Improved Security of data using Cryptography and Audio-Video Steganography

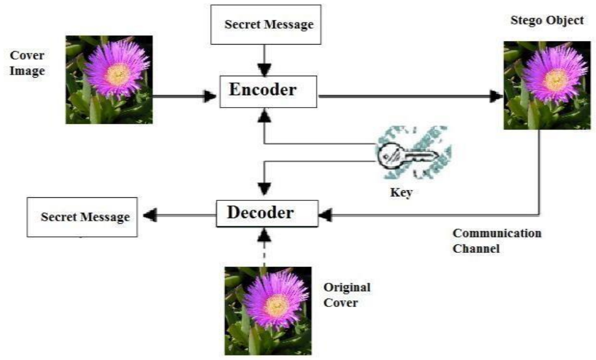
Monika Yadav, Mr. Sarjender Yadav
Department of Computer Science and Engineering, Rao Pahlad Singh Group of Institutions, Balana, Mohindergarh

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.

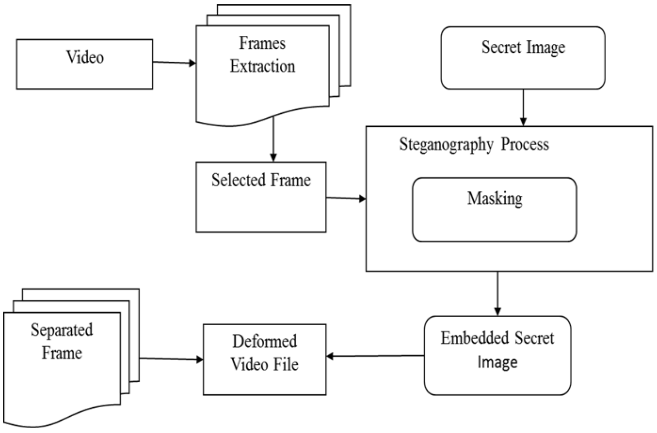


Audio Steganography

The basic model of Audio steganography includes Carrier (Audio archive), Message and Password. Carrier is generally called a cover-record, which covers the puzzle information. Encoding puzzle messages in audio is the most troublesome strategy in light of the way that the human sound-related system (HAS) has such a dynamic range, to the point that it can tune in wrapped up. Audio records are by and large pressed for limit or snappier transmission. Audio reports can be sent in short stay singular sections. There are diverse makes and technique out of data stowing endlessly in audio like Least Significant Bit Encoding and Phase coding. Embedding riddle messages in audio archive is more troublesome than embeddings messages in electronic picture.

II. VIDEO STEGANOGRAPHY

Video is an electronic medium for the chronicle, replicating and broadcasting of moving visual pictures. Video Steganography is a method to conceal any sort of documents into a conveying Video record. The utilization of the video based Steganography can be more qualified than other sight and sound documents, as a result of its size and memory prerequisites. Recordings are the arrangement of pictures. The quantity of still pictures per unit of time of video ranges from six to eight edges for each second.In video steganography information holes up behind the video utilizing distinctive methods. Fundamentally there are three implanting methods for pictures by and by, to be specific Least Significant Bit (LSB), Transform based and Masking and sifting. The best procedure is that to shroud mystery message without influencing the nature of video, structure and substance of video. In the wake of concealing a mystery information in video make "stego " video record which is send to the collector..



III. LITERATURE SURVEY

Arup Kumar Bhaumik, Minkyu Choi et.al, [1] there are three standard necessities of any data covering system i.e. security, point of confinement and healthiness. Each one of these factors are on the other hand in respect to each other and thusly, it is particularly difficult to achieve them together. Here, the makers have focused on growing the two parts, security and utmost of data covering system. This data hiding design uses a high assurance modernized video as a cover signal that infers a video is embedded behind a video and they have in like manner used a photo for affirmation. In this manner, they have used huge payloads like video in video and a photo in video as a cover media. The objective of stowing without end such data depends upon the application and the necessities of the customer of that electronic media.

Sunil K. Moon, Rajshree D. Raut, [3] in this work maker has anticipated that would cover riddle information behind picture and audio of video archive. By introducing content behind audio record and a confirmation picture is embedded behind housings of video report. As video is the use of various still housings of audio and picture (i.e. picture), any packaging can be browsed video and signs from the audio for hiding secret data. Makers have used 4LSB system for picture steganography however Phase Coding count for audio steganography. They have endeavored to extend the security of data by using sensible parameter of security and confirmations, for instance, PSNR and histogram that can be obtain at transmitter and authority side

Burate D. J., M. R. Dixit, [4] used another technique for disguising content in talk in disturbance free condition. They have worked in the modernized space to disguise the substance information inside talk hail using audio steganography technique. Data covering rate can be extended in light of this strategy. They have kept up the imaginativeness of the talk transporter movements by embedding the secret message instead of performing substitution assignment on it. They have united steganography with cryptography to grow security of the system, anyway rather than using any of the cryptography method, they have used coding procedures in this strategy. In light of this approach the quality of the cover hail is kept up and a higher disguising limit regarding different audio and talk signal assessed at different frequencies is proficient and also examined at different piece rates. So this methodology gives higher hiding limit when diverged from various frameworks.

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.

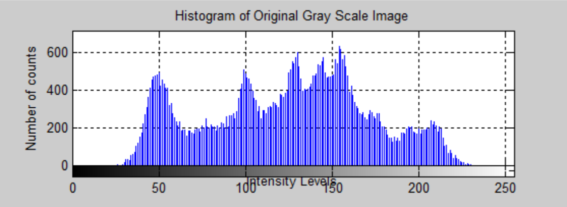
V. WORKING OF RECEIVER SIDE

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. RESULT ANALYSIS

In the proposed method image hiding behind the video and text behind the audio and after embedding secret image and data we merge the stego audio and sego video file. The proposed method improve the embedding capability of audio and video also increase the quality of cover media after hiding the secret data as well as decrease the distortion rate of cover file.

Histogram of original gray image from video



Histogram of Recovered Gray Scale image from video

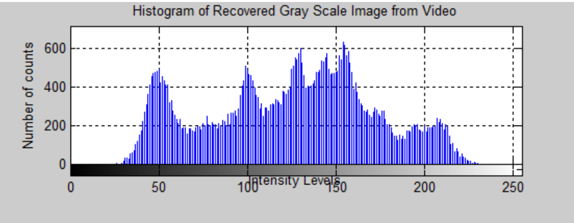


Figure: Histogram for original gray image and extracted gray Image

Audio Amplitude before and after hiding data

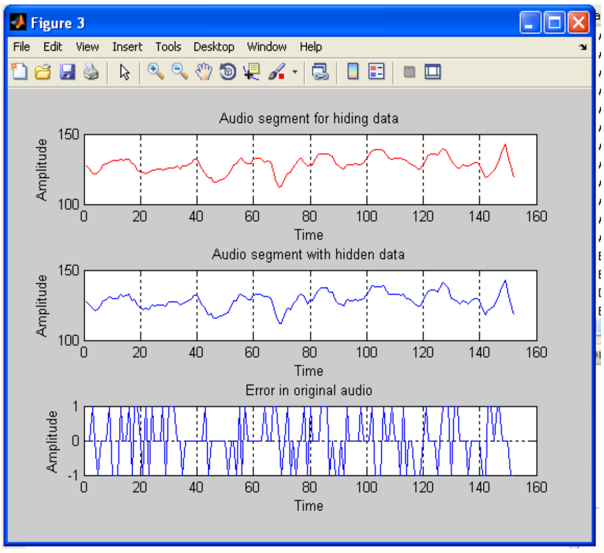
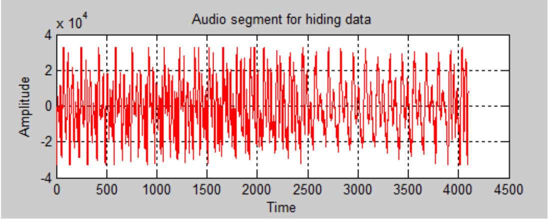
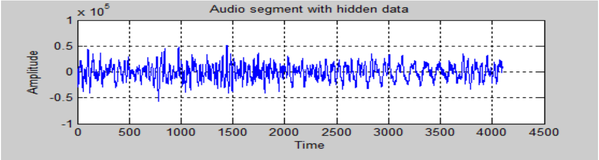


Figure: Audio Amplitude before and after hiding data



Audio segment after hiding data by using existing system



Audio segment after hiding data by proposed system

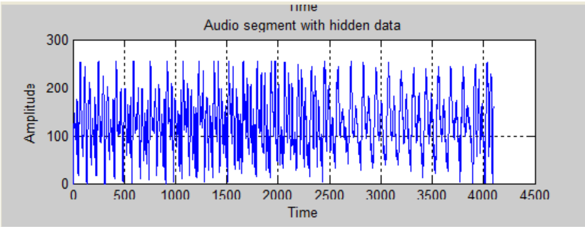


Figure: Audio Steganography graph

VII. 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.

VIII. REFERENCES

[1]. 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, Deepankar Verma, "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