# An Extensive Review on Enhancing Audio and Video Steganography Technique

Nensi Rai[1], Prof. Amarjeet Ghosh[2]

*[1]M.Tech Scholar, [2]Research Guide*

*Department of Electronics and Communication Engg., VITS Bhopal*

***Abstract- In the age of information, multimedia content (e.g, audio, and image, video and computer graphics models) in digital form is being used in a wide range of application areas. However, at the same time, an increasing number of security problems have been revealed. For instance, the proliferation of intelligent editing tools can also facilitate misuse, illegal copying and distribution, plagiarism and misappropriation, which could seriously ruin the interests of the creator or owner of the multimedia work. This is creating a strong need for schemes that can efficiently cope with multimedia security and privacy, including copyright protection and integrity authentication. This work presents an extensive literature review on the techniques of data hiding and Steganography.***

***Keywords- Steganography, Data Hiding, Information Security, Image Audio and Video Steganography, Cryptography, Hybrid Steganography algorithm.***

## I. INTRODUCTION

In today’s era Information is power. So, in this information age there is a need to transfer information very carefully. The way of transferring confidential information hiding inside a cover medium is called as Steganography. This word Steganography is a combination of two Greek words. The two sub-words are “Steganos” and “Graphia”. In Greek “Graphia” means “writing” whereas “Steganos” means “Covered”.

This technique is not new for this world. It was practiced long before, since 440 BC. The war messages were transferred through different media such as writing message on wood then covering that by wax, writing with invisible inks which can be read in a particular light, writing inside the stomach of the rabbit. They also used human as a secret medium to transfer data, first they used to shave the head, tattood the secret message on scalp, then wait until the hair grows. After the hair grows completely they send the person to the destination and the secret message extracted by shaving the head of that person again.

Now, internet is the main media of communication. After the invention of social media sites images, videos are transferred in enormous amount daily using internet. So, today Steganography depends upon images audio and videos for covert media.

Steganography is a Greek word which means concealed writing. The word steganos means covered and graphia means writing. Thus, steganography is not only the art of hiding data but also hiding the fact of transmission of message. Thus, steganography is an art as well as science of transmission of secret message by embedding the message into cover body such that the existence of information is invisible. The cover body when carries the secret message is called as stegomedium. In ancient time, the data was protected by hiding it on the back of wax, stomach of rabbits, on the scalp of slaves. But today most of the data is transferred through text, images, audio and video over a network. So, for the transmission of any confidential data, the chosen stego-mediums are text, images, audio and video.

Since 1990s, the investigation of a technology that is able to serve as a complement to cryptography has attracted extensive attention from both academic and industrial organization. Information hiding has been widely deemed as a fairly promising technology to fulfill this purpose. Information hiding works by secretly embedding a message within a host digital signal. The message to be embedded can be whatever want to insert, such as a personal identification code, a company logo or a to-be-delivered secret information string, depending on the specific application scenarios. Because of its potential applications, information hiding has become an emerging research area over the past few decades.

In contrast to cryptography which tries to make the meaning of information obscure to a person who intercepts it, information hiding technique aims chiefly at keeping the existence of the information secret or making the embedded information imperceptible. While cryptography arouses suspicion due to the unreadability of encrypted information, information hiding avoids this through invisible message embedding. The embedding of message is achieved by employing human binaural or perceptual redundancies. More specifically, the redundancies are the details of a multimedia signal that a human ear cannot hear or that a human eye cannot perceive. Basic hiding techniques include modifying the least significant bits of the pixels of a host image and adding tabs and spaces at the end of the lines of an HTML document.

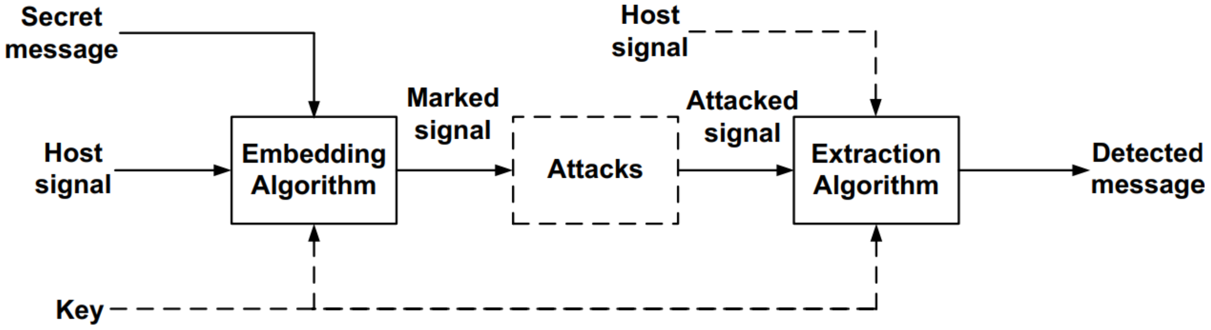

Fig. A generic framework for message embedding and extraction.

As Fig. 1.1 shows, information hiding usually consists of two procedures: message embedding and message extraction

## II. STEGANOGRAPHY TECHNIQUES

Until now he have spoken about steganography as a set of methods for hiding information. Strictly speaking this is not a hundred percent correct definition, as the set of methods used to hide information is in fact called information hiding methods, being steganography a subset of them. Information hiding is the science that includes any method that serves for hiding any type of information, what- ever its nature is, its means, or its purposes. Therefore, inside the information hiding can speak of watermarking, which consists in introducing little amounts of information to serve as copyrights to protect authors' rights; fingerprints, also small amounts of information but this time with the purpose to identify a concrete object, in a way that afterwards it is possible to trace a chain of illegal copies to the original source (a technique known as traitor tracing; the steganography, strictly speaking, focuses in transmitting high amounts of in- formation in an imperceptible manner, although less robust; and yet another field, totally different, but still information hiding, is the anonymity, which with techniques like Onion Routing allows the original sender of a given information to hide his identity to the recipient.

By linguistic steganography understand the steganography whose carrier is a written text, while the technical steganography is used for any other carrier type, be it audio, image, video, etc. At the other side, copyright marking techniques are divided into fragile marking, in which the introduced marks serve as means for detecting when a content has been modified and does not fulfill certain requirements it should it it were original. Therefore fragile marking techniques are expected to introduce easily removable but yet imperceptible marks. Robust marking, at the contrary, tries to introduce secure marks (difficult to remove even for intentional attacks). Fingerprinting techniques hide serial numbers to allow, for example, the identification of the source of an illegal copies chain. Watermarking techniques introduce the so called watermarks as copyrights, to allow the identification of the legitimate author of a given information. Watermarks can either be perceptible or imperceptible, but must be secure and robust. Lastly, the establishments of hidden channels and anonimity branches have a self explanatory name.

So, steganography, which is an information hiding branch that aims relatively high capacities, high invisibility and low robustness. As seen, the media over which the steganography is to be applied, has to be studied carefully, to reach the desired objectives and be able to choose the more adequate steganographic methods. Even with that methodology, developing an steganographic method is a delicate task. It is not enough with taking care at designing time. For a steganographic method to be considered effective in terms of capacity, invisibility and robustness, it has to be subject to the experts scrutiny, and deep statistical and perceptual analysis. Just designing a steganographic method and claiming it is invincible or undetectable without following the mentioned steps, as for every security application, is like a “show for the gallery”.

As steganographic techniques require a high level of knowledge of the stegano- graphic techniques they pretend to detect, identify and break, we’ll first center our attention into steganographic techniques, and afterwards, once known the most important algorithms, will focus in steganalytic methods that let us detect and/or cancel the studied steganographic methods.

Steganographic algorithms can be classified in several ways: depending on the carrier type (images, audio, video, or text, mainly); the very algorithm type (LSB hiding, statistical variations, order permutations, etc.); in terms of the degree of capacity, robustness or invisibility achieved; or the objective pursued.

### *A. Color Palette Modification (Image)*

Palette base images (mainly BMP and GIF), are composed by a set of concrete colors. Each one of these colors is assigned a vector, representing the value of the color, and an index, creating in this way a palette. In the different image positions the index to the color in the palette corresponding to the value of the pixel to represent will be used, instead of the value itself. Therefore, to hide information in images of this kind, what one can do is to modify the color values stored in the palette (using, e.g., some technique as LSB substitution), or changing the way of ordering the colors of the palette, given that, having a N colors size of palette, there will be N ! different orderings, being this an important size even for a little number of colors; one can also choose to modify the image itself, but in this case special care has to be taken, because near indexes do not imply perceptually similar colors. Therefore, a rearrangement of the palette in such a manner that colors are grouped by perceptual resemblance.

*B. Substitution Methods*

- LSB Substitution (image and audio):

There exist different steganographic techniques based in the modification of the least significant bits, or LSBs, also referred in the literature as low- bit coding techniques. This kind of methods are based in the modification of the bits which provide less value to the carrier signal and, for this very reason, they will be the bits which introduce less error when modified. The only drawback of this approach is that, precisely due to that fact, they are the favourite candidates to be modified during a subsequent signal process- ing, decreasing drastically the robustness of this methods. But, as have already said, in this study prioritize capacity over robustness, and these techniques produce the highest capacity. Related to imperceptibility, several strategies can be taken to reduce the effect of the introduced modifications.

- Block parity (image and audio):

Another substitution method is based in dividing the carrier (an image or an audio track) into blocks or segments of a given size. Establishing an arbitrary ordering of the resulting blocks, each block's parity will be obtained and, if the parity of block bi matches the i-th bit of the subliminal message, nothing needs to be done; if they don't match, the least significant bit of one of the block's elements will be flipped. The receiver will just have to calculate the parity of the blocks, obviously using the same ordering than the sender used.

*C. Steganography Over Text*

Steganography over text is specially delicated, as almost any change could arouse suspicion, and for methods introducing less perceptible changes, the achieved capacity is very low. Also, for steganography over image or audio is mainly based in mainpulation and processing of the signals, while steganography over text does not have much in common with them. It is important to emphasize that with text are referring here to pure text, not scanned and stored in an image. As saw in the previous subsection, scanned text or text stored as an image can be treated just like any other image, with a little more of restrictions, but like an image in the end.

## III. LITERATURE REVIEW

| ***Sr. No.*** | ***Title*** | ***Authors*** | ***Year*** | ***Approach*** |
|---|---|---|---|---|
| 1 | Enhancing Audio and Video Steganography Technique Using Hybrid Algorithm | S. Teotia and P. Srivastava | 2018 | Author introduces a hybrid algorithm which reduces the error in audio and video steganography and gives better values of PSNR and MSE |
| 2 | Enhanced blend of image steganography and cryptography | R. S. Phadte and R. Dhanaraj | 2017 | a new method is proposed by author to provide security to 24 bit color images, by integrating Steganography and Cryptography |
| 3 | A security enhanced approach for video Steganography using K-Means clustering and direct mapping | P. K. Sethy, K. Pradhan and S. K. Behera | 2016 | Author reported a novel approach to resolve the remained problems such as robustness and capacity of image and video Steganography |
| 4 | An improved LSB based image steganography technique for RGB images | A. Singh and H. Singh | 2015 | Author introduced an improved LSB technique for color images by embedding the information into three planes of RGB image in a way that enhances the quality of image and achieves high embedding capacit |
| 5 | Enhanced stego-crypto | C. R. Geetha and C. | 2015 | Author reported data hiding by |

| | | | | |
|---|---|---|---|---|
| | techniques of data hiding through geometrical figures in an image | Puttamadappa | | embedding the message of interest using geometric style of cryptographic algorithm, thus providing high security |
| 6 | Highly randomized image steganography using secret keys | S. Dagar | 2014 | A new approach of image steganography which uses two secret keys to randomize the bit hiding process is reported. |
| 7 | A secure video steganography with encryption based on LSB technique | P. Yadav, N. Mishra and S. Sharma | 2013 | In proposed scheme video steganography is used to hide a secret video stream in cover video stream. |

S. Teotia and P. Srivastava [1] as the technology is developing, people have tend to find out methods which are not only capable in hiding an information but also capable of even hiding the existence of a message or information. Steganography was introduced as a result of such different research works, but despite of so many researches still have problems of minimizing the error and obtaining better PSNR values. Audio Steganography is a technique or technology which is used to transfer secret information or message by changing an audio signal into an imperceptible way. It's the ability of thrashing confidential message or audio data in a host or another message, Video Steganography refers to hiding a confidential data or message, it can be a text message or an image inside a larger or another one in a style that by only looking or seeing at it an unknown person cannot notice the existence of hidden message. Proposed examination presents a hybrid algorithm which reduces the error in audio and video steganography and gives better values of PSNR and MSE.

R. S. Phadte and R. Dhanaraj, [2] as there is large advancements in internet technology, there has been huge text as well as multimedia data transfer over the internet. Due to this data security is a vital necessity. Steganography and Cryptography are the sets of techniques to provide security to data. Steganography is an art of hiding secret information into another cover medium like image, audio, video, etc. Cryptography is an art of converting plain data into unreadable format. Steganography can be integrated with Cryptography in order to enhance the security of data. In this examination, a new method is proposed to provide security to 24 bit color images, by integrating Steganography and Cryptography. In this method, randomized LSB based method is used to hide an image in another image. The resulting stego image is then encrypted using chaotic theory. This new integrated method ensures the enhancement in the data hiding capacity, the security of the image and lossless recovery of the secret data.

P. K. Sethy, K. Pradhan and S. K. Behera, [3] Communication security has taken vital role with the advancement in digital communication. The universal use of internet for communication has increased the attacks to users. The security of information is the present issue related to privacy and safety during storage and communication. Cryptography and Steganography are two popular ways of sending essential information in a confidential way. Cryptography is the method of converting plain text into cipher text but in Steganography messages are converted into an encrypted format using a key and then this cipher text is hidden into an image, audio or video file as per user's choice. The information-hiding process in a steganographic system starts by identifying a cover medium's redundant bits (those that can be modified without destroying that medium's integrity). The embedding process starts with creating a stego medium by replacing these redundant bits with data from the hidden message. In this examination, present a novel approach to resolve the remained problems such as robustness and capacity of image and video Steganography. In the proposed algorithm, message bits are clustered and grouped together using K-Means clustering and then the clustered message is embedded inside the cover medium by using direct mapping which result increase the robustness and capacity of the cover medium. The robustness specially would be increased against those intended attacks which try to reveal the hidden message and also some unintended attacks like noise addition as well.

A. Singh and H. Singh [4] Steganography is the art and science of invisible communication by hiding secret information into other sources of information like text, video, audio, image etc. In image steganography the digital image is used as cover image in which hide data and the message implanted image is called stego-image. There are number of steganography techniques proposed to hide data like LSB, DCT, pixel-value differencing, DFT etc. into images with precision level. But these techniques suffering from some problems like less hiding capacity, degrade the quality of image and security of hidden data after hiding more data into it. To overcome these problems this examination proposed an improved LSB technique for color images by embedding the information into three planes of RGB image in a way that enhances the quality of image and achieves high embedding capacity. The PSNR value of the proposed technique is better than previous steganography methods.

C. R. Geetha and C. Puttamadappa [5] Cryptography is a technique for secret communication where as obscuring the secret communication using for different data is Steganography. The secret communication is carried through many sources like image, audio &amp; video files. This work is mainly proposing data hiding by embedding the message of interest using geometric style of cryptographic algorithm, thus providing high security. Wavelet and curvelet transform algorithms are used to perform preprocessing of images. Even if the image carrying embedded data i.e., Stego image undergoes a reverse operation and data cannot be extracted if the receiver is unaware of the exact coordinates of the geometric shape. Hence retrieving secret image for an attacker becomes a hard task. Proposed experimental results are verified for both the properties of Cryptography and Steganography it may be applicable for kind of multimedia applications.

S. Dagar [6] Steganography is an art and specially a science of hiding secret information inside a carrier like image, audio, video. This examination proposes a new approach of image steganography which uses two secret keys to randomize the bit hiding process. Use of two secret keys enhances the security of secret information. This approach uses red, green and blue values of a pixel and performs some calculation. Based on this calculation, secret information bits will be placed at the random position of the pixels. This approach maintains high data hiding capacity like LSB substitution but maintains a much better security level, which is not present in LSB substitution as LSB substitution technique is predictable. As the hidden information is highly randomized, so it is difficult for attacker to retrieve the secret information from stego image. I used PSNR value to determine the quality of stego image and also compare it with other efficient image steganography techniques. The obtained result showed that this algorithm is highly efficient as compared to many other techniques.

[P. Yadav, N. Mishra and S. Sharma [7] Need of hiding information from intruders has been around since ancient times. Nowadays Digital media is getting advanced like text, image, audio, video etc. To maintain the secrecy of information, different methods of hiding have been evolved. One of them is Steganography, which means hiding information under some other information without noticeable change in cover information. Recently Video Steganography has become a boon for providing large amount of data to be transferred secretly. Video is simply a sequence of images; hence much space is available in between for hiding information. In proposed scheme video steganography is used to hide a secret video stream in cover video stream. Each frame of secret video will be broken into individual components then converted into 8-bit binary values, and encrypted using XOR with secret key and encrypted frames will be hidden in the least significant bit of each frames using sequential encoding of Cover video. To enhance more security each bit of secret frames will be stored in cover frames following a pattern BGRRGBGR.

## IV. PROBLEM FORMULATION

The information revolution is the key technology in which the information has been gathered, processed and distributed as an interface between users, and many of the offices in this world. The development of communication makes the source of information to be more valuable and content with active speed like the International Network (Internet). The security issue is the main requirement for every system or protocol, which deals with information. To keep something secret, two basic ideas can be used: Audio Video and Hybrid steganography is an efficient method to secure embedded data and sent it through internet. Unfortintully the complexity of system and encryption with robustness is still a challenge for researchers.

## V. CONCLUSION

This work presents an extensive survey of literature based on related work and development work displays a broad review of writing based on related work and improvement in the field of data hiding. Data is shared universally through the Internet, in advanced structure. There are issues and difficulties with respect to the security of data in travel from senders to beneficiaries. The serious issue is the insurance of advanced information against any type of interruption, penetration, and theft. The real test is building up asolution for ensure data and guarantee their security amid transmission. Three segments of data security are classification, respectability, and accessibility. Privacy guarantees that data is stayed discreet from any unapproved get to. This should be possible through data hiding systems, in particular cryptography and steganography.

## REFERENCES

[1] S. Teotia and P. Srivastava, "Enhancing Audio and Video Steganography Technique Using Hybrid Algorithm," 2018 International Conference on Communication and Signal Processing (ICCSP), Chennai, 2018, pp. 1059-1063.

[2] R. S. Phadte and R. Dhanaraj, "Enhanced blend of image steganography and cryptography," 2017 International

Conference on Computing Methodologies and Communication (ICCMC), Erode, 2017, pp. 230-235.

[3] P. K. Sethy, K. Pradhan and S. K. Behera, "A security enhanced approach for video Steganography using K-Means clustering and direct mapping," 2016 International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT), Pune, 2016, pp. 618-622.

[4] A. Singh and H. Singh, "An improved LSB based image steganography technique for RGB images," 2015 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT), Coimbatore, 2015, pp. 1-4.

[5] C. R. Geetha and C. Puttamadappa, "Enhanced stego-crypto techniques of data hiding through geometrical figures in an image," 2015 2nd International Conference on Electronics and Communication Systems (ICECS), Coimbatore, 2015, pp. 116-122.

[6] S. Dagar, "Highly randomized image steganography using secret keys," International Conference on Recent Advances and Innovations in Engineering (ICRAIE-2014), Jaipur, 2014, pp. 1-5. doi: 10.1109/ICRAIE.2014.6909116].

[7] P. Yadav, N. Mishra and S. Sharma, "A secure video steganography with encryption based on LSB technique," 2013 IEEE International Conference on Computational Intelligence and Computing Research, Enathi, 2013, pp. 1-5.

[8] Malviya Swati, Dr Anubhuti Khare, Manish Saxena “Audio Steganography by Different Methods”. In proceedings of International Journal for Emerging Technologies ,Advanced Engineering ISSN- 2250-2459- Volume 2, Issue- 7 (2012)).

[9] Khan, Mohammad Kamran “Distributed Least Significant Bit technique for data hiding in images” in proceedings of Multitopic Conference (INMIC) 2011 IEEE 14th International. IEEE, 2011.

[10] HS. Anupama “Information Hiding uses Audio Steganography- a Survey” in proceedings of International Journal on Multimedia and Its Applications (2011).

[11] K Sherly A P and Amritha P “A Compressed video Steganography using TPVD”,in proceedings of International Journal for Databases Management Systems Vol.2.3 August,2010.

[12] Dutta Poulami, Debnath Bhattacharya & Tai,hoon Kim- “Data hiding in audio signal-A review.” In proceedings of International journal of databases theory and application 2.2 (2009).

[13] Amr A Hanafy Gouda I Salama and Yahya Z.Mohasseb “A Secure Covert Communication Model Based on Video Steganography,”in proceedings of Military Communications Conference 2008.

[14] Keio University Yokohama, japan, May 20-22-2009 NSC97-2221-E-468-006 International-conference on computational, intelligence, multimedia application 2007.