Volume 4, Issue 6, June 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Review of Digital Image Steganography Techniques

Swapnil S. Thakare*
PG Student,
Department of Computer Engineering,
MCOERC, Nashik,
Pune University, India

Niranjan L. Bhale
Professor, Head
Department of Information Technology,
MCOERC, Nashik,
Pune University, India

Abstract— Steganography can be defined as the study of invisible communication that usually deals with the ways of hiding the existence of the communicated message. Steganography is now more important due to need of secure communication in this era of potential and vulnerable computer users. Generally data embedding is achieved in text, image, audio, video, network for the purpose of secret communication. It has application in the area of copyright, military communication, authentication and many other purposes. In this paper we have analyzed various steganographic techniques secret communication is achieved to embed a message into cover image and generate a stego-image.

Keywords— Adaptive pixel pair matching (APPM), Data hiding, Least significant bit (LSB), Optimal Pixel Adjustment Process (OPAP), Steganography.

I. INTRODUCTION

As need of Internet-based applications is highly increased, so it is required to use the secrecy in communication. To achieve this goal, there are mainly three techniques are available, cryptography, watermarking and steganography. Steganography is the art of hiding information through original object/carrier in such a manner that the existence of the message is unknown. The term steganography is comes from Greek word Steganos, which means, "Covered Writing". The original objects can be referred to as covered/carrier objects. After inserting the secret message in to the cover image it is called as stego image. A stego key is used for hiding. [5], [6]

Steganography is different from cryptography. The main objective of cryptography is to secure communications by using encryption techniques. But steganography techniques are used to hide the messages, which makes difficult for a third party / person to find out the message. [5], [6] Watermarking and fingerprinting related to steganography are basically used for intellectual property protection [5], [6].

Making the throughout observation of history there have been two major types of steganography, technical and linguistic. Technical steganography is more based upon scientific methods of hiding information while linguistic employs more creative and non-apparent methods [5], [6]. Linguistic steganography utilizes more openly visible methods of hiding information that depend on manipulation of language and text and not technology. It can be subdivided into two categories: open codes and semagrams. Open codes hide messages in other reasonable messages in ways that aren't obvious to the average reader. [5], [6]

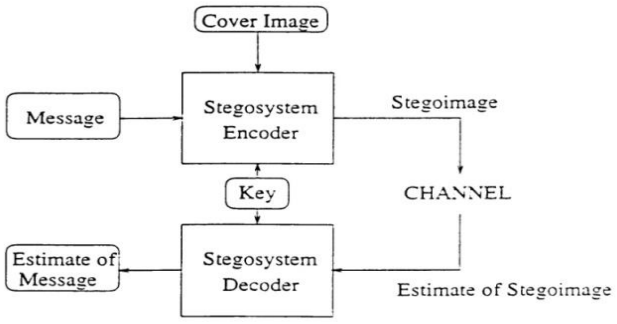

Fig.1. Block Diagram of Steganography

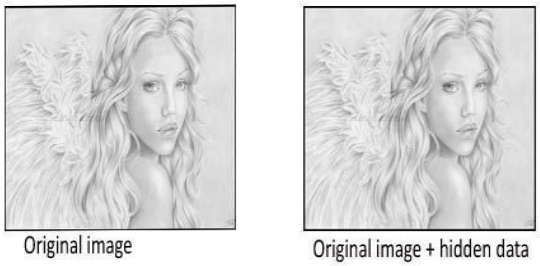

Fig. 2. Cover and Stego Image

In modern steganography to embed secret data into a cover message of a network, there are mainly three types of protocol steganography is used these are as follows Pure Steganography, Secret Key Steganography, and Public Key Steganography [5], [6]. In Pure Steganography there is no necessity of exchange of ciphers as a stego-key. This method of steganography is the least secure as the sender and receiver has to rely only upon the presumption that no other parties are aware of this secret data [5], [6]. In Secret Key Steganography the exchange of a secret key (stego-key) is takes place. In this technique before the communication takes place it embeds the secret data in to a cover message using a secret key.

Here only that parties who know the secret key can reverse the whole process to get the secret data [5], [6]. In Public Key Steganography technique uses the public key and a private key to secure the communication between the two or more parties which wants to communicate secretly [4]. Here in the process of encoding the sender uses the public key and at the receivers point the private key is used to extract the hidden secret message. The public and private keys have a hidden mathematical relationship between them.

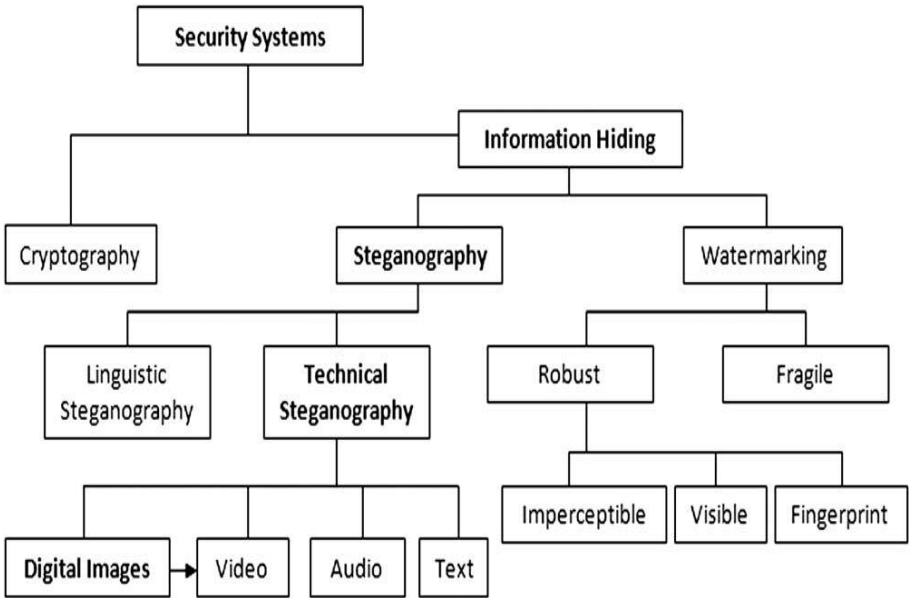

Fig. 3. Information Hiding Techniques

II. DIFFERENT KINDS OF STEGANOGRAPHY

The five main categories of file formats that can be used for steganography are:

A. Text Steganography

This method is used to hide a secret message in a text message for that number of tabs, white spaces, and capital letters, just like Morse code is used. In earlier day this technique is in very much boom but after booming of Internet and different type of digital file formats its importance gets decreased. [5], [6]

B. Image Steganography

Digital images are widely used over the internet as well as that are also popular. Now using this phenomenon the digital images can be used as a cover images/objects for the steganography. In this technique a secret message is embedded/hide in a digital image through an embedding procedure/ algorithm with the help of secret key to produce a stego image. [5], [6]

C. Audio Steganography

Audio stenography is another type of steganography in which the properties of the human ear is considered to hide information. An audible, sound can be made inaudible in the presence of another louder audible sound. Audio steganography uses only digital audio formats such as WAVE, MIDI, AVI MPEG or etc. [5], [6]

D. Video Steganography

Video Steganography is a technique used to hide any kind of files or information into digital video format. Here video is used as carrier for hidden information. Video steganography uses following types of video files such as H.264, Mp4, MPEG, AVI or other video formats. [5], [6]

E. Protocol Steganography

The term protocol steganography is to embedding information within network protocols such as TCP/IP. We can hide information in the header of a TCP/IP packet in some fields that can be either optional or are never used. The protocol steganography uses the TCP, UDP, IP network protocols for data hiding. [5], [6]

III. STEGANOGRAPHIC TECHNIQUES

Digital image steganography techniques can be divided into following domains.

A. Spatial Domain Techniques

There are many versions present in spatial steganography that all are related to make changes directly with some bits of the digital image pixel values to hide data. [5], [6]

Least significant bit (LSB) - based steganography is one of the simplest techniques/method that is used to hide a secret message in digital image. In this technique the pixel value of least significant bit (LSB) are get replaced with bits of secret message and all this is done without introducing many perceptible distortions. The embedding of message bits can be done either sequentially or randomly. [5], [6]

In spatial domain following techniques comes these are as follows such as LSB substitution/replacement, LSB matching, Matrix embedding and Pixel value, differencing etc. [5], [6]

B. Transform Domain Techniques

This is a more complex technique of hiding information in an image. In this various transformation algorithms are used to hide data behind the image [5], [6]. This technique also is termed as a domain of embedding techniques. In this technique a number of algorithms are exists. Most of the strong steganographic systems work in the transform domain because the process of embedding data in the frequency domain of a signal is much stronger than any other domain such as time or etc. [5], [6]

Transform domain techniques are more advantageous than spatial domain because it hides information in such parts of image that are less exposed to image processing, cropping and compression.

Transform domain techniques are mainly classified as follows:

1. Discrete Fourier transformation technique (DFT).
2. Discrete cosine transformation technique (DCT).
3. Discrete Wavelet transformation technique (DWT).
4. Lossless or reversible method (DCT)
5. Embedding in coefficient bits

C. Distortion Techniques

This technique works on the principle of differences between the cover image and the stego image and for that it needs to keep a track of cover image. While embedding the secret message by this technique the encoder adds a sequence of changes to the cover image i.e. way in which and how/where the secret message get embedded. For this process the difference in the signal distortion is considered.

But before the embedding a secret message into the cover image it has to encode it for that the encoder chooses the pixels of cover image pseudo-randomly and changes that pixel bit with message bit in a such manner the statistical properties of the image are not get affected. [5] [6]

However, this method has one drawback as cover image should never be used more than once. As well as an attacker can easily tampers the stego-image by cropping, scaling or rotating.

D. Masking and Filtering

This technique has resemblance with the technique of paper watermark. In this technique information is get concealed by marking an image for that purpose it uses the noise levels of the cover images. The main advantage of this technique is that the hidden message is more integral to the cover image and watermarking techniques can be easily applied as well as there is no fear of image destruction. [5] [6]

This method has one more advantage as it is much more robust than LSB replacement with respect to comparison made based on the following the categories such as compression and the information is hidden in the visible parts of the image. [5][6]

This technique also has the disadvantage as it only works on gray scale images.

IV. LITERATURE SURVEY

This section provides the knowledge of different data hiding techniques are used to hide the data. These are as follows:

In paper "Hiding Data in Images by Simple LSB Substitution" authors proposed an LSB substitution for hiding the data into the image. To achieve better visual quality of stego-image it takes care of noise sensitive area for embedding. This method intelligently differentiates normal texture and edges area of an image as well as it takes the advantage of these areas for the embedding. This method analyses the different LSB values as well as edges, texture masking and brightness of the cover image to calculate the number of k-bit LSB for secret data embedding. It also utilizes the pixel adjustment method for better stego-image visual quality through LSB substitution method. [9]

Optimal pixel adjustment process is also used to generate the stego-image which is obtained by the simple LSB substitution method. The proposed method also termed as OPAP (Optimal Pixel Adjustment Process). [9]

The overall result shows a good high hidden capacity with high image quality of the stego-image can be greatly improved with low extra computational complexity. [9] The main shortcoming of this technique is the worst mean-square-error between the stego-image and the cover-image is derived. [9]

In Paper "An Image Steganographic Scheme Based on Pixel-Value Differencing and LSB Replacement Methods" author proposed a Pixel value difference (PVD) and simple least significant bits scheme are used to achieve adaptive least significant bits data embedding. In pixel value differencing (PVD) where the size of the hidden data bits can be anticipated by difference between the two consecutive pixels in cover image using simple relationship between two pixels. PVD method provides a better imperceptibility by calculating the difference of two consecutive pixels which determine the depth of the embedded bits. [7] This method hides large data with the help of LSB substitution at edge area of image and uses the PVD for smooth region of image to hide the data. Though this technique provides larger capacity but has low visual quality as well as this method is complex. [7]

In paper "LSB matching revisited" author provides a new approach to data hiding scheme by revisiting the previous LSB substitution method by replacing it with the new approach. Here the author introduced the LSB matching choice, in that it decides whether to add or subtract one from the cover image pixel and it is done purely on random basis. This new method uses the choice set of a binary function to select the at most two cover pixels of the required value. Then the actual embedding is done using a pair of pixels selecting/taken as a unit. Now in this process the LSB of the first pixel carries only one bit of secret message and another one carries another bit of secret message. [13] The main shortcoming of this technique is that it made fewer changes in the original image. [13]

In Paper "Matrix Embedding for Large Payloads" authors proposed Matrix Embedding method in that common pattern of bits are made by using the combination of P x Q size rows and columns (of a block/matrix) with the help of random key value. In embedding procedure, each and every pattern of bits is matched with secret message bits, if that pattern get matched and satisfied then it modifies the LSB bits of cover image with the secret message bits, otherwise cover image remains the same. This technique is mainly used to achieve to get security of hidden message in stego-image using a common pattern key. This proposed method has low hidden capacity because to hide only single secret bit it requires a block of (P x Q) pixels. [14]

In paper "Efficient Steganographic Embedding by Exploiting Modification Direction" author provides a new approach to data hiding scheme by introducing a novel method of steganographic embedding in digital images is described, in which each secret digit in a (2n+1) notational system is carried and hide by n pixels of the cover image. In this method at most only one pixel is increased or decreased by 1. It is not suitable for applications that requiring high payload is the main shortcoming of this technique. [8]

In paper "A Double Layered "Plus-Minus One" Data Embedding Scheme" author proposed method that uses the pixels to hide a data. First select a pixel now set their greyscale value and then by adding/subtracting one to/from the gray value we can hide data to an image. In this author also used binary covering codes and wet paper codes to hide messages in the LSB plane and the second LSB plane, respectively. [1] Using this method author achieved the upper bound on the embedding efficiency. [1]

In paper "Labeling Method in Steganography" authors have introduced a data hiding technique where it first find out the dark area of the image then convert it to binary image. Afterwards it labels each dark objects using 8 pixels and used the LSB substitution method to hide data in it. This method required high computation to find dark region. Its hiding capacity totally depends on texture of image. [11]

In paper "RGB Intensity Based Variable-Bits Image Steganography" author have proposed a pixel indicator technique with variable bits. Firstly it chooses one of the color channels such as red channel, green channel and blue channel. Then it embeds secret message bits into various LSB bits of the chosen color channel based on the secret message bits that matches with pixels of that chosen color channel for that it uses the intensity of the pixels that decides the variable bits to embed into cover image. The channel selection criteria are sequential and the capacity depends on the cover image color channel bits. Proposed method has almost same histogram of stego-image that to the cover-image. Here actually color intensity pixel values are getting changed to hide the secret message bits. [17]

In paper "Novel Approach for High Secure and High Rate Data Hidden in the Image Using Image Texture Analysis" author proposed a texture based image steganography. The texture analysis technique divides the texture areas into two groups, simple texture area and complex texture area. Simple texture is used to hide the 3-3-2 LSB bit patterns i.e. 3 bits for Red color channel, 3 bits for Green color channel and 2 bits for Blue color channel. While for the complex texture area 4 LSB bits are used for embedding secret message bits. The above method used the both (2 to 4 LSB for each channel) methods depending on texture classification for better visual quality. Proposed method has high hidden capacity with considering the perceptual transparency measures e.g. PSNR etc. [15]

In paper "Lossless Data Hiding using Bit Depth Embedding for JPEG2000 Compressed Bit-Stream" author proposed novel lossless or reversible data hiding scheme for binary images. This technique uses a JPEG2000 compressed dataset. In the process JPEG2000 compression, full colour images with RGB (colour model) with three colours are transformed to YCrCb colour space, after that for each colour component the wavelet transform, quantization and entropy coding is get calculated independently. Now the wavelet a coefficient of each colour component is get quantized and after that least significant bit plane (LSB) get extracted. Then hide the secret data into the quantized wavelet coefficients of the Y colour component in a reversible way. The proposed data embedding method is useful for binary images not for gray or colour images as well as it suffers from problem of alteration detection. [12]

In paper "High Capacity Filter Based Steganography" author uses 4 LSB bits of each RGB color channel to embed secret data bits. This method also applies median filtering technique to the image to enhance the quality of the stego image. Afterwards with the help of key data i.e. key it embeds secret data bits and key data in the cover image to form the stego image and all this is done as per the calculated difference. In decoding phase the stego-image is added with key data to extract the hidden secret message data. This method increases the complexity by applying filtering technique and also has to manage stego-key. Proposed scheme has high capacity to hide secret messages. [10]

In paper "A Novel Image Data Hiding Scheme with Diamond Encoding" author provides a new approach to data hiding scheme by introducing Diamond Encoding. In this technique, first the process is portioning and embedding of the cover image into non-overlapping blocks of two consecutive pixels. Then it transforms the secret messages into a series of digits which are equivalent to those blocks. Afterward the diamond encoding technique is applied on those blocks to calculate the diamond characteristic values i.e. DCV to hide/concealed secret –ary digits into the diamond characteristic values. After that the diamond characteristic value is gets modified by secret message digit and which can be done by adjusting pixel values in blocks. The main shortcoming of this technique is that it suffers from higher distortion for various lower payload with lower image quality and can be attacked by some well-known steganalysis techniques as well as it does not provide more compact Neighborhood sets. It also not allows embedding digits in any notational system. [3]

In paper "A Novel Image Steganography Method with Adaptive Number of Least Significant Bits Modification Based on Private Stego-Keys" authors have proposed an adaptive least significant bit spatial domain embedding method. This method divides the image pixels. That ranges from 0-255 and generates a stego-key. This stego-key is private and has 5 different gray level ranges of image. The each range indicates to substitute fixed number of bits to embed in LSB bits of image. The strength of this method is its integrity of secret hidden information in stego-image and high hidden capacity.

[4] The limitation is to hide extra bits of signature with hidden message for its integrity purpose. It also has to convert color image into blue channel for information hiding. [4]

In paper "Reversible Data Embedding for High Quality Images using Interpolation and Reference Pixel Distribution Mechanism" author used the reversible data hiding method based on image interpolation and the detection of smooth and complex regions in the cover images. For that purpose a binary image is used. Now with the reference this image location of pixels is constructed according the local image activity. In this case only the complex regions' more reference pixels are chosen and these pixels are used for embedding, which reduces the image degradation. After that the pixels are interpolated according to the newly constructed binary image, and the interpolation errors are used to embed data with the help of histogram shifting. Now the pixel values in the cover image are modified using greyscale unit to produce high quality stego image. [16] This method provides better image quality and embedding capacity and PSNR. Its shortcoming is in smooth regions it introduces very little distortion. [16]

In paper "A Novel Data Embedding Method Using Adaptive Pixel Pair Matching" author proposed APPM Method in that it first selects the pixel pair then use that pixel pair's value as reference coordinate. After that it searches the coordinate in the neighborhood set of these pixel pairs according to a given message digit after that the pixel pair is then replaced by the searched coordinate to obscure the digit. It has chance of future improvement in case of high definition color images and further more it is possible to improve it for more high data capacity. [2]

Table 1: Summary and Analysis of Literature Survey

Sr. No.	Name of Techniques	Technique used	Advantages	Limitations
1	LSB Substitution	Hiding data in images by simple LSB substitution and applying an optimal pixel Adjustment	Good hidden capacity and low complexity	Worst MSE between the stego-image and cover-image is derived
2	Pixel value Differencing	Data gets hide based upon difference between the two consecutive pixels in cover image	This method hides large data with the help of LSB substitution at edge area of image	Visibility of the hiding effect present in the PVD method
3	Matrix Embedding	Each pattern bit is matched with message bit, if satisfied it modifies the LSB bits by data bits	Provides high security	Suffers from low hidden capacity
4	Exploiting Modification Direction	At most, only one pixel is increased or decreased by 1 to embed in (2p+1) notational system	Provides Stable and convenient security	It does not work properly on high payload
5	Double Layered "Plus-Minus One" Data Embedding Scheme	Based on greyscale value of pixel adding/subtracting one to/from the image is done to hide data	This achieves the upper bound on the embedding efficiency	Does not give better result on low quality images
6	RGB Intensity Based Variable-Bits Image Steganography	It chooses one colour channel among red, green and blue and embeds data into variable LSB of chosen channel	Almost Same histogram of stego-image against cover image	Hidden capacity depended on cover image pixel intensities
7	Texture Based Image Steganography	It divides the texture areas into two groups, simple and complex and these are used to hide the information	Provides high hidden capacity	high hidden capacity degrade the visual quality PSNR
8	Bit Depth Embedding for JPEG2000	RGB images are transformed to YCrCb colour space, and then, wavelet transform, quantization and entropy coding are performed to extract LSB then hides the secret data	Provides lossless, reversible data hiding scheme for binary images	Not supported to Gray and Color image as well as suffers from alteration detection

Sr. No.	Name of Techniques	Technique used	Advantages	Limitations
9	Data Hiding Scheme with Diamond Encoding	Diamond characteristic value of each non-overlapping block of two consecutive pixels is calculated and which is used to concealed message digit.	Provides high quality stego-image and conceals large amount of data	It suffers from higher distortion for various payload as well as it does not provide more compact Neighborhood Set.
10	LSB Modification Based on Private Stego-Keys	It divides the image pixels ranging 0-255 and generates a private stego-key based on 5 different gray level ranges of image.	Provides Integrity of secret hidden information with High Capacity	It hides extra bits of with hidden message
11	Reversible Data Embedding using Interpolation and Reference Pixel Distribution Mechanism	Divides the image in smooth and complex regions then more data is embedded in complex region than simple one	This method provides better image quality and embedding capacity and PSNR.	It introduces little distortion in smooth regions
12	Data Embedding Method Using Adaptive Pixel Pair Matching	It uses the values of pixel pair as a reference coordinate, and search a co-ordinate in the Neighborhood set of this pixel pair according to a given message digit then the pixel pair is then replaced by the searched coordinate to conceal the digit.	It offers smaller MSE compared with OPAP and DE as well as does not produces artifacts in stego images. It also offers a secure communication under adjustable embedding capacity.	It has a chance to increase embedding capacity with smaller MSE

V. CONCLUSION

This paper gives an overview of different steganographic techniques its major types and classification of steganography which have been proposed in the literature during last few years. To conclude this review paper, we conjecture that different mechanisms are involved for Securing and hiding the information or secrete messages that are mean by steganography. Now from the point of security, with the concept's understanding the future scope is that it has chance of further improvement in case of high definition colour images and further more it is possible to improve it for more high data capacity.

ACKNOWLEDGMENT

Sincerely thank the all experts who have contributed towards development of this paper.

REFERENCES

[1] W. Zhang, X. Zhang, and S. Wang, "A double layered plus-minus one data embedding scheme," *IEEE Signal Process. Lett*, vol. 14, no. 11, pp. 848–851, Nov. 2007.

[2] Wien Hong and Tung-Shou Chen, "A Novel Data Embedding Method Using Adaptive Pixel Pair Matching", *IEEE Transactions on Information Forensics and Security*, Vol. 7, No. 1, February 2012

[3] R.M. Chao, H. C. Wu, C. C. Lee, and Y. P. Chu, "A novel image data hiding scheme with diamond encoding," *EURASIP J. Inf. Security*, vol. 2009, 2009, DOI: 10.1155/2009/658047, Article ID 658047.

[4] Y. K. Jain and R. R. Ahirwal, "A Novel Image Steganography Method With Adaptive Number of Least Significant Bits Modification Based on Private Stego-Keys", *International Journal of Computer Science and Security (IJCSS)*, vol. 4, March 2010.

[5] Pratap Chandra Mandal, "Modern Steganographic technique: A Survey", *International Journal of Computer Science & Engineering Technology (IJCSET)* Vol. 3 No. 9 Sep 2012

[6] Mehdi Hussain and Mureed Hussain, "A Survey of Image Steganography Techniques", *International Journal of Advanced Science and Technology* Vol. 54, May, 2013

[7] Hsien-Chu Wu Na-I Wu Chwei-Shyong Tsai Min-Shiang Hwang, "An Image Steganographic Scheme Based on Pixel-Value Differencing and LSB Replacement Methods", *National Science Council, Taiwan*, Nov 2004

[8] X. Zhang and S. Wang, "Efficient steganographic embedding by exploiting modification direction," *IEEE Commun. Lett.* vol. 10, no. 11, pp. 781–783, Nov. 2006.

[9] K. Chan, L. M. Cheng, "Hiding data in images by simple LSB substitution", *Pattern Recognition*, vol. 37, no: 3, pp: 469–474, 2004.

[10] B. Ahuja, M. Kaur and M. Rachna, "High Capacity Filter Based Steganography", *International Journal of Recent Trends in Engineering*, vol. 1, no. 1, May 2009.

[11] H. Motameni, M. Norouzi, M. Jahandar and A. Hatami, "Labeling Method in Steganography", *World Academy of Science, Engineering and Technology*, France, 2007.

[12] S. Ohyama, M. Niimi, K. Yamawaki and H. Noda, "Lossless data hiding using bit depth embedding for JPEG2000 compressed bit-stream", *Journal of Communication and Computer*, vol. 6, no. 2, Feb 2009**.**

[13] J. Mielikainen, "LSB matching revisited," *IEEE Signal Process. Lett.* vol. 13, no. 5, pp. 285–287, May 2006.

[14] J. Fridrich and D. Soukal, "Matrix embedding for large payloads," *IEEE Trans. Inf. Forensics Security*, vol. 1, no. 3, pp. 390–394, Sep. 2006.

[15] M. Hamid and M. L. M. Kiah, "Novel Approach for High Secure and High Rate Data Hidden in the Image Using Image Texture Analysis", *International Journal of Engineering and Technology (IJET):* 0975-4042, 2009.

[16] W. Hong and T. S. Chen, "Reversible data embedding for high quality images using interpolation and reference pixel distribution mechanism," *J. Vis. Commun. Image Represent,* Vol: 22, no. 2, pp. 131–140, 2011.

[17] M. Tanvir Parvez and A. Abdul-Aziz Gutub, "RGB Intensity Based Variable-Bits Image Steganography", *IEEE Asia-Pacific Services Computing Conference*, pp. 1322-1327. 2008

