A QR-code based audio watermarking technique for tracing traitors

Faten Chaabane, Maha Charfeddine, William Puech, Chokri Ben-Amar

A QR-CODE BASED AUDIO WATERMARKING TECHNIQUE FOR TRACING TRAITORS

Faten Chaabane[a], Maha Charfeddine[a], William Puech[b] and Chokri Ben Amar[a]

[a]REGIM-Lab.: REsearch Groups in Intelligent Machines, University of Sfax, ENIS,
BP 1173, Sfax, 3038, Tunisia
[b]LIRMM Laboratory, UMR 5506 CNRS, University of Montpellier II,
161, Rue Ada, 34392, Montpellier Cedex 05, France

ABSTRACT

Handling a great number of users and surviving different types of attacks present fundamental challenges of the majority fingerprinting systems in the tracing traitor field. In this paper, the proposed technique consists in embedding a fingerprint, a QR code in the audio stream extracted from the media release. Using the QR-code provides several advantages as supporting a large amount of information in a compact format end damage resiliency. This paper proposes to encode the identifier which is a parallel concatenation of two tracing codes: Boneh Shaw and Tardos codes into QR-code. The proposed approach should not only improve the two-stage tracing strategy by reducing the complexity computation, but also enhance the secure side of the proposed technique by the preprocessing treatment before generating the QR-code.

Index Terms— QR-code, tracing traitors, Boneh Shaw, Tardos, preprocessing

1. INTRODUCTION

The non-stop evolution of the Internet and networks has currently entaileld more than an illegal treatments closed to the copyright violation. These manipulations, simple but illegal, are observed especially in multimedia distribution systems like the Video On Demand ones. They enclose copying, editing and sharing multimedia releases. Obviously, it was imperative for the media distributor to find remedial measures to prevent the copyright infringement and provide more security in the legal distribution operations. The first propositions in the literature focused on the watermarking field which consists in embedding a watermark in a digital content in order to identify its supplier and to protect it from any piracy operation. But it still remains insufficient in the tracing traitors' context [1]. Indeed, the principal goal of a media holder in a multimedia distribution platform is to ensure the safe usage of media releases and to trace back the illegitime users in a piracy trial. That is why tracing traitors involves two main components: the tracing code and the robust watermarking technique. The tracing code should be unique and specific to each legitim user [2]. The watermarking technique which is applied to embed the message in the media content should be robust to different types of attacks [2]. In the literature, two different fingerprinting approaches were thus derivated: a first approach is focused on the watermarking layer and the second one had rather enhanced the study of the tracing code [2]. The watermarking-based fingerprinting systems proposed a spread spectrum signal as a fingerprint for each user [3]. While this approach has good rates of tracing, it presents heavy computational costs. The code-based fingerprinting systems were oriented in improving the code construction and providing a good compromise between the detection rate, the code length and the robustness to the different attacks [4]. In this way, several codes were proposed in the literature [5], especially the Tardos code [6] and propose to improve its decoding step [7, 8]. Some of them propose to combine another tracing code to the Tardos code in order to ameliorate its performance as in [9, 10] which the principal idea is to propose a two-level tracing strategy where the tracing code is the combination of an outer code and an inner one the Tardos code. The problem with these techniques is the important required length of a video sequence for a large size of audience. This criterion seems to be relevant in the case of the multimedia distribution systems where the number of users can exceed 10^5. In this paper, we propose a QR-based watermarking technique as an improvement to the two-stage tracing strategy proposed by [10]. The QR-code has the ability to support a large size of information in a reduced space which will require less embedding time and less complexity computation. The paper is arranged as follows: In Section 2, we detail the different steps of the proposed tracing system. In section 3, we present the different experimental tests we carry out to validate the performance the proposed technique. We summarize with a conclusion and future work in Section 4.

2. THE PROPOSED TRACING SYSTEM

In the two-stage tracing strategy proposed in [10], the tracing code is a combination between the Boneh Shaw as an outer code and the Tardos code as an inner code. The two codes have the same length m. This strategy was proposed

978-0-9928626-3-3/15/$31.00 ©2015 IEEE

in a group-based fingerprinting system where each user belongs to a group and has consequently a group identifier concatenated to his personal identifier. To survive the problem of the code length, authors in [10] propose to enlarge the alphabet size from a binary alphabet to a 4-length cardinalty one. Although this technique affords to reduce the codeword length from *2*m* to *m*, it still requires an important embedding time. The proposed technique consists in converting Boneh-Shaw Tardos code to a QR-code. This format should provide not only less embedding time but also a good robustness to attacks due to its internal channel coding based on Reed Solomon code. In 3.1, we describe in detail each step of the technique.

2.1. The watermark preprocessing step

The identifier, the Boneh-Shaw Tardos code, is the starting-point of the watermark preprocessing process. As depicted in Figure 1, this step includes:

- the generation of the QR-code: the Boneh-Shaw Tardos code is converted to a QR-code.
- The QR-code has four templates which do not contain any encoded information but are easily identifiable and are used essentially in the detection of the watermark. Three among these templates are similar and called Template 1, the fourth one is called Template 2. as shown in Figure1. The QR-code then is divided to k overlapped blocks of

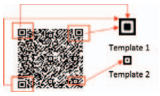

Fig. 1. The four identifiable template in a QR-code

$(\frac{m}{k}+1)$*$(\frac{m}{k}+1)$ size. In this step, k depends on two requirements: the length of the embedded code and the payload of the watermarking technique.

- The scrambling process: in this level, the Arnold Transform is applied to the original blocks to obtain k blocks scrambled A_p times. To retrieve descrambled blocks, the parameter A_p should be known by the video distributor. The different blocks are then inserted sequentially in equal fragments of the audio stream extracted from the video. In 2.2, we detail the embedding step.

2.2. The watermark embedding step

The adopted watermarking technique is an audio watermarking technique proposed in [11]. The different steps of the embedding process are presented in Figure 3. In fact, the audio stream is extracted from the media copy and then divided into 512-size independent blocks. A DCT transform is then applied to each block. In the same time, after the watermark preprocessing step, we obtain k scrambled blocks $Sc_{i,i\in\{1..k\}}$ having a size of pq. After that, pq randomly selected indexes are chosen from the original blocks. The watermark symbols are embedded in Middle Frequencies MF band of each block, a choice which was proven by a study made in [11]. The Back Propagation Neural Network, BPNN, is trained and simulated to choose the best embedding position. The watermarked audio is obtained by applying the IDCT transform. It is relevant to indicate that each scrambled block is embedded in a fragment $f_{i,i\in\{1..k\}}$ of the audio stream. The length of the audio required to embed all the watermark is thus equal to k * f_k. We add the A_p: the parameter of the Arnold transform which is saved as a secret watermarking key to retrieve blocks of the QR-code before the scrambling operation.

2.3. The watermark detection step

The adopted watermarking technique is a blind watermarking scheme and so to retrieve the watermark Sc_i', we need only the pq MF positions, the random indexes, the A_p and the coordinates of Template 1. This step is presented in Figure 4, it consists in the inverse of the embedding one.

2.4. The descrambling step

In this step, we proceed to the inverse of the Arnold transform to each detected block Sc_i'. Knowing the number of iterations A_p of the scrambling operation We obtrain k descrambled blocks DSc_i'.

2.5. The matching step

Matching the different descrambled blocks $DSc_{i,i\in\{1..k\}}$' to retrieve the detected QR-code should be difficult when the digital content is attacked, which can damage the embedded watermark. We propose in this step, as presented in Figure 5, to use two measures, the *NCC*, Normalized Croos Correlation, to retrieve the first detected blocks DSc_1' and then the *SAD*, the Sum of Absolute Differences, to gather the remaining overlapped blocks. The proposed matching algorithm is summarized as follows:

1. Read the image of Template 1 and the image of the descrambled block $DSc_{i,i\in\{1..k\}}$'
2. Iterate Template 2 over DSc_i' and compute the *NCC* matrix
3. The coordinates where the value of *NCC* is the largest correspond to the best similarity and so to the required position,
4. Given that the coordinates of Template 1 are knwon, we compare them to the saved ones and according to that we obtain the first block in the detected watermark.
5. Iterate DSc_1' over the remaining $DSc_{i,i\in\{2..k\}}$' and compute the the *SAD*. The block which is overlapped to the first block has the coordinates where the lowest *SAD* value

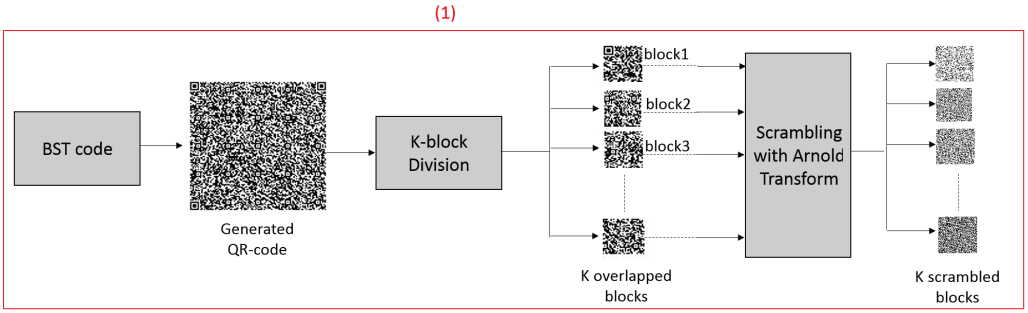

Fig. 2. The watermark preprocessing step

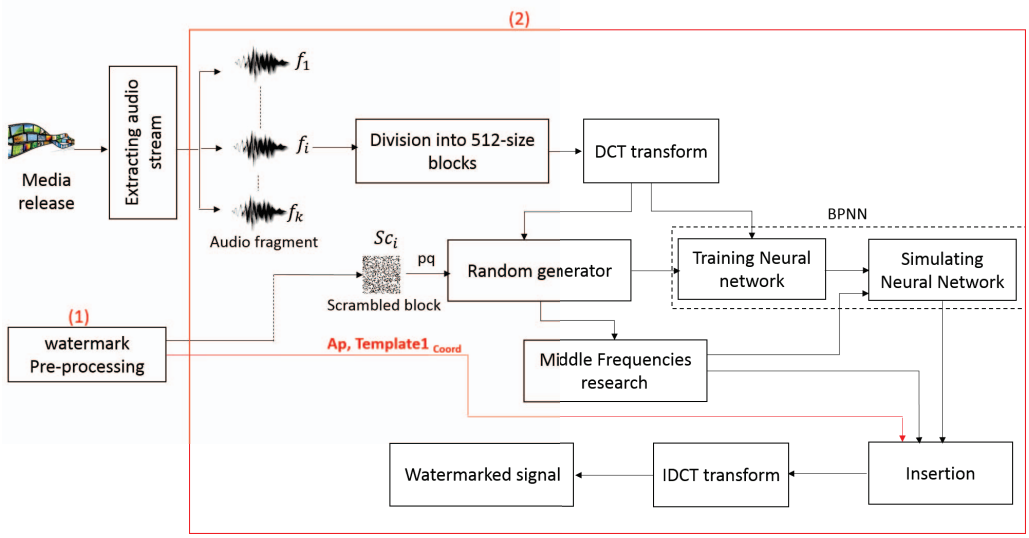

Fig. 3. The watermark embedding step

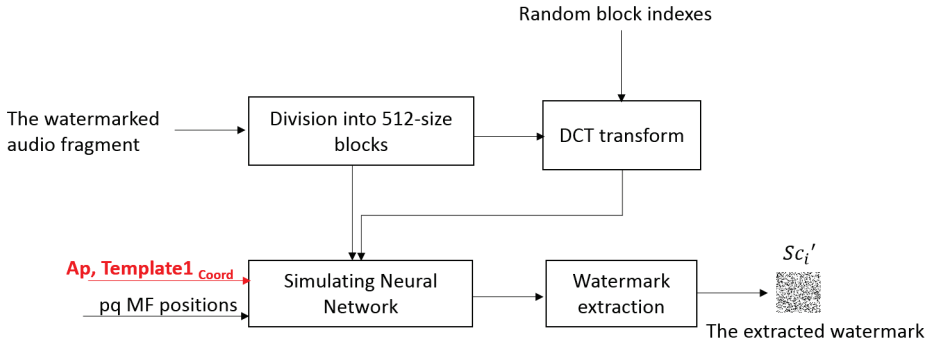

Fig. 4. The watermark detection step

is obtained. Save the block position coordinates and iterate 4 for the other $DSc_{i,i\in\{3..k\}}$'.

6. According to the obtained coordinates, combine the detected blocks and construct the retrieved watermark.
After detecting the QR watermark, it is possible to check tha validity of the watermarking technique.

3. EXPERIMENTAL RESULTS

In this section, we evaluate the proposed technique according to different criteria: the QR-code capacity which implies a high watermarking payload and less embedding time when varying the code length m and the robustness to the almost

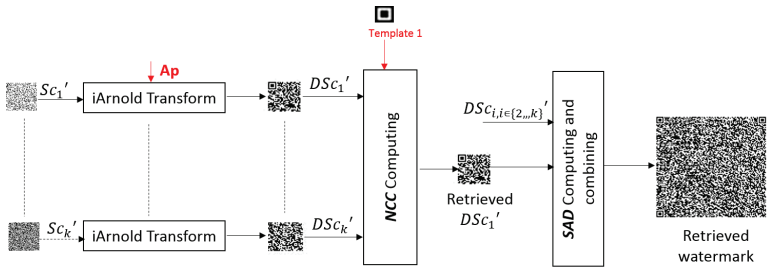

Fig. 5. The watermark matching step

Tracing strategy	required clip duration
Tardos [6]	$\approx$ 20 min
Tardos-Tardos [9]	$\approx$ 40 min
Boneh Shaw-Tardos [10]	$\approx$ 21 min
The proposed technique	5 min 20s

Table 1. Comparison of existing tracing strategies

collusion attacks and to other attacks tied to the audio signal. To have good watermarking robustness and inaudibility results, we choose the same parameters required by the audio watermarking technique proposed in [11]. All the extracted audio signals are divided into fragments of 20 s and are sampled in 44.1 KHz with 16 bits/sample. In each audio fragment, we insert a scrambled block which dimension should not exceed 32*32 bits. To support the various code length values, we choose the suitable QR-code version to garantee a good embedding capacity.

3.1. Embedding time

In Table 1, we show how the proposed technique takes few the lesat embedding time compared to respectively three fingerprinting systems [6, 9, 10]. In thi case, the code length is around m=2048 and the number of users is equal to 10^4. We choose the *version* 20 and the level *h* as error correcting level. This version offers to convert 2061 numeric symbols into a 97*97 QR-code dimension. In Figure 6, we vary the embedded code length m and we compare the embedding time required to embed a fingerprint in a video for the original Boneh-Shaw Tardos proposed in [10] and the QR-based improved technique. While the embedding time for the proposed technique is around few minutes, it is over 25 min for $m > 10^4$ which can not be allowed for some video sequences in VOD context.

3.2. Tracing results

The proposed technique is a group-based tracing strategy, Boneh-Shaw Tardos code, inspired from [10]. This technique has reflected, due to a group selection, a high tracing rates.

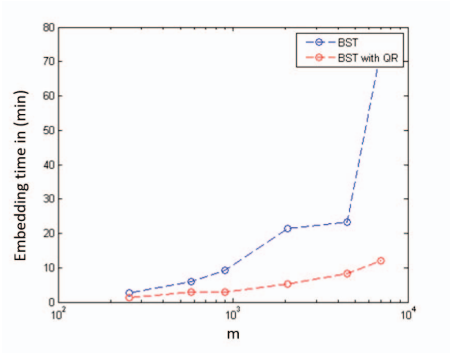

Fig. 6. The embedding time for the proposed technique vs [10]

We choose a Tardos length m eqaul 5330 symbols which is tied to a number of users equel to 10^7, ε_1 set to $10^{-}6$ and c the number of colluders equal to 2. To embed the fingerprint, the suitable version of QR-code is version 35 with L as an error correcting level, this version affords to carry 5529 numeric characters. In Figure 6, we show that the proposed technique affords a good detection probability P_d of more than 20 colluders against several collusion attacks.

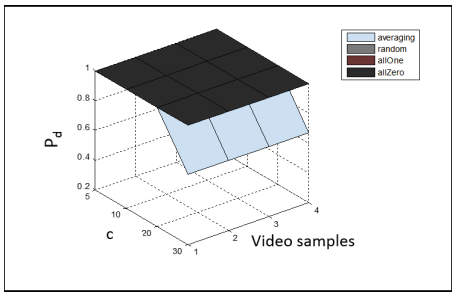

Fig. 7. Robustness to different types of collusion attacks

3.3. Watermarking robustness and inaudibility

In Table 2, we calculate the SNR values for four different tested video samples. We notice that all these values exceed 20dB and so garantees good inaudibility results. To verify the watermarking robustness of the proposed technique, we

Video name (.avi)	SNR values(dB)
match	52.5765
film	49.03
song1	48.73
song2	38.47

Table 2. Inaudibility results obtained with the different tested videos

are interested only by audio attacks and so we carry out a set of audio Stirmarkaudio attacks : noising, filtering and MP3 compression for different rates: 128, 96 and 64... As depicted in Figure 7, NC values are closed to 1 and reveal good robustness results which is enhanced by the error correcting capability of the QR-code.

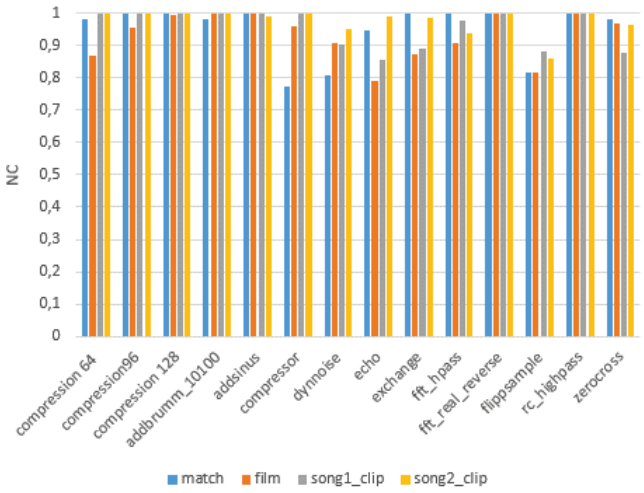

Fig. 8. Robustness to several stirmarkaudio attacks

4. CONCLUSION

In this paper, we have proposed a QR-based watermarking technique in tracing traitors' for VOD platforms. The construction of the fingerprint is based on the QR-code and thus provides the possibility to embed a great amount of information and so to trace a great number of users in a less embedding time without altering the media quality. The security side of the technique is also improved by the proposed fingerprint preprocessing step. To validate the fingerprinting system, a set of experiments were realized according to several criteria: embedding time, inaudibility and robustness to collusion and other audio attacks. This technique was proposed for static tracing schemes where the fingerprint is constructed in the distributor side and tracing colluders is made after diffusing all the copies. In a future work, we will focus on adapting this technique in dynamic tracing schemes where it is possible to trace colluders for each round.

REFERENCES

[1] Caroline Fontaine, *How to protect multimedia pieces of content, from their creation to their distribution*, Ph.D. thesis, Universit de Bretagne Occidentale, cole doctorale SICMA, 2011.

[2] Faten Chaabane, Maha Charfeddine, and Chokri Ben Amar, "A survey on digital tracing traitors schemes," in *9th International Conference on Information Assurance and Security, IAS 2013, Gammarth, Tunisia, December 4-6, 2013*, 2013, pp. 85–90.

[3] Byung-Ho Cha and C.-C.Jay Kuo, "Design and analysis of high-capacity anti-collusion hiding codes," *Circuits, Systems & Signal Processing*, vol. 27, no. 2, pp. 195–211, 2008.

[4] Alexander Barg and Grigory Kabatiansky, "Robust parent-identifying codes and combinatorial arrays," *IEEE Transactions on Information Theory*, vol. 59, no. 2, pp. 994–1003, 2013.

[5] Dan Boneh and James Shaw, "Collusion-secure fingerprinting for digital data," *IEEE Transactions on Information Theory*, vol. 44, no. 5, pp. 1897–1905, 1998.

[6] Gábor Tardos, "Optimal probabilistic fingerprint codes," in *STOC*, 2003, pp. 116–125.

[7] Boris Skoric, Stefan Katzenbeisser, and Mehmet Utku Celik, "Symmetric Tardos fingerprinting codes for arbitrary alphabet sizes," *IACR Cryptology ePrint Archive*, vol. 2007, pp. 41, 2007.

[8] N. Akashi, M. Kuribayashi, and M. Morii, "Hierarchical construction of Tardos code," in *Information Theory and Its Applications, 2008. ISITA 2008. International Symposium on*, Dec 2008, pp. 1–6.

[9] Minoru Kuribayashi and Masakatu Morii, "Systematic generation of Tardos's fingerprint codes," *IEICE Transactions*, vol. 93-A, no. 2, pp. 508–515, 2010.

[10] Mathiew Desoubeaux, Gaetan Le Guelvouit, and William Puech, "Fast detection of Tardos codes with boneh-shaw types," in *Proc. SPIE 8303, Media Watermarking, Security, and Forensics*, 2012.

[11] Maha Charfeddine, Maher Elarbi, Mohamed Koubaa, and Chokri Ben Amar, "Dct based blind audio watermarking scheme," in *SIGMAP*, 2010, pp. 139–144.