm in image steganography that will be able to provide more secure feature for data hiding. Possible improvement that might be adopted can be classified as under.

a) ***Increasing embedding efficiency:*** Most steganography algorithm overwrites bits (LSB in special domain algorithm and LSB of DCT coefficient in the transform domain). Overwriting bits cause more alteration of the statistical properties of images and it is therefore crucial to work on algorithm that has minimum overwriting. The F5 algorithm is a trend setting example. However statistical properties of image change when it is modified after its creation. If secrete data bits are embedded into the image during its very creation, it is possible to produce stego images resistant to blind steganalysis [4].

b) ***Decreasing embedding distortion:*** Improving the security of steganography algorithms also consists of decreasing the amount of distortion produced by the embedding algorithm. One way of distortion minimization is by adjusting statistical property of the image after embedding to preserve the original characteristics. This, however, should be dealt with the utmost care because it is shown that the statistics preserving algorithm (OutGuess) itself leaves detectable marks during the modification process resulting in blockiness. So, statistics preserving technique must be carefully developed, so that the adjustments are not sensitive to statistical steganalysis [4].

c) ***Using alternate colour space:*** The majority of the available image steganography schemes use RGB or the gray scale images. It has been observed that colour spaces like HSV (Hue Saturation Value) and YCbCR colour spaces have a particular property that is quite useful for steganography purpose. Embedding in the hue component of HSV colour space or yellow (luminosity) component of YCbCR color space creates much less distortion as change in mentioned colour can deceive human visual system better. In addition embedding in the luminance component can provide more resistance to cropping and other accidental or intentional distortion [4].

V. CONCLUSION

Image steganography is a considerably new dimension in the field of information hiding. Though, there have been many active researchers in the field, many research issues are yet to be explored. This paper evaluates some of the most established algorithms for image steganography in different embedding domains based on the degree of security, capacity and factors such as the statistical property of image, which may deviate as a consequence of its embedding mechanism. Based on the information gathered through the analysis, some important characteristics of a good steganographic system have been proposed and future possibilities of research in the area of image steganography have also been pointed out.

VI. REFERENCES

[1]. S. K. Wajid, M. ArfanJaffar, WajidRasul, and Anwar M.Mirza, “Robust and imperceptible Image Watermarking using Full Counter Propagation neural Networks” 2009 International Conference on Machine Learning and Computing, IPCSITvol.3, 2011, IACSIT Press, Singapore pp 385-391.

[2]. R. Chandramouli, M. Kharrazi, and N. Memon, “Image Steganography and Steganalysis: Concepts and Practice”, T. Kalker et al. (Eds.): IWDW 2003, LNCS 2939, Springer-Verlag Berlin Heidelberg, 2004, pp. 35–49.

[3]. F.A.P. Petitcolas, R. J. Anderson, “On the Limits of Steganography”,IEEE Journal of Selected Areas in Communications, 16(4):474-481, May 98, Special Issue on Copyright & Privacy Protection. ISSN 0733- 8716, pp 474-482.

[4]. Ratnakirti Roy, Suvamoy Changder, Anirban Sarkar& Narayan C Debnath, “Evaluating Image Steganography Techniques: Future Research Challenges”, 2013, IEEE International Conference On Computing Management and

Telecommunication (Com Man Tel) 978-1-4673-2088-7/13.

[5]. N. Provos and P. Honeyman, "Hide and Seek: An introduction tosteganography", IEEE Security and Privacy Journal, 2003, pp 32.

[6]. Sumeet Kaur, SavinaBansal and R. K. Bansal,"Steganography and Classification of Image Steganography Techniques", 2014, IEEEInternational Conference On Computing For Sustainable Global Develpoement (INDIACom), 978-93-80544-12-0/14.

[7]. Chi-Kwong Chan, L.M. Cheng, "Improved hiding data in images by optimal moderately signifcant-bit replacement", IEE Electron Lett. 37 (16) (2001) 1017–1018.

[8]. Mehdi Kharrazi, Husrev T. Sencar, NasirMemon, "Image Steganography: Concepts and Practice", WPSC/Lecture Note Series, pp. 4, April, 2004. Source: www2.ims.nus.edu.sg/preprints/ab2004-25.pdf

[9]. R. Amritharajan, R. Akila, P. Deepikachowdavarapu, "A Comparative Analysis of Image Steganography", International Journal of Computer Applications, Vol. 2, No.3, pp. 41-47, 2010.

[10]. Adnan Abdul-Aziz Gutub, "Pixel Indicator Technique for RGB Image Steganography", Journal of Emerging Technologies in Web Intelligence, Vol 2, No 1 (2010), pp. 56-64, Feb 2010.

[11]. D. C. Wu and W. H. Tsai, "A steganographic method for images by pixel-value differencing," Pattern Recognition Letters, vol. 24, no. 9-10, pp. 1613–1626, 2003.

[12]. C.M. Wang, N.I. Wu, C.S. Tsai, M.S. Hwang, "A high qualitysteganography method with pixel-value differencing and modulusfunction", J. Syst. Software Vol. 81, No. 1, pp. 150-158, 2008.

[13]. Young-Ran Park, Hyun-Ho Kang, Sang-Uk Shin, and Ki-Ryong Kwon, "An Image Steganography Using Pixel Characteristics", Y.Hao*et al.* (Eds.): CIS 2005, Part II, Springer-Verlag Berlin Heidelberg LNAI 3802, 2005, pp. 581– 588.

[14]. VajihehSabeti, ShadrokhSamavi, MojtabaMahdavi, ShahramShirani, "Steganalysis of Pixel-Value Differencing Steganographic Method", Proc. IEEE PacificRim Conference on Communications, Computers and Signal Processing, 2007, pp. 292-295.

[15]. F. A.P. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Information Hiding– A Survey", Proceedings of the IEEE, special issue on protection of mutimediacontens, July 1999, pp 1062-1078.

[16]. Ron Crandall, "Some Notes on Steganography", Posted on Steganography Mailing List, 1998. Source: http://www.dia.unisa.it/~ads/corso-security/www/CORSO 0203/steganografia/LINKS%20LOCALI/matrix-encoding.pdf

[17]. Jessica Fridrich, MiroslavGoljan, DorinHogea, "Attacking the OutGuess", Proc. of 2002 ACM Workshop on Multimedia and Security, ACM Press, pp. 3-6, 2002.

[18]. Jessica Fridrich, MiroslavGoljan, DorinHogea, "Steganalysis of JPEG Images: Breaking the F5 Algorithm", Proc. of the 5th Information Hiding Workshop, Springer, vol. 2578, pp. 310-323, 2002.

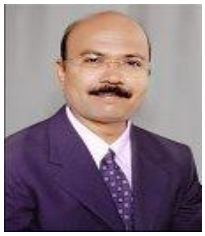
[19]. Juan José Roque, JesúsMaríaMinguet, "SLSB: Improving the Steganographic Algorithm LSB", Universidad Nacional de Educación a Distancia (Spain). Source: http://www.fing.edu.uy/inco/eventos/cibsi09/docs/Papers/CIBSI-Dia3-Sesion9(1).pdf.

[20]. R. Krenn, "Steganography and steganalysis" Internet Publication, March 2004. Available at: http://www.krenn.nl/univ/cry/steg/article.pdf

[21]. R. Chandramouli, Nasir Memon, "Analysis of LSB based Image Steganography Techniques", Proc. International Conference on Image Processing, 2001, Vol. 3, pp. 1019-1022, 2001.

Short Bio Data for the Author

Ms. Archana O. Vyas was born in Indore, Madhyapradesh in 1980. She received the B.E. Degree in Electronics and Tele-communication from S.G.B. Amravati University, Amravati in 2009 and completed her M.Tech. in Electronic Systems and Communication from Government college of Engineering Amravati in 2011. Currently she is working as Assistant Professor in Electronics and Tele communication Engg. Department at G. H. Raisoni College of Engineering & Management, Amravati. She is pursuing PhD. degree in Electronics Engineering from Sant Gadge Baba Amravati University, Amravati, India. Her interest of research is image steganography and steganalysis using computational intelligence approach.



Sanjay V. Dudul was born on 28th August 1964 at Amravati, Maharashtra. He was conferred on Ph.D. in Electronics Engineering on topic of Computational Intelligence by Sant Gadge Baba Amravati University, Amravati in 2003. He obtained B.E. degree in Electronics Engineering in 1986 from Nagpur University. He received M.E. degree in Electronics Engineering with specialization in Computer Applications in 1989. Currently, he is the Professor and Head of the Department of Applied Electronics at Sant Gadage Baba Amravati University, Amravati, India. He has published 81 research articles in peer reviewed and refereed International journals and 12 research articles in refereed National Journals. His numerous publications have been listed in SCOPUS. Hitherto, 10 students have been awarded Ph.D. degree in Electronics Engineering under his guidance. He has filed 5 Indian patents. He is a member of editorial boards of many International Journals. His research area includes Image Processing, AI in Pattern Recognition, Prediction and Regression, Machine Intelligence: A Soft-Computing Approach, Advance digital signal processing, Pattern Recognition, Analysis and Machine Intelligence, Computational Intelligence, Bio-medical Signal Processing, Intelligent/Smart Sensors and Learning Systems.