ПОРІВНЯЛЬНИЙ АНАЛІЗ ЕФЕКТИВНОСТІ МЕТОДІВ ВБУДОВУВАННЯ ЦИФРОВИХ ВОДЯНИХ ЗНАКІВ В ВІДЕОФАЙЛИ

Шостак Н.В.
Харківський національний університет радіоелектроніки
Астраханцев А.А.
Харківський національний університет радіоелектроніки,доцент
Романько С.В.
Харківський національний університет радіоелектроніки
Харків

COMPARATIVE ANALYSIS OF EFFECTIVENESS VIDEO WATERMARKING TECHNIQUES

Shostak N.
Kharkiv National University of Radioelectronics
Astrakhantsev A.
Kharkiv National University of Radioelectronics, docent
Romanko S.
Kharkiv National University of Radioelectronics
Kharkiv

АНОТАЦІЯ

Вбудовування цифрових водяних знаків в відео є головним рішенням питання автентифікації і управління правами на інформацію представлену в цифровому вигляді. Стійкість до зміни формату і шуму дозволяє захистити відео від основних типів атак з боку зловмисників. Запропоновано новий метод вбудовування ЦВЗ в відео на основі вейвлет-перетворень та теорії кодування. Цей метод має такі переваги як кращу смугу пропускання, стійкість та значення MSE серед існуючих методів і порівняно велику швидкість вбудовування.

ABSTRACT

Video watermarking is a main solution for authority and digital rights management. Resistance to change the format and noise allows to protect the video against basic types of attacks by malicious parties. A new method of embedding watermarking in video based on wavelet transform and error-coding theory is proposed. The proposed method has the advantages like a bandwidth, resistance and the MSE value over existing methods and has comparable speed of embedding.

Ключові слова: метрика, PSNR, автентифікація, відео, стеганографія, пропускна здатність.

Keywords: metric, PSNR, authentication, video, steganography, capacity.

Introduction

The digital revolution has changed the paradigm of multimedia distribution. High quality copies of digital data are produced and distributed through the internet by exploiting recent network and software technologies. A broad range of application achieved for video such as video broad casting, video conferencing, DVD, video on-demand and high definition TV which has made a security issues, videos can be tampered, forged or altered easily. Illegal acts such as tampering, forging and altering violates the copyright and the security in respect with cases of authentication. Security techniques that are based on cryptography only provide assurances for data confidentiality, authenticity, and integrity during data transmission through a public channel such as transmission through an open network. However, such security techniques do not provide protection against unauthorized copying or transmitting of illegal materials. This leads to the need for digital watermarking technologies providing detection for copyrighted materials and content authentication.

Steganography is one of the techniques used for secure transmission of secret information. The secret information is concealed in a carrier and transmitted. Basically digital watermarking involves embedding copyright marks and other information such as origin, ownership and destination within digital images, video, audio and other multimedia objects [1][2].

In video steganography a video clip can be a carrier. A video stream consists of many images and audio frames. All these frames can be used to hide the secret information, so, any image or audio steganography techniques can be used with video steganography too.

1 Watermarking Requirements

The trade off between the watermarking requirements can make the effectiveness of each approach. The relative importance of each requirement is somewhat application dependent. In copyright protection the need to retrieve watermark (independent form the image) focus on robustness among the requirements for this application, but in authentication the criteria

changes as the goal is to discriminate between malicious and non-malicious attacks and localization of tampered area [3].

The fundamental characteristics for effective watermark are as follows:

- *Robustness.* The watermark should endure all geometric distortions and attacks, even after processing the signal. Optimal watermarking bears watermark deportation attacks and distortions which are categorized under malignant attacks. Watermarking level depends upon specific applications. Improvement in security techniques will also embellish the robustness of the algorithm.
- *Imperceptibility and Fidelity.* Watermarked image should resemble the original input image. The observer must not identify the embedded watermark. Active watermarking should endure high fidelity level. Distortion level exhibited during embedding phase should not exceed the maximal range.
- *Speed.* Emerging trends in high accelerating hardware made speed as least requirement in watermarking. In cost effective devices main consideration is about less weight and simple watermarking algorithms.
- *Capacity.* The amount of embedded information must be large enough to uniquely identify the owner of the video. Capacity refers to a maximum number of bits are allowed to embed in a cover media. In video watermarking capacity is not a high priority requirement due to the nature of cover object which is big size. The size of the watermark depends on the application which determines the type of watermark data and embedding policy.

2 Quality measurements

To quantify the magnitude of the distortion of the original video file it is usually used such parameters that are described below [4].

The mean square error (MSE). The MSE has been the basis for image quality measure. Usually, one of the images (the original) is assumed to contain no distortions while the other image is contaminated by noise or some other kind of error. MSE for video files is a measure of the dispersion of pixel values of original image and stegoimage (quantity of distortion of original image). The MSE is calculated for each frame of the video file separately. MSE video will be the arithmetic average MSE of the frames that can be seen from the following formula:

$$MSE = \frac{1}{m \cdot n} \cdot \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} (V_{ij} V_{ij}^{*})^2 , \qquad (1)$$

where: V – the value of the pixel of original image;

V^{*} – the value of the pixel of stego image;

m – the number of times of the frame;

n – the number of columns of the frame.

Peak Signal to Noise Ratio (PSNR). PSNR is the ratio of the maximum possible pixel value and the power (magnitude) distortion, which is caused by embedding of the watermark [5]. Due to the fact that the amount of distortion you can imagine using the measure MSE, PSNR can be calculated with the MSE using the following formula:

$$PSNR = 10 \cdot \log_{10}(\frac{MAX^2}{MSE}), \qquad (2)$$

where *MAX* – the maximum value of the pixel.

PSNR and MSE are calculated for each frame of the video file separately.

Structural Similarity (SSIM). The SSIM is a recently proposed image fidelity measure which has proved highly effective in measuring the fidelity of signals. SSIM approach was originally motivated by the observation that natural images have highly structured signals with strong neighborhood dependencies. These dependencies carry useful information about the structures of the objects in the visual scene.

The SSIM index is a full reference metric; in other words, the measuring of image quality based on an initial uncompressed or distortion-free image as reference [6]. SSIM is designed to improve on traditional methods like peak signal-to-noise ratio (PSNR) and mean squared error (MSE), which have proven to be inconsistent with human eye perception.

$$Q = \frac{\sigma_{xy}}{\sigma_x \sigma_y} \cdot \frac{2\overline{xy}}{(\overline{x})^2 + (\overline{y})^2} \cdot \frac{2\sigma_x \sigma_y}{\sigma_x^2 + \sigma_y^2} . \qquad (3)$$

The first component in equation above is the correlation coefficient between *x* and *y*. It measures the degree of correlation between *x* and *y*. Its dynamic range is [−1, 1] and the best value 1 is obtained when y_i is linear with respect to x_i for all $i = 1, 2, ..., N$ i.e. $y_i = ax_i + b$.

The second component has a value range of [0, 1]. It measures the mean luminance between *x*. It equals 1 if and only if $\overline{x} = \overline{y}$.

The third component measures the similarity of the contrast between *x* and *y*. Its range is also [0, 1], where the best value is 1. This occurs only when $\sigma_x = \sigma_y$.

Capacity. The number of bits of the hidden message that can be transferred by the method in a fixed-size image.

Write time. Time that is needed for embedding hidden message into video.

Read Time. Time that is needed for detecting hidden message from video.

3 Embedding methods

A large number of data hiding techniques in digital images existing now. They can be divided into 3 main groups based on the domain that the watermark is embedded, they are spatial domain, frequency domain and MPEG coding structure based. Most of the proposed video watermarking scheme based on the techniques of

the image watermarking and applied to raw video or the compressed video.

The method of replacing the least significant bits (LSB - least significant bit) is the most common among the methods change in spatial region. Least significant bit image carries the least information, and in most cases people are not able to see it change. So it can be used for embedding information by replacing the least significant bits of pixels in the image bits of the secret message.

One of the most common methods currently hiding sensitive information in the frequency domain image is the replacement method relative magnitudes of the coefficients of the discrete cosine transform (DCT), which is described E. Koch and J. Zhao[7]. To use the method of replacement frequency coefficients, the video should be viewed as a sequence of frames. Each frame is treated as an independent image, and the watermark is embedded in each frame.

During the research it was suggested the following modified method:

- as an area of embedding it was chosen the side diagonal of the matrix of DCT;
- added the ability to embed up to 4 bits of watermark in each block of DCT. In each block it is selected up to 4 pairs of distinct elements of the DCT matrix and in each of these pairs of bits is embedded DCT.
- implemented normalization of block after the inverse DCT. Normalization is to detect values out of range, and bringing these values to the value of the nearest range boundary.
- added error-correction coding of Hamming code.

Characteristics of resistance to certain attacks of modified method can be improved by using Hamming codes. Hamming codes are probably one of the most famous codes that smokerise. Hamming codes allow to correct single error (error in one bit) and find a double error. To implement this algorithm it was used Hamming codes (7,4). This means that four bits of watermark were coded by seven bits of code. In this code, four bits would be informative, and three in control group.

To encode the information it is necessary to generate sequence of seven bits. Control bits would be items where the indices are degrees of 2, that is, the indexes 1, 2, 4. In other elements of the sequence information is recorded.

Another possible domain for watermark embedding is that of the wavelet domain. The DWT (Discrete Wavelet Transform) separates an image into a lower resolution approximation image (LL) as well as horizontal (HL), vertical (LH) and diagonal (HH) detail components. The process can then be repeated to computes multiple ”scale” wavelet decomposition, as in the 2 scale wavelet transform. One of the most straightforward techniques is to use a similar embedding technique to that used in the DCT. One of the many advantages over the wavelet transform is that that it is believed to more accurately model aspects of the HVS as compared to the FFT or DCT. This allows us to use higher energy watermarks in regions that the HVS is known to be less sensitive to, such as the high resolution detail bands (LH, HL, HH). Embedding watermarks in these regions allow us to increase the robustness of our watermark, at little to no additional impact on image quality.

4 Comparative analysis

For the research it was used such methods: the method of replacing the least significant bits, the method of replacement frequency coefficients (Koch-Zhao) and method of Discrete Wavelet Transform (DWT). Also these methods have been implemented using Hamming codes, Koch-Zhao’s and DWT methods with the possibility of embedding 1, 2 or 4 bits of the watermark in the DCT block and DWT method with the possibility of embedding in different frequency domain (HL or LH).

Results of calculation of the metrics that are described above, for all these methods are shown in Table 1.

Table 1

Results of calculation of the metrics for methods of embegging watermark into video.

	WriteTime, ms	ReadTime, ms	Capacity, bit	MSE	PSNR	SSIM
LSB	6493	5343	524800	5,1380	41,0228	0,9447
LSB + Hamming Codes	7230	5301	921600	4,9321	41,2005	0,9444
Koch-Zhao (1 bit / block)	41903	22044	14400	6,4030	40,0669	0,9468
Koch-Zhao (1 bit / block) + Hamming Codes	44743	19906	8200	6,4000	40,0690	0,9468
Koch-Zhao (4 bit / block)	40560	19362	57600	8,7525	38,7095	0,9466
Koch-Zhao (4 bit / block) + Hamming Codes	41383	20262	32800	8,7641	38,7037	0,9466
DWT-DCT HL (1 bit / block)	39850	19598	14400	9,6305	38,2943	0,9465

DWT-DCT HL (1 bit / block) + Hamming Codes	41697	20808	8200	9,6311	38,2940	0,9465
DWT-DCT HL (2 bit / block)	40658	21394	28800	9,6305	38,2943	0,9465
DWT-DCT HL (2 bit / block) + Hamming Codes	39053	19084	16400	9,6311	38,2940	0,9465
DWT-DCT LH (1 bit / block)	39797	24634	14400	7,3080	39,4928	0,9467
DWT-DCT LH (1 bit / block) + Hamming Codes	38454	18609	8200	7,2974	39,4991	0,9467
DWT-DCT LH (2 bit / block)	40082	18696	28800	7,3080	39,4928	0,9467
DWT-DCT LH (2 bit / block) + Hamming Codes	39425	20099	16400	7,2974	39,4991	0,9467

The results show that methods of hiding information in spatial domain have better values of quality measurements than methods in frequency domain. The time that is needed to embed hidden message into video and for detecting hidden message from video in spatial domain methods is less in a few times than frequency domain methods. Besides capacity in methods of hiding information in spatial domain is higher in several times than methods in frequency domain. Also, as it is seen methods of embegging in frequency domain with application of Hamming codes have worse values of all metrics than methods with using Hamming codes.

Conclusion

In this work different metrics are described that allows us to quantify the magnitude of the distortion of the original video file and to choose the best method of embedding watermark into video. The most informative metric is capacity as it shows the number of bits of the hidden message that can be transferred by the method, the least informative metric is SSIM. The calculation of the metrics helps us to identify the best algorithm, which is the method of replacing the least significant bits with application of Hamming codes. This method needs the least read time(5,3 seconds), also it has the biggest capacity (921 600 bits), the lowest values of MSE and SSIM though this method has the biggest value of PSNR among all presented methods.

References

1. S. Maity and M. Kundu, "Perceptually adaptive spread transform image watermarking scheme using hadamard transform," Information Sciences, vol. 181, no. 3, pp. 450–465, 2011.

2. A. Agarwal, B. Paul, H. Mahmoodi, A. Datta, and K. Roy, "A process-tolerant cache architecture for improved yield in nanoscale technologies," Very Large Scale Integration (VLSI) Systems, IEEE Transactions on, vol. 13, no. 1, pp. 27–38, 2005.

3. C. Rey and J. Dugelay, "A survey of watermarking algorithms for image authentication," EURASIP Journal on Applied Signal Processing, vol. 2002, no. 1, pp. 613–621, 2002.

4. Gopika V Mane, G. G. Chiddarwar ,"Review Paper on Video Watermarking Techniques," International Journal of Scientific and Research Publications, Vol. 3, Issue 4, 1 ISSN 2250-3153, 2013.

5. Wang, Y. Survey of Objective Video Quality Measurements. EMC Corporation Hopkinton, MA 01748, USA, pp.1-7, 2006.

6. Winkler, S. Video Quality Measurement Standards –Current Status and Trends. Proc. 7th International Conference on Information, Communications & Signal Processing, (pp. 1-5), 2009.

7. Konakhovich, G., Puzyrenko, A. Computer steganography. Theory and Practice (MK-Press, 2006).