

Audio Video Steganography using Hybrid method of security and Optimization technique for Data Security and Authenticity

Amanjot kaur¹, Er.Jyoti Rani²

SHAHEED UDHAM SINGH COLLEGE OF ENGG. & TECH.

(E-mail: amarbagga89@gmail.com)

Abstract—Now days, it is very risky to handle the data in internet against intruders. Data is generally in the form of text, audio, video and image. Steganography is one of the best methods to share the data secretly and securely. Modern steganography is the art and science of covert communication which sends secret messages under the camouflage of innocent-looking cover media, such as digital images and videos, without arousing any suspicion. The main objective of steganography is to avoid drawing attention to the transmission of hidden information to achieve the security of the secret message, meanwhile, if the hackers noticed any change in the sent message then this observer will try to know the hidden information inside the message. Steganography has various useful applications and the technique employed depends on the requirements of the application to be designed for. For instance applications may require absolute invisibility of the secret data, larger secret data to be hidden or high degree of robustness of the carrier.

In the paper, hiding of the image and text behind video and audio file using the PSO optimization technique has been performed. The proposed work has also performed decoding of the audio file and extract the secrete text message. The objective of the research is to ensure the security, safety and using strong method of secrecy for the convenient communication between the different parties. We also analyzed the performance of the proposed method by using the techniques like correlation, Entropy, PSNR, MSE, SNR for detecting data presence in suspected multimedia file.

Keywords—PSO; DES; HAS; SHA hash key;

I. INTRODUCTION

Information security [1] in today's world is a sense of declaration against threats, means that important information must be secured and there risks of attacks as well as controls must be balanced. Information security actually starts with the emergence of first main frame computer. But with the introduction of information security many viruses and code breakers were also developed that breaks the security channel and damage the important information. Information security has two important aspects that are:

- IT security

- Information assurance

IT security referred to as the security of technology, which can be office systems or home desktops. A computer is a device with processor and memory; such systems are called standalone systems used for small purposes. IT specialists are always called when there is need of data with large businesses. They are responsible to manage data as well as keep the systems secure from cyber-attacks which actually reach the private information and try to gain the entire control of the system. Information assurance is the way of assuring that the private information is still secure not lost or stolen. Information is not only theft but it can be damaged by system malfunction or any other. Information security is further divided into three dimensions that are

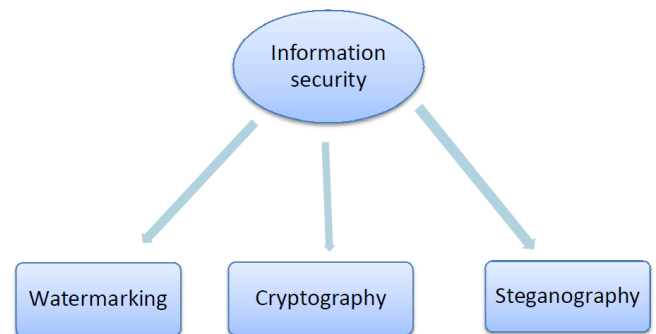


Fig. 1 Information security

Watermarking [8] is a recognizable image pattern that may be darker or lighter in tone, indicates the copy rights of particular documents. Usually watermarking has been used in government documents, currency notes, and stamp papers for legal purpose, passports for security features.

Cryptography [6] comes from a Greek word meaning hidden or secret writing for secure communication in the presence of third parties or Un-authorized persons. Cryptography actually hides the information from illegal sources. Earlier forms of secret writing are classic cryptography, cipher texts. Cipher machine was also introduced by French but with the development of latest computers much more complex ciphers were developed and they encrypt data of any kind, whether it's a binary format, plaintext or hexadecimal data. The technique of concealing a message in such a way that only the intended recipient and the

sender should know about it is called a steganography. It is used to hide data inside data. Steganography is not a new concept, but it has been utilized since the ancient times, when the secret messages were kept written on the paper in the covert mode, which could be read by pouring the special kind of ink or paper over fire, etc.

II. STEGANOGRAPHY

Steganography is used to hide data inside data. Steganography is not a new concept, but it has been utilized since the ancient times, when the secret messages were kept written on the paper in the covert mode, which could be read by pouring the special kind of ink or paper over fire, etc.

A. General Terms Of Steganography

- **Hidden data:** The secret data, which is being protected or embedded, is called the secret data. The secret data can be an image, signal, speech, text or video. Every kind of data requires the specific types of cover media for the robust embedding.
- **Cover Media:** The cover media is the data which is used to embed the hidden or secret data. This can be any data such as video, audio, signal, image, etc but in the larger size than the hidden data.
- **Stego Key:** The stego key is used to establish the robust cryptographic methodology over the hidden data in order to enhance the security level. The cryptography adds the additional security layer and robust protection even when the data is revealed through the various steganalysis methods.
- **Stego-media:** The cover media after embedding is called the stego-media, which contains the secret or hidden data within. The users on the receiver end can extract the hidden information by using the reverse steganography methods from the stego-media.

B. Features of Steganography

The general specifications that must be kept in mind, when implementing steganography, are described below:

- The embedded data must not downgrade the quality of cover media. Quality of cover media should be such that it must look like original media. The media size should not increase tremendously as it can look suspicious to the casual viewer. It must have good Peak Signal to Noise Ratio.
- The data that is to be hidden should be embedded in the information part of cover media, not in the header. The data must be temper resistance to the attacks of the third party.
- Integrity of data should be maintained, it must be robust enough so that it must not be modified in between the way.
- A cover file must be of enough size so that it can hide a large amount of message.

- The message hidden must be invisible to the viewer.
- The hidden message must be undetectable during steganalysis process.

C. Types of Steganography

There are four basic types of steganography represented in the following figure:

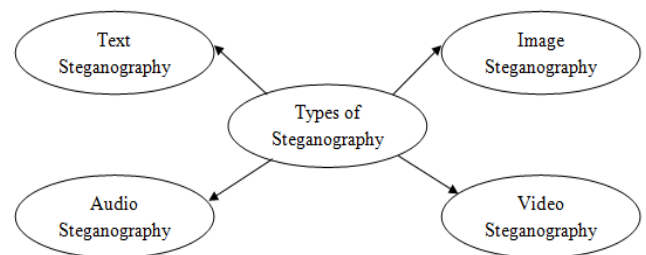


Fig. 2 Types of Steganography

1) **Text Steganography:** Text steganography [2][7] can be achieved by changing the text format, or by changing certain features of textual elements such as alphabets. The major goal of the steganographic methods is to protect the hidden data with reliability and robustness. The minimized chances of the decoding by utilizing the steganalysis attacks should be there in order to protect the level of security. Also the visible changes should be avoided during the incorporation of the steganographic methods.

2) **Image Steganography:** To a computer an image file is simply a file that shows different colours and intensities of light on different areas of an image. The best type of image file to hide information inside of is a 24 Bit BMP (Bitmap) image. The reason being is this is the largest type of file and it normally is of the highest quality. When an image is of high quality and resolution it is a lot easier to hide and mask information inside of. Although 24 Bit images are best for hiding information inside of due to their size some people may choose to use 8 Bit BMP's or possibly another image format such as GIF, the reason being is that posting of large images on the internet may arouse suspicion.

3) **Audio Steganography:** Information hiding in audio is based on the interpretation of sound made by Human Auditory System. The steganography in audio is a challenging task because Human Auditory System (HAS) is extremely sensitive. Auditory realization is based on the critical band analysis in the inner ear where frequency to location transformation takes place with basilar membrane. HAS cannot interpret sound which is silent or very stressful. This weakness is exploited to implement audio steganography [9].

4) **Video Steganography:** A video is a combination of audio and image. A continuous flow of image constitutes a video. Therefore, the techniques that can be applied on audio and image separately, they can be applied on video also. The main advantage of video is that it is comprised of large

amount of data, therefore a small distortion in data does not put any adverse effect on video quality and it can go unobserved through human eyes [7].

D. Literature Review

Disha, et.al, (2017), have explained that private or delicate information is embedded inside something using steganography that gives different impression than used in regular data. The audio tracks, videos, text documents and digital images like different carrier file formats can be used but the use of video steganography has gain very popularity due to increase in advancement of information over web. In this steganography the information is kept safe from gate crashes by concealing secret information inside a video. Number of researchers has proposed different techniques that hide secret information inside a video and all have their own advantages and disadvantages. There are two categories of video steganography name as frequency domain and spatial domain steganography techniques. In this paper, authors have given a review about different steganography methods that comes under spatial domain.

Lindawati, et.al, (2017), have analyzed that number of new ways has been come with the increase growth in telecommunication science and technology. This makes hackers, carder, crackers and preacher like peoples to threat private information. There will be a loss of information if it is transmitted on wrong side so there is need to secure the information which is confidential. The digital media messages can be hide using method of steganography. Digital Steganography using digital media as the container vessel such as images, sounds, text, and video. The images, videos, audio or text can include a hidden secret data but in this paper authors have implemented a audio steganography. The Least Significant Bit (LSB) method of steganography can be implemented which added encryption and decryption form cryptography. This method works is messages that have been encrypted beforehand will be hidden evenly on each region in MP3 or WAV already divided, with modify / change the LSB of the media container with the bits of information to be hidden.

Himanshu Wadekar, et.al, (2017), has explained that steganography is a process of hiding information or data by embedding it in video, audio or text like medium. Earlier the secret information is sent using Morse code, invisible ink like different techniques for sending secret information between two places. Now, the wood, paper like medium has been turned into multimedia by steganography medium added in digitization world. The information or data is embedded into frames of videos using video steganography but distortion is introduced in pixels due to storing significant amount of data. This will increase the secret data suspension present in it. In traditional techniques Least Significant Bit of the pixel is used for embedding information in image and encrypted using Advance Encryption Standard. This results in introduction of distortion in the image that can easily recognize by intruder. In the proposed approach data is stored in the form of remainder, quotient and divisor and there is distribution, encryption of location key which is stored in various frames.

Sachin Jangid, et.al, (2017), have predicted that digital information is embedded inside image, video, audio signal and text like digital medium using steganography without revealing its presence in the medium. The medium is covered by video file in case of video steganography inside which any secret information can be embedded. The performance of video steganography based on MLC (Multilevel Clustering) gets improve in case of proposed video steganography used in this paper. The cover frame is clustered using K-mean clustering in proposed MLC technique. The Mean square error (MSE), Peak signal to noise ratio (PSNR) are different parameters on the basis of which the proposed algorithm has been tested. The results are compared with existing video steganography technique based on Integer Wavelet Transform (IWT) that shows a increase in PSNR using proposed MSE technique.

Siva Shankar. S, et.al, (2017), have predicted that digital information is embedded inside image, video, audio signal and text like digital medium using steganography. When processing is applied on cover media then inserted messages should not be destroyed so, noise removal, format conversion, lossless or loss compression or enhancement like image processing operation should be applied on it. In this paper, authors have used random puzzle based multi-layer image encryption and decryption method that embedded the secret information into cover image. The results show that robust embedding has been achieved using it as it enhances the security. In this work, they have used a 8×8 Sudoku puzzle which has a 64×64 reference matrix and 5 bits per pixel average capacity has been achieved using it.

Hemalatha S, et.al, (2017), have recommended the use if video steganography for sending secret information which is hidden inside a video file. In this paper, authors have proposed a method for hiding image and audio data in wavelet domain and name it MP4 steganography method. The I, P and B are frames exist in video in which without referring to other frames data is decoded independently using intra or I frame. The motions are captured using B and P frames and all three together are known as Group of Pictures (GOP). The I frame is the starting of GOP and according to the used codec its length will vary. They have been used for embedding purpose as they are not lost during any kind of signal proceeding or compression operations.

Hera Arif, et.al, (2017), have referred steganography as hiding information in ordinary, not secret and insignificant video, pdf, image, audio and text like medium. After applying steganography attackers will not be able to detect the hidden messages are exist in which medium. This is the reason a non-suspicious medium is used for hiding data. An input images are used as a tools of steganography that can embedded data inside a images or text after that output image is created by hiding the image or text into input image. The secret information inside an image or text that looks same as input image. The different steganography algorithms are tools are compared in this paper.

Kunal Hossain, et.al, (2016), have analyzed that information access has become easy by the increase in use of internet that also increase the development in applications based on multimedia. The issue of security has become very

challenging and crucial as image, video and audio like media carry information and now its security has become very hot research topic for researchers. In this paper, a media type is converted into different form in proposed video, audio and image steganography based methodology. The intended video is encoded in such a that it is segmented into different frames using proposed steganography technique which is further consider as single RGB image. The frames are then converted into respective number of sound files. Then reverse procedure is applied to retrieve the original video by decrypted the steganography or sound files. In the retrieved data the music and speech is present in ordinary sound files that were encoded into RGB image in which decoded procedure is applied to retrieve them are four basic types of steganography represented in the following figure:

III. PROBLEM FORMULATION

Now days, it is very risky to handle the data in internet against intruders. Data is generally in the form of text, audio, video and image. Steganography is one of the best method to share the data secretly and securely. Steganography algorithm can be applied to audio, video and image file. Secret data may in the form of text, image or even in the form of video and audio. Hiding secret information in video file is known as video steganography. Data hiding in audio video file with the help of computer forensic technique provide better hiding and security to the secret information. The main objective of steganography is to avoid drawing attention to the transmission of hidden information to achieve the security of the secret message, meanwhile, if the hackers noticed any change in the sent message then this observer will try to know the hidden information inside the message. The focus is on hiding image and text behind video and audio file and extracted from an .avi file at sender side and computer forensic techniques at receiver side to cross check the security parameter by providing authentication at receiver side for the purpose of triple security of data.

The proposed work has hiding the text into audio file successfully and also decode the audio file and extract the secrete text message. For the purpose of security and optimization of data, the hybrid technique of security and PSO for optimality has also been proposed.

The objective of the research is to ensure the security, safety and using strong method of secrecy for the convenient communication between the different parties. To analyze the result of proposed method by using the techniques like correlation, Entropy, PSNR, MSE, SNR can be used for detecting data presence in suspected multimedia file. It helps in detecting terrorist activities on web.

A. Objective

The Objective of the proposed work is to achieve the security, integrity and optimality of data using audio and video Steganography.

The Objectives of the research work are:

- To study the various security methods those are used for Steganography.
- To study the various optimization techniques, that can be applied to the research work.
- To implement proposed hybrid security method for secrecy of the text message from the hackers.
- To apply the PSO optimization techniques for the enhancement of the proposed method.
- To analyze the behavior of proposed method using parameters such as correlation, Entropy, PSNR, MSE, SNR.

IV. RESULTS AND DISCUSSION

Steganography deals with the hidden information detected in the broadcasting media using robust steganography approach. In this research area, an efficient process is projected to detect material hidden in vectors in the bit-streams of the video and audio and also the extraction of the hidden information to achieve high signal to noise ratio which is well known as the video and audio steganography. In this approach authors have proposed a novel technique to assure hybrid secure approach using DES and SHA. Also the performance is optimized using particle swarm optimization and the performance is evaluated in terms of peak signal to noise ratio, signal to noise ratio and mean square error rate.

A. Proposed Algorithm

The template is designed so that author affiliations are not repeated each time for multiple authors of the same affiliation. Please keep your affiliations as succinct as possible (for example, do not differentiate among departments of the same organization). This template was designed for two affiliations.

1) *Particle Swarm Optimization (PSO)*: Particle Swarm Optimization (PSO) is a simplified algorithm and optimizes the problem in an iterative manner which will provide global best solutions from the number of solutions. It deals with free space search operations over the particle's position and velocity and can seek vast spaces to get best optimize solution. So, PSO is generally considered for the sake of optimization which is popularly known as routing optimization.

For every particle $j = 1, \dots, \text{swarm}$

Set the particle's location with a consistently dispersed random vector X_i

Set the particle's best recognized location to its initial location P_i

If $f(P_i) < f(g_b)$ then

1. Update the swarm's finest known position: g_b

2. Set the particle's speed: v_i

3. While a finishing is not encountered do

For each particle $ij = 1, \dots, \text{Swarm}$ do

For each measurement $d = 1, \dots, n$ do

4. Evaluate fitness function

5. Update the particle's speed: v_i , Update the particle's location: x_i , Update the best known location: g_b

Where gbest the resultant global best optimize solution which is done in the iterative manner.

2) *DES (Data Encryption Scheme)*: The Data Encryption Standard is a symmetric-key process which deals with the cipher text discovered by the National Institute of Standards and Technology. DES is the operation of a Cipher process. It uses 16 round structures. The chunk scope is 64-bit message. However, key distance is 64-bit; it has an actual key distance of 56 moments, out of which 8 of the 64 moments of the key are not cast-off by the encryption algorithm.

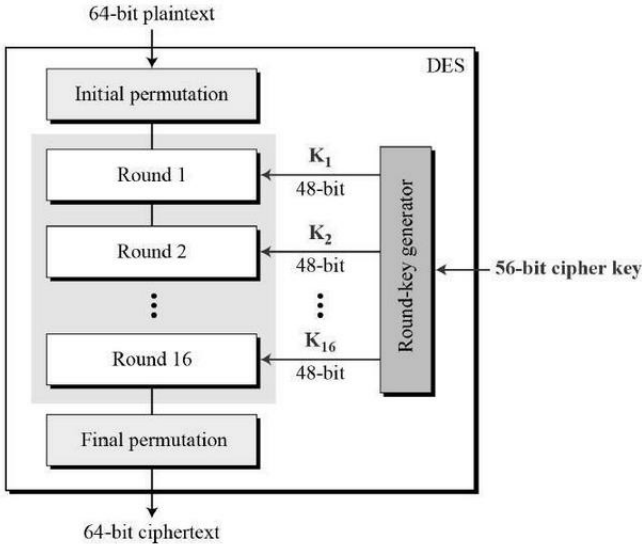


Fig. 3: DES operations

The result explanation of the proposed approach is discussed below:

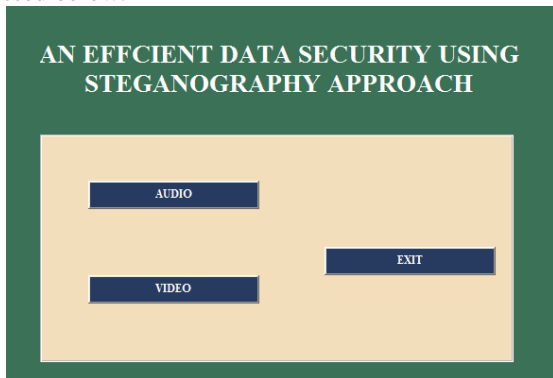


Fig. 4 Main Panel

In figure 4, the GUI panel is built using graphical user interface using user interface controls such as pushbuttons, panel, static texts etc.



Fig. 5 Speech panel

Figure 5 shows speech panel which is made using GUI controls which shows the different operations to achieve the desired results.

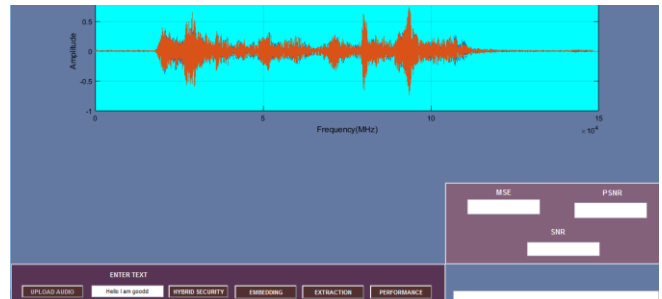


Fig. 6 Signal Uploading

Figure 6 shows the uploading of the signal panel in which the original sample is uploaded in which the message is to be hide and also we can see the message in the edit box which shows the enter text to be hide in the original sample

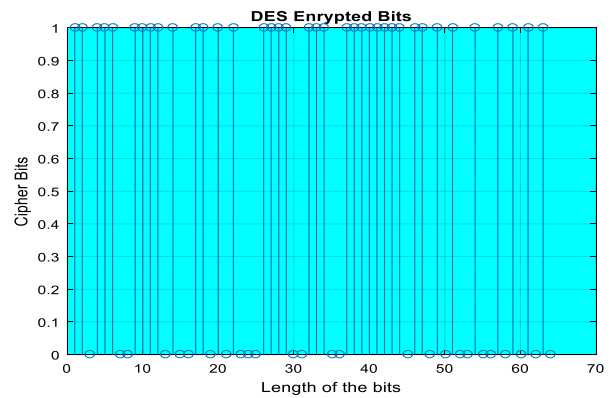


Fig. 7.1 DES Bits



Fig. 7.2 SHA hash keys

Figure 7.1 and 7.2 shows the DES and SHA operations in which the encrypted bits and hash security is shown after applying hybrid approach to make the system more secure

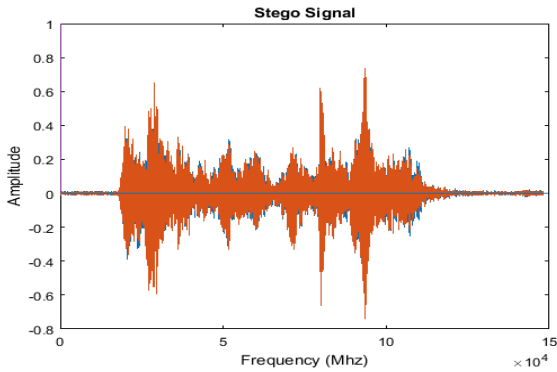


Fig. 8 Stego Signal

The figure 8 shows the stego signal which is exact replica of the original signal and is embed message in that signal which is shown in terms of amplitude with respect to the frequency

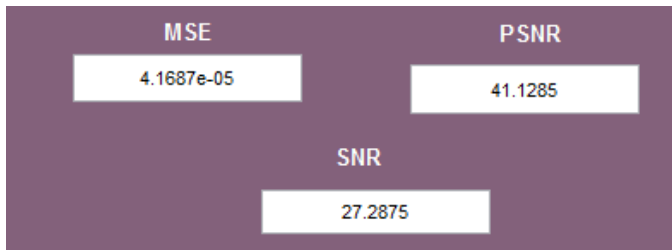


Fig. 9 Performance Evaluation

The figure 9 shows the performance evaluation in terms of mean square error rate, peak signal to noise ratio and signal to noise ratio. The PSNR must be high for better efficiency and MSE must be low for less error rate probabilities



Fig. 10 Uploaded video sample

The figure 10 shows the uploaded video sample on which the video steganography will be performed using hybrid steganography and optimization approach

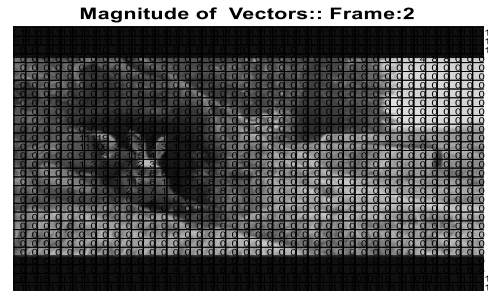


Fig.11 Magnitude Vector

The figure 11 shows the selection of the object from the uploaded image using selection process which neglects all other segmented regions and evaluate only the object detections of the uploaded video sample and which the embedding process is done and the resultant stego frame. It shows the reconstruction of the frames of the video which shows that the uploaded sample is reconstructed after the embedding of the image which shows that the our proposed approach is able to reconstruct the image sample in an efficient manner

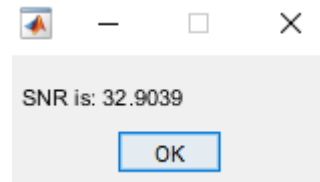


Fig. 12 Signal to Noise Ratio

The figure 12 shows the high signal to noise ratio which shows that the system is able to achieve high signal to noise ratio and it must be high for high efficiency of the system.

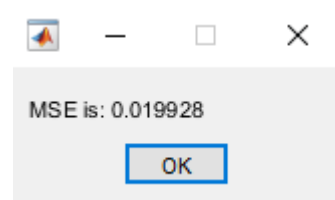


Fig. 13 Mean Square Error rate

The figure 13 shows that how much error rate our proposed system is able to achieve to perform video steganography and it also must be low

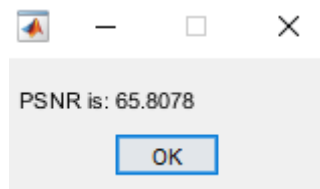


Fig. 14 Peak Signal to Noise Ratio

Fig 14 shows the peak signal to noise ratio which shows the strength of the vectors of the embedding and extraction to be the less distorted which

TABLE I. Performance Comparison

Parameters	Proposed
PSNR (db)	65.80
MSE	0.019
SNR	32.9023

From above figure we can see the performance comparison of the proposed system with the base and we can see that the proposed system is able to achieve high performance in terms of peak signal to noise ratio and Mean square error rate and high signal to noise ratio

CONCLUSION AND FUTURE SCOPE

Security for information has become a great concern in today's internet era. Thus sending sensitive information from one end to another end via common communicating channel has become inevitable. Steganography has various useful applications and the technique employed depends on the requirements of the application to be designed for. Data hiding in audio video file with the help of computer forensic technique provide better hiding and security to the secret information. The goal of steganalysis is to detect the presence of secretly hidden data in an object. Digital media files, such as images, video, and audio, are ideal cover objects for steganography as they typically consist of a large number of individual elements that can be slightly modified to embed a secret message. Moreover, such empirical covers are rather difficult to model accurately using statistical descriptors, which substantially complicates detection of embedding changes.

This work deals with the hiding image and text behind video and audio file and extracted from an .avi file at sender side and computer forensic techniques at receiver side to cross check the security parameter by providing authentication at receiver side for the purpose of triple security of data. The proposed work has hiding the text into audio file successfully and also decode the audio file and extract the secret text message. For the purpose of security and optimization of data, the hybrid technique of security and PSO for optimality has been implemented. The objective of the research was to ensure the security, safety and using strong method of secrecy for the convenient communication between the different parties. The future work can deal with the hybridization of the optimization

techniques for audio video steganography. The most important use of steganographic techniques will probably lie in the field of digital watermarking.

REFERENCES

- [1] Disha, Khushil Saini, "A Review on Video Steganography techniques in Spatial Domain", Control, Automation & Power Engineering (RDCAPE), 2017 Recent Developments in, pp. 366-371, 2017.
- [2] Lindawati, Rita Siburian, "Steganography Implementation on Android Smartphone Using the LSB (Least Significant Bit) to MP3 and WAV Audio", The 3rd International Conference on Wireless and Telematics 2017, pp. 170-174, 2017.
- [3] Himanshu Wadekar, Aishwarya Babu, Vaishali Bhavadia, Tatwadarsi P. N. , "A New Approach to Video Steganography using Pixel Pattern Matching and Key Segmentation", A New Approach to Video Steganography using Pixel Pattern Matching and Key Segmentation, pp. 121-126, 2017.
- [4] Sachin Jangid, Somesh Sharma, "High PSNR based Video Steganography by MLC(Multi-Level Clustering) Algorithm", International Conference on Intelligent Computing and Control Systems ICICCS 2017, pp. 589-594, 2017.
- [5] Siva Shankar. S, Dr. Rengarajan. A, "Puzzle based Highly Secure Steganography", Algorithms, Methodology, Models and Applications in Emerging Technologies (ICAMMAET), 2017 International Conference on, pp. 91-95, 2017.
- [6] Hemalatha S, U. Dinesh Acharya, Shamathmika, "MP4 Video Steganography in Wavelet Domain", Advances in Computing, Communications and Informatics (ICACCI), 2017 International Conference, pp. 1229-1235, 2017.
- [7] Hera Arif, Hassan Hajjdiab, "A Comparison between Steganography Software Tools", Computer and Information Science (ICIS), 2017 IEEE/ACIS 16th International Conference on, pp. 423-428, 2017.
- [8] Kunal Hossain, Ranjan Parekh, "An Approach Towards Image, Audio and Video Steganography", ICRCRCN, pp. 302-306, 2016.
- [9] K. Rosemary Euphrasi, M. Mary Shanthi Rani, A Comparative Study On Video Steganography in Spatial and IWT Domain, 2016 IEEE International Conference on Advances in Computer Applications (ICACA), pp. 104-109, 2016.
- [10] Rini Indrayani, Hanung Adi Nugroho, Risanuri Hidayat, Irfan Pratama, "Increasing the Security of MP3 Steganography Using AES Encryption and MD5 Hash Function", 2016 2nd International Conference on Science and Technology-Computer (ICST), pp. 107-111, 2016.
- [11] Prabira Kumar Sethy, Kamal Pradhan, Santi Kumari Behera, "A Security Enhanced Approach for Video Steganography using K-Means Clustering and Direct Mapping", 2016 International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT), pp. 618-622, 2016.
- [12] Achmad Solichin, Painem, "Motion-based Less Significant Frame for Improving LSB-based Video Steganography", 2016 International Seminar on Application for Technology of Information and Communication, pp. 179-183, 2016.
- [13] S. NANDA KISHOR, Dr. G. N. KODANDA RAMAIAH, Dr. S. A. K. JILANI, "A review on steganography through multimedia", Research Advances in Integrated Navigation Systems (RAINS), International Conference, pp. 1026-1032, 2016.
- [14] Siddharth Gosalia, Shaan Shetty, A. S. Revathi, "Embedding audioinside a digital video using LSB steganography", Computing for Sustainable Global Development (INDIACom), 2016 3rd International Conference, pp. 21-25, 2016.
- [15] Ramandeep Kaur, Pooja, Varsha, "A Hybrid Approach for Video Steganography using Edge Detection and Identical Match

- Techniques”, IEEE WiSPNET 2016 conference, pp. 867-871, 2016.
- [16] Mazhar Tayel, Ahmed Gamal, Hamed Shawky , “A Proposed Implementation Method of an Audio Steganography Technique “, Advanced Communication Technology (ICACT), 2016 18th International Conference, pp. 1-5, 2016.
- [17] Sameh A. Abbas, Taha I. B. El Arif, “Optimized Video Steganography Using Cuckoo Search Algorithm”, 2015 IEEE Seventh International Conference on Intelligent Computing and Information Systems (ICICIS'15), pp. 572-577, 2015.
- [18] Mahmood Maher Salih, Mohammed Salem Atoum, “Applying AWGN MP3 Steganography Attack in BiLSB and SLSB Techniques”, 2015 4th International Conference on Advanced Computer Science Applications and Technologies, pp. 62-67, 2015.
- [19] Santhoshi Bhattt, Arghya Ray, Avishake Ghoshttt, Ananya Ray, “Image Steganography and Visible Watermarking using LSB Extraction Technique”, IEEE Sponsored 9th International Conference on Intelligent Systems and Control (ISCO)2015, pp. 32-37, 2015.
- [20] P. Selvigrija, E. Ramya, “Dual Steganography for Hiding Text in Video by Linked List Method”, 2015 IEEE International Conference on Engineering and Technology (ICETECH), pp. 25-30, 2015.
- [21] Amritpal Singh, Harpal Singh, “An Improved LSB based Image Steganography Technique for RGB Images”, Electrical,

