Evaluating Image Steganography Techniques: Future Research Challenges

Ratnakirti Roy[1], Suvamoy Changder[1], Anirban Sarkar[1], Narayan C Debnath[2]
[1]Department of Computer Applications, National Institute of Technology, Durgapur, India
[2]Department of Computer Science, Winona State University, MN, USA
{rroy.nitdgp@gmail.com, suvamoy.nitdgp@gmail.com, sarkar.anirban@gmail.com, ndebnath@winona.edu}

Abstract— **Steganography is the art of "concealed writing" and it refers to techniques that hide information inside innocuous looking objects known as "Cover Objects". There are different types of covers available for embedding secret information but images are pervasive in day to day applications and have high redundancy in representation. Thus, they are appealing contenders to be used as cover objects. This paper evaluates the different algorithms for digital image steganography both in the spatial and transform domain like LSB substitution, OPAP, Pixel Indicator Technique, F5 etc. and tries to put light on some possible future research directions in the topic of consideration.**

Keywords- Steganography, cover objects, LSB substitution, F5, OPAP, Pixel Indicator Technique.

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 communication. As a result a new domain dealing with security of data has evolved and is known as information hiding. Steganography is a comparatively new inclusion in the field of digital information hiding but it traces its origin to long back in history.

The word "Steganography" is derived from Greek 'Steganos" meaning hidden or concealed. Thus, "Steganography" stands for "concealed writing". Steganography is all about creating a form of secret communication between two parties and it is a complement of cryptography whose goal is to conceal the content of a message. Steganography uses a medium like an image, video, audio or text file to hide some information inside it in such a way that it does not attract any attention and looks like an innocent medium [1]. The media with and without hidden information are called stego-media and cover media, respectively [2].

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.

A typical Steganographic system is portrayed using the Prisoner's Problem [33] where two inmates Alice and Bob are hatching out an escape plan. The warden, Wendy observes communication between the two and would put them to solitary confinement if she finds them communicating secretly. Thus, Alice and Bob must communicate in such a manner that Wendy does not get to perceive their secret communication. So they need to hide messages inside innocuous objects so that Wendy cannot perceive its very existence [3].In this context, steganalysis is the set of techniques, visual or statistical, by which it is possible to check for the existence of steganographic content in a cover object. Thus, it is through steganalysis that Wendy can test for existence of a hidden message concealed in the medium of communication of Alice and Bob.

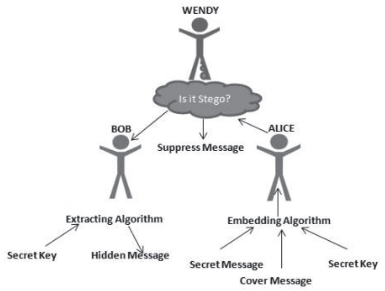

Figure 1. Graphical Representation of the Prisoner's Problem

Recently, images have been a very popular choice as a cover medium primarily because of its redundancy in representation and pervasiveness in applications in daily life [4]. Over the years, many algorithms for hiding data in images have been proposed and developing newer algorithms are a topic of current research. In this paper, few of the most popular and effective among the image steganography algorithms are analyzed for their mechanisms, merits and demerits, which might be a valuable guide to future research openings.

The remaining part of the paper is organized as follows: The next section defines some important terms related to Steganography. Further next, the contemporary algorithms which have been developed are described briefly as related research. Following to that the proposed evaluation parameters are defined. Tabular comparison of the algorithms based on the parameters defined in the preceding section and their respective techniques are presented along with discussion on the tables. This paves the way for the proposal for some possible research directions. The paper concludes in section VII.

978-1-4673-2088-7/13/$31.00 ©2013 IEEE

II. Relevant Terminologies

All image steganography systems, irrespective of the algorithms by which they are implemented adhere to the following terms.

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

(ii) 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.

(iii) Stego Image: The cover image with a secret message concealed within it is known as the *Stego* image. It is used at the recipient site for extracting the hidden message.

(iv) 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 [6] or can just be a password for decoding the embedding location.

(v) 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.

III. Related Research Works

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 available 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.

A. Spatial Domain Techniques

(i) 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 [11]. 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.

$$Y_i = 2\left\lfloor \frac{X_i}{2} \right\rfloor + m_i$$

where m_i, X_i and Y_i are the i^{th} 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 [12] context. However, LSB substitution fall 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].

(ii) Optimal Pixel Adjustment Procedure (OPAP): Originally proposed by Chi-Kwon Chan and L.M Cheng [13, 14], the OPAP scheme was developed as an improvement over the LSB based algorithm and described in [15]. 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 p_i and the pixel p_i' of the stego-image. If the difference is δ_i 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 [16].

(iii) Pixel Indicator Technique (PIT) [17]: 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 following 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.

(iv) Pixel Value Differencing: In the Pixel Value Differencing or PVD scheme [18] number of insertion bits in PVD depends on whether the pixel is an edge or a smooth area [16]. 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 [19, 20]. 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 and χ^2*-attack* [21].

(v) SLSB: The Selected LSB algorithm or the SLSB proposed in [31] embeds into single colour components of the pixels. It does not necessarily embed into the LSBs only but chooses 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 alteration 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.

B. *Transform Domain Techniques*

(i) JSteg: The JSteg algorithm is acclaimed as the first commercially available steganographic tool for JPEG images [22]. 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 χ^2*-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 [23]. However, JSteg provided an embedding capacity of 12% [25].

(ii) Outguess: The algorithm was developed by N. Provos *et al.* [23] as 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 χ^2*-attack*. However, Fridrich *et al.* [24] have successfully steganalyzed OutGuess by calculating the blockiness of the image. 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 each *8X8* block will increase.

(iii) F5: The F5 algorithm was proposed as a steganographic technique that allows higher capacity of embedding and better security at the same time [25]. 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 [26]. F5 embeds at a rate of 3.8 bits per change and is secure against most statistical attacks like the histogram attack, the χ^2*-attack*, blockiness detection etc. Moreover it has a high embedding capacity. However, F5 remained a challenging algorithm to break until Fridrich *et al.* steganalyzed F5 by estimating the original histogram of the cover image from the stego image [27]. It is done 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.

(iv) Singular Value Decomposition (SVD) transform based method (RHISSVD): The SVD based steganographic method proposed in [32] transforms the image into singular values and then embeds into them. Singular Values correspond to the luminance in the image and minor changes into 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* $\leqslant$ *60 %*. It has an average embedding capacity of 0.44 bits per singular value coefficient for an image with compression *quality 50%*.

IV. Proposed Evaluation Parameters

In order to evaluate the performance of different techniques for image steganography, it is important to define some acceptable evaluation criteria based on the quality of the objectives. Moreover, setting up specific evaluation parameters helps in leading to development of newer algorithms and also to improve the performance of the existing algorithms. Three common requirements namely level of security, capacity and imperceptibility may be used as evaluation criteria for the image steganography algorithms [7]. Apart from these we also take into consideration parameters like domain of embedding, image format and time complexity.

(i) Level of Security: There have been many approaches till date in defining the security of a steganographic system. Zollner *et al.* [8] 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-object and stego-object. These conditions, however, ensure Undetectibility against an attacker who knows the stego-object but has no information available about the in deterministic embedding operation. In [9], Cachin defined steganographic security from the information theoretic perspective. 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

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

Thus, for a completely secure stego system, *D=0* and if $D \leqslant \epsilon$, then it is ϵ*-secure*. Perfectly secure stego systems may be shown to exist theoretically but they are impractical. In short, security of a stego system is defined in terms of indefectibility. A steganographic system is said to be undetectable or secure if no statistical tests can distinguish between the cover and the stego-image [10].

(ii) Capacity: Capacity of a steganographic system implies the amount of data that can be effectively hidden within a selected cover medium by a steganography algorithm. The embedding rate is mostly given in absolute measurement (such as the size of the secret message) or in relative measurement called the data embedding rate (given mostly in bits per pixel or *bpp*, bits per non-zero DCT coefficients or *bpnc*, etc.).

(iii) 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 the stego image implies better imperceptibility.

(iv) Domain of Embedding: Domain of embedding plays a vital role in determining the overall performance of the steganographic algorithms. Spatial domain algorithms often offer higher capacity but fall prey to statistical steganalysis. Transform domain algorithms, on the other hand are more resistant to statistical steganalysis.

(v) Type of Images Supported: Images are available in a large number of formats. Thus, it is important to understand which types of images are suitable for the steganographic algorithms of the various types. Images primarily use lossy or lossless compression mechanisms and the properties of images affect the steganographic methods applicable to those images.

(vi) Time Complexity: Steganographic algorithms vary according to their 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 the algorithm for embedding into large images and also their implementation in low resource systems such as mobile devices etc.

V. EVALUATING THE ALGORITHMS

Table I shows the performance based comparison of the different algorithms of the spatial and the transform domain with respect to the parameters proposed in IV and Table II lists the embedding characteristics and the statistical deviations produced by the algorithms under consideration.

The parametric comparison of the different image steganography algorithms (Table I) reveals that the security level of the transform domain techniques are higher than that of the spatial domain algorithms. This is primarily because transform domain techniques abstain from modifying the pixels of an image directly. But at the same time spatial techniques do offer larger capacity of embedding. Algorithm such as F5 has a very low rate of bit-flipping which makes it immune to most steganalysis attacks. Spatial domain schemes are generally of low complexity in terms of their time and resource requirements. Techniques that use transforms and other statistics preserving mechanisms are inherently more complex. Spatial domain techniques work well with lossless images such as TIFF, BMP etc. but are not applicable to lossy compressed images such as JPEG/JPEG2000. Transform domain techniques however can be applied to both lossless and lossy images. This makes them more versatile with respect to the choice of image. It is also found that increase in the embedding rate compromises the fidelity of the image and hence the security level. The second table gives an idea that even the algorithms that offer high fidelity under usual circumstances do leave behind statistical signatures.

An algorithm such as OutGuess which preserves histogram after embedding also leaves *Blockiness* in the DCT groups. F5 algorithm offers a very high degree of security against majority of steganalytic methods primarily because it minimizes the necessity of overwriting bits. But, it produces shrinkage which makes it vulnerable to the calibration attack. Thus, in the light of the above discussion it may be proposed that a good steganographic algorithm should be expected to have the properties such as high fidelity, optimized embedding capacity and level of security (in terms of statistical Undetectibility), extensive image support (lossless and lossy formats), and optimized complexity allowing implementation across multiple platforms (e.g. embedding and extraction system might work on both mobile devices and PCs).

TABLE I. PARAMETER BASED COMPARISON

Domain	**Algo**	**Security Level**	**Capacity**	**Fidelity**	**Image support**	**Complexity**
Spatial	Direct LSB	Low	1-3 bpp	High	Lossless	Low
	PIT	Medium	>1 bpp	High*	Lossless	Low
	OPAP	Medium	1 bpp	High	Lossless(GS)	Medium
	PVD	Medium	>1 bpp	High$^{\$}$	Lossless(GS)	Medium
	SLSB	Medium	1-3 bpp	High*	Lossless	Medium
Transform	Jsteg	Medium	<1 bpnc	High	Lossy/Lossless	Medium
	OutGuess	High	0.4 bpnc	High	Lossy/Lossless	High
	F5	Very High	0.8 bpnc	High	Lossy/Lossless	High
	RHISSVD	Medium	0.44 bpsc	High$^{\#}$	Lossy/Lossless	High

*-*Till capacity <3 bpp*; **$**-*Till capacity < 4bpp;* **GS**-*Grayscale*; **bpsc**- *Bits per singular value coefficient*; *#-Till compression ≤ 50%*

TABLE II. MECHANISM AND DEVIATED IMAGE STATISTICS

Algo	**Mechanism**	**Deviated Statistics**
LSB	Substitute the LSB	Pair of Value in histogram
PIT	One colour channel LSB selects embedding for the remaining two.	Histogram deviation for embedding > 3 bpp
OPAP	Adjust the pixels before the embedded pixels for better visibility	Visual distortion (PSNR < 35) for embedding in the LSB>3
PVD	Embeds data in difference of neighbouring pixels (edge and smooth)	Step effect in pixel difference histogram
SLSB	Embeds data in the colour component which has maximum variation	Embedding more than 1 bpp might alter randomness of the pixels
JSteg	Substitute LSB of JPEG DCT coefficient	POV in DCT histogram
OG	Preserves order-1 stats. Of DCT histogram	Blockiness
F5	Uses Matrix Encoding, decrease coefficient abs. value	Increased zero coefficients
RHISSVD	Uses SVD transform to embed into singular value coefficients	Probable visual distortion(PSNR<35) for compression ratio >60%

VI. FUTURE RESEARCH SCOPES

The previous section provides details of how algorithms have evolved over time with respect to the nature of the cover image and the respective domains. Apart from this, the preceding section also proposes some characteristics that are extremely necessary for a good steganographic system. Incorporating all of these into a single system is itself a matter of extensive research. However, in the light of information gathered till yet, some of the possibilities of future research in the field of digital image steganography are listed below.

(i) Mathematically relating the security and the capacity: Security and Capacity trade-off is an important issue in steganography. It has been observed that increase in the capacity leads to sacrificing the security to some extent. There has not been much theoretical exploration in relating the security and capacity parameters mathematically. A mathematical model relating the two basic requirements for a steganographic system can be an area of active interest for reasons such as optimizing performance of embedding algorithms in future, development of algorithms which provide both high security and capacity despite better steganalysis and can provide mathematical basis for optimizing existing algorithms for performance. However, the difficulty in modelling the statistical features of images has perhaps prevented research from fruitfulness. This has also been pointed in [6].

(ii) Development of Algorithms based on objects in images: As the steganalysis techniques are getting stronger and eventually most steganographic algorithms are falling prey to them, there is a trend in developing algorithms which targets selective parts of images for embedding. These algorithms are called object oriented steganography [28]. The main concept of these algorithms is to identify areas in an image also known as Region of Interests (ROI) where the embedding will cause minimum distortion. One such object is human skin-tone. For example, Human skin tone falls within a threshold value in the HSV colour space ($S_{min}= 0.23,\ S_{max} =0.68,\ H_{min} =0°$ *and* $H_{max}=50°$) [29]. There are a few algorithms that focus on embedding in the human skin tone pixels. One of them, proposed in [30] uses DWT or Discrete Wavelet Transform to select the higher frequency sub band from an image in RGB format and then look for skin tone pixels in them using a skin tone detector mechanism and embed into them. But the method has some hindrances like selective embedding into human skin tone region offers security but limits capacity, overwriting of bits causes alteration in the statistical integrity of the images and can thus be detected by steganalyzers. There may be certain modifications that might be implied upon the mentioned technique like choosing colour planes with relatively low contribution to skin tone such as from blue and green from the RGB colour plane, as their component in the human skin-tone is less and thus produces less distortion. As it is shown in [25], less overwriting of bits implies lesser change in the statistical properties of the image, thus it is necessary to choose algorithms which embed data with lesser bit replacements. When ROIs objects are chosen to embed data, the space available for embedding is obviously reduced, so an algorithm that maximizes capacity is to be taken to consideration. Also, password-key may be used to seed a PRNG in order to select pixels randomly in the target plane.

The ROIs in an image is not restricted to human skin tone pixels only. Any object in an image can serve the purpose of being an ROI provided that they produce less distortion as a result of embedding. Automated systems using advances in the field of computer vision can be thought of which will identify potential ROIs from an image.

(iii) Improving the steganographic algorithms: It is observed that all steganographic algorithms, be that in the spatial domain or the transform domain (frequency domain), ultimately alter statistical properties of images and as a result of which they fall prey to statistical steganalysis techniques. Thus, it is evident that there still remains ample scope for research in developing algorithms in image steganography that will be able to provide more secure features for data hiding. We can categorize the possible improvements that might be adopted to build future steganographic systems as:

(a) Increasing embedding efficiency: Most steganographic algorithms overwrite bits (LSBs in spatial domain algorithms and LSB of DCT coefficients in the transform domain). Overwriting bits cause more alteration of the statistical properties of images and it is hence crucial to work on algorithms that have lowest overwriting. The F5 algorithm [25] is a trend setting example. However, statistical properties of images change when they are modified after their creation. If secret data bits are embedded into the image during its very creation, it is possible to produce stego images resistant to blind steganalysis.

(b) Decreasing embedding distortion: Improving the security of steganographic algorithms also includes decreasing the amount of distortion produced by the embedding algorithm. One way of distortion minimization is by adjusting the statistical properties of the image after embedding to preserve the original characteristics. This however should be dealt with care as it is shown in [24] that statistics preserving algorithm OutGuess itself leaves detectable marks during the modification process resulting in *blockiness*. So, statistics preserving techniques must be carefully developed so that the adjustments are not sensitive to statistical steganalysis. One possibility can be to embed into pixels without overwriting their bits. This can be done by altering the value of the pixel component itself in such a manner that the alteration corresponds to the message to be hidden and can also be used for later extraction. In the case of embedding into transform coefficients, modification must be done into coefficients which have lowest distortion for modification. However, it is applicable only when all coefficients are not utilized. Similarly, perturbed quantization based schemes can also be used for decreasing the embedding distortions [10].

(c) Choosing alternate colour spaces: The majority of the available image steganographic schemes use the RGB or the grey scale images. It has been observed that colour spaces like the HSV (Hue Saturation Value) and the YCbCr (Yellow Blue-Chromaticity Red-Chromaticity) colour spaces have a particular property that is quite useful for steganographic purposes. Embedding in the Hue component of HSV colour space or the Yellow (Luminosity) component of the YCbCr colour space creates much less distortion as change in the mentioned colour space can deceive human visual system better. Moreover, embedding in the luminance component can provide more resistance to cropping and other accidental or intentional distortions. There are many more colour spaces like *UVW, LSLM, L*a*b*, L*u*v*, LHC, LHS, HSI, YUV, YIQ*

[28]. The suitability of these colour spaces for steganographic purposes are yet to be explored to the full.

VII. Conclusion

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

Future work will concentrate on the formal definition and enhancement of the proposed set of evaluation criteria towards the evaluation of image steganography algorithms.

References

[1] T Morkel, J.H.P Eloff, M.S Olivier, "AN OVERVIEW OF IMAGE STEGANOGRAPHY". Proceedings of the Fifth Annual Information Security South Africa Conference (ISSA2005), 2005.

[2] Birgit Pitzmann, "Information hiding terminology-results of an informal plenary meeting and additional proposals", Proc. of the First International Workshop on Information Hiding, vol. 1174, pp.347-350. Springer, 1996.

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

[4] Bin Li, Junhui He, Jiwu Huang, Yun Qing Shi, "A Survey on Image Steganography and Steganalysis", Journal of Information Hiding and Multimedia Signal Processing, Vol.2, Issue 2, pp. 142-172, April 2011.

[5] Neil F. Johnson, Stefan C. Katzenbeisser, "A Survey of Steganographic Techniques", Information Hiding Techniques for Steganography and Watermarking, edited by Stefan Katzenbeisser and Fabien A.P. Petitcolas, pp. 45, Artech House Inc, 2000.

[6] Mehdi Kharrazi, Husrev T. Sencar, Nasir Memon, "Image Steganography: Concepts and Practice", WPSC/Lecture Note Series, pp. 3, April, 2004. Source: www2.ims.nus.edu.sg/preprints/ab2004-25.pdf

[7] Ingemar J. Cox *et al.*, Digital Watermarking and Steganography, pp.36-41, Second Edition, Morgan Kaufmann, Burlington, USA, 2008.

[8] J. Zollner, H. Federrath, H. Klimant, A. Pitzman, R. Piotraschke, A. Westfeld, G. Wicke, and G. Wolf, "Modeling the security of steganographic systems," 2nd Information Hiding Workshop, pp. 345-355, April 1998.

[9] C. Cachin, "An information-theoretic model for steganography," Proc. 2nd International Workshop Information Hiding LNCS 1525, pp. 306–318, 1998.

[10] Jessica Fridrich, Tomáš Pevný, Jan Kodovský, "Statistically Undetectable JPEG Steganography: Dead Ends, Challenges and Opportunities", Proc. 9th Workshop on Multimedia and Security,2007, pp. 3-14, ACM, New York, USA.

[11] W. Bender, D. Gruhl, N. Morimoto, and A. Lu, "Techniques for data hiding", IBM System Journal, vol. 35, no. 3, pp. 313-336, 1996.

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

[13] 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.

[14] Chi-Kwong Chan, L.M. Cheng, "Hiding data in images by simple LSB substitution", Pattern Recognition, Vol.37, pp. 469-474, 2010.

[15] RAN-ZAN WANG, CHI-FANG LIN, and JA-CHEN LIN: 'Hiding data in images by optiinal moderately-significant-bit replacement', IEE Electron. Lett., 2000, 36, (25), pp. 2069-2070.

[16] 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.

[17] 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.

[18] 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.

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

[20] 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.

[21] Vajiheh Sabeti, Shadrokh Samavi, Mojtaba Mahdavi, Shahram Shirani, "Steganalysis of Pixel-Value Differencing Steganographic Method", Proc. IEEE PacificRim Conference on Communications, Computers and Signal Processing, 2007, pp. 292-295.

[22] N.Provos, P.Honeyman, "Hide and seek: an introduction to steganography", IEEE Security and Privacy, 1(3)(2003)32–44.

[23] A. Cheddad, J. Condell, K. Curran and P. Mc Kevitt, "Digital Image Steganography: Survey and Analyses of Current Methods", Signal Processing, Volume 90, Issue 3, Pages 727-752, March 2010.

[24] Jessica Fridrich, Miroslav Goljan, Dorin Hogea, "Attacking the OutGuess", Proc. of 2002 ACM Workshop on Multimedia and Security, ACM Press, pp. 3-6, 2002.

[25] A. Westfeld, "F5-A Steganographic Algorithm: High capacity despite better steganalysis," Proc. 4th International Workshop on Information Hiding., 2001, vol. 2137, pp. 289-302, Springer, 2001.

[26] 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

[27] Jessica Fridrich, Miroslav Goljan, Dorin Hogea, "Steganalysis of JPEG Images: Breaking the F5 Algorithm", Proc. of the 5th Information Hiding Workshop, Springer, vol. 2578, pp. 310-323, 2002.

[28] A. Cheddad, J. Condell, K. Curran and P. Mc Kevitt, "Biometric inspired digital image Steganography", Proceedings of the 15th Annual IEEE International Conference and Workshops on the Engg.of Computer-Based Systems (ECBS'08), Belfast, 2008, pp. 159-168.

[29] K. Sobottka, I. Pitas, "Extraction of facial regions and features using color and shape information.", Proc. IEEE International Conference on Image Processing, pp. 483-486, 1996.

[30] Anjali A. Shejul, Umesh L. Kulkarni, "A Secure Skin Tone based Steganography Using Wavelet Transform", International Journal of Computer Theory and Engineering, Vol.3, No.1, pp. 16-22,February, 2011.

[31] Juan José Roque, Jesús María Minguet, "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.

[32] K S. Babu, K B Raja, U. M. Rao, Rashmi K A, Venugopal K R, L M Patnaik, "Robust and High Capacity Image Steganography using SVD", IET-UK International Conference on Information and Communication Technology in Electrical Sciences, 2007, pp. 718-723.

[33] G. Simmons, "The prisoners problem and the subliminal channel", CRYPTO, pp. 51-67, 1983.