Efficient Algorithm For STEGANOGRAPHY In Compressed Video Frame

Vijay Solanki[1], Mahesh Kumar Porwal[2], Surendra Verma[3]
M. Tech. Scholar[1], Associate Professor[2-3]
Shrinathji Institute of Technology & Engineering, Nathdwara, Nathdwara[1-2],
Dungarpur College of Engineering & Technology, Dungarpur[3]
vijay24solanki1988@gmailo.com[1], porwal5@yahoo.com[2], er_suru@yahoo.co.in[3]

***Abstract* - Rapid development of data transfer through internet made it easier to send the data more accurately and faster to the destination. One of the most important factors of information technology and communication is the security of the information. In present scenario, data is protected by many layers of security. Data activity may be hidden, in addition to encryption, to make it more secure. Steganography provides a possible solution, hiding the data by embedding it into another data, to further enhance the data security. In this research, we introduce a novel secure steganography approach for defending video data against attacks. In this approach, instead of original message an encoded message by Huffman Coding Algorithm is hidden into a H.264 standard video using Least Significant Bit (LSB) and Parity Coding, which provides more security than conventional approaches. MATLAB 2009 is used to implement the proposed video steganography method.**

1. INTRODUCTION

Steganography in video data has been a very active topic and attracted many researchers as well as commercial companies due to its wide range of application domains such as military, national defense, economy, commerce, and so on.

Definition of steganography: The practice of concealing messages or information within other non-secret text or data.

2.1 Steganography

The Steganography is a technology concerned with ways of embedding a secret message in a cover message – also known as a cover object – in such a way that the existence of the embedded information is hidden (Anderson & Petitcolas, 1998). A secret message can be plaintext, cipher text, an image, or anything that can be represented as a bit stream (Johnson &Jajodia, 1998). The embedding process is sometimes parameterized by a secret key, called a stego key, and without knowledge of this key it is difficult for an unauthorized party to detect and extract the secret message. Once the cover object has information embedded in it, it is called a stego object.

In steganography, the possible cover carriers are innocent looking carriers (images, audio, video, text, or some other digitally representative code) which will hold the hidden information. A message is the information hidden and may be plaintext, cipher text, images, or anything that can be embedded into a bit stream. Together the cover carrier and the embedded message create a stego-carrier. Hiding information may require a stego key which is additional secret information, such as a password, required for embedding the information. For example, when a secret message is hidden within a cover image/video, the resulting product is a stego-image/video.

A possible formula of the process may be represented as:

Cover medium + embedded message + stego key = stego-medium

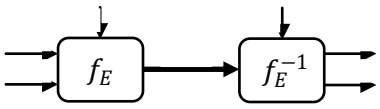

Figure 1.1 Graphical Version of the Steganographic System

f_E : Steganographic function "embedding"
f_E^{-1}: Steganographic function "extracting"
Cover: cover data in which emb will be hidden
emb: message to be hidden
Stego: cover data with the hidden message

The advantage of steganography is that it can be used to secretly transmit messages without the fact of the transmission being discovered. Often, using encryption might identify the sender or receiver as somebody with something to hide.

2.1.1. General properties of Steganography

a) *Confidentiality:* The adversary should not be able to gain any information about the cover data being sent in the system.
b) *Un-detectability:* The adversary should not be able to distinguish cover media created by legitimate users which does not hide information
c) *Robustness:* The adversary should not be able to prevent message from getting to their destination.

2.2 Motivation & Research Problem

Free speech, taken for granted in many democratic countries, is not possible in many other countries. Since some governments restrict the use of encryption, this has motivated people to learn other secret communication methods. Steganography can be considered as a solution to exchange information and news between people or civil rights organizations around the world over the Internet without any fear of the message being detected. On the other hand, there

has been a great concern about preserving the intellectual property rights of digital media such as text, image, audio, and video. Another concern regarded the ban of using encryption techniques on the Internet. This has significantly motivated the interest in information hiding techniques over the recent years. Additionally, the growing concern about the ease of copying, reproducing, and theft of digital works has motivated and increased the interest of publishing and broadcasting industries in watermarking and authentication techniques.

Cryptography converts the secret information into a scrambled code in such a way that only the intended recipient, who has the decoding key, can read this secret message. Furthermore, a third party can tell that a secret message has been sent from one party to another but he/she cannot read this message. However, steganography hides the very existence of this secret message. Thus, a third party cannot even know that a secret message has been embedded within a stego file or sent over a network.

Any digital media can be used as a cover media. The cover media can be a text, image (colour, gray), audio or video etc. Cover media is required in order to hide and carry the information. Usually digital images are required in order to hide secret messages. The secret message is hidden within the digital image. After the message is embedded within the cover media. An innocuous image or video consisting of scenery, people and other objects are the nominees for cover media. Video files are generally a collection of images and sounds, so most of the steganography 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 images and sounds. Therefore, any small but otherwise noticeable distortions might go by unobserved by humans because of the continuous flow of information. Today however, growing popularity of video based applications such as Internet multimedia, wireless videos, personal video recorders, video-on-demand, set-top box, videophone and videoconferencing has increased the demand for a secure distribution of videos. Apparently any image steganography technique can be extended to video steganography, but in reality video steganography techniques need to meet other challenges than that in image steganography schemes. Some of the video characteristics that impact steganography include:

i. High correlation between successive frames. If independent secret messages are embedded on each frame, an attacker could perform frame averaging to remove significant portions of that secret message.
ii. Some applications like broadcast monitoring require real time processing and therefore should have low complexity.
iii. The unbalance between the motion and motionless regions.
iv. Steganographic video sequences are very much susceptible to pirate attacks such as frame averaging, frame swapping, statistical analysis, digital-analog (AD/DA) conversions and lossy compressions.

It is concluded that the security of such digital data is major concern in the field of steganography without losing the efficiency of the steganography system (That is, without interrupting the quality of digital cover media).

3.1 Video Steganography

Video steganography is an emerging sub-field of digital steganography. Most digital steganographic methods have relied on exploiting file formats to hide information in parts of files either not parsed or parts invisible to the user in normal processing and use. Some more advanced methods hide data in the noise produced by lossy compression formats, such as JPEG images or MP3 audio files. For example, compare the two flowers in Figure 2.1 and try to decide which one is stegged (Steganographic).

Many of the JPEG image steganographic techniques carry over to MPEG video, however the steganalysis for video can be different because of the increase in the volume of data. Given the relatively high capacity of video, it is likely that it will be the next most popular carrier to discreetly transfer large amounts of data.

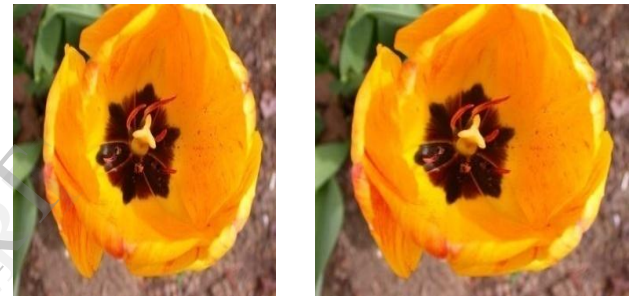

Figure 2.1: Clean and stegged versions of an image

The adoption rate of steganography in general and video steganography in particular is not well known, however there have been recent accounts in the news of law enforcement finding evidence of its use on suspect machines. Since steganography scanning tools are not yet mature enough for regular use, most of the evidence comes from steganographic tools themselves being installed.
Videos provide fairly high bandwidth for data embedding and are frequently posted and transferred on-line. The goal of steganalysis is to reduce the effective bit rate of data embedding in video by reliably detecting the higher embedding rates.Almost all lossy techniques that deal with perceived media exploit that human senses do not distinguish small changes in high frequency information. Visually this manifests as high detail areas of an image. In raw video every pixel is represented by 3 bytes, either by separating into red, green and blue (RGB), or, more likely, luma and two chroma components, called YUV or YCbCr. The human eye is less sensitive to colour than intensity so MPEG always encodes using YUV with the chroma components down sampled by a factor of two horizontally and vertically. Here we are using H.264 (or MPEG-4 Part 10 or Advanced Video Coding, used by the x264 encoder) video format. Section 2.2 details about this format.

3.1.1 Motion Vector

In video steganography, a motion vector is used for motion estimation process. It is used to represent a macro block in a picture. Authenticated person after taking the second privacy key, can see the video in particular application, in that video it can detect the motion vector. After seeing this, the member uses the key to see the message sent to the administrator. There can be 2 types of Motion Vectors: Forward (next frame) and Backward (previous frame). Forward vectors are more frequent, and when no information is provided as to whether it is forward or backward, one can assume it is forward. The way motion vectors are stored is through the Red and Green channels of an image, and there are essentially two formats: Absolute and Normalized.

3.1.1.1 Absolute Motion Vectors

Absolute Motion Vectors is the format that all tools that support motion vectors inside of Flame and Smoke are expecting and generating.

This format implicitly means that the vectors are stored in a float or half-float image format (Open EXR), and the particularity is that the pixel no movement is set to 0 in the Red and Green channel, with colour information being positive and negative using the whole float precision and are self-contained in terms of vector magnitude.

3.1.1.2 Normalized Motion Vectors

Normalized Motion Vector need to be converted to the Absolute format to be used colour range, so colour values can get way beyond what monitor can display. The usage of a histogram is necessary to understand what is going on with these types of files. The main advantage is that they can be of a really highwith any Flame and Smoke tools supporting Motion Vectors. There are currently two tools applying the conversion: Motion Convert and Motion Blur. In both tools, the conversion requires manual interaction because, in essence, normalized vectors signify that the pixel displacement has been compressed in a limited colour range.The H.264/MPEG-4 AVC standard defines motion vector as:

Motion Vector: A two-dimensional vector used for inter prediction that provides an offset from the coordinates in the decoded picture to the coordinates in a reference picture.

4. METHODOLOGY

Here, Huffman coding is used to encode the secret message, and then the encoded message is embedded on the least significant bit (LSB) of the pixel frame using parity coding (See section 4.2).

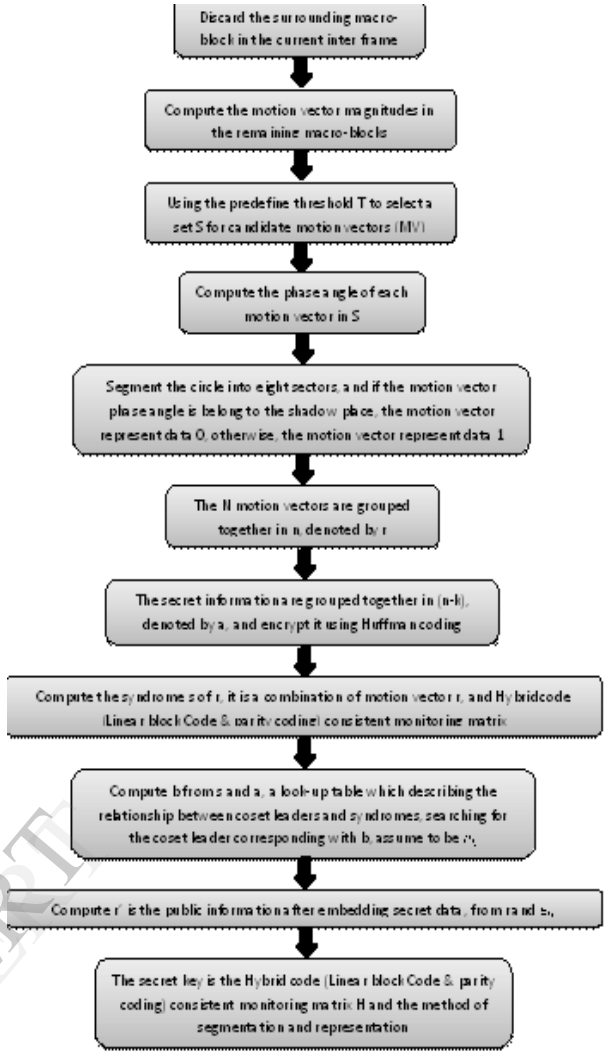

Figure 4.1: Flow diagram for Embedding

The work flow for embedding and extraction are given below in Figure 4.1 and Figure 4.2 The receiver gets the steganography video and recovers the secret information using the secret key. The extraction process is as follows: The step 1-6 is the same with the embedding process, thus the receiver gets r' .This research deals with data hiding in compressed video. Unlike data hiding in images and raw video which operates on the images themselves

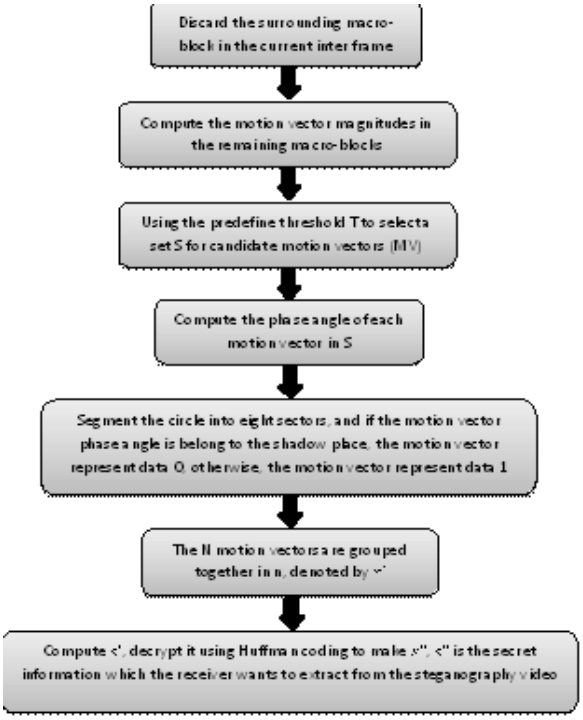

Figure 4.2: Flow diagram for Extraction

in the spatial or transformed domain which are Vectors used to encode and reconstruct both the forward predictive (P)-frame and bidirectional (B)-frames in compressed video. The choice of candidate subset of these motion vectors are based on their associated macro block Mean squared error, which is different from the approaches based on the motion vector attributes such as the magnitude and phase angle, etc.

A greedy adaptive threshold is searched for every frame to achieve robustness while maintaining a low prediction error level. The secret message bit stream is encoded through Huffman coding and embedded in the least significant bit of both components of the candidate motion vectors.

5. CONCLUSION

Digital Steganography is a fascinating scientific area which falls under the roof of security systems. This synopsis presents a secure and robust steganography method for the H.264 (MPEG-4 Part 10) standard. Besides the better security and robustness, these approaches have advantages of the state-of-the-arts of steganography solutions to video data. Additionally, we examine the reliability of PSNR, a principal measure used to evaluate the performance of steganography methods through measuring the quality of their stego-video. These methods have better PSNR as compare to conventional ones.

6. REFERENCES

[1] XikaiXu, Jing Dong, Wei Wang, Tieniu Tan, "Video Steganalysis Based On The Constraints Of Motion Vectors", IEEE, International Conference on Image Processing (ICIP), pp. 4422-4426, September 2013.

[2] Hemant Gupta, Dr.SetuChaturvedi, "Video Steganography through LSB Based Hybrid Approach", International Journal of Engineering Research and Development, PP. 32-42, Volume 6, Issue 12, May 2013.

[3] Tintu E. R., T. BlesslinSheeba, "Improved Video Steganography Using Inter Pixel Value Coding", International Journal of Research in Engineering & Advanced Technology (IJREAT),ISSN: 2320 – 8791, Volume 1, Issue 1, March, 2013.

[4] Andreas Neufeld and Andrew D. Ker, "A Study of Embedding Operations and Locations for Steganography in H.264 Video", Proc. SPIE 8665, Media Watermarking, Security, and Forensics, March 2013.

[5] B. Suneetha, Ch.HimaBindu, S. Sarath Chandra, "Secured Data Transmission Based Video Steganography", International Journal of Mechanical and Production Engineering (IJMPE), ISSN No.: 2315-4489, Volume 2, Issue 1, PP. 78-81, 2013.

[6] Deepika R. Chaudhari, RanjitGawande, "Data hiding in Motion Vectors of Compressed Video Based On their Associated Prediction Error", International Journal of Emerging Technology and Advanced Engineering (IJETAE), ISSN 2250-2459, Volume 2, Issue 10, PP. 586-590, October 2012.

[7] A. Swathi, Dr. S. A. K. Jilani, "Video Steganography by LSB Substitution Using Different Polynomial Equations", International Journal of Computational Engineering Research (ijceronline.com) Vol. 2, Issue. 5, ISSN: 2250-3005, PP. 1620-1623, September 2012.

[8] ThonduruMadhavi, Vijayalakshmi, "Stenography Analysis on Compressed Video Based on Prediction Motion Error", International Conference on Advancement in Engineering Studies & Technology, ISBN: 978-93-81693-72-8, PP. 107-112, July, 2012.

[9] NeethuPrabhakaran, D. Shanthi, "A New Cryptic Steganographic Approach using Video Steganography", International Journal of Computer Applications, PP. 0975 – 8887, Volume 49, No.7, July 2012.

[10] AbhishekMangudkar, PrachiKshirsagar, VidyaKawatikwar, UmeshJadhav, "Data Hiding Technique using Steganography and Dynamic Video Generation", International Journal of Scientific & Engineering Research, ISSN: 2229-5518, Volume 3, Issue 6, June 2012.

[11] Gandharba Swain, Saroj Kumar Lenka, "A Technique for Secret Communication Using a New Block Cipher with Dynamic Steganography", International Journal of Security and Its Applications, Vol.6, No2, April, 12.

[12] KousikDasgupta, J. K. Mandal, Paramartha Dutta, "Hash Based Least Significant Bit Technique For Video Steganography(HLSB)", International Journal of Security, Privacy and Trust Management (IJSPTM), Vol. 1, No 2, April 2012.

[13] Siddharth Tiwari, Prashant Kumar Koshta, "A Novel Information Security Scheme by Creptic Video Stegnography", International Journal of Computer Technology and Electronics Engineering (IJCTEE), ISSN: 2249-6343, Volume 2, Issue 1, PP. 65-69, February 2012.

[14] P. Paulpandi, Dr. T. Meyyappan, "Hiding Messages Using Motion Vector Technique in Video Steganography", International Journal of Engineering Trends and Technology, Volume 3, Issue 3,ISSN: 2231-538, PP. 361-365, 2012.