ISSN No. 0976-5697

Volume 8, No. 3, March – April 2017

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

A Review On Video Steganography Techniques

Anamika Saini
University Institute of Engineering and Technology
Maharshi Dayanand University
Rohtak, India

Kamaldeep Joshi
University Institute of Engineering and Technology
Maharshi Dayanand University
Rohtak, India

Sachin Allawadhi
University Institute of Engineering and Technology
Maharshi Dayanand University
Rohtak, India

Abstract: Secure communication is the necessary requirement in present cyber environment. For this we need a security system by which we can communicate in such a way that third party can't access our sensitive data. The main focus of the security system is the protection of secret information. For this security, we have different types of security mechanisms like Cryptography, Information Hiding. Steganography technique is applied where the cryptography is ineffective. We have different Steganography techniques like image, audio, video etc. As the structure of video is complex than image so the former is better than latter one to conceal information in video files than that of image file in terms of security. In this paper we are reviewing the basics of steganography and different video steganography techniques

Keywords: Video Steganography; LSB; AES; Hash Based LSB; DLSB

I. INTRODUCTION

In the data communication, when sensitive data is sent to the receiver over insecure network, we use different techniques to make the communication secure. For the security of information we have basically three types of techniques which are Cryptography, Watermarking and Steganography.

Cryptography is a science of ciphers which uses mathematics for the conversion of original text into unreadable encrypted format. [1] We use different encryption techniques but still the secret message becomes a subject to attack.

Watermarking is used for the identification of the owner copyright. Its main focus is to preserve the digital media's originality and integrity.

"Steganography" is a Greek word which means secret or concealed writing. The word "steganos" means "covered or protected" and "graphical" means "writing".[2]

Steganography is hidden communication and its impetus is to conceal the communication's existence by embedding and extracting method so that third person can't feel the presence of the secret message.

Using steganography we can hide different types of data like images, audio, text etc. Steganography is a technique in which by adding imperceptibility, it is the mixture of cryptography and watermarking. There are three types of protocols are used in steganography according to ***Stefan C. Katzenbeisser*** [3]

A. Pure Key Steganography

There is not any requirement of the interchange of a cipher key or stego key. The assumption of sender and receiver that no one knows about the secret message makes it least secure.

B. Secret Key Steganography

It requires the exchange of secret key. Secret key helps the receiver for extracting message.

C. Public Key Steganography

In this technique public key is used for encoding process and private key is used for decipher the message. Both key has a direct mathematical relationship with each other.

Table 1: Comparison of three Techniques [4]

Criteria	Cryptography	Watermarking	Steganography
Objective	Protection	Copyright Protection	Secret communication
Secret Information	Text files are used	Watermarks are used	Any type of file can be used
Secret Key	Key is necessary	Key is optional to use	Key is optional to use
Carrier Object	Text or image file	Only digital image/audio	Any media can be used

Selection of cover	N/A	Restriction in cover selection	Any type of cover can be chosen.
Visibility	Due to encryption, it is easy to know that there is hidden data but deciphering is difficult.	May or may not be visible to human eye.	Never perceptible to the normal human vision.
Detection and retrieval	Full retrieval of data can be done without the need of the cover	Cross-correlation helps in data retrieval.	Full retrieval of data is possible and cover is not needed for recovery.
Capacity	High	Low	High
Attacks	Cryptanalysis	Steganalysis	Replacement of watermarks
Security	High	High	Very High

II. BACKGROUND OF STEGANOGRAPHY

Steganography is a technique which conceals the transmission's fact of confidential data. Roots of steganography were tracked in 440 BC. In written texts, Steganography appears in 1606 published in Frankfurt by Johannes Trithemius.

A. *Early proof of Steganography*

In ancient times, secret information was hidden such as tattooed on the scalp of bondsman, concealed on tablets cover or rabbit's stomachs. The written steganography account used during 484-425 BC.

In ancient Greece, for writing the text, wax covered tablets were used. As the tablets appeared to be unused and blank by snippet the wax the message which was hidden can be reveled. Aeneas Tactician proposed another technique of steganography, who was a Greek writer. His technique was to hide the secret message by using pigeons or women's earrings.

B. *Linguistic Steganography*

It is the oldest forms of steganography. The founder of linguistic steganography was Aeneas Tactician. He alters the elevation of letters with small holes or spot.

A largest example of Linguistic Steganography was in 14th Century when Giovanni Boccaccio who was a poet, in his acrostic poem encoded over 1500 letters taken from three sonnets. Francis Bacon's method was to conceal the message by binary representation using italic or normal font. This technique is most interesting technique and forefather to modern steganography techniques.

A photographic technique in 1857 suggested by Brewster, it allows text to be shrunk down to a dirt-sized fleck. Only under big exaggeration the message is readable. During World War I, the Germans used this technique. On more modification of linguistic steganography is Null cipher.

C. *Modern Steganography*

Modern Steganography is necessary with the origin of present day technology and Internet. Dissimilar multimedia presents interesting digital file formats for hiding the information. Secure data transmission is the main demand of the internet applications nowadays. In communication system data communication is not assured because of illegitimate manipulation by spy. And the solution of this complication is one and only Steganography, it conceals the data in such a manner that only sender and receiver knows about the existence of secret message. No one apart from them guess the presence of secret data. [5]

We have a general steganography model for understanding the basics of the steganography in which we have different steps for converting the data in a secret message. [6]

This model contains basically six steps which are shown below in diagram:-

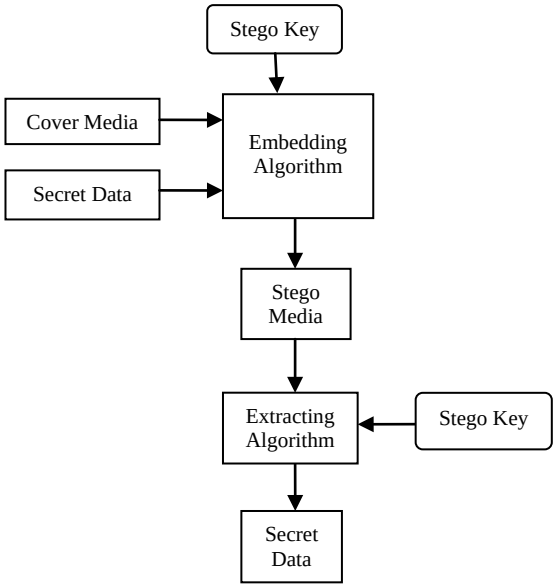

Figure 1. GENERAL STEGANOGRAPHY MODEL

- *Secret data* – The data to be concealed in the cover media.
- *Cover Media* – Concealed data is implanted in this so that the presence of data is difficult to detect.
- *Stego key* - It is the confidential key using for embedding and extracting the data.
- *Data Embedding Algorithm* - It is the process of converting the cover media into stego media with the help of stego key, secret data and cover media.
- *Stego- Media* - It is obtained after embedding the secret information.
- *Data Extracting Algorithm* - Secret process of converting the stego media to secret message with the help of stego key.
- *Steganalysis* - The presence of secret data in cover media is detecting in this process.

III. TYPES OF STEGANOGRAPHY

For the safely transmission of the sensitive data the multimedia objects are used as the cover for hiding. We can apply the data hiding techniques in different types of files according to our need.

Hiding the secret data without diminishing the quality of cover is the best technique. [7]

On the basis of the nature of the cover item steganography is divided into different types. [8] Some of the types are given below:-

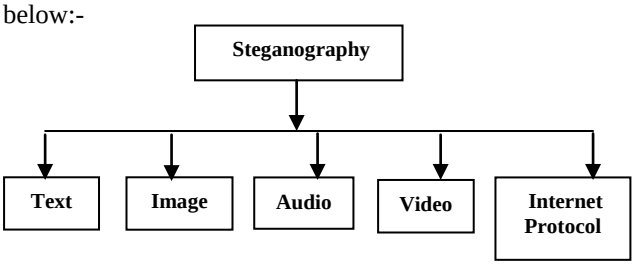

Figure 2. TYPES OF STEGANOGRAPHY

A. ***TEXT STEGANOGRAPHY***

Information to be hidden inside the text files. The secret data is hidden in text messages beyond every nth letter of every word. In the hiding process different techniques like random character sequence, changing words within text are used. [9]

There are different methods of text steganography:-

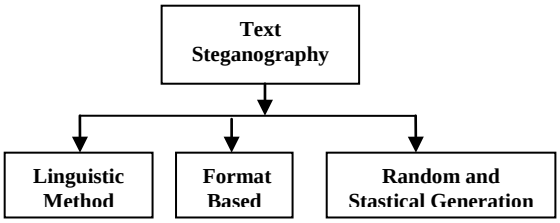

Figure 3. TYPES OF TEXT STEGANOGRAPHY

B. ***IMAGE STEGANOGRAPHY***

This technique considers "Image (colored/Gray)" as the cover-medium for the information to be hidden which in turn are stored on different pixels of the cover-image. There are three categories of image steganography as shown below:-

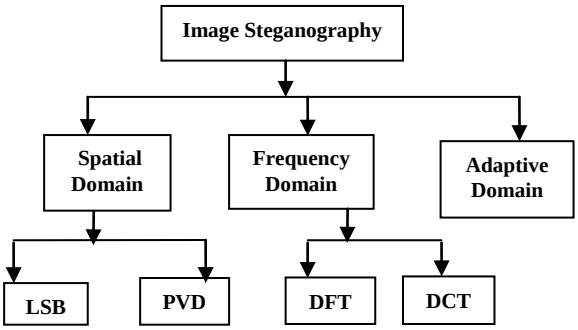

Figure 4. TYPES OF IMAGE STEGANOGRAPHY

- Spatial Domain-By the substitution of new value of secret message in the place of value of image pixel.[10]
- Frequency Domain-The hiding capacity is increased by using this method. The different transformation techniques are used in this method like DCT, DWT etc.
- Adaptive Domain- Special case of both spatial and frequency domain method is called adaptive domain and also called "Masking"

C. ***AUDIO STEGANOGRAPHY***

The data is hidden in audio file by changing the binary sequence. In audio steganography carrier (audio file), password & message are used. Carrier conceals the message and also known as cover file. [11]

This method hides the data in different types of files like MP3, WAV & AU files. Different techniques of audio steganography are:-

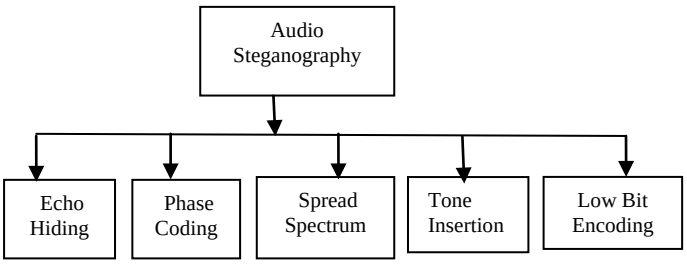

Figure 5. TYPES OF AUDIO STEGANOGRAPHY

D. ***INTERNET PROTOCOL STEGANOGRAPHY***

As the cover object network protocol like TCP, IP, ICMP or UDP etc. are used for conceal the information. Steganography can be used in OSI model in the convert channels. [12]

IV. VIDEO STEGANOGRAPHY

This is technique in which we hide data into digital video format. For hiding the information a video file which is collection of various image frames is used as the carrier.

Generally discrete cosine transform (DCT) is used because it is unrecognized by human eyes. Different types of formats like H.264, Mp4, MPEG, AVI used in video steganography.

The basic block diagram is given below:-

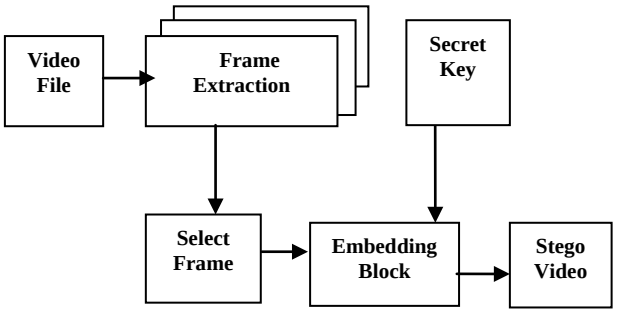

Figure 6. BASIC BLOCK DIGRAM FOR VIDEO STEGANOGRAPHY[13]

Some basic steps performed in the video steganography:-

1. Select a particular video in which we want to embed the data.
2. Split the video in small frames.
3. Select a particular frame in which we want to embed our secret data.
4. Secret key is placed with that particular frame for embedding and then stego video sent to the sender.

And the reverse of this process is performed for the EXTRACTION of the video.

By selecting a particular frame with secret key in the extracting block we can generate our video for the extraction. Different types of video steganography are: [14]

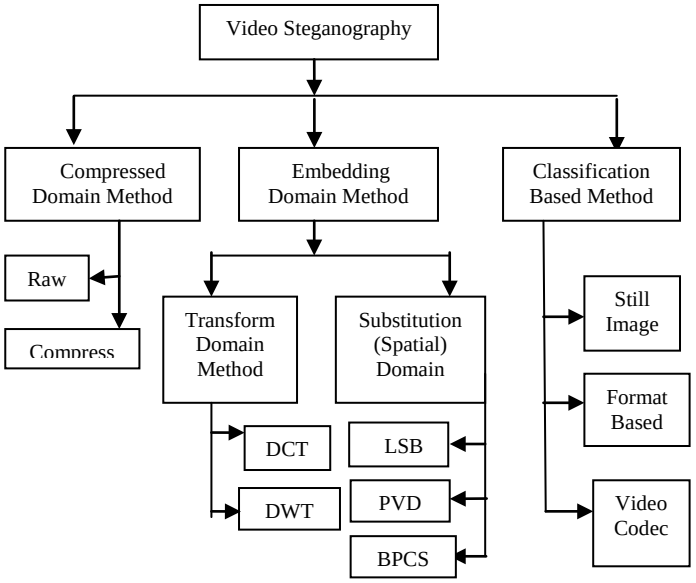

Figure 7. TYPES OF VIDEO STEGANOGRAPHY

Due to the diversity of our techniques, we can also classify our video steganography in different types: [15]

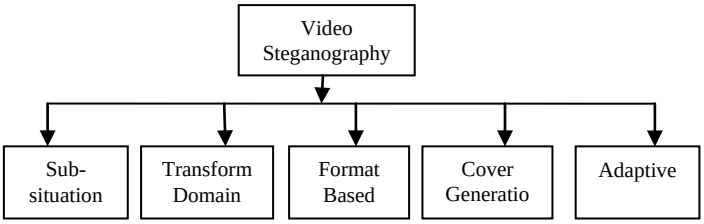

Figure 8. TYPES OF VIDEO STEGANOGRAPHY.

We have different type of techniques and their combinations used in the video steganography.

Here is the comparison of the different techniques using in video steganography:-

Table: 2 COMPARISONS OF VIDEO TECHNIQUES

SR. NO.	TECHNIQUES	AUTHOR'S	EMBEDDING TECHNIQUES	ADVANTAGES	LIMITATIONS
1.	**LSB**	Kamred Udham Singh [16]	Uses LSB of cover frame and find the position of embedding data	Simplicity and more embedding capacity	Less robust and Steganalysis is easy
2.	**DLSB**	Wafaa hasan alwan [17]	By adding 4 LSB of cover and 4 MSB of hidden frame the position of embedding data is generated	Security is high as compared to LSB	Complexity level increases
3.	**HASH BASED LSB**	Kousik Dasgupta1, J.K. Mandal and Paramartha Dutta [18]	Uses 4 LSB of cover frame and then hash function for find the position of embedding the data	Can be applied on different format files with minor changes	PSNR value is low as compared to LSB which decreases the quality
4.	**AES**	Vipula Madhukar Wajgade, Dr. Suresh Kumar [19]	For encryption AES is used and SHA-1 is used for the generation of hash key	Fast and more secure as compared to DES[20]	Complexity is high because of two layers of encryption
5.	**WATERMARKING**	Shivani Khosla, Paramjeet Kaur [21]	Use a graphical password and then convert that in binary form apply LSB and after that DCT and DWT is applied for getting watermarked video.	Security level increases because of using three combination of techniques	Encryption is more complex
6.	**BIT EXCHANGE METHOD AND INDEXING**	Pritish Bhautmage, Prof. Amuth Jeyakumar, Ashish Dahatonde [22]	Encode the confidential message by simple bit shifting and XOR operation. The message embedded in alternate bytes form, then substitute in LSB & LSB +3 bits in cover media.	Video error correction , less computational time, high secure	Because of indexing it is easy to find the secure data

7.	**NEURAL NETWORK AND GENETIC ALGORITHM**	Heena Goyal, Preeti Bansal [23]	DCT is used for quantization and segmentation and GA is used for optimization and then feed forward neural network is used.	Effective approach for hiding data by neural network and genetic algorithm so very effective to use AI	For training the network we have to take different steps which makes it more complex
8.	**HLSB AND RSA**	Manpreet kaur, amandeep kaur[24]	Conversion of private data by RSA and then put that data into the randomly selected frames by using HLSB	RSA is not easy to break that's why security is increased as compared to other techniques	If we are using not small values then it is difficult to factorized in RSA
9.	**AES AND HLSB**	Pooja Shinde Tasneem Bano Rehman[25]	HUFFMAN coding used for compression and AES algorithm used for encryption and position of hiding data is find by using HLSB	AES makes it more secure and HLSB makes it more secure for hiding the data	Slow performance and weak cipher
10.	**XOR ENCRYPTION**	Ramandeep Kaur, Pooja[26]	10 digit secret key applied first and after that frames are selected randomly and at last XOR is applied by 1LSB substitution	More secure because of 10 digits assign for authentication so always data is protected before encryption	If 10 digit code is leaked then it is easy to Steganalysis

V. APPLICATIONS OF STEGANOGRAPHY

- Used for the protection of data in Intelligence Services.
- For Scientists, Secret Formula hiding can be done by this technique.
- In military, this technique can be used for hiding sensitive data from terrorists.[27]
- In open system environment there are three most researched and accepted uses of steganography are digital watermarking, convert channels and embedded data.[28]
- Counter intelligence and Law enforcement agencies use this technique to detect and trace hidden messages.[29]

VI. CONCLUSION

Steganography is becoming the essential tool for information security for secure communication. This paper reviewed about the different steganography methods which can be applied on different cover media. Video steganography enhanced the security level as compared to images because of having complex structure. The different techniques based on video steganography with their embedding techniques having different pros and cons and the different applications of steganography discussed in the paper.

VII. REFERENCES

[1] Joshi, K. and Yadav, R.,"A New LSB-S Image Steganography Method Blend With Cryptography For Secret Communication*", In Image Information Processing (ICIIP),Third International Conference on (pp. 86-90). IEEE,* December, 2015

[2] Jasleen Kour and Deepankar Verma,"Steganography Techniques –A Review Paper", *International Journal of Emerging Research in Management &Technology*, Volume-3, Issue-5, May 2014

[3] C.P.Sumathi, T.Santanam and G. Umamaheswari,"A Study of Various Steganographic Techniques Used for Information Hiding", *International Journal of Computer Science & Engineering Survey*,Volume-4,No.-6, December 2013

[4] Bharti Chandel and Dr.Shaily Jain,"Video Steganography: A Survey", *IOSR Journal of Computer Engineering*, Volume-18, Issue-1, Jan – Feb 2016

[5] Swetha V, Prajith V and Kshema V, "Data Hiding Using Video Steganography-A Survey",*International Journal of Computer Science & Engineering Technology*,Volume-5, Issue-6, June 2015

[6] Kedar Nath Choudry, Aakash Wanjari, "A Survey Paper On Video Steganography",*International Journal of Computer Science and Information Technologies*, Volume- 6 (3) 2015

[7] Syeda Musfia Nasreen,Gaurav Jalewal and Saurabh Sutradhar, "A Study On Video Steganographic Techniques",*International Journal of Computational Engineering Research*,Volume-05, Issue-10,October 2015

[8] Ramadhan J. Mstafa & Khaled M. Elleithy,"Compressed And Raw Video Steganography Techniques:A Comprehensive Survey And Analysis", *Springer Science +Business Media New York 2016*

[9] Navneet Kaur and Sunny Behal,"A Survey On Various Types Of Steganography And Analysis Of Hiding Techniques", *International Journal of Engineering Trends and Technology*,Volume-11, No.-8, May 2014

[10] Kamaldeep Joshi, Rajkumar Yadav and Gaurav Chawla, "An Enhanced Method For Data Hiding Using 2-Bit XOR In Image Steganography",*International Journal of Engineering and Technology*,Volume-8,No-6,Dec 2016-Jan 2017

[11] Jayaram P, Ranganatha H R and Anupama H S, "Information Hiding Using Audio Steganography – A Survey",*The International Journal of Multimedia & Its Applications*,Volume-3, No-3, August 2011

[12] Athira Mohanan, Reshma Remanan, Dr. Sasidhar Babu Suvanam and Dr. Kalyankar N V,"Audio – Video Steganography Using Forensic Techniquefor Data Security",Volume-5, Issue-12, December 2014

[13] Poonam V Bodhak, Baisa L Gunjal, "Improved Protection In Video Steganography Using DCT & LSB", *International Journal of Engineering and Innovative Technology*, Volume-1, Issue-4, April 2012

[14] Abhinav Thakur, Harbinder Singh and Shikha Sharda, "Different Techniques of Image and Video Steganography: A Review*",International Journal Of Electronics And Electrical Engineering*,Volume-2,Issue-2, 2015

[15] Mennatallah M. Sadek, Amal S. Khalifa & Mostafa G. M. Mostafa,"Video Steganography: A Comprehensive Review", *Published online: 20 March 2014 # Springer Science+Business Media New York 2014*

[16] Kamred Udham Singh,"Video Steganography: Text Hiding In Video By LSB Substitution", *International Journal of Engineering Research and Applications*,Volume-4, Issue 5, May 2014

[17] Wafaa hasan alwan,"Dynamic Least Significant Bit Technique For Video Steganography", *Journal of Kerbala University*,Volume-11, No.4, 2013

[18] Kousik Dasgupta, J.K. Mandal and Paramartha Dutta, "Hash Based Least Significant Bit Technique For Video Steganography",*International Journal of Security, Privacy and Trust Management*,Volume-1,No.-2,April 2012

[19] Vipula Madhukar Wajgade and Dr. Suresh Kumar, "Enhancing Data Security Using Video Steganography", *International Journal of Emerging Technology and Advanced Engineering*,Volume-3, Issue-4, April 2013

[20] Chhaya Varade, Danish Shaikh, Girish Gund, Vishal Kumar and Shahrukh Qureshi,"A Technique For Data Hiding Using Audio And Video Steganography", *International Journal of Advanced Research in Computer Science and Software Engineering*,Volume-6,Issue-2, February 2016

[21] Shivani Khosla and Paramjeet Kaur,"Secure Data Hiding Technique Using Video Steganography and Watermarking",*International Journal of Computer Applications*,Voume-95,No.-20,June 2014

[22] Pritish Bhautmage and Prof. Amutha Jeyakumar, "Advanced Video Steganography Algorithm", *International Journal of Engineering Research and Applications*,Volume-3, Issue-1, January -February 2013

[23] Heena Goyal and Preeti Bansal,"Video Steganography Using Neural Network And Genetic Algorithm", *International Journal of Emerging Technology and Innovative Engineering*,Volume-1,Issue-9,September 2015

[24] Mandeep Kaur and Amandeep Kaur,"Improved Security Mechanism Of Text In Video Using Steganographic Technique",*International Journal of Advance Research in Computer Science and Management Studies*,Volume-2, Issue-10,October 2014

[25] Pooja Shinde and Tasneem Bano Rehman,"A Novel Video Steganography Technique",*International Journal of Advanced Research in Computer Science and Software Engineering*,Volume-5, Issue-12, December 2015

[26] Ramandeep Kaur and Pooja,"XOR Encryption Based Video Steganography",*International Journal of Science and Research* ,ISSN (Online): 2319-7064

[27] Prof. Dr. P. R. Deshmukh and Bhagyashri Rahangdale, "Data Hiding Using Video Steganography*", International Journal of Engineering Research & Technology*,Volume-3, Issue-4, April 2014

[28] Sadoon Hussein Abdullah, "Steganography Methods And Some Application (The Hidden Secret Data In Image)", *Iraq Academic Scientific Journal*, (Received 1 / 6 / 2008 , Accepted 12 / 4 / 2009)

[29] H. Motameni, M. Norouzi, M. Jahandar, and A. Hatami, "Labeling Method In Steganography*",World Academy of Science, Engineering and Technology International Journal of Computer, Electrical, Automation, Control and Information Engineering*, Voume-1, No.-6, 2007

