ISSN NO. 2320-5407

Journal homepage: http://www.journalijar.com
Journal DOI: 10.21474/IJAR01

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH

RESEARCH ARTICLE

Visteal – Videos Transmission and Encryption within an Auxiliary Video.

Pooja. S. Babu[1] and Dr. M. Prabu[2].

1. Student, National Institute of Engineering, Mysore.
2. Professor, Department of CSE, Adhiyamaan college of Engineering, Hosur.

Manuscript Info

Manuscript History:

Received: 12 May 2016
Final Accepted: 19 June 2016
Published Online: July 2016

Key words:

Corresponding Author

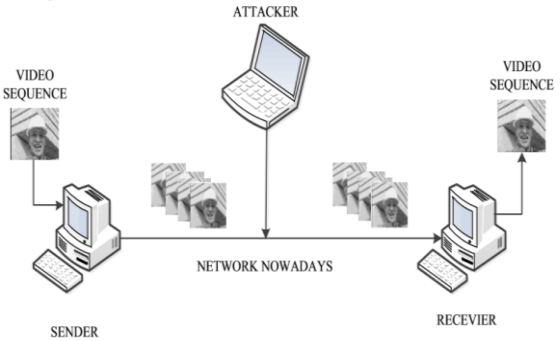
Pooja. S. Babu.

Abstract

In today's internet world the data transmission should be fast and secured. The secret signal data may get hacked by breaking the password assigns to the system. Thus it is very important designing a robust encrypted method for perfect data security. Many public places such as Banking sectors, Share markets, Educational sectors, IT industries, Government sectors and Medical sectors required secured secret data transmission. Steganography is an art of hiding the secret data or information inside the digitally covered information. The hidden message can be text, image, speech (audio) or even video and the cover can be chosen accordingly from either a text, an image, an audio or a video. If the video is seen by normal person, it is found that there is nothing but the normal video, but only the known persons can find out the decrypted message from the video.

Introduction:-

The word steganography is derived from the Greek words 'stegos' meaning cover and 'grafia' meaning writing, thus defining it as covered writing. Steganography is the art and science of secret communication. It is the practice of embedding secret information in a manner such that the existence of the information is invisible. Cryptography and Steganography are two different things. Steganography hides the existence of data from a third party, where as cryptography makes the data unreadable by a third party. Data can be hidden in audio signal, video signal or a jpeg image. Audio steganography is a technique used to transmit hidden information by modifying an audio signal in an imperceptible manner. It is the science of hiding secret text or audio information in the host message.



Transmit video sequence in high speed n/w

Today steganography algorithms based on image has made a lot of achievements. However, because of the limited capacity of the digital images, the capacity of secret information that we want to embed in the image is also restricted. Compared with digital image, video has more advantages, like large capacity, more redundancy, high communication quality, and robustness. . Video steganography is a technique to hide a secret information inside a video. The addition of this information to the video is not recognizable by the human eye as the change of the pixel

color is negligible. As a new standard, H.264 has been greatly improved over the previous standard, which is excellent in terms of compression of digital TV broadcasting, video real-time communication, network video streaming and multimedia messaging, etc. Its biggest feature is the high reliability, high compression efficiency. So the study of stenographic methods based on video for H.264/AVC has become one of the new lively issues[6].

Literature survey:-

Johannes Trithemius was a German Abbot. His writing, "Steganographia: Hoe Est Ars Per Occultam Scripturam Animi Sui Voluntatem Absentibus Aperiendi Certa" is ostensibly a work describing methods to communicate with spirits. A rough translation of the Latin title is: "Steganography: the art through which writing is hidden requiring recovery by the minds of men." Although people have hidden secrets in plain sight—now called steganography—throughout the ages, the recent growth in computational power and technology has propelled it to the forefront of today's security techniques.Many developed steganographic techniques use digital image/video-Frame as carrier. The analysis focuses on three steganographic algorithms. One of the most popular and easy to implement digital steganography technique is LSB embedding. In this method, the LSB position of each pixel in the cover image is substituted by one bit of secret data. We can improve the quality of the carried image obtained from LSB substitution method by applying optimal pixel adjustment. However, the simplicity of the LSB technique allows the embedded bits to be easily detected by applying the retrieval method of the scheme. To address such issue, an enhanced LSB method based on selecting specific bits from the host image and swapping them with secret data bits has been provided. Further study has been introduced where the security level of the LSB method was increased by embedding secret data into different LSB positions based on a secret key.BPCS algorithm embeds the secret information in bit-plane complex regions where the cover images are divided into "informative" and "noise." The first region consists of the simple pattern, whereas the second region consists of complex pattern. The BPCS algorithm provided highly efficient results in terms of hiding up to 50% of data. The PVD algorithm provides larger data hiding capacity. Data bits are embedded based on the calculated difference between a pixel value and its neighbor value and through the use of the width range table. If the difference value is slight, the assigned secret data bits are hidden into the smooth area of non-overlapping two-pixel segmented blocks. However, if the difference value is large, the determined bits are hidden into an edge area of non-overlapping two-pixel segmented blocks. The amounts of bits that will be hidden are determined by the width range table. An improved version of PVD, which combined the PVD technique with the well-known LSB substitution steganography, was proposed. The method embeds the secret data into the smooth areas of the host image using LSB replacement and into the edge areas using the PVD scheme. Steganography in computer forensics: Computer forensic technique is used to find the parameter like height and width, frame number of data, PSNR, histogram of secrete message data before and after hiding to audio-video. If all these parameters are verified and found to be correct, then only it will send to receiver otherwise it stops the secrete message data in computer forensic block. Anti-Forensics with steganography data embedding in digital images: Digital images are used to communicate visual information. Various forensic techniques have been developed to verify the authenticity of digital images. Set of digital image forensic techniques are proposed for detecting global and local contrast enhancement, identifying the use of histogram equalization, and detecting the global addition of noise to a JPEG compressed image[3]. In this project we are embedding video inside another video using LSB technique.

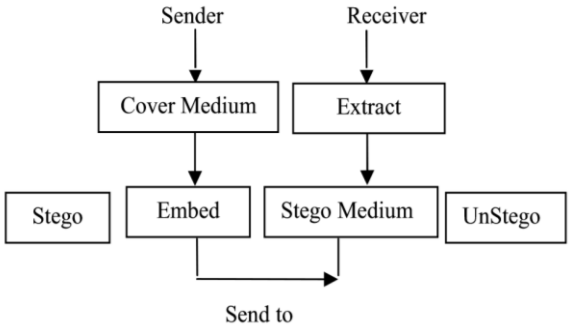
Existing System:-

The general process of Steganography is that a data message is embedded within a cover signal. The output of the embedder is called a stego signal. After transmission, recording and other signal processing which may contaminate and distort the stego signal, the embedded message is retrieved using the appropriate stego key in the block called extractor. The carrier of steganography can be an image, text, audio or a video file. Most of the steganography systems are developed in order to embed a text file, image or an audio file in a carrier file. Only a few algorithms are developed to embed a video file in a video file. This research is mainly carried out in order to embed a video in a video.The existing methods have several issues. The GOP method (group of picture), increases the size of the embedded video unusually. Thus, it is easy to detect the existence of a hidden message. The constraints of embedding in DCT domain are that many of the 64 coefficients are equal to zero and changing too many zeros to non-zero values will have an effect on the compression rate[5]. Nowadays, with the developing of network, the bandwidth has highly improved, so we can transmit video sequence as easy as a picture, it would not interest by attacker, so we can hide secret information on the cover media, it also satisfy the original intention of steganography that hide the truth that the secret information exist, so our algorithm will catch a highly security in network of protecting the information safety. When embedding secrets in spatial domain,,it is easy to detected by many

steganalysis algorithms. G. L. Hua, Z. B. Li, B. Feng. [16] proposed a video steganography algorithm based on H.264/AVC, the algorithm can be implemented to achieve embedding and extracting, but the algorithm is weak in anti-attack. X. J. Ma. The Research on Video Data Hiding Algorithms Based on H.264/AVC [D].Wuhan: Huazhong Univercity of Science and Technology, 2010 has proposed a novel algorithm based on H.264, it improves the visual quality, but the embedding efficiency and embedding capacity needs to be improved. W. W. Zhang has proposed robust video watermarking algorithm for H.264/AVC based on texture feature, it has little impact on the video quality and bit rate, but it has little capacity to embed. C. H. Liu, O. T. Chen. Data Hiding in Intra Prediction Modes of H.264/AVC [J]. IEEE Press. 2008, 3025-3028 has proposed a method based on macro-block segmentation, the bit rate increase is very low, but it is weak in the anti-steganalysis detection. Above all, the video steganography algorithms still have some problems such as the large impact of video quality, high complexity in embedding, less capacity of embedding and so on.

Proposed System:-

Generally, in data hiding, the actual information is not maintained in its original format. The format is converted into an alternative equivalent multimedia files like images, video or audio.

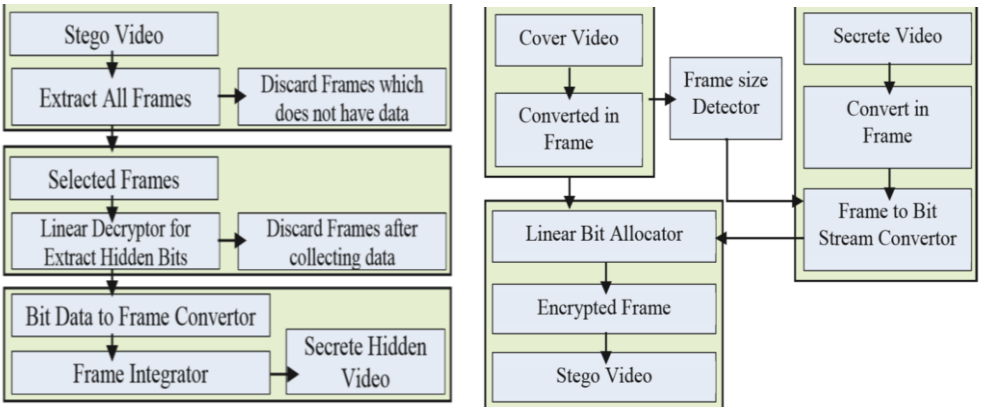


Steganography mechanism

Steganographic process: cover_medium + hidden_data + secret_key = stego_medium. The cover_medium is the file in which we will hide the hidden_data, which might be encrypted using the secret_key. Stego is the steganography process by using secret key and bit number. UnStego is the extraction process which is opposite of embedding process, here receiver should also know the secret key and bit number. The resultant file is the stego_medium. The cover_medium are typically image audio and video files. In this paper, we will focus on video file therefore, refer to the cover_image and stego_image[4]. The LSB (Least Significant Bit) is used here to hide the data. The first frame is selected as index frame and it contains the information regarding where the information is stored, in which form information is getting stored, what is file type of the information, and other information are stored in the Index Frame. If the first frame is received properly and if the receiver recognizes the information then it is very easy to get the hidden information from steganography video file. Here some predefined sequences are well known to sender and the receiver. Over this predefined location the secrete message is made hidden and this can be easily detected at the receiving end. This is something like private key technique. To hide a secret message inside an image, a proper cover image is needed. Because this method uses bits of each pixel in the image, it is necessary to use a lossless compression format, otherwise the hidden information will get lost in the transformations of a lossy compression algorithm. Decoding method is just opposite to the Encoding method.Video in another Video Technique: In video steganography, we can hide the video in another video. In Encoding method for video in another video first we will read cover file and segment that secret video streams into frames. After finding frames, find the size of cover video. Simultaneously segment video streams into frames then split the secret message bit stream into R × C group size then each group of messages are rearranged to specific pattern for hiding. Encrypt small message into a byte of data bit on LSB and check whether all small messages are completed or not. If completed then check in all frames hidden messages are included or not. If hidden messages are included then create the rule list for receiver and generate stego vidProposed framework for video in another video(encoding)

In Decoding method for video in another video first read the stego video then segment video streams into frames. As we know that video is made up with combining all frames of images. Read rule list from first frame and separate out frames which contain the hidden information. Decrypt small message from the frame for each column, row and extract LSB. Restore all extracted data bit as byte size vector. Check for rule list, is the last frame contains hidden

data or not. If the last frame contains hidden data then merge all the data to single vector and split out vector into specific size of hidden message frame. Arrange splinted vector into hidden message frame size and generate the secret video message [1][2].



Proposed framework for video in another video(decoding).

Conclusion:-

Steganography is an excellent means of conversing covertly if there are guarantees on the integrity of the channel of communication. It is not necessary for the two parties to agree to a specific hiding format. If the video is seen by normal person, it is found that there is nothing but the normal video, but only the known persons can find out the decrypted message from the video. The Different encryption format can be agreed by the two persons in such a way that no one can find the information from the video. Each technique can be implemented easily, but if someone tries to find out the tricks after knowing that someone using the stego-video file, then there are good chances of finding out the hidden information. In order to avoid this, the some hybrid system is used, in such a way that even though someone finds out the one technique, it is used only on few frames and other frames contains different kind of steganography and hence total secrete message is not delivered.

References:-

1. Steganography over Video File by Hiding Video in another Video File, Random Byte Hiding and LSB Technique Rachna Patel, Asst. Prof., Computer Engineering Department, CGPIT, Uka Tarsadia University (UTU), Maliba Campus, Bardoli, Gujarat, India. Mukesh Patel, Asst. Prof., B.V. Patel Inst. of Business Management, Computer & Information Technology, BVPBMC&IT, Uka Tarsadia University (UTU), Maliba Campus, Bardoli, Gujarat.
   2014 IEEE International Conference on Computational Intelligence and Computing Research
2. Steganography over Video File using Random Byte Hiding and LSB Technique
   Ashish T. Bhole, Rachna Patel, Department of Computer Engineering, SSBT's COE & T, Bambhori, Jalgaon, India 2012 IEEE International Conference on Computational Intelligence and Computing Research.
3. Audio-Video steganography Yugeshwari Kakde, Priyanka Gonnade, Prashant Dahiwale, Rajiv Gandhi College of Engineering & Research RTMNU Nagpur University Nagpur, India
   IEEE Sponsored 2nd International Conference on Innovations in Information Embedded and Communication Systems ICIIECS'15.
4. Video Steganography by LSB Technique using Neural Network Richa Khare, Rachana Mishra, Indrabhan Arya CSE Dept, Oriental College of Tech Bhopal, India 2014 Sixth International Conference on Computational Intelligence and Communication Networks.
5. Video Steganography A. Munasinghe, Anuja Dharmaratne, Kasun De Zoysa University of Colombo School of Computing Colombo, Sri Lanka. 2013 International Conference on Advances in ICT for Emerging Regions (ICTer)
6. Video Steganography Algorithm Based on Trailing Coefficients Yingnan Zhang, Minqing Zhang ,Ke Niu, Jia Liu Key Laboratory of Network&Information Security of PAPF, Engineering University of the PAPF Xi'an, China. 2015 International Conference on Intelligent Networking and Collaborative System.
7. Video Steganography using Flash Video (FLV)

A.J. Mozo, M.E. Obien, C.J. Rigor, D.F. Rayel, K. Chua, G. Tangonan Electronics, Communications and Computer Engineering Department Ateneo de Manila University Quezon City, Philippines I2MTC 2009 - International Instrumentation and Measurement Technology Conference Singapore, 5-7 May 2009.

8. The cover_medium are typically image audio and video files. In this paper, we will focus on video file therefore, refer to the cover_image and stego_image. The Third International Conference on Availability, Reliability and Security IEEE 2008.
9. STEGANOGRAPHY ALGORITHM BASED ON DISCRETE COSINE TRANSFORM FOR DATA EMBEDDING INTO RAW VIDEO STREAMS, Rajesh G.R and A. Shajin Nargunam, Research Scholar, Noorul Islam University, Thuckalay, TN
   Chennai Fourth International Conference on Sustainable Energy and Intelligent System 2013
10. A Novel Video Steganography based on Non-uniform Rectangular Partition ShengDun Hu, KinTak U Faculty of Information Technology Macau University of Science and Technology Macau, China. IEEE International Conference on Computational Science and Engineering-2011
11. Bit-Plane Decomposition Steganography Using Wavelet Compressed Video Tomonori Furuta Hideki Noda, Michiham Niimi, Eji Kawaguchi Kyushu Institute of Technology, Dept. of Electrical, Electronic and Computer Engineering, Sensui-cho, Tobata-ku, Kitakyushu, Japan.
    1cIcs-m2003 15-18 DeCemkrZM), Singapore A Novel Video Steganography Algorithm in the Wavelet Domain Based on the KLT Tracking Algorithm and BCH Codes Ramadhan J. Mstafa, IEEE Student Member,
    Khaled M. Elleithy, IEEE senior member, Department of Computer Science and Engineering University of Bridgeport Bridgeport, CT 06604, USA. 2015 IEEE.
12. Comparative Analysis of Steganographic Algorithms Within Compressed Video Domain. Tarik Faraj Idbeaa, Salina Abdul Samad, Hafizah Husain Department of Electrical, Electronics and Systems Engineering Universiti Kebangsaan Malaysia. 2014 IEEE
13. Android Mobile Forensic Analyzer for Stegno data Walter. T. Mambodza, NagoorMeeran A.R Department of Information Technology SRM University Chennai, India 2015 International Conference on Circuit, Power and Computing Technologies [ICCPCT]
14. A Review on Steganography and Cryptography Rina Mishra, Praveen Bhanodiya Department of Computer Science & Engineering Patel College of Science & Technology Indore,India 2015 International Conference on Advances in Computer Engineering and Applications (ICACEA) IMS Engineering College, Ghaziabad, India.
16. G. L. Hua, Z. B. Li, B. Feng. [1]Low frequency steganography algorithm for H.264/AVC [J]. Journal on Communications, 2013, 34(Z2), 47-50.