International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

ANALYSIS OF IMAGE STEGANOGRAHY TECHNIQUES

V. Abinaya[1], Dr. M. Chidambaram[2]
[1]Research Scholar, [2]Reasearch Supervisor
PG and Research Department of Computer Science, Rajah Serfoji Government College, Thanjavur-613005
Affiliated to Bharathidasan University, Trichirappalli, TamilNadu, India

ABSTRACT: Nowadays, computer-based communications are at the opening of making life easier for everyone in the world; from sharing information, to communicating with each other, to exchanging documents and to checking bank balances and paying bills. It can be defined as the study of unseen communication that frequently deals with the ways of defeat the survival of the communication message. The data embedding is achieved in communication, validation and many other purposes. Generally data embedding is achieved in communication, validation and many other purposes. The hidden data can be text, audio, image or video accordingly to that can be enclosing from moreover image or video. The result presented in this paper, we enclose analyzed various Steganography techniques and also covered classification and application.

Keywords: Data hiding, Image Steganography Techniques, Encryption, sego file, image, video

1. INTRODUCTION

In today's world, the communication is the basic necessity of every growing area. Everyone wants the privacy and safety of their communicating data. In our daily life, we apply many secure pathways like internet or telephone for transferring and sharing information, but it's not safe at a assured level. Steganography is distinct as the skill and ability of concealing a covert message in different files types, for instance: digital image files, digital audio files, digital video files, and text files. Steganography word is originated from Greek words staginess (covered), and Grantors (writing) which literally means" cover writing". Steganography is known as "invisible" communication. It is different from projecting the actual content of a message. In simple word it would be like that, hiding information into other information.

1.1 STEGANOGRAPHY

Steganography is the exercise of concealing communication or information within other non-secret text or data. In this project, we are concealing information contained by images and hence the name "image Steganography". The information we are hiding can either be text or other images. Generally speaking, the project aims at hiding images/text inside images. Steganography means is not to change the structure of the secret message, but hides it inside a carrier object. Steganography is compared to Cryptography is that Cryptography scrambles a message so it cannot be understood, while Steganography hidden data cannot be seen. So, hiding information and projecting informations are totally different from one another. Steganography can be achieved by the following four scenarios:

- The Hiding text inside a grey-scale image.
- The hiding a text inside an RGB image.
- The Hiding a grey-scale image inside an RGB image.
- The Hiding an RGB image inside another RGB image.

For hiding text inside a grey-scale image, the LSB method is used. The text to be hidden is first converted in 8-bit ASCII and then appended with a 128-bit pattern on both sides. This pattern will help while decrypting the message as we will have a specific bit pattern to look for. Next, a random pixel is chosen in the image and for every pixel thereon, the 8^{th} bit is adjusted by adding/subtracting a few Intensity values in such a way that it matches a 0 or 1 binary value. This is encryption. While decrypting, the 128-bit pattern is searched by the function and the bits between the two 128 bit patterns is extracted and converted to text.

For hiding text into an RGB image, a similar approach is used except that one of the three channels(R, G, B) is used instead of the grey intensity values used in the above scheme.

For hiding an image inside another image, we use a method called 4-MSB. We only store the 4 most significant bits of both the images. The 4-MSB of the hidden image are stored as the 4-MSB in order to be hidden.

1.2 Steganography in Digital Processing:

Depending on the type of the cover object there are many suitable Steganography techniques which are followed in order to obtain security. It can be shown in figure-1

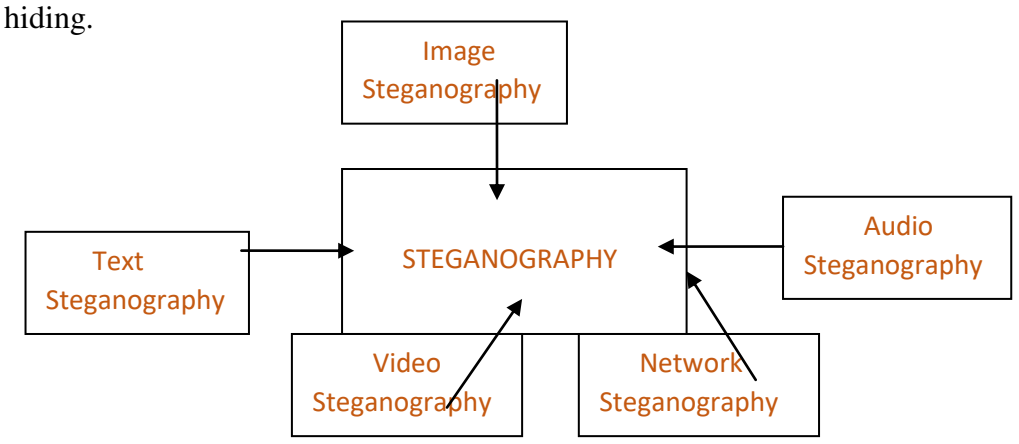
1.2.1. Image Steganography: Taking the cover object as image in steganography is known as image steganography. Generally, in this technique pixel intensities are used to hide the information.

1.2.2. Network Steganography: When taking cover object as network protocol, such as TCP, UDP, ICMP, IP etc, where protocol is used as carrier, is known as network protocol Steganography. In the OSI network layer model there exist covert channels where steganography can be achieved in unused header bits of TCP/IP fields [24].

1.2.3. Video Steganography: Video Steganography is a technique to hide any kind of files or information into digital video format. Video is used as carrier for hidden information. Generally discrete cosine transform (DCT) alter values which is used to hide the information in each of the images in the video, which is not noticeable by the human eye. Video steganography uses such as H.264, Mp4, MPEG, AVI or other video formats**.**

1.2.4. Audio Steganography: When taking audio as a carrier for information hiding it is called audio steganography. It has becomes very significant medium due to voice over IP (VOIP) popularity. Audio steganography uses digital audio formats such as WAVE, MIDI, AVI MPEG or etc for steganography.

1.2.5. Text Steganography: General technique in text steganography, such as number of tabs, white spaces, capital letters, just like Morse code [21] and etc is used to achieve information hiding.



1.3 Image Steganography Techniques

Image Steganography techniques can be divided into following domains.

1.3.1 Spatial Domain Method: The most basic and important image Steganography techniques method is least significant bits technique. There are many versions of special Steganography, all directly change some bits in the image pixel values in hiding data. Least significant bit (LSB) based Steganography is one of the simplest techniques that hides a secret messages in the LSB of pixel values without many perceptible distortions. In this technique data can be hidden in the least significant bits of the cover image and the human eye would be unable to notice the hidden image in the cover file. There are 256 possible intensities of each primary colour, so, changing the LSB of a pixel results in small changes in the intensity of the colours. These changes cannot be perceived by the human eye, thus the message is successfully hidden.

1. Least significant bit (LSB)
2. Pixel value differencing (PVD)
3. Edges based data embedding method (EBE)
4. Random pixel embedding method (RPE)
5. Mapping pixel to hidden data method
6. Labels connectivity method
7. Pixel intensive based method
8. Texture based method

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

9. Histogram shifting method

Advantage of spatial domain LSB technique:

1. There is less chance for degradation of the original image.
2. More information can be stored in an image.

Disadvantage of LSB Technique:

1. Less robust, the hidden data can be lost with image manipulation.
2. Hidden data can be easily destroyed by simple attacks.

1.3.2 Transform Domain Technique: This is a more complex way of hiding information in an image. The process of embedding data in the frequency domain of a signal is much stronger than embedding principles that operate in the time domain. Most of the strong Steganography systems today operate within the transform domain Transform domain techniques have an advantage over spatial domain techniques as they hide information in areas of the image that are less exposed to compression, cropping, and image processing. Some transform domain techniques do not seem dependent on the image format and they may outrun lossless and Lousy format conversions.

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.

1.3.3 Distortion Techniques: Distortion techniques need knowledge of the original cover image during the decoding process where the decoder function to check for differences between the original cover image and the distorted cover image in order to restore the secret message. The encoder adds a sequence of changes to the cover image. So, information is described as being stored by signal distortion. Using this technique, a sego object is created by applying a sequence of modifications to the cover image. This sequence of modifications is use to match the secret message required to transmit. The message is encoded at pseudo-randomly chosen pixels. If the sego-image is different from the cover image at the given message pixel, the message bit is a "1." otherwise, the message bit is a "0." The encoder can modify the "1" value pixels in such a manner that the statistical properties of the image are not affected. However, the need for sending the cover image limits the benefits of this technique. In any Steganography technique, the cover image should never be used more than once. If an attacker tampers with the stego-image by cropping, scaling or rotating, the receiver can easily detect it [1]. In some cases, if the message is encoded with error correcting information, the change can even be reversed and the original message can be recovered.

1.3.4 Masking and Filtering: These techniques hide information by marking an image, in the same way as to paper watermarks. These techniques embed the information in the more significant areas than just hiding it into the noise level. The hidden message is more integral to the cover image. The advantage of this method is much more robust than LSB replacement with respect to compression since the information is hidden in the visible parts of the image. The disadvantage of this technique is it can be applied only to gray scale images and restricted to 24 bits. Adaptive Steganography Adaptive steganography is special case of two former methods. It is also known as "Statistics aware embedding" and "Masking". This method takes statistical global features of the image before attempting to embed secret data in DCT or DWT coefficients. The statistics will dictate where to make changes

2. Literature Review

In this paper [1], author has proposed a new method based on unable visual image quality and data lossless method in spatial domain based on a genetic algorithm (GA). The most important proposal of that technique is modelling the Steganography difficulty as a search and optimization problem. Here author has make an effort to get best place for embedding modified secret data in host image to accomplish high level of protection. The process of embedding is achieved in two most important steps; initially they modify secret bits and then to embed it into host image. Due to hosting image in different places in defined by order of scanning host pixels and starting point of scanning and best LSBs of each pixel. However several techniques have been suggested for image Steganography, restricted studies have been done on met heuristic-based image Steganography and these efforts could not present logical reasons for benefit of their techniques. An experimental result shows that in comparison with existing accepted Steganography methods, demonstrate that the proposed algorithm not only accomplishes high embedding capacity but also improves the PSNR of the Sego image.

Here author [2] has presents the application of wavelet transform and genetic algorithm (GA) in a new Steganography method. Here they try to provide work for a GA based mapping function to embed data in discrete wavelet transform (DWT) coefficients in 4 * 4 blocks on the wrap image. The optimal pixel adjustment process (OPAP) is useful after embedding the message. Here they try to utilize the frequency domain to get better the strength of Steganography and then they implement GA and OPAP to obtain an optimal mapping function to condense the difference error between the cover and the sego-image, consequently improving the hiding capacity with low distortions. An experimental result shows that in comparison reveal that the new method do better than adaptive Steganography technique based on wavelet transform in expressions of PSNR and capacity, 39.94 dB and 50% correspondingly. IJSER International Journal of Scientific & Engineering Research, Volume 7, Issue 2, February-2016 420 ISSN 2229-5518 IJSER © 2016 http://www.ijser.org A new morphed Steganography algorithm is proposed [8] in this paper. Basically the image security is a difficult problem in now-a- days. So here author using Steganography technique for hiding secret data in cover medium. The Least Significant Bit is a typical Steganography technique that has several restrictions. The drawbacks are less capability to hide from view data, reduced sego image quality, and imperceptibility. Here author has to focuses on these drawbacks and new Steganography algorithm is proposed based on the morphing conception is being used for image Steganography to overcome these drawbacks. The PSNR and standard deviation are well thought-out as determine to get better sego image quality and morphed image selection, correspondingly. The sego keys are produced during the morphed Steganography embedding and extracting procedure. Sego keys are employed to embed and remove the secret image. As compare on experimental results with existing method which is based on hiding capacity and PSNR using proposed algorithm accomplishes an enhance in hiding capacity, sego image quality, and imperceptibility. The experimental results were compared with state of the art Steganography techniques. In this proposed work [9], here they studied the Steganography standard of data hiding in usual digital images. This proposed system presents a new method to increase the data hiding capacity and the imperceptibility of the image after embedding the secret message. In proposed work Optimal Pixel Adjustment Process also useful to minimize the error difference between the wrap and sego image. By this effort best effects have been acquired as compared to offered efforts. The proposed Steganography model decreases the embedding error and presents higher embedding capacity. Detection of message survival will be very inflexible for those sego images that manufactured using the proposed technique. Experimental result shows the highest embedding capability and security against Reversible Statistical attack.

Chen and Lin [3] propose a new Steganography technique which embeds the secret messages in frequency domain to show that the PSNR is still a satisfactory value even when the highest capacity case is applied. By looking at the results of simulation, the PSNR is still a relaxed value even when the highest capacity is applied. This is due to the different characteristics of DWT coefficients in different sub bands. Since, the most essential portion (the low frequency part) is kept unchanged while the secret messages are embedded in the high frequency sub-bands (corresponding to the edges portion of the image), good PSNR is not a imaginary result. In addition, corresponding security is maintained as well since no message can be extracted without the "Key matrix" and decoding rules. Amrita Nag, Susana Biwa's, Debaser Sakkara and Parthia Partum Sakkara [4] present a technique for image Steganography based on DWT. This paper presents a novel

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

technique for Image Steganography based on DWT, where DWT is used to transform original image (cover image) from spatial domain to frequency domain. First, two dimensional Discrete Wavelet Transform (2-D DWT) is performed on a gray level cover image of size M × N and Huffman encoding is performed on the secret messages/image before embedding. Then each bit of Huffman code of secret message/image is embedded in the high frequency coefficients resulted from Discrete Wavelet Transform. Image quality is to be improved by preserving the wavelet coefficients in the low frequency sub-band also.

J. K. Mandal et al. present another GA-based algorithm termed DEGGA. Focus in this method is on large amount of hidden data and the results are compared with another method by Ran- Zan et al. [5]. In Mandal method, large volume of message/ image is embedded in spatial domain using 3 x 3 masks from the source image. Four bits of the secret message / image is embedded per byte of the source image onto the rightmost 4 bit of each pixel. Mutation is applied on the embedded image. Also, a method of bit handling is applied to keep the fidelity high. In the process of embedding dimension of the secret message / image followed by the content of it. Reverse process is followed during decoding. Genetic algorithm is used to enhance a security level. Various statistical parameters computed that are compared with the Ran- Zan et al. method shows that proposed DEGGA obtained better results in terms of PSNR. Proposed method use gray scale image for secure message transmission. An authenticating image of size m x n is chosen as secret message. The size of the host image is p x q. Input: Host image of size pxq, authenticating image of size pxq. In follow, embedding algorithm is listed. Output of algorithm is embedded image of size pxq. The purpose is inserting the authenticating image (secure message) bitwise into the source image .

In [6] authors have proposed an adaptive least significant bit spatial domain embedding method. This method divides the image pixels ranges and generates a sego-key. This private sego-key has 5 different gray level ranges of image and each range indicates to substitute fixed number of bits to embed in least significant bits of image. The strength of proposed method is its integrity of secret hidden information in stego-image and high hidden capacity. The limitation is to hide extra bits of signature with hidden message for its integrity purpose. It also proposed a method for colour image just to modify the blue channel with this scheme for information hiding. This method is targeted to achieve high hidden capacity plus security of hidden message.

In [7] Author have proposed LSB's based image hiding method. Common pattern bits are used to hide data. The LSB's of the pixel are modified depending on the pattern bits and the secret message bits. Pattern bits are combination of M x N size rows and columns and random key value. In embedding procedure, each pattern bit is matched with message bit, if satisfied it modifies the 2^{nd} LSB bits of cover image otherwise remains the same. This technique targets to achieve security of hidden message in sego-image using a common pattern key. This proposed method has low hidden capacity because single secret bit requires a block of (M x N) pixels.

In [8] 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 estimated by difference between the two consecutive pixel is cover image using simple relationship between two pixels. PVD method generally provides a good imperceptibility by calculating the difference of two consecutive pixels which determine the depth of the embedded bits. Proposed method hides large and adaptive k-LSB substitution at edge area of image and PVD for smooth region of image. So in this way the technique provide both larger capacity and high visual quality according to experimental results. This method is complex due to adaptive k generation for substitution of LSB.

In [9], a novel lossless or reversible data hiding scheme for binary images is proposed. JPEG2000 compressed data is used and the bit-depth of the quantized coefficients are also embedded into some code-blocks. Proposed data embedding method is useful for binary image not for gray or colour images.

Babbitt et al. In [10] uses 4 LSB of each RGB channel to embed data bits, apply median filtering to enhance the quality of the stego image and then encode the difference of cover and stego image as key data. In decoding phase the sego-image is added with key data to extract the hidden data. It increases the complexity to applying filtering and also has to manage sego-key. Proposed scheme has high secret data hiding capacity

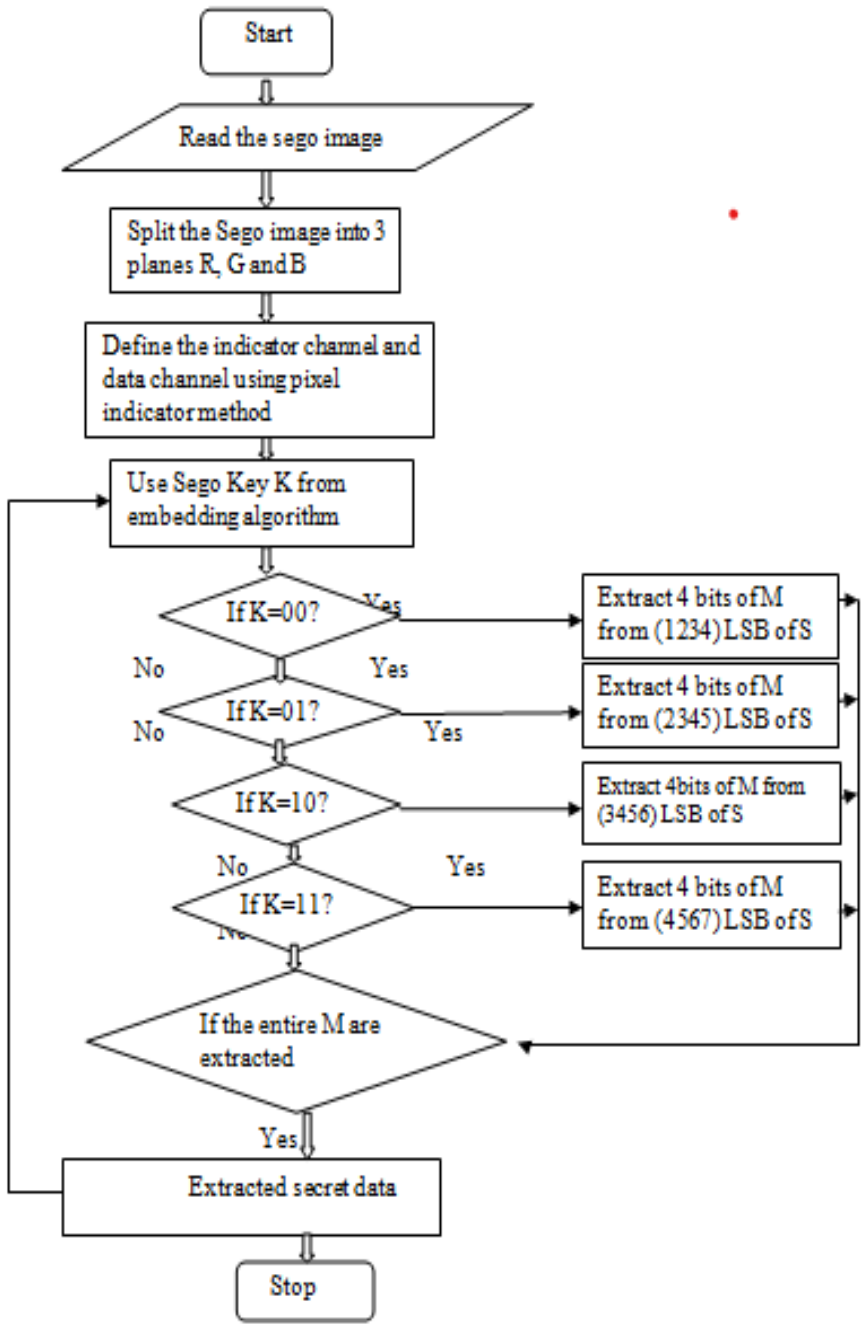
Humid et al. In [11] have proposed a texture based image Steganography. The texture analysis technique divides the texture areas into two groups, simple texture area and complex texture area. Simple texture is used to hide the 3-3-2 LSB(3 bits for Red, 3 bits for Green, 2 bits for Blue channels) method. On the other hand over complex texture area 4 LSB embedding technique is applied for information hiding. 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.

K. S. Babe et al. In [12] proposed hiding secret information in image Steganography for authentication which is used to verify the integrity of the secret message from the Sego image. The original hidden message is first transformed from spatial domain to discrete wavelet transform (DWT); the coefficients of DWT are then permuted with the verification code and then embedded in the special domain of the cover image. The verification code is also computer by special coefficient of the DWT. So this method can verify each row of the image of modified or tampered by any attacker.

3. Methodology

3.1. Analysis Flowchart:

The following flowchart describes how to extract the secret data from the given image.



International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

3.2 Analysis Table: The following table clearly explains the features of various techniques used in image processing.

.

Lit. Ref	Domain	Technique	Capacity	observation	Robustness	Temper	Computation	Advantage	Disadvantage
1.	Spatial	Adaptive Least significant bits	Y	N	N	N	N	Integrity of secret hidden information with High Capacity. It Support all image format.	Hide extra bit of signature with hidden message
2.	Spatial	Texture, image, Brightness and Edge Based Adaptive	Y	Y	N	N	N	High Hidden Capacity with Considering of Good Visual Quality	Limited space for embedding a message.
3.	Spatial	Combine sample bits with secret message using Least significant bits	N	N	N	N	N	Security of Least significantbits technique improved Hidden Data	Hidden Capacity is Low
4.	Spatial	PVD with Adaptive Least significant bits	Y	Y	N	N	Y	High Hidden Capacity With allowing for of Good Visual Quality.	Computationally complex
5.	Spatial	MPD with Least significant bits	Y	Y	N	N	N	Better than universal Pixel-value Differencing methods	Experimental Dataset is limited and threshold key required for both ends
6.	Spatial	PVD with Adaptive LSB	Y	Y	N	N	N	Histogram of cover and sego image is almost same	Dataset for experimental is too small.
7.	Spatial	Simple and complex Texture based Least significant bits replacement	Y	Y	N	N	N	High Hidden Capacity	High Hidden Capacity degrade the visual quality PSNR
8.	Spatial	Least significant bits replacement with average Filtering	Y	N	N	N	N	High Hidden Capacity	Computationally Complex
9.	Spatial	Least significant bits replacement with arbitrary pixel selection	N	N	N	N	N	Security of technique is improve hidden image is Sego image	Embedding data without considering Visual quality in Random pixel selection
10.	Spatial	Pixel pointer with variable Least significant bits replacement	Y	N	N	N	N	Almost same Histogram of sego- image against cover image	Hidden capacity depended on Cover image pixel intensities
11.	Spatial	LSB replacement on gloomy region of Image	N	Y	N	N	N	Useful for flat region with frozen boundary of object based dataset	High computation required
12.	Spatial	Mapping Pixel to secreted alphanumeric letters	N	Y	N	N	N	Just Mapping of pixel with letter no need of image processing	Have to keep Matching Pattern for Extracting Procedure Plus Only useful for Letter based hidden data
13.	Spatial	Hybrid boundary detection with Least significant bits	Y	Y	N	N	N	High PSNR with high hidden capacity	Limited dataset with ideal image
14.	Transform	3D image Coefficient	Y	Y	N	Y	N	High PSNR. It design support Multilayer.	Neticeable artefact of hidden data
15.	Transform	DWT Coefficient	N	N	N	N	N	Integrity of hidden data in sego-image	Computationally complex. It uses DWT method which has a negatie impact on performance
16.	Transform	Secret bits Pulse Bit-depth embedded into coded block	N	Y	N	Y	N	Useful for dual image	Not for Color image support. It does not provide an encryption.

Conclusion:

This paper reviewed different Steganography techniques its major types and classification of Steganography which has been proposed in literature during last few years. These techniques include modifying the image in the spatial domain method, The transform Domain , The image file formatting. The most important factors of Steganography design is undetectability, Capacity, Temper, robustness and Computation. We have critical analyzed techniques which show that visual quality of the image is degraded when hidden data increased up to certain limits using LSB based methods. This research carries out advantages and disadvantages and also demonstrates how the research is evaluated.

Result and Discussion:

In this paper, analysis of LSB methods can be successfully implemented and result can be delivered. Comparative analysis of LSB based, Steganography has been done on basis of parameters like PSNR, MSE, BER on different images and the result are evaluated.

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

REFERENSE:

[1]. Volume-2, Issue-5, May-2015 ISSN: 2349-7637 (Online) RESEARCH HUB – International Multidisciplinary Research Journal (RHIMRJ) Research Paper Available online at: www.rhimrj.com 2015, RHIMRJ, All Rights Reserved Page 1 of 5 ISSN: 2349-7637 (Online) A Survey Paper on Steganography and Cryptography Z. V. Patel1st Student, M. Tech. C. U. Shah College of Engineering and Technology, Surendranagar, Gujarat (India) S. A. Gadhiya2nd Head, B.E.(IT) C. U. Shah College of Engineering and Technology, Surendranagar, Gujarat (India)

[2]. Volume 4, Issue 1, January 2014 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering Research Paper Available online at: www.ijarcsse.com An Overview of Different Type of Data Hiding Scheme in Image using Steganography Techniques Mikes Garg A. P. Guru M. Tech. Scholar H.O.D in CSE Department Jing Institute of Engineering & Technology Jing Institute of Engineering & Techno

[3]. Volume 4, Issue 1, January 2014 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering Research Paper Available online at: www.ijarcsse.com An Overview of Different Type of Data Hiding Scheme in Image using Steganography Techniques A. P. Guru M. Tech. Scholar H.O.D in CSE Department Jinx Institute of Engineering & Technology Jind Institute of Engineering & Technology Jinx, Haryana 126102, India Jinx, Haryana 126102, India

[4]. International Journal of Innovative Research in Computer and Communication Engineering (A High Impact Factor, Monthly, Peer Reviewed Journal) Vol. 4, Issue 1, January 2016 Copyright to IJIRCCE DOI: 10.15680/IJIRCCE.2016. 0401158 721 A Survey Paper on Steganography Techniques Dr. Rajkumar L Biradar1 , Ambika Umashetty2 Associate Professor, Dept. of Electronics and Telemetric, G. Narayanamma Institute of Technology & Science, Hyderabad, India1 Dept. of Computer Science & Engineering, Appal Institute of Engineering & Technology, Kalaburagi, India2

[5] R. J. Anderson and F. A. P. Petit colas. “On the limits of Steganography” IEEE Journal of Selected Area in Communications [Online]. 16(4), pp. 474-481. Available: http://www.cl.cam.ac.uk/~rja14/Papers/jsac98-limsteg.pdf [Jun., 2011].

[6] I. J. Cox, M. L. Bloom, J. A. Fredric, and T. Albert. “Digital Watermarking and Steganography”. USA: Morgan Kaufman Publishers, 2008, pp. 1-591.

[7] N.F. Johnson and S. Jajodia. “Exploring Steganography: seeing the unseen.” IEEE Computer Journal “[Online]. 31(2), pp. 26-34. Available: http://www.jjtc.com/pub/r2026.pdf [Jun. 2011].

[8] A. Cheddar, J. Condell, K. Curran and P. M. Levitt (2010). “Digital image Steganography: survey and analysis of current methods." Signal Processing Journal” [Online]. 90(3), pp. 727-752. Available: http://www.abbascheddad.net/Survey.pdf [Aug. 2011].

[9] M. FORTRAN. “Steganography and digital watermarking: A global view” University of California, Davis. Available: http://lia.deis.unibo.it/Courses/RetiDiCalcolatori/Progetti00/fortini/project.pdf [June 2011].

[10] N. Provo’s and P. Honey man. (2003, Jun.). “Hide and seek: An introduction to Steganography.” IEEE Security and Privacy Journal [Online], 1(3), pp. 32-44. Available: http://niels.xtdnet.nl/papers/practical.pdf [Jul., 2011].