Copyright protection for video content based on digital watermarking

Ivanenko Vitaliy and Ushakov Nikita
National Research Nuclear University "MEPhI", Russia
VGIvanenko@mephi.ru, u.nick@inbox.ru

Abstract

The paper proposes the method of digital watermark usage for video copyright protection, that may be a solution to the piracy of digital content. This paper studies different watermark embedding methods for videos. Modified DEW watermarking algorithm is proposed. This method stands out for its technique - the watermark is embedded exclusively by discarding certain high frequency coefficients. Different attacks on video container were studied. The watermark was exposed to most of the common attacks. Performance factors of this algorithm were calculated, they depend on three parameters: energy difference, cut-off point and the number of DCT blocks. Effective values of the parameters were found. The suggested method may act as an effective option for copyright protection.

Keywords: digital watermarks, video, embedding information, DEW

Digital media have enjoyed rapid growth in recent years, especially videos. This has resulted in the need of protecting the multimedia information. A lot of copyright owners are concerned about controlling any illegal duplication of their data or products. The core of the problem lies in the simplicity of digital content copying. This explains why so much attention has been focused on the development of the schemes for the protection of digital images. Of the many approaches possible the digital watermarking is probably the one that has generated the most considerable interest [1,3].

Digital watermark is a special label that is embedded in a container for its copyright and integrity protection. Digital watermarks are used to protect digital content such as images, audios and videos against illegal copying and usage. A violator who has been receiving illicit copies can be tracked down [2].

Digital watermarks are usually invisible (indistinguishable) and therefore cannot be visually detected. For the efficient protection the digital watermarks should also be distributed inside the

container [2]. Generally, information that identifies the author of a product is embedded, however data about the user who has received the particular copy can also be implanted.

Most common attacks on video content in internet are: re-encoding, cutting, re-labeling, changing of bit-rate. To provide protection of the qualitative video copyright a digital watermark must be robust to this attacks. The invisibility of a digital watermark can be achieved in several ways, for example by modifying the discrete cosine transform coefficients. Minor changes of brightness are imperceptible for a human eye, and thus the considerable amount of information can be concealed in one frame.

There are different areas of digital watermarks use: copyright protection, digital imprints, transmission tracing, steganography [3].

Many of modern video compression methods are based on discrete cosine transform (DCT). DCT processes 8*8 pixel blocks. As soon as the transformation has occurred in every cell of the block, the brightness value is replaced with DCT coefficient.

There are three main methods of embedding information in MPEG video. They are based on discrete cosine transformation:

- bit domain labelling method;
- coefficient domain labelling method;
- DEW algorithm [1].

The bit domain labelling method resembles the LSB method for static images. It modifies less significant bits of code words. This method is characterized by small computational complexity and high transmission capacity, but at the same time a digital watermark embedded by this method is vulnerable to most common attacks [4].

The coefficient domain labelling method fixes information by adding a pseudorandom massive to the direct current coefficients of the MPEG video. This method shows high computation complexity. In addition, in this case the digital watermark is not invisible, it can easily be detected

The present paper mostly focuses on the detailed study of the DEW algorithm because of its robustness and the invisible digital watermark. The DEW algorithm embeds label bits by changing the energy difference between high frequency DCT coefficients of top and bottom halves of the pixel block. If the embedding is 0, then the high frequency coefficients of the lower half are equating to 0, if it's 1 then to the coefficients of the upper half. Thus the DEW algorithm embeds label bits by selectively discarding high frequency DCT coefficients in certain image regions.

The undertaken research has shown that the watermark, embedded with DEW method is robust to different attacks such as re-encoding, cutting, re-labeling, changing of bit-rate. However, it's vulnerable to scaling. Removal of a watermark can only be done by image-based processing operations, which requires full decoding and re-encoding of the watermarked video streams [5].

The most reasonable parameter values have been acquired: cut-off point(c) 15, energy difference(D) 20 and size of DCT block 16. Cut-off point is the number of DCT coefficients that are

not used in the process of embedding information. Energy difference shows the amount of coefficients used for embedding of 1 bit of a digital watermark. Figure 1 shows the original video and the video with an embedded digital watermark. With this parameters the watermark is invisible to human eye.

(a) Original video (b) Video with the digital watermark

Figure 1: Embedded digital watermark

Firstly, the container the digital watermark embedded with the DEW method was subjected to different modifications. The number of errors rose inverse proportionally to the bitrate, it's shown of the figure 2. It's not possible to extract original digital watermark after bitrate reaches the 2Mbit/s mark, however such bitrate also affects the quality of the video content.

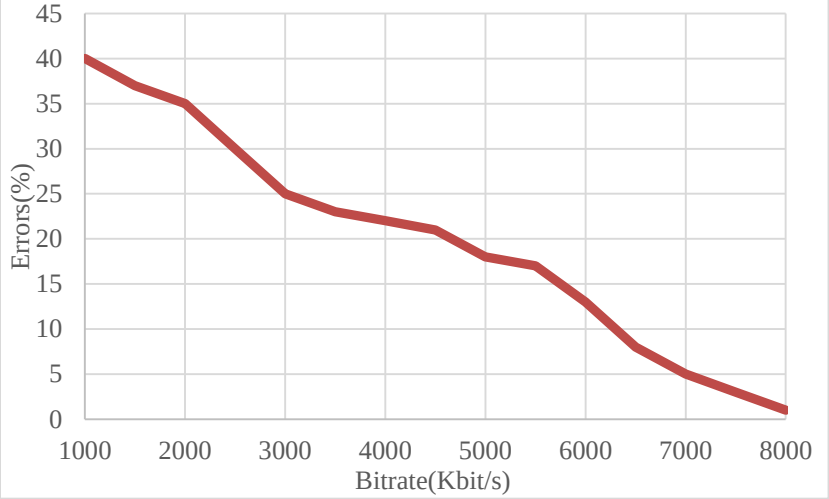

Figure 2: Errors after lowering the bitrate

If the video with an embedded digital watermark is scaled, the watermark is distorted. Even if the original scale is restored, initial watermark can't be extracted. It's not a major drawback, because such operation requires full re-encoding of the video, which is a very computationally demanding task.

Digital watermark embedded by this method is robust to transcoding, original watermark can still be extracted. This quality makes the DEW algorithm extremely useful for video content protection on the internet.

To verify the acquired results, all of the above mentioned tests were also used on 2 different videos, their parameters are listed in table 1.

	Bitrate (Kbit/s)	Resolution(pixels)
Video 1	8000	320*240
Video 2	4200	1280*720

Table 1: Video parameters

It's possible to embed large digital watermarks, they're still invisible. The results of embedding various amount of information with the aforesaid parameters are in table 2.

	64 bit	128 bit	256 bit
Video 1	Digital watermark is invisible	Digital watermark is too large for this resolution	Digital watermark is too large for this resolution
Video 2	Digital watermark is invisible	Digital watermark is invisible	Digital watermark is invisible

Table 2: Embedding results

The robustness of DEW algorithm watermark is shown in table 3.

	Video 1	Video 2
Scaling	-	-
Cutting	+	+
Transcoding	+	+
Re-labeling	+	+
Changing the bitrate	+	+

Table 3: Robustness to different attacks

Having analyzed the results of our research we can draw a conclusion that this method is efficient in copyright protection of video streams. Digital watermarking is the promising method of copyright protection for digital content in whole. Providing certain legislative acts have been introduced, the digital watermarks could be used both for tracing illegal digital copies and well as for copyright proof in court.

References

1. Ivanenko V.G., Rodchenko S.V. Digital watermarks embedding in audio signals // IT security, 2011, №1, p. 94-95 (In Russian)
2. Gribunin V.G., Okov I.N., Turincev I.V. Digital steganography: Salon-Press, 2009. (In Russian)
3. Ivanenko V.G., Shabaeva Y.R., Image protection from modification using less significant bit method. // IT security, 2013, №1, p.103-104 (In Russian)

4. Wu T., Wu S. Selective encryption and watermarking of MPEG video // International Conference on Image Science, Systems, and Technology. 1997.
5. Langelaar G., Lagendijk R., Optimal differential energy watermarking(DEW) of DCT encoded images and video// IEEE Transactions on image processing, vol.10, no.1, January 2001, p. 148-158