Improved Video Steganography Using Inter Pixel Value Coding

Tintu.E.R[1] & T.Blesslin Sheeba[2]

[1]PG Scholar, Department of of Electronics & Communication and Engineering

[2]Professor, Department of Electronics & Communication and Engineering

RMK Engineering College, Kavaraipettai, Anna University, Chennai

Abstract-- Steganography is the art of hiding information in ways that avert the revealing of hiding messages. This paper proposes a new efficient Video Steganography scheme. The design of algorithm enhances the entropy of the data scheme. To enlarge the capacity of the hidden secret information and to provide an imperceptible stego-image for human vision, a steganography approach called using inter pixel value coding (IPV) is used for embedding. The advantage of this algorithm is we need no decompression schemes for retrieval of data. Arnold transformation is performed to scrambles the secret image.

This method is based on the real-time hiding of information in Video steganography. This method of steganography is very similar to the two dimensional image steganography. A new type of compressed video secure steganography (CVSS) algorithm is proposed. In this algorithm, embedding and detection operations are both executed entirely in the compressed domain, with no need for the decompression process. The results show that the proposed algorithm for modified steganography is highly secured with certain strength in addition to good perceptual invisibility. Here we took some effort to prove the entropy of given algorithm is better than the existing one.

Keywords: Steganography, Arnold transformation, Inter Pixel Value Coding

1. INTRODUCTION

Steganography is the science that involves communicating secret data in an appropriate multimedia carrier, e.g., image, audio, and video files. It comes under the assumption that if the feature is visible, the point of attack is evident, thus the goal here is always to conceal the very existence of the embedded data and it has various useful applications.

Steganography's ultimate objectives and the main factors that separate it from related techniques such as watermarking and cryptography are un detectability, robustness (resistance to various image processing methods and compression) and capacity of the hidden data. Further those Schemes are being designed to address the requirements of very different kinds of applications, e.g. internet, color facsimile, printing, scanning, digital photography, remote sensing, mobile applications, medical imagery, digital library, military application and e-commerce.

The present study shows to achieve fastest compression and decompression techniques in video steganography using Arnold Transformation and Diamond search based Motion Estimation. The main organization of the paper includes the following (i)Proposes a new Compressed Video Secure Steganography (CVSS) algorithm(ii)Due to increased entropy, image may also be added to the video using steganography(iii)Arnold transformation is used for scrambling the image(iv) Inter pixel value coding is assumed for faster coding.

2. RELATED WORKS

There are several methodology has been proposed. However, the proposed method involves different methods for various steganographic techniques.

A modified secure and high capacity based steganography scheme of hiding a large-size secret image into a small-size cover image and Arnold transformation is performed to scrambles the secret image. With the techniques for steganography in discrete wavelet transform as associated to gray scale image. [1]. The system is to provide a good, efficient method for hiding the data from hackers and sent to the destination in a safe manner and the method is secure in the way that even if the attacker detects and extracts the embedded message from the stego-image, one would not be able to recover the secret message without the encoded key[2].An algorithm is designed for motion vector component feature to control embedding, and also to be the secret carrier thus obtains higher carrier utilization and embedding efficiency, and also has large embedding capacity with good visual invisibility and statistical invisibility[3].The proposed algorithm can not only decrease the modification rate of motion vector, but also achieve high video quality and embedding capacity hence the secret information is hidden. Compared with other schemes the proposed steganographic scheme can not only keep highly

utilization rate but also reduce the modification rate of the motion vectors[4].A novel image steganography algorithm is designed based on the non-uniform rectangular partition algorithm. Different initial partitions, bivariate polynomials and control errors lead different partition codes thus the user can use different combination of them as the security key to enhance the security of the steganography algorithm [5]. The system is proposed with two novel approaches to hide the message and the quantization scale of a CBR video is either incremented or decremented according to the underlying message bit in the first approach. The second approach proposed includes both CBR and VBR coding for achieving a message [6]. A new data-hiding method in the motion vectors of MPEG-2 compressed video and the process includes embedding and extraction algorithms are implemented and integrated to the MPEG-2 encoder/decoder [7]. The work demonstrates the potential of framework and the use of temporal processing for effective steganalysis and the video steganalysis algorithm that takes advantage of the temporal redundancy present in the video [8].

3. STEGANOGRAPHY

Steganography is the technique of hiding confidential information within any media. Steganography is often confused with cryptography because the two are similar in the way that they both are used to protect confidential information. The difference between the two is in the appearance in the processed output; the output of steganography operation is not apparently visible but in cryptography the output is scrambled so that it can draw attention. The objective of steganography is to hide a secret message within a cover-media in such a way that others cannot discern the presence of the hidden message. Technically in simple words "steganography means hiding one piece of data within another".

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, the resulting product is a stego-image. A possible formula of the process may be represented as:

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

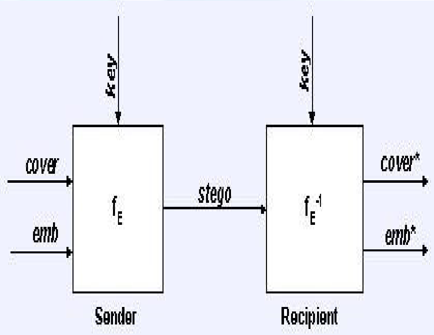

Figure 1.1 Graphical Version of the Steganographic System

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.

3.1 Modern Techniques

The common modern technique of steganography exploits the property of the media itself to convey a message. The following media are the candidate for digitally embedding message:

- Plaintext

- Still imagery
- Audio and Video
- IP datagram

3.1.1 Plaintext steganography

In this technique the message is hidden within a plain text file using different schemes like use of selected characters, extra white spaces of the cover text etc. A number of extra blank spaces are inserted between consecutive words of cover text. This numbers are mapped to a hidden message through an index of a lookup table. For example extra three spaces between adjacent words indicate the number "3" which subsequently indicates a specific text of a look-up table which is available to the both communicating parties as a prior agreement.

3.1.2 Still imagery steganography

The most widely used technique today is hiding of secret messages into a digital image. This steganography technique exploits the weakness of the human visual system (HVS). HVS cannot detect the variation in luminance of color vectors at higher frequency side of the visual spectrum. A picture can be represented by a collection of color pixels. The individual pixels can be represented by their optical characteristics like 'brightness', 'chroma' etc. Each of these characteristics can be digitally expressed in terms of 1s and 0s.

For example: a 24-bit bitmap will have 8 bits, representing each of the three color values (red, green, and blue) at each pixel. If we consider just the blue there will be 28 different values of blue. The difference between 11111111 and 11111110 in the value for blue intensity is likely to be undetectable by the human eye. Hence, if the terminal recipient of the data is nothing but human visual system (HVS) then the Least Significant Bit (LSB) can be used for something else other than color information.This technique can be directly applied on digital image in bitmap format as well as for the compressed image format like JPEG.

3.1.3 Audio and Video Steganography

In audio steganography, secret message is embedded into digitized audio signal which result slight altering of binary sequence of the corresponding audio file. There are several methods are available for audio steganography. They are

- LSB Coding
- Phase Coding
- Spread Spectrum
- Echo Hiding

Video files are generally consists of images and sounds, so most of the relevant techniques for hiding data into images and audio are also applicable to video media. In the case of Video steganography sender sends the secret message to the recipient using a video sequence as cover media. Optional secret key 'K' can also be used during embedding the secret message to the cover media to produce 'stego-video'. After that the stego-video is communicated over public channel to the receiver. At the receiving end, receiver uses the secret key along with the extracting algorithm to extract the secret message from the stego-object. The original cover video consists of frames represented by Ck(m,n) where 1 £ k £ N. 'N' is the total number of frame and m,n are the row and column indices of the pixels, respectively. The binary secret message denoted by Mk(m, n) is embedded into the cover video media by modulating it into a signal.

4. ARCHITECTURAL DIAGRAM

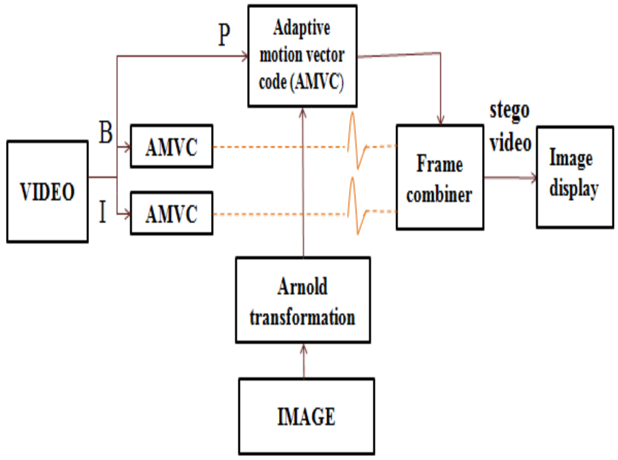

Figure 4.1 Architectural Diagram

The figure 4.1 shows architectural diagram of the proposed system. The video is captured and displayed using graphical user interface (GUI). Motion vector is adaptable based on luminance and embedded with lowest luminance values. The video is converted into frames. An image is embedded into the video and Arnold transformation is used for scrambling the image. Again frames are converted into video and the hidden image is extracted from the stego video. Motion estimation is the process of determining motion vectors that describe the transformation from one 2D image to another; usually from adjacent frames in a video sequence. It is an ill-posed problem as the motion is in three dimensions but the images are a projection of the 3D scene onto a 2D plane. The motion vectors may relate to the whole image (global motion estimation) or specific parts, such as rectangular blocks, arbitrary shaped patches or even per pixel. The motion vectors may be represented by a translational model or many other models that can approximate the motion of a real video camera, such as rotation and translation in all three dimensions and zoom.

5. SIMULATION RESULTS

5.1 Simulation results

The simulation is done with MATLAB (simulink). MATLAB is a programming language developed by Math Works. It is started out as a matrix programming language where linear algebra programming was simple. It can be run both under interactive sessions and as a batch job. Most MATLAB scripts and functions can be run in the open source program octave. This is freely available for most computing platforms.

Simulink, developed by Math Works, is a commercial tool for modeling, simulating and analyzing multi domain dynamic systems. Its primary interface is a graphical block diagramming tool and a customizable set of block libraries. It offers tight integration with the rest of the MATLAB environment and can either drive MATLAB or be scripted from it. Simulink is widely used in control theory and digital signal processing for multi domain simulation and Model-Based Design.

Simulink provides a graphical user interface (GUI) that is used in building block diagrams, performing simulations, as well as analyzing results.

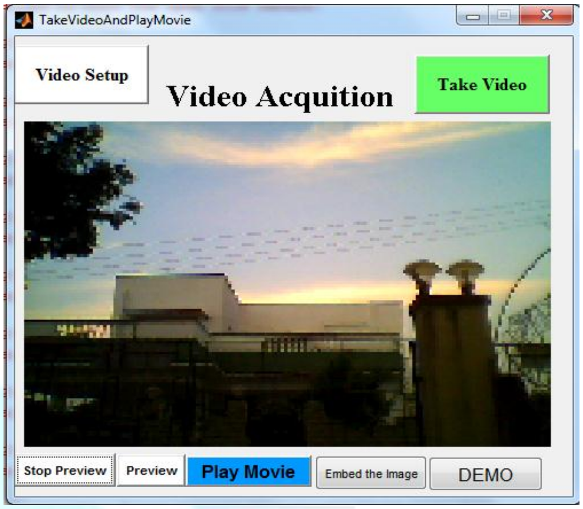

Figure 5.1 Take video and play movie

This figure 5.1 shows the graphical user interface (GUI) for take video and play movie setup. Using this setup, the video is captured and the preview is displayed. After capturing the video an image is embedded into this video.

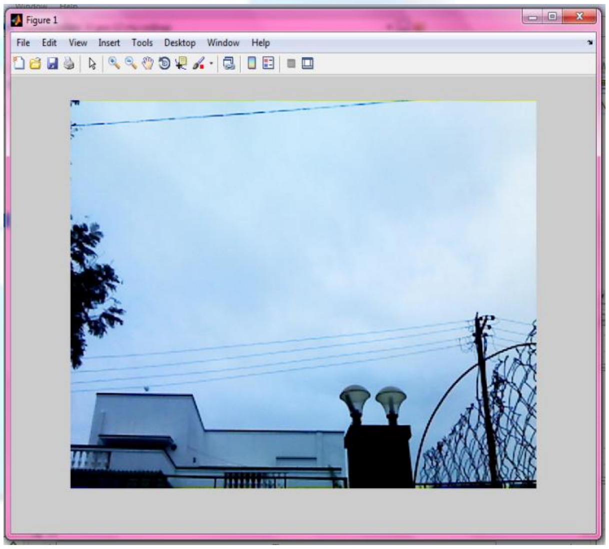

Figure 5.2 Steganographic creator

Figure 5.2 shows steganography creator, which shows a preview of video where the image is stored. Here the video is converted into frames and vice versa. The embedding image is scrambled using arnold transformation.

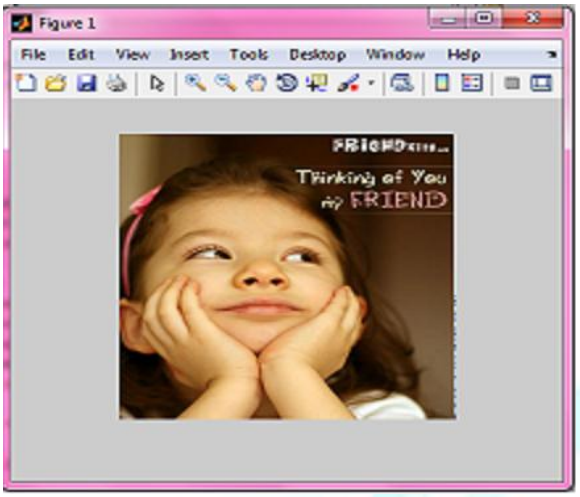

Figure 5.3 Hidden image display

Figure 5.3 shows the hidden image display. The original image is extracted from the stego video. Thus the experimental results demonstrate that the proposed algorithm has high imperceptibility and capacity.

6. CONCLUSION

This method is based on the real-time hiding of information in Video steganography. This method of steganography is very similar to the two dimensional of image steganography. In this paper, a video steganography algorithm based on motion vectors and matrix encoding was proposed to hide secret information. A new type of compressed video secure steganography (CVSS) algorithm is proposed. In this algorithm, embedding and detection operations are both executed entirely in the compressed domain, with no need for the decompression process. The new criteria employing statistical invisibility of contiguous frames is used to adjust the embedding strategy and capacity, which increases the security of proposed algorithm. Therefore, the collusion resistant properties re obtained. In addition, this method gives more capacity and high security to transfer images in communication field. Experimental results show that our method gets stego-image with perceptual invisibility, high security and certain robustness. In this paper, a video steganography algorithm using Arnold Transformation and Diamond search based Motion Estimation was proposed.

As for the further work, an effective method of video steganography in FPGA using inter pixel value coding (IPV) is implemented. The results show that the proposed algorithm for modified steganography is highly secured with certain strength in addition to good perceptual invisibility.

REFERENCES

1. Prabakaran, G.; Bhavani, R.(2012) "A modified secure digital image steganography based on Discrete Wavelet Transform " , Computing, Electronics and Electrical Technologies (ICCEET), 2012 International Conference on Digital Object Identifier: 10.1109/ICCEET.2012.6203811.

2. V.Sathyal,K.Balasuhramaniyam,(2012)"Digital Video Steganalysis Exploiting Statistical Visibility in the Temporal Domain" IEEE-International Conference On Advances In Engineering, Science And Management (ICAESM-2012).

3. Wang Jue; Zhang Min-qing; Sun Juan-li . (2011)"Video steganography using motion vector components", Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on Digital Object Identifier: 10.1109/ICCSN.2011.6013642.

4. HAO-BIN,ZHAO LI-YI, ZHONG Wei-Dong(2011) "A Novel Steganography Algorithm Based on Motion Vector and Matrix Encoding"Key Laboratory of Network & Information Security of APF, Engineering College of APF, Xi'an 710086,China.

5. ShengDun Hu, KinTak U (2011) "A Novel Video Steganography based on Non-uniform Rectangular Partition" Faculty of Information Technology Macau University of Science and Technology Macau, China.

6. Tamer Shanableh (2011) "Data Hiding in MPEG Video Files Using Multivariate Regression and Flexible Macroblock Ordering" IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 7, NO. 2.

7. Hussein A. Aly, *Member, (*2011) "Data Hiding in Motion Vectors of Compressed Video Based on Their Associated Prediction Error" IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 6, NO. 1.

8. Udit Budhia, Deepa Kundur , (2006)"Data Hiding in audio signal, video signal text and JPEG images" IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 1, NO. 4.