EFFECTIVE INTERFERENCE REDUCTION METHOD FOR SPREAD SPECTRUM FINGERPRINTING

Minoru Kuribayashi
Graduate School of Engineering, Kobe University, 1-1, Rokkodai-cho, Nada, Kobe, 657-8501, Hyogo, Japan

Keywords: Spread spectrum fingerprinting, Collusion attack, Removal operation, Iterative detection.

Abstract: The iterative detection method was proposed in IH2008 specified for the CDMA-based fingerprinting scheme which embedding procedure was additive watermarking method. Such a detection method is applicable for the multiplicative watermarking method that modulates a fingerprint using the characteristic of a content. In this study, we study the interference among fingerprints embedded in a content in the hierarchical version of Cox's scheme, and propose the effective detection method that iteratively detects colluders combined with a removal operation. By introducing two kinds of thresholds, the removal operation is adaptively performed to reduce the interference without causing serious false detection.

1 INTRODUCTION

A growing number of techniques have been proposed to provide collusion resistance in multimedia fingerprinting systems. Many of them can be categorized into two approaches; the orthogonal sequence and fingerprinting code. Orthogonal fingerprinting is a typical example of designing fingerprint signals. It assigns a spread spectrum sequence to each user and the sequences among users are mutually orthogonal. The design of collusion-resistant fingerprint codes was presented by Boneh ans Shaw (Boneh and Shaw, 1998) for generic data. This fingerprinting scheme is further improved in (Yacobi, 2001) by combining a spread spectrum watermarking like Cox's scheme (Cox et al., 1997) with the Boneh-Shaw's code. Such a two-layered fingerprinting scheme is intensively studied to improve the collusion resistance and the required computational resource points of view. It is worth mentioning that most of the variants of the two-layered scheme use the Cox's scheme in some manner.

In Cox's scheme (Cox et al., 1997), a spread spectrum sequence following an i.i.d. Gaussian distribution with zero mean and variance 1, $N(0,1)$ is embedded into the frequency components of a digital image. Since normally distributed values allow the theoretical and statistical analysis of the method, modeling of a variety of attacks has been studied. Studies in (Zhao et al., 2005) have shown that a number of non-linear collusions such as an interleaving attack can be well approximated by averaging collusion plus additive noise. One of the drawbacks of Cox's scheme is the amount of computational resources required for the detection that is linearly increased with the number of users in the fingerprinting system. Wang et al. (Wang et al., 2004) reduced the computational costs by introducing the idea of grouping. This concept of grouping has been applied to variants of spread spectrum fingerprinting (He and Wu, 2006), (Hayashi et al., 2007) and to the construction of a collusion secure code (Lin et al., 2007). In (Hayashi et al., 2007), a fingerprint sequence was designed using DCT basic vectors modulated by PN sequences such as the M-sequence and Gold sequence in order to further reduce the computational costs. In (Kuribayashi and Morii, 2008), the traceability of the fingerprinting scheme whose embedding operation is additive watermarking was improved by the iterative detection with the removal operation. By introducing two kinds of thresholds, an adaptive detection for both group and user IDs is performed.

In this paper, we study the characteristic of multiplicative watermarking method and present the iterative detection method combined with the removal operation for the hierarchical version of Cox's scheme. The amount of fingerprint signals can be detected from the extracted signal from a pirated copy using the similarity measurement. However, the similarity function presented in Cox's scheme is normalized

Kuribayashi M..
EFFECTIVE INTERFERENCE REDUCTION METHOD FOR SPREAD SPECTRUM FINGERPRINTING.
DOI: 10.5220/0003497101670172
In *Proceedings of the International Conference on Signal Processing and Multimedia Applications* (SIGMAP-2011), pages 167-172
ISBN: 978-989-8425-72-0

correlation score, which is not the amount of energy. By calculating the energy from the similarity measurement, the corresponding fingerprint signals can be removed from the extracted signal in order to reduce the interference among fingerprint signals. We consider the interference among detected fingerprint signals and propose a specific removal operation to further improve the traceability.

2 PRELIMINARIES

2.1 Spread Spectrum Watermarking

In Cox's scheme (Cox et al., 1997), a spread spectrum sequence following an i.i.d. Gaussian distribution with zero mean and variance 1, $N(0,1)$ is embedded into the frequency components of a digital image.

Let $v = \{v_0, \ldots, v_{\ell-1}\}$ be the frequency components of a digital image and $w = \{w_0, \ldots, w_{\ell-1}\}$ be the fingerprint sequence. We insert w into v to obtain a watermarked sequence v^*. At the detector side, we determine which SS sequences are present in a pirated copy by evaluating the similarity of sequences. When a sequence $\tilde{w}$ is extracted by calculating the difference between an original copy and pirated one, and its similarity with w is obtained as follows.

$$\mathsf{sim}(w, \tilde{w}) = \frac{w \cdot \tilde{w}}{\sqrt{\tilde{w} \cdot \tilde{w}}}, \tag{1}$$

If the value exceeds a threshold, the embedded sequence is regarded as w.

When we insert a watermark w into v, we specify a scaling parameter α and select one of the three embedding formulas for computing v^*.

$$v_t^* = v_t + \alpha w_t \tag{2}$$
$$v_t^* = v_t(1 + \alpha w_t) \tag{3}$$
$$v_t^* = v_t(e^{\alpha w_t}) \tag{4}$$

Specifically, the watermarking scheme that use Eq.(2) is called additive and the scheme that use Eq.(3) is called multiplicative. In this paper, we employ Eq.(3) to embed fingerprints.

In a fingerprinting scheme, each watermarked copy is slightly different; hence, malicious users can collect c copies $D_1, \ldots, D_c$ with respective watermarks $w_1, \ldots, w_c$ in order to remove/alter the watermarks. A simple, yet effective way is to average them because when c copies are averaged, $\tilde{D} = (D_1 + \ldots + D_c)/c$, the similarity value calculated by Eq.(1) is reduced by a factor of c. Studies in (Zhao et al., 2005) have shown that a number of nonlinear collusions such as interleaving attack can be well approximated by averaging collusion plus additive noise.

2.2 Grouping

There is a common disadvantage in Cox's scheme and its variants such that high computational resources are required for the detection because the correlation values of all spread spectrum sequences must be calculated. For the reduction of computational costs, hierarchical spread spectrum fingerprinting schemes have been proposed. The motivation of the scheme proposed by Wang et al. (Wang et al., 2004) is to divide a set of users into different subset and assign each subset to a specific group whose members are more likely to collude with each other than with members from other groups. With the assumption that the users in the same group are equally likely to collude with each other, the fingerprints in one group have equal correlation. At the detection, the independency among groups limits the amount of innocent users falsely placed under suspicion within a group, because the probability of accusing another group is very large.

We assume that the number of groups is ℓ and that of users in individual group is also ℓ for simplicity. Thus, the total number of users is $\ell \times \ell$. The fingerprint sequence $w^{(i,j)}$ assigned to the j-th user within the i-th group consists of two components.

$$w^{(i,j)} = w_g^{(i)} + w_u^{(i,j)}, \tag{5}$$

where $w_g^{(i)}$ is the spread spectrum sequence for the i-th group and $w_u^{(i,j)}$ is that for the j-th user. Because of the presence of the common vector $w_g^{(i)}$, when colluders from the same group average their copies, the energy of the vector is not attenuated; hence, the detector can accurately identify the group. The detection algorithm consists of two stages; one involves the identification of groups containing colluders, and the other, the identification of colluders within each suspicious group.

Let $\tilde{v} = \{\tilde{v}_0, \ldots, \tilde{v}_{\ell-1}\}$ be the frequency components extracted from a pirated copy. Since a fingerprint sequence is embedded by the formula in Eq.(3), the sequence $\tilde{w} = \{\tilde{w}_0, \ldots, \tilde{w}_{\ell-1}\}$ is calculated by removing the frequency components of original image from $\tilde{v}$ as follows.

$$\tilde{w}_t = \frac{\tilde{v}_t - v_t}{\alpha v_t} \tag{6}$$

Using the original sequences $w_g^{(i)}$ assigned for groups, the detection of group ID is performed as follows.

1. Calculate the similarity values $S_g^{(i)}$ of all groups.

$$S_g^{(i)} = \mathsf{sim}(\tilde{w}, w_g^{(i)}) \tag{7}$$

2. Calculate the variance σ_g^2 of $S_g^{(i)}$ by considering the property of its distribution and determine a

threshold T_g from a given false-positive probability P_g.

$$T_g = \sqrt{2\sigma_g^2}\mathrm{erfc}^{-1}(2P_g) \quad (8)$$

3. If $S_g^{(i)} \geq T_g$, the i-th group is judged guilty group.

If a pirated copy is generated from multiple fingerprinted copies, the number of the guilty group is equal or more than 1.

For each guilty group, the detection of colluders involved in the group is performed as follows.

1. Calculate the similarity values $S_u^{(i,j)}$ of all users in the i-th group.

$$S_u^{(i,j)} = \mathrm{sim}(\tilde{w}, w_u^{(i,j)}) \quad (9)$$

2. Calculate the variance σ_u^2 of $S_u^{(i,j)}$ by considering the property of its distribution and determine a threshold T_u from a given false-positive probability P_u.

$$T_u = \sqrt{2\sigma_u^2}\mathrm{erfc}^{-1}(2P_u) \quad (10)$$

3. If $S_u^{(i,j)} \geq T_u$, the j-th user in the i-th group is judged guilty.

2.3 Iterative Detection

In (Hayashi et al., 2007), the fingerprint sequences are designed by DCT basic vectors modulated by PN sequences such as M-sequence and Gold-sequence in order to further reduce the computational costs. Because of the assistance of fast DCT algorithm, the computation of correlation values at the detector is dropped to logarithmic scale. The embedding formula used in (Hayashi et al., 2007) is Eq.(2), and hence, it is additive watermarking. The detection procedure is further improved in (Kuribayashi and Morii, 2008) to catch more colluders without increasing the probability of false-positive by introducing the idea of iterative detection and removal operation.

Because the sequence extracted from a pirated copy will contain some colluders' fingerprint signals, they work as an interference at the detection of each objective signal. For example, once a certain group ID is detected, its signal is merely a noise at the detection of user ID. Thus, if a detected fingerprint signal is removed from the extracted sequence, the traceability can be improved. In (Kuribayashi and Morii, 2008), the removal operation is performed sequentially for the detected signals and the detection procedure using removal operation is performed iteratively. However, due to the increase of the number of colluders, wrong signals will be accidentally detected because the effects of interference are increased with respect to the number. In such a case, the undetected fingerprint signal is attenuated by the removal operation.

For the detection of group ID, the false-negative detection of fingerprinted signals is much serious because the following detection of the user ID is not conducted. Even if the false-positive detection of group ID is increased, the actual false-positive detection is bounded to the detection of the user ID. When the threshold T_g for group ID goes down, the number of detected group ID is increased. It provides the chance for mining the corresponding user ID from a detection sequence. If all detected signals are removed as an interference, wrongly detected signals at the detection of group ID are also removed and the detection operation is performed again with the threshold which goes down after the removal under a constantly designed false-positive rate. Hence, the repeat of detection operation provides the chance, regretfully, to detect wrong ID by mistake, which causes the increase of the false detection. In order not to remove too much, two kinds of thresholds both for group ID and user ID are introduced in (Kuribayashi and Morii, 2008).

Using those two kinds of thresholds, the fingerprint signals are detected adaptively as follows. We first detect as many suspicious group IDs as possible using a lower threshold, and the detected signals that exceed a higher threshold are removed from the detection sequence. Then, for the detected suspicious groups, we attempt to detect the corresponding users. The detected signals as the user ID are removed from the detection sequence, and if the fingerprint signals of group IDs corresponding the detected user IDs have not been removed, they are also removed. Such operations are repeatedly performed until no user ID is detected. Finally, some candidates of user ID are judged using a higher threshold, and guilty users are identified.

3 PROPOSED SCHEME

Our goal is to identify as many colluders as possible from the sequence $\tilde{w}$ with small and constant false-positive probability for the group-based fingerprinting scheme that embeds spread spectrum sequences by a multiplicative watermarking method.

For the detection of group ID, the false negative detection of fingerprinted signals is much serious because the following detection of the user ID is not conducted. In order to mining more colluders without removing too much signals by the removal operation, two kinds of thresholds both for group ID and user ID are introduced. These thresholds and related parame-

ters are classified into high and low using the capitals "H" and "L".

1. Calculate the similarity values $S_g^{(i)}$ of all groups.
2. Calculate the variance σ_g^2 of $S_g^{(i)}$ by considering the property of its distribution and determine two thresholds T_g^L and T_g^H by Eq.(8) from given false-positive probabilities P_g^L and P_g^H, respectively.
3. If $S_g^{(i)} \geq T_g^L$, the i-th group is judged suspicious group.
4. If $S_g^{(i)} \geq T_g^H$, then the corresponding fingerprint signals are removed from $\tilde{w}$,

$$\tilde{w} \leftarrow \tilde{w} - \sum_{S_g^{(i)} \geq T_g^H} \frac{S_g^{(i)}}{\sqrt{\ell}} w_g^{(i)}, \tag{11}$$

   and the values $S_g^{(i)}$ are stored in $\hat{S}_g^{(i)}$.
5. For each suspicious group, if no user has been judged suspect yet, the detection of colluders involved in the group is performed as follows.
   5-1 Calculate the similarity values $S_u^{(i,j)}$ of all users in the i-th group.
   5-2 Calculate the variance σ_u^2 of $S_u^{(i,j)}$ by considering the property of its distribution and determine a threshold T_u^L from a given false-positive probability P_u^L.
   5-3 If $S_u^{(i,j)} \geq T_u^L$, the j-th user in the i-th group is judged suspect, and the corresponding fingerprint signals are removed from $\tilde{w}$.

$$\tilde{w} \leftarrow \tilde{w} - \sum_{S_u^{(i,j)} \geq T_u^L} \frac{S_u^{(i,j)}}{\sqrt{\ell}} w_u^{(i,j)} \tag{12}$$

   The values $S_u^{(i,j)}$ are stored in $\hat{S}_u^{(i,j)}$.
   5-4 For the i-th group such that the i-th user is judged suspect, if $S_g^{(i)} \ngeq T_g^H$ at Step.4, recalculate $S_g^{(i)}$ and remove the corresponding fingerprint signal from $\tilde{w}$.

$$\tilde{w} \leftarrow \tilde{w} - \frac{S_g^{(i)}}{\sqrt{\ell}} w_g^{(i)} \tag{13}$$

   The value $S_g^{(i)}$ is stored in $\hat{S}_g^{(i)}$.
6. For the groups and users judged suspects, recalculate $S_g^{(i)}$ and $S_u^{(i,j)}$, and remove the corresponding fingerprint signals from $\tilde{w}$. The stored values $\hat{S}_g^{(i)}$ and $\hat{S}_u^{(i,j)}$ are incremented as follows.

$$\hat{S}_g^{(i)} \leftarrow \hat{S}_g^{(i)} + S_g^{(i)} \tag{14}$$

$$\hat{S}_u^{(i,j)} \leftarrow \hat{S}_u^{(i,j)} + S_u^{(i,j)} \tag{15}$$

7. At least one suspect user ID is detected by Step 5, go to Step 1; otherwise, go to Step 8.
8. Calculate a higher threshold T_u^H from a given false-positive probability P_u^H using the variance σ_u^2.
9. If $\hat{S}_g^{(i)} \geq T_u^H$ and $\hat{S}_u^{(i,j)} \geq T_u^H$, then the j-th user in the i-th group is finally judged guilty.

The actual probability of false-positive at the detection is strongly related to the final decision, and the critical parameter is the higher threshold T_u^H. Regretfully, the design in the conventional method (Kuribayashi and Morii, 2008) completely ignores the number of trials for detecting user ID, denoted by N^{trial}, because the actual probability of false-positive is estimated as $N^{trial} P_u^H$. In the above detection procedure, N^{trial} is the number of trials performing Step 5. So, the threshold T_u^H is calculated by the following equation:

$$T_u^H = \sqrt{2\sigma_u^2}\,\mathrm{erfc}^{-1}\left(\frac{2P_u^H}{N^{trial}}\right) \tag{16}$$

It is worth mentioning that the removal operation in Step 6 adjusts properly the detected similarity values. Because of the mutual interference among fingerprint sequences, the similarity values calculated at early stage in the detection process involve large noise term, and the amount of noise energy is, in general, large when the number of fingerprint sequences involved in $\tilde{w}$ is large. Therefore, the similarity values detected at the early stage involve much noise. The removal operation for the corresponding signals may not reduces the interference, but rather causes further distortion, which results in the increase of the false-positive probability. Thus, the removal operation in Step 6 controls the above effect in order to properly remove the fingerprint signals. For the comparison, the method without Step 6 is denoted by "method I" and that with Step 6, by "method II", and the performance is evaluated in the next section.

4 EXPERIMENTAL RESULTS

The performance of the proposed methods is evaluated by detecting colluders using different 10^4 kinds of combination of IDs. We use a standard "lena" image with a 256-level gray scale and a size of 512×512 pixels. The scaling parameter is fixed in our simulation by $\alpha = 0.07$ and the length of sequence is $\ell = 1000$. The number of groups is 10^3 and that of users in an individual group is also 10^3, hence, the total number of users is 10^6 in this simulation. Then, the PSNR value of a fingerprinted image is about 35 [dB] when a fingerprint is embedded into an image

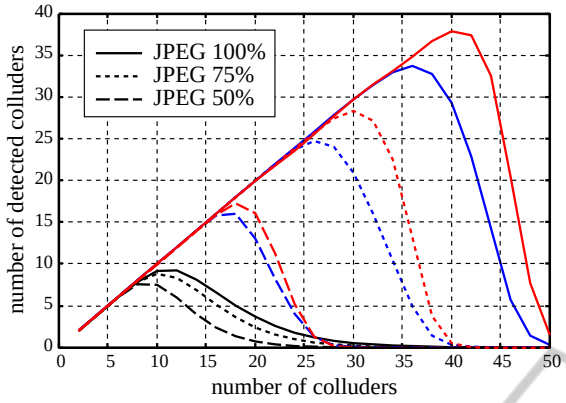


Figure 1: Number of detected colluders, where black, blue, and red lines are the results using the original detection method, method I, and method Ⅱ, respectively.

"lena" using the above parameters. The given false-positive probabilities are fixed by $P_g^L = 0.5 \times 10^{-2}$, $P_g^H = 1.0 \times 10^{-4}$, $P_u^L = 1.0 \times 10^{-5}$, and $P_u^H = 1.0 \times 10^{-8}$. It is noted that the final false-positive probability is designed to be 1.0×10^{-4} by Eq.(16). A pirated copy is produced by averaging c copies whose fingerprint is randomly selected from 10^6 candidates. It implies that colluders are likely to come from different groups, which is the worst case in group-based scheme.

The number of detected colluders is measured under the conditions such that fingerprinted images are averaged and compressed by JPEG algorithm. When the quality factor is large, the additive noise caused by the attack is small. Figure 1 show the number of detected colluders, where solid, dotted, and dashed lines are the results using the JPEG quality factor 100%, 75% and 50%, respectively. The number of detected colluders are considerably increased using the proposed iterative detection methods. It is because the removal operation effectively reduces the interference term involved in $\tilde{w}$, and the iteration of the detecting operation enables us to catch more colluders from the incremented $\tilde{w}$. It is noticed that the method Ⅱ detects more colluders than the method I. The improvement of the performance comes from the operation in Step 6 that controls the amount of the signals removed from $\tilde{w}$.

The probability of false-positive is also measured under the above conditions. The average probability accusing innocent users is shown in Table 1. Compared with the probabilities of original method, those of method I are larger. The reason comes from the wrong detection of fingerprint signals of innocent groups and users at the early stage in the iterative detection. Even if such wrongly detected innocent users

Table 1: Probability of false-positive $[\times 10^{-4}]$.

JPEG	original	method I	method Ⅱ
50	0.92	404.24	2.36
75	0.84	1230.04	3.84
100	0.76	2432.00	1.92

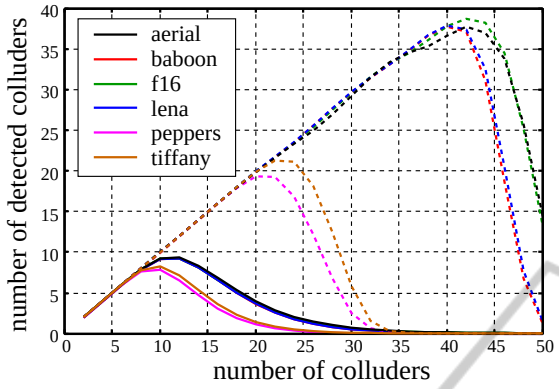
are excluded with high probability at the final judgment, the distortions caused by the removal operation further degrade $\tilde{w}$ and they increase the probability of false-positive. It is noticed from the results of method Ⅱ that the control of removal operation in Step 6 also reduce such distortions.

The performance of proposed method Ⅱ is evaluated under averaging collusion. For simplicity, no additional attacks for a pirated copy is done in this experiment. Figure 2 show the number of detected colluders for images "aerial", "baboon", "f16", "lena", "peppers", and "tiffany". Because the some results of original method are almost equal, those lines lap over. It is observed that the number of detected colluders is drastically increased by the proposed method compared with the original method. It confirms that the iterative detection with removal operation effectively improves the performance. However, we can see from the figure that the performance is strongly dependent on the characteristic of host image. It is because of the property of the multiplicative watermarking. The probability of false-positive is shown in Table 2. It is observed that the probability of proposed scheme is slightly increased from that of original one. This comes from the removal operation that occasionally removes wrongly detected signals. An adaptive setting of the thresholds T_g^L, T_g^H, T_u^L, and T_u^H will enhance the performance. The detailed analysis of the dependency among those thresholds and the number of detected colluders is left for our future work.

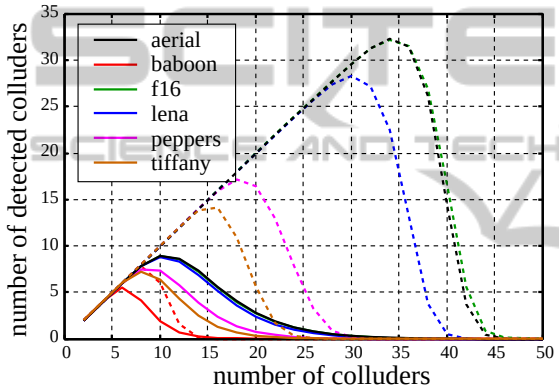
5 CONCLUSIONS

In this paper, we implemented the iterative detection method plus the removal operation for the hierarchical version of Cox's fingerprinting scheme. Considering the characteristic of multiplicative watermarking, the amount of removed signals is controlled in the detection procedure. From the experimental results, the number of detected colluders of proposed methods is considerably increased compared with that of the original method. Even if the false-positive probability is slightly increased in the proposed method, the control of the amount of fingerprint signals removed from the extracted signal effectively improve the performance. If the removal operation can further clas-

sify the innocent/guilty groups and users, the performance of the proposed methods can be improved.



(a) JPEG 100%



(b) JPEG 75%

Figure 2: Number of detected colluders for various images, where solid and dot lines are the results using the original method and method Ⅱ, respectively.

Table 2: Probability of false-positive $[\times 10^{-4}]$ for various images.

image	detector	JPEG quality		
		100%	75%	50%
aerial	original	0.64	0.64	0.60
	method Ⅱ	3.72	4.16	3.04
baboon	original	0.56	8.80	2.56
	method Ⅱ	2.20	0.32	0.12
f16	original	0.52	0.68	0.80
	method Ⅱ	3.16	4.56	2.88
lena	original	0.76	0.84	0.92
	method Ⅱ	1.92	3.84	2.36
peppers	original	0.80	0.52	0.76
	method Ⅱ	0.44	0.80	1.72
tiffany	original	0.80	0.40	0.60
	method Ⅱ	0.44	1.08	0.32

REFERENCES

Boneh, D. and Shaw, J. (1998). Collusion-secure fingerprinting for digital data. *IEEE Trans. Inform. Theory*, 44(5):1897–1905.

Cox, I. J., Kilian, J., Leighton, F. T., and Shamson, T. (1997). Secure spread spectrum watermarking for multimedia. *IEEE Trans. Image Process.*, 6(12):1673–1687.

Hayashi, N., Kuribayashi, M., and Morii, M. (2007). Collusion-resistant fingerprinting scheme based on the CDMA-technique. In *IWSEC2007*, volume 4752 of *LNCS*, pages 28–43. Springer, Heidelberg.

He, S. and Wu, M. (2006). Joint coding and embedding techniques for multimedia fingerprinting. *IEEE Trans. Inf. Forensics Security*, 1(2):231–247.

Kuribayashi, M. and Morii, M. (2008). Iterative detection method for CDMA-based fingerprinting scheme. In *IH2008*, volume 5284 of *LNCS*, pages 357–371. Springer, Heidelberg.

Lin, Y. T., Wu, J. L., and Huang, C. H. (2007). Concatenated construction of traceability codes for multimedia fingerprinting. *Optical Engineering*, 46(10):107202.1–107202.15.

Wang, Z. J., Wu, M., Trappe, W., and Liu, K. J. R. (2004). Group-oriented fingerprinting for multimedia forensics. *EURASIP J. Appl. Signal Process.*, 14:2142–2162.

Yacobi, Y. (2001). Improved Bone-Shaw content fingerprinting. In *CT-RSA2001*, volume 2020 of *LNCS*, pages 378–391. Springer, Heidelberg.

Zhao, H. V., Wu, M., Wang, Z. J., and Liu, K. J. R. (2005). Forensic analysis of nonlinear collusion attacks for multimedia fingerprinting. *IEEE Trans. Image Process.*, 14(5):646–661.