International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Data Hiding Using Steganography: A Review

Nishigandha P. Mangle[1], Prof. Sanjay S. Dhopte[2]

[1]Master of Engineering, Information Technology Department, Prof. Ram Meghe Institute of Technology & Research, Amravati, India

[2]Information Technology Department, Prof. Ram Meghe Institute of Technology & Research, Amravati, India

Abstract: ***Internet technologies are currently charring an important role in our day to day life. It has the benefit as well as disadvantages also. Which in term generates the wants of data activity technology for maintaining the secrecy of the key information. In this paper, we have a tendency to gift a completely unique high bit rate LSB Image data activity technique. The fundamental plan of the proposed LSB algorithmic program is knowledge embedding that causes token embedding distortion of the host image. Using the planned ballroom dance algorithmic program, knowledge activity bit are embedded into higher LSB layers, ensuing in increased strength against noise addition or image compression. Listening tests showed that the perceptual quality of knowledge hided image is higher within the case of the proposed technique than within the common place LSB technique.***

Keywords: Higher LSB, Guard Pixels, Steganography, Multi- carrier, Information hiding, data Encryption

1. Introduction

Steganography is that the follow of concealment data "inplain sight". Steganography provides the authentication over the data using some tag or labeling on some objects like text, audio, video, image. The goal of steganography is to cover the presence of a message and to form a covert channel. The message is hidden in another object as a result the transmitted object are going to be identical wanting to each individual's eye. Steganoanalysis is that the art of detective work any hidden message on the communicating. If the existence of the hidden message is exposed, the goal of steganography is crushed.

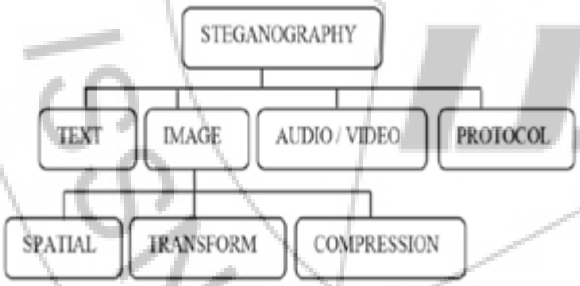

Figure 1: Classification of steganographic Techniques

The Text Steganography have basic three classes that square measure as follows [1], Format-based methods: Hide the steganographic text within the existing cover text by dynamical information like insertion of areas or non-displayed characters, careful errors tinny throughout the text and resizing of fonts. Random and applied mathematics generation method: In this case avoid comparison with a proverbial plaintext, steganographers typically resort to generating their own cover texts. Linguistic methods: Serious of linguistic analysis makes this a remarkable medium for steganographic information concealment. In audio Steganography [8], messages square measure embedded into digitized audio signal that result slight alteration of binary sequence of the corresponding audio file. Low-bit Encoding: The binary version of the secret information message is substituted with the smallest amount vital bit (LSB) of every sample of the audio cover file. Phase coding: part cryptography on the fact that the part elements of sound are not as perceptible to the human ear as noise. Many new approaches square measure studied in video information steganography literature [8]. The approaches are application of BPCS Steganography to ripple Compressed Video, Associate in Nursing Optical Video Cryptosystem with Adaptive Steganography. A Secure Covert Communication Model supported VIDEO Steganography, Lossless Steganography on AVI File using swapping formula, and brand new invertible information concealment in Compressed Videos or Images etc. In image steganographic techniques varied ways in that square measure used which square measure as follows [9]: Substitution technique in spatial Domain: during this case the smallest amount vital bits of the duvet item square measure replaced while not modifying the complete cover image. Remodel domain technique: separate trigonometric function remodel (DCT), separate ripple Trans- kind (DWT) and quick Fourier remodel (FFT) square measure accustomed hide data in remodel coefficients of the cover pictures. Unfold spectrum technique: The message is contact a large frequency information measure than the minimum needed information measure to send the data. Applied mathematics technique: Here the data is encoded by changing varied numerical properties of copy image and therefore the message bits square measure hidden within the block of copy image. Distortion technique: data is keep by signal distortion. Constituent Mapping technique (PMM) [10]: Embedding positions are chosen by some operate and depends on the element intensity price of the seed element and its eight neighbours. Information embedding are done by mapping every two or four bits of the key message in every of the neighbor element supported some options of that element. This method depends on a message being encoded and hidden during a transport layer in such how on create the existence of the message unknown to an observer. Significantly, the transport layer the carrier file is not secret and may thus be viewed by observers from whom the key message itself ought to be concealed. The ability of steganography is out of sight the key message by obscurity, concealing its existence during a non-secret file. There in sense, steganography is different from cryptography, that involves creating the content of the key message illegible

whereas not preventing non-intended observers from learning concerning its existence1.Because the success of the technique depends entirely on the flexibility to cover the message specified an observer would not suspect it is there in the slightest degree, the best effort should go into making certain that the message is invisible unless one is aware of what to seem for. The way in that this is often done can take issue for the precise media that are will not to hide the data.

In every case, the worth of a steganographic approach are often measured by how abundant data are often hide during a carrier before it becomes detectable, every technique will therefore be thought of in terms of its capability for data concealing. There are various ways wont to hide information within image, Image and Video files. The desire to send a message as safely and as firmly as possible has been the purpose of dialogue since time immemorial. data is that the wealth of any organization. This makes security-issues high priority to Associate in Nursing organization dealing with confidential information. no matter is that the method we opt for the protection purpose, the burning concern is the degree of security. Steganography is that the art of covered or hidden writing. the aim of steganography is covert communication to cover a message from a third party. Steganography is often confused with scientific discipline as results of the two are similar in the means that they each are will not to defend important information. The distinction between the two is that Steganography involves concealing data therefore it appears that no data is hidden in the slightest degree. If an individual or persons views the item that the knowledge is hidden inside of he or she is going to do not have any concept that there is any hidden information, thus the person won\'t decide to decode the data. Steganography within the modern day sense of the word typically refers to data or a file that has been hide within a digital image. Video or Image file. What Steganography primarily will is exploit human perception; human senses are not trained to seem for files that have data hidden inside of them. Generally, in steganography, the actual information is not maintained in its original format and thereby it is reborn into another equivalent multimedia file like image, video or image that in turn is being hidden at intervals another object. This apparent message (known as cowl text in usual terms) is sent through the network to the recipient, wherever the actual message is separated from it. There are several to embed information into a preferred media mistreatment steganography. A good example of this is often the link between are coded song, and its lyrics. The image file containing the recording is way larger than the song lyrics stored as an understandable code files. thus it\'s in all probability safe to assume that the smaller file may be steganographically embedded into the larger one while not impacting the quality. Vital domains, besides classic computing, where steganography are often applied are domains mistreatment mobile and embedded devices particularly mobile phones. In this project we tend to state the actual fact that steganography will be successfully enforced and used into a next generation of computing technology with image and video process talents. The LSB methodology used for this project that satisfies the necessity of steganogaphy protocols. This analysis can embody implementation of steganographic formula for secret writing information within video files, still as technique to dynamically extract that data as original. Communication of knowledge over the web is apace increasing because of the progression of upper availableness of the Internet and also the increase in information measure transmission speed. However, responsibility problems concerning to information transmission such as confidentiality, information security and information loss are becoming serious considerations. The consumer needs that; the transmitted information should not be lost, broken or manipulated by any unauthorized third party. information lost can even result from network congestion because of further overhead the process of concealing data within another media is named stegnography. The media with secret information is named stego media and while not hidden information is named covar media [I]. Steganalysis is a process of extracting data from the stego media.Steganalysis is simply opposite to stegnography.

A.Basic construct any image is created from pixels. every element represents a color price and depends upon the image the element size can be from one bit to four bytes. These pixels are hold on during a computer memory in binary kind. allow us to think about a picture with element size a pair of bytes for discussion. The element with a pair of computer memory unit size will ready to represent 216 completely different colors, range from 0000000000000000 to 1111111111111l. Usually for human eyes the color 1111000011110000* and 1111000011110001* can appear as if similar, since the distinction is just too low. Which implies that the modification in least vital bit (*LSB) might not be noticed by human eyes. If we tend to alter 11110000111lO000 as zero III 0000 1111 0000, then the color of a element can modification to a different color. That is the modification within the most significant bit (MSB), can modification the color dramatically. This can be simply known by everybody. Therefore it is clear that the secret data should be hold on within the LSB and not in MSB of the duvet image to cut back the detectable distortion. Let as think about a scenario, that an individual \"Saravanan\" needs to send secret data to a different person \"Srinivasan\" and the secret data is \"Tomorrow American states Me in College\". This data should not be proverbial to an individual \"Gnanasekar\" World Health Organization is Associate in Nursing knowledgeable in hacking. During this scenario Saravanan should take a can copy image of size eight times greater than secret information as shown in figure one. He has to convert the key information into binary type and so he has to store the key information within the LSB of every constituent one by one. The resultant images (stego image) are going to be sent to Srinivasan via network. Currently the Gnanasekar can catch the packets and he will construct the image send by Saravanan to Srinivasan. Currently Gnanasekar will simply see the image and he may suppose that there is no secret in their communication. This is often however one can cheat the hacker’s exploitation stegnography

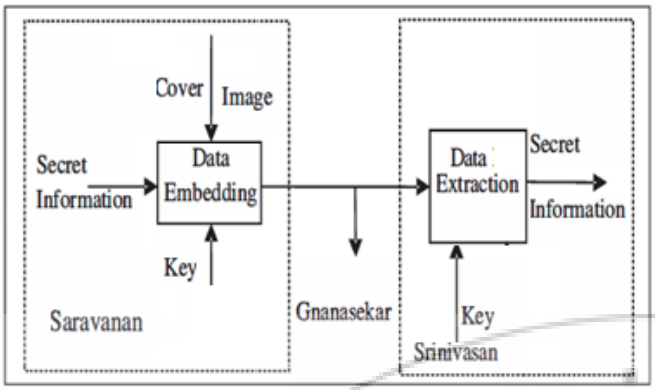

Figure 2: Stegnography

The performance of a stegnography may be measured by three factors. They are security, capability and detectable distortion (DD). The protection should be high, so the active attacks and passive attacks should not reach founding secret information. Security may be achieved by dynamical method of storing the bits. For instance rather than storing first bit. Second bit and third little bit of secret information into LSB of initial, second and third pixels severally, it may be keep in second, fourth and sixth pixels severally. By doing such variation within the bit alteration could confuse the steganalyisist. Normally capability of the stegnography may be raised by altering additional bits of a constituent. For instance rather than dynamical only one LSB of a constituent, if we tend to alter 2 LSBs then the capability will become double. However increasing the capability on the far side sure level can produce detectable distortion within the stego image. Without increasing the detectable distortion the capability should be raised. The Doctor of Divinity of a stegnography should be low that is the stegno image should not have high visual artifacts.

2. Literature Survey

For learning the ideas of text steganography, we have got surveyed several latest papers. During this section we have delineated the relevant papers of various authors. We give thanks these authors for providing the information of text steganography. These papers were terribly important for learning the fundamental conception Debnath Bhattacharyya, Poulami Das, Samir Kumar Bandyopadhyay, and Tai-hoon Ki [1], the most necessities of any data hiding system are security, capability and lustiness. It is very tough to archive of these factors together because these are reciprocally proportional to every alternative. Authors have focuses on maximizing security and capacity issue of information concealment. The information concealment method uses high resolution digital image as a can copy signal. It provides the power to cover a major quality of information creating it totally different from typical knowledge hiding mechanisms. They need used the massive payloads like video in video and film in video as a canopy image. Ms. Megha B. Goel,Mr. M. S. Chaudhari [2], the confidential communications over public networks are often done victimization digital media like text, images, image and video on the web. Simply concealment the content of a message using cryptography was not adequate. Concealment of message should give a further layer of security. To provide a lot of security the author advised the new procedures in steganography for concealment ciphered information within a digital color picture image. 3 Satish Singh Verma , Ravindra Gupta , Gaurav Shrivastava [3] He has used quadratic methodology looking on the locations concluded by the binary image, beside of public key cryptography. He had completed that the conjunction between cryptography and steganography produce immune data. Xikai Xu [4], during this work author has delineated a steganographic system that embeds secret messages into a video stream. Usually the compression methods are employed in video conferences for securing acceptable quality. However sometimes, compression strategies are lossy because reconstructed image might not be identical with the original. There are some disadvantage of compression and knowledge embedding methodology. Signal noise and irrelevance are common samples of knowledge embedding. But compression strategies try and take away signal noise and irrelevance. If signal is compressed a lot of, then there are fewer prospects of information embedding. The author have solved this downside, they need investigated a typical signal path for knowledge embedding. during this algorithmic rule security is established by indeterminism at intervals the signal path. Arvind Kumar, Km. Pooja [5], during this paper author have projected afresh compressed video Steganographic theme. In this scheme the information is hidden compressed domain. The data are embedded within the macro blocks of I, P frames and in B frames. The novel embedding technique Triway Pixel Value Differencing (TPVD) is employed to extend the capacity of the hidden secret data and for to providing an invisible stego-image for human vision. These algorithmic rules are often applied on compressed videos while not degradation in visual quality. V. Saravanan, A. Neeraja [6], have conferred a novel approach of concealment image in an exceedingly video. During this approach, one LSB of every component is replaced by the one bit of secrete message. Thus it's terribly tough to search out that image is hidden within the video of thirty frames per second. The analysis is extremely tough as a result of every row of image pixels is hidden in multiple frames of the video. The trespasser needs full video to unhide image. Authors have delineated the LSB algorithmic rule during this paper. The projected algorithmic rule is extremely helpful in sending sensitive data firmly.[7], have projected new Real time Compressed video secure Steganography (CVSS) algorithmic rule victimization video bit stream. In this, embedding and detection operations are both dead entirely within the compressed. The proposed algorithm will increase the protection as a result of the statistical invisibility of contiguous frames is employed to regulate the embedding strategy and capability. Now a days we tend to are hiding the information in video format, thus within the future implementation of uncompressed formats could possible as well, thus it should support IMAGE4 format. Ms. G. S. Sravanthi [8]. Multiple frames embedding are doable. Currently we tend to are embedding single frame at a time, however in future multiple frames embedding is additionally doable. Conclusion we conferred a reduced distortion algorithmic rule for LSB image steganography. The key plan of the algorithmic rule is knowledge concealment bit embedding that causes minimal embedding distortion of the host image. Visualization tests showed that delineated algorithmic rule succeeds in increasing the depth

of the embedding layer from 1th to 5LSBlayer while not touching the sensory activity transparency of the knowledge hided image signal. the development in lustiness in presence of additive noise is clear, as the projected algorithmic rule obtains considerably lower bit error rates than the quality algorithmic rule. The steganalysis of the projected algorithmic rule is more difficult similarly, because there is a major cryptography provided for knowledge security. The image steganography are often doable in 2 domains, one is special and another is frequency domain. There are numerous techniques and modules developed by totally different researchers [8].Some of them are mentioned below: One of the common techniques is predicated on manipulating the least-significant-bit (LSB) planes by directly commutation the LSBs of the cover-image with the message bits. LSB strategies usually come through high capability however sadly LSB insertion is prone to slight image manipulation like cropping and compression. The pixel-value differencing (PVD) technique planned by Chinese and Tsai will with success give both high embedding capability and outstanding physical property for the Stego-image. The pixel-value differencing (PVD) technique segments the quilt image into non overlapping blocks. Block containing 2 connecting pixels and modifies the constituent distinction in every try for knowledge embedding. a bigger distinction within the original constituent values permits a bigger modification. Within the extraction section, the first vary table is important. It is accustomed partition the Stego image by a similar technique as accustomed the quilt image. Supported PVD technique, numerous approaches have conjointly been proposed among them. Proposes a replacement technique victimization tri-way pixel-value differencing that is better than original PVD technique with relevancy the embedding capability and PSNR. In 2004, Potdaretal. proposes GLM (Gray level modification) technique that is employed to map knowledge by modifying the grey level of the image pixels[9]. grey level modification Steganography could be a technique to map knowledge hide by modifying the gray level values of the image pixels. GLM technique uses the idea and even numbers to map knowledge within a picture. it\'s a matched mapping between the binary knowledge and also the elite pixels in a picture [9] and PPM introduced a replacement technique supported constituent try matching (PPM). In PPM use the values of pixel try as a reference coordinate and search a coordinate within the neighborhood set of this constituent try in keeping with a given message digit.[10] Exploiting modification direction (EMD) and diamond encryption (DE) are 2 data-hiding methods conjointly planned supported PPM. Che-Wei Lee associate degreed Wen-Hsiang have blind an authentication technique based on the key sharing technique with a knowledge repair capability for grey scale document pictures by generating block of a grey scale image, which, in conjunction with the binaries block content. They used the computed values are mapped into a spread of alpha channel prices close to their most value of 255 to surrender a clear Stego image with a disguise impact. Shunquan Tan and Bin Li, establish that the readjusting section of edge adaptational image steganography supported LSB matching revisited introduces a pulse distortion to the long exponential tail of the bar chart of absolutely the distinction of the constituent pairs. A targeted steganalytic technique supported B-Spline fitting is planned in their technique. Sian-Jheng Maya Lin and Wei-Ho Chung, initiate the concept of Reversible information embedding (RIE) in their paper. This can be a way remodeling host signals and also the message into the Stego-signals and the Stego-signals may be lossless reversed to the host signals and also the message. G.Karthigai Seivi, Leon Mariadhasan, K. L. Shunmuganathan ,worked on most typical and easiest way for embedding messages in an image i.e. least-significant bit (LSB) insertion technique which might effectively resist image steganalysis supported statistical analysis. Ching-Nung rule, Chih-Cheng Chinese, Yi-Chin Maya Lin and Cheonshik Kim , planned associate degree economical matrix based mostly secret image sharing (MSIS) theme supported straightforward binary matrix operations. Manpreet Kaur, Sonika Jindal, Sunny Behal[11] Digital watermark is a code that is embedded inside an image. It acts as a digital signature, giving the image a sense of ownership or authenticity. Watermarking is very similar to steganography in a number of respects. Both seek to embed information inside a cover message with little to no degradation of the cover-object. Watermarking however adds the additional requirement of robustness. An ideal steganographic system would embed a large amount of information, perfectly securely with no visible degradation to the cover object. An ideal watermarking system however would embed an amount of information that could not be removed or altered without making the cover object entirely unusable. Bhattacharyya and Sanyal‘s Transformation: Bhattacharyya and Sanyal[12] planned a replacement image transformation technique in better-known as constituent Mapping technique (PMM), a way for info activity inside the abstraction domain of any grey scale image. Embedding constituents are elite supported some mathematical relation that depends on the pixel intensity value of the seed constituent and its eight neighbors are elite in counter clockwise direction. Knowledge embedding are done by mapping every 2 or four bits of the key message in every of the neighbor constituent supported some options of that pixel. At the receiver aspect alternative completely different reverse operations has been allotted to induce back the first information D. Biswasa, S. Biswasb, A. Majumdera, D. Sarkara, D. Sinhaa, A. Chowdhurya, S. K. Dasa (2012)[13] Steganography refers to the science of “invisible” communication. Unlike cryptography, where the goal is to secure communications from an eavesdropper, steganographic techniques strive to hide the very presence of the message itself from an observer. The general idea of hiding some information in digital content has a wider class of applications that go beyond steganography. Here we propose a new innovative technique for hiding and then retrieving a secret image. The technique consists of two processes viz. encoding and decoding. Main focus in the encoding phase is to hide the secret RGB colour image in a cover image and get some shares which are to be transmitted to the receiver.[12] In the decoding phase, main focus is to get back the retrieved image back to the original image quality as much as possible from the shares in the received end. In this paper we mainly focus on digital image steganography which is all about using digital images to hide information. Satish Singh Verma , Ravindra Gupta , Gaurav Shrivastava [14] Steganography has proven to be one of the practical ways of securing data. It is a new kind of secret communication used mainly to hide secret data inside

other innocent digital mediums. Steganographic algorithms can be characterized by a number of defining properties like Transparency, Capacity, and Robustness. We have presented a high capacity and high stegosignal quality audio steganography scheme based on samples comparison in DWT domain where selected coefficient of a segment value is change by a threshold value depending upon the embedding cipher text bit. The strength of our algorithm is depend on the segment size and their strength are enabled the algorithm to achieve very high embedding capacity for different data type that can reach up to 25% from the input audio file size with lest of 35 dB SNR for the output stego signal.[15]

References

[1] Debnath Bhattacharyya1, Poulami Das,Samir Kumar Bandyopadhyay, and Tai-hoon Kim," Text Steganography: A Novel Approach", International Journal of Advanced Science and Technology Vol. 3, February, 2009
[2] Ms. Megha B. Goel,Mr. M. S. Chaudhari"A Review on Data Hiding Using Steganography & Visual Cryptography", International Journal of engineering development & research vol. 2,2014
[3] Satish Singh Verma , Ravindra Gupta , Gaurav Shrivastava," A Novel Technique for Data Hiding.
[4] Xikai Xu, jing dong, wei wang and tieniu tan,"Video steganalysis based on the constraints of motion vectors", Center for Research on Intelligent Perception and Computing,National Laboratory of Pattern Recognition,Institute of Automation, Chinese Academy of Sciences
[5] Arvind Kumar,Km. Pooja," Steganography- A Data Hiding Technique" International Journal of Computer Applications (0975 – 8887) Volume 9– No.7, November 2010
[6] V. Saravanan, A. Neeraja,"Security Issues in Computer Networks and Stegnography", International Conference on Intelligent Systems and Control (ISCO 2013) ©2012 IEEE
[7] Mrs. Kavitha, Kavita Kadam, Ashwini Koshti, Priya Dunghav," Steganography Using Least Signicant Bit Algorithm", International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 Vol. 2, Issue 3, May-Jun 2012, pp. 338-341
[8] Ms.G.S.Sravanthi, Mrs.B.Sunitha Devi, S.M.Riyazoddin& M.Janga "A Spatial Domain Image Steganography Technique Based on Plane Bit Substitution Method",Global Journal or Computer Science and Technology Graphics & Vision Volume 12 Issue 15 Version 1.0 Year 2012
[9] Gurmeet Kaur and Aarti Kochhar," Digital Watermarking and Other Data Hiding Techniques", nternational Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-2, Issue-5, April 2013
[10] Hirdesh Kumar, Awadhesh Srivastava ,"A Secret Sharing Scheme for Secure Transmission of Color Images", 2014 International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT) IEEE
[11] Indradip Banerjee, Souvik Bhattacharyyab, Gautam Sanyalc, "Hiding & Analyzing Data in Image Using Extended PMM", International Conference on Computational Intelligence: Modeling Techniques and Applications (CIMTA) 2013
[12] Sherly A P and Amritha P P,"A Compressed Video Steganography using TPVD", International Journal of Database Management Systems(IJDMS) Vol.2, No.3,August 2010 DOI:10.5121/ijdms.2010.2307 67
[13] D. Biswasa, S. Biswasb, A. Majumdera, D. Sarkara, D. Sinhaa, A. Chowdhurya, S. K. Dasa," Digital Image Steganography using Dithering Technique", SciVerse ScienceDirectric, Procedia Technology 4 (2012) 251 – 255
[14] Satish Singh Verma , Ravindra Gupta , Gaurav Shrivastava," A Novel Technique for Data Hiding Domain in Audio Carrier by Using Sample Comparison in DWT", 2014 Fourth International Conference on Communication Systems and Network Technologies
[15] Richard E. Woods & Rafael C. Gonzalez"Digital Image Processing" Book.