IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)
An International Open Access, Peer-reviewed, Refereed Journal

Insight of Steganography: Concealed Message in Images

Pavitra Gadhar
asstistant professor
dept of CSE rural engineering college hulkoti

Preeti Bhandi
student
dept of CSE rural engineering college hulkoti

Abstract:

The innovation of technology and having fast internet make information to distribute over the planet easily and economically. this is often made people worry about privacy and works. Steganography may be a technique that forestalls unauthorized users to possess access to big data. The steganography provides methods that users can hide and blend their information with other information that make them difficult to acknowledge by attackers. In this, we review some techniques of steganography spatial and frequency domains. Also, we explain the kinds of steganography host documents. It also can pose serious problems due to it difficult to detect. Network surveillance and monitoring systems won't flag messages or files that contain steganographic data. and that we also see some applications, pros, and cons of steganography.

Introduction:

Steganography may be a Greek word meaning concealed writing. The word stegano means covered and graphical means writing. Thus, steganography isn't only the art of hiding data but also hiding the very fact of the transmission of secret data. Steganography hides the key data in another enter such how that only the recipient knows the existence of the message. In past , the info was protected by hiding it on the rear of wax, writing tables, the stomach of rabbits or on the scalp of the slaves. But today's most of the people transmit the info within the sort of text, images, video, and audio over the medium. to securely transmission of confidential data, the multimedia object like audio, video, images are used as cover sources to cover the info . Steganography is defined because the study of invisible communication. Steganography usually deals with the ways of hiding the existence of the communicated data in such how that it remains confidential. It maintains secrecy between two communicating parties. In image steganography, secrecy is achieved by embedding data into a canopy image and generating a stego-image. There are differing types of steganography techniques each has its strengths and weaknesses. during this paper, we review the various security and data hiding techniques that are wont to implement steganography like LSB, ISB, MLSB, etc. In today's world, communication is that the basic necessity of each growing area. Everyone wants the secrecy and safety of their communicating data. In our lifestyle, we use many secure pathways just like the Internet or telephone for transferring and sharing information, but it isn't safe at a particular level. To share the knowledge during a concealed manner two techniques might be used. These mechanisms are cryptography and steganography. In cryptography, the message is modified in an encrypted form with the assistance of the encryption key which is understood to the sender and receiver only. The message can't be accessed by anyone without using the encryption key. However, the transmission of encrypted messages may easily arouse attacker suspicion, and therefore the encrypted message may thus be intercepted, attacked or decrypted violently. to beat the shortcomings of cryptographic techniques, steganography techniques are developed. Steganography is that the art and science of communicating in such how that it hides the existence of the communication. Thus, steganography hides the existence of knowledge in order that nobody can detect its presence. In steganography the method of hiding information content inside any multimedia content like image, audio, video mentioned as Embedding. For increasing confidentiality of communicating data both techniques could also be combined.

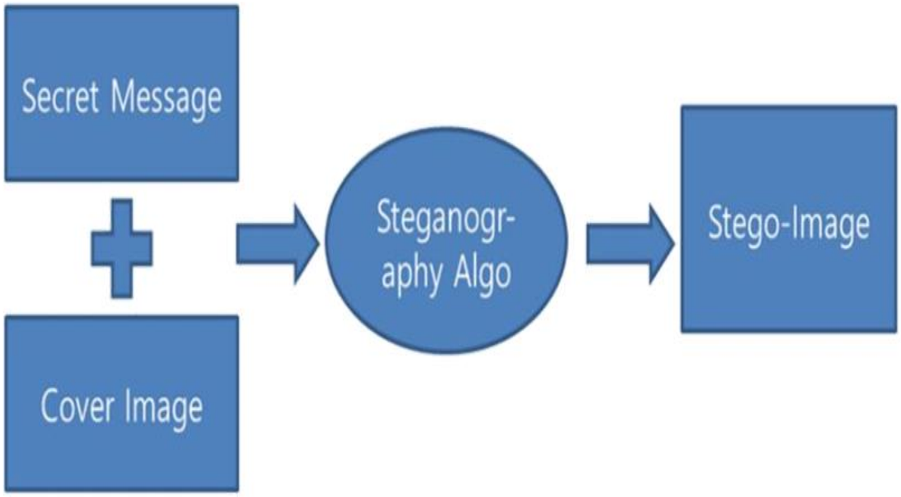
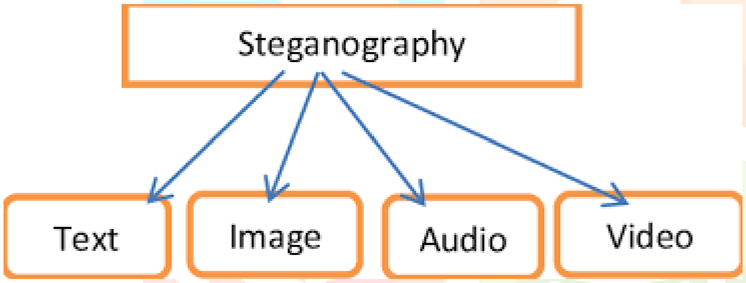


Figure: Representation of Steganography

Types of Steganography:



MESSAGES IN TEXT program is named SPAM MIMIC. Secret messages are often hidden in text format by reframing the text of the carrier file while maintaining the context. One sort of steganography may be a program called Spam Mimic.

Based on a group of rules called a mimic engine by Peter Wayner, it encodes your message into what seems like your typical, quickly deleted Spam message. However, hiding a message in plain text may be a thing of the past, as people are suspicious of irrelevant text.

MESSAGES IN STILL IMAGES the foremost popular tool is outguessed.

MESSAGES IN AUDIO data is hidden in layer III of the encoding process of the MP3 file. Messages in audio are always sent along side ambient noise. the info is hidden within the heart of the layer III encoding process of the MP3 file, namely the inner loop during compression. The inner loop limits the input file and increases the step size until the info are often coded with the available number of bits. the info is compressed, encrypted then hidden within the MP3 bitstream.

MESSAGES IN VIDEO embedding information into multimedia data has gained increasing attention lately. the tactic of encryption is that the same as in audio steganography. Video files are generally excellent carrier files since they need tons of irrelevant bits.

AN EXAMPLE

Fishing freshwater bends and saltwater coasts reward anyone feeling stressed. Resourceful anglers usually find masterful leapers fun and admit swordfish rank overwhelming any day.

“Send lawyers guns and money”

Here during this example, we will see that the hidden message to be sent to the receiver is to send lawyers guns and money it's hidden inside the opposite text message. we will see the opposite text message therein the underlined third letter of each word has one character of hidden message. this is often how steganography in text messages works.

Literature Survey:

In [1] authors have proposed an adaptive least significant bit spatial domain embedding method. This method divides the image pixels ranges (0-255) and generates a stego-key. This private stego-key has 5 different gray level ranges of image and every range indicates to substitute a hard and fast number of bits to embed within the least significant bits of the image. The strength of the proposed method is its integrity of secret hidden information in stego-image and high hidden capacity. The limitation is to cover extra bits of signature with a hidden message for its integrity purpose. It also proposed a way for a color image just to switch the blue channel with this scheme for information hiding. This method is targeted to realize high hidden capacity plus the safety of the hidden message.

Yang et al., [2] proposed an adaptive LSB subtitution based data hiding method for the image. To achieve a far better visual quality of stego-image it takes care of the noise-sensitive area for embedding. The proposed method differentiates and takes advantage of normal texture and edges area for embedding. This method analyzes the sides, brightness and texture masking of the duvet image to calculate the amount of k-bit LSB for secret data embedding. The value of k is high at non-sensitive image region and over-sensitive image area k value remains small to balance the overall visual quality of an image. The LSB's (k) for embedding is computed by the high-order bits of the image. It also utilizes the pixel adjustment method for better stegoimage visual quality through the LSB substitution method. The overall result shows an honest high hidden capacity, but dataset for experimental results are limited; there's not one image which has many edges with noise region like 'Baboon.tif’.

In [3] anthers have proposed LSB based image hiding method. Common pattern bits (stego-key) are wont to hide data. The LSB's of the pixel is modified counting on the (stego-key) pattern bits and therefore the secret message bits. Pattern bits are a mix of MxN size rows and columns (of a block) and with the random key value. In embedding procedure, each pattern bit is matched with message bit, if satisfied it modifies the 2nd LSB bits of the duvet image otherwise remains an equivalent. This technique targets to achieve the security of hidden messages in stego-image using a common pattern key. This proposed method has low hidden capacity because a single secret bit requires a block of (MxN) pixels.

In [4] author proposed a Pixel value difference (PVD) and the simple least significant bits scheme is used to achieve adaptive least significant bits of data embedding. In pixel value differencing (PVD) where the dimensions of the hidden data bits are often estimated by the difference between the 2 consecutive pixels during a cover image using a simple relationship between two pixels. PVD method generally provides an honest imperceptibility by calculating the difference of two consecutive pixels which determine the depth of the embedded bits. The proposed method hides large and adaptive k-LSB substitution at the edge area of image and PVD for the smooth region of an image. So during this way the technique provides both larger capacity and high visual quality consistent with experimental results. This method is complex thanks to adaptive k generation for substitution of LSB.

In [5] authors proposed a way of Multi-Pixel Differencing (MPD) that used quite two pixels to estimate the smoothness of every pixel for data embedding and it calculates the sum of difference value of 4 pixels block. For small difference value it uses the LSB otherwise for high difference value it uses the MPD method for data embedding. Strength is its simplicity of algorithm but the experimental dataset is too limited.

Steganography in Images:

Hiding information inside images may be a popular technique nowadays. An image with a secret message inside can easily be cover the planet wide web or in newsgroups. The use of steganography in newsgroups has been researched by German steganographic expert Niels Proves, who created a scanning cluster which detects the presence of hidden messages inside images that were posted on the net. However, after checking a million images, no hidden messages were found, therefore the practical use of steganography still seems to be limited image Steganography is that the technique of hiding the data within the image in such how that forestalls the unintended user from the detection of the hidden messages or data.

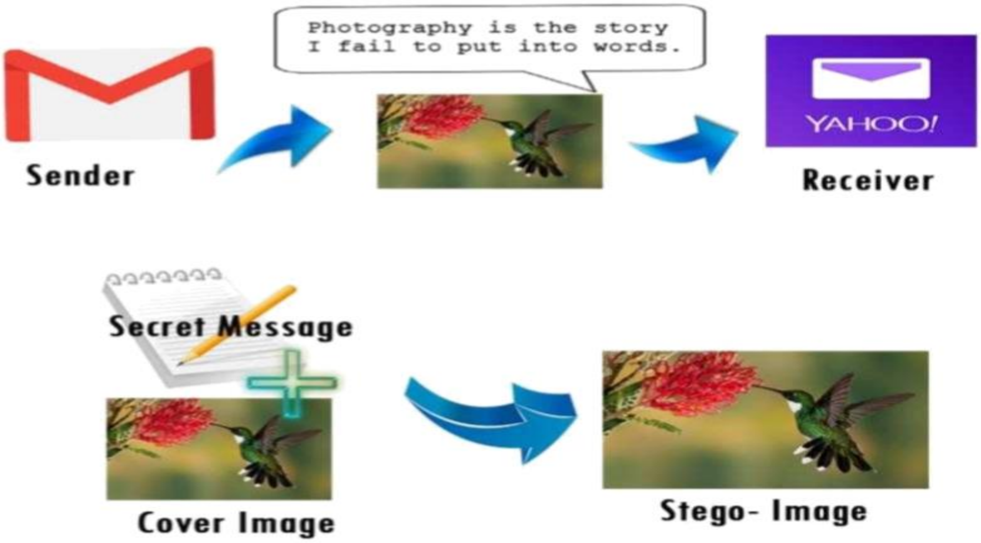


Figure: Communication Through Steganography

To hide a message inside an image without changing its visible properties, a cover source are often altered in noisy areas with many color variations, so less attention will draw to the notifications. The most common methods to form these alterations involve the usage of the least-significant bit or LSB, masking, filtering and transformations on the duvet image. These techniques are often used with varying degrees of success on differing types of image files. The project deals with learning about the varied sorts of steganography available. Image steganography is performed for images and therefore the concerning data is additionally decrypted to retrieve the message image. Since this will be wiped out several ways, image steganography is studied and one among the methods is employed to demonstrate it. Image steganography refers to hiding information i.e. text, images or audio files in another image or video files. The current project aims to use steganography for a picture with another image using spatial domain techniques. This hidden information can be retrieved only through proper decoding techniques. This encryption and decryption of images are done in steganographic technique.

Technical Details

- Using java.awt.Image,ImageIO

- The package contains all the required classes and methods alongside interfaces that are necessary for the manipulation of the pictures.

The Encoding Process

The steganography technique used is LSB coding. The offset of the image is retrieved from its header. That offset is left because it is to preserve the integrity of the header, and from subsequent byte, we start our encoding process. For encoding, we first take the input carrier file i.e. an image file then direct the user to the choice of the document.

Creation of User Space

• User Space is created for preserving the original file so that all the modifications are done in the userspace.

• In the object of BufferedImage, using an image.read method we take the original image.

• Using create graphics and drawRenderedlinage method of Graphics class, we create our user space in a BufferedImage object. The text file is taken as input and separated in a stream of bytes. Now, each little bit of these bytes is encoded within the LSB of every next pixel. And, finally, we get the final image that contains the encoded message and it is saved, at the specified path given by the user, in PNG format using ImageIO.write method. This completes the encoding process.

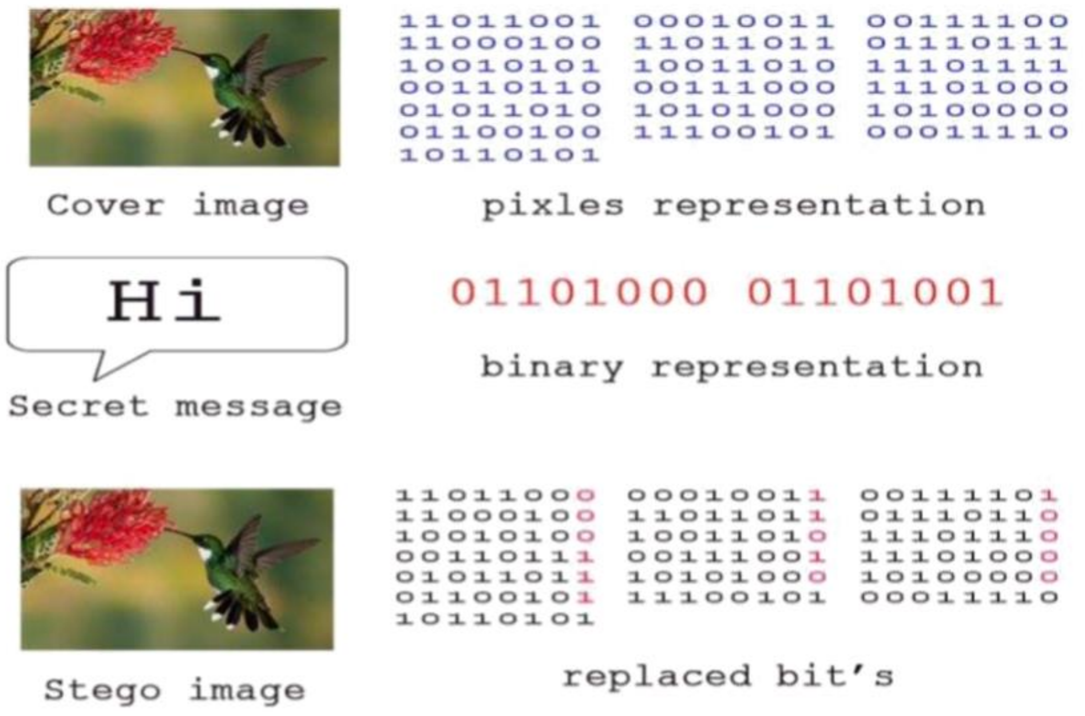


Figure: LSB Operation

The Decoding Process

The offset of the image is retrieved from its header. Create the user space using an equivalent process as within the Encoding. Using getRaster() and getDataBuffer() methods of Writable Raster and DataBufferByte classes. The data of the image is taken into a byte array. Using the above byte array, the bitstream of the original text file is retrieved into another byte array. And above byte array is written into the decoded document, which results in the first message.

LSB (Least Significant Bit)

There are two different methods for image steganography:

1. Spatial methods

2. Transform methods but we are using Spatial Methods.

Spatial Method

In the spatial method, the most common method used is the LSB substitution method. The least significant bit (LSB) method may be a common, simple approach to embedding information during a cover file. In steganography, the LSB substitution method is used. I.e. since every image has three components (RGB). This pixel information is stored in an encoded format in one byte. The first bits containing this information for each pixel are often modified to store the hidden text. For this, the preliminary condition is that the text to be stored has to be smaller or of equal size to the image used to hide the text. LSB based method is a spatial domain method. But this is vulnerable to cropping and noise. In this method, the MSB (most significant bits) of the message image to be hidden are stored in the LSB (least significant bits) of the image used as the cover image. It is known that the pixels in an image are stored in the form of bits. In a grayscale image, the intensity of each pixel is stored in 8 bits (1 byte). Similarily for a color (RGB-red, green, blue) image, each pixel requires 24 bits (8bits for each layer). The Human visual system (HVS) cannot detect changes in the color or intensity of a pixel when the LSB bit is modified. This is psycho-visual redundancy since this will be used as a plus to store information within the se bits and yet notice no major difference in the image. Algorithm of LSB method of steganography. There could be two different phases of the LSB method, embedding phase and extracting phase. Algorithms of both of the phases are given below:

Embedding phase Procedure:

Step 1: Extract all the pixels from the given image and store them in some array named (image array).

Step 2: Extract all the characters from the given text file (message file) and store it in the array called (message array).

Step 3: Retrieve the characters from the Stego key and store them in an array called Keyarray. A stego- the key is used to control the hiding process to restrict the detection and/or recovery of the embedded data.

Step 4: Take the first pixel and characters from Key- array and place it in the first component of the pixel. If there are more characters in Key array, then place rest in the first component of the next pixels.

Step 5: Place the sonic terminating symbol to indicate the end of the key. 0 has been used as a terminating symbol during this algorithm.

Step 6: Place characters of message Array in each component of the next pixels by replacing it. Step 7: Repeat step 6 until all the characters are embedded.

Step 8: Again place some terminating symbol to indicate the end of data.

Step 9: The obtained image will hide all the characters of that input.

The simplest steganography techniques embed the bits of the message directly into the smallest amount significant bit plane of the duvet image during a deterministic sequence. Modulating the smallest amount significant bit doesn't end in a human-perceptible difference because the amplitude of the change is little. To hide a secret message inside a picture, a correct cover image is required. Because this method uses bits of every pixel within the image, it's necessary to use a lossless compression format, otherwise, the hidden information will stray within the transformations of a lossy compression algorithm. When employing a 24-bit color image, a touch of every of the red, green and blue color components are often used, so a complete of three bits are often stored in each pixel. For example, the subsequent grid are often considered as 3 pixels of a 24-bit color image, using 9 bytes of memory:

(00100111 11101001 11001000)

(00100111 11001000 11101001)

(11001000 00100111 11101001)

When the character A, which binary value equals 10000001, is inserted, the subsequent grid results:

(00100111 11101000 11001000)

(00100110 11001000 11101000)

(11001000 00100111 11101001)

In this case, only three bits need to be changed to insert the character successfully. On average, only half the bits in a picture will got to be modified to cover a secret message using the maximal cover size. The result changes that are made to the least significant bits are too small to be recognized by the human visual system (HVS), so the message is effectively hidden. As you see, the least significant bit of the third color remains without any changes. It are often used for checking the correctness of 8 bits which are embedded in these 3 pixels. In other words, it could be used as a parity bit.

Masking and filtering

Masking and filtering techniques, usually restricted to 24 bits or grayscale images, take a special approach to hiding a message. These methods are effectively almost like paper watermarks, creating markings in a picture. This can be achieved for instance by modifying the luminance of parts of the image. While masking does change the visible properties of a picture, it are often wiped out such how that the human eye won't notice the anomalies. Since masking uses visible aspects of the image, it's more robust than LSB modification for compression, cropping and different sorts of image processing. The information isn't hidden at the background level but is inside the visible a part of the image, which makes it more suitable than LSB modifications just in case a lossy compression algorithm like JPEG is being used.

Advantages:

The main advantages of this system are

The security that it provides security to your messages without knowing to the third party.

The number of bits has been replaced according to user or sender, therefore third party cannot guess password.

Normal network users can’t guess images.

In steganography anyone can’t jump on the suspect by looking images.

It is Reliable.

Easy to use.

Easy Maintenance.

The system has been secured by password authentication.

Disadvantages:

Images can have attacks like diluting, nosing, contrast changes and so on.

Number bits of the pixel should be replaced by equal bits of the message.

If someone is eavesdropping then there is the probability of message gets unfold.

If more than two people having the same steganography software then the hidden message can acquire.

This software has been implemented by jam, which is an open-source, therefore code is readable so anyone with a bad mentality can make software perform inverse operation.

Only unintended users may know the actual working of the software.

An intruder may penetrate suspecting images to get hidden data.

Application of Steganography:

Steganography are often used anytime you would like to cover data. There are many reasons to cover data but all of them boil right down to the will to stop unauthorized persons from becoming conscious of the existence of a message. With these new techniques, a hidden message is indistinguishable from noise. Even if the message is suspected, there is no proof of its existence. In the business world steganography are often wont to hide a secret formula or plans for a replacement invention. Steganography also can be used for corporate espionage by sending out trade secrets without anyone at the corporate being any the wiser.

Terrorists also can use steganography to stay their communications secret and to coordinate attacks. All of this sounds fairly nefarious, and therefore the obvious uses of steganography are for things like espionage. But there are several peaceful applications. The simplest and oldest are utilized in map making, where cartographers sometimes add a small fictional street to their maps, allowing them to prosecute copycats. A similar trick is to feature fictional names to mailing lists as a check against unauthorized resellers.

Most of the newer applications use steganography sort of a watermark, to guard copyright on information. Photo collections, sold on CD, often have hidden messages within the photos which permit detection of unauthorized use. The same technique applied to DVDs is even simpler since the industry builds DVD recorders to detect and disallow copying of protected DVDs.

i) Confidential Communication and Secret Data Storing

ii) Protection of Data Alteration

iii) Access Control System for Digital Content Distribution

iv) E-Commerce

v) Media

vi) Database Systems.

vii) digital watermarking.

Conclusion:

Although just some of the most steganographic techniques were discussed during this work, one can see that there exists an outsized selection of approaches to hiding information in images. All the main image file formats have different methods of hiding messages, with different strong and weak points respectively. Hiding a message with steganography methods reduces the prospect of the message being detected. In and of itself, steganography isn't an honest solution to secrecy, but neither is straightforward substitution and short block permutation for encryption. But if these methods are combined, you've got much stronger encryption routines. like all tool, steganography is neither inherently good nor evil, it's how it's used which can determine whether it's a benefit or a detriment to our society. In today‟s world, we frequently hear a well-liked term "Hacking". Hacking is nothing but unauthorized access to data which will be collected at the time of knowledge transmission. Concerning steganography this problem is usually taken as Steganalysis. Steganalysis may be a process during which a steganalyzer cracks the duvet object to urge the hidden data. So, whatever be the technique are going to be developed within the future, the degree of security-related thereupon has got to be kept in mind. it's hoped that Dual Steganography, Steganography along Cryptography makes data transformation safer.

References:

[1] Y. K. Jain and R. R. Ahirwal, "A Novel Image Steganography Method With Adaptive Number of Least Significant Bits Modification supported Private Stego-Keys", International Journal of computing and Security (IJCSS), vol. 4, (2010) March 1.

[2] H. Yang, X. Sun and G. Sun, "A High-Capacity Image Data Hiding Scheme Using Adaptive LSB Substitution", Journal: Radioengineering, vol. 18, no. 4, (2009), pp. 509-516.

[3] S. Channalli and A. Jadhav, "Steganography an Art of Hiding Data", International Journal on computing and Engineering, IJCSE, vol. 1, no. 3, (2009).

[4] C.-H. Yang, C.-Y. Weng, S.-J. Wang, Member, IEEE and H.-M. Sun, "Adaptive Data Hiding in Edge Areas of Images with Spatial LSB Domain Systems", IEEE Transactions on Information Forensics and Security, vol. 3, no. (2008) September 3, pp. 488-497.

[5] K.-H. Jung, K.-J. Ha and K.-Y. Yoo, "Image data hiding method supported multi-pixel differencing and LSB substitution methods", Proc. 2008 International Conference on Convergence and Hybrid Information Technology (ICHIT '08), Daejeon (Korea), (2008) August 28-30, pp. 355-358.

[6] H. Zhang, G. Geng and C. Xiong, "Image Steganography Using Pixel-Value Differencing", Electronic Commerce and Security, ISECS '09. Second International Symposium on (2009) May.

[7] W. J. Chen, C. C. Chang and T. H. N. Le, "High Payload Steganography Mechanism Using Hybrid Edge Detector", Expert Systems with Applications (ESWA 2010), vol. 37, pp. 3292-3301, (2010) April 4.

[8] V. Madhu Viswanatham and J. Manikonda, "A Novel Technique for Embedding Data in Spatial Domain", International Journal on computing and Engineering, IJCSE, vol. 2, (2010).

[9] M. A. Al-Husainy, "Image Steganography by Mapping Pixels to Letters", Journal of computing , vol. 5, no. 1, (2009),pp. 33-38.

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

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

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

[13] A. M. Hamid and M. L. M. Kiah, “Novel Approach for top Secure and High Rate Data Hidden within the Image Using Image Texture Analysis”, International Journal of Engineering and Technology (IJET): 0975-4042, (2009).

[14] M. Chaumont and W. Puech, “DCT-Based Data Hiding Method To Embed the colour Information during a JPEG Grey Level Image”, 14th European Signal Processing Conference (EUSIPCO 2006), Florence, Italy, copyright by EURASIP, (2006) September 4-8.

[15] K. S. Babu, K. B. Raja, K. Kiran Kumar, T. H. Manjula Devi, K. R. Venugopal and L. M. Pataki, “Authentication of secret information in image steganography”, IEEE Region 10 Conference, TENCON2008, (2008) November, pp. 1-6.

[16] 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, (2009) February.

[17] N. F. Johnson and S. Katzenbeisser, “A Survey of steganographic techniques. in Information Hiding Techniques for Steganography and Digital Watermarking, S.Katzenbeisser and F.Petitcolas, Ed. London: Artech House, (2000), pp. 43-78.

[18] H. S. Majunatha Reddy and K. B. Raja, (2009) High capacity and security steganography using discrete wavelet transform. International Journal of computing and Security. pp. 462-472.