International Journal of Engineering Research and General Science Volume 3, Issue 4, July-August, 2015
ISSN 2091-2730

A review on various approaches using video steganography

Jasvir Kaur, Neha Jain, Mohita Garg

Punjab technical University, jassgrewal256@gmail.com

ABSTRACT- Steganography is an excellent means of conversing if there is guarantee on the integrity of the channel of communication. Each technique can be implemented easily, but if someone tries to find out the tricks after knowing that someone using the stego-video file, then there are good chances of finding out the hidden information. In order to avoid this, some hybrid system is used, in such a way that even though someone finds out the one technique, it is used only on few frames and other frames contains different kind of steganography and hence total secrete message is not delivered. Due to these embedding the video Steganography get dispersed using different types. In Video Steganography data is encrypted behind the least significant bits of video frame. Main problem arises because due to embedding behind least significant bits of video frames stagnalysis can be one easily on these frames to retrieved data. This does not provide security to secret data. Second issue is that on embedding the data size of data gets increases which are not easy to transmit over the network. In the proposed work, to overcome these problem occurred in video Steganography various types of approaches has been studied and MLSB is taken as most appropriate approach for embedding of data. Size of embedded data can be reduced by performing compression to stego video file.

Keywords : conversing; integrity; compression; embedding; stagnalysis; encrypted; hidden information

1.1 INTRODUCTION

Steganography is the strategy of undetectable correspondence. This is proficient through concealing data in other data, along these lines concealing the presence of the imparted data. The steganography is the blend of words "stegos" signifying "spread" and "grafia" signifying "written work characterizing it as "secured composition" [4]. In picture steganography the data is shrouded solely in pictures. The thought and routine of concealing data has a long history. In Histories the Greek antiquarian Herodotus composes of an aristocrat, Histaeus, who expected to speak with his child in-law in Greece. He shaved the leader of one of his most trusted slaves and tattooed the message onto the slave's scalp [6]. At the point when the slave's hair developed back the slave was dispatched with the concealed message. In the Second World War the Microdot procedure was produced by the Germans. Data, particularly photos, was decreased in size until it was the extent of a wrote period. To a great degree hard to distinguish, a typical spread message was sent more than an unstable channel with one of the periods on the paper containing concealed data. Today steganography is for the most part utilized on PCs with computerized information being the transporters and systems being the rapid conveyance channels [5].

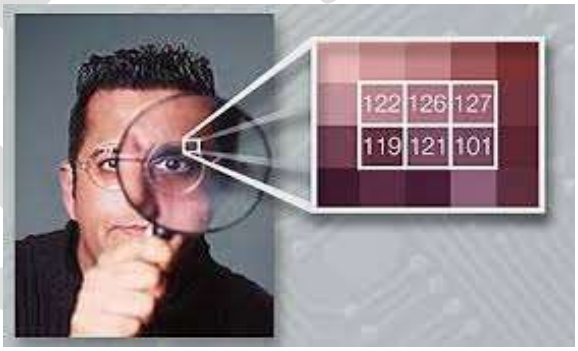

Fig 1: Image showing Stenography

Steganography contrasts with cryptography as in where cryptography concentrates on keeping the properties of a message secret, steganography concentrates on keeping the presence of a message. Steganography and cryptography are both approaches to shield data from undesirable clients however neither technology alone is accurate and can be accepted [8]. Once the presence of data is released or even suspected, the reason for steganography is partially defeated. The quality of steganography can along these lines be increased by consolidating it with cryptography [1].

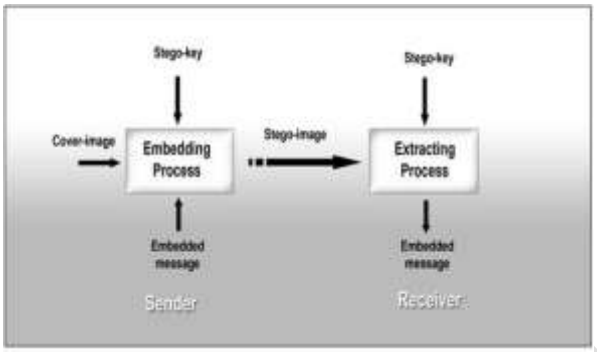

Fig 2 Block Diagram of steganography

Two different technologies that are firmly identified with steganography are watermarking and fingerprinting [5]. These advances are essentially concerned with the insurance of licensed innovation, in this way the calculations have diverse necessities than steganography [2]. These requirement of a decent stenographic calculation will be talked about underneath. In watermarking the majority of the examples of an item are "checked" in the same way. The sort of data covered up in articles when utilizing watermarking is typically a mark to imply source or possession with the end goal of copyright protection [6]. With fingerprinting then again, distinctive, remarkable imprints are installed in particular duplicates of the transporter question that are supplied to diverse clients. This empowers the licensed innovation proprietor to distinguish clients who break their permitting understanding by supplying the property to outsiders. In watermarking and fingerprinting the way that data is covered up inside the documents may be open learning – now and then it may even be noticeable – while in steganography the vagueness of the data is urgent. A fruitful assault on a steganography framework comprises of an enemy watching that there is data covered up inside a record, while an effective assault on a watermarking or fingerprinting framework would not be to recognize the imprint, but rather to remove it [5].

Research in steganography has basically been driven by an absence of quality in cryptographic frameworks. Numerous government have made laws as far as possible the quality of a cryptographic framework or to forbid it through and through, constraining individuals to study different routines for secure data exchange [3]. Organizations have likewise begun to understand the capability of steganography in conveying competitive advantages or new item data. Evading correspondence through no doubt understood channels extraordinarily decreases the danger of data being spilled in exchanging data in a photo of the organization outing is less suspicious than conveying an encoded record. To give an outline of steganography, terms and ideas ought to first be clarified. A review of the various types of steganography is given at a later stage [2].

The benefit of steganography is that it can be utilized to furtively transmit messages without the truth of the transmission being found. Regularly, utilizing encryption may distinguish the sender or beneficiary as someone with something to cover up. Case in point, the photo of our feline could disguise the arrangements for our organization's most recent specialized development [5].

1.1.1 Objective

- To apply Direct Cosine Transform for retrieval of frames of video file.
- To implement hybrid ISB- LSB on each frames of video file forextraction of least significant bits of each region.
- To implement compression for reducing size of video data.
- Analysis of various parameters for performance evaluation.

1.2 DIFFERENT KIND OF STENOGRAPHY:

1.2.1 VEDIO STEAGNOGRAPHY

In spite of the fact that BMP records are ideal for stenographic usage, they find themselves able to carry just small documents. So there is an issue, how to get sufficiently much documents to conceal our message, and what to do to peruse them in a right request? Great way out is to hide data in a feature document, in light of the fact that as we probably are aware, AVI records are made out of bitmaps, joined into one piece, which are played in right request and with suitable time gap. Remembering that we should simply to get out is document single frame and spare them as BMP documents. If we use algorithm for concealing information in computerized pictures, we can hide our message in bitmap acquired along these lines, and afterward spare it into new AVI document.

We'll investigate just uncompressed AVI record, in light of the fact that if any pressure is executed records loses its information.

AVI records are made out of couple streams. Fundamental record stream is a feature stream and sound stream, which can be document of any augmentation, for instance WAVE. In light of presence of those streams, it is conceivable to shroud information in document's edges as well as in specified sound stream. On account of this we can consolidate chances of concealing information in computerized pictures and in sound records.

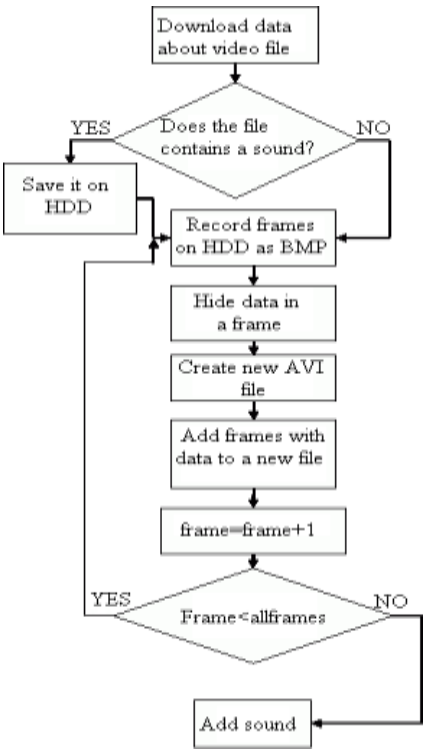

Fig 3. Algorithm of hiding messages in video files

1.2.2 TEXT STENOGRAPHY:

Hiding data in content is the most vital technique for steganography. The strategy was for hiding the secret message I each nth letter i of each expression of an instant message. After booming of Internet and diverse kind of advanced document positions it has diminished in significance. Text stenography as indicated in Fig. 4, utilizing advanced records is not utilized frequently in light of the fact that the text documents have a little measure of repetitive information [9].

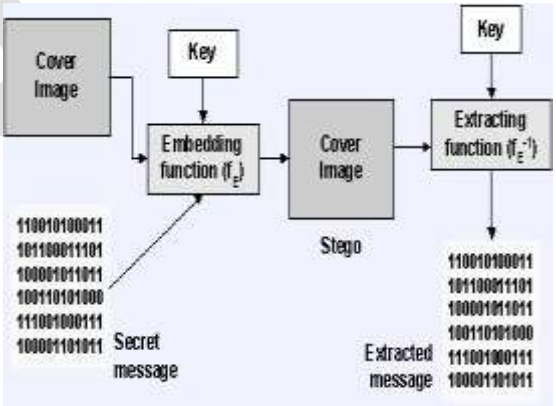

Fig 4 Image showing Text steganography

1.2.2 IMAGE STENOGRAPHY:

Images are utilized as the popular cover objects for steganography as indicated in Fig 5. A message is installed in a computerized image through an algorithm, utilizing the secret key [4]. The subsequent stego picture is Send to the recipient.

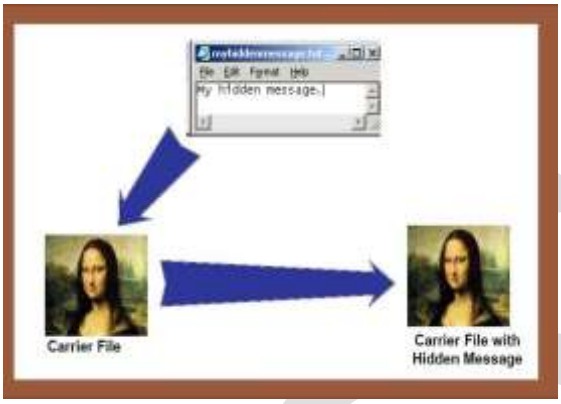

Fig 5 Image showing image steganography

On the other side, it is prepared by the extraction calculation utilizing the same key. Amid the transmission of steno picture unauthenticated persons can just notice the transmission of a picture however can't figure the presence of the concealed message [4].

1.2.3 AUDIO STENOGRAPHY:

Audio stenography is masking, which uses the properties of the human ear to hide data unnoticeably. A discernable, sound can be quiet in the presence of another louder perceptible sound .This property permits to choose the divert in which to hide data [8].

1.2.4 PROTOCOL STEGANOGRAPHY:

The term protocol steganography is to inserting data inside of system conventions, for example, TCP/IP. We hide data in the header of a TCP/IP parcel in a few fields that can be either optional or are never utilized [5].

2. RECENT WORK

Tiwari et al. [1]"Color Guided Image Steganography" Author need to suggest that the majority of the information hiding routines in picture steganography utilized a strategy known as LSB ie. Least significant bit. This, typically, create changes in the spread media however with no noteworthy impact. All the LSBs of pixels of spread picture can be utilized for concealing the secret bits. The hided data can undoubtedly be uncovered utilizing numerous known factual steganalysis methods.

Marwaha et al. [2] "Pixel Indicator High Capacity Technique for RGB Image Based Steganography" in this paper author want to say that the multimedia steganocryptic system, the message will first be encrypted using public key encryption algorithm, and then this encrypted data will be hidden into an image file. Each color in the multimedia data when considered as an element in an arrangement of 3D matrix with R, G and B as axis can be used to write a cipher (encoded message) on a 3D space. The method which we will use to map the data is a block or a grid cipher. This cipher will contain the data which will be mapped in a 3-D matrix form where the x-axis can be for R (red), y-axis can be for G green) and z-axis can be for B (blue)..Only jpeg image will be used as it reflects the least impact of steganography.

Gutub et al. [3] "Pixel Indicator Technique for RGB Image Steganography" in gathering, if the first pointer determination is the Red divert in the pixel, the Green is channel 1 and the Blue is the channel 2 i.e. the progression is RGB. In the second pixel in case we select, Green as the pointer, then Red is channel 1 and Blue is channel 2 i.e. the course of action is GRB. If in third pixel Blue is the pointer, then Red is channel 1 and Green is channel 2. The progression of the figuring is given underneath. The beginning 8 bytes toward the begin of the photo are used to store the degree of the covered message, which is furthermore used to describe the begin of the marker channel gathering. These 8 bytes exhausts all LSBs of the RGB channels, tolerating it is adequate to store the measure of the covered bits. Determinations are unending supply of bits.All six possible decisions are obtained from the length of message (N), if N worth is neither even nor prime, "else" line is picked, selecting the pointer to be G and the channels R and B are for riddle data holding.

Bailey and Curran [4] "Visual cryptographic steganography in pictures "Creator depicted a picture based multi-bit steganography procedure to expand limit concealing mysteries in number of bits, i.e. Stego-1bit, Stego-2bits, Stego-3bits and Stego-4bits. Stego-1bit is the least complex of this, where it embeds the mystery message information into one LSB (lower request bit) of the picture pixels, which is imperceptible. Find the stowaway is an illustration of this procedure. In the Stego-2bits system two bits of lower request LSB in RGB picture steganography is utilized; Stego-2bits multiplied the limit of message covering up with insignificant security decrease. The limit can be upgraded all the more as in Stego-3bits and much all the more in stego-4bits, which are risking security appropriately.

3. APPROACHES FOR THE PROPOSED WORK

3.1 STEGANOGRAPHIC TECHNIQUES

3.1.1 SUBSTITUTION TECHNIQUE

In the substitution strategy; the excess parts are secured with a mystery message [5]. This system incorporates the Least Significant Bit Substitution technique, where we select the subpart of principle picture and substitute the slightest huge bits of every component by the message bits. This is a simple technique yet is helpless against debasement because of little changes in bearer [9].

3.1.2 TRANSFORM DOMAIN TECHNIQUE

In the exchange area strategy; the mystery message is installed in the change space (e.g. recurrence area) of the spread. A case of this technique incorporates the Discrete Cosine Transform (DCT) area. The spread picture is split into 8*8 squares and every piece is utilized to encode one message bit. The squares are picked in a pseudorandom way. The relative size of two predefined [8].

3.3.3 SPREAD SPECTRUM TECHNIQUE

This technique uses the concept of spread spectrum. The signal to noise ratio in every frequency band is so small that it is difficult to detect [7]. Hence, it is tough to remove the message fullydestroying the cover .It is a very robust technique that finds application in military communication.

3.1.4 STATISTICAL TECHNIQUES

In the factual methods, the data is encoded by changing a few properties of the spread. The spread is split into blocks.If the message bit is one, then the spread piece is altered generally not. This strategy is hard to apply on the grounds that a decent test must be found that considers legitimate qualification in the middle of adjusted and unmodified spread pieces [10].

3.1.5 DISTORTION TECHNIQUES

The data is put away by bending the sign. The encoder applies a game plan of changes to the spread. This course of action identifies with the riddle message. The decoder measures the complexities between the first cover and the bended spread to recognize the course of action of modifications and in this manner recover the riddle message [6]. This methodology is not used as a piece of various applications in light of the fact that the decoder must have permission to the first cover.

3.1.6 PROTECTION OF DATA ALTERATION

We exploit the delicacy of the installed information in this application zone Gutub et al. [12]. On the off chance that it is executed, individuals can send their "advanced testament information" to wherever on the planet through Internet. Nobody can fashion, adjust, nor alter such authentication information. In the event that fashioned, changed, or altered, it is effortlessly distinguished by the extraction program.

3.1.7 ACCESS CONTROL SYSTEM FOR DIGITAL CONTENT DISTRIBUTION

Since the coming of computer science, the field of correspondence has been reformed. We can rightly call 21st century the period of PCs, web and data innovation. The web as with all way breaking mechanical improvements gives us each chance to go about as worldwide group; publicize and work over all boondocks, over fringes and outside the ability to control of any national Government. The extreme volume of data, the effortlessness of its move and straightforwardness in this field make a considerable measure of issues. Responsibility for is difficult to secure; the illegal reuse of copyright material is ordinary in our times. Corporate houses everywhere throughout the world have the anxiety of their information being abused by their rivals with ulterior thought process [5].

Indeed, even the Governments have developed exceptionally careful and ready in such manner. Subsequently the specialists in the field of computer science encouraged by the rule or proverb: 'need is the mother of all creations' produced steganography with the end goal of keeping the critical information and data mystery. A few universal foundations are likewise endeavoring to create information security standards which may be perceived and held fast to globally. Private data and information are of an incredible centrality in the cutting edge universe of globalization commanded by rivalry.

A broker or business element tries to acquire however much data as could reasonably be expected concerning the matter of his opponents and to keep its own data and information as disguised as could be allowed. The data may be a competitive advantage, for instance, a technique for creation not ensured by a patent, or a business mystery, for example, money related organizing of a major

house or a bit of household 'in house' data like the compensation sizes of workers, or the effectiveness of the company's information accumulation and preservation.

3.1.8. MEDIA DATABASE SYSTEMS

In this application territory of steganography mystery is not essential, but rather bringing together two sorts of information into one is the most vital.

Media information (photograph picture, film, music, and so on.) have some relationship with other data. A photograph picture, for occurrence, may have the accompanying [1].

•The title of the photo and some physical item data

•The date and the time when the photo was taken

•The camera and the picture taker's data

Steganalysis is the specialty of distinguishing the vicinity of shrouded information in documents [1], and is a method for concealed data identification and extraction. At this point, numerous widespread steganalysis systems for JPEG pictures have been proposed, among which the all inclusive steganalysis technique in view of different eigenvector with bolster vector machine (SVM) is the most well known one. Most steganalysis identification routines utilize the SVM or different classifiers for the preparation and recognition forms. Then again, these strategies have heaps of deficiencies, for example, undesirable expectation precision, inexorability of "over fitting

3.2 SPATIAL DOMAIN STEGANOGRAPHY

These techniques use the pixel gray levels and their color values channels forencoding the message bits. These techniques are some of the simplest schemes interms of embedding and extraction complexity [15]. For loss compression schemeslike JPEG, some of the message bits get lost during the compression step.The most common algorithm belonging to this class of techniques is the Least Significant Bit (LSB) replacement technique in which the least significant bit of the binary representation of the pixel gray levels is used to represent the message bit. This kind of embedding leads to an addition of a noise of 0:5p on average in the pixels of the image where p is the embedding rate in bits/pixel [12].

Advantages

- Along with traditional media, steganography is also very popular in digital media
- The embedded information is usually hidden to senses and the carrier media do not attract
- Attention to itself.

Disadvantage

- The major drawback of these methods is amount of additive noise that creeps in the image which channels affects the Peak Signal to Noise Ratio and the statistical properties of the image.
- Moreover these embedding algorithms are applicable mainly to lossless image-compression schemes like TIFF images.

3.2.1 RENDER PIXEL

Sub pixel rendering is an approach to build the evident resolution of a PC's Liquid crystal display (LCD) or organic light-emitting diode (OLED) show by rendering pixels to consider the screen sort's physical properties. It exploits the way that every pixel on a color LCD is really made out of individual red, green, and blue or other shading sub pixels to against assumed name content with more noteworthy point of interest or to build the determination of all picture sorts on formats which are particularly intended to be perfect with sub pixel rendering[13].

3.2.2DISCRETE WAVELET TRANSFORM

The wavelet transform has gained widespread acceptance in signal processing and image compression. Recently the JPEG committee has released its new image coding standard, JPEG-2000, which has been based upon DWT. Wavelet transform decomposes a signal into a set of basic functions. These basis functions are called wavelets. Wavelets are obtained from a single prototype wavelet called mother wavelet by dilations and shifting [13]. The DWT has been introduced as a highly efficient and flexible method for sub band decomposition of signals. The 2DDWT is nowadays established as a key operation in image processing .It is multi-resolution analysis and it decomposes images into wavelet coefficients and scaling function. In Discrete Wavelet Transform, signal energy concentrates to specific wavelet coefficients. This characteristic is useful for compressing images[9]. Wavelets convert the image into a series of

wavelets that can be stored more efficiently than pixel blocks. Wavelets have rough edges, they are able to render pictures better by eliminating the ―blockings.

Advantage

- DWT ismuch preferred because it provides both a simultaneous spatial localization and a frequency spread of thewatermark within the host image.
- The basic idea of discrete wavelet transform in image process is to multidifferentiateddecompose the image into sub-image of different spatial domain and independent frequencies[1][6] .

Disadvantage

- Robustness can be achieved by increasing the strength of the embedded watermark, but the visible distortion would be increased as well

3.2.3 DISCRETE COSINE TRANSFORM

A discrete cosine transform (DCT) expresses a finite sequence of data points in terms of a sum of cosine functions oscillating at different frequencies. The use of cosine rather than sine functions is critical for compression, since it turns out (as described below) that fewer cosine functions are needed to approximate a typical signal, whereas for differential equations the cosines express a particular choice of boundary conditions [11].

In particular, a DCT is a Fourier-related transform similar to the discrete Fourier transform (DFT), but using only real numbers. DCTs are equivalent to DFTs of roughly twice the length, operating on real data with even symmetry (since the Fourier transform of a real and even function is real and even), where in some variants the input and/or output data are shifted by half a sample. There are eight standard DCT variants, of which four are common.

Advantages:

- Semantically meaningful watermark pattern
- Good perceptual invisibility
- Acceptable robustness
- Reasonable complexity/execution time

Disadvantage

- They are difficult to implement
- Computationally more expensive. At the same time they are weak against geometric attacks like rotation, scaling, cropping etc.

4. CONCLUSION

- For the analysis of the proposed problem, there are various phases in which information will be encoded. It is comprise of three phases.
- Firstly, video will be compressed by adding various bits. The encoder will encrypt the video by using secret key to hide information so that it should be shared secretly.
- Then decompression will be done. Itcovert the information so that the existence and nature of the information will be only known by the sender and intended recipient.
- The information will be hidden into a file and send to the receiver for decryption.The least significant bits will be decrypted by the receiver to get the secret information.

REFERENCES:

[1]. Behera, S.K. “Colour Guided Colour Image Steganography”, Universal Journal of Computer Science and Engineering Technology**,** Vol. 1, No. 1, pp. 16-23, IEEE, 2010.

[2]. Gutub, A. “Pixel Indicator High Capacity Technique for RGB Image Based Steganography”, WoSPA 2008 – 5th IEEE International Workshop on Signal Processing and its Applications, University of Sharjah, U.A.E**.,** pp. 154-159,IEEE,2008.

[3]. Gutub, A. “Pixel Indicator Technique for RGB Image Steganography”, Journal of Emerging Technologies in Web Intelligence,Vol. 2, No.1, pp. 193-198,IEEE,2010.

[4]. Marwaha, P. "Visual cryptographic steganography in images", Second International conference on Computing, Communication and Networking Technologies, pp. 34-39, IEEE, 2010.
[5]. Bailey, K. "An evaluation of image based steganography methods", Journal of Multimedia Tools and Applications,Vol. 30, No. 1**,** pp. 55-88,IEEE,2006.
[6]. Mahata, S.K. "A Novel Approach of Steganography using Hill Cipher", International Conference on Computing, Communication and Sensor Network (CCSN), pp 0975-888, IEEE, 2012.
[7]. Chapman, M. Davida G, and Rennhard M. "A Practical and Effective Approach to Large Scale Automated Linguistic Steganography" found online at http://www.nicetext.com/doc/isc01.pdf.
[8]. Mehboob, B. "A stegnography implementation", Biometrics and Security Technologies, 2008. ISBAST 2008. International Symposium, ISSN 978-1-4244-2427-6, pp 1 – 5, IEEE, 2008.
[9]. Saravanan, V. "Security issues in computer networks and stegnography", Intelligent Systems and Control (ISCO), 2013 7th International Conference, ISSN 978-1-4673-4359-6,pp 363 – 366,IEEE,2013.
[10]. Moon, S.K. "Data Security Using Data Hiding" Conference on Computational Intelligence and Multimedia Applications, 2007. International Conference, ISSN 0-7695-3050-8,pp 247 – 251,IEEE,2007.
[11]. Andrew B. Watson,"Image Compression Using the Discrete Cosine Transform ", Mathematica Journal, 4(1), 1994, p. 81-88.
[12]. A.M.Raid, W.M.Khedr, M. A. El-dosuky1," Jpeg Image Compression Using Discrete Cosine- A Survey",International Journal of Computer Science & Engineering Survey (IJCSES) Vol.5, No.2, April 2014, pp 39-47.
[13]. M. MozammelHoque Chowdhury and Amina Khatun,"Image Compression Using Discrete Wavelet Transform", IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 4, No 1, July 2012, pp 327-330.
[14]. Daneshkhah," A More Secure Steganography Method in Spatial Domain", Intelligent Systems, Modelling and Simulation (ISMS), 2011 Second International Conference on, 25-27 Jan. 2011, pp 189 – 194.
[15]. G.S.Sravanthi, .B.Sunitha Devi," A Spatial Domain Image Steganography Technique Based onPlane Bit Substitution Method" Global Journal of Computer Science and Technology Graphics & Vision Volume 12 Issue 15 Version 1.0 Year 2012