Hiding Messages Using Motion Vector Technique In Video Steganography

P.Paulpandi[1], Dr.T.Meyyappan,M.sc.,M.Phil.,M.BA.,Ph.D[2]
Research Scholar[1], Associate professor[2]
Department of Computer Science & Engineering,
Alagappa University,Karaikudi.
Tamil Nadu,India.

Abstract- **Steganography is the art of hiding information in ways that avert the revealing of hiding messages.Video files are generally a collection of images. so most of the presented techniques on images and audio can be applied to video files too. The great advantages of video are the large amount of data that can be hidden inside and the fact that it is a moving stream of image. In this paper, we proposed a new technique using the motion vector, to hide the data in the moving objects. Moreover, to enhance the security of the data, the data is encrypted by using the AES algorithm and then hided. The data is hided in the horizontal and the vertical components of the moving objects. The PSNR value is calculated so that the quality of the video after the data hiding is evaluated.**

Keywords- Data hiding, Video Steganography,PSNR, Moving objects, AES Algorithm.

I. INTRODUCTION

Since the rise of the Internet one of the most important factors of information technology and communication has been the security of information. Steganography is a technology that hides a user defined information within an object, a text, or a picture or in a video files. Steganography is Greek word has the meaning of , “Stegano”, or “covered” and “graphy” or “writing” which does not convey the transformation of information, but rather its hidden aspect.

In steganography, the object of communication is the hidden message and the cover data are only the means of sending it. Secret information as well as cover data can be any multimedia data like text, image, audio, video etc The objective of this work is to develop a Compressed Video Steganographic Scheme that can provide provable security with high computing speed, that embed secret messages into images without producing noticeable changes. Here we are embedding data in video frames.

Cryptography protects information by transforming it into an unreadable format. It is useful to achieve 1from Greek, it literally means”covered writing” confidential transmission over a public network. The original text, or plaintext, is converted into a coded equivalent called cipher text via an encryption algorithm. Only those who possess a secret key can decipher (decrypt) the cipher text into plaintext. Steganography in video can be divided into two main classes. One is embedding data in uncompressed raw video, which is compressed later[2,3].

The other, which is more difficult, tries to embed data directly in compressed video stream[4,5,6]. Advanced Encryption Standard (AES) is a specification for the encryption of electronic data. The algorithm described by AES is a symmetric-key algorithm, meaning the same key is used for both encrypting and decrypting the data.

The paper is organized as follows. The related works that are done on the steganographic techniques and encryption techniques are provided in the section 2. The proposed research contribution with the motion vector technique, video compression, and extraction is placed in the section 3. The results and the discussions are given in the section 4.The paper is concluded with the results in section 5.

II. RELATED WORK

This section gives a brief overview on the related work done on the video compression using adaptive block based compression and Motion vector based on the MPEG-2 video Steganography. Moreover, the encryption algorithm used for text encryption is discussed.

F.A.P.Petitcolas,R.J. Anderson and M.G. Kuhn presented method of cryptography works to mask the content of a message,steganography works to mask the very existence of the message[1] and Niels Provos and Peter Honey man presented the Greek used to pass secret information by writing in wax-covered tablets:wax was first scraped off a tablet, the secret message was written on the tablet, and then the tablet was covered again with the wax [4].

Mobasseri presented the method of a message either encrypted or unencrypted, can be hidden in a computer video file (containing the picture of, for instance, an innocent 2 year old baby) and transmitted over the Internet, a CD or DVD, or any other medium [5].Shiguo lian provide the main goal of steganography is to communicate securely in a completely undetectable manner and to avoid drawing suspicion to the transmission of a hidden data [4].

F.A.P.Petitcolas, R.J.Anderson and M.G.Kuhn have proposed the information hiding is a recently rapidly developed technique in the field of information security and has received significant attention from both industry and academia. It contains two main branches: digital watermarking and steganography. The former is mainly used for copyright protection of electronic products. while steganography, as a new way of covert communication, the main purpose is to convey data secretly by concealing the very existence of communication[1].

J. J. Chae,and B. S. Manjunath presented the method of the Steganography in video can be divided into two main classes. One is embedding data in uncompressed raw video, which is compressed later[6,7]. Giuseppe Caccia and Rosa Lancini presented the other method of which is more difficult, tries to embed data directly in compressed video stream[2,3,6].

III. PROPOSED WORK

A. Video Compression

Video compression uses modern coding techniques to reduce redundancy in video data. Video compression typically operates on square-shaped groups of neighboring pixels, often called macro blocks. These pixel groups or blocks of pixels are compared from one frame to the next and the video compression code sends only the differences within those blocks. In areas of video with more motion, the compression must encode more data to keep up with the larger number of pixels that are changing.

Generally, the motion field in video compression is assumed to be translational with horizontal component and vertical component and denoted in vector form by for the spatial variables in the underlying image. Such as three steps search, etc., This is based on the video device processing power, the required compression ratio, and the reconstruction quality.Admin has to be choose one video file along with one key, both will be compression and create one encoding key send to the member. The Authenticated member uncompressed the video file and takes the second privacy key.

B. Motion Vector

In video compression, a motion vector is the key element in the motion estimation process. It is used to represent a macro block in a picture based on the position of this macro block (or a similar one) in another picture, called the reference picture. Authenticated person after taking the second privacy key he has only the authority what are the video which was sent by Admin, the member can see the video in our application, in that video it can detect the motion vector. After seeing this, the member obtain both of the key and given to the login section and send the message to the Admin.

C. Encryption

Encryption is the conversion of data into a form, called a cipher text that cannot be easily understood by unauthorized people. Original message is being hidden within a carrier such that the changes so occurred in the carrier are not observable. The information about the user defined information, the

private key used to encrypt the text and the average time of the frame format is given. The encryption of the text is done by using the AES standard algorithm since the key size is larger for the AES.

D. Extraction of original data

Decryption is the process of converting encrypted data back into its original form, so it can be understood. When the user inputs the correct key that is used at the decryption process, this will extract the original message that is encrypted and embedded.

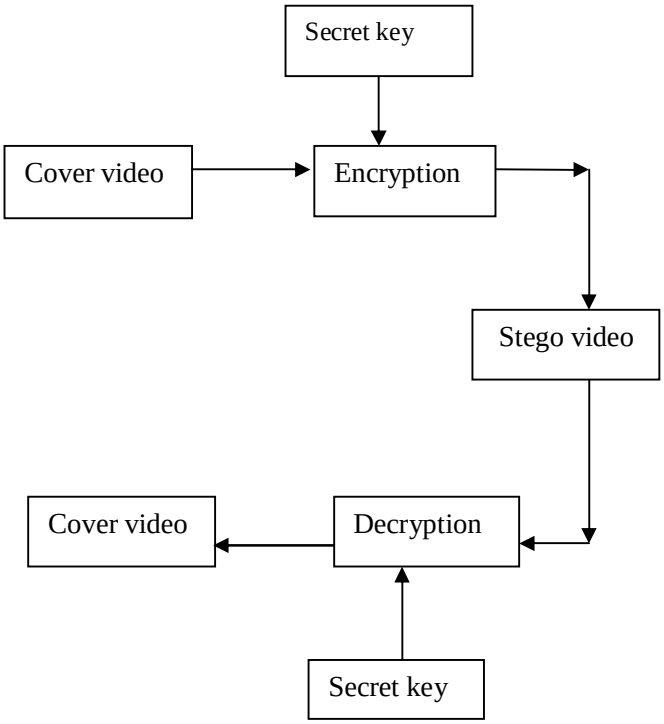

Figure 1. video Steganography

E. Peak signal-to-Noise Ratio

Larger SNR and PSNR indicate a smaller difference between the original (without noise) and reconstructed image. The main advantage of this measure is ease of computation but it does not reflect perceptual quality. An important property of PSNR is that a slight spatial shift of an image can cause a large numerical distortion but no visual distortion and conversely a small average distortion can result in a damaging visual artifact, if all the error is concentrated in a small important region.

The PSNR is defined as:

$$PSNR = 10 \cdot \log_{10}\left(\frac{MAX_I^2}{MSE}\right)$$
$$= 20 \cdot \log_{10}\left(\frac{MAX_I}{\sqrt{MSE}}\right)$$
$$= 20 \cdot \log_{10}(MAX_I) - 10 \cdot \log_{10}(MSE)$$

The definition of PSNR is the same except the MSE is the sum over all squared value differences divided by image size and by three.

F. Calculate PSNR value

The given table describes to calculate between the original video PSNR value and stego video PSNR values.

Cover video	Original video PSNR Value	Stego Video PSNR value
Video1 (256frame)	25	21.3
Video2 (350frame)	30	26.53
Video3 (400frame)	90	45.53

IV. RESULTS AND DISCUSSIONS

Conversion of a video in each frame the quality may be differing from one video to other depending on the video. In the case of conversion video, it is important to reproduce the video close to the original video so that even the smallest details are readable. Conventional measures are designed to

quantify the error, sensitivity between the original video and the converted one, while keeping most of the signal characteristics together.

Video systems may introduce some amounts of distortion or artifacts in the signal, so the quality measures are an important problem. There are several techniques and metrics that can be measured objectively and automatically evaluated by a computer program. Therefore, they can be classified as full-reference (FR) methods and no-reference (NR) methods. In FR video quality assessment methods, the quality of a test video is evaluated by comparing it with a reference video that is assumed to have perfect quality. NR metrics try to assess the quality of an image without any reference to the original one. In this paper we are using FR methods to measure the quality from original video to Converted videos.

The figures(1),(2),(3)describes the compression of the video, the text encryption and the data are included in this section. The PSNR value is also calculated so that the quality of the video is enhanced.This shows the selection of the cover video file in which the text has to be embedded. The files in the FLV (Flash Video) Format are used here. The above figure shows **the** information about the user defined information, the private key used to encrypt the text and the average time of the frame format is given. The encryption of the text is done by using the AES standard algorithm since the key size is larger for the AES.The PSNR value is calculated after the user defined information is embedded.

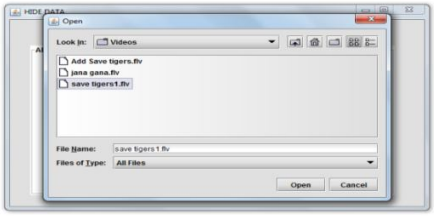

Fig (1).Select video file

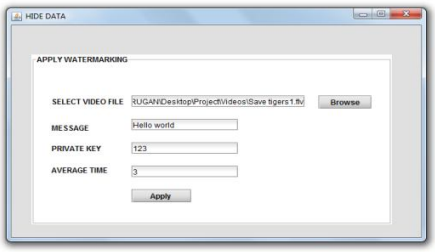

Fig (2) Apply video file, data and key

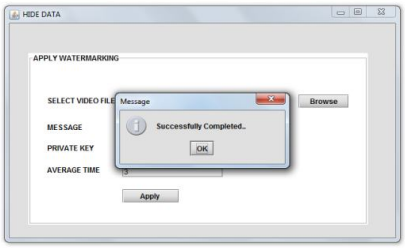

Fig (3) Data embedded

The below figures shows that the pixel components are either distorted or not. The data is stored in the horizontal and in the vertical components of the frame disclosed. The data is stored in the moving objects than in the still pictures. The MPEG -2 compressed video is used for the purpose so that a large volume of data has been stored. When the user inputs the right key that is used at the encryption process, this will extract the original message that is encrypted and embedded.

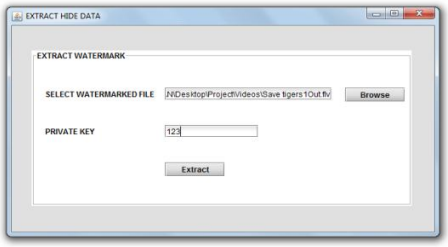

Fig (4) Extract data

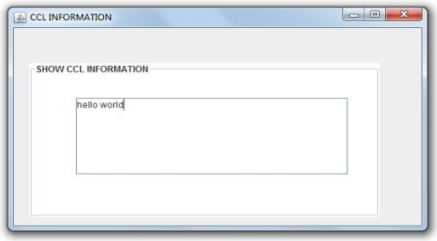

Fig (5) Retrieve messages

V. CONCLUSION

In this paper, we propose and investigate the data hiding method using the motion vector technique for the moving objects. In the existing works the data is hided within the still pictures where as it will ended in the image distortion. By embedding the data in the moving objects the quality of the video is increased. In this paper, the compressed video is used for the data transmission since it can hold large volume of the data. The adaptive based compression technique is evaluated such that the data is embedding in the vertical and horizontal component pixels. The PSNR value is calculated to show that the frame is transmitted without any loss or distortion. As a result, the motion vector technique is found as the better solution since it hides the data in the moving objects rather than in the still pictures. The encryption enhances the security of the data being transmitted.

REFERENCES

[1]F.A.P. Petitcolas, R.J. Anderson, and M.G. Kuhn, "Information Hiding—A Survey," Proc. IEEE, 1999

[2] A. Giannoula, D. Hatzinakos, "Compressive Data Hiding for Video Signals", *Proceedings of International Conference on Image Processing,* 2003, pp. I529- I532.

[3] Giuseppe Caccia, Rosa Lancini, "Data Hiding in MPEG2 Bit Stream Domain", *Proceedings of International Conference on Trends in Communications,* 2001, pp.363-364.

[4] Niels Provos and Peter Honeyman, "Hide and Seek: An Introduction to Steganography", University of Michigan, IEEE 2003.

[5] Mobasseri, B.: Direct sequence watermarking of digital video using mframes, Proc. International Conference on Image Processing, Chicago,IL, pp 399- 403, 1998.

[6] J. J. Chae, B. S. Manjunath, "Data Hiding in Video", *Proceedings of the 6th IEEE International Conference on Image Processing,* 1999, pp.311-315.

[7] Sutaone, M.S.; Khandare, "Image based Steganography using LSB insertion technique", IET, 2008.

[8] Neil F. Johnson, Duric, Z., Jajodia, S. Information Hiding Steganography and Watermarking Attacks and Countermeasure. Kluwer Academic Press. Norwrll, MA, New York, The Huague, London vol 32.8(2010) 79-94.

[9] Mamta Juneja, Parvinder S. Sandhu, and Ekta Walia,‖Application of LSB Based Steganographic Technique for 8-bit Color Images‖, WASET 2009.

[10] F.A.P.Petitcolas, R.J.Anderson, M.G.Kuhn, "Information Hiding-A Survey", *Proceeding of the IEEE,* vol. 87, no. 7, June 1999, pp.1062-1078.

[11] Melih Pazarci, Vadi Dipcin, "Data Embedding in Scrambled Digital Video", *Proceedings of the 8th IEEE International Symposium on Computers and Communication,* 2003, pp. 498-503.

AUTHORS BIOGRAPHY

Mrs.P.PaulPandi

Mrs.P.PaulPandi is a Research scholar in the Department of Computer Science and Engineering, Alagappa University, Karaikudi, Tamilnadu, India. She has received her M.Sc., in Computer Science from Alagappa University, Karaikudi and Tamilnadu. She has presented her work in National level conferences. Her areas of research interests include Image Processing.

Dr.T.Meyyappan

Dr.T.Meyyappan received his Ph.D. degree in computer science and Engineering from Alagappa University,Karaikudi,TamilNadu. He has obtained his M.SC.,M.Phil.,MBA.,.He is currently working as an associate professor in the Department of Computer Science and Engineering of Alagappa University,karaikudi,TamilNadu. He has presented and published number of papers in International and National Conferences, International and National Journals.His research areas of interest are cryptography, Operation Research, Data Mining, Security and Image Processing.