JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Video Steganographic Techniques

Siddiqui Bushra Zareen, Asst.Prof Dr.Rafiq Zakaria College For Women Auranagabad, Maharashtra, India.

Abstract--- Information hiding is a part of information Security. Steganography is a technique of information hiding that focuses on hiding the existence of secret messages. The aim of steganographic methods is to hide the existence of the communication and therefore to keep any third-party unaware of the presence of the Steganographic exchange. More it is used to make sure that your secrete data transfer over the network without any problem, It has ability to conceal and reveal the exact hidden data from video file without disturbing the running application or new application

The main goal of steganography is to communicate securely in a completely undetectable manner and to avoid drawing suspicion to the transmission of a hidden data. It is not to keep others from knowing the hidden information, but it is to keep others from thinking that the information even exists. If a Steganography method causes someone to suspect the carrier medium, then the method has failed.

Until recently, information hiding techniques received very much less attention from the research community and from industry than cryptography. This situation is, however, changing rapidly and the first academic conference on this topic was organized in 1996. There has been a rapid growth of interest in steganography for two main reasons:

(i) The publishing and broadcasting industries have become interested in techniques for hiding encrypted copyright marks and serial numbers in digital films, audio recordings, books and multimedia products.

(ii) Moves by various governments to restrict the availability of encryption services have motivated people to study methods by which private messages can be embedded in seemingly innocuous cover messages.

Keywords--- Cryptography, Data Communication, Steganography, Least Significant Bit (LSB), Hidden Messages.

I. Introduction

In the field of Data Communication, security-issues have got the top priority. So, of late the degree of security provided by a security tool has become the main evolutionary criteria of it. Classical cryptography is one of the ways to secure plain text messages. Along with that at the time of data transmission, security is also implemented by introducing the concept of steganography, watermarking, etc.

Steganography is a technique for information hiding. It aims to embed secret data into a digital cover media, such as digital audio, image, video, etc., without being suspicious. Steganography is hiding private or secret data within a carrier in invisible manner. The word Steganography is of Greek origin and means "concealed writing" from the Greek words ‘steganos’ meaning covered or protected, and ‘graphei’ meaning writing. The medium where the secret data is hidden is called as cover medium, this can be image, video or anaudio +file. Any steganographic algorithm removes the redundant bits in the cover media and inserts the secret data into the space. Higher the quality of video or sound more redundant bits are available for hiding.

Steganography is an ancient art of conveying messages in a secret way that only the receiver knows the existence of message. The subject of steganography has been brought into the limelight by several intelligence agencies and the news media in recent times. Apart from using state of the art, communication technologies and media, the agencies are using cryptography as well as steganography to aid themselves with their objective. So, a fundamental requirement for a steganographic method is imperceptibility; this means that the embedded messages should not be discernible to the human eye.

Application of Steganography varies from military, industrial applications to copyright and Intellectual Property Rights (IPR). By using lossless Steganography techniques messages can be sent and received securely. Traditionally, Steganography was based on hiding secret information in image files. But modern work suggests that there has been growing interest among research fraternity in applying steganographic techniques to video files as well.

The advantage of using video files in hiding information is the added security against the attack of hacker due to the relative complexity of the structure of video compared to image files.

Video based steganographic techniques are broadly classified into temporal domain and spatial domain. In frequency domain, images are transformed to frequency components by using FFT, DCT or DWT and then messages are embedded in some or all of the transformed coefficients. Embedding may be bit level or in block level. Moreover in spatial domain the bits of the message can be inserted in intensity pixels of the video in LSB positions. The advantage in the method is that the amount of data (payload) that can be embedded is more in LSB techniques. However most of the LSB techniques are prone to attack. This makes research fraternity interested in designing new methods. Techniques other than LSB substitution also exist in literature and have been discussed in the next section and also the flow of project is described.

II. Literature Review

A literature review is usually included into a research report as a background to how you choose your own topic and research area. That being said, the literature review is going to include what other studies on this

topic have already been done, the method used to obtain the results, the results of the study, and what you felt they left out of the study, or how the study could be improved.

2.1. Information Gathering

There are mainly three basic data embedding techniques for images in practice, namely Least Significant Bit (LSB) Method, Masking and filtering and Transform based. The primitive method is embedding in LSB. Although there are several disadvantages to this approach, the relative easiness to implement it makes it a popular method. In this method we embed information in the LSB of pixels colours. The changes of LSB may not be noticeable because of the imperfect sensitivity of the human eyes. On an average, only half of the bits in an image will need to be modified to embed a secret message using the maximal cover size. While using a 24-bit image gives a relatively large amount of space to hide messages, it is also possible to use an 8-bit image as a cover source. Because of the smaller space and different properties, 8-bit images require a more careful approach. Where 24-bit images use three bytes to represent a pixel, an 8-bit image uses only one. Changing the LSB of that byte will result in a visible change of colour, as another colour in the available palette will be displayed. Therefore, the cover image needs to be selected more carefully and preferably be in gray scale, as the human eye will not detect the difference between different gray values as easy as with different colours [5].

Masking and filtering techniques, usually restricted to 24 bits or gray scale images, take a different approach to embedding a message. These methods are effectively similar to paper watermarks, creating markings in an image. This can be achieved, for example, by modifying the luminance of parts of the image. While masking does change the visible properties of an image, it can be done in such a way that the human eye will not notice the difference. Since masking uses visible aspects of the image, it is more robust than LSB modification with respect to compression, cropping and different kinds of image processing. The information is not hidden at the noise level but is in the visible part of the image which makes it more suitable than LSB modifications in case a lossy compression algorithm like JPEG is being used. In transform based data embedding, the cover image is transformed into another domain. Then the data is embedded in the transform coefficients. This method is highly robust and complex. The major transformations used are DCT and DWT. DCT is used in JPEG compression algorithm to transform successive 8_8 pixel blocks of the image, into 64 DCT coefficients each. After calculating the coefficients, the quantizing operation is performed. Although a modification of a single DCT will affect all 64 image pixels, the LSB of the quantized DCT coefficient can be used to embed information [1].

Steganographic techniques

Physical steganography

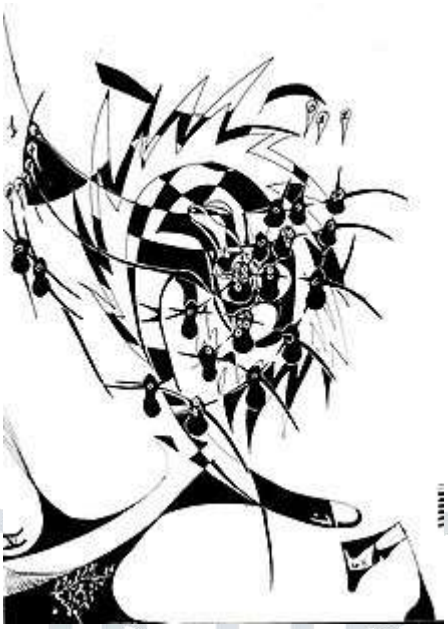


Fig 2.1 Physical Steganography

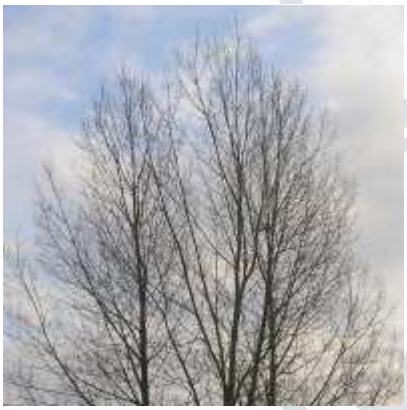
Steganart example: Within this picture, the letter positions of a hidden message are represented by increasing numbers (1 to 20), and a letter value is given by its intersection position in the grid. For instance, the first letter of the hidden message is at the intersection of 1 and 4. So, after a few tries, the first letter of the message seems to be the 14th letter of the alphabet; the last one (number 20) is the 5th letter of the alphabet. Steganography has been widely used, including in recent historical times and the present day. Possible permutations are endless and known examples include:

- Hidden messages within wax tablets: In ancient Greece, people wrote messages on the wood, and then covered it with wax upon which an innocent covering message was written.
- Hidden messages on messenger's body: Also used in ancient Greece. Herodotus tells the story of a message tattooed on a slave's shaved head, hidden by the growth of his hair, and exposed by shaving his head again. The message allegedly carried a warning to Greece about Persian invasion splans. This method has obvious drawbacks, such as delayed transmission while waiting for the slave's hair to grow, and the restrictions on the number and size of messages that can be encoded on one person's scalp.
- In WWII, the French Resistance sent some messages written on the backs of couriers using invisible ink.
- Hidden messages on paper written in secret inks, under other messages or on the blank parts of other messages.
- Messages written in Morse code on knitting yarn and then knitted into a piece of clothing worn by a courier.
- Messages written on the back of postage stamps.
- During and after World War II, espionage agents used photographically produced microdots to send information back and forth. Microdots were typically minute, approximately less than the size of the period

produced by a typewriter. WWII microdots needed to be embedded in the paper and covered with an adhesive (such as collodion). This was reflective and thus detectable by viewing against glancing light. Alternative techniques included inserting microdots into slits cut into the edge of post cards.

- During World War II, a spy for Japan in New York City, Velvalee Dickinson, sent information to accommodation addresses in neutral South America. She was a dealer in dolls, and her letters discussed how many of this or that doll to ship. The stego text was the doll orders, while the concealed "plaintext" was itself encoded and gave information about ship movements, etc. Her case became somewhat famous and she became known as the Doll Woman.
- Cold War counter-propaganda. In 1968, crew members of the USS Pueblo (AGER-2) intelligence ship held as prisoners by North Korea, communicated in sign language during staged photo opportunities, informing the United States they were not defectors but rather were being held captive by the North Koreans. In other photos presented to the US, crew members gave "the finger" to the unsuspecting North Koreans, in an attempt to discredit photos that showed them smiling and comfortable.

Digital steganography



(a) Image of a tree.

(b) Image of a cat.

Fig 2.2 Digital Steganography

Image of a tree: Removing all but the two least significant bits of each color component produces an almost completely black image. Making that image 85 times brighter produces the image above.

Image of a cat extracted from above image. Modern Steganography entered the world in 1985 with the advent of the personal computer being applied to classical Steganography problems. Development following that was slow, but has since taken off, going by the number of "stego" programs available: Over 800 digital Steganography applications have been identified by the Steganography Analysis and Research Center. Digital Steganography techniques include:

- Concealing messages within the lowest bits of noisy images or sound files.
- Concealing data within encrypted data or within random data. The data to be concealed is first encrypted before being used to overwrite part of a much larger block of encrypted data or a block of random

data (an unbreakable cipher like the one-time pad generates cipher texts that look perfectly random if you don't have the private key).

- Chaffing and winnowing.
- Mimic functions convert one file to have the statistical profile of another. This can thwart statistical methods that help brute-force attacks identify the right solution in a cipher text-only attack.
- Concealed messages in tampered executable files, exploiting redundancy in the i386 instruction set.
- Pictures embedded in video material (optionally played at slower or faster speed).
- Injecting imperceptible delays to packets sent over the network from the keyboard. Delays in key presses in some applications (telnet or remote desktop software) can mean a delay in packets, and the delays in the packets can be used to encode data.
- Content-Aware Steganography hides information in the semantics a human user assigns to a datagram. These systems offer security against a non-human adversary/warden.
- Blog-Steganography. Messages are fractionalized and the (encrypted) pieces are added as comments of orphaned web-logs (or pin boards on social network platforms). In this case the selection of blogs is the symmetric key that sender and recipient are using; the carrier of the hidden message is the whole blogosphere.

Network steganography

All information hiding techniques that may be used to exchange steganograms in telecommunication networks can be classified under the general term of network Steganography. This nomenclature was originally introduced by Krzysztof Szczypiorski in 2003. Contrary to the typical steganographic methods which utilize digital media (images, audio and video files) as a cover for hidden data, network Steganography utilizes communication protocols control elements and their basic intrinsic functionality. As a result, such methods are harder to detect and eliminate.

Typical network Steganography methods involve modification of the properties of a single network protocol. Such modification can be applied to the PDU (Protocol Data Unit), to the time relations between the exchanged PDUs, or both (hybrid methods).

Moreover, it is feasible to utilize the relation between two or more different network protocols to enable secret communication. These applications fall under the term inter-protocol Steganography.

Network Steganography covers a broad spectrum of techniques, which include, among others:

- Steganophony -The concealment of messages in Voice-over-IP conversations, e.g. the employment of delayed or corrupted packets that would normally be ignored by the receiver (this method is called LACK - Lost Audio Packets Steganography), or, alternatively, hiding information in unused header fields.
- WLAN Steganography – the utilization of methods that may be exercised to transmit steganograms in Wireless Local Area Networks. A practical example of WLAN Steganography is the HICCUPS system (Hidden Communication System for Corrupted Networks)

Printed steganography

Digital Steganography output may be in the form of printed documents. A message, the plaintext, may be first encrypted by traditional means, producing a cipher text. Then, an innocuous cover text is modified in some way so as to contain the cipher text, resulting in the stego text. For example, the letter size, spacing, typeface, or other characteristics of a cover text can be manipulated to carry the hidden message. Only a recipient who knows the technique used can recover the message and then decrypt it. Francis Bacon developed Bacon's cipher as such a technique.

The cipher text produced by most digital Steganography methods, however, is not printable. Traditional digital methods rely on perturbing noise in the channel file to hide the message, as such the channel file must be transmitted to the recipient with no additional noise from the transmission. Printing introduces much noise in the cipher text, generally rendering the message unrecoverable. There are techniques that address this limitation, one notable example is ASCII Art Steganography.

Steganography using sudoku puzzle

This is the art of concealing data in an image using Sudoku which is used like a key to hide the data within an image. Steganography using Sudoku puzzle makes Steganography a very strong method since Sudoku is used as a key. The strongest feature about Sudoku is the number of possible solutions of a Sudoku puzzle, which is 6.71×10^{21}. This is equivalent to around 70 bits in binary making it much stronger than DES method which uses 56 bit key.

2.1.3. Countermeasures and detection

Detection of physical Steganography requires careful physical examination, including the use of magnification, developer chemicals and ultraviolet light. It is a time-consuming process with obvious resource implications, even in countries where large numbers of people are employed to spy on their fellow nationals. However, it is feasible to screen mail of certain suspected individuals or institutions, such as prisons or prisoner-of-war (POW) camps. During World War II, a technology used to ease monitoring of POW mail was specially treated paper that would reveal invisible ink. An article in the June 24, 1948 issue of Paper Trade Journal by the Technical Director of the United States Government Printing Office, Morris S. Kantrowitz, describes in general terms the development of this paper, three prototypes of which were named Sensicoat, Anilith, and Coatalith paper. These were for the manufacture of post cards and stationery to be given to German prisoners of war in the US and Canada. If POWs tried to write a hidden message the special paper would render it visible. At least two US patents were granted related to this technology, one to Mr. Kantrowitz, No. 2,515,232, "Water-Detecting paper and Water-Detecting Coating Composition Therefor", patented July 18, 1950, and an earlier one, "Moisture-Sensitive Paper and the Manufacture Thereof", No. 2,445,586, patented July 20, 1948. A similar strategy is to issue prisoners with writing paper ruled with a water-soluble ink that "runs" when in contact with a water-based invisible ink.

In computing, detection of steganographically encoded packages is called steganalysis. The simplest method to detect modified files, however, is to compare them to known originals. For example, to detect information being moved through the graphics on a website, an analyst can maintain known-clean copies of these materials and compare them against the current contents of the site. The differences, assuming the carrier is the same, will compose the payload. In general, using extremely high compression rate makes steganography difficult, but not impossible. While compression errors provide a hiding place for data, high compression reduces the amount of data available to hide the payload in, raising the encoding density and facilitating easier detection (in the extreme case, even by casual observation).

2.1.4. Applications

Steganography is applicable to, but not limited to, the following areas.

- Confidential communication and secret data storing
- Protection of data alteration
- Access control system for digital content distribution
- Media Database systems

Confidential communication and secret data storing

The "secrecy" of the embedded data is essential in this area. Historically, Steganography have been approached in this area. Steganography provides us with:

- Potential capability to hide the existence of confidential data
- Hardness of detecting the hidden (i.e., embedded) data
- Strengthening of the secrecy of the encrypted data

In practice, when you use some Steganography, you must first select a vessel data according to the size of the embedding data. The vessel should be innocuous. Then, you embed the confidential data by using an embedding program (which is one component of the Steganography software) together with some key. When extracting, you (or your party) use an extracting program (another component) to recover the embedded data by the same key ("common key" in terms of cryptography). In this case you need a "key negotiation" before you start communication.

Attaching a stego file to an e-mail message is the simplest example in this application area. But you and your party must do a "sending-and-receiving" action that could be noticed by a third party. So, e-mailing is not a completely secret communication method.

There is an easy method that has no key-negotiation. We have a model of "Anonymous Covert Mailing System."

There is some other communication method that uses the Internet Webpage. In this method you don't need to send anything to your party, and no one can detect your communication.

Each secrecy based application needs an embedding process which leaves the smallest embedding evidence. You may follow the following.

- Choose a large vessel, larger the better, compared with the embedding data.
- Discard the original vessel after embedding.

Protection of data alteration

We take advantage of the fragility of the embedded data in this application area.We asserted in the Home Page that "the embedded data can rather be fragile than be very robust." Actually, embedded data are fragile in most Steganography programs. Especially, Qtech Hide & View program embeds data in an extremely fragile manner. We demonstrate this in the other page.

However, this fragility opens a new direction toward an information-alteration protective system such as a "Digital Certificate Document System." The most novel point among others is that "no authentication bureau is needed." If it is implemented, people can send their "digital certificate data" to any place in the world through Internet. No one can forge, alter, nor tamper such certificate data. If forged, altered, or tampered, it is easily detected by the extraction program.

Access control system for digital content distribution

In this area embedded data is "hidden", but is "explained" to publicize the content. Today, digital contents are getting more and more commonly distributed by Internet than ever before. For example, music companies release new albums on their Webpage in a free or charged manner. However, in this case, all the contents are equally distributed to the people who accessed the page. So, an ordinary Web distribution scheme is not suited for a "case-by-case" and "selective" distribution. Of course it is always possible to attach digital content to e-mail messages and send to the customers. But it will take a lot of cost in time and labor.

If you have some valuable content, which you think it is okay to provide others if they really need it, and if it is possible to upload such content on the Web in some covert manner. And if you can issue a special "access key" to extract the content selectively, you will be very happy about it. A steganographic scheme can help realize to this type of system.

We have developed a prototype of an "Access Control System" for digital content distribution through Internet. The following steps explain the scheme.

- A content owner classify his/ her digital contents in a folder-by-folder manner, and embed the whole folders in some large vessel according to a steganographic method using folder access keys, and upload the embedded vessel (stego data) on his/her own Webpage.
- On that Webpage the owner explains the contents in depth and publicize worldwide. The contact information to the owner (post mail address, e-mail address, phone number, etc.) will be posted there.

- The owner may receive an access-request from a customer who watched that Webpage. In that case, the owner may (or may not) creates an access key and provide it to the customer (free or charged).
- In this mechanism the most important point is, a "selective extraction" is possible or not.

2.1.5. Steganography tools

- Puff: BMP_file_format, Jpg, Portable_Network_Graphics, Portable_Executable, Mp3, Wav, 3gp, Mp4, MPEG-1, MPEG-2, Vob, Swf, Flv
- S-Tools: BMP_file_format, Gif, Wav, unused floppy disk space
- MP3Stego: Mp3
- Invisible Secrets: BMP_file_format,Portable_Network_Graphics, Jpg, Wav, Html
- StegFS; Steganographic_file_system
- Steganography tools
- PhilProxy PNG Steganography

2.1.6. Usage in modern printers

Steganography is used by some modern printers, including HP and Xerox brand color laser printers. Tiny yellow dots are added to each page. The dots are barely visible and contain encoded printer serial numbers, as well as date and time stamps.

2.1.7. Example from modern practice

The larger the cover message is (in data content terms—number of bits) relative to the hidden message, the easier it is to hide the latter. For this reason, digital pictures (which contain large amounts of data) are used to hide messages on the Internet and on other communication media. It is not clear how commonly this is actually done. For example: a 24-bit bitmap will have 8 bits representing each of the three color values (red, green, and blue) at each pixel. If we consider just the blue there will be 2^8 different values of blue. The difference between 11111111 and 11111110 in the value for blue intensity is likely to be undetectable by the human eye. Therefore, the least significant bit can be used (more or less undetectably) for something else other than color information. If we do it with the green and the red as well we can get one letter of ASCII text for every three pixels.

Stated somewhat more formally, the objective for making steganographic encoding difficult to detect is to ensure that the changes to the carrier (the original signal) due to the injection of the payload (the signal to covertly embed) are visually (and ideally, statistically) negligible; that is to say, the changes are indistinguishable from the noise floor of the carrier. Any medium can be a carrier, but media with a large amount of redundant or compressible information are better suited.

From an information theoretical point of view, this means that the channel must have more capacity than the "surface" signal requires; that is, there must be redundancy. For a digital image, this may be noise from the imaging element; for digital audio, it may be noise from recording techniques or amplification equipment. In general, electronics that digitize an analog signal suffer from several noise sources such as thermal noise, flicker noise, and shot noise. This noise provides enough variation in the captured digital information that it can be exploited as a noise cover for hidden data. In addition, lossy compression schemes (such as JPEG) always introduce some error into the decompressed data; it is possible to exploit this for steganographic use as well.

Steganography can be used for digital watermarking, where a message (being simply an identifier) is hidden in an image so that its source can be tracked or verified (for example, Coded Anti-Piracy), or even just to identify an image (as in the EURion constellation)

2.1.8. Alleged use by terrorists

When one considers that messages could be encrypted steganographically in e-mail messages, particularly e-mail spam, the notion of junk e-mail takes on a whole new light. Coupled with the "chaffing and winnowing" technique, a sender could get messages out and cover their tracks all at once.

Rumours about terrorists using steganography started first in the daily newspaper USA Today on February 5, 2001 in two articles titled "Terrorist instructions hidden online" and "Terror groups hide behind Web encryption". In July the same year, an article was titled even more precisely: "Militants wire Web with links to jihad". A citation from the article: "Lately, al-Qaeda operatives have been sending hundreds of encrypted messages that have been hidden in files on digital photographs on the auction site eBay.com".

2.2. The Scope of Steganography

With the boost in computer power, the internet and with the development of digital signal processing (DSP), information theory and coding theory, steganography has gone “digital”. In the realm of this digital world, steganography has created an atmosphere of corporate vigilance that has spawned various interesting applications, thus its continuing evolution is guaranteed. Cyber-crime is believed to benefit from this digital revolution. Hence an immediate concern is to find out best possible attacks to carry out steganalysis, and simultaneously, finding out techniques to strengthen existing steganography techniques against popular attacks like steganalysis.

2.3. Cryptography

Cryptography encodes information in such a way that nobody can read it, except the person who holds the key. More advanced crypto techniques ensure that the information being transmitted has not been modified in transit. There is some difference in cryptography and steganography, in cryptography the hidden message is always visible, because information is in plain text form but in steganography hidden message is invisible.

2.4. Steganography versus Cryptography

The comparison and contrast between steganography and cryptography is illustrated from the following table 2.1

Table 2.1 Comparison and contrast between Steganography and Cryptography.

Conclusion

Sr. No.	Context	Steganography	Cryptography
1	Files	Image, Audio, Video Text, etc.	Mostly Text Files
2	Hidden Files	Image, Audio, Video Text, etc.	Mostly Text Files
3	Result	Stego File	Cipher text
4	Type of Attacks	Steganalysis: Analysis of a file with an objective of finding whether it is stego file or not.	Cryptanalysis

Hidden messages remain an important and evolving science facilitating the secure transmission of information. Steganographic techniques and processes exploit detection limitations in the human visual system to store messages in underutilized/redundant bits used by digital media.

References

[1] Du, Hansong, Jiufen Liu, Yuguo Tian, and Xiangyang Luo. "Cryptographic Secrecy Analysis of Adaptive Steganographic Syndrome-Trellis Codes." *Security and Communication Networks* 2021 (July 27, 2021): 1–16. http://dx.doi.org/10.1155/2021/5495941.

[2] Chen, Zhe, Jicang Lu, Pengfei Yang, and Xiangyang Luo. "Recognizing Substitution Steganography of Spatial Domain Based on the Characteristics of Pixels Correlation." *International Journal of Digital Crime and Forensics* 9, no. 4 (2017): 48–61. http://dx.doi.org/10.4018/ijdcf.2017100105.

[3] Mritha Ramalingam, Stego Machine Video Steganography using Modified LSB Algorithm, in World Academy of Science, Engineering and Technology 74 2011, pp. 502-505, 2011Jiawei, H. and Micheline,

[4] Juan Jose Roque and Jesus Maria Minguet, SLSB: Improving the Steganographic Algorithm LSB, in the 7th International Workshop on Security in Information Systems (WOSIS 2009), Milan, Italy, pp.1-11, 2009.

[5] Heena GoyalInternational Journal of Emerging Technology and Innovative Engineering Volume 1, Issue 9, September 2015 (ISSN: 2394 – 6598)Osborne, D., & Wernicke, S.

[6] *Simaranjit Kaur International Journal of Computer Science Trends and Technology (IJCST) – Volume 3 Issue 2, Mar-Apr 2015*

[7] Kharrazi, M., Sencar, H. T., and Memon, N. (2004). Image steganography: Concepts and practice. In WSPC Lecture Notes Series

[8] Mazdak Zamani, Azizah A. Manaf, and Shahidan Abdullah, ―A Genetic-Algorithm-Based Approach for Audio Steganography‖ WASET 2009