Breaking the Digital Video Steganography

Yueqiang Li*[1], Qiuju Liu[2]
[1]Department of Public Teaching, Huaihua Medical College
Huaihua City, China, Ph./Fax: +86 0745-2383280/2385075
[2]Department of Foreign Languages and Culture, Huaihua University
Huaihua City, China, Ph./Fax: +86 0745-2864039/2854961
Corresponding author, e-mail: liyueqiang@163.com[1], annelqj @yahoo.com.cn[2]

Abstract

In this paper we provide a new digital video steganalysis algorithm. When frames of the cover video are embedded with secret messages, both number of connected component and number of holes will change dramatically, thus Euler number of the stego-frame will has pulsing increase. This proposed steganalysis algorithm is applied to stego-video, estimating steganographic algorithm for frames chosen and estimating steganographic capacity. Experimental results indicate that it's much simpler and faster, more sensitive and robust, steganography rate as small as 0.0154% can be reliably detected. It's effective and efficient to detect any format video, because this algorithm is only correlated with the connected components number and holes number of the frames.

Keywords*: steganography, steganalysis, digital video, Euler number*

1. Introduction

With the fast development of multimedia information technology, as well as cyber technology, information security has gained more attention than ever. Since the early 1990s, information hiding has emerged as an increasingly active research area. There has been an increased interest both in digital watermark for the purpose of intellectual property protection, and in steganography for the purpose of covert communication.

With the advent of steganographic techniques, there have been fatal threats to cybersecurity. Thus in the fields of cybersecurity, there exists an increased interest in steganalysis, i.e. the science of identifying steganographic secret message. In the future steganography vs steganalysis will emerge as the focus of cybersphere.

There are two steganalysis approaches, including qualitative steganalysis[1] and quantitative steganalysis[2]. Qualitative steganalysis aims to detect the existence of steganographic secret message, while quantitative steganalysis based on qualitative steganalysis aims to estimate the capacity[3], to decode the secret key[4], to guess the steganographic algorithm**Error! Reference source not found.**, ultimately, to extract the hidden information.

Steganalysis aims to discover the hidden information from a given cover media. However, it's quite difficult. There are three main challenges. Firstly, there exist wide availability of covers, such as digital video, image, audio, text etc. Secondly, there exist large numbers of covers. Thirdly, there exist wide range of algorithms. Thus it's rather difficult to detect the hidden information from the covers. Therefore the primary goal of steganalysis is qualitative steganalysis. Although the hidden information cannot be retrieved by qualitative steganalysis itself, once the existence of the steganographic data is discovered, the purpose of covert communication can be prevented via deletion and active attack, etc.

2. Digital Video Steganalysis

2.1 Euler Number

Euler number of image (frame) is one of the most important characteristics in topological, it remains invariant under translation, rotation, scaling, and rubber sheet transformation of the image.

Received December 19, 2012; Revised January 27, 2013; Accepted February 10, 2013

The Euler number is defined as Equation 1 below [6]:

$$E=C-H \quad (1)$$

Where C is number of connected components. H is number of holes. Holes are the background region based on the foreground of the border. E is Euler number.

2.2 Qualitative Steganalysis

The digital video is composed of a series of still images, these images are called frames. Usually scenes in a shot change little, thus the Euler number of the frames changes indistinctively.

Once digital video frames are embedded with secret information, usually the data of the frames will be modified, C and H will change distinctively, Thus Euler number of the stego-frame will has pulsing increase. Therefore this approach can be exploited to detect the existence of steganographic secret message.

After digital video frames are embedded with hidden information, in order to detect changes of the Euler number, we choose 2 video samples. Sample 1, 500 frames, 360×288 pixels, 25fps, AVI, none video compression, true colour. Sample 2, 372 frames, 720×576 pixels, 25fps, AVI, DX50 video compression, true colour.

Secret information is respectively embedded in the frames of 10th, 20th, 30th ,…, the steganography rate of frames is 10%.

Cover media is embedded with 40 × 40, 32 × 32, 24 × 24, 16 × 16, 8 × 8 pixels monochrome BMP images respectively.

Steganographic algorithm is as follows:

To transform successive 8 × 8 pixel blocks of the frame, the secret message has been embedded into intermediate frequency of the DCT coefficient, thus resulting in 5 stego-videos for each sample.

To detect respectively the 2 samples Euler number and the 10 stego-videos Euler number, results are as shown in Fig. 1, Fig. 2, Fig. 3, Fig. 4. To observe clearly and vividly, results of frames from 1st to 100th are shown.

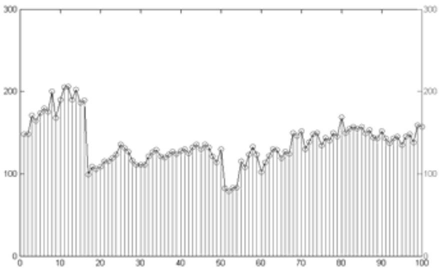

Figure 1. Sample 1. cover-object Euler number

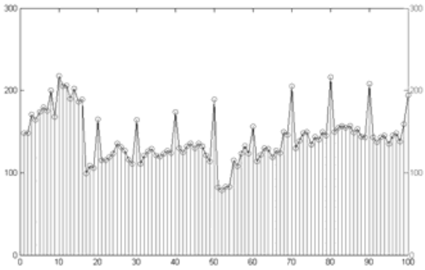

Figure 2. Sample 1. 40×40 stego-object Euler number (steganography rate 1.54%)

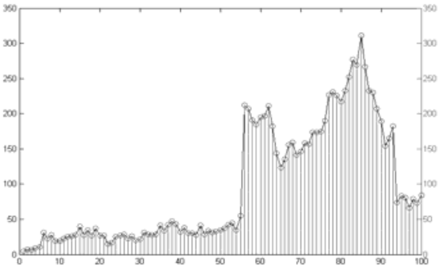

Figure 3. Sample 2. cover-object Euler number

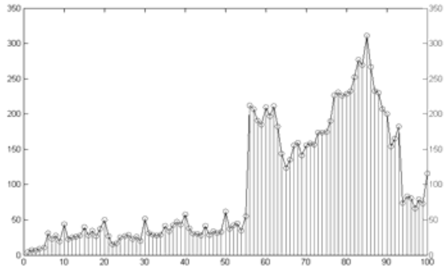

Figure 4. Sample 2. 40×40 stego-object Euler number (steganography rate 0.0154%)

As for Sample 1, embedded with 40 × 40, cover-object Euler number and stego-object Euler number are demonstrated respectively in Fig. 1 and Fig. 2, steganography embedding rate is 1.54%. As for Sample 2, embedded with 8×8, cover-object Euler number and stego-object Euler number are demonstrated respectively in Fig. 3 and Fig. 4, steganography embedding rate is 0.0154%.

As shown in Fig. 2, Fig. 4, once some frames are embedded with secret information, we can compare the cover-frame Euler number with the stego-frame Euler number, the stego-frame Euler number will has pulsing increase, the increase pace is 5 to 400. Additionally, more embedded, larger is the pace.

Pulsing increase of Euler number is evaluated by Equation 2 below

$$D=Ei-(Ei-1+Ei+1)/2 \tag{2}$$

Where Ei is Euler number of Frame i, Ei-1 is Euler number of Frame i-1, Ei+1 is Euler number of Frame i+1, D is difference.

If D is greater than or equal to limit，then Frame i is embedded with covert information.

To detect respectively the 5 stego-videos of Sample 1，utilizing limits 10, 20, 30, 40 and 50.

To evaluate the result, this paper adopts the following standards:

Detectable rate P1 is given by Equation 3 below

$$P1=M1/M \tag{3}$$

Where M1 is detected stego-frame, M is embedded stego-frame

Missing report rate P2 is given by Equation 4 below

$$P2=M2/M \tag{4}$$

Where M2 is detected non-stego-frame, M is embedded stego-frame.

False alarm probability P3 is given by Equation 5 below

$$P3=N1/N \tag{5}$$

Where N1 is detected non-stego-frame, N is non-stego-frame.

As shown in Table 1, Detectable rate P1max= 94%, Missing report rate P2min=6%, False alarm probability P3min=0.89%.

Take the three rates into consideration, the appropriate limit is 20 to 40. Limit increases with the capacity of the cover-frame.

2.3 Estimating Steganographic Algorithm for Frame Chosen

The distribution of the covert information can be easily judged from the figure of the sample Euler number. Thus it’s possible to estimate the steganographic algorithm for frame chosen.

The distance between the stego-frames is constant, which is called fixed steganographic algorithm for frame chosen.

The distance between the stego-frames is variable, which is called non-fixed steganographic algorithm for frame chosen, selected by some eigenvalues, for instance, independent component analysis(ICA) [7]，motion vector[8], skewness[9], kurtosis[10],Euler number etc.

2.4 Estimating Steganographic Capacity

As shown in Fig. 2, Fig. 4, frames are embedded with different capacities of covert information, Euler number increases with the capacities.

To evaluate and calculate non-stego-frame Euler number and stego-frame Euler number of the 5stego-videos of Sample 2 on average respectively. Results are shown in Table 2.

As shown in Table 2., Euler number increases with the capacities of covert information embedded in frames. Furthermore, Euler number increases in proportion to the capacities of covert information. i.e. Euler number increases approximately linearly as capacities increase.

The experiments show that the increase of Euler number is closely related to not only the capacity but also the distribution of the secret information. If it’s evenly distributed in the frames, then Euler number increases distinctively on average. If it’s unevenly distributed in the frames, then Euler number increases indistinctively on average.

Relation between estimating capacity and increase of average Euler number is shown in Table 3.

3 Simulation Results

Utilizing the proposed approach, we make a simulation detection based on the steo-video of Sample 3. Sample 3, 720×576 pixels,282 frames, 25fps, AVI, DX50 video compression, true colour.

Detection methods are as follows.

Step 1 : Qualitative steganalysis. As shown in Fig. 5 is Sample 3.Euler number. When observe Fig. 5 carefully, we find that Euler number increases sharply in some frames. To be more objective, Equation 2 is used as screening condition. Due to the large capacity of Sample 3 (720 ×576 pixels), if D⩾40, then 37 frames are qualified. Therefore the result is that secret information is embedded in Sample 3.

Table 1. Results of the 5 stego-videos of Sample 1.

Capacity	Limit	P1	P2	P3
40×40	D≥10	86.00%	86.00%	9.56%
	D≥20	84.00%	48.00%	5.33%
	D≥30	82.00%	22.00%	2.44%
	D≥40	68.00%	16.00%	1.78%
	D≥50	54.00%	8.00%	0.89%
32×32	D≥10	88.00%	140.00%	16.00%
	D≥20	86.00%	50.00%	5.56%
	D≥30	74.00%	22.00%	2.44%
	D≥40	54.00%	20.00%	2.22%
	D≥50	38.00%	8.00%	0.89%
24×24	D≥10	94.00%	136.00%	15.11%
	D≥20	86.00%	44.00%	4.89%
	D≥30	70.00%	16.00%	1.78%
	D≥40	52.00%	14.00%	1.56%
	D≥50	32.00%	6.00%	0.67%
16×16	D≥10	94.00%	136.00%	15.11%
	D≥20	80.00%	42.00%	4.67%
	D≥30	66.00%	16.00%	1.78%
	D≥40	46.00%	14.00%	1.56%
	D≥50	20.00%	8.00%	0.89%
8×8	D≥10	86.00%	136.00%	15.11%
	D≥20	70.00%	44.00%	4.89%
	D≥30	50.00%	16.00%	1.78%
	D≥40	20.00%	14.00%	1.56%
	D≥50	14.00%	8.00%	0.89%

Table 2. Capacities & effects on Euler number

Capacities	Average Euler number of non-stego-frame	Average Euler number of stego-frame	Increased Average Euler number of stego-frame
40×40	143.07	244.95	101.88
32×32	143.07	218.35	75.28
24×24	143.07	201.19	58.12
16×16	143.07	189.95	46.88
8×8	143.07	157.27	14.20

Table 3. Capacities & effects on Euler number

Capacities	Increase of average Euler number	
(bit)	Even distribution	Uneven distribution
1000~2000	80~120	180~230
500~1000	50~80	130~180
200~500	30~50	80~130
50~200	10~30	30~80

Table 4. Results of Sample 3

P1	P2	P3
92.11%	2.63%	0.40%

Step 2 : Estimating steganographic algorithm for frame chosen. According to Fig. 5 and the screening results, we find out that Sample 3 has two properties. Secret information is embedded in every other frame in some shots. Therefore the estimating algorithm for frame chosen is based on even / odd frames. While in some other shots, nothing is embedded in. Therefore the estimating algorithm for frame chosen is based on eigenvalues of frames and even / odd frames.

Step 3 : Estimating steganographic capacity. In Sample 3, the 37 stego-frames Euler number is 382.51, while the non-stego-frames Euler number is 181.17, the Euler number is increased by 201.34 on average. According to Table 3, the capacity is 500 to 2000 bit.

In fact, in Sample 3 there are 38 stego-frames in 282 cover-frames, each embeded capacity is 32×32bit.

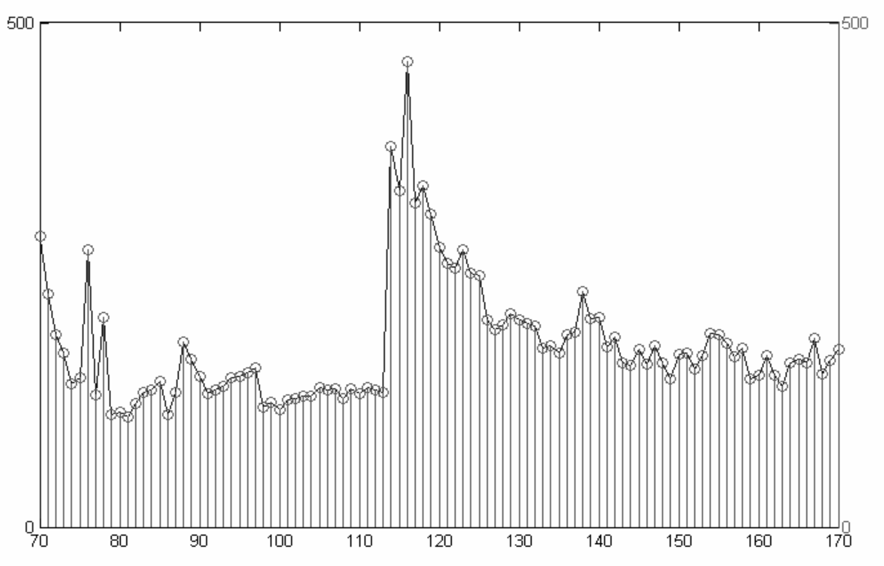

Figure 4. Sample 3.Euler number

Steganographic algorithm is as follows:

Do not name the stego-frames, but to select the qualified frames whose kurtosis eigenvalue is greater than 20 as well as even number frames. As for V component of HSV color space, to transform successive 8 × 8 pixel blocks of the frame, the secret message has been embedded into intermediate frequency of the DCT coefficient, each is embedded with 1 bit.

P1,P2 and P3 are shown in Table 4.

As shown in Table 4, Steganalysis result is reliable.

4. Conclusion

Euler number is sensitive to image data, once the frames is modified, Euler number will has pulsing increase, it can be applied to video and image steganalysis. It's much simpler and faster, more sensitive and robust, steganography rate as small as 0.0154% can be reliably detected. Euler number has topological characteristics, it remains invariant under translation, rotation, scaling, and rubber sheet transformation of the image. Therefore, this proposed steganalysis algorithm is robust. This algorithm is effective and efficient to detect any format video, because it is only correlated with the Euler number of the frames.

Acknowledgment

The work on this pager is supported by Hunan Provincial Science & Technology Department of China(No. 2012GK3033).

References

[1] Andrew D. Ker. *Fourth-order structural steganalysis and analysis of cover assumptions*. In Security, Steganography and Water-marking of Multimedia Contents VIII. 2006; 6072: 25–38.

[2] Jan Kodovsky, Jessica Fridrich. *Quantitative steganalysis of LSB embedding in JPEG domain*. in Proc.12th ACM Workshop on Multimedia and Security. Roma. 2010: 187–198.

[3] Farzin Yaghmaee and Mansour Jamzad. Estimating watermarking capacity in gray scale images based on image complexity. *EURASIP Journal on Advances in Signal Processing.* 2010: 1–9.

[4] J. Fridrich, M. Goljan and D. Soukal. *Searching for the stego key.* In. Proc. SPIE, Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents VI. 2004; 5306:70-82.

[5] J. Fridrich, M. Goljan, and D. Hogea. *Steganalysis of JPEG images: breaking the F5 algorithm.* In: F. A. P. Petitcolas (ed.), Proc. of Information Hiding, 5th Int. Workshop, IH 2002, Noordwijkerhout, The Netherlands, LNCS 2003;2578:310-323.

[6] X.Lin, Y. Wu, D. Fu, W.Qian. Analysis of computation complexity on Euler Number of binary image. *Journal of Microelectronics & Computer*. 2007; 25(7):14-16.

[7] S. Bounkong, B. Toch, D. Saad, and D. Lowe. ICA for watermarking digital images. *Journal of Machine Learning Research*. 2002; Vol.1:1–25.

[8] J. Zhang, J. Li, and L. Zhang. *Video watermark technique in motion vector.* In Proc. 14th Computer Graphics and Image Processing. Brazilian Symp. 2001: 179–182.

[9] ZHOU Zhi-yuan, LI Yue-qiang, SUN Xing-ming. Video watermarking algorithm based on skewness. *Journal of Computer Engineering and Application.* 2008; 44(25):96-195.

[10] LI Yue-qiang, QUAN Tong-gui, ZHOU Zhi-yuan, SUN Xing-ming. Application of kurtosis eigenvalue in video watermarking. *Journal of Computer Engineering and Applications*. 2009; 45(14):90-92.