Analysis of Image Steganography Techniques: A Survey

Pooja Rai
M.Tech Student,
Department of CSE, Sikkim
Manipal Institute of Technology,
Sikkim Manipal University,
Sikkim

Sandeep Gurung
Associate Professor
Department of CSE,Sikkim
Manipal Institute of Technology,
Sikkim Manipal University,
Sikkim

M.K. Ghose
Dean (Academics),
Department of CSE, Sikkim
Manipal Institute of Technology,
Sikkim Manipal University,
Sikkim

ABSTRACT

Steganography is the technique of hiding data in an appropriate multimedia carrier, e.g., image, audio, and video files known as Cover. Images are mostly used as the cover medium due to their pervasiveness in different applications and representation with high redundancy. This paper provides a review and analysis of many existing methods for digital image steganography in the spatial as well as transform domain. The performance evaluation of the algorithms with respect to the proposed analysis parameters are summarized along with their limitations inorder to throw some light on the utility of the algorithm as per the requirement of application.

General Terms

Steganography

Keywords

Cover, Steganography, Stegos, grafia, blockiness

1. INTRODUCTION

In today's world internet plays a vital role in data communication providing cheaper and fastest way of data transmission over the web. However, demand for the security of data over the internet still exists. The data transmitted via the World Wide Web consists of many kinds of data i.e. casual data as well as confidential details like medical diagnostics, financial, credentials and military data. Hence there may be threat to the confidentiality of sensitive information for which there should be some mechanism to safeguard the contents of the data. Inorder to keep the integrity of data intact cryptography is one of the data hiding techniques that conceals the secret information by scrambling the contents. Unlike cryptography, steganography is another data hiding technique that safeguards the secret information by the use of a medium to conceal the very existence of the secret information which can be revealed only by the deliberate receiver. Steganography is a technique having its origin since decades but its inclusion in the digital information hiding is rather novel. Unlike cryptography (which uses the concealment of secret information) steganography uses a cover medium to conceal the existence of the secret information [2]. Data hiding can be achieved with the steganography and cryptography implemented together resulting in greater data security as well as data integrity.

The word Steganography consists of the word Stegos in Greek which means hidden and grafia means writing thus leading to secret writing [22, 25]. Steganography is a hide and seek method of communication in which the secret information is concealed inside the cover medium by the sender such that even if the adversary seeks, the hidden information is not revealed. Moreover, the cover medium looks innocuous even after the secret embedding [22]. Due to its popularity in applications, images have been a very accepted choice as a cover medium amongst all the existing media. Embedding of secret information direct into the pixel values of the cover image is done in spatial domain steganography whereas in transform domain based steganography, the cover image is firstly converted into frequency domain using some mathematical transformation and then the embedding is done into the transformed coefficients. In yester years, research on image based data hiding has been carried out extensively resulting in the development of various new techniques. In this paper, few of the most popular and efficient among the image steganography techniques are taken for analysis to have a look at the pros and cons of each, which may lead to further enhancement as well as the incorporation of the existing techniques to develop the more efficient algorithms.

Simmons et al. [1] have given a basic steganographic system using the Prisoner's Problem where two inmates Alice and Bob are hatching out an escape plan [22]. Figure 1 depicts an overall structure of steganography [22]. Image is the most often used file format for steganography and is only discussed here where the secret message is embedded in cover image. Applications of steganography include copyright control of data, improving the image search engines' robustness and smart id's, feature tagging, secret communication, video-audio synchronization, TV broadcasting, TCP/IP packets etc. [11,12]. The contents of this paper are organized as follows: Section 2 defines some important terms related to steganography. The different types of steganography and the related research works are defined in section 3 and section 4 respectively. Section 5 discusses the proposed evaluation parameters. Tabular comparison of the algorithms based on the parameters defined in the preceding section and their respective mechanism are presented along with discussion in the section 6. This provides the direction towards the probable research works in the field of data hiding. The conclusion is given in the section 7.

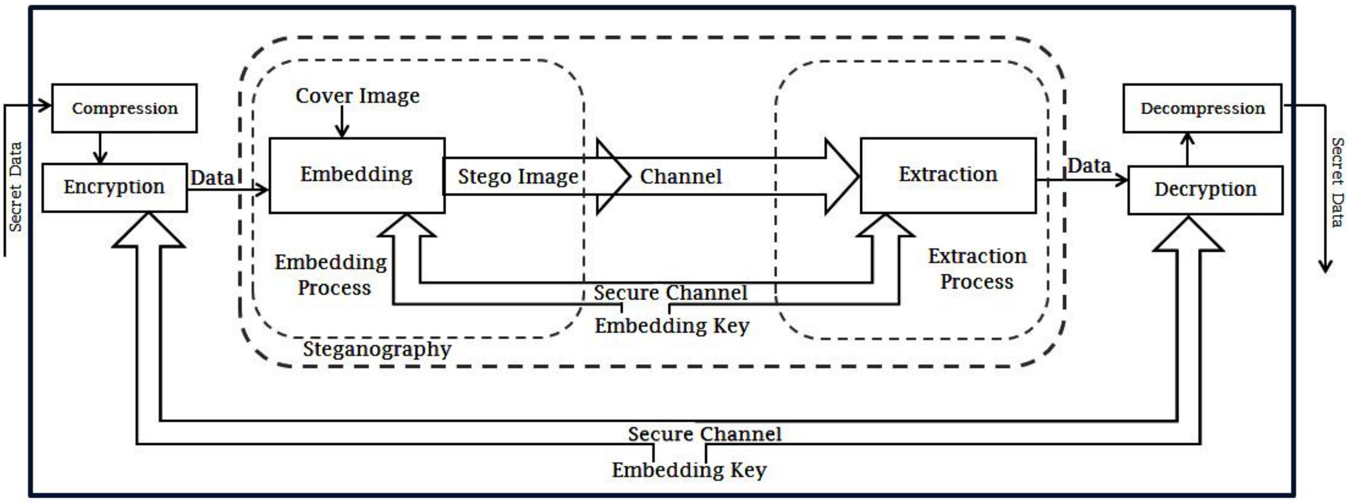


Figure 1: General model of Steganography [25]

2. RELEVANT TERMINOLOGIES

The basic terms related to the digital image steganography are as follows:

2.1 Image: An image represents the visual perception (of an object, scene, person or abstraction). An image I is a discrete function which assigns a color vector c(i, j) to the pixel (i, j) [3].

2.2 Cover Image: The image used for carrying the secret information in a secure manner is known as cover image. It is used by the sender to embed the required information.

2.3 Stego Image: The cover image after the embedding of the secret information in it is known as the stego image. It has the least possible visual difference to that of the cover image. It is required by the receiver to reveal the secret information.

2.4 Stego Key: The key to entrench data in a cover which is again used to retrieve the data embedded is known as stego key. It may be a number generated by a pseudo-random number generator [12] or can be a password for finding out the potential locations of embedding.

2.5 Embedding Domain: The characteristics of the cover medium which are exploited for secret information embedding is known as embedding domain. The domain may be spatial or frequency domain. In the spatial domain, the secret embedding is done directly into the cover whereas in frequency domain or transform domain, carrier medium is firstly transformed into frequency domain and then the secret embedding is carried out with the transformed contents of the cover (eg. frequency coefficients).

2.6 Peak Signal to Noise Ratio (PSNR): It measures the quality of a stego image. This performance metric is used to determine perceptual transparency of the stego image with respect to host image [21].

PSNR = $\frac{\mathrm{MN}\ \max_{x,y}\ \mathrm{P}_{x,y}^{2}}{\sum_{x,y}\left(\mathrm{P}_{x,y} - \overline{\mathrm{P}}_{x,y}\right)^{2}}$ Where, M and N are number of rows and columns in cover image, $\mathrm{P}_{x,y}$ and $\overline{\mathrm{P}}_{x,y}$ are the pixels of original image and the stego image respectively.

2.7 Bit Error Rate: Bit Error Rate (BER) is used to measure the error while retrieving the secret information. This error occurs due to the lack of an ideal channel for communicating the secret information among the sender and intended receiver [21]. The cover image is represented as covg and stego image as steg in the given equation: where i is the pixel position.

BER = $\frac{1}{\mathrm{image}^{\ \mathrm{covg}}} \sum_{\mathrm{i}=0}^{\mathrm{all\ pixels}} |\mathrm{image}^{\mathrm{covg}} - \mathrm{image}^{\mathrm{steg}}|$

3. IMAGE STEGANOGRAPHY TYPES

The prominent objective of digital image steganography is to conceal the secret information inside the cover image with least visual distortion and maximum possible embedding capacity to achieve secret communication. Inorder to achieve so, large number of research activities has taken place in the field of digital image steganography which has led to the different types of steganography. Hence, image steganography can be generally categorized into spatial domain, transform domain or frequency domain and model-based steganography.

3.1 Spatial Domain based Steganography

This technique involves the direct modification of the contents (pixel values) of the cover image to embed the secret information. Ease in the implementation and high embedding capacity are the attractive features of this technique. But this technique is less immune to image processing operations and susceptible to stego attacks.

3.2 Transform domain based Steganography

A digital image consists of two types of frequency namely, high frequency and low frequency. Low frequency represents smooth and plane areas whereas edges are represented by high frequency values. Unlike high frequency regions, changes in the low frequency regions are apparent to the Human Visual System (HVS) and there is a strong correlation among the pixel values of low frequency regions [25]. Hence, regions of high frequency are preferable than that of the low frequency. In transform domain technique, the transformation of pixel values into the frequency coefficients is done using any of the transforms such as Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) etc. The secret information is then embedded into the coefficients. Transform domain methods are more immune to image processing operations and less susceptible to stego attacks. Hence, they are preferred over the spatial domain based techniques [25].

3.2 Adaptive Steganography

Adaptive steganography is another category of steganography which is a special case of two former methods [17]. It was first proposed by P. Sallee [9] in 2003 based on some statistical properties of the cover medium. It is also known as ‘‘Statistics-aware embedding’’ [10] or ‘‘Model-Based’’ [9]. Prior to embedding this method finds out the potential locations for embedding into pixel value or frequency coefficients by taking statistical global features of the image either in spatial or frequency domain. This novel technique helps to embed the secret message with additional layer of security, robustness and high capacity with acceptable perceptual transparency.

4. RELATED RESEARCH WORKS

4.1 Spatial Domain Steganography

Spatial domain based steganography is the simplest of data hiding techniques by simply modifying the pixel values of the cover image.

4.1.1 Least Significant bit substitution (LSB) method: The basic idea of LSB substitution technique is to embed the secret information at the rightmost bits of a pixel (bits with the smallest weight) randomly, without affecting the original pixel value significantly. LSB substitution affects pixels by ±1, that is, the distortion produced by the mechanism is perceptually transparent [6]. This method is the easiest one but it is vulnerable to signal processing or noises as well as image processing operations such as cropping, scaling etc. Steganalysis of LSB embedding is easily done due to PoVs (Pair of Values) in the image [11].

4.1.2 Pixel Indicator Technique (PIT): In order to enhance the security of the existing LSB scheme, Pixel Indicator Technique was developed [20].The use of 24-bit/pixel color images is done where two LSB of one channel indicates the presence of data in the other two channels. For choosing the selection channel, key is derived from the size of secret data. The two channels (indicator channel and the embedding channel) are ordered in the following way: RGB, RBG, GBR, GRB, BRG, and BGR. PIT produces very low visual distortion when the embedding rate is less than 3 bits thus low vulnerable to histogram and visual attacks.

4.1.3 Optimal Pixel Adjustment Procedure (OPAP): The OPAP is an improvement over the LSB based algorithm [4]. The improvement is done by calculating the pixel differences between original pixel and the pixel of the stego-image. The OPAP scheme modifies the embedded bits in order to improve the overall visibility of the stego image [18].OPAP provides high PSNR values (55.96 and 56.71) for standard test images Baboon and Lena [19].

4.1.4 Secure Key Based Image Realization Steganography [23]: Instead of embedding the secret information directly into the cover image, image realization has been proposed in this paper. Embedding of some mapping information related to the secret information into the cover image is done using Matrix Encoding Technique and the realization of the secret is done using a highly secured pass key. Mapping of secret message, key generation and the embedding are done in the first phase followed by the extraction procedure in the next phase. One of the planes (red plane in [23]) of RGB image is used for creating the mapping matrix. The selected plane (C_i) is represented as the multiples of secret image and divided into different blocks. The difference of the secret image and the blocks of the selected plane is calculated to create the mapping matrix. The block of mapping matrix having minimum difference with Ci is then embedded into the other two planes of the cover image. The key is being generated using pairing function. The embedding procedure is given in the figure below, where C_i is any one of the planes namely red plane (C_r), green plane (C_g) and blue plane (C_b). S denotes the secret information. The mapping operation is mathematically expressed as $C_{min} \otimes S=M$, where M is the mapping matrix, C_{min} is the block in C_i with minimum difference with S and $\otimes$ is the mapping operator used which may be any discrete operator or any function used for mapping.

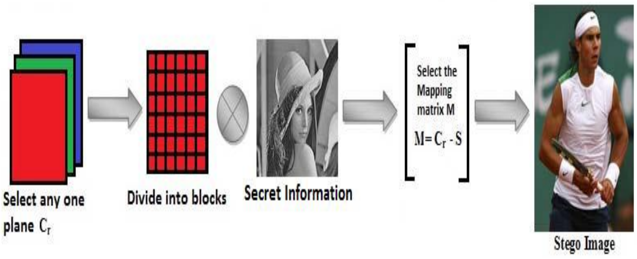


Figure 2: Map Generation Technique [23]

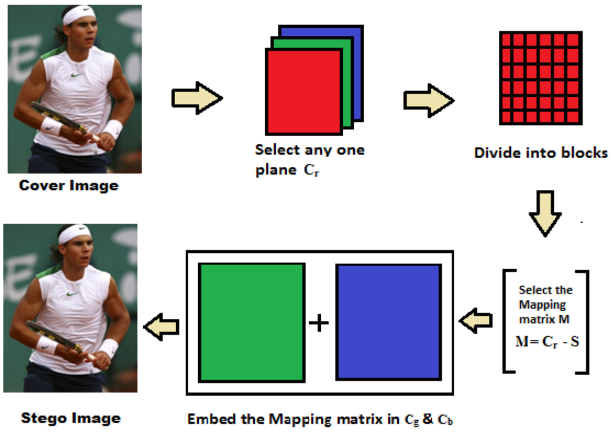

Cover Image
Select any one plane C_r
Divide into blocks
Select the Mapping matrix M
$M= C_r - S$
+
Stego Image
Embed the Mapping matrix in C_g & C_b

Figure 3: Embedding Mechanism [23]

The extraction procedure is just the reverse of embedding algorithm. The size of the secret information and the location of the matrix are extracted from the key and the retrieval of secret information is done by finding the difference between the matrix got from the key and the original matrix value. This technique is secure against Brute Force attack since the decoding key has a sufficiently large key space [23]. High securities against statistical attacks as well as histogram attacks are also the achievements of this method.

4.1.5 Image Realization Steganography with LCS based Mapping [26]: As an enhancement over the technique discussed in [23] a new cover-secret mapping technique is developed by Ratnakirti Roy and Suvamoy Changder taking secret information as a Least Common Subsequence (LCS) of the cover image for mapping. The Longest Common Subsequence (LCS) problem is as follows: Given two strings S of length n, and T of length m, the goal is to produce their longest common subsequence: the longest sequence of characters that appears left-to-right (but continuity is not mandatory) in both strings. For example, consider S = ABAZDC and T = BACBAD. In this case, the LCS has length 4 and is the string ABAD. This can be found out using the following process: let us consider LCS[i,j] is the length of the LCS of S[1..i] with T[1..j].The solution for LCS[i,j] in terms of the LCS's of the smaller problems is given as follows:

$$\mathrm{LCS}[i, j] = \begin{cases} \max(\mathrm{LCS}[i-1, j], \mathrm{LCS}[i, j-1]), \text{ if } S[i] \neq T[j] \\ 1 + \mathrm{LCS}[i-1, j-1], \text{ if } S[i] = T[j]. \end{cases}$$

In [26], the map generation is done by choosing one of the planes (RGB) of the cover image and the other two are used for the embedding of the secret information, if any. The LCS of the secret image is taken row-wise. If the mapping between the cover image and the secret information is not complete then the embedding is required. Map generation phase creates two maps, one containing the information required for secret-cover mapping and the other one containing the information required for extraction if some secret information is embedded (the number of bits embedded for each row of the secret image). The latter map will be empty if the row of secret image is completely found as a LCS of cover image i.e. whole of the secret information is mapped as cover image's LCS. These maps are used in the receiver side to realize the secret information along with the key (composed of the number of rows, number of columns and bit depth of secret image) generated by the integer pairing function [26].The mapping level of this method is very high because the length of the binary string representation of the cover image is quite larger than the length of the binary string corresponding to each row of the secret image and each of these binary strings are random in nature. The strength of the key used in this method is very high since the probability of decoding the key correctly is very small. Hence the method is highly secure against the Brute-Force attacks. As shown in [26], the complete mapping of the secret image to the cover image is possible thus achieving the higher payload carrying capacity than the existing steganography technique. However, the map is not embedded into the cover image since it reduces the realization capacity. Inorder to make the secret more secure, it has to be revealed by using key in addition to the maps generated thus making the existence of any one of them useless. Thus, this method enhances the technique discussed in [23] by avoiding the map embedding into the cover image thus increasing the hiding capacity.

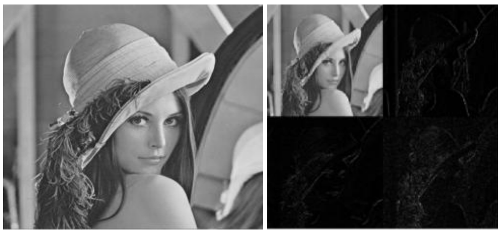
4.2 Transform Domain Steganography

4.2.1 JSteg: The JSteg algorithm is the first commercially available steganography tool for JPEG images [10].The algorithm applies Discrete Cosine Transform (DCT) to the 8X8 image blocks and serially embeds the data into LSBs of the DCT coefficients. JSteg provided an embedding capacity of 12% [4]. However, it is steg-analyzed using the χ2-attack. The DCT coefficients should be handled with extreme care in order to prevent the algorithm from leaving major statistical signatures [17].

4.2.2 Outguess: The algorithm improves the existing JSteg algorithm [17]. The pixels are randomized before embedding using a PRNG (Pseudo Random Number Generator) and DCT coefficients with values 0 and 1 are ignored because a Pair of Value is formed by them when their LSB changes. The DCT coefficients which are not used for embedding are used to preserve the histogram of the original image. Though this algorithm is immune to attacks like the visual attack, histogram attack and the χ2-attack, Fridrich et al. [7] have successfully steg-analyzed Outguess by calculating the blockiness of the image. Though this algorithm preserves histogram even after embedding, blockiness results in the DCT groups [22].

4.2.3 F5: The F5 algorithm achieves higher embedding capacity as well as better security [4] and it is the first implementation of the matrix encoding method proposed in [2] .Unlike other steganography algorithm overwriting of the LSBs of DCT coefficients are not done since doing so alters the statistical properties of the image leaving it vulnerable to many attacks rather it increment/decrement the value of the DC coefficients depending on need. 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 because it minimizes the necessity of overwriting bits. However, Fridrich et al. estimated the cover image histogram from the stego image thus making F5 detectable [8]. It is done by decompressing the stego-image to spatial domain. Cropping is done by 4 pixels in both directions followed by recompression using the same quality factor as the stego image [22]. Due to shrinkage production this algorithm is susceptible to the calibration attack [22].

4.2.4 A DWT Based Approach for Image Steganography [14]: In this algorithm, coefficients in the low frequency sub-band are preserved unaltered to keep the image quality intact thus embedding only in the coefficients in the high frequency sub-bands. Some basic mathematical operations are performed on the secret messages before embedding. The proposed scheme is classified as varying mode and fix mode. In varying mode, there is no specific range for the capacity whereas fix mode has a specific range for required capacity. A secured key matrix is made with some mapping rule so that even if the key matrix is found by the adversary, without knowing its mapping rule it is impossible to decode the secret information.



(a) **(b)**

Figure 4: (a) Lena image, (b) Image after the first-order 2-D Haar-DWT [14]

The visual distortion is satisfactory even the highest capacity case is applied because DWT gives multi-resolution characteristics of coefficients in different sub-bands.

4.2.5 A Session based Multiple Image Hiding Technique using DWT and DCT [21]: Tanmay Bhattacharya et al. [21] have proposed this work for hiding three secret images into the Red, Green and Blue (RGB) planes of a color image by transforming each plane from spatial domain to frequency domain. The Discrete Wavelet Transform (DWT) is used to first divide each plane into four sub-bands and the selected Discrete Cosine Transform (DCT) coefficients of the diagonal sub-bands of each plane are used for the secret embedding by using pseudo random sequence and a session key. The secret extraction is done by the session key and the size of the images by decomposing the stego image into different planes. Due to random embedding in the frequency domain this approach is immune to conventional steganalysis methods.

4.2.6 Secret Data Hiding in Images by using DWT Technique's [24]:

This is a Skin Tone based Secret Data hiding in images by using Haar Wavelet [24]. It is an object-based steganography technique in which the high frequency sub-bands of the human skin tone region of the cover image is used for embedding secret information. Data within skin tone region are not much sensitive to Human Visual System (HVS). So embedding is done in the skin tone region. Firstly, the skin tone detection is performed using HSV (Hue, Saturation and Value) color space followed by the cropping of the skin tone region. Cover image is transformed in frequency domain. Finally secret data embedding is performed in one of the high frequency sub-bands by tracing skin pixels in that band. Instead of whole image, the secret embedding is done only in the cropped region. Cropping of the skin tone region is done inorder to achieve high security and it works as a key for secret extraction in the recipient side.

5. ANALYSIS PARAMETERS

It is important to have some criteria for analysis of the different image steganography techniques in order to bring improvement in the existing algorithms or to introduce novel algorithms. Following are the different analysis parameters that are used to analyze different steganography techniques.

5.1 Invisibility (Perceptual Transparency):

Perceptual Transparency ensures that the visual quality of the cover medium remains intact. This concept is based on the properties of the human visual system. If an average human subject is unable to distinguish between carriers containing hidden information and those that do not, then the embedded information is undetectable. It is important that the embedding occurs without a significant degradation or loss of perceptual quality of the cover.

5.2 Hiding Capacity:

The amount of information concealed, relative to the cover image size with acceptable distortion. The embedding rate is given as the size of the secret message or in bits per pixel or bpp, bits per non-zero DCT/DWT coefficients or bpnc, etc [24].

5.3 Robustness:

It is the ability of the embedded data to remain intact if the stego image undergoes transformation due to intelligent stego attacks or any image processing task.

5.4 Security:

This refers to adversary's inability to detect the concealed information. A steganography system is said to be secure if no statistical tests can make a distinction between the cover and the stego-image [24].

5.5 Embedding Domain:

Inorder to provide the different level of security the domain of cover image for embedding is important. Spatial domain based algorithms are simple and provide high capacity but the level of security is poor whereas the domain based algorithms provide the second level of security with limited capacity.

5.6 Time Complexity [22]:

The effort required for the different techniques vary according to the type of steganography. The spatial domain based methods are less time consuming as compared to the domain based methods. This parameter is helpful in finding out the applicability of a particular technique as per the need.

6. ANALYSIS OF THE ALGORITHMS

The evaluation of the different algorithms based on the evaluation parameters mentioned in the section 5 of this paper is shown in the table 1. Table 2 shows the mechanisms and the limitations of the mentioned algorithms.

Table 1. Comparison of Steganography Techniques [22]

Domain	Algorithm	Invisibility	Capacity	Robustness	Security	Complexity
Spatial	LSB	High	1-3bpp	Low	Low	Low
	PIT	Medium	>1 bpp	Low	High#	Low
	OPAP	Medium	1 bpp	Low	High	Medium
	ShabnamSamima et al. [23]	Very High	2bpp [23]	High	High	Medium
	Ratnakirti Roy et al. [26]	Very High	NA*	High	High	Medium
Transform	JSteg	Medium	<1 bpnc	Medium	High	Medium
	Outguess	High	0.4 bpnc	Medium	High	High
	F5	Very High	0.8 bpnc	Medium	High	High
	Po-Yueh Chen et al. [14]	Medium	<1 bpnc	High	High	Medium
	Tanmay Bhattacharya et al. [21]	High	<1 bpnc (3 secret images per cover image)	Medium	High	Medium
	SwapnaliZagade et al. [24]	High	<1 bpnc	High	High	Medium

#-Till capacity < 3 bpp. *- capacity varies on the degree of mapping; it cannot be calculated in bpp. bpp- bit per pixel, bpnc- bit per non-zero coefficient.

Table 2. Mechanisms of Algorithms with Limitations [22]

Algorithm	Mechanism	Limitation
LSB	Substitute the LSB	Pair of Value in histogram
PIT	One color 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
JSteg	Substitute LSB of JPEGDCT coefficient	POV in DCT histogram
Outguess	Preserves order-1 stats. Of DCT histogram	Blockiness
F5	Uses Matrix Encoding, decrease coefficient absolute value	Increased zero coefficients
Po-Yueh Chen et al. [14]	Uses Key Matrix and decoding rules	Visual distortion for large Key Matrix(extra data in the stego-image)
Tanmay Bhattacharya et al. [21]	Embedding into the DCT coefficients of high frequency band of Red, Green and Blue planes.	Constraint on the secret image size
Swapnali Zagade et al. [24]	Embedding into the coefficients involving the skin pixels of high frequency sub-bands of Green and Blue layers	Extraction quality differs with different types of Wavelets
Shabnam Samima et al. [23]	Secret information is mapped in a matrix using one of the planes (RGB) and embedding of mapping information into the other two planes is done using Matrix Encoding Technique[23]	One of the planes out of the three planes is unused which hampers the capacity
Ratnakirti Roy et al. [26]	The cover-secret map representing the secret image as the Least Common Subsequence of the cover image is created along with key and the auxiliary map containing the secret embedding information (if any).	Overhead of handling map along with the cover image. Iterative method of finding LCS for large secret image may hamper the performance of the technique

The above comparison of the different steganography techniques (Table 1) depicts that the spatial domain based techniques are prone to various statistical attacks though they have good carrying capacity. Transform domain based techniques are more secure than the spatial domain based techniques since the former provides additional layer of security by transforming the original contents of the secret image into a different form. However, the image realization techniques in the spatial domain prove that working with spatial domain is worth to have high carrying capacity, security as well as robustness with acceptable computational overhead.

7. CONCLUSION

This paper presented a background discussion on the major algorithms of digital image steganography considering the spatial domain and transform domain. For small payload, emerging techniques based on DCT, DWT are not easily susceptible to attacks because they alter coefficients in the transform domain, keeping the image distortion as minimum as possible. Usually these methods have a lower embedding capacity compared to spatial domain algorithms but they are more immune to attacks than that of spatial domain based methods. However, ease of implementation is the most attractive feature of the spatial domain based methods. Digital image steganography is a considerably new research area in the field of information hiding. Many significant researches have been done in this field. One of the most significant techniques is the realization of hidden information from the cover image without actually having secret embedding and is known as Image Realization. It is a good alternative to the encryption schemes where there is no concept of pre-embedding encryption and the actual secret embedding. However, many research issues are yet to be explored. This can be achieved by exploring more on adaptive based as well as object based methods. Enhancement of the proposed set of assessment criteria towards the analysis of image steganography algorithms will be the future work.

8. REFERENCES

[1] G. Simmons, The Prisoners problem and the subliminal channel, CRYPTO, pp. 51-67, 1983.

[2] 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

[3] 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.

[4] 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.

[5] 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.

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

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

[8] 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.

[9] P. Sallee, Model-based steganography, in: Proceedings of the Second International Workshop on Digital Watermarking, Seoul, Korea, October 20–22, 2003, Lecture Notes in Computer Science, vol. 2939, pp. 254–260.

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

[11] 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

[12] Mehdi Kharrazi, Husrev T. Sencar, Nasir Memon, Image Steganography: Concepts and Practice, WPSC/Lecture Note Series, pp.3, April, 2004.

[13] 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.

[14] Po-Yueh Chen and Hung-Ju Lin, A DWT Based Approach for Image Steganography. International Journal of Applied Science and Engineering 2006. 4, 3: 275-290

[15] N.-I. Wu, M.-S. Hwang, Data hiding: Current status and key issues, Int. J. Netw. Secur. 4 (2007) 1–9.

[16] 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.

[17] A. Cheddad, J. Condell, K. Curran and P. McKevitt, Digital Image Steganography: Survey and Analysis of Current Methods, Signal Processing, Volume 90, Issue 3, pp. 727-752, March 2010.

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

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

[20] 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.

[21] Tanmay Bhattacharya, Nilanjan Dey, S. R. Bhadra Chaudhuri, A Session based Multiple Image Hiding Technique using DWT and DCT, International Journal of Computer Applications (0975 – 8887) Volume 38– No.5, January 2012

[22] Ratnakirti Roy, Suvamoy Changder, Anirban Sarkar, Narayan C Debnath.Evaluating Image Steganography Techniques: Future Research Challenges.2978-1-4673-2088-7/13/$31.00 ,2013, IEEE

[23] Shabnam Samima, Ratnakirti Roy, Suvamoy Changder. Secure Key Based Image Realization Steganography in Image Information Processing (ICIIP), 2013 IEEE Second International Conference on 01/2013 pp.377-382

[24] Swapnali Zagade, Smita Bhosale, Secret Data Hiding in Images by using DWT Technique's . International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-3, Issue-5, June 2014

[25] Mansi S. Subhedara, Vijay H. Mankarb. Current status and key issues in image steganography: A survey. COMPUTER SCIENCE REVIEW 13–14 (2014) 95–113

[26] Ratnakirti Roy, Suvamoy Changder. Image Realization Steganography with LCS based Mapping. Proc. Contemporary Computing (IC3), 2014 Seventh International Conference. ISBN: 978-1-4799-5172-7, pp. 218 – 223, August 2014, IEEE