**IMAGE STEGANOGRAPHY**

S.Srithar - Assistant Professor

S.Karthik,N,Lavanya-UG Student

Department of CSE,RVS College of Engineering and Technology,Coimbatore

[sss.srithar@gmail.com,karthiksmashh@gmail.com,lavanya21399@gmail.com](mailto:sss.srithar@gmail.com,karthiksmashh@gmail.com,lavanya21399@gmail.com)

**I.Abstract**

Steganography is a useful technique for hiding data behind the carrier file such as image, audio, video etc. and that data securely transfer from sender to receiver. The cryptography is also another technique which is used for the protecting information. The Combining encryption methods of cryptography and steganography enables the user to transmit information which is masked inside of a file in plain view. This will provide more security to transferring data.This paper provides a general overview of Steganography techniques in which Text, ImageAudio and Video Medias used for the information hiding behind channels. Also the Cryptography will be applied on the information for the better security.

**Keywords**: Image Steganography, Audio Steganography, Video Steganography, Spatial domain and Transform domain.

**II.Introduction**

Steganography refers to the art and science of concealing secret information in other media. The information to be hidden is called the secret message and the medium in which the information is hidden is called the cover of the document or cover page.The cover that contains the hidden message is called stego-document. The algorithms used to hide the message on the cover medium at the sender end and extract the hidden message from the stego document at the end of the receiver is called the stegosystem.Steganography in the modern sense refers to information or a file that has been hidden within a digital image, video or audio file. This science of concealing the information is done in such a way that no one suspects that the hidden information exists. Steganography is usually combined with cryptography Steganography can be classified into several sub classes such as text, audio, video or image Steganography, depending upon whether text, audio, video or image is used as the cover medium. Out of all these available forms of Steganography, digital image Steganographic procedures are more popular among the researchers as images are more common forms of mediums that are used worldwide for data transmission and also due to their data hiding capacity. Before discussing further about this form of Steganography, let’s first define what a digital image is.

Thus the steganography technique is mainly based on Image processing domain.Image processing is the field of signal processing where both the input and output signals are images. Images can be thought of as two-dimensional signals via a matrix representation, and image processing can be understood as applying standard one- dimensional signal processing techniques to two-dimensional signals. Image processing is a very important subject, and finds applications in such fields as photography, satellite imaging, medical imaging, and image compression, just to name a few.Digital image processing is the use of computer algorithms to perform image processing on digital images. As a subcategory or ﬁeld of digital signal processing, digital image processing has many advantages over analog image processing. It allows a much wider range of algorithms to be applied to the inputdata and can avoid problems such as the build-up of noise and signal distortion during processing. Since images are deﬁned over two dimensions (perhaps more) digital image processing may be modeled in the form of multidimensional systems.

**III**.**Literature survey**

**[1]** Pooyan and Delforouzi (2007)proposed LSB-basedAudio Steganography Method Based onLifting Wavelet Transform. The encrypted covert data is embedded into the wavelet coefficients of hostaudio signal. They calculate hearing threshold in wavelet domain. Then according to this threshold data

bits are embedded in the least significant bits of lifting wavelet technique is reformed to increase therobustness coefficients. Inverse lifting wavelet transform is applied to modified coefficients toconstruct stego signal in time domain. Haar wavelet transform was used.

**[2]** Yang, Weng, Wang (2008)Proposed the new adaptive LSB technique using Pixel Valuedifferencing with spatial LSB domain technique. It gives high embedding capacity and imperceptibleStego image. This method is used to distinguish between edge areas and smooth areas. The edge areasare used for the higher embedding capacity for data hiding .This technique comes under the spatial

domain image processing and this method applied on grayscale images. The quality of stegoimagescalculated from the peak signal to noise ratio (PSNR).

**[3]** Kim, Jung and Yoo (2008)proposed A high capacity data hiding using PVD and LSBReplacement Method. This method calculates the difference value between two consecutive pixels. TheLSB substitution method is used when the difference value is small (i.e smooth areas) and PVD is usedwhen it is large (i.e edge areas) of cover image pixels. The pixels belong to the edge areas could embedmore data than the smooth area of image thus LSB substitution is used to embed more data on smootharea without distortion to the human visual system. This method is useful for the grayscale images.

**[4]** Garay, Medina, Rivera and Ponomaryov (2008)Proposedsteganographic communicationchannel using mp3 and wave audio signals. It uses Direct Sequence Spread Spectrum (DSSS) to insertconfidential information in MP3 and WAV audio digital signals. Filtering, re-sampling, noise addition,echo addition and MPEG compression were used to evaluate the proposed algorithm.

**[5]** Bhattacharya, Das, Bandopadhya and Kim (2009) Proposed a security model for the Textsteganography. The model combines cryptography, steganography and along with that an extra layer ofsecurity has been imposed in between them. This extra layer of security changes the format of normalencrypted message and the security layer followed by it embeds the encrypted message behind amultimedia cover object. It gives privacy and secrecy by using cryptography and steganography resp.Two secret keys are used. This algorithm is useful for the color images, audio and video covers Medias.

**[6]** Yang, Sun and Guang Sun (2009) Proposed a high capacity data hiding scheme using adaptiveLSB substitution technique. This technique focuses on to avoid abrupt changes in image edge areas, aswell as to achieve better quality of the Stego-image. This scheme exploits the brightness, edges, andtexture masking of the host image to estimate the number k of LSBs for data hiding. The methodproposed a human visual system (HVS) and LSB substitution, which obeys the concept that the edgescannot tolerate great change. The method was applied on the 512 × 512 grayscale image.

**[7]** Bhaumik, Choi, Robles, and Balitanas (2009) Proposed a data hiding and extraction procedurefor high resolution Audio Video Interleave (avi) videos. The main intention of this method is to provideproper protection on data during transmission. Accuracy of the correct message output that extractfrom source can estimated by using tools for comparison and statistical analysis.

**[8]** Elsadig, Kiah, Zaidan and Zaidan (2009) proposed LSB insertion method on video images orframes. This method considers the digital image file as separate frames and changing the output imagedisplayed on each video frame by hidden data that does not visually change the image. The result was

successful on extracted set of video frames.

**[9]** Dao, Bai and Yu (2009) proposed A High Bit rate Information Hiding Algorithm for Video inVideo. Experimental result shows that the host video which is embedded numerous auxiliary information have little visually quality decline. Peak Signal to Noise Ratio (PSNR) of host video onlydegrades 0.22dB in average, while the hidden information has a high percentage of survives and keepsa high robustness in H.264/AVC compression, the average Bit Error Rate (BER) of hiding informationis 0.015%. This technique will be very useful in captioning, picture-in-video, speech-in-video etc. itenhances the efficiency of multimedia information.

**[10]**Mozo, Obien, Rigor, Rayel, Chua and Tangonan (2009)-proposed a Video Steganography usingFLV. In this method FLV file extension used because of its simple file structure, its relatively small

size compared to other video file formats, and its popularity in video-hosting websites. The FLV filesize changes when a file is hidden but the picture and sound quality of the FLV with the embedded datais perfectly maintained. This would allow doctors and medical personnel to embed multiple medicalrecords such as electrocardiogram signals, ultrasound files, medical prescriptions, urinalysis, and manymore medical files into a single video file (flv).

**[11]**Kim,Cheng and Young Yoo (2009) proposed A New Steganography Scheme based on an IndexcolorImage. This method first divides the secret data into several parts based on the number of colorsin the cover image, and then embeds secret data into the cover image. The cover image can berecovered easily without loss. This technique can be applied to BMP, gif and PNG image formatswhich use the index-color technique.

**[12]**Luo, Huang and Jiwu Huang (2010)proposed edge based LSB Matching Revisited imagesteganography algorithm. In that embedding region selected from the size of the secret message and thedifference between two consecutive pixels in the cover image. Lower embedding rates, only sharperedge regions are used while keeping the other smoother regions as they are. This algorithm applied ongrayscale images which gives higher visual quality and better security. This method will be applied onaudio/video steganography in the spatial or frequency domains.

[13]Nikoukar (2010) proposed an Image steganography Method Based on RGB (Red/Green/Blue)color Image. In this technique BMP file format images are used which performs least variations in the

cover images. Every pixel in BMP file contain 24bits - R, G, B channels in which one is pixel indicatorand remaining two are used to hide the data. Secret key and randomization technique are used forselection of number of bits used and color channel that are used. Data detection is more difficult than

the previous technique.

**[14]**Wei, Guo and Wang (2010) proposed method on Advanced Audio Coding (AAC) and MPEG-2and MPEG-4 the audio format are used. Encryption takes place on hidden data and then encoded intoAAC bit stream. This method use Huffman and differential coding for encoding each bit of the hidden

data as the parity of the number of bits. AAC is a lossy compression encoding scheme for digital audio,which achieves better sound quality than MP3 at the same bit rate.

**[15]**Djebbar, Ayad, Hamam and Meraim (2011) proposed A perfect audio Steganographic techniqueaim at embedding data in an imperceptible, robust and secure way and then extracting it by authorized

people. This paper presents a review of the current state of art literature in digital audio steganographytechniques and approaches. The Audio steganography methods Low bit encoding, Echo hiding,Magnitude spectrum, Phase spectrum, Tone insertion, Spread spectrum, Cepstral domain, Waveletcoefficients, Codebook Modification, Bit stream hiding etc. was introduced.

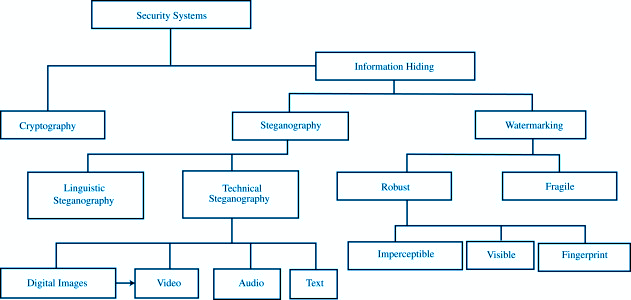
**[16]**Gadicha1 (2011) proposed audio wave steganography method that reduces embedding distortionof the host audio and message bits are embedded into 4th LSB layers, resulting in increased robustnessagainst noise addition. This method introduces smaller error during watermark embedding. If the 4thLSB layer is used, the absolute error value ranges from 1 to 4 Quantization Signal, while the standardmethod in the same conditions causes constant absolute error of 8 Quantization Signal. LSB coding

method introduced the average power of noise is smaller i.e. 9.31db.

Origins of Steganography

Steganography was around long before computers were invented. As long as people have desired to communicate in secret, steganography has been there, allowing them to at least attempt to do so. The term "steganography" dates back to 440 BC and derives from a Greek word meaning "covered or hidden writing."

**Disciplines of Security Systems based on Information Hiding**



**IV.Methodology**

User needs to run the application. The user has two tab options – encrypt and decrypt. If user select encrypt, application give the screen to select image file, information file and option to save the image file. If user select decrypt, application gives the screen to select only image file and ask path where user want to save the secrete file.This project has two methods – Encrypt and Decrypt.In encryption the secrete information is hiding in with any type of image file.Decryption is getting the secrete information from image file.

**Lease Significant Bit:**

Consider the following pixels,(Before changing)

10010101 00001101 11001001

10010110 00001111 11001010

10011111 00010000 11001011

Now suppose we want to hide the letter **“A”**The **ASCII** value for “A” is 65

The binary value for “A” is **01000001**.

The pixel values (After changing)

10010101 00001100 11001001

10010110 00001110 11001010

10011110 00010000 11001011

**V. DISCUSSION AND RESEARCH SCOPE**

After reviewing the various papers in area of steganography it is found that -

It is observed that most of the Steganography techniques are suitable to hide text as massage only andnot able to hide any binary message. Many image Steganography techniques are only for gray scaleimages but not applicable for color image. In comparison with video and audio as carrier, there aremany Steganography techniques for image but very few are for audio and video. Image Steganographytechniques are used for video Steganography but there is need of performance improvement in term of

security, hiding capacity, visual quality and attack analysis. The video and audio steganography aregood for storing large amount of message than other Steganography techniques.Spatial domain Steganography techniques are easy for attacks so they need to combine with externalsecurity such as cryptography. Some Spatial Domain Steganography techniques are based on secret keyso secrecy of key is required to provide externally. There is a research scope in making image, audio

and video steganography techniques parallel to improve their embedding and extraction processesspeedy. Particularly in image and video there is more scope to do a parallelism and also improve hidingcapacity. At the same time, attack analysis process should also parallelize to minimize the time of

steganalysis.

**VI. CONLUSION**

Paper present the review of all existing steganographic methods for data hiding inside the text,image, audio and video channels. Some steganographic methods need to improve security by usingcryptography against attacks. Image and audio steganography both techniques are useful for the video

stegnography to increase the hiding capacity of secure data inside the carrier fie. The parallelization ofsteganography technique is an important task in steganographic area to increase the processing speed of

the steganoghraphic algorithm.The various steganographic techniques such as image, audio and video steganography need to befocused on hiding capacity, detectability, Level of Visibility and robustness against malicious andunintentional attacks.

VII.**REFERENCES**

**[1] Chan K. C, Cheng L. M (2003**), “hiding data in images in simple LSB substitution”, Journal of

pattern recognition, pp.469-474.

**[2] Zlii Li,Yang S. A. F. , Xian Y (2003),”** A LSB Steganography Detection Algorithm”, The 14th

IEEE 2003 International Symposium on Persona1,lndoor and Mobile Radio Communication

Proceedings.pp.2780-2783.

**[3] Sutaone M. S. and Khandare M. V. (2004)** ,“Image Based Steganography Using LSB Insertion

Technique”, pp.146-151.

**[4] Ru X. M, Zhang H. J, Huang X (2005),** “Steganalysis Of Audio: Attacking The Steghide”,

Proceedings of the Fourth International Conference on Machine Learning and Cybernetics, Guangzhou,

pp.3937-3942, pp.18-21.

**[5] Shahreza M. S and Shahreza M. H. S (2007)** ,“Text Steganography in SMS”, International

Conference on Convergence Information Technology, pp.2260-2265.

**[6] Pooyan M, Delforouzi A (2007)** , “LSB-based Audio Steganography Method Based on Lifting

Wavelet Transform”, 2007 IEEE International Symposium on Signal Processing and information

technology, pp.600-603.

**[7] Yang C. H, Weng C. Y, Wang S. J and Sun H. M (2008**), “Adaptive data hiding in edge areas of

images with spatial LSB domain systems,” IEEE Trans. Inf. Forensics Security, vol. 3, no. 3, pp. 488–

497.

**[8] Kim K. J, Jung K. H and Yoo K. Y (2008)** , “A high capacity data hiding method using PVD and

LSB replacement”,International Conference on Computer Science and Software Engineering, pp.876-

879.

**[9] Garay S. H, Medina R. V, Rivera L. V and Ponomaryov V (2008**), “Steganographic

Communication Channel Using Audio Signals” ,12th International Conference on Mathematical

Methods in Electromagnetic Theory, pp.427-429.

**[10] Bhattacharya D, Das P, Bandyopadhyay S. K., Kim T (2009)** ,“Text Steganography: A Novel

Approach ”, International Journal of Advance Science and Technology,Vol.3, pp.79-86.

**[11] Yang H ,Sun X, Sun G (2009**), “A High-Capacity Image Data Hiding Scheme Using Adaptive

LSB Substitution” Radio Engineering, Vol. 18, No. 4, pp. 509-516.

**[12] Bhaumik A. K, Choi M, Robles R. J and Balitanas M. O (2009**) , “Data Hiding in Video”,

International Journal of Database Theory and Application Vol. 2, No. 2, pp.9-16.

**[13] Kiah E ,Zaidan B. B and Zaidan A. A (2009)** , “High rate video streaming steganography”,

International Conference on Information Management and Engineering, pp.550-554.

**[14] Dao W. S, Bai X. C and Yu Li (2009)** , “A High Bitrate Information Hiding Algorithm for Video

in Video”,World Academy of Science, Engineering and Technology 59, pp. 413-419.

**[15] Mozo A. J, Obien M. E, Rigor C. J, Rayel D. F, Chua K. and Tangonan G (2009)** , “Video

Steganography using Flash Video (FLV)”, I2MTC 2009 - International Instrumentation and

Measurement Technology Conference Singapore, pp.5-7.

**[16] Kim S. M, Cheng Z and Yoo K.Y (2009)** , “A New Steganography Scheme based on an Indexcolor

Image”, 2009 Sixth International Conference on Information Technology: New Generations,

pp.376-381.

**[17] Luo W, Huang F and Huang J (2010)** , “Edge Adaptive Image Steganography Based on LSB

Matching Revisited”, IEEE Transactions On Information Forensics And Security, Vol. 5, No. 2,

pp.201-214

**[18] Nikoukar A. A (2010)** , “An Image Steganography method with high data hiding Capacity Based

on RGB Image”, International Journal of Signal and Processing, pp.238-241.

**[19] Wei Y, Guo L, Wang Y (2010**) , “Controlling Bitrate Steganography on AAC Audio”, 2010 3rd

International Congress on Image and Signal Processing (CISP2010), pp.4373-4375.

**[20] Djebbar F, Ayad B, Hamam H and Meraim K. A (2011)** , “A view on latest audio steganography

techniques”, 2011 international conference on innovations in information and technology, pp.409-414.

**[21] Gadicha1 A. B (2011**), “Audio Wave Steganography”, International Journal of Soft Computing

and Engineering (IJSCE) ISSN: 2231-2307, Volume-1, Issue-5, pp.174-176.