An Adaptive Video Digital Steganography Algorithm

Guangqi Liu, Lianhai Wang, Shuhui Zhang, Shumian Yang, Qiuxiang Guo

Shandong Computer Science Center (National Supercomputer Center in Jinan), Shandong Provincial Key Laboratory of Computer Networks, Jinan 250014, China, liuguangqi@sdas.org

Keywords: Digital steganography; Adaptive algorithm; System Security.

Abstract

In this paper, we propose an adaptive video digital steganography algorithm, it mainly includes information steganography and information extraction of two parts. Information steganography is mainly includes three steps, first to split video file into the I frame, B&P frame. Second we divide B&P frame into 16×16 block, choose the big macro block of motion vector as secret information embedding location, at the same time divide I frame into 8×8 block, select the texture region as the location of the control information steganography. Third, embed secret information in B&P frame, embed control information in I frame. The control information is occurring in the process of secret information embedding position information and number of embeded frame, etc. Extract part of the algorithm, first split the video file into I frame, B&P frame. Then, we divide I frame into 8×8 block and extract the control information in the texture region. Third, we extract the secret information in the B&P frame by the corresponding position embedding algorithm and control information. The algorithm is effective to solve the problems of greater influence on the quality and small embedded capacity. The algorithm not only has strong adaptability, but also can greatly improve the security of the system.

1 Introduction

With the rapid development of computer technology and network communication technology, more and more people through the network to obtain all kinds of information conveniently, e-commerce, e-government and network office has become a modern society in colleges and universities is indispensable in operation works, E-mail, online chat, BBS, blog, microblog, WeChat become the new way of daily communication. However, the internet give people bring convenient while, also brought the information security challenges: involving national security, the government can confidential files on the network security of transmission; whether corporate secrets hidden in the electronic commerce business spy stealing. Personal privacy, such as account number and password can be security. How to solve a series of security problems become a research hot spot in the current and even quite a long period of time.

As a new research direction in the field of information security technology, information hiding for the security of multimedia information on the network, storage and transport has opened up an effective way, has received the widespread attention of the academic and business circles. Digital steganography algorithm as a branch of information hiding[1~4], that has its own unique advantages in the field of information security technology. Due to the screen for the carrier of the public, external performance are the content and characteristics of the carrier signal, the application value of the carrier has not changed, it has stronger information security, the third party is difficult to detect the existence of secret information. With the development of network and multimedia technology, video transmission is more and more widely, network video strong momentum of development, for the application of digital steganography provides a huge space. Large capacity, wide spread make video have more potential than digital image steganography carrier, the network has caused wide public concern, video steganography[5~8] analysis algorithm began to emerge in recent years.

However digital steganography techniques is a double-edged sword, it not only can be used in public communication network to transfer national political, economic, safe and reliable information, but also be used by the enemy spy agencies or terrorist organization for planning and organizing criminal activities, such as they make the public information network undermined social stability, endangering state security and public security communication tools. Since the "9.11" incident, the use of public information network to the image data, voice, video and other digital media as a carrier for secret communication, that engaged in undermining social stability and harm social security illegal activities have caused extensive concern of governments and the public. In the digital steganography techniques, the carrier of hidden information can be still images, video, audio, text and other files on the network transmission [9~11].

Video compression technology and the development of network streaming media business, make video application scope is more and more wide, at the same time, with the growing popularity of the home video, and a variety of video editing software application is easy to operate, so people can be convenient for video recording, editing and publishing on the Internet and communication. Video transmission on the network is more and more common. Therefore, video as a common form of digital media has become an important carrier of the digital steganography. Because of its large amount of data is complex, rich in content and the characteristics of statistics.

2 Algorithm design

Badura Stanislaw[12] put forward a method of combining the embedding information by using VLC and DCT, and uses an adaptive AC coefficient method to reduce the impact on the quality of video embedding procedure. At the same time, extract the information needed to control information embedded into audio signal, thus improved steganography security.Daniela Stanescu[13] put forward that only embed information in I frame DCT coefficients not in P, B frames. He believed that P and B frame compared with the I frame smaller energy, to achieve a larger embedding capacity and less effect to the video, the algorithm is more demanding and easy to deviate from the video compression standards.Dai[14] put forward a mpeg-2 video embedded in the message to the large amplitude motion vector in the embedding method. According to the characteristics of human visual system, such as sensitivity to fast moving objects, high sensitivity to slow motion objects. The analysis says the greater amplitude of motion vector shows the location of the macro block move faster, in case the same modifier, modifying greatly amplitude of the motion vector is smaller than modify motion vector is not easy to detect.Zhang Weiming[15], fully use the embedded secret information bits, obtain higher embedding efficiency, under the same amount of embedded into better concealment.

Although the researchers have proposed many video digital steganography algorithm, but the concealment of embedding capacity algorithm can be improved in the very large space. Video digital steganography techniques are the mainstream of development direction in the field of multimedia information security. That can be widely used in the Internet, e-commerce, online audio and video on demand, remote teaching, advertising, monitoring and other business and so on. The research has important application value and the huge economic benefits.

At the same time, in this digital era, video digital steganography techniques research has the extremely broad prospect of industrialization, that can not only keep up with the domestic information security industry to promote the development of the situation but also can bring significant social and military benefits.

An adaptive video digital steganography method is proposed in this paper in order to overcome the shortage of the existing technology. This method adaptability is strong, simple operation, reliable performance. That can effectively solve the video steganography questions of greater influence on the video quality and the small information embedded capacity in the process.

3 Steganography algorithm

Information steganography process includes the following steps.

a. Decomposition video files, video file is brown down into I frame, B&P frame according to the corresponding decoding format, and get the GOP information.

b. Choose fast macroblock motion, put B&P frame to 16×16 pixel size of macro block; Then according to the size of the macro block motion vector, select the rapid movement of the macro block, set H_i , V_i as motion vector horizontal component and vertical component of macro block divided from B&P frame, ε as meet the conditions of the macroblock motion vector threshold; Can choose according to the following method to macro block:

b-1. Compared with the size of the $\sqrt{H_i^2 + V_i^2}$;

b-2. If $\varepsilon > \sqrt{H_i^2 + V_i^2}$, the macro block meet the conditions for fast moving macro block, the horizontal component and the vertical component of the motion vectors can be to embed secret information;

b-3. If $\varepsilon \le \sqrt{H_i^2 + V_i^2}$, the macro block does not comply with the conditions of macro block, these motion vectors should not embed secret information;

c. Selecting texture area, put I frame according to 8×8 the pixel size of block, according to the texture region determine conditions to select the area.

d. Embed secret information, embed the secret information and key in the motion vector of the selected steps b, form the B&P steganography secret information frame; At the same time produce control information with the process of embed secret information. Control information generated in this step including: B&P frames in video GOP index, B&P frame sitting in a GOP index number, select the macro block in B&P frame location and the index number, number of motion vector implicit writing conditions.

e. Embed control information: embed the control information to texture area of I frame, that generated in step d step c;

f. Synthetic new video file, wrote a secret hidden information steganography in B&P frame and control information in the I frame synthetic new video files.

Among them, the video file is divided into three categories with MPEG codec encoding image respectively called I frame, P frame and B frame, at the time it is divided into multiple video files of GOP, each GOP contains an I frame and multiple B frame, P frame. I frame adopts frame coding method, i.e. using only a single frame image in the spatial correlation, and no use of time. P frame and B frame adopts inter frame coding method, i.e. at the same time, on the use of space and time correlation. P frame the prediction to the time before, only can improve the image quality and compression efficiency, B frame adopts two-way time prediction, can greatly improve the compression ratio.

The algorithm block diagram in figure 1 as shown.

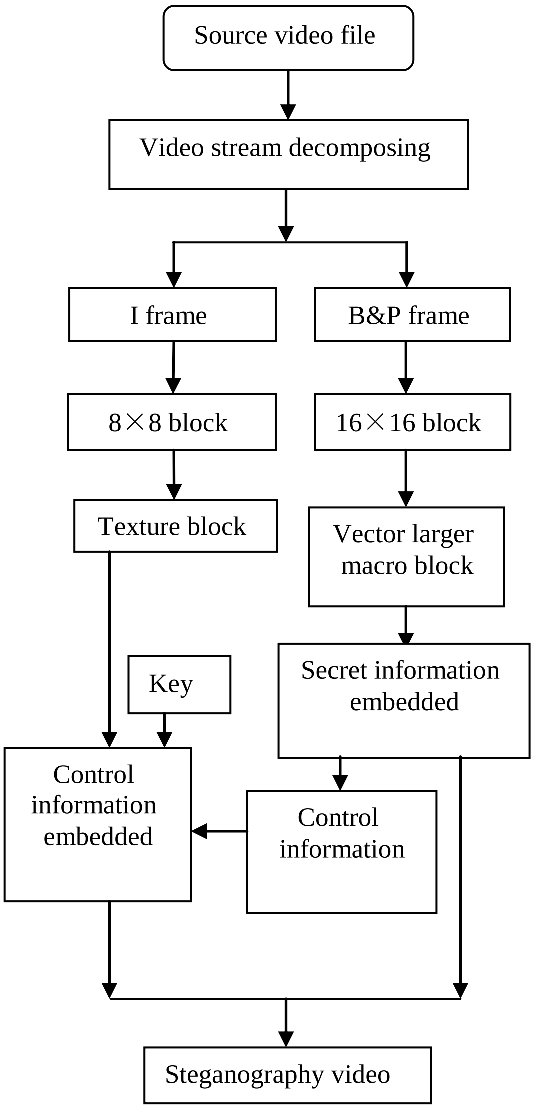

Figure 1: Diagram of steganography algorithm

Steps b, the macro blocks are the zone of rapid movement faster area of the object, the interval between frames change is bigger, because of its rapid movement, the human eye sensitivity is low, these regions steganography information not easy to be found in the region. Movement area selection principle is fast, set the horizontal component and vertical component of each block H_i and V_i , respectively, among them i is choose the i macro block, if the values $(H_i^2+V_i^2)^{1/2}$ for each macro block margin f_i , that is $f_i=(H_i^2+V_i^2)^{1/2}$, we compare f_i and setting threshold ε , if $f_i \succ \varepsilon$, then determine the region is fast sports area, suitable for steganography secret information, the opposite is not suitable for steganography information.

Step c, methods to determine the texture area of I frame: the image texture area is some local image texture feature of image area. Because of I frame use independent frame coding, because its texture feature is different, so its ability to hide the secret information is also different, there are many kinds of image texture feature expression method, such as roughness, contrast, direction, linearity, neat degrees and a rough degree of six attributes. And gray level co-occurrence matrix, the autoregressive model is often used in image texture features.

Step d, in the process of embedding secret information, in order to prevent data loss, can transfer of secret information embedded in the form of redundant embedding,

Step e, the control information embedded in I frame texture DCT coefficients.

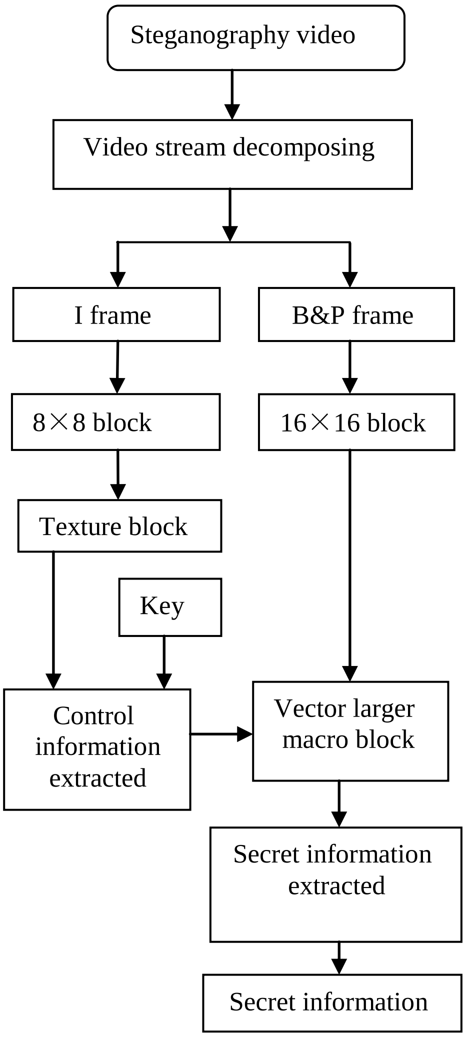

Figure 2: Information extraction process

4 Extraction algorithm

Secret information extraction, the first by the video of the parsing process to get B&P frame of motion vector and the I frame texture area, and then extract the texture from the I frame control information, according to the control information and the key to extract secret information from the motion vector. Information extraction process is shown in figure 2.

The main steps are as follows:

1). Load decomposition of video files, put video files into I frame, B&P frame according to the corresponding decoding format.

2). Extract the control information, put I frame into 8×8 block according to the pixel size, according to the same as in step c of steganography algorithm, texture area determine conditions to select the area, and control information can be extracted from the texture in the chosen area.

3). Extract the secret information, put B&P frame into macro block by 16×16 pixel size, according step b of steganography algorithm in the same way to select the rapid movement of macro block. According to the control information in step 2) and the key in the access to fast macroblock motion vector of motion to extract the secret information.

5. Conclusions

Video digital steganography techniques is the mainstream of development direction in the field of multimedia information security, that can be widely used in the Internet, download in e-commerce, online audio and video on demand, remote teaching, advertising, monitoring and other business, it has important application value and huge economic benefits.

The proposed adaptive video digital steganography algorithm can effectively solve the problems of video steganography had a greater influence on the quality of video and embedding information capacity small in the process. Because the area of image texture masking is stronger, and the sensitivity of the human eye vision system is low for rapid movement area, in these regions to embed secret information can improve the visual perceptual and statistics is perceptual, the use of the shared key also to enhance the system security.

Acknowledgements

R.B.G. thanks the National Science Foundation (61572297 & 61602281), Shandong Provincial Natural Science Foundation (ZR2015YL018 & ZR2016YL011 & ZR2016YL014 & ZR2014FM003), Shandong Province Outstanding Research Award Fund for Young Scientists of China (BS2015DX006 & BS2014DX007), Shandong Academy of Sciences Youth Fund Projects (2014QN011).

References

[1] Cox I, Miller M, Bloom J, et al. Digital watermarking and steganography [M]. Morgan Kaufmann, (2007).

[2] Balaji R, Naveen G. Secure data transmission using video Steganography [C], Electro Information Technology (EIT), 2011 IEEE International Conference on. IEEE, pp. 1-5, (2011).

[3] Sadek M M, Khalifa A S, Mostafa M G M. Video steganography: a comprehensive review[J]. multimedia tools and applications, **74(17),** pp. 7063-7094, (2015).

[4] Pandit A S, Khope S R, Student F. Review on Image Steganography[J]. International Journal of Engineering Science 6115, (2016).

[5] Cheddad A, Condell J, Curran K, et al. Digital image steganography: Survey and analysis of current methods[J]. Signal processing, **90(3)**, pp. 727-752, (2010).

[6] Liu B, Liu F, Yang C, et al. Secure steganography in compressed video bitstreams[C], Availability, Reliability and Security, 2008. ARES 08. Third International Conference on. IEEE, pp. 1382-1387, (2008).

[7] Qian L, Li Z, Zhou P, et al. An Improved Matrix Encoding Steganography Algorithm Based on H. 264 Video[C], Cyber Security and Cloud Computing (CSCloud), 2016 IEEE 3rd International Conference on. IEEE, pp. 256-260, (2016).

[8] Fridrich J. Steganography in digital media: principles, algorithms, and applications[M]. Cambridge University Press, (2009).

[9] Budhia U, Kundur D, Zourntos T. Digital video steganalysis exploiting statistical visibility in the temporal domain[J]. IEEE Transactions on Information Forensics and Security, **1(4)**, pp. 502-516, (2006).

[10] Cetin O, Ozcerit A T. A new steganography algorithm based on color histograms for data embedding into raw video streams[J]. computers & security, **28(7)**, pp. 670-682, (2009).

[11] Walia E, Jain P, Navdeep N. An analysis of LSB & DCT based steganography[J]. Global Journal of Computer Science and Technology, **10(1)**, (2010).

[12] Badura S, Rymaszewski S. Transform domain steganography in DVD video and audio content[C],2007 IEEE International Workshop on Imaging Systems and Techniques. IEEE, pp. 1-5, (2007).

[13] Stanescu D, Stratulat M, Ciubotaru B, et al. Embedding data in video stream using steganography[C],2007 4th International Symposium on Applied Computational Intelligence and Informatics, (2007).

[14] Dai Y J, Zhang L H, Yang Y X. A New Method of MPEG Video Watermarking Technology. In: Proc Int Conf on Communication Technology. Beijing, pp. 1845-1847, (2003).

[15] Zhang Wei-ming, Li Shi-Qu, Liu Jiu-Fen. Extracting attack to LSB steganography in spatial domain. Chinese Journal of Computers, **30(9)**, pp. 1625-1631, (2007).