Advanced Steganography for Hiding Data and Image using Audio-Video

[1]Miss Madhuri R. Shende, [2]Prof. Amit Welekar, [3]Prof. S.V.Wajurkar Nagpur, India
Information Technology dept., TGPCET, Nagpur, India
[1]*madhurishende19@gmail.com.* [2]*Welekar.amit@gmail.com*

Abstract— Steganography is an art of hiding the secrete message that is being send in the other non secret text. The benefit of steganography is that the expected mystery message does not pull in thoughtfulness regarding itself as an object of investigation. Our point is to conceal mystery data and picture behind the sound and feature document individually with. Sound records are generally compacted for capacity or speedier transmission. Sound records can be sent in short remain solitary portions. 4LSB is used for video steganography and cryptographic algorithm for encryption and decryption. Parity coding is used for Audio Steganography.

Keywords — *Steganography, Cryptography, Encryption Algorithm*

*****

1. INTRODUCTION

Security has turned into a critical issue as data innovation. The encryption field serves to give security on pictures and information, for example, secrecy, substance validation and information beginning confirmation. Steganography concentrates on concealing data in a manner that the message is imperceptible for pariahs and just appears to the sender and proposed beneficiary. It is helpful instrument that permits clandestine transmission of data over an over correspondences channel.

The benefit of steganography over cryptography alone is that the expected mystery message does not pull in thoughtfulness regarding itself as an object of investigation. Sound feature crypto steganography which is the mix of picture steganography and sound steganography utilizing PC legal sciences system as an apparatus for verification.

The following Figure 1. Show four types of steganography methodology:

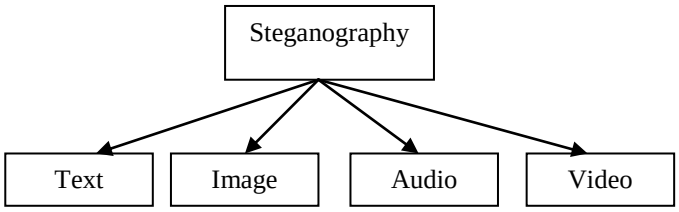


Figure 1:-Types of Steganography

Our point is to conceal mystery data and picture behind the sound and feature document individually. Sound records are generally compacted for capacity or speedier transmission. Sound records can be sent in short remain solitary portions. There are different sorts and procedure of information stowing away in sound like Least Significant Bit Encoding and Phase coding. In LSB coding is the least difficult approach to implant data in a computerized sound record. By substituting the slightest critical bit of every inspecting point with a double message, LSB coding takes into consideration a lot of information to be encoded. In Phase coding addresses the commotion's detriments instigating systems for sound steganography.

1.1 Steganography

Steganography focus on hiding information in such a way that the message is undetectable for outsiders and only appears to the sender and intended recipient. It is useful tool that allows covert transmission of information over and over communications channel. Steganography is a technique which is used to hide the message and prevent the detection of hidden message. Various modern techniques of steganography are

a) Video Steganography c) Audio Steganography

Audio Video stegnography is a modern way of hiding information in a way that the unwanted people may not access the information. The propose method is to hide secret information and image behind the audio and video file respectively.

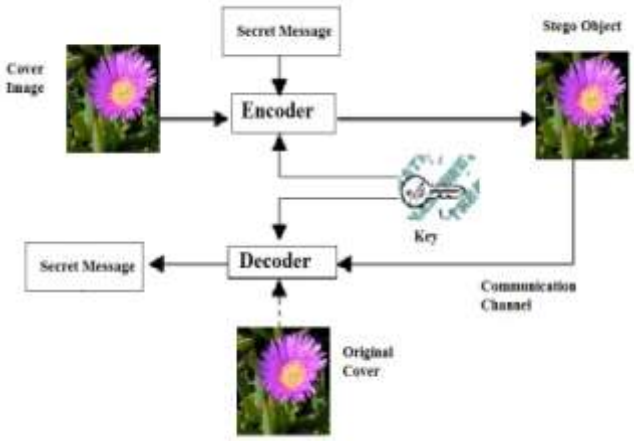


Fig 2:- Stenography Mechanisms

1.2 Audio Steganography

Audio steganography software can embed messages in WAV, AU, and even MP3 sound files. In audio steganography sound file is modified in a a way they contain a hidden information. This modification done in such a way that secrete data must be secure and without destroying the original signal. The basic model of Audio steganography consists of Carrier (Audio file), Message and Password. Carrier is also known as a cover-file, which conceals the secret information. Encoding secret messages in audio is the most challenging technique

because the human auditory system (HAS) has such a dynamic range that it can listen over. Audio files are usually compressed for storage or faster transmission. Audio files can be sent in short stand-alone segments. There are various types and technique of data hiding in audio like Least Significant Bit Encoding and Phase coding.Embedding secret messages in audio file is more difficult than embedding messages in digital image. In order to hide secret messages, various methods for embedding information in digital audio like Least significant bit, parity bit coding, phase coding, spread spectrum etc.

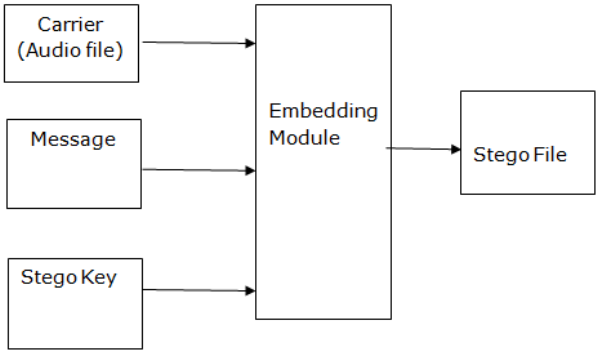


Figure 3:- Basic Audio Steganographic Model

1.3 Video Stegnography

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.

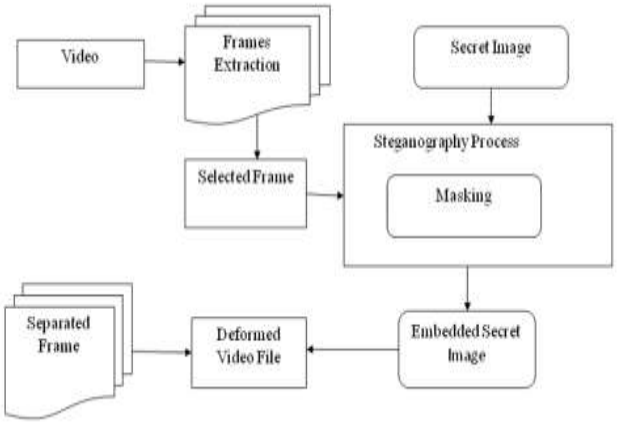


Figure 4:-Hiding Image Behind Video File

2. Related Work

In computer vision, steganography is a vast area of study and research that have been done throughout. There are many Techniques of video steganography such as Least Significant Bit method (LSB), Spread Spectrum, and Discrete Cosine Transform (DCT). Least Significant Bit method (LSB) is one of the most common and successful method which hide the secret data in the least significant bit of the cover video. Along with this many Author's had also used different methods and Encryption Algorithms to provide more secrecy to the message.

May 2014, Manpreet Kaur, Er. Amandeep Kaur [1] used Hash-LSB method which is an efficient steganographic method for embedding the secret message into cover video Here the author has applied cryptographic method i.e. RSA algorithm to secure a secret message.

April 2014, Deepak Kumar Sharma, Astha Gautam, [2] A twofold hash capacity procedure is utilized to choose the pixel from line and segment. A quadratic testing system is utilized for tackling the issue of impact where we are including a prime number with the current hash esteem rather than direct hunt. A division strategy system is utilized to call attention to the pixel in an edge that is pixel's area in line and section in a casing. At the point when pixel is discovered, the character of data that is to shroud, a twofold estimation of that solitary character is supplanted by unique pixel's red part, then second casing is to choose and second character's parallel worth is supplanted by the first pixel's green segment, this will proceed until the every paired character of the data are covered up.

December 2010, Kriti Saroha, Pradeep Kumar Singh, [3] Shows another steganographic technique for installing a picture in an Audio record. Accentuation will be on the proposed plan of picture covering up in sound and its correlation with straightforward Least Significant Bit (LSB) insertion strategy for information stowing away in sound.

May 2009, Cheng-Hung Chuang and Guo-Shiang Lin, [4] an optical cryptosystem with versatile Steganography is proposed for feature arrangement encryption and decoding. The optical cryptosystem utilizes a twofold arbitrary stage May 2009, Cheng-Hung Chuang and Guo-Shiang Lin, [4] an optical cryptosystem with versatile Steganography is proposed for feature arrangement encryption and decoding. The optical cryptosystem utilizes a twofold arbitrary stage encoding calculation to scramble and unscramble feature arrangements. The feature sign is initially exchanged to RGB model and after that isolated into three channels: red, green, and blue. Every channel is encoded by two irregular stage veils created from session keys. For higher security, a topsy-turvy technique is connected to figure session keys. The figured keys are then installed into the scrambled feature outline by a substance subordinate and low mutilation information inserting system. The key conveyance is refined by concealing figured information into the scrambled feature outline with a particular concealing arrangement created by the zero-LSB sorting system.

2007, Malik, H.M.A, Ansari, R., KhokharA, [5] presented novel method for information covering up in advanced sound that adventures the low affectability of the human sound-related framework to stage twisting. Indiscernible however controlled stage changes are presented in the host sound

utilizing an arrangement of allpass channels (APFs) with particular parameters of allpass channels, i.e., shaft zero areas. The APF parameters are decided to encode the inserting data. Amid the location stage, the force range of the sound information is evaluated in the z-plane far from the unit circle. The force range is utilized to evaluate APF shaft areas, for data translating.

3. PROPOSED METHODOLOGY

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. The Blowfish algorithm is used for more security purpose.

Sender selects any one audio-video file. After that 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 depends 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 16 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 Sender will select a for the transmission which we will be embedded in video by the system in the video frame signals of the audio-video file and the encryption key will be hidden behind the video frame.

Fig 5:- Working at Sender Side

At the receiver side the secret data and the image is extract from the stego audio and stego video file. For extracting secret data receiver used same passkey which is used by the sender. The receiver will cover exact data which is send by the sender

The system asks for the PASSWORD. The sender enters the same username and password which is received by him/her by the transmitter privately. After getting and password as input from the user the system generates a 16 byte key from the matlab function getFixWidth() which is required for matching with the key that will be extracted from the video frame. The system then asks whether the user is TRANSMITTER or RECEIVER to proceed further. After getting confirmation that the user is receiver the system will display the Receiver Interface.

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.

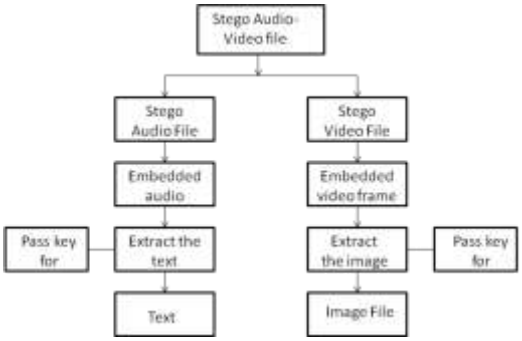


Fig 6: Working of Receiver side

3.1 LSB Coding

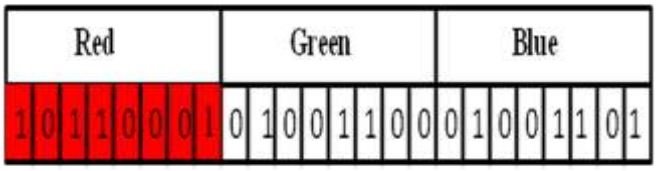
A very popular methodology is the LSB (least significant bit), which replaces the least significant bit in some bytes of the cover file to hide a sequence of bytes containing the hidden data. That's usually an effective technique in cases where the LSB substitution doesn't cause significant quality degradation, such as in 24-bit bitmaps. In computing, LSB is the bit position in a binary integer giving the units

value, i.e., 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.

Fig 7: Binary representation of Decimal 149

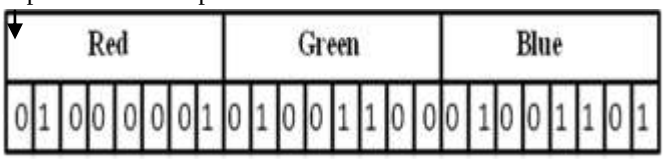
The binary representation of decimal 149, with the LSB highlighted. The MSB in an 8-bit binary number represents a value of 128 decimal.
An algorithm of vide steganography is based on the face that each pixel is represented by 3 bytes where each byte reprinting the intensity of 3 primary colors that is RGB(Red, Green, and blue) . Size of images file is directly related to number of pixel and granularity of color definition.

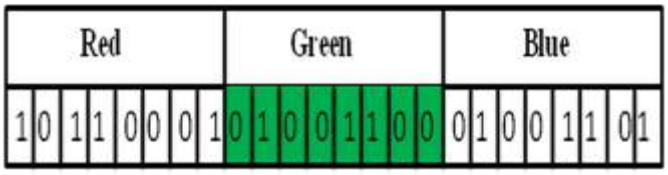
Lets data to be hidden =ABC
ASCII code of A= 65 and corresponding binary is 01000001.
ASCII code of B= 66 and corresponding binary is 01000010
ASCII code of C= 67 and corresponding binary is 01000011
Let the first pixel's RGB component



Red component is replaced with binary of 65i.e. A

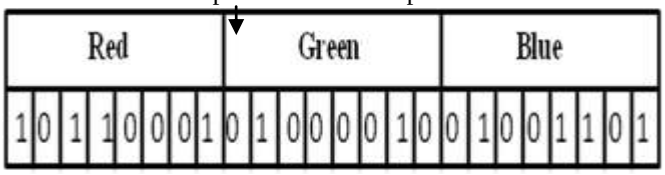
Replaced Red components

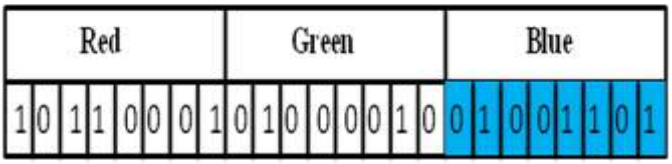




Green component of second pixel is replaced with binary of 66 i.e. B.

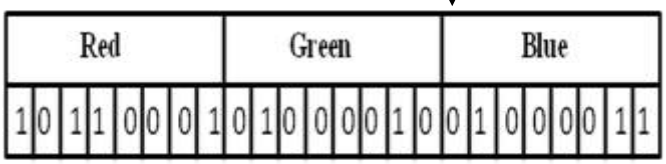
Replaced Green components





Blue component of third pixel is replaced with binary of 67i.e. C

Replaced Blue components



And the process is continues.

In proposed method hiding a secret image behind the video using LSB algorithm. Video is nothing but a collection of frames. Here we used LSB algorithm for hiding secrete message using 2 frames. For the less distortion of cover media and accurate recovery of data at reciver side.

Consider pixel of the cover media is 254
Binary representation is 1 1 1 1 1 1 1 0
This binary code can be encrypting by using some masking. We can use any sequence of binary number.
Consider the binary number which is used for mask is 1 1 1 1 0 0 0 0
Perform the ANDing operation of the binary representation of the first pixel of the cover image and binary number used for mask.

X1= 1 1 1 1 1 1 1 0
⊕
Mask= 1 1 1 1 0 0 0 0

A = 1 1 1 1 0 0 0 0

Now select the first pixel of secrete image. The image which we want to hide. Suppose the first pixel of the secrete image is Y=127
Binary representation of Y is = 0 1 1 1 1 1 1 1
Again perform the ANDing operation of the first pixel of the secrete image and binary number of mask.

- Y = 0 1 1 1 1 1 1 1
- Mask = 1 1 1 1 0 0 0 0
  ⊕

- B = 0 1 1 1 0 0 0 0

Now performing LSB substitution on process. In LSB substitution the 4 bit of the of the every secrete image in the four bit of every bit of the cover file.

- A = 1 1 1 1 0 0 0 0

➨ B = 0 1 1 1 0 0 0 0

After Appling LSB algorithm the modified A is =11110111. This representation is converted into digital the value of A=247.

The original values of pixel of the cover media is 254 and after embedding the secrete image the value of pixel is 247. If we do the calculation 254-247=7

That means there is only lost of 7 bit. This lost do not effect on cover media. So there is no distortions detect.

3.2 Parity coding

Parity coding is one of the robust audio steganographic techniques. Instead of breaking a signal into individual samples, this method breaks a signal into separate samples and embeds each bit of the secret message from a parity bit. If the parity bit of a selected region does not match the secret bit to be encoded, the process inverts the LSB of one of the samples in the region. Thus, the sender has more of a choice in encoding the secret bit. If the parity bit of a selected region does not match the secret bit to be encoded, the process flips the LSB of one of the samples in the region.

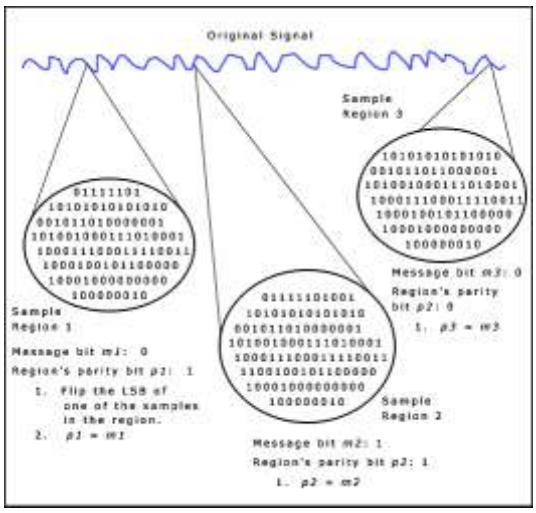


Fig 8:- Parity Coding Procedure.

4. RESULT AND DISCUSSION

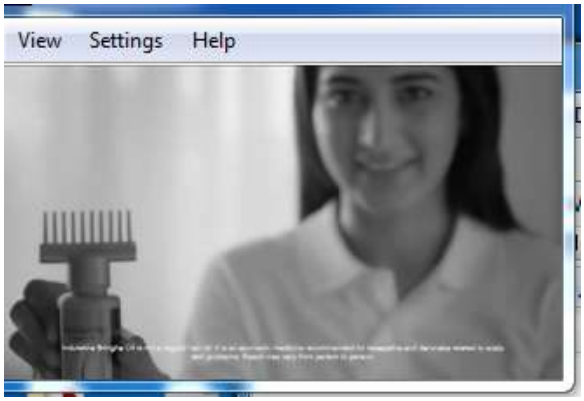


Fig 8: Original Video

Runing Original Audio-video file

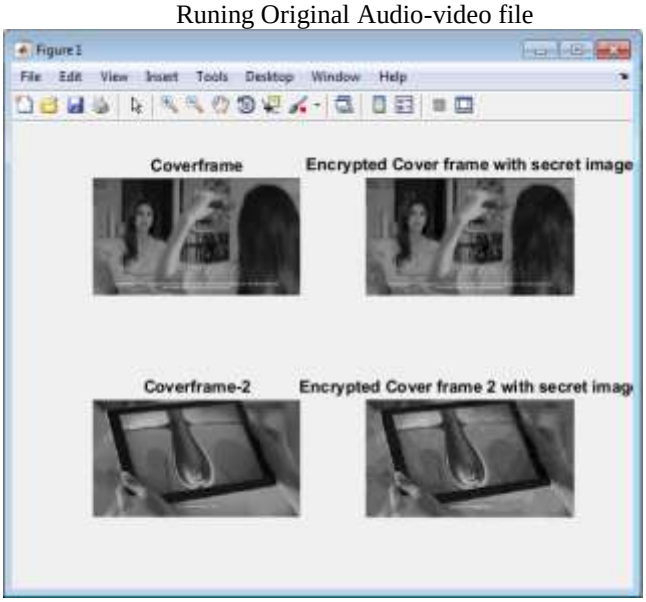


Fig 10: Video Stegnography Module

In this module, select the corresponding two frames of the video and hiding the secret image in the frames. After hiding the LSB and MSB of the image into the frame Encrypted cover frame with secret image will be displayed.

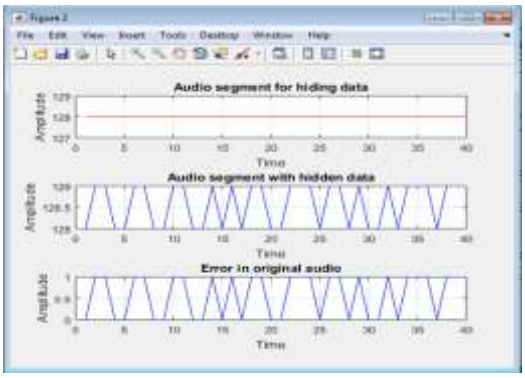


Fig 11: Audio Amplitude before and after hiding data

Natural Audio segment for hiding data

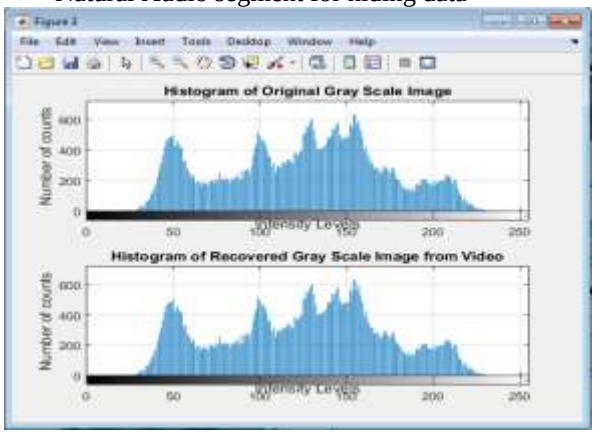


Fig 12: Histograms for video stenography

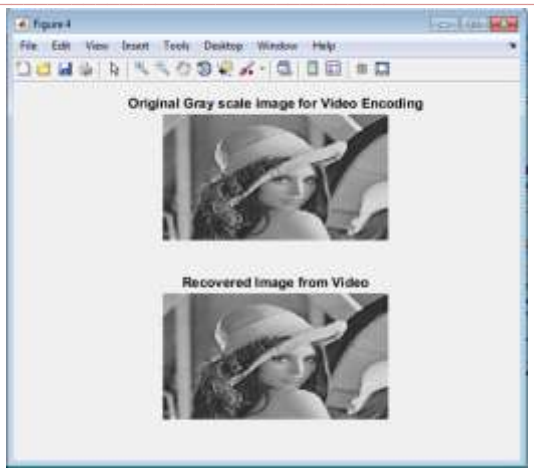


Fig 13: Recovered Image from Video

If any image hide behind the audio, after recover binary image from audio it will be exact match with the original binary image.

5. CONCLUSION AND FUTURE SCOPE

In this paper, diverse systems are talked about for installing information in content picture, sound/feature signs and IP datagram as spread media. All the proposed techniques have a few confinements. The stego sight and sound delivered by specified routines for mixed media steganography are pretty much defenseless against assault like media organizing, pressure and so forth. The exploration to gadget solid steganographic procedure is a ceaseless process. We are going to propose a framework that will give better stego documents utilizing sound video approach. Information security using data hiding Audio-Video with the help of computer forensic technique providing better hiding capacity and security. This method is very safe and secured. Data recover at the receiver side is error free. In future we plan to provide much better security using different encryption algorithms which may require less time as required to blowfish. Again we aim to provide better PSNR ratio and improve the quality of video steganography.

In future we plan to provide much better security using different encryption algorithms which may require less time as required to blowfish. Again we aim to provide better PSNR ratio and improve the quality of video steganography.

References

[1] Manpreet Kaur Er. Amandeep Kaur, " Improved Security Mechanisam of text in Video by using Steganographic Technique" ,International Journal of Advanced Research in Computer Science and Software Engineering, pp.216-220, Chandigarh University, Gharuan, Punjab, India ,May 2014

[2] Deepak Kumar Sharma, AsthaGautam, " An approach to hide data in video using steganography" , IJRET: International Journal of Research in Engineering and Technology eISSN: 2319-1163 | pISSN: 2321-7308; Volume: 03 Issue: 04 , Apr-2014

[3] KritiSaroha,Pradeep Kumar Singh ,"A Variant of LSB Steganography for Hiding Images in Audio", Internaltionalhounal of computer applications 0975-8887 Vol 11 No 6. December 2010.

[4] Cheng-Hung Chuang and Guo-Shiang Lin, "An Optical Video Cryptosystem with Adaptive Steganography", Proceedings of International Association for Pattern Recognition (IAPR) Conference on Machine Vision Applications (MVA'09), pp. 439-442, Keio University, Yokohama, Japan, May 20-22, 2009. (NSC97-2221-E-468-006

[5] Malik, H.M.A. ; Ansari, R. ; KhokharA.,"Robust Data Hiding in Audio Using Allpass Filters" A. Audio, Speech, and Language Processing, IEEE Transactions on Volume: 15 , Issue: 4 DOI: 10.1109/TASL.2007.894509 Publication Year: 2007 , Page(s):1296-1304

[6] Pritha Roy, Dr.AsokeNath " New Steganography approach using encrypted secret message inside Audio and Video media" International Journal of Advance Research in Computer Science and Management Studies, Volume 2, Issue 12, December 2014, pp.47-59

[7] R. Shanthakumari1 and Dr.S. Malliga2, "Video Steganography Using LSB Matching Revisited Algorithm",IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 16, Issue 6, Ver. IV(Nov – Dec. 2014), PP 01-06

[8] ShivaniKhosla&Paramjeet Kaur, " Secure Data Hiding Technique Using Video Steganography and Watermarking"International Journal of Computer Applications (0975 – 8887) Volume 95– No.20, June 2014, pp.7-12

[9] Rohit G Bal, Dr P Ezhilarasu, "An Efficient Safe and Secured Video Steganography Using Shadow Derivation",International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) , Vol. 2, Issue 3, March 2014, pp.3251-3258

[10] Hemant Gupta&SetuChaturvedi, "Video Steganography through LSB Based Hybrid Approach", IJCSNS International Journal of Computer Science and Network Security,VOL.14 No.3, March 2014, pp.99-106

[11] 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 (IJCSES, Vol.4, No.6, December 2013),pp.9-25

[12] PritishBhautmage, Prof. AmuthaJeyakumar, Ashish Dahatonde, " Advanced Video Steganography Algorithm", International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 3, Issue 1, January - February 2013, pp.1641-1644

[13] Wafaahasanalwan,"Dynamic least significant bit technique for video steganography", Journal of Kerbala University , Vol. 11 No.4 Scientific . 2013,pp.7-16

[14] A. Swathi , Dr. S.A.K Jilani, Ph.D, "Video Steganography by LSB Substitution Using Different Polynomial Equations",International Journal Of Computational Engineering Research (ijceronline.com) Vol. 2 Issue. 5,Sep2012,pp.1620-1623

[15] R Sridevi, Dr. A Damodaram and Dr.Svl. Narasimham, "Efficient Method of Audio Steganography by Modified LSB Algorithm and Strong Encryption Key with Enhanced Security", Journal of Theoretical and Applied Information Technology, pp. 771-778, 2009.

[16] 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.

[17] 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.

[18] 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: 0975-3397

[19] Saurabh Singh and Gaurav Agarwal, "Hiding image to video: A new approach of LSB replacement", International Journal of Engineering Science and Technology Vol. 2(12), 2010, 6999-7003

[20] Sherly A P and Amritha P P, "A Compressed Video Steganography using TPVD", International Journal of Database Management Systems(IJDMS) Vol.2, No.3, August 2010 DOI:10.5121/ijdms.2010.2307 67

[21] Gunjan Nehru and Puja Dhar, "A Detailed Look Of Audio Steganography Techniques Using LSB And Genetic Algorithm Approach", International Journal of Computer Science (IJCSI), Vol. 9, pp. 402-406, Jan. 2012.

[22] Ajay.B.Gadicha, "Audio wave Steganography", International Journal of Soft Computing and Engineering (IJSCE), Vol. 1, pp. 174-177, Nov. 2011.

[23] 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.

[24] 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

[25] 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.

[26] 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.

[27] 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