International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 6 Issue: 3 258 - 261

Audio-Video Security using Steganography and Cryptography

Pranali Bhitre, Prof. M. R. Sayankar
Department of Computer Science and Engineering
BDCE Wardha

Abstract- Security is most essential issue in advanced correspondence. Information security implies defensive computerized security measures that are connected to forestall unapproved access to PCs, immense databases and online information it is likewise shields information from defilement. Security is most vital issue in computerized correspondence. Cryptography and steganography are two prominent techniques accessible to give security. Steganography centers around concealing data such that the message is imperceptible for pariahs and just appears to the sender and expected beneficiary. It is valuable instrument that permits secret transmission of data again and again interchanges channel. Steganography is a method which is utilized to conceal the message and keep the identification of shrouded message. Different present day methods of steganography are: a) Video Steganography b) Audio Steganography

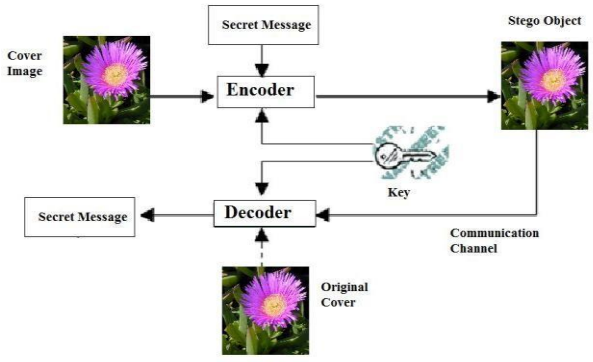
Audio Video steganography is a cutting edge steganography of concealing data in a way that the undesirable individuals may not get to the data.

Keywords—*Steganography, Audio Steganography, Video Steganography*

*****

I. Introduction

Steganography centers around concealing data such that the message is imperceptible for untouchables and just appears to the sender and proposed beneficiary. It is valuable instrument that permits clandestine transmission of data again and again interchanges channel. Steganography is a method which is utilized to shroud the message and keep the recognition of concealed message. Audio Video steganography is a cutting edge method for concealing data in a way that the undesirable individuals may not get to the data. The propose strategy is to shroud mystery data and picture behind the audio and video record individually.



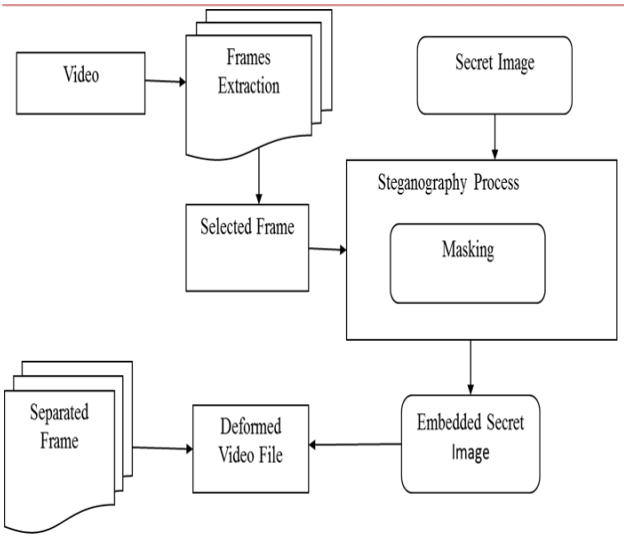
Audio Steganography

The fundamental model of Audio steganography comprises of Carrier (Audio document), Message and Password. Bearer is otherwise called a cover-record, which covers the mystery data. Encoding mystery messages in audio is the most difficult method in light of the fact that the human sound-related framework (HAS) has such a dynamic range, to the point that it can tune in finished. Audio records are generally packed for capacity or quicker transmission. Audio documents can be sent in short remain solitary fragments. There are different composes and procedure of information stowing away in audio like Least Significant Bit Encoding and Phase coding. Implanting mystery messages in audio document is more troublesome than inserting messages in computerized picture.

II. Video Steganography

Video is an electronic medium for the recording, copying and broadcasting of moving visual images. Video

Steganography is a technique to hide any kind of files into a carrying Video file. The use of the video based Steganography can be more eligible than other multimedia files, because of its size and memory requirements. Videos are the set of images. The number of still pictures per unit of time of video ranges from six to eight frames per second.In video steganography data hides behind the video using different techniques. Basically there are three embedding techniques for images in practice, namely Least Significant Bit (LSB), Transform based and Masking and filtering. The best technique is that to hide secret message without affecting the quality of video, structure and content of video. After hiding a secret data in video create “stego “ video file which is send to the receiver.



III. Literature Survey

Arup Kumar Bhaumik, Minkyu Choi et.al, [1] there are three principle necessities of any information concealing framework i.e. security, limit and heartiness. Every one of these variables are conversely relative to each other and along these lines, it is exceptionally hard to accomplish them together. Here, the creators have concentrated on expanding the two components, security and limit of information concealing technique. This information concealing plan utilizes a high determination computerized video as a cover flag that implies a video is implanted behind a video and they have likewise utilized a picture for confirmation. Therefore, they have utilized vast payloads like video in video and a picture in video as a cover media. The target of stowing away such information relies upon the application and the necessities of the client of that computerized media.

Sunil K. Moon, Rajshree D. Raut, [3] in this work creator has expected to shroud mystery data behind picture and audio of video document. By installing content behind audio record and a verification picture is implanted behind casings of video document. As video is the utilization of numerous still casings of audio and picture (i.e. picture), any casing can be chosen from video and signs from the audio for concealing mystery information. Creators have utilized 4LSB strategy for picture steganography though Phase Coding calculation for audio steganography. They have attempted to expand the security of information by utilizing reasonable parameter of security and verifications, for example, PSNR and histogram that can be acquire at transmitter and collector side

Burate D. J., M. R. Dixit, [4] utilized another method for concealing content in discourse in commotion free condition. They have worked in the computerized space to conceal the content data inside discourse flag utilizing audio steganography procedure. Information concealing rate can be expanded because of this technique. They have kept up the inventiveness of the discourse transporter motions by implanting the mystery message as opposed to performing substitution task on it. They have consolidated steganography with cryptography to expand security of the framework, however as opposed to utilizing any of the cryptography procedure, they have utilized coding strategies in this technique. Because of this approach the strength of the cover flag is kept up and a higher concealing limit with respect to various audio and discourse flag inspected at various frequencies is accomplished and additionally perused at various piece rates. So this strategy gives higher concealing limit when contrasted with different systems.

IV. Proposed System

Working of Sender side

We are combining cryptography and steganography for hiding data behind audio and image behind video in audio-video file. For hiding image behind video we used LSB replacement technique and for hiding data behind the audio used Parity coding algorithm. Data is encrypted for more security purpose.

Sender selects any one audio-video file. This audio-video file separate using in build software. Now sender will select a secret image which will be transmitted to the receiver. In next step select the video file. Video is nothing but a collection of multiple frames. The number of still pictures per unit of time of video ranges from six to eight frames per second. The algorithm of video stegnography is based on the fact that each pixel represented by 3 bytes where each byte representing the intensity of 3 primary colors that is RGB Red, Green and Blue) Size of image file is directly related to number of pixels and granularity of color definition. Sender selects the more than one frame and using LSB algorithm embedded the secret image into the frame. The part of LSB of secret image embedded in one frame and MSB in another frame. The selection of frames is depend on the user or sender. He can be selecting each time new frames.

The system asked for passkey for the user. The user entered the passkey to the system in a number. This passkey number internal selects the frame number . Suppose selected frame no 15 of video then next selected frame is selected automatically.

Now the part of LSB of secret image hide in first frame and MSB part of image hide in next frame.
For hiding secret message behind audio select the audio file and select the secret message. This message first encrypted and then apply the parity algorithm to it. The message will be hide according to odd or even parity.

V. Working of Receiver side

The receiver will now perform extraction of key and image from the output video received by the transmitter. The receiver gives the output video as input to the system. The system separates the stego audio-video file (i.e. the received video) into stego audio signals and stego frames using matlab function "vision.VideoFileReader ()".. Then the embedded image is being extracted from the audio signals and the key is being extracted from the video frame. This extracted key is then matched with the 16 byte key. If the keys are matched then the key is provided to the extracted encrypted image, for its decryption and thus, the secret image is finally received by the receiver. And if the keys do not match the system get to know that the user is an unauthenticated user and thus, it displays a "Keys do not match" message and stops the system. Thus if any unauthorized user tries to extract the secret image from the stego audio-video file, the system will decline the process and will not show the embedded image to the user in any condition. Thus, a secret image is securely transmitted from one user to another by informing the username and password to receiver end privately. Pixels and granularity of color definition. Sender selects the more than one frame and using LSB algorithm embedded the secret image into the frame. The part of LSB of secret image embedded in one frame and MSB in another frame. The selection of frames is depending on the user or sender. He can be selecting each time new frames.

VI. Conclusion

Securing the secret data by embedding it in audio-video file with an appropriate steganographic technique provides high security. We are hiding an encrypted secret image behind audio signals of the audio-video file and the encryption key behind a video frame using LSB (Least Significant Bit) replacement technique. Satisfactory results are obtained in both audio and video steganography. The use of LSB substitution technique for steganography and encryption has made it possible to maintain the integrity of the secret image. Here, a robust method of imperceptible data hiding is introduced. The system provides a good and efficient method for hiding the data from hackers and sent to the destination in a safe manner. This method do not compromise with the quality of the data sent, exact image is recovered at the receiver side. Thus we conclude that audiovideo data hiding techniques can be used for a number of purposes other than covert communication or deniable data storage, information tracing and finger printing, tamper detection. As the sky is not limit so is not for the development. Man is now pushing away its own boundaries to make every thought possible. So similarly these operations described above can be further modified as it is in the world of Information Technology. **References**

[1] A. K. Bhaumik, Minkyu Choi, Rosslin R. Robles, Maricel O. Balitanas "Data Hiding In Video" from International Journal of Database Theory and Application Vol.2-2 June 2009.

[2] Prof. D. P. Gaikwad, Trupti Jagdale, Swati Dhanokar, Abhijeet Moghe, Akash Pathak "Hiding the Text and Image Message of Variable Size Using Encryption and Compression Algorithms in Video steganography", International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 Vol. 1, Issue 2, pp.102-108

[3] Sunil k. Moon, Rajshree D. Raut, "Application of data hiding in Audio-Video using anti forensics techniques for authentication and data security", Advanced Computing Conference (IACC) 2014IEEE International.

[4] Burate D. J., M. R. Dixit "Performance Improving LSB Audio Steganography Technique" Volume 1, Issue 4, September 2013 International Journal of Advance Research in Computer Science and Management Studies.

[5] Padmashree G., Venugopala P. S., "Audio Steganography and Cryptography: Using LSB algorithm at 4th and 5th LSB layers", ISSN: 2277-3754 ISO 9001:2008 Certified International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 4, October 2012 [6] K.A. Navas, Vidya V., Sonia V. Dass, "High security data embedding in video", Recent Advances in Intelligent Computational Systems (RAICS), 2011 IEEE

[7] Praveen. P, Arun. R, "Audio-video Crypto Steganography using LSB substitution and advanced chaotic algorithm", International Journal of Engineering Inventions e-ISSN: 2278-7461, p-ISSN: 2319-6491 Volume 4, Issue 2 (August 2014) PP: 01-07

[8] Lovey Rana, Saikat Banerjee, "Dual Layer Randomization in Audio Steganography Using Random Byte Position Encoding" , International Journal of Engineering and Innovative Technology, Volume 2, Issue 8, February 2013

[9] Muhammad Asad, Junaid Gilani, Adnan Khalid, "Three Layered Model for Audio Steganography", 2012 International Conference on Emerging Technologies (ICET)

[10] Kamalpreet Kaur, DeepankarVerma, "Multi-Level Steganographic Algorithm for Audio Steganography using LSB, Parity Coding and Phase Coding Technique", IJARCSSE, Volume 4, Issue 1, January 2014

[11] S.S. Divya, M. Ram Mohan Reddy, "Hiding Text In Audio Using Multiple LSB Steganography And Provide Security Using Cryptography", International Journal of Scientific &Technology Research, Vol. 1, pp. 68-70, July 2012.

[12] Kirti Gandhi, Gaurav Garg, "Modified LSB Audio Steganography Approach", International Journal of Emerging Technology and Advanced Engineering, Volume 3, Issue 6, June 2012, pp 158-161

[13] Ahmed Ch. Shakir, "Stegno Encrypted Message in Any Language for Network Communication Using Quadratic

Method", Journal of Computer Science 6 (3): 320-322, 2010 ISSN 1549-3636 © 2010 Science Publications.

[14] Andreas Westfeld and Gritta Wolf, "Steganography in a Video Conferencing System", Information Hiding 1998, LNCS 1525, pp. 32-47, 1998. Springer-Verlag Berlin Heidelberg 1998.

[15] S. Suma Christal Mary, "Improved Protection in Video Steganopgraphy Used Compressed Video Bitstream", International Journal on Computer Science and Engineering Vol. 02, No. 03, 2010, 764-766, ISSN: 09753397