International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

Secure Secret Information Transmission with Audio-Video Steganography Using Encryption and Data Authentication

Mandeep Singh[1], Garima Mahajan[2]

[1]Research Scholar in Computer Science Department, Baba Farid College of Engineering and Technology, Bathinda

[2]Assistant Professor in Computer Science Department, Baba Farid College of Engineering and Technology, Bathinda

Abstract: ***Video steganography is an emerging field of research in recent years. In the recent years due to advancements in transmission channel huge amount of data can be transmitted using channel bandwidth. Huge amount can be transmitted over the channel using video steganography in secure manner because due to availability of number of frames in a file data can be embedded secretly behind any frame. Various approaches had been used for embedding of secret information behind the cover object behind cover object in video steganography. LSB, random pixel selection, frequency division, time domain division and RGBGBR approaches had been used for hiding of secret information. In this paper secure steganography has been done using MLSB and phase coding approach for data embedding behind video and audio signals. This approach provides better steganography than other approaches.***

Keywords: Steganography, Video Steganography, LSB, MLSB,AES and phase coding

1. Introduction

1.1 Stegnography

Steganography is the art and science of invisible communication. This is accomplished through hiding information in other information, thus hiding the existence of the communicated information. The word steganography is derived from the Greek words "*stegos*" meaning "cover" and "*grafia*" meaning "writing defining it as "covered writing". In image steganography the information is hidden exclusively in images. The idea and practice of hiding information has a long history. In *Histories* the Greek historian Herodotus writes of a nobleman, Histaeus, who needed to communicate with his son-in-law in Greece. He shaved the head of one of his most trusted slaves and tattooed the message onto the slave's scalp. When the slave's hair grew back the slave was dispatched with the hidden message.

Figure 1.1: Stenography

Steganography differs from cryptography in the sense that where cryptography focuses on keeping the contents of a message secret, steganography focuses on keeping the existence of a message secret. Steganography and cryptography are both ways to protect information from unwanted parties but neither technology alone is perfect and can be compromised. Once the presence of hidden information is revealed or even suspected, the purpose of steganography is partly defeated. The strength of steganography can thus be amplified by combining it with cryptography.

1.2 Different kind of Stenography

1.2.1 Text stenography

Hiding data in content is the most vital strategy for steganography. The method was to hide a mystery message in every nth letter of each expression of an instant message. In the wake of blasting of Internet and diverse kind of advanced document groups it has diminished in importance. Content stenography utilizing computerized records is not utilized frequently in light of the fact that the content documents have a little measure of repetitive information.

1.2.2 Audio stenography

Audio stenography is veiling, which misuses the properties of the human ear to shroud data unnoticeably. A perceptible, sound can be imperceptible in the vicinity of an alternate louder audible sound. This property permits to choose the divert in which to shroud data.

1.2.3 Image stenography

Pictures are utilized as the prominent spread items for steganography. A message is implanted in a computerized picture through an implanting calculation, utilizing the mystery key. The resulting stego picture is send to the receiver. On the other side, it is handled by the extraction calculation utilizing the same key. During the transmission of steno picture unauthenticated persons can just recognize the transmission of a picture however can't figure the presence of the concealed message.

1.2.4 Protocol steganography

The term protocol steganography is to embedding information within network protocols such as TCP/IP. We

hide information in the header of a TCP/IP packet in some fields that can be either optional or are never used.

1.2.5 Video Steganography

Video Steganography is a method to conceal any sort of records into convey Video document. The utilization of the feature based Steganography can be more qualified than other interactive media documents, on account of its size and memory prerequisites. The least significant bit (LSB) insertion is an essential methodology for implanting data in a transporter record. Least significant bit (LSB) insertion system works on LSB bit of the media document to conceal the data bit. In this extend, an information concealing plan will be produced to conceal the data in particular casings of the feature and in particular area of the edge by LSB substitution utilizing polynomial mathematical statement. Video Steganography is a system to hide any sort of records in any extension into a carrying Video file. This venture is the application created to insert any sort of data (File) in an alternate document, which is called transporter record. The bearer document must be a feature record. It is concerned with inserting data in a harmless spread media in a protected and powerful way. This framework makes the Files more secure by utilizing the ideas Steganography and Cryptography.

1.3 Applications of Steganography

- Steganography can be a solution which makes it possible to send news and information without being censored and without the fear of the messages being intercepted and traced back to us.
- It is also possible to simply use steganography to store information on a location. For example, several information sources like our private banking information, some military secrets, can be stored in a cover source. When we are required to unhide the secret information in our cover source, we can easily reveal our banking data and it will be impossible to prove the existence of the military secrets inside [8].
- Steganography can also be used to implement watermarking. Although the concept of watermarking is not necessarily steganography, there are several steganography techniques that are being used to store watermarks in data. The main difference is on intent, while the purpose of steganography is hiding information, watermarking is merely extending the cover source with extra information. Since people will not accept noticeable changes in images, audio or video files because of a watermark, Steganography methods can be used to hide this.
- E-commerce allows for an interesting use of steganography. In current e-commerce transactions, most users are protected by a username and password, with no real method of verifying that the user is the actual card holder. Biometric finger print scanning, combined with unique session IDs embedded into the fingerprint images via steganography, allow for a very secure option to open ecommerce transaction verification.
- Paired with existing communication methods, steganography can be used to carry out hidden exchanges. Governments are interested in two types of hidden communications: those that support national security and those that do not. Digital steganography provides vast potential for both types. Businesses may have similar concerns Regarding trade secrets or new product information.
- The transportation of sensitive data is another key use of steganography. A potential problem with cryptography is that eavesdroppers know they have an encrypted message when they see one. Steganography allows to transport of sensitive data past eavesdroppers without them knowing any sensitive data has passed them. The idea of using steganography in data transportation can be applied to just about any data transportation method, from E-Mail to images on Internet websites [9].

1.4 Algorithm Used

- **Least significant bit**

LSB can also stand for least significant byte. The meaning is parallel to the above: it is the byte in that position of a multi-byte number which has the least potential value. If the abbreviation's meaning least significant byte isn't obvious from context, it should be stated explicitly to avoid confusion with least significant bit.To avoid this ambiguity, the less abbreviated terms “lsbit” or “lsbyte” are often used. In computing, the least significant bit (LSB) is the bit position in a binary integer giving the units value, that is, determining whether the number is even or odd. The LSB is sometimes referred to as the right-most bit, due to the convention in positional notation of writing less significant digit further to the right. It is analogous to the least significant digit of a decimal integer, which is the digit in the ones (right-most) position.

- **Most significant bit**

In computing, the most significant bit (MSB, also called the high-order bit) is the bit position in a binary number having the greatest value. The MSB is sometimes referred to as the left-most bit due to the convention in positional notation of writing more significant digits further to the left. The MSB can also correspond to the sign bit of a signed binary number in one's or two's complement notation, "1" meaning negative and "0" meaning positive. It is common to assign each bit a position number, ranging from zero to N-1, where N is the number of bits in the binary representation used. Normally, this is simply the exponent for the corresponding bit weight in base-2.

2. Review of Literature

Islam M.R. et al [1] “An efficient filtering based approach improving LSB image steganography using status bit along with AES cryptography” in this paper author was purposed an approach that is used for hiding the text behind the cover image using the AES encryption scheme. In this approach the two processes have been undergoes. These processes have been used for converting secret message into cipher text. The AES approach uses a password that convert the plain text into cipher text using 128 bit encryption.

Yi-Chun Liao et al [2] “Data hiding in video using adaptive LSB”, in this paper author purposes an adaptive LSB

approach for embedding of secret information behind the cover object. In this approach the region has to be extracted behind that the data have to be embedded. This region that has been extracted dividends different 3 dimensional matrixes that are used for hiding the secret information. The color clustering approach was used for extraction of the region in which data has to embed. By using this approach different data is extracted and the least significant bits have been used for hiding secret information. Then after embedding the region is pasted into the file and transmitted to the user. The issue in this approach that it is much complex approach because a minor change in the region that has been extracted can affect the secret information.

PoojaYadav et al [3] "A Secure Video Steganography with Encryption Based on LSB Technique" in this paper author was purposed an approach that has been used for secure transmission of secret data using video files. In this approach the data has been hidden behind the frames of the video file and embedded using XOR operation. In this approach the video file have been divided into different frames and on the basis of these frames least significant bits have to be computes. Least significant bits available in each frame pixel have been extracted by using binary conversion of pixel value. This approach provides better steganography of secret information. But the major issues in this approach that if any attacker performs staganalysis attack that can easily extract the data behind the least significant bits of cover object. So this approach does not provide secure transmission of secret data. Data can be secured using encryption scheme on the secret data.

MstafaR.J. et al [4] "A highly secure video steganography using Hamming code" Because of the rapid of web and advances in innovation, individuals are getting to be more agonized over data being hacked by aggressors. As of late, numerous calculations of steganography and information stowing away have been proposed. Steganography is a procedure of installing the mystery data inside the host medium (content, sound, picture and feature). Simultaneously, a large portion of the intense stenographic examination programming projects have been given to unapproved clients to recover the significant mystery data that was inserted in the bearer documents. Some steganography calculations can be effectively recognized by steganalytical locators in view of the absence of security and installing productivity.

AbhinavThakur ET. al. [5], "Secure Video Steganography based on Discrete WaveletTransform and Arnold Transform", in this paper author purposed an approach for data hiding in video files using discrete wavelet transformation for data embedding. By changing the nature of the internet huge amount of data can be transmitted to different location easily, but security and integrity is the major concern for data transmitting. In this paper cover video has been divided into frames for embedding of secret information behind the cover objects frames. After this process DWT has been used to decompose the frame into different parts that are LL, LH, HL and HH. Key has been used for encoding and decoding process of the data hiding for security aspects.

3. Proposed Work

Steagnograhy is aprocess that haa been used for hidding infromation behind cover signal for secure transmission of secret informatioon. In this paper audio video steagnography has been discussed for data preservation behind an audio and video signals using secure steagnographic approach. In the process of audio video steagnography data has been hidded behind both audio and video signals of a video file. These cover signals from a single video file has been extracted using "EASY AUDIO VIDEO SEPRATOR". This seprator has been used for extraction of audio signal from video file in wav format.

After extarction of audio and video signal data has been embedded behind both signal using secure steagnogrhy approaches.

- **Audio Steagnography**

In the purposed work audio signal ahs been used for hiding secret text information behind cover signal. In the purposed work secret text that have to embeded behind audio signal has been encypted using AES encryption approach. In this process audio signal has been used for embedding of encrypted text using phase coding approach.

a. Read audio wav format signal using wavread function.
b. Load secret text that and store in a varibale.
c. Encrypt secerte text using AES encryption scheme. Encryption approach convert secret text into cipher text.
d. Read header of the audio file and store it in a header1 variable. Header store values of audio signal length, bits.
e. Read next 16 bit samples fom audio and use this samples for embedding of secret information.
f. Convert cipher text into vector format and manipulate this vector to binary values and use one bit for embedding in audio wav signal phase using phase coding approach.
g. If embedding information contain bit 0 new phase has been developed by adding $\pi/2$ to old phase of audio signal.
h. For bit 1 $\pi/2$ has been subtracted from old phase of audio signal.
i. Repeat step g, h until whole message has been embeeded behind audio signal.
j. Add header to audio signal and write stego audio signal using audio writer fuction.

After embeddig of secret information new generated audio signal can be used for transmitting information to reciever side using tranmsisison channel.

- **Video Steganography**

In the process of video steganography data has been embedded behind frames of video cover object. In these process frames of the video file has been extracted using "MOV" function. After extraction of frames from video file these frames have been used for embedding of secret information. In the purposed work video file has been added to a variable and the frames of the video file have been used for embedding of secret information.

Secret image has been used for embedding behind frames of the cover video so that data can be easily transmitted to

receiver without acknowledgment to any attacker. In the purposed work secret information has been encrypted using bit shifting approach. This approach mixes the pixels values by using different intervals so that original content cannot be seen through naked eyes. After this information has been embedded behind different frames of cover video using multiple least significant bits.

a. Read video file using video reader function and store video into a variable v1.
b. Extract frames of the video using read function and store these frames in the array MOV.
c. Load secret image that have to be embedded behind cover frames of video file.
d. Convert secret image into RGB color format for embedding behind different frames of video file.
e. Apply encryption approach on each color subspace to convert originality of image.
f. Convert image pixel value into binary values and embedded behind multiple least significant bits of the cover video object.
g. Select a user defined frame number for authentication process to validation user validation at receiver end. Embed user defined frame number behind least significant bits of first frame pixel.
h. Set secret information binary bit with cover frame least significant bit using bit set operation.
i. Embed all the color sub space behind frames of video file and replace stego frames object with original frames of video.
j. Write stego video using video writer function.

In the purposed work audio and video data has been embedded behind cover frames of video file. In this process of steganography user authentication and data security has been achieved using encryption approach that use private key to encrypt secret information and frame number selection provides receiver authentication.

At receiver end user receiver stego signal and extract information from video data using inverse procedure of video embedding process. At receiver end user provide frame number that contains secret information embedded behind these frames. If the frame number matches that has been stored in audio and video file then user is able to extract information else system will crash automatically.

In the purposed work various parameters have been analyzed for performance evaluation of purposed system these parameters have been discussed in result section.

4. Results

Steganography is a process of hiding information behind the cover objects so that easily data can be transmitted without knowledge to other users. Secret data has been transmitted in such a manner that can't be seen through naked eyes. In the purposed work authenticated audio video steganography has been done using both audio and video files. Data has been embedded behind audio and video data of a single video file. Data has been extracted from a video file using audio video separator that separate audio information from the video file in WAV format. After separation secret information that is text and image has been embedded behind audio and video respectively. Audio data has been embedding using phase coding approach and video data has been embedded using multiple least significant bits approach with bit set operation.

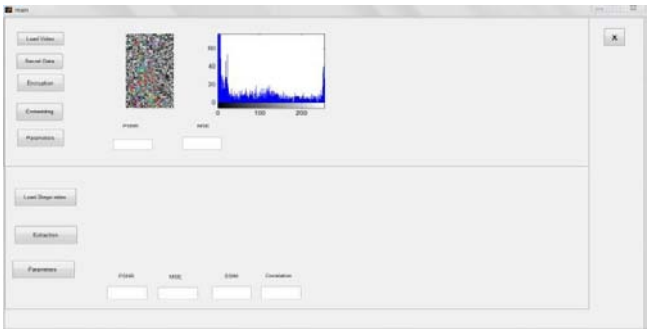

Figure 4.1: Encryption of secret data

This figure represents secret information that has to be embedded behind the pixels of cover object for secure transmission through the channel. The secret information has been loaded to the system for embedding behind the cover objects pixels.

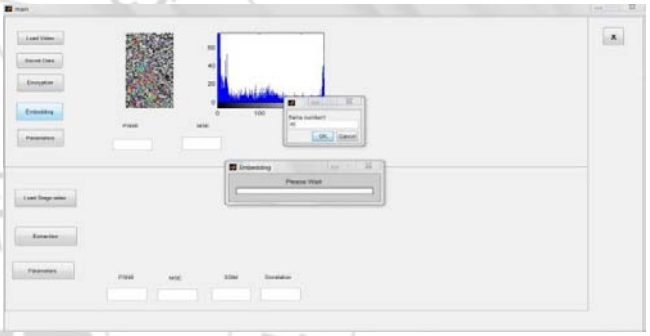

Figure 4.2: Embedding of secret information to cover data

This figure represents secret data has been encrypted using different encryption standards for security purpose of the secret information. Various encryption schemes have been utilized for encryption of secret information. In the purposed work encryption has been done using MSLB approach. In the process of MLSB video pixels have been shifted on the basis of different bits that have been input to the system for shifting process. In the process of MLSB video bits have been shifted according to the input provided by the user.

Figure 5.4: Loading Stego video

This figure represents stego video, which has been loaded to the system for extraction of secret data.

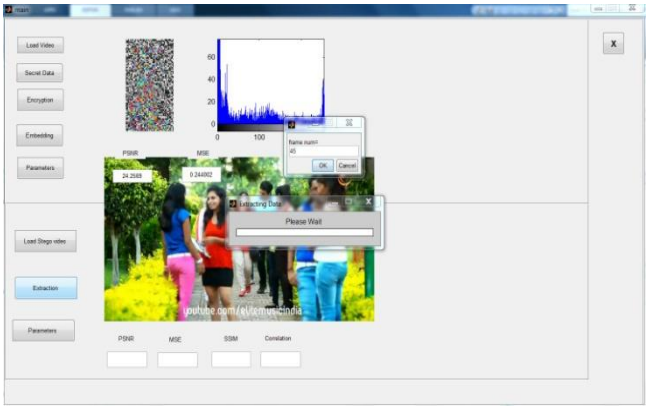

Figure 5.5: User validation checking

This window is use to represent the frame number for the authentication of users. After getting this password user can login.

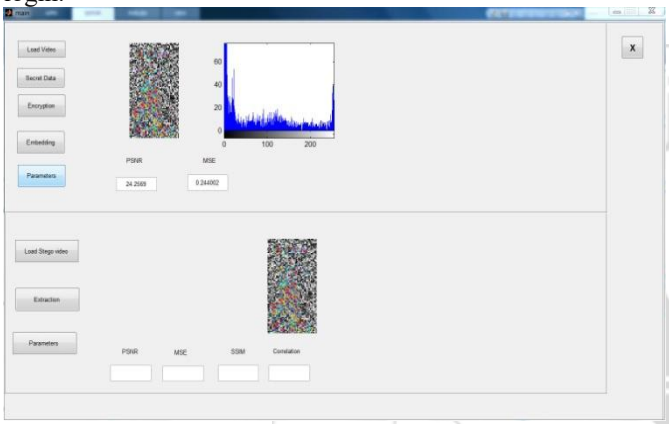

Figure 5.6: Extraction of secret information before decryption

In the shown snap there is the image showing the secret information of the embedded image in the video.

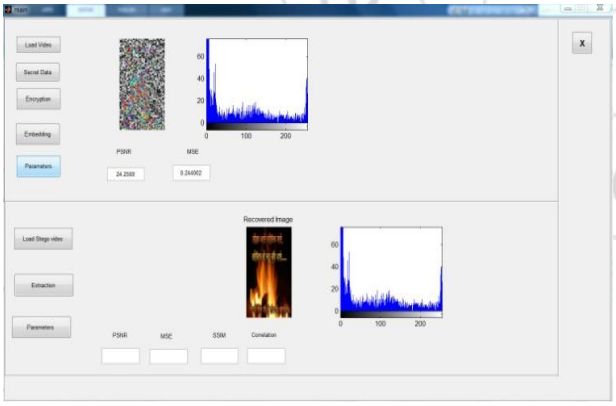

Figure 5.7: Extraction of secret information after decryption

This figure represents secret information that has been extracted from video frames using bitget operations from multiple least significant bits of stego video.

Table 5.1: PSNR for different videos using proposed and previous approach

Video	*Proposed*	*Previous*
Video 1	64.93	41.54
Video 2	64.95	40.27
Video 3	60.23	41.51
Video 4	63.03	41.72

This table describes PSNR values for various video files that have been used for embedding of secret information.

Table 5.2: MSE for different videos using proposed and previous approach

Video	Proposed	Previous
Video 1	0.02	4.56
Video 2	0.02	6.09
Video 3	0.06	4.58
Video 4	0.04	4.36

This table describes MSE values for various video files that have been used for embedding of secret information.

5. Conclusion

Steganography is process of hiding secret information behind any image and video file for the secure transmission of data. Image steganography is used for hiding information in the form of text and images. But due to lack of security reason and early detection of hiding information video steganography has been come into utilization. Video steganography comprises various frames in a single video file from which prediction of secret data availability is not come so easy process in this research various performance evaluation parameters have been analyzed for performance measurement. Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE), Structure Similarity Index Matrix (SSIM) and correlation coefficient has been measured. These parameters provide information about distortion occurred in original and stego file. By analyzing these parameters we can say that purposed video steganography approach provides much better results than that of previous approaches.

References

[1] Islam, M.R. "An efficient filtering based approach improving LSB image steganography using status bit along with AES cryptography", IEEE Conf. on Informatics, Electronics & Vision (ICIEV), 2014, pp 1 – 6.

[2] Yi-Chun Liao "Data hiding in video using adaptive LSB", IEEE Conf. on Pervasive Computing (JCPC), 2009, pp 185 – 190.

[3] PoojaYadav "A Secure Video Steganography with Encryption Based on LSB Technique" 2013 IEEE International Conference on Computational Intelligence and Computing Research.

[4] Mstafa, R.J. Elleithy, K.M. "A highly secure video steganography using Hamming code"*IEEE Long IslandSystems, Applications and Technology Conference (LISAT), 2014*, pp. 1 – 6.

[5] Abhinav Thakur, Harbinder Singh, SikhaSharda, "Secure Video Steganography based on Discrete Wavelet Transform and Arnold Transform", International Journal of Computer Applications (0975 – 8887, Volume 123 – No.11, August 2015.

[6] Kousik Das gupta, J. K. Mandal and Paramartha Dutta, "HASH BASED LEAST SIGNIFICANT BIT TECHNIQUEFOR VIDEOSTEGANOGRAPHY (HLSB)", International Journal of Security, Privacy and Trust Management (IJSPTM), Vol. 1, No 2, April 2012.

[7] K. Ramesh Babu, Depavath Harinath , P. Satyanarayana and M. V. Ramana Murthy, "Enhancing Security Using Video Steganography and Water Marking", Advances in Image and Video Processing, Volume 3 No 5, October (2015); pp. 1-9
[8] Metaliya Viral G, Anurag Rishishwar Manish Trivedi, "A Real Time Approach for Secure Image Transmission Using Video Steganography",International Journal of Electronics, Communication & Soft Computing Science and Engineering, ISSN: 2277-9477, Volume 4, Issue 2.
[9] Snehal Satpute,Sunayana Shahane, Shivani Singh, "An Approach towards Video Steganography Using FZDH (Forbidden Zone Data Hiding)", International Journal of Innovations & Advancement in Computer Science, ISSN 2347 – 8616, Volume 4, Issue 1, January 2015
[10] Heena Goyal, Preeti Bansal, "An Analytical Study on Video Steganography Techniques", International Journal of Advanced Research in Computer Science, Volume 6, No. 5, May - June 2015
[11] Uddin, M.P, Ferdousi, S.J., Ibn Afjal, M. "Developing an efficient solution to information hiding through text steganography along with cryptography" *IEEE 9th International Forum onStrategic Technology*, pp. 14-17, 2014.
[12] Bug. r, G., Broda, M., Levický, D. "Data hiding in still images based on blind algorithm of steganography", *IEEE 24th International Conference on Radio elektronika,* pp. 1-4, 2014.
[13] Ge Huayong, Huang Mingsheng , Wang Qian "Steganography and steganalysis based on digital image" *IEEE 4th International Congress on Image and Signal Processing*, pp. 252-255, 2011
[14] Selvi, G. K, Mariadhasan, L. , Shunmuganathan, K.L. "Steganography using edge adaptive image", *IEEE International Conference onComputing, Electronics and Electrical Technologies,* pp. 1023-1027, 2012.
[15] Dagar, S "Highly randomized image steganography using secret keys" *IEEERecentAdvances and Innovations in Engineering*, pp. 1-5, 2014.