ISSN: 2277-9655
Impact Factor: 4.116

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

A NEW SYSTEM FOR INSERTING A MARK PATTERN INTO H264 VIDEO

Tran Thu Ha [*], Tran Quang Duc and Tran Minh Son
[*] Ho Chi Minh City University of Technology and Education, Vietnam
[**] Ha Noi University of Science and Technology, Vietnam
[*] Nagra France, France

DOI: 10.5281/zenodo.60121

ABSTRACT

Watermarking seems to be an exclusive method to discourage the illegal content sharing. This Watermarking officially selected as a requirement to be able to redistribute Hollywood movies **Error! Reference source not found.**, research on an efficient Watermarking technique remains a challenge to experts on the domain. The current work proposes a new technique to insert a visible watermarking into the video encoded with the latest video compression standard H264 /H265. The mark insertion is performed in the compressed domain with simply superposing the unique visible pattern onto the compressed syntax elements. The technique proves to be a light complexity but ensuring high security integration in video distributing chain.

KEYWORDS: Watermarking, Fingerprinting, Overlay, H264, H254, Video compression.

INTRODUCTION

Recent evolution in capacities of multimedia hardware at affordable prices opens up huge possibilities for unauthorised third parties to redistribute video contents – even when such content is protected under encryption means. Technologies exist whereby media content may be marked in order that the content may be traceable either to the original content owner or distributor or to a third party who leaks the content. Such technologies may also be used as a compliment to known encryption techniques in an ecosystem for more efficient protection.

Whereas media encryption may be said to provide proactive protection by limiting access as far as possible to the media in question, marking of media content can be said providing a reactive means of protection since marking renders that particular content traceable should any proactive protection techniques fail, thereby allowing the content to fall into the control of malicious third parties.

Although pertaining to the same domain of embedding information into a host content, a distinction is to be made between two types of marking technique: watermarking and fingerprinting. When content is marked by watermarking methods, this renders the content traceable usually to the content owner or to the original, or otherwise authorized, distributor of the content. On the other hand, when content is marked using fingerprinting techniques, the inserted mark is usually based on an identifier allowing for the intended original recipient of the content to be traced. Fingerprinting techniques therefore render re-distributed content traceable, usually to its originally intended recipient. It would then be reasonable to assume that this traced source is an unauthorized re-distributor of the pirated content.

In the state of the art, when referring to media content which is video, the terms visible mark and invisible mark are used to mean that the content has been marked in a way which renders the mark perceptible to a human eye, or marked in a way which renders the mark substantially imperceptible to the human eye, respectively.

Invisible fingerprinting is an ideal solution against the illegal distribution of content. But its complexity and its robustness are the prohibiting factor to truncate its usage. Toward an efficient tradeoff between simplicity, transparency and robustness, this work proposes a new technique to insert a visible mark into a content to be protected. The technique inherits the light process based on overlaying operator without losing the virtue of visibility and persistence.

The paper is organized as the following. Next section overviews a straightforward application of On-screen Display system to insert a mark. The technique is adapted to the compressed media domain in the Section 3. Section 4 closes with conclusion and perspectives.

VISIBLE MARK INSERTION BASED ON ON-SCREEN DISPLAY SYSTEM

The state of the art [7] includes systems and methods for inserting a mark into media content just before it is consumed by the user. This involves processing the content to be marked while such content is in its raw, uncompressed state. In the case where the media content is a video, inserting a mark in this manner may involve modifying the data at the level of the display memory buffer, just before the data which is held in the buffer is presented for rendering to a display. State of the art systems which are configured to perform such operations are known and include those which are configured to provide on-screen display functionality (OSD). Such systems usually include an OSD insertion module and form part of what is generally known as graphics overlay systems, largely supported in modern rendering systems at a middleware or hardware level. OSD insertion modules generally include additional information over and above the content to be displayed, such information being included in an overlay fashion, visible on top of or mixed with the content. Examples of this are a subtitle text, a control menu or control icons such as a volume slider.

Known, rather straightforward, OSD insertion techniques can be used to insert a mark, such as a watermark, into a media content. Without exception, even if content is distributed in encrypted and compressed form, there comes a point in the distribution chain where the content has to appear in decrypted, decompressed form [1][2]. The output of the audio / video decoder is an example. Embedding the mark at this point facilitates the control of the level of visibility of the mark: raw video is well perceived by the human eye and so the direct processing of raw video to insert the mark allows for the result to be easily inspected in order to control the level of distortion caused by the mark insertion without resorting to any complex transformation techniques. It is therefore convenient to use this point for performing the insertion of the mark. However, at this point may, credential information required to form a watermark (for example, user ID and/or operator identification) is no longer available. Such information is usually incorporated in the descrambling phase, occurring far earlier in the chain, well before the media decoder stage. For this reason, a securely reinforced transmission means is required to feed such crucial information to the OSD insertion module before the content is rendered. In some systems, even those which incorporate such securely reinforced transmission means, pirates can simply disable the OSD chipset thereby thwarting any attempt at providing mark insertion security features.

Fig. ***1*** illustrates a snapshot of a marked video frame. A series of relatively small points are carefully superposed over the original video frame to carry visually a unique mark. The spatial pattern of these points can be designed to obscure at least the original content.

Fig. 1. Overlaying a series of points in a predefined pattern to mark the video

ISSN: 2277-9655
Impact Factor: 4.116

OSD-BASED MARK INSERTION APPLICABLE TO H264 COMPRESSED VIDEO

As discussed above, it would be conceivable for a malicious third party to bypass a watermarking or fingerprinting process which employs simple OSD overlay techniques because they are usually performed on the raw uncompressed media just before being sent to the display device. The present work therefore deals with methods and systems for inserting watermarks or fingerprints into the content in the compressed domain where a content owner still has control (within the secure environment surrounding the descrambling unit) over how his content will be displayed. Conventional OSD overlay techniques are not usually suitable for inserting marks in the compressed domain because the input frame of the compressed video data is no longer a simple two-dimensional array of pixels as is the case in the raw domain. It is disclosed herein that techniques similar to the known OSD overlay principle can still be used advantageously to insert marks into compressed video, thereby providing a simple and secure method for inserting visible (or even invisible) marks with robust enforcement.

The method can be applied to video stream compressed with H264 and H265 standard [3]. Such video stream consists of plurality of Network Abstract Layer Units (NALUs) – normalized data structure syntaxes. NALU can carry the system information necessary to decode the video. Some typical such NALs are SPS Sequence Parameter Set and PPS Picture Parameter Set. Other NALUs contain the compressed video itself. These NALUs are grouped by video frames: each (uncompressed) frame video is divided into several slices – segments of that frame (Fig. 2); Each slice, after being compressed, is encapsulated into a NALU ([4]). The position of that NAL inside the frame is identified with the syntax element first_mb_in_slice, implying the position (in macroblock unit – block of 16x16 pixel) of the very first macroblock of the slice

In order to embed into the stream of NALUs a specific pattern in an overlay fashion (an illustration is shown in Fig. 3), the following steps can be executed:

A pre-defined NALU - hereafter referred to as Marking NALU (MNALU) - is generated once, preloaded to client terminal,

Client terminal quickly parses the compressed video stream to identify the start of the first NALU of a video frame in the stream. The first NALU has first_mb_in_slice equal to zero.

Client terminal browses to a next NALU in the same frame.

Client terminal detects the type (Intra I, Prediction P or Bi-direction B) and the position (the value of the syntax first_mb_in_slice) of each NALU by rapidly analyzing its header.

Client terminal inserts MNALU just before or right after a NALU complete syntax in the stream

The syntax element first_mb_in_slice of MNALU is modified accordingly to 2 following factors:

Ensuring the ascending order of the first_mb_in_slice per frame in the stream

Respecting the spatial position of (a part of) the marking pattern to be inserted. Fig. 3 demonstrates a marking pattern having 3 MNALU at three predefined spatial positions (three predefined values of the syntax element first_mb_in_slice)

Some other important syntax elements of MNALU should be adjusted to the same values as those of the NALUs in the same frame, the most important syntax elements are the following:

In case of MNALU type Intra, the syntax element idr_pic_id must be changed accordingly

In case of MNALU type P or B, the syntax element frame_num and pic_order_cnt_lsb must be changed accordingly

Repeat the steps 4 - 6 until the full shape of pattern is inserted

Repeating the steps 2 – 8 to insert the pattern again in other video frame.

The minimum size of MNALU is one macroblock unit. With this size, the method produces the minimum disturbing effect to honest user (e.g. a black square of size 1 macroblock of 16x16 pixels)

The MNALU can be pre-generated and pre-loaded into client terminal in three 3 types: I, P and B. Upon a command from the HE, client terminal is instructed to use which types of MNALU (can be even mixed) to inject into the compressed stream.

Experiment shows that with MNALU of type P and B, invisible / imperceptible mark is successfully embedded. Fig. 5 highlights the corner left of a marked video, where a MNALU is inserted at the 4th macroblock position. The bottom zoom-in view of this region shows a “blocky” (marked) transition between the sky and clown, while the top view represents the normal image. Such distortion can be considered as invisible to viewers.

The pre-generation of the MNALU can be skipped by duplication of the same ordinal NAL in a frame wherever a mark is expected to be inserted. Then only the value of its first_mb_in_slice should be changed to shift apart the two

ISSN: 2277-9655
Impact Factor: 4.116

(identical) segments. In such a case, although the steps 1 and 7 are saved, the overlaid slice produces degradation proportional to its complete size. Therefore it is recommended only when the original size is relatively small.

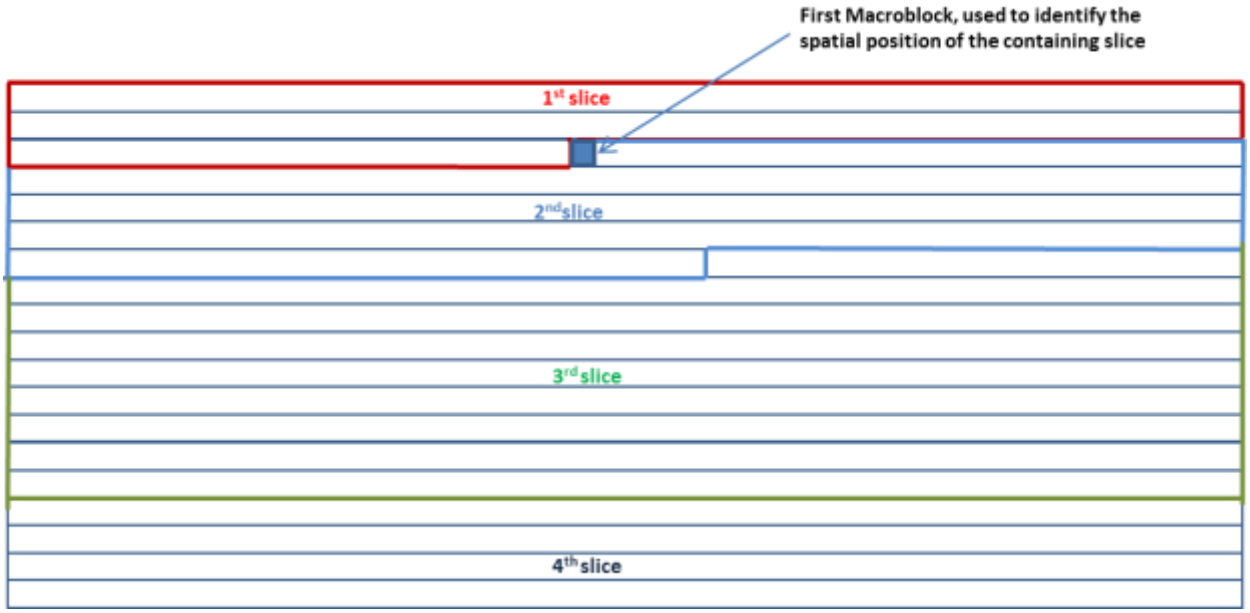

Fig. 2. A frame video divided into 4 slices – 4 NALUs

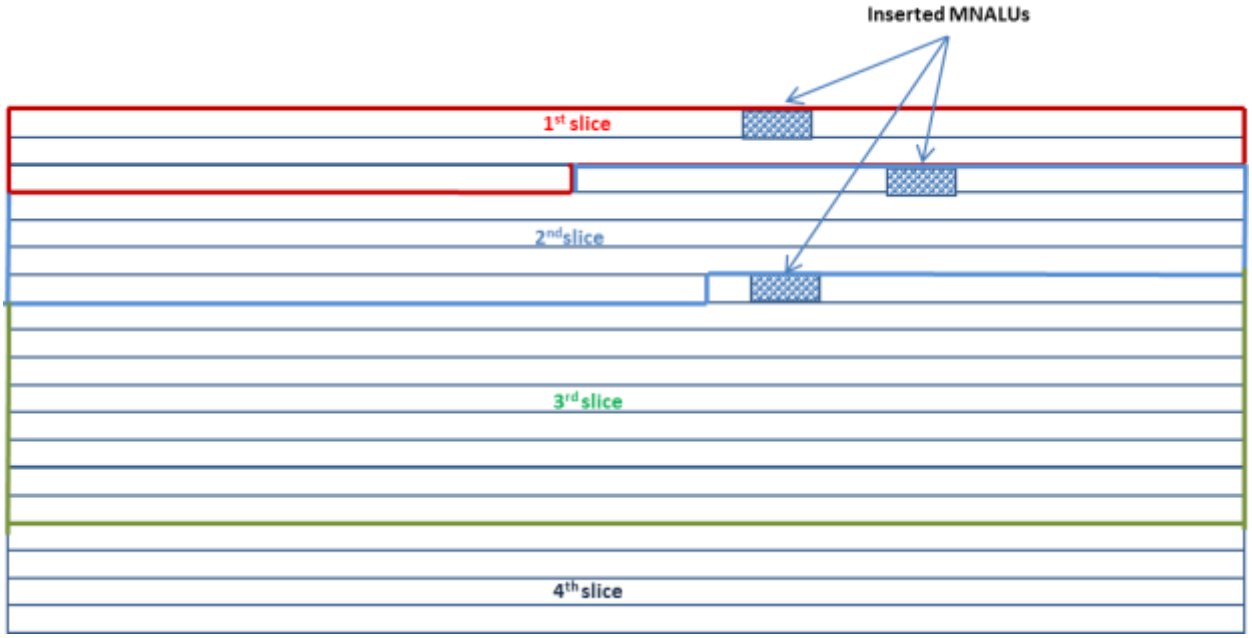

Fig. 3. Illustration of OSD marking with 3 additional Marking NALUs, building a specific pattern

ISSN: 2277-9655
Impact Factor: 4.116

Fig. 4: 1 MNALU of type I (its size is 16x 80 pixels) is overlaid at the position 31 (in Macroblock units)

Fig. 5: Original video frame of type B with zoom-in snapshot where a MNAL will be inserted

CONCLUSION

Watermarking / fingerprinting technique plays more and more important role in struggling against content pirates. Such reactive protection is efficient only if its integration is practically feasible without compromise of security and impact on the quality of the protected content. Toward this goal, the present work proposes a new embedding technique for the latest compression standard H.264, H265. The mark is inserted directly on the compressed domain, immediately after the descrambling. It means that if the necessary security level is ensured at descrambling operation (indispensable requirement of all scrambling technique), the mark insertion operation right after the output of descrambling can be certainly performed correctly. A safe path between encryption and marking entities are then

guaranteed. The transition state - the gap of security which is often exploited by hackers - no longer exist between the two complementary operations. As result, the overall security of the system is improved.

The marking manner is also improved. The mark pattern can be embedded into the original compressed stream in the same way as On Screen Display system overlay additional information upon raw video. The latest standard of video compression is exploited to make such insertion possible. Furthermore, by carefully designing the MNAL, additional marking component, transparent mark can be also obtained.

In the future research, we investigate on the blind detection of the marks to further improve the efficiency of the marking technique

REFERENCES

[1] M. S. Tran, P-S. D. Sarda, G. V. Baudin, Security method for preventing the unauthorized use of multimedia content, Pending US patent, US 2011/0293092.
[2] P-S. D. Sarda, M. S. Tran, Method to trace video content processed by a decoder, pending US patent US 2012/0134530.
[3] ISO/IEC 14496-10 Information technology – Coding of audio-visual objects – Part 10 Advanced Video Coding.
[4] A. Puri, X. Chen, A. Luthra: Video coding using the H.264/MPEG-4 AVC compression standard, Signal Processing: image Communication 19, 2004 pp 793-849.
[5] D. Zou, J. A Bloom: H.264 streamm replacement watermarking with CABAC encoding. Proc. of the 2010 IEEE International Conference on Multimedia & Expo ICME, Suntec, Singapore.
[6] Tardos G.: Optimal probabilistic fingerprint codes. Proc. Of the 35th annual ACM symposium on theory of computing, San Diego, CA, USA 2003 pp 116-125.
[7] I. J. Cox, M. L. Miller, J. A. Bloom, J. Fridrich, T. Kalker: Digital Watermarking and Steganography, Second edition, Elsevier 2008.
[8] Movielabs Specification for Enhanced Content Protection – Version 1.0.