A Multimedia Tracing Traitors Scheme Using Multi-level Hierarchical Structure for Tardos Fingerprint Based Audio Watermarking

Faten Chaabane, Maha Charfeddine and Chokri Ben Amar
REGIM: REsearch Groups on Intelligent Machines, University of Sfax, National Engineering School of Sfax (ENIS), BP 1173, Sfax, 3038, Tunisia

Keywords: Tracing Traitors, Hierarchical, Tardos, Watermarking, Fingerprint, Computational.

Abstract: This paper presents a novel approach in tracing traitors field. It proposes a multi-level hierarchical structure to the used probabilistic fingerprinting code; the well known Tardos code. This proposed structure is performed to address the problem of computational costs and time of Tardos code during its accusation step. The generated fingerprint is embedded in the extracted audio stream of the media by an audio watermarking technique operating in the frequency domain. The watermarking technique represents an original choice compared to the existing works in the literature. We assume that the strategy of collusion is known, we compare then the performance of our tracing traitors framework against different types of attacks. We show in this paper how the proposed hierarchy and the watermarking layer have a satisfying impact on the performance of our tracing system.

1 INTRODUCTION

Several manipulations like copying, editing and diffusing multimedia tracks through the internet and Peer to Peer networks do not represent any challenge even to simple users but constitute a dangerous phenomenon for the software industry. The purpose of researchers was to find mechanisms performing copyright protection. First works were proposed in watermarking field which consists in embedding a specific message in the digital content to protect it from fraud. In the recent years, with the evolution of cloud and networks, watermarking techniques can be easily circumvented by a group of experienced users who try to cooperate together by applying more complex collusion attacks in order to create and share illegally a new copy with unknown fingerprint. This type of manipulations has led to the development of collusion resilient secure fingerprints. These codes, associated to the watermarking technique, are able to trace traitors who collude together (Charpentier et al., 2011).In tracing traitors field, there are two major schemes: static tracing scheme and dynamic one (Laarhoven, 2013).The choice of the tracing strategy depends on the number of needed fingerprints in the scheme to capture dishonest persons. In the VOD context, the video supplier generates a single individual fingerprint specific to each authorized user and inserts it in every sold release. When an illegal copy is distributed, he is able to discover the forgery, to trace at least one colluder and so to delete this suspicious copy to prevent any other redistribution. In the dynamic scenario, such as the online streaming systems, the media distributor has the ability to generate a novel set of fingerprints when collusion is discovered and thus disconnect accused persons from the system.

In our work, we are interested in the VOD context, and in figure 1 below; we present the generic static tracing scheme. We distinguish, in the first side, the generation step where the fingerprint, based on the Tardos code is constructed and diffused to n users $u_{i\{1..n\}}$. In the distributor side, a group of colluders $colluder_{j\{1..c\}}$ mix their copies and participate together in the construction of a suspicious copy with unknown fingerprint. Once the suspicious copy is detected, the video supplier proceeds by extracting the colluded fingerprint and analyzing it to retrieve dishonest users .

The paper is arranged as follows: the second section consists in an overview of related works in tracing field. In section 3, we detail our tracing algorithm based on generating a multi-level hierarchical fingerprint and its embedding in the stream sound of a video. In section 4, the performance and the security of our proposed tracing system is shown. Finally, we give a conclusion and some future perspectives.

Chaabane F., Charfeddine M. and Ben Amar C..
A Multimedia Tracing Traitors Scheme Using Multi-level Hierarchical Structure for Tardos Fingerprint Based Audio Watermarking.
DOI: 10.5220/0005066602890296
In *Proceedings of the 11th International Conference on Signal Processing and Multimedia Applications* (SIGMAP-2014), pages 289-296
ISBN: 978-989-758-046-8

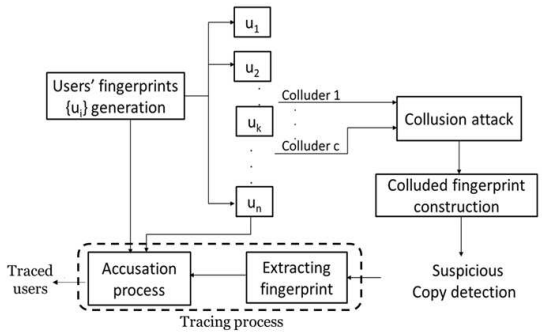

Figure 1: The general static tracing traitors scheme.

2 RELATED WORKS

Unauthorized manipulations on digital media present an important challenge. The tracing traitors techniques, called also transactional watermarking techniques were proposed by researchers as a suitable solution to trace back illegal media redistribution. The principle of these systems is to hide by a watermarking technique a specific message in every sold release. The choice of the watermark is not arbitrary; it is a mathematical code, known as secure collusion fingerprinting code. Its structure has to resist to almost all types of attacks and needs huge payload (Charpentier et al., 2011) (Charpentier et al., 2009). Recent works proposed in tracing field try to improve the tracing performance and respond to several requirements tied to the length of inserted code whenever the collusion size increases . In our previous paper (Chaabane et al., 2013), we have dressed a survey of existing fingerprinting techniques and we have tried to classify these techniques according to the improvement they propose. In some works, like in (Hayashi et al., 2007), the hierarchical structure was proposed in fingerprint generation process, assigning users to a group is made randomly without considering relationships inter or intra groups which doesnt present an optimal choice to ameliorate the Tardos performances. In (Ye et al., 2013),authors analyze users relationships in a social network to construct a multi-level hierarchical fingerprint for digital content diffusion through the internet and Peer to Peer networks. The resulting fingerprint of each user is the combination of BS code as an outer the Tardos code as an inner code. However, the limitation of this work is that it tests its proposal system only against the majority vote attack. Some other contributions (Hamida et al., 2011) have proven that reducing the complexity of the decoding step have a positive impact on the accusation process thus they propose to use a hierarchical embedded fingerprint, this hierarchy in (Hamida et al., 2011) is inspired from (Wang et al., 2004) and is based on regrouping users according to their social and geographic belongings under the assumption that users having the same characteristics have more probability to cooperate together than with others. In (Shahid et al., 2013), the proposed tracing scheme embeds the well known fingerprinting code, the Tardos code (Tardos, 2003) (Laarhoven and de Weger, 2011), in video signals in compressed domains; it used the H.264/AVC as a compression standard and the spread spectrum as a watermarking technique. The weakness of this work is that the number of users used in experimentation didnt exceed 100 whereas in VOD applications it can reach many thousand.

Some works try to optimize the accusation functions (Furon et al., 2009) of the Tardos code to ameliorate its robustness to the worst collusion attacks. In (Desoubeaux et al., 2011), a tracing algorithm is proposed where the accusation function of Tardos code is improved to suit to a specific watermarking technique: the zero bit watermarking technique, this combination provides short fingerprint for great number of users but needs some adjustment in the tracing process. According to related works, we have focused on rising to the challenge of ameliorating robustness results and accusation rates of improved Tardos code, thus we try to decrease the complexity of Tardos computing by proposing a multi-level hierarchical fingerprint and we embed it by an original robust watermarking technique. Our proposed framework will be explained below.

3 THE PROPOSED ALGORITHM

In our tracing traitors framework, as shown in figure 2, , we distinguish three main steps: the multi-level hierarchical Tardos fingerprint generation, its embedding in the extracted audio stream and the tracing step which occurs in the distributor side and in which a tracking operation is applied to accuse at least one of the colluders participating to the collusion scheme. We will explain later each step separately.

3.1 Multi-level Fingerprint Generation Step

Reducing the search space of dishonest users by assigning a user to a specific group represents a suitable solution to face the Tardos accusation costs. The user assignment to a group can be used to counter different types of coalitions: temporal, geographic, social, etc. In the hierarchy we embrace, each chosen con-

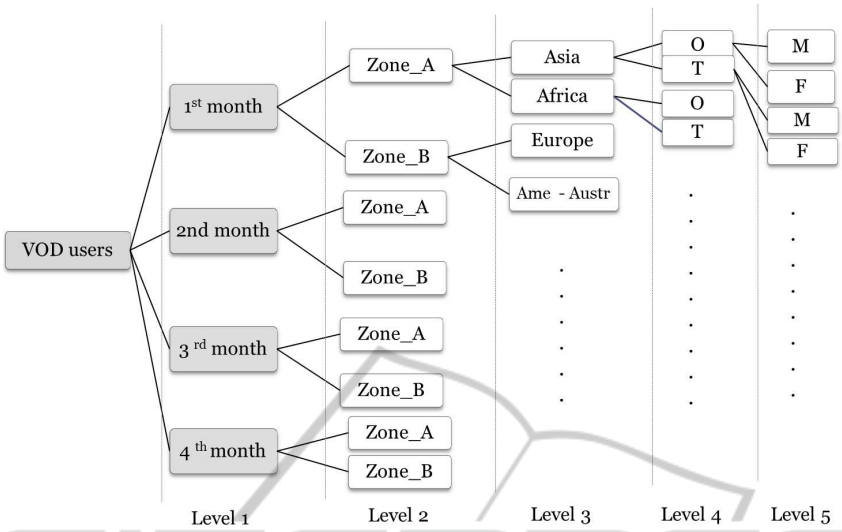

Figure 2: The proposed 5-level hierarchy for the fingerprint.

straint corresponds to a level. We detail our construction more precisely in the following.

3.1.1 Temporal Constraint

This constraint is tied to the time a video stays accessed by viewers. The frequency of the access to a video in a VOD platform depends on its popularity. In the beginning, when a video belonging to the Top 10 is added to a VOD platform, users are very curious and the frequency accessing is very important, this behavior changers later to decrease significantly over time. In (Choi et al., 2012), the viewer interest decreases from 100% to less than 10% during a 4-month period. Thats why, in the time level,we choose to represent the four first months by four groups where each group is one month spent by a video in VOD application.

3.1.2 Geographic Constraint

According to this constraint, we assume that two users belonging to the same geographic place are more able to collude together than with other users from other regions. We have studied later in (Chaabane et al., 2013), according to BSA report, that the software piracy is more important in some countries than in others.

3.1.3 Social Constraints

We have enhanced our study with statistics shared by the NPD, National Purchase Diary Group, known for its consumer market research. The NPD has studied the media traffic in one of the most popular

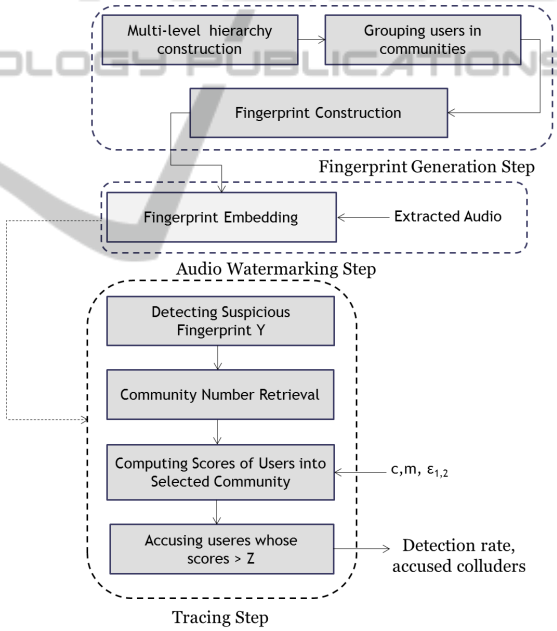

Figure 3: The proposed tracing traitors framework.

VOD service, Netflix, and has shown that audience behavior changes depending on the age and the gender, the highest rate of users in a week is noted with persons under 15 years old age, this study demonstrates also that men are less interested with VOD services than women.Thus, according to these statistics, we remind the 5-level hierarchy we adopted in (Chaabane et al., 2013), where each criterion is represented by a level in the hierarchy. The first level is the time level where we assume that the most important period for a video life in a VOD platform is about 4 months (Choi et al., 2012), (Liu et al.,

2014). Thats why, we considerate four groups in this way:in the first group, users curiosity is moderately important, it increases in the second month to reach the maximal audience interest, it decreases later in the third month to the minimal bound in the fourth one. The second level in the hierarchy represents the geographic criterion where we propose to divide VOD users to two essential regions:Zone_A where the piracy phenomenon is very important, especially in Asia and Africa continents, and Zone_B where the piracy phenomenon is less important especially in Europe, America and Austria. We divide each continent to two groups of principal countries in the third level. In the fourth and the fifth levels, we are interested in social criteria, respectively the age and the gender ones. Once the hierarchy is fixed, we form communities so that users having the same characteristics belong to the same community and have more probability to collude together in a forgery attempt than with users belonging to other communities. The resulting fingerprint for each user is the concatenation of his community identifier concatenated to his personal identifier which is encoded with Tardos code.

$$Final\_identifer = id\_level1 + id\_level2 + .. + id\_level5 + personal\_id \quad (1)$$

This hierarchy strategy is taken especially to reduce computational costs and time during the Tardos accusation process. Instead of parsing the totality of embedded codewords, we search firstly the committee having the highest similarity to the group identifier of the colluded codeword, and then we compute users scores belonging to it. The VOD context does not require that the tracing step should be performed in real time. The whole operations of decoding and accusation are made offline. In the next section, we describe the used watermarking technique.

3.2 Embedding Strategy: Audio Watermarking Technique using DCT Transform

Embedding collusion secure fingerprint codes with a robust watermarking technique has necessarily impacts in a tracing scheme, mainly against different types of attacks. In our tracing approach, we propose to use an audio watermarking technique described in details in (Charfeddine et al., 2010) and then applying DCT to them. The watermark is inserted in the middle frequencies of each block. The watermark is hidden especially in the sample closest to the average value of a localized middle frequencies band. The neural Network is used here to be trained to retrieve from eight neighbors samples the nearest sample having the best embedding position. The resulting watermarked signal is obtained after applying the IDCT. The detection step is the inverse process of the insertion one. Once the multi-level fingerprint is embedded, the video is diffused. The tracing process is launched then in the distributor side.

3.3 Tracing Process

As shown in figure 2, the whole framework can be divided into multiple phases: when the supplier detects a copy with unknown fingerprint Y, he decides to trace back colluders by analyzing the watermark to extract its ID_{group} and retrieving its belonging to a community. The tracing is performed by the Tardos code, which represents our forensic code. This probabilistic code consists in generating firstly a set of density probabilities $\{p_1 \cdots p_m\} \in \{0 \cdots 1\}$ and then constructing a matrix of n codewords X_{ji} of length m with Prob[X_{ji}=1] = p_i .In our approach, we use the symmetric function to decode whatever is the collusion strategy. The correlation between the suspicious fingerprint and codewords and the score $S_{j,j\in\{1...n\}}$ per user are computed with ε_1 and ε_2 are respectively the false positive and the false negative error probabilities:

$$S_j = \sum_{i=1}^{m} g(Y_i, X_{ji}, p_i) \quad (2)$$

$$g(1,1,p) = g(0,0,1-p) = \sqrt{\frac{(1-p)}{p}} \quad (3)$$

$$g(1,0,p) = g(0,1,1-p) = -\sqrt{\frac{p}{(1-p)}}$$

It is applied only to users in the selected community. We assume that users in the same community have more probability to collude together (Desoubeaux et al., 2012) than with users belonging to another community. We compute the score Sj per user in the corresponding community. The principle of Tardos accusation is to compute the similarity between the codeword X_j and the suspicious word Y for each position j.The user whose score is higher than the threshold Z is thus accused. Steps of the Tardos accusation process are more detailed in (Chaabane et al., 2013). At the last, as a result of our tracing algorithm, we compute the detection rate of our system, if we obtain a detection rate det_rate close to 100%, the accusation is successful, which means that the number of retrieved users Retrieved_collu is equal to the real number of Our tracing algorithm is briefly detailed below; we assume that inputs are respectively: the code length m, the collusion size c, the threshold Z and the suspicious word Y. colluders c.

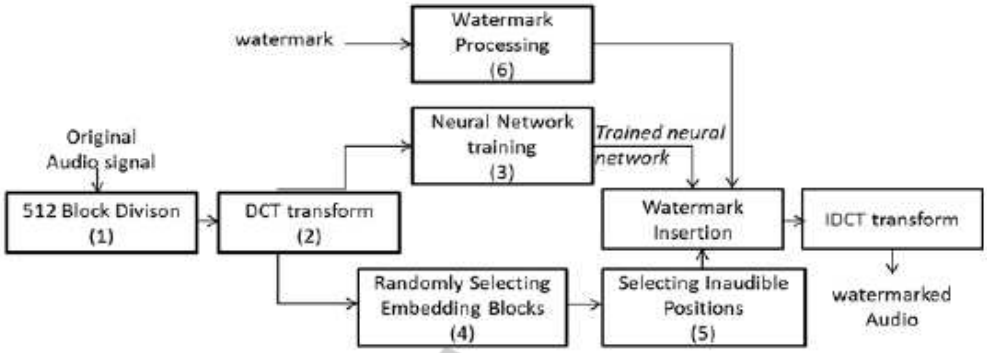

Figure 4: Embedding step of the used audio watermarking technique.

```
Begin

Procedure calcul_rate(m,Z: Real; c: Int,Y: Vector;
 var det_rate, Sj: Real);
ID_community := ID_group(Y);
nb := size(ID_community);
While (j < c) and (j < nb) do
sj :=score (xj, Y, m) ;
if (sj > Z) then
return xj;
Retrived_collu := Retrieved_collu+1;
end
j := j+1;
end
det_rate := retrieved_coll / c;

End.
```

Figure 5: Snapshots samples of experimented videos respectively tv_prog.avi, ice_film.avi, music_clip.avi and sport.avi.

4 EXPERIMENTAL RESULTS

The real challenge of a tracing traitors scheme is to cover the gap between theoretical and practical results. Optimizing the fingerprinting code parameters and preserving the robustness even if the collusion size increases are the most important requirements for a tracing traitors scheme. According to the studies made by (Choi et al., 2012) the most required videos in a VOD platform are films, TV reality programs, sport competitions and music clips. For this reason, we have chosen four avi video samples belonging to the four types. The extracted audio files are of duration of 5min16s. In our paper, we show experimental results obtained by ice_film.avi and we prove firstly the robustness of our scheme against all types of attacks and then we vary collusion size and we present the detection results.

4.1 Tracing Traitor Attacks

Attacks in tracing traitor field are classified according to the layer they attack. We distinguish as a first class attacks on the watermarking scheme, which are applied to destroy the watermark, this type of attacks reflect the robustness of the watermarking technique. In experimentation section, we test the robustness of our scheme against compression (128, 96 and 64 Kbps) and some Stirmark attacks. The second class consists in a scenario made by a group of users to construct a false video copy with unknown fingerprint. Colluders participating to such strategies try to make their identification too hard to the supplier. In our work, we suppose that the type of colluders strategy is known and we are interested to the most common collusion attacks (Hamida et al., 2011): majority/minority vote, all1 and all0 attacks.

In the table below, we present for each collusion attack an example to describe it.

Table 1: The most common collusion attacks.

Attack strategy	Example
Majority vote attack	0 1 0 1 0 0 1 1 1 1 1 0
Minority vote attack	0 1 0 1 0 0 1 1 1 0 0 1
Allone attack	0 1 0 1 0 0 1 1 1 1 1 1
Allzero attack	0 1 0 1 0 0 1 1 1 0 0 0

4.2 Robustness and Inaudibility Results

We use two major criteria in this experimental part: NC, the Normalized Cross Correlation, which value reflects the similarity between the original watermark and the detected one, and the SNR, the Signal to Noise Ratio, which is an objective measure to show the quality of the audio after the insertion step.

$$SNR = 10 \times \log\left(\frac{\sum_i Y_i^2}{\sum_i \left(Y_i - Y'\right)^2}\right) \quad (4)$$

Y and Y are respectively the original audio and the watermarked one.

$$NC = \frac{\sum_{x=1}^{N} W(x) \cdot W'(x)}{\sqrt{\sum_{x=1}^{N} W(x)^2 \cdot \sum_{x=1}^{N} W'(x)^2}} \quad (5)$$

W and W are respectively the original watermark and the detected one.
We remind that Tardos parameters m and c are tied by the equation below:

$$m = 2\Pi^2 c^2 \left[\ln \frac{1}{\varepsilon_1}\right] \quad (6)$$

In the table above, we show the different values of collusion size c, the false alarm probability and the code length variations. We vary also the total number of users from 10, 100 and 1000.

Table 2: Collusion size, false alarm probability and code length variations.

Collusion size	False alarm value	Code length
c=5	$\varepsilon_1 = 10^{-3}$	m=3455
c=5	$\varepsilon_1 = 10^{-4}$	m=4935
c=5	$\varepsilon_1 = 10^{-7}$	m=8390

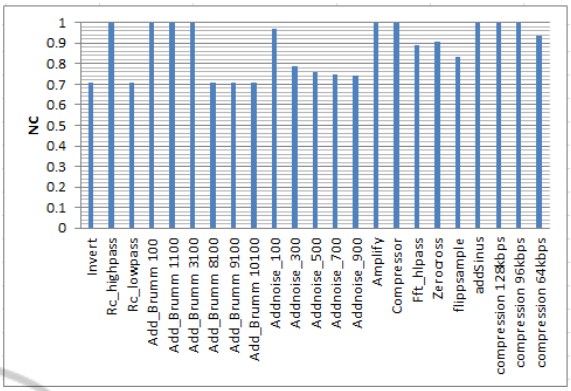

Figure 6: Robustness against Stirmark and compression attacks with Tardos parameters: n=100, $\varepsilon_1 = 10^{-3}, c = 5, SNR = 53.0262$.

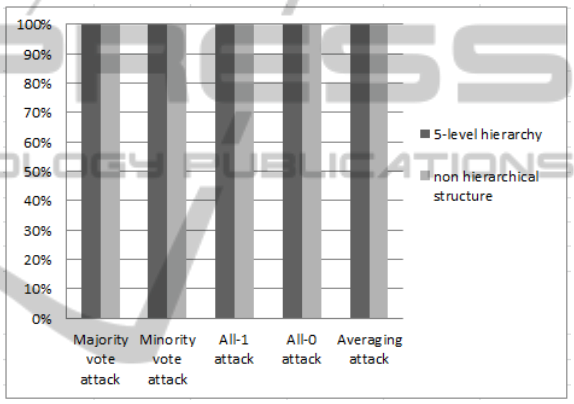

Figure 7: Detection rates for the two structures with Tardos parameters: n=100,$\varepsilon_1 = 10^{-3}, c = 5, 100 trials$.

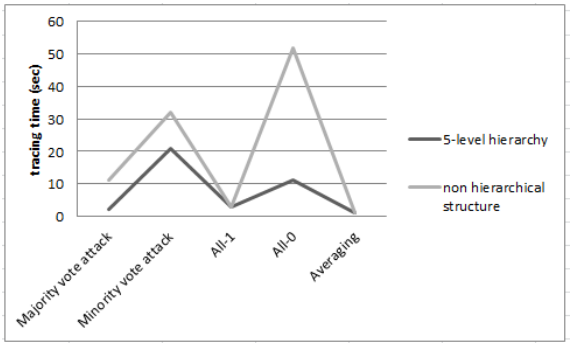

Figure 8: Tracing time for the two types of structures in the case for clip.avi, Tardos parameters: n=100,$\varepsilon_1 = 10^{-3}, c = 5, 100 trials$.

In order to test our system performance against different types of attacks, we compare it to a nonhierarchical fingerprint under the same parameters the fingerprint length m = 3455, the number of users n=100 and the collusion size c=5. The detection rate and the CPU time are important tracing criteria. We can remark from figures 6, 7, 8, 9, 10, 11 and 12 that

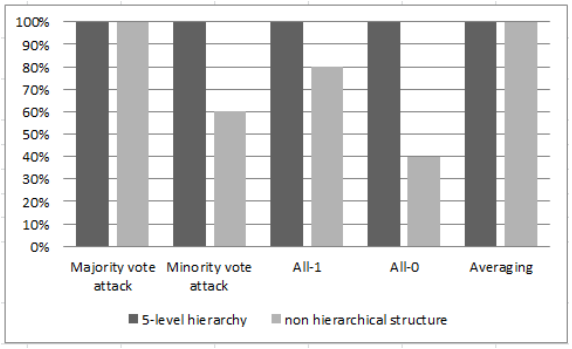

Figure 9: Detection rates for the two structures with Tardos parameters: n=1000,$\varepsilon_1 = 10^{-4}, c = 5,100 trials$.

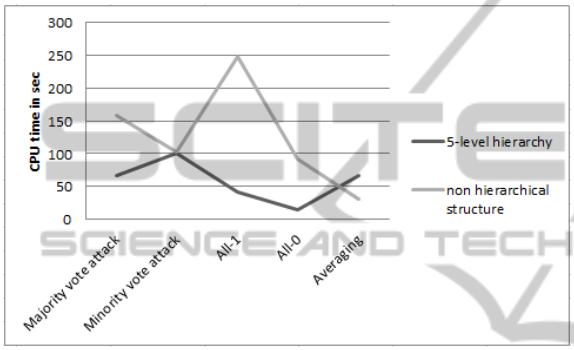

Figure 10: Tracing time for the two types of structures with Tardos parameters: n=1000,$\varepsilon_1 = 10^{-4}, c = 5,100 trials$.

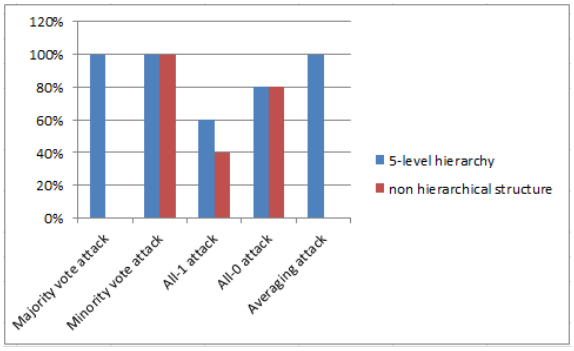

Figure 11: Detection rates for the two structures with Tardos parameters: n=1000,,$\varepsilon_1 = 10^{-7}, c = 5 for clip.avi, 100 trials$.

the detection rates of our hierarchical fingerprint are preserved while the nonhierarchical structure performance decreases notably if the user number increases and the false probability decreased.

5 CONCLUSIONS

In this paper, we have presented our contribution in tracing traitors field. We have proposed a multilevel hierarchical fingerprint to reduce tracing and computational costs of Tardos code; we have proposed also to hide this fingerprint with a robust audio watermarking technique which is a choice different from proposed works in literature. Our proposed system has provided good robustness against different types of attacks and good detection rates. In future work, we propose to assume that the collusion strategy is unknown and we will try to estimate it.

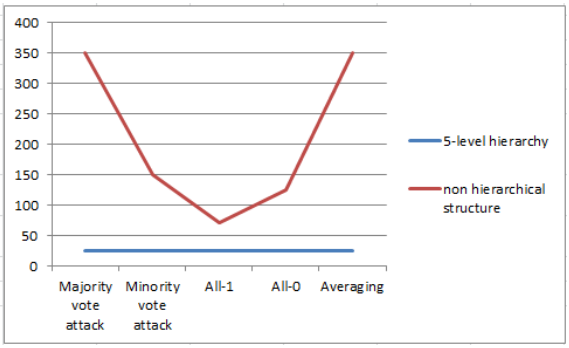

Figure 12: Tracing time for the two types of structures with Tardos parameters: n=1000,,$\varepsilon_1 = 10^{-7}, c = 5100 trials$.

REFERENCES

Chaabane, F., Charfeddine, M., and Amar, C. B. (2013). A survey on digital tracing traitors schemes. In *Information Assurance and Security*, pages 85–90.

Charfeddine, M., El'arbi, M., Koubàa, M., and Amar, C. B. (2010). Dct based blind audio watermarking scheme. In *SIGMAP*, pages 139–144.

Charpentier, A., Fontaine, C., Furon, T., and Cox, I. J. (2011). An asymmetric fingerprinting scheme based on tardos codes. In *Information Hiding*, pages 43–58.

Charpentier, A., Xie, F., Fontaine, C., and Furon, T. (2009). Expectation maximization decoding of tardos probabilistic fingerprinting code. In *Media Forensics and Security*, page 72540.

Choi, J., Reaz, A. S., and Mukherjee, B. (2012). A survey of user behavior in vod service and bandwidth-saving multicast streaming schemes. *IEEE Communications Surveys and Tutorials*, 14(1):156–169.

Desoubeaux, M., Guelvouita, G. L., and Puech, W. (2011). Probabilistic fingerprinting codes used to detect traitor zero-bit watermark. In *SPIE Proceedings Vol. 7880: Media Watermarking, Security, and Forensics III*.

Desoubeaux, M., Guelvouita, G. L., and Puech, W. (2012). Fast detection of tardos codes with boneh-shaw types. In *Proc. SPIE 8303, Media Watermarking, Security, and Forensics*.

Furon, T., Pérez-Freire, L., Guyader, A., and Cérou, F. (2009). Estimating the minimal length of tardos code. In *Information Hiding*, pages 176–190.

Hamida, A. B., Koubàa, M., and Nicolas, H. (2011). Hierarchical traceability of multimedia documents. In

Computational Intelligence in Cyber Security, pages 108–113.

Hayashi, N., Kuribayashi, M., and Morii, M. (2007). Collusion-resistant fingerprinting scheme based on the cdma-technique. In *IWSEC*, pages 28–43.

Laarhoven, T. (2013). Dynamic traitor tracing schemes, revisited. *CoRR*, abs/1307.0214.

Laarhoven, T. and de Weger, B. (2011). Optimal symmetric tardos traitor tracing schemes. *CoRR*, abs/1107.3441.

Shahid, Z., Chaumont, M., and Puech, W. (2013). H.264/avc video watermarking for active fingerprinting based on tardos code. *Signal, Image and Video Processing*, 7(4):679–694.

Tardos, G. (2003). Optimal probabilistic fingerprint codes. In *STOC*, pages 116–125.

Wang, Z. J., Wu, M., Trappe, W., and Liu, K. J. R. (2004). Group-oriented fingerprinting for multimedia forensics. *EURASIP J. Adv. Sig. Proc.*, 2004(14):2153–2173.

Ye, C., Ling, H., Zou, F., and Lu, Z. (2013). A new fingerprinting scheme using social network analysis for majority attack. *Telecommunication Systems*, 54(3):315–331.