IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 5, May 2016

A Short Survey on Cover Objects for Hidden Communications

Vidya[1], Abhishek Kajal[2]

Student of M.Tech, Department of Computer Science & Engineering, Guru Jambheshwar University of Science & Technology, Hisar, Haryana, India[1]

Assistant Professor, Department of Computer Science & Engineering, Guru Jambheshwar University of Science & Technology, Hisar, Haryana, India[2]

Abstract: In this survey paper we will discuss about the types of the steganography cover objects. Steganography is an art and science of Hide the data in a cover image using some techniques that it remains undetected by the unauthorized access. We hide the data in a manner that the stego image looks like a single entry by any third person. No one has doubt that the image is the stego image. We use some different methods that keep data to be secret. It is a powerful tool for security with which we can keep the data secret behind an object. An object may be Text, Audio, Video, and Image. The factor that affects the steganography methods are PSNR, MSE, SNR, Payload Capacity and Robustness.

Keywords: Steganography, PSNR, MSE, Stego-Image, Stego-Key, Data covering, Data Extraction, Cryptography.

I. INTRODUCTION TO STEGANOGRAPHY

Exponentially increase in the use of internet it becomes important to secure the confidential data and information on internet. Hence, there is need to cover the defensive information on the internet. To avoid these problems many methods are used to hide the data in digital media that are below.

One is Cryptography; it only keeps the contents of the message secret i.e. No one can understand the secret message. But sometimes it is necessary to keep the existence of the message is secure that no one can think even a single secret bit is existing. So, a technique which keeps the existence of a message secret is known a steganography [1].

Steganography is an art and science of hiding information [2] in some cover media. It aims is to hide the presence of the secret message behind any object (Text, Image, Video, Audio) file By embedding one piece of data inside of another, the two entity become a new single entity, thus eliminating the need to keep a link between the two distinct pieces of data, or risk the chance of their separation. After hide the message in any object file called Stego Image. In this technology we will use many type of techniques using different type of the cover objects.

One application that demonstrate the advantage of this regards of steganography is the embedding of patient information within the medical imaging. By doing so a persistent association between these two information objects is generate [3-5].

"What You See Is What You Get" this concepts which we encounter sometimes does not always hold true. Images can be more than what we see with our Visual System; hence they can convey more than merely 1000 words. Figure1.1 (Types of the Steganography cover objects) shows how a Stenographic system works [6, 7].

II. TYPES OF STEGANOGRAPHY COVER OBJECTS

There are many types of the cover objects we have to study. Cover object is the object which is used to hide the secret bits in the bits of the cover objects bits. We have to modify the bits to hide the data in the cover objects. The detailed explanation of the cover objects.

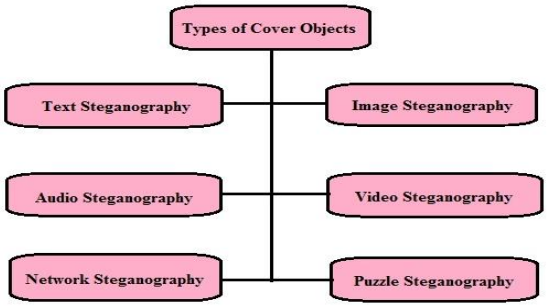

Fig. 1. Types of the Steganography cover objects

1. TEXT STEGANOGRAPHY

Text Steganography is depends on the formatting of text, or by altering certain characteristics of textual elements e.g.; Characters. : Conveying information secretly and establishing hidden relationship has been of interest. Text documents have been widely used for many years ago. So, we have witnessed distinct method of covering information in texts data (text steganography) since origins to the present. In this paper we introduce a new approach for steganography in Persian and Arabic texts.[15] The objective in the design of coding methods is to develop

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 5, May 2016

alterations that are reliably decode (in presence of noise) yet largely indiscernible to the reader. These criteria, reliable extraction and minimum visible change, are somewhat conflicting; The document format file is a computer file describing the document content and page formatting, using standard format description languages. It is less usually and gives less security. The three coding techniques that we explain have many approaches. Each technique has own benefits or advantages as we discuss below:

1. Line- Shift Coding

This is an approach of altering a document by vertically shifting the placement of text lines to put in to the code the document uniquely .This encoding may be applied either to the format file or to the bitmap of a page image. The Code or secret data embedded may be extracted or mining from the stego text or bitmap. In certain cases this decoding can be execute without need of the original image, since the original is known to have equable line spacing between adjacent lines within a Paragraph.

2. Word-Shift Coding

It is a method of adjust a document by horizontally drift the locations of words within text lines to encode the document uniquely while maintaining a natural content apparent. This encoding can also be applied to either the format file or the page image bitmap. The method is implementing only to documents with variable spacing between adjacent words.as a result of this variable content, it is significant to have the original photo, or to know the spacing between words in the un-coded document. For each text-line, the largest and smallest spaces between words are found. To code a line, the largest spacing is reduced by a convincing amount, and the basic is protected by the same amount. This maintains the line length, and produces little visible change to the text. The differences in spacing would reveal encoded data.

3. Feature Coding

The third method for text steganography is feature coding which applied either on Bitmap image or t a format file. In this Type of coding some text feature are altered, or not altered, it depends on the code word. Generally, before encoding, feature randomization takes place. Character end line lengths would be randomly lengthened or shortened, then altered again to encode the specific data. It removes the possibility of visual decoding as the original end line lengths would not be known. When trying to attack a feature-coded document, it is interesting that a purely random adjustment of endline [8] lengths is not a particularly strong attack on this coding method. This is another form of text steganography defined by Chapman. It is a method of using written natural language to conceal a secret message [9].

2. IMAGE STEGANOGRAPHY

In computer, a picture is an array of numbers that show light intensities at different points (pixels).In an image there are very much redundancy where the intensity of a pixel is same to we can use the image in the steganography removing the redundancy from the image and place the secret data bit in the image. Using this approach the size of the image is not exceeding because we replace the bit after removing the redundancy. An image with the secret information is spread over all the world and no one knows about the secret data. The use of steganography in newsgroups has been explored by German steganographic expert Niels Provos, who created a scanning cluster which detects the existence of covered messages inside images that were posted on the net Instead of after checking one million images, no hidden messages were found, and so the practical use of steganography still seems to be limited. Hide the message in image without changing its visibility property or limited changes due to the message hidden, less noise. Hiding the message is performing like that no more change in the image intensity or not more visible by the user or any third party. The process of the steganography is shown in fig 2.2(Steganography Process).

The most using method is LSB method, masking, filtering and transformations on the cover image. Digital images are typically stored in either 8-bit or 24-bit files. A 24-bit image provides the most space for hiding information; however, it can be quite large (with the exception of JPEG images).

IMAGE COMPRESSION

An image is a collection of numbers that constitute different light intensities in different areas of the picture. This numeric illustration forms a grid and the unique points are referred to as pixels (picture element). Greyscale images has 8 bits for each and every pixel and able to display 256 different colours of grey. Digital true colours images are typically stored in 24-bit files and use the RGB colour model, also known as true color [7]. All colour variations for the pixels of a 24-bit image are derived from three primary colours: red, green and blue, and each primary colour is represented by 8 bits [11]. Thus in one given pixel, there can be 256 different quantities of red, green and blue [7].

There are two forms of compression. These are:

1. Lossless compression (ex: GIF, BMP): where the original image can be reconstructed exactly like original. This is preferred where the original message must remain intact without any discrepancies in the information which is desired to be sent secretly.

2. Lossy compression (ex: JPEG): where it may not contain the unity of the original image but it flex very good compression.

An example of lossy compression that will use lossy compression technique is JPEG (Joint Photographic Experts Group) [7] When we embed the data in an image then we need two things cover image and hidden data. Cover image is the image that contains the hidden data. And 2nd is the hidden message that will hold by the cover image. The data which will be hidden in any form i.e. Plain

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 5, May 2016

text, cipher text and other image. When we combined cover image and message hidden then the output image is called Stegoimage .To hide the message we use a key that is called Stego-key. This key is also used for extracting the message at the receiver side. Once a suitable cover image has been selected, an image encoding technique needs to be chosen. [10]

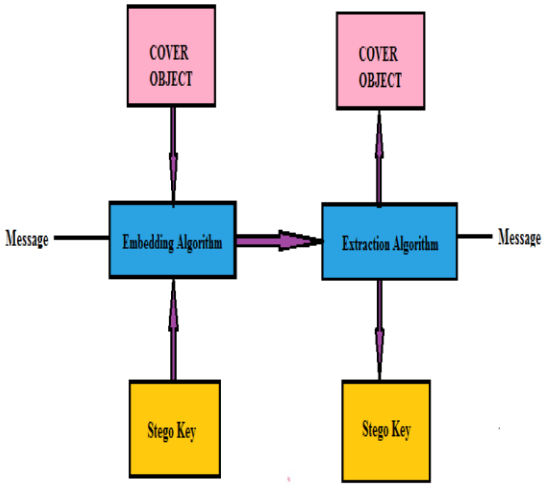

Fig. 2. Steganography Process

3. AUDIO STEGANOGRAPHY

Information hiding technique is a new kind of secret communication technology. Audio steganography is an approach used to transmit hidden some secret data by changing the digitized audio signal in an manner which results slight altering of binary sequences of the corresponding audio file.

[13] .Here the cover image is used as an audio signal in which we hide our message by changing the audio signal of the audio

[12]. Embedding the secret data in the audio signal is more difficult process impractically. In audio steganography, secret message is embedded into digitized audio signal which arise slight modified of binary sequence of the corresponding audio file.

Least Significant Bit (LSB) technique is one of the easiest techniques for secure data transfer. In this different data hiding methods used to protect the information. Audio data hiding is one of the most effective ways to protect the privacy. [14].
There are many methods of audio steganography. These methods are as follows:

i) Low Bit Encoding
ii) Phase Coding
iii) Spread Spectrum.

4. VIDEO STEGANOGRAPHY

It is very necessary to send the important data like banking and military secret data in a secure and covered manner. Video steganography is the method of covering some undercover information inside a video. The cover image is here a video. The inclusion of this information to the video is not noticeable by the human eye as the change of a pixel color is negligible [17] by the third party. Video is steganographically inject to convey a plural bit data without inject apparent fixed basis noise. The video comprises plural frames, each of which includes plural touple of video data. Inject of data reflects a pattern of changes to a touple of elementary (original) video to yield a touple of encoded video. But that touple—in a successive frame (e.g., the next frame)—is changed by a different pattern. Fixed pattern antiquities are thus neglected. In some adjustments, the frames transmit different messages. In others the frames transmit the same message, but the apparent effect is changed by different noise data used in the encoding [16].

5. NETWORK STEGANOGRAPHY

Many Steganographic Object are used in the steganography methods. If the cover object which is used to cover the secret data is Telecommunication Media or Network then it will classified under the Network Steganography the following we will discuss are other type cover object.

This is introduced by the "Krzyszlof Szcypiorski" in 2003[32]. It is typical method that will use the communication Protocol elements and inseparable functionality. It results a strong cover media object that is difficult to detect alteration and deletion. Generally this steganography involve the modification of the resources of single network protocol. This type of change can be implemented on the PDU (Protocol Data Unit) [33]34] [35] in time relation according to interchanged PDU's. Furthermore it is also possible to use the relation between the two or more distinct protocol to cover the secret data.

Network Security covers a big spectrum of techniques which is as follows:
1. The Covering of the secret message in the Voice-over-IP conversations. For E.g. the Delayed or the damaged packets of conversations that would generally ignored by the receivers. This is called LACK (LOST Audio Packets Steganography). Also we will hide the message in the header of the packet which contains the unused header fields [36].
2. Wireless LAN Steganography: In this wireless LAN steganography, basically we use the HICCUPS system which is stands for Hidden Communication System for Corrupted Networks [37].

6. USING PUZZLE STEGANOGRAPHY

The method of hiding the data in the Puzzles is a great idea because it can take the advantage of the degree of the freedom, using the information to put into any code means encoding a key inward the puzzles o puzzles images also. In the Sudoku puzzles we have many keys are there are many feasible solutions of the Sudoku puzzles which are $6.71* 10^{21}$.This is around to 70 bits. It makes this very stronger than the DES method. DES method have 56 bit key.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 5, May 2016

III. SOME STEGANOGRAPHY MEASURE ALGORITHMS

Steganographic measures are the measures that affect our steganography. This tells about the quality or efficiency of the steganography techniques. The effectiveness is determined by the difference between the Cover object and stego object.

1. **SSIM Index (Structural Similarity Index):** This index [31] is used to find out the similarity between two Images. This Index is mainly used to ensure the quality of measure regarding the image. It measures the accurate comparison of the images in respect to the perfect quality. It is improved version of the universal quality image quality image index before. SSIM PLUS is also used for the measurement of the videos Quality of Experience (QoE) Index is designed for the practical use.

2. **Computational Complexity:** Computational complexity is the complexity which tells the cost of the message hiding and the message extraction using the steganography.

3. **Robustness:** Robustness[25] refers to the ability of embedded data to remain intact if the stego-image undergoes transfiguration, likewise linear and non-linear filtering, sharpening or blurring, addition of random noise, rotations and scaling, cropping or decimation, lossy compression.[26]

4. **Imperceptibility:** The imperceptibility [27] means invisibility of a stenographic algorithm. Because it is the first and foremost requirement, since the strength of steganography lies in its ability to be unnoticed by the human eye [26] [28].

5. **Payload Capacity:** It refers the capacity [26] of a stego image that hides the amount of the secret data. Watermarking [29] [30] usually store the copyright information. Whereas, steganography concentrate at hidden communication and therefore have sufficient hiding data capacity.

6. **Peak Signal to Noise Ratio (PSNR):** It is described as the ratio between the maximum possible power of a signal and the power of corrupting noise that reflects the accuracy of its representation.

The peak signal-to-noise ratio (PSNR) is the most common metric used to evaluate the stego image quality. However, subjective evaluation is the most reliable method to measure the image quality.

7. **MSE (Mean Square Error):** It is described as metrics of error used to compare image compression. The mean square error represents the progressive average squared error difference between an original picture and the changed image. The smaller the MSE, the best is image steganography technique. MSE is calculated pixel-by-pixel by sum the squared differences of all the pixels and dividing by the total pixel count [26].

TABLE I: Steganography measures that affects the steganography

Factors that affecting Steganography	Advantage	Disadvantage
SSIM Index	LOW	HIGH
Computational Complexity	LOW	HIGH
Robustness	HIGH	LOW
Imperceptibility	HIGH	LOW
Payload Capacity	HIGH	LOW
Peak Signal to noise Ratio	HIGH	LOW
Mean Square Error	LOW	HIGH

IV. RELATED WORK

Karim, S. M., Rahman, M. S., & Hossain, M. I. [18] et al presented the "LSB based image steganography using secret key". This paper introduces an efficient approach in image steganography using LSB technique. This enhances the efficiency of the existing LSB Insertion method to enhance the efficiency of the security level of the confidential data. This approach is used for the true color image in which we substitute LSB of the image. In this we also use the encryption scheme for the secret data using a secret encryption key to protect the data from unauthorized access. Usually in the LSB method, the secret bit is inserted in the LSB of the R, G, B bit values or a specific positions I s used to insert the secret bit of the LSB of the Image.

In this method the data is stored using a specific pattern that depends on the secret Key called Stego key. The reason behind is that the extraction of the messages is difficult because it only depends on the secret key. The peak signal to noise ratio is used to measure the quality of the stego image. The PSNR value is better because the propose system not change many bits. This system after measure the quality of the image, the results are better than Existing and provide good security issue and PSNR value than the general LSB Steganographic method. Chan, C. K., & Cheng, L. M. [19] et al presented the hiding data in images by simple LSB substitution. This paper introduces a data hiding method which uses the simple LSB method Simple LSB insertion method is used. Using this approach we give optimum pixel adjustments process on the stego image which will be obtained by applying the LSB

substitution method. The quality of the image after the LSB insertion is greatly improved because only LSB of the image is substituted, so not more change in the stego image than the cover image but with some extra complexity. The mean square error (MSE) of the stego image or the Cover image is calculated. The experimental results tell that the cover image is not more different from the stego image. The intensity is not more change of the image. The results also show a significant improve from the existing LSB

Zhang, T., & Ping, X. [21] et al presented a New Approach to reliable detection of LSB steganography in natural image, This paper represents a new stenographic scheme in which they focus on the statistical observation on the different histogram of the images for the best or reliable detection of the LSB(least significant bit)Steganography. It is mainly used for the detection of the steganography that an image contains the secret data or not using the histogram of the image (stego image or cover image). A physical quantity is derived from the transition coefficients between difference pictures histograms of an image and its processed version produced by setting all bits in the LSB plane to zero. It appears that this measure is a good quantity measure of the weak correlation between successive bit planes and can be used it differentiate the stego image and the cover images. It also indicates that the functional relationship between the quantity and the length of message embedded. Based on these facts, an equation is formed to estimate the amount of the date may be embedded in the cover image. Experimental results show that the proposed algorithm is comparable to previously proposed techniques. This technique is used for both the LSB method either for Random bit LSB and Sequential LSB.

Bailey, K., & Curran, K. [20] et al presented an evaluation of image based steganography method .This paper introduces that Steganography is an art and science of hiding information in some cover media. It aims is to hide the presence of the secret message behind any object (Text, Image, Video, Audio) file By embedding one piece of data inside of another, the two entity become a new single entity, thus eliminating the need to keep a link between the two distinct pieces of data or risk the chance of their separation. After hide the message in any object file –called Stego Image.

The initial aim of this study was to inspect steganography and how it will appliance. Based on this work a number of common methods of steganography could then be appliance and criticize. The strengths and weaknesses of the chosen methods can then be analyzed. Generally the GIF image is used for common frame of reference all of steganography technique. The methods were selected for their different strengths in terms of resistance to different types of steganalysis or their ability to magnify the size of the message they could store. All these technique is mainly based on the manipulation of the bit array of the pixel of the image or some pattern manipulation which correspond to the message being hidden.

Johnson, N. F., & Jajodia, S. [11] et al represents the Exploring steganography: Seeing the unseen. This paper introduce the Steganography is the art of hiding information in ways that the existence of the secret message is hidden. So no unauthorized access is possible in way. Here we are talking about that no one can see the message is here in the background of the image. Using steganography we prevent the existence of the message. It includes many techniques to implement the steganography. These methods include invisible inks, microdots, character arrangement, digital signatures, covert channels, and spread spectrum communications. Steganography and cryptography is little bit same because both are using for security of the secret data in the spy world or in the digital word. Cryptography is used to encode the message using a key (Symmetric key and Asymmetric Key).The unauthorized user know the encoded data but can't understand the data without the key. But in steganography the existence of the data is hidden from the third party. This article the authors discuss image files and how to hide information in them, and discuss results obtained from evaluating available steganographic software. They argue that steganography by itself does not ensure secrecy, but neither does simple encryption.

If these methods are combined, however, stronger encryption methods result. If an encrypted message is intercepted, the interceptor knows the text is an encrypted message. But with steganography, the interceptor may not know that a hidden message even exists. For a brief look at how steganography evolved, there is included a sidebar titled "Steganography: Some Yadav, R. [22] et al represents the analysis of incremental growth in image steganography techniques for various parameters. This paper states that Data security is getting very popular in the digital world for the security reasons during last two decades. So to implement this we mainly use the steganography since last few years. Steganography is an art and science of covering the data in some cover media like image file, audio file, video file, text file etc. Out of the various cover media are here but image file is generally used as cover media. There are many techniques that are widely used for image steganography during the last decade. In this paper, we will analyze how the incremental growth takes place in different image steganography techniques for many different parameters. Different parameters give different results which are may be good or bad results.

Batra, S., & Rishi, R. [23] et al., This paper represents an approach in which the probability of the message entering at 1st time is from 50% to 85.93%. This paper states that we will work on the 6th, 7th and 8th bit of the binary equivalent. In this we will suggest a new thing i.e. time factor. In this the sender sends the three cover images. These cover image one is having the secret message but other two don't have any message. This approach is very advantageous because no one knows which object having the secret data and which one is not having the messages bit. So it means if intruder has the cover images and

DOI 10.17148/IJARCCE.2016.55107

change the LSB bits of the pixels of the images even then the message can't extracted. Saini, R., & Yadav, R. [24] et al., used the logical AND operation on both selected pixel position and selected pixel intensity. According to this paper first step is that we will convert the pixel position and pixel intensity into the binary format. Then the 2nd step is the four LSB bits of this binary equivalent are deleted and the logical AND operation is applied on these for bits.

When we want to insert the bit 0 then the logical AND must be the 0. Likewise if want to insert the value 1 then the result is also must be greater than 0 after the Logical AND. If this is not done then the pixel intensity are changed as result greater than 0 after the logical AND. This is all done to the sender side where we perform the data hiding steganography. At the receiver side first we calculate the Logical AND of the pixel position and pixel intensity. After calculating if the result is 0 then the message is 0 otherwise the message bit 1. This gives advantageous is that the extraction process is more difficult. The reason behind is that the bits are uniformly distributed on all bits of the pixels value.

V. CONCLUSION AND FUTURE SCOPE

In this survey paper we have review many paper on the steganography cover objects. This paper is good enough to start the research for a new comer. LSB is the mainly used technique in the steganography techniques using the image object as cover object and also with all the type of the cover objects. These cover objects are also used by all the techniques like MSB, Watermarking, Spatial Technique, and Distortion Techniques. Using these Cover objects, it gives a great meaning of the secure transmission in steganography. In the related work it will help a lot to the starter in the field of the steganography cover objects. We use different type of the cover objects for the high security and hiding data. In future research we may use the cryptographic algorithm with data reduction and then implement the steganography called Hybrid steganography. It will increase the security of data and also increase the capacity of the cover object for hiding more data.

REFERENCES

[1]. Morkel, T., Eloff, J. H., & Olivier, M. S. (2005, June). An overview of image steganography. In ISSA (pp. 1-11).
[2]. Petitcolas, F. A., Anderson, R. J., & Kuhn, M. G. (1999). Information hiding-a survey. Proceedings of the IEEE, 87(7), 1062-1078.
[3]. Marvel, L. M. (1999). Image steganography for hidden communication (Doctoral dissertation, University of Delaware).
[4]. Chandramouli, R., Kharrazi, M., & Memon, N. (2003). Image steganography and steganalysis: Concepts and practice. In Digital Watermarking (pp. 35-49). Springer Berlin Heidelberg.
[5]. Al-Mohammad, A. (2010). Steganography-based secret and reliable communications: Improving steganographic capacity and imperceptibility (Doctoral dissertation, Brunel University, School of Information Systems, Computing and Mathematics Theses).
[6]. Morkel, T., Eloff, J. H., & Olivier, M. S. (2005, June). An overview of image steganography. In ISSA (pp. 1-11).
[7]. Cheddad, A., Condell, J., Curran, K., & Mc Kevitt, P. (2010). Digital image steganography: Survey and analysis of current methods. Signal processing, 90(3), 727-752.
[8]. Brassil, J. T., Low, S., Maxemchuk, N. F., & Gorman, L. O. (1995). Electronic marking and identification techniques to discourage document copying. Selected Areas in Communications, IEEE Journal on, 13(8), 1495-1504.
[9]. Chapman, M., Davida, G. I., & Rennhard, M. (2001). A practical and effective approach to large-scale automated linguistic steganography. In Information Security (pp. 156-165). Springer Berlin Heidelberg.
[10]. Chanu, Y. J., Tuithung, T., & Manglem Singh, K. (2012, March). A short survey on image steganography and steganalysis techniques. In Emerging Trends and Applications in Computer Science (NCETACS), 2012 3rd National Conference on (pp. 52-55). IEEE.
[11]. Johnson, N. F., & Jajodia, S. (1998). Exploring steganography: Seeing the unseen. Computer, 31(2), 26-34.
[12]. Djebbar, F., Ayad, B., Hamam, H., & Abed-Meraim, K. (2011, April). A view on latest audio steganography techniques. In Innovations in Information Technology (IIT), 2011 International Conference on (pp. 409-414). IEEE.
[13]. Balgurgi, P. P., & Jagtap, S. K. (2013). Audio steganography used for secure data transmission. In Proceedings of international conference on advances in computing(pp. 699-706). Springer India.
[14]. Kekre, H. B., Athawale, A., Rao, S., & Athawale, U. (2010). Information hiding in audio signals. International Journal of Computer Applications (0975–8887) Volume.
[15]. S Shirali-Shahreza, M. H., & Shirali-Shahreza, M. (2006, July). A new approach to Persian/Arabic text steganography. In Computer and Information Science, 2006 and 2006 1st IEEE /ACIS International Workshop on Component-Based Software Engineering, Software Architecture and Reuse. ICIS-COMSAR 2006. 5th IEEE/ACIS International Conference on (pp. 310-315). IEEE.
[16]. Rhoads, G. B. (2002). U.S. Patent No. 6,449,379. Washington, DC: U.S. Patent and Trademark Office.
[17]. Balaji, R., & Naveen, G. (2011, May). Secure data transmission using video Steganography. In Electro/Information Technology (EIT), 2011 IEEE International Conference on (pp. 1-5). IEEE.
[18]. Karim, S. M., Rahman, M. S., & Hossain, M. I. (2011, December). A new approach for LSB based image steganography using secret key. In Computer and Information Technology (ICCIT), 2011 14th International Conference on (pp. 286-291). IEEE.
[19]. Chan, C. K., & Cheng, L. M. (2004). Hiding data in images by simple LSB substitution. Pattern recognition, 37(3), 469-474.
[20]. Bailey, K., & Curran, K. (2006). An evaluation of image based steganography methods. Multimedia Tools and Applications, 30(1), 55-88.
[21]. Zhang, T., & Ping, X. (2003). A new approach to reliable detection of LSB steganography in natural images. Signal Processing, 83(10), 2085-2093.
[22]. Yadav, R. (2011). Analysis of Incremental Growth in Image Steganography Techniques for Various Parameters. Int. J. Comp. Tech. Appl, 2(6), 1867-1870.
[23]. Batra, S., & Rishi, R. (2010). Insertion of message in 6th, 7th and 8th bit of pixel values and its retrieval in case intruder changes the retrieval in case intruder changes the least significant bit of image. International Journal of Security and Its Applications, 4(3), 1-10.
[24]. Saini, R., & Yadav, R. (2012). A New Data Hiding method using Pixel Position and Logical AND operation. IJCER, 1(1).
[25]. Akhtar, N., Johri, P., & Khan, S. (2013, September). Enhancing the security and quality of LSB based image steganography. In Computational Intelligence and Communication Networks (CICN), 2013 5th International Conference on (pp. 385-390). IEEE.
[26]. Kour, J., & Verma, D. (2014). Steganography Techniques–A Review Paper. International Journal of Emerging Research in Management &Technology ISSN, 2278-9359.
[27]. Ma, X. Y., & Lin, J. J. (2009, September). Imperceptibility Evaluation for Color Stego Image. In Intelligent Information Hiding and Multimedia Signal Processing, 2009. IIH-MSP'09. Fifth International Conference on (pp. 783-786). IEEE.
[28]. Xiu-ying, M., & Jia-jun, L. (2009). HVS-Based Imperceptibility Evaluation for Steganography. In Scalable Information Systems (pp. 152-161). Springer Berlin Heidelberg.
[29]. Liu, Q., & Ying, J. (2012, June). Grayscale image digital watermarking technology based on wavelet analysis. In Electrical & Electronics Engineering (EEESYM), 2012 IEEE Symposium on (pp. 618-621). IEEE.

[30]. Steinebach, M., Hauer, E., & Wolf, P. (2007, November). Efficient watermarking strategies. In Automated Production of Cross Media Content for Multi-Channel Distribution, 2007. AXMEDIS'07. Third International Conference on (pp. 65-71). IEEE.
[31]. Wang, Z., Bovik, A. C., Sheikh, H. R., & Simoncelli, E. P. (2004). Image quality assessment: from error visibility to structural similarity. Image Processing, IEEE Transactions on, 13(4), 600-612.
[32]. Szczypiorski, K. (2003, October). HICCUPS: Hidden communication system for corrupted networks. In International Multi-Conference on Advanced Computer Systems (pp. 31-40).
[33]. Rowland, C. H. (1997). Covert channels in the TCP/IP protocol suite. First Monday, 2(5).
[34]. Murdoch, S. J., & Lewis, S. (2005, June). Embedding covert channels into TCP/IP. In Information hiding (pp. 247-261). Springer Berlin Heidelberg.
[35]. Ahsan, K., & Kundur, D. (2002, December). Practical data hiding in TCP/IP. In Proc. Workshop on Multimedia Security at ACM Multimedia (Vol. 2, No. 7).
[36]. Lubacz, J., Mazurczyk, W., & Szczypiorski, K. (2010). Vice over IP. Spectrum, IEEE, 47(2), 42-47.
[37]. Szczypiorski, K. (2003, October). HICCUPS: Hidden communication system for corrupted networks. In International Multi-Conference on Advanced Computer Systems (pp. 31-40).

DOI 10.17148/IJARCCE.2016.55107