Research Highlights

Identification of illegal users from pirated copies of multimedia contents

To identify illegal users from pirated copies, information about the identities of each user— so called fingerprints— should be inserted into multimedia content before selling. The most challenging issue is robustness against a collusion attack where a coalition of users remove/modify fingerprints by comparing their copies. Fingerprinting code is one of the most promising approaches for the collusion-secure tracing system.

In the identification of illegal users, each user's codeword is checked by calculating the similarity score with the codeword extracted from a pirated copy. Although an optimal scoring function has been reported using a conventional method, the realization is difficult because the number of illegal users and their attack strategy are inevitable.

Now, Minoru Kuribayashi and colleagues at Okayama University have developed a new scoring function and proposed a semi-optimal method which can effectively classify illegal and innocent users with a simple operation.

Their method estimates the attack strategy in order to select its corresponding weight for calculating similarity scores. The advantage of this method is the simplicity required for the estimation because it only observes the bias of symbols '0' and '1' and then roughly classifies the strategy into three classes.

The method also assumes a realistic situation such that a pirated copy may be distorted by additional attacks which intend to delete the fingerprint in a signal processing domain.

The performance was evaluated in the presence of additive white Gaussian noise, and it was compared with some state-of-the-art methods. As a result, it was confirmed that the best performance was obtained by the proposed method and it was very close to the optimal one.

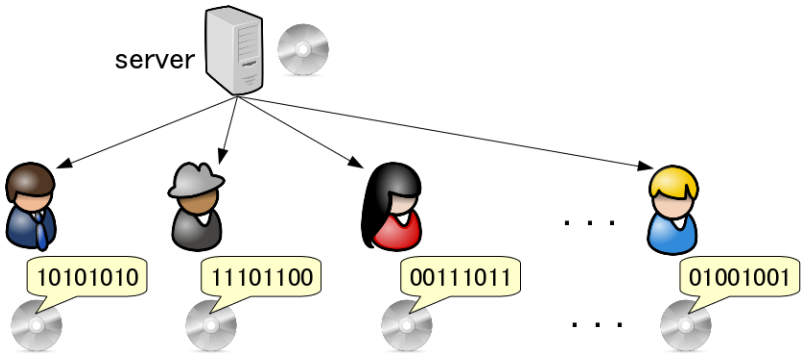

Fig.1: Framework of the fingerprinting system.

At the distribution of multimedia content, a server inserts unique ID information called fingerprint into the content. Once a copy is found, the illegal users can be identified if the fingerprint is correctly extracted.

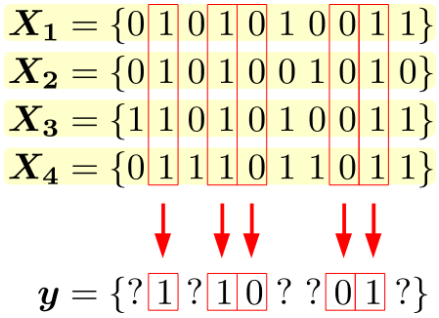

Fig.2: Collusion attack

If a coalition of users compares their codewords, they can find the positions where some of their symbols are same and they cannot modify the symbols at such positions. Otherwise, they can select the symbols with an arbitrary strategy such as majority voting, minority voting, and so on.

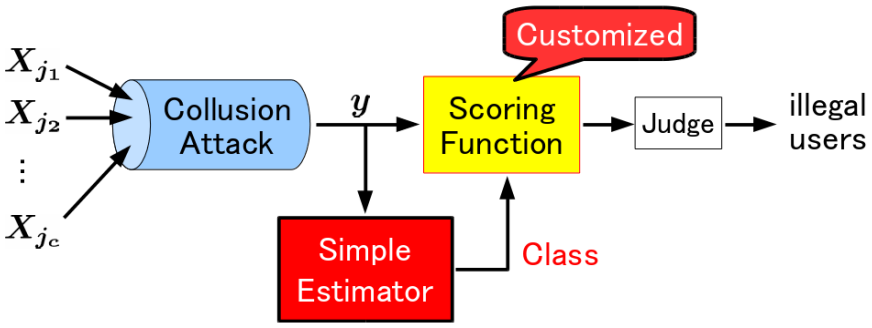

Fig.3: Flowchart of the proposed method

The proposed method first estimates the attack strategy into three classes, and then customizes the scoring function according to the estimated strategy. Both the estimator and scoring function exploit the bias of symbols in a pirated codeword $\boldsymbol{y}$ which can be observed directly from the codeword.

Reference

Authors

Minoru Kuribayashi and Nobuo Funabiki.

Title of original paper

Universal Scoring Function Based on Bias Equalizer for Bias-Based Fingerprinting Codes.

Journal, volume, pages and year

IEICE Trans. **E101-D**, No.1, 119-128, (2018).

Digital Object Identifier (DOI)

10.1587/transfun.E101.A.119

Journal website

http://search.ieice.org/bin/summary.php?id=e101-a_1_119

Affiliations

Graduate School of Natural Science and Technology, Okayama University.

Department website

http://www.ec.okayama-u.ac.jp/~dist/kuribayashi

