

A Novel Video Steganography based on Non-uniform Rectangular Partition

ShengDun Hu, KinTak U
Faculty of Information Technology
Macau University of Science and Technology
Macau, China
hsdlya@hotmail.com, ktu@must.edu.mo

Abstract—This paper proposes a novel Video Steganography which can hide an uncompressed secret video stream in a host video stream with almost the same size. Each frame of the secret video will be Non-uniform rectangular partitioned and the partitioned codes obtained can be an encrypted version of the original frame. These codes will be hidden in the Least 4 Significant Bits of each frames of the host video. Experimental results showed that this algorithm can hide a same-size video in the host video without obvious distortion in the host video.

Keywords-Video Steganography; Image Steganography; Non-uniformed rectangular partition; LSB

I. INTRODUCTION

As the rapid growth of high speed computer networks such as the Internet, data getting snooped during transmission becomes more and more serious. The security problems of various data communication via Internet can be addressed by Cryptography and Steganography. Steganography methods become more important in avoiding data being snooped because of its significant effective to preventing others from attempting to decrypt the information hidden in the host object while the Cryptography method always causing the others to do the decryption for its encrypted secret data. Therefore, Steganography is an art of hiding secret information and make them altogether invisible[1],[2]. Two important properties of steganographic technique are perception and capacity. Steganography generally exploits human perception because human senses are not trained to look for file that has hidden information inside of them. Therefore, Steganography disguises information from people who try to hack them. Capacity is the amount of information that can be hidden in the cover object.

Typical Steganography methods can be divided into the time-domain methods and transformation-domain methods. Time-domain methods always can have a big capacity in hiding the information while the transformation ones often equip with robust function from being attacked. The method proposed in this paper is one kind of time-domain method which tries to get a larger data-hiding capacity without causing obvious distortion in the host video stream. Therefore a video stream can be embedded into the host video stream after encoding the secret video by applying the non-uniform rectangular partition. The coding process can be controlled by some key parameters which can be treated as

the encryption key and this can increase the difficulty from being steganalyzed.

II. NON-UNIFORM RECTANGULAR PARTITION OF IMAGE

Paper [3] proposed the algorithm of the non-uniform rectangular partition of image according to the pixel gray values. When the initial partition, the bivariate polynomial and the error control value are all determined, this adaptive partition algorithm can be applied to do the non-uniform rectangular partition of image. The main principle of this algorithm is that it uses the Optimal Quadratic Approximation with a specified bivariate polynomial (with undetermined coefficients) to approximate the gray values within the sub-images, if the determined bivariate polynomial can recover the original sub-image under the required control error, then the partition process will be stopped, otherwise the current sub-image will be divided into four smaller congruent rectangles and repeat the approximation process again until the approximation requirement reaches or the number of the undetermined coefficients of the bivariate polynomial is less than or equal to the pixel number within the sub-rectangle. Finally, according to the partitioned codes obtained, the original image can be reconstructed approximately.

In summary, there are three main factors in non-uniform rectangular partition process. They are the Initial Partition, the Bivariate Polynomial $f(x, y)$ and the control error \mathcal{E} .

Some Initial Partition examples are shown in Figure 1 below. As a convenience, we normally choose the whole image area like Fig 1(a) as the initial partition. In fact, if we can get a more suitable initial partition, the partition results may be better. That means we may get a better reconstructed image with fewer number of partition grids and codes.

Bivariate Polynomial is used to approximate the gray values within each rectangle and its undetermined coefficients can be specified after applying the Optimal Quadratic Approximation to the gray values within it. Some typical Bivariate Polynomial examples are $f(x, y) = ax + by + c$, $f(x, y) = ax + by + cxy + d$, etc. When one of the Bivariate Polynomials is selected, one specific partition pattern is obtained. Generally, the order of it may not be higher than three. The higher the order, the more complicated calculation is needed, but the number of the obtained sub-areas may be fewer for the same control

error. The selection of the Bivariate Polynomial is concerned with specific problems.

Error Control Value is used to check if the partitioning process can be stopped or not. Some Error Control Value examples are $\varepsilon = 30, 10, 5$ and 1.

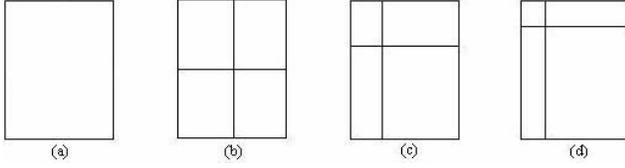


Figure 1. Examples of the Initial Partition

As an example, we choose the control error $\varepsilon = 10, 7$ and 4 and the Bivariate Polynomial as $f(x, y) = ax + by + cxy + d$. The following table shows the partition results and the corresponding reconstructed images. As you can see, the smaller the error, the better the reconstruction results of image obtained. Some square effects may happen in the reconstructed image if the error is not small enough.

TABLE I. NON-UNIFORM RECTANGULAR PARTITION GRIDS AND THE RECONSTRUCTED IMAGE FOR ERROR $\varepsilon = 10, 7$ AND 4 IN ROW ORDER

Original Image with Partition Grids	Reconstructed Image	PSNR
		29.52 dB
		32.81 dB
		36.34 dB

III. IMAGE STEGANOGRAPHY BASED ON NON-UNIFORM RECTANGULAR PARTITION

“Tangram” is one kind of the puzzle game which appeared early in China and then spread all over the world.

The author of Paper [4] and [5] involved the idea of Tangram in computer image processing and formed a novel so-called Tangram algorithm by building the transformation between two images. That algorithm is one kind of image steganography. Many experiments were done and proved that the algorithm was robust but its disadvantage rested with the long coding time.

Here a novel image steganography method based on the idea of Tangram is proposed. The implementation process is almost totally different for the two following main points:

- Adaptive non-uniform rectangular partition is used.
- Partition information of the hidden image is recorded and carried by the open host image.

High encoding and decoding speed are the obvious advantage of this algorithm. As shown in Table II, the partitioning time for a standard 256*256 gray image is about 0.1 seconds while the reconstruction time is around 0.01 seconds.

TABLE II. NON-UNIFORM RECTANGULAR PARTITION AND RECONSTRUCTION TIME FOR ERROR $\varepsilon = 4$

Rectangular Partition Grid+Original Image	Reconstructed Image	Partition Time(s)	Reconstruction Time(s)
		0.103	0.011
		0.101	0.012

Suppose the hidden Image is A , choose Image B (arbitrarily!) as the disguised image and it is open. According to the following algorithm, the codes of Image A can be hidden in Image B without any obvious quality distortion and cause others' interest:

A. Encoding of the Image Steganograph

The encoding process can be described as follows:

- Choose an initial partition, the original image area is most convenient one used. Specify the control error ε , its effective range for generally image is between 2 and 6. Here we use $\varepsilon = 4$. Suppose the Bivariate Polynomial is $f(x, y) = ax + by + cxy + d$, get the partition grids of Image A by following the non-uniform rectangular partition algorithm mentioned above.
- Put the partition grids of image A onto image B and read the gray values of $\{z\}$ and $\{z'\}$ for both images over the grids and record $h_1 = z_1 - z_1'$, $h_2 = z_2 - z_2'$,

$h_3 = z_3 - z_3'$ and $h_4 = z_4 - z_4'$. Here z_1, z_2, z_3, z_4 and z_1', z_2', z_3', z_4' are the gray values of four vertexes of each rectangular sub-area.

- Hide all of the partition codes and its corresponding gray difference $\{h\}$ into the four lowest significant bits of each gray byte of Image **B**.

For RGB image, apply the above algorithm three times for R, G and B components separately.

B. Decoding of the Image Steganography

When receiving Image **B**, follow the decoding process below to extract the hidden image:

- Extract the codes from Image **B**. Those are partition number and their corresponding gray difference set of $\{h\}$.
- With the set of $\{h\}$, calculate the gray values $z_1 \sim z_4$ of four vertexes of each sub-area in **A**. With the set of $\{z\}$, solve for the coefficients a, b, c, d of each plane $Z = ax + by + cxy + d$ in each partitioned sub-area.
- According to each set of $\{a, b, c, d\}$ and plane coordinates, each sub-area can be re-constructed. All reconstructed sub-areas form the whole original image area **A** finally.

C. Testing Experimental Results

In order to investigate the feasibility and effect of the proposed image Steganography algorithm, many experiments have been done. Here, four groups of results are listed below with the control error $\varepsilon = 1$ and 6 and the bivariate polynomial is $f(x, y) = ax + by + cxy + d$.

Each group gives (a) the hidden image, that is the original image itself, (b) the disguising image or host image, chosen arbitrarily and is significantly different from the hidden image, (c) the disguising image with information of the hidden image, (d) the reconstructed image, whose quality depends on the actual problem and the subjective judgment. In the illustration of images, the image size, encoding time(s), reconstruction time (s) and its PSNR (dB) are also given as reference.

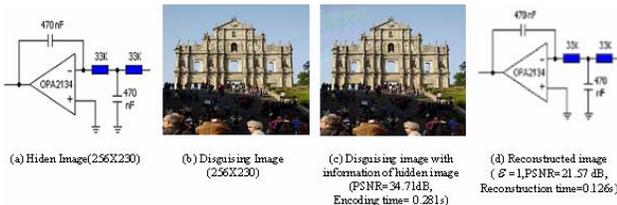


Figure 2. Testing Results of Group 1

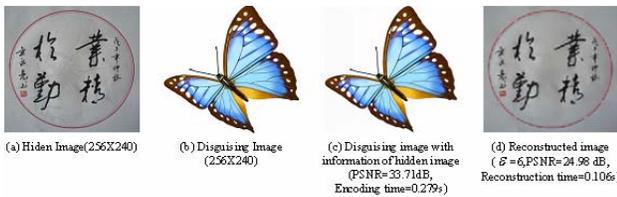


Figure 3. Testing Results of Group 2



Figure 4. Testing Results of Group 3

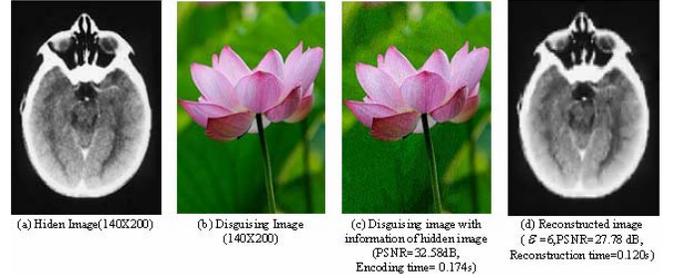


Figure 5. Testing Results of Group 4

The programming environment is: Intel Due-core 1.86G, 1G Ram, Visual C#2003. From group data above, we can see that the encoding speeds vary between 0.16 and 0.30 seconds while the reconstruction speeds vary between 0.10 and 0.14 seconds, which makes it possible to extend this algorithm to video steganography. In fact, the computation speed can be increased more and this paper has only proposed the idea of this algorithm without any managing details.

IV. VIDEO STEGANOGRAPHY BASED ON IMAGE STEGANOGRAPHY

Due to the high encoding speed of the image steganography algorithm above, we extend the image hidden technique to video one. Here we simply consider the steganography in the uncompressed video. That means we try to hide a video stream in another video stream with almost the same size. The main idea is that we treat each frame of both videos as the images and apply the image steganography for each frame with some necessary mechanism. Suppose the host video stream is F , hidden video stream is H . The frame length of F is longer than or equal to that of H . The encoding and decoding process can be described as follows.

A. Encoding of the Video Steganography

- Extract each frame from video stream F and H to R_F, G_F, B_F and R_H, G_H, B_H correspondingly as some static images.
- For each group of $\{R_F, R_H\}, \{G_F, G_H\}$ and $\{B_F, B_H\}$, apply the above image steganography algorithm to hide $\{R_H, G_H, B_H\}$ into $\{R_F, G_F, B_F\}$ to form $\{R2_F, G2_F, B2_F\}$. Here we should choose a suitable control error so that the length of the partitioning codes do not exceed the embedding space of the host. Usually, the control error of 6 is chosen and then the non-uniform rectangular partition is performed, if the embedding-length requirement is not satisfactory, increase the control error

by 0.5 and try the coding again until the requirement is reached although this may further reduce the reconstruction quality.

- c. Reform each set of $\{R2_F, G2_F, B2_F\}$ to the whole video stream $F2$ with the codes of the hidden video stream.

B. Decoding of the Video Steganograph

When receiving the video stream $F2$, the hidden video can be reconstructed by following the decoding process below:

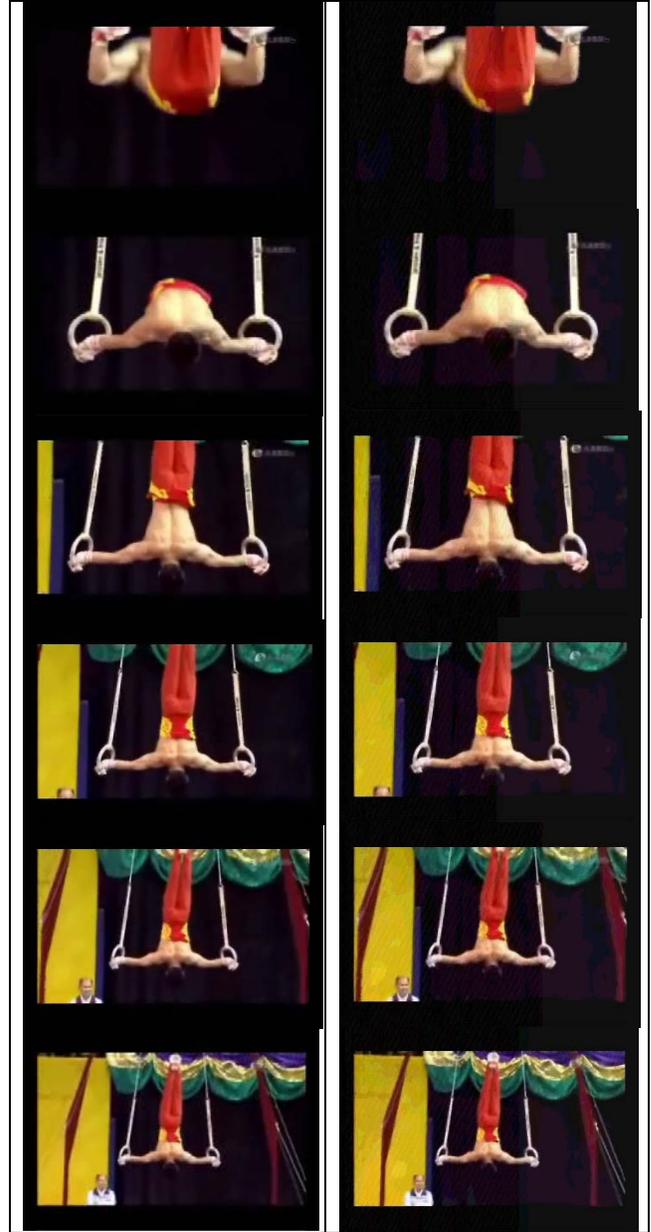
- a. Divide each frame of the video stream $F2$ and F into static-image group $\{R2_F, G2_F, B2_F\}$ and $\{R_F, G_F, B_F\}$.
- b. Apply the decoding process of image steganography algorithm to extract each hidden frame from $\{R2_F, G2_F, B2_F\}$ and $\{R_F, G_F, B_F\}$ to $\{R2_H, G2_H, B2_H\}$.
- c. Reform each set of $\{R2_H, G2_H, B2_H\}$ to the whole reconstructed hidden video stream $H2$.

V. TESTING RESULTS OF VIDEO STEGANOGRAPHY

To test the effect of the above algorithm, we have two uncompressed AVI video streams F (the host video, totally 150 frames, 15 frame/sec) and H (hidden video, totally 137 frames, 15 frame/sec) to be processed. After applying the encoding process and decoding process, we obtain the $F2$ with hidden information of H and the reconstructed video stream $H2$. Table III gives the frame-per-second comparison between F and $F2$ visually. Table V gives the maximum PSNR, average PSNR and the minimum PSNR values among the corresponding frames of F and $F2$. We can see that there no obvious distortion happening in frames of $F2$ so that no one will think that there is something being hidden in $F2$ and all kinds of PSNRs are larger than 28dB.

TABLE III. FFRAME/SECOND COMPARISON BETWEEN F AND $F2$

The Host Video Stream F	Video Stream $F2$ with hidden information
	
	
	



As we can see in Table IV, the visual quality of the reconstructed hidden video stream is acceptable and all PNSRs between H and $H2$ are round 28dB as shown in Table VI.

TABLE IV. FFRAME/SECOND COMPARISON BETWEEN H AND $H2$

The Hidden Video Stream H	The Reconstructed Video Stream $H2$
	



TABLE V. FFRAME-PSNR COMPARISON BETWEEN F AND $F2$

Number of frame to be compared	150 frames
Maximum PSNR between F and $F2$	29.75dB
Average PSNR between F and $F2$	29.15dB
Minimum PSNR between F and $F2$	28.19dB

TABLE VI. FFRAME-PSNR COMPARISON BETWEEN H AND $H2$

Number of frame to be compared	137 frames
Maximum PSNR between H and $H2$	29.37dB
Average PSNR between H and $H2$	28.64dB
Minimum PSNR between H and $H2$	27.42dB

VI. CONCLUSION

Image can be partitioned adaptively by following the non-uniform rectangular partition algorithm. The partition codes obtained can be used to reconstruct the original image approximately. 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. This paper proposes a novel secure large-capacity uncompressed-video steganography algorithm based on that image steganography algorithm. Experimental results show that there is no obvious visual distortion happening in host video stream while the quality of the reconstructed video stream is also acceptable for the practical use.

ACKNOWLEDGMENT

This work was supported in part by National Basic Research Program of China (No.2011CB302400), Science and Technology Development Fund of Macao SAR (No. 006/2011/A1), NSF-CHINA Project (No.10631080) and National Key Basic Research Project of China grant (No.2004CB 318000)

REFERENCES

- [1] Ross J. Anderson and Fabien A.P. Petitcolas, "On the limits of steganography," IEEE Journal on Selected Areas in Communications (J-SAC), Special Issue on Copyright & Privacy Protection, vol. 16 no. 4, pp 474-481, May 1998.
- [2] T Mrkel, JHP Eloff and MS Olivier. "An Overview of Image Steganography," in Proceedings of the fifth annual Information Security South Africa Conference, 2005.
- [3] U Kin Tak, Zesheng Tang, Dongxu Qi. "A non-uniform rectangular partition coding of digital image and its application", Proceedings of the 2009 IEEE International Conference on Information and Automation, 2009, pp. 995-999.
- [4] Dongxu Qi, Wei Ding and Huashan Li. Tangram Algorithm: Image Transformation For Storing And Transmitting Visual Secrets, Proc. Of the 5th International Conference on Computer-Aided Design & Computer Graphics, International Academic Publishers, Vol. 1, 1997-11, Shenzhen, China, 135-139; Journal of Computer Science and Technology, Vol. 13(Supp.), 1998-12, pp.17-21.
- [5] Wei Ding, Dongxu Qi. Digital Image Transformation and Information Hiding and Disguising Technology. Chinese J. Computers. Vol.21, No.9, 1998, pp.838-843.