




Review

Survey on Decentralized Fingerprinting Solutions: Copyright Protection through Piracy Tracing

David Megías ^{1,*}, Minoru Kuribayashi ² and Amna Qureshi ¹

¹ Internet Interdisciplinary Institute (IN3), Universitat Oberta de Catalunya (UOC), CYBERCAT-Center for Cybersecurity Research of Catalonia, Castelldefels (Barcelona), 08860 Catalonia, Spain; aqureshi@uoc.edu

² Graduate School of Natural Science and Technology, Okayama University, Okayama 700-8530, Japan; kminoru@okayama-u.ac.jp

* Correspondence: dmegias@uoc.edu

Received: 13 March 2020; Accepted: 30 March 2020; Published: 3 April 2020



Abstract: Copyright protection is one of the most relevant challenges in the network society. This paper focuses on digital fingerprinting, a technology that facilitates the tracing of the source of an illegal redistribution, making it possible for the copyright holder to take legal action in case of copyright violation. The paper reviews recent digital fingerprinting solutions that are available for two particularly relevant scenarios: peer-to-peer distribution networks and broadcasting. After analyzing those solutions, a discussion is carried out to highlight the properties and the limitations of those techniques. Finally, some directions for further research on this topic are suggested.

Keywords: copyright infringement; piracy tracing; fingerprinting; peer-to-peer distribution; broadcasting

1. Introduction

Nowadays, digital technologies allow users to generate near-perfect quality identical copies of the content at low costs. Therefore, the amount of the digital data that is illegally redistributed is growing, making businesses lose income. Content creators and multimedia producers are concerned about the consequences of illegal copying and redistribution on a massive scale. Consequently, the need for a protection system that can provide copyright protection by prosecuting unauthorized copying has arisen in recent years.

Copyright protection is a relevant topic both for policy makers and researchers in academia. The purpose of this paper is to make known the digital fingerprinting technology to policy makers and researchers in the fields of engineering and law, arising awareness of which kind of technologies are available to fight piracy, and which are their properties and features in terms of both security and privacy. With this paper, we expect that policy makers can take into account the possibilities of digital fingerprinting when discussing about copyright regulations.

Traditionally, copyright protection of multimedia data has been accomplished by utilizing encryption techniques to prevent unauthorized users from accessing digital media content. Encrypting the entire multimedia content using standard encryption methods is referred to as the naïve approach. Audio and video data are typically very large in size, which makes the naïve approach computationally demanding. Nowadays, many new algorithms (e.g., public-key algorithms based on chaotic maps) for image [1,2], audio [3], speech [4] and video [5] encryption have been proposed to avoid the naïve approach and gain better efficiency. Although multimedia encryption is typically used in Digital Rights Management (DRM) distribution of multimedia contents, this solution cannot prevent a user from redistributing the data illegally once they have been received and decrypted.

Digital watermarking is recognized as a promising technique developed to address the problems of copyright protection, content authentication, tamper detection, and others. Watermarking schemes

work by embedding a merchant specific mark (watermark) imperceptibly into the content, which upon extraction enables provable ownership. Digital watermarking systems can be measured based on certain properties that depend on the application. Each of these following properties must be taken into consideration when applying a certain watermarking technique [6]:

- **Imperceptibility:** It is defined as the perceptual similarity between the original and the watermarked versions of the digital content. The embedded watermark must be transparent and must not introduce distortion, which can cause quality degradation.
- **Robustness:** It is defined as the ability to detect the watermark after common signal processing operations (e.g., cropping, compression, scaling, additive noise, filtering, etc.) A watermark must be robust enough to withstand all kinds of signal processing operations (at least below some distortion threshold).
- **Capacity:** It is defined as the number of bits a watermark encodes within a unit of time (or space in the case of still images). Capacity is usually given in bits per pixel for images and bits per second for audio.
- **Security:** It refers to the ability to resist intentional or malicious attacks. A watermarking algorithm must be secure in the sense that an attacker must not be able to detect/extract the existence of embedded data, let alone remove the embedded data. Watermark information should only be accessible to the authorized parties.

Digital watermarks can be sub-divided into various categories, i.e. they can be classified according to the applications and techniques.

1. Watermarking applications: The following are a few applications of digital watermarking:

- **Copyright protection:** This is the most prominent application of digital watermarking. The aim is to evade other parties from claiming the copyright by embedding the information such as a logo that identifies the copyright owner of the multimedia data [7,8].
- **Digital fingerprinting or transaction tracking:** In fingerprinting applications, a unique fingerprint (a type of a watermark that identifies the recipient of a multimedia content) is embedded in each individual copy of the content. This application acts as a deterrent to illegal redistribution by enabling the owner of the content to trace the source of the redistributed copy [9,10].
- **Content authentication:** The goal of this application is to provide assurance that the origin of the content is authentic, and its integrity can be proved. Effective authentication enables the owner to reliably authenticate data and identify possible tampering of the content [11].
- **Broadcast monitoring:** This application is used to verify the programs broadcasted on TV or radio. It provides cost effective means of monitoring advertisement airtime on TV and radio broadcasts [12].
- **Copy control:** In copy control applications, the embedded watermark represents a certain copy control or access control policy to prevent intentional or accidental unauthorized copying [13].
- **Device control:** In this application, watermarks are embedded to control access to a resource using a verifying device, which is equipped with a suitable detector. Depending on the information carried by the watermark, the verifying device can allow or prohibit certain operations on the content [6].
- **Legacy enhancement:** These applications enhance the functionality of legacy systems while maintaining compatibility with deployed devices.

2. Watermarking types: Digital watermarks can be divided into the following types on the basis of robustness requirement:

- **Robust watermarking:** This type of technique enables the watermarked data to resist a variety of malicious attacks and benign modifications [6]. This technique can be used in copyright protection, fingerprinting, and copy control. However, this watermarking type cannot determine whether the content is tampered or not.

- **Fragile watermarking:** The watermark in this type is designed to be destroyed at any kind of modification, to detect any illegal manipulation, even slight changes, involving incidental and intentional attacks. It considers the digital content as an entirety and does not allow any tampering. A special class of fragile watermarking, reversible watermarking (also called lossless watermarking) [7,14] enables the recovery of the original (unwatermarked) content after the watermarked content has been identified as authentic. This technique is mainly used in content authentication and integrity verification.
- **Semi-fragile watermarking:** This type of technique provides robustness against incidental modifications but is fragile against malicious attacks. It is used for content authentication.

Although digital watermarking is capable of determining the copyright of multimedia content, it is incapable of tracing back the source of illegal redistribution. An application of digital watermarking, fingerprinting (or transaction tracking), enables the merchant to trace the source of the redistributed copy by embedding a user-specific identification code into a digital content (e.g., an audio or a video file). The fingerprinting techniques of multimedia contents require the generation of a fingerprint, the embedding operation (which involves at least two parties: the merchant and the buyer), and the tracing protocol in case of detecting an illegal redistribution [6].

Instead of preventing multimedia contents from being copied or redistributed, digital fingerprinting focuses on identifying traitors who are responsible for unlawful redistribution, making it possible to undertake legal or technical actions against them. Several solutions have been proposed for “traditional” fingerprinting applications in which a merchant engages in one-to-one protocols with the buyers of the content.

Digital fingerprinting solutions are typically endowed with several of the following properties or requirements:

1. **Piracy tracing:** The merchant (with or without the collaboration of other parties) is able to identify the source(s) of an illegal redistribution.
2. **Asymmetry:** Only the buyer obtains the fingerprinted version of the content in such a way that no other party can frame an innocent buyer in the case of illegal redistribution [15].
3. **Anonymity:** Transactions and users’ private data are kept anonymous. Under the General Data Protection Regulation (GDPR) introduced by the European Union (EU), personal data of the buyer must be processed in a manner that ensures appropriate security of his/her personal data, including protection against unauthorized or unlawful processing [16]. However, in the case of illegal redistribution, the buyer’s privacy can be revoked by the merchant [17].
4. **Collusion resistance:** The fingerprints are constructed (encoded) in such a way that the collusion of several buyers to delete their fingerprints makes it possible to identify at least one of the traitors [9].
5. **Dispute resolution:** An arbiter should be able to resolve disputes without requiring the buyer to surrender his/her identity or private key.
6. **Non-repudiation:** A buyer accused of redistribution will not be able to claim that the copy was created by the merchant or by a different user.
7. **Unlinkability:** Nobody will be able to determine whether different contents were purchased by the same buyer.

Whereas the watermarking properties—such as transparency, capacity, and robustness—are typically quantifiable and different measurements have been proposed for them [18], the fingerprinting properties are typically binary (yes/no), with the exception of collusion resistance, for which the maximum collusion size is typically specified. However, the maximum collusion size basically depends on the underlying collusion-resistant code and the capacity of the watermarking system. Thus, a yes/no attribute is usually enough to denote whether a specific fingerprinting scheme provides collusion resistance or not.

Fingerprinting properties have been successfully obtained by different authors in the unicast (one-to-one) distribution scenario. However, the unicast scenario has become less attractive with the

latest developments. While the prices of “pay-per-use” platforms, such as Spotify [19] for music or Netflix [20] for video contents, are low enough to reach a large number of customers, thus reducing the effect of piracy, some multimedia contents are still expensive and this encourages piracy. Live sport events broadcast by licensed platforms are a good example of copyright violation.

The unicast scenario is particularly unsuitable for many current applications. First, decentralized distribution platforms based on peer-to-peer (P2P) protocols are widespread and allow an efficient and scalable solution for the distribution of multimedia contents. If a new content company wants to enter the media distribution market, they will possibly not have the resources (CPU capacity and bandwidth) to deploy a unicast distribution system to compete with the giant corporations that cover the entire market. This leads to a situation of less competition, which involves higher prices for customers. Second, in broadcasting (or streaming), standard unicast solutions are difficult or impossible to apply, for several reasons. Multiple embedding in such a way that a different version of a same content is transmitted to each buyer is not scalable for broadcasting scenarios with millions of simultaneous transmissions. A simple extension from the unicast scenario is not practical from the bandwidth and computational resources point of view. Furthermore, it is not an easy task for a broadcaster to adjust the system for dynamically changing group of users who are privileged to receive the content.

This paper focuses on the solutions available in these two decentralized distributions scenarios: P2P distribution platforms, which are not easy to control, and broadcasting, which pushes the limits of digital fingerprinting due to the highly demanding requirements. Both scenarios deviate from the unicast solutions and share a few common features that make these two areas worth investigating. Furthermore, the idea of decentralized tracing protocol is reviewed to consider a distributed management system.

The rest of the paper is organized as follows. Section 2 introduces general terms and definitions that are used in the fingerprinting literature. Section 3 provides a review of the existing fingerprinting solutions of P2P distribution systems. Section 4 presents a survey of the most relevant fingerprinting schemes for broadcasting systems. In addition, a few decentralized tracing protocols are reviewed in Section 5. Then, Section 6 analyzes and discusses how the existing solutions for P2P and broadcasting platforms can be combined in order to obtain more powerful schemes that can fit the demands that are not covered yet, and provides some directions for further research. Finally, Section 7 presents the conclusions of this work.

2. Background

Fingerprinting systems share some building blocks and architecture. The basic entities and technologies that are typically found in fingerprinting systems are summarized in this section.

A list of entities that are usually involved in fingerprinting applications is provided below:

1. A merchant M is an entity that distributes the copyrighted content to the buyers, either directly or using an auxiliary network of proxies or peers.
2. A buyer B_i is an entity that can either play the role of the data requester or the provider in the case of P2P distribution.
3. A certification authority CA is a trusted party that is responsible of issuing certificates to the participants in the fingerprinting protocol (merchant, buyers, peers, proxies, etc.)
4. A monitor MO is a trusted or semi-trusted party that can execute parts of the protocol in such a way that the buyers are protected from a potentially malicious merchant.
5. A judge J (or authority) is a trusted party that resolves disputes between M and the buyers B_i , with the cooperation of MO and CA if required.

The underlying technologies that are typically used within fingerprinting protocols are listed below:

1. **Cryptography:** To protect the contents during transmission, cryptographic algorithms are usually applied. This includes symmetric cryptography (when the encrypting and decrypting keys are identical) and asymmetric or public-key cryptography (when the encrypting and decrypting keys differ). A particularly useful variant of public-key cryptography is homomorphic cryptography. In this case, some operations (such as sums of products, but typically not both) can be carried out over encrypted data in such a way that the result is equivalent to encrypt the result of the operation computed with plaintext data. This makes it possible to make some computations without decrypting the data and, thus, security is maintained until the final decryption is performed.
2. **Collusion-resistant codes:** Since buyers know that their copies of the content are slightly different, a set of malicious buyers (colluders) may try to combine their copies in such a way that the fingerprints are erased and, then, they can distribute the fabricated copy without fearing of being traced. In case of multimedia content, it is reasonable to partition the content into small segments and to embed fingerprint into the segments. If each bit of fingerprint information is inserted into each segment of content, a coalition of users can find differently watermarked segments. Hence, they can modify the embedded fingerprint only at those segments and can select either the '0' or the '1' symbol for each bit of fingerprint. Such an attack—called collusion attack—is essentially unavoidable in a fingerprinting system and the tolerance against the collusion attack is inevitable. Collusion-resistant codes [21] have been designed in such a way that they can identify at least one of the colluders in such scenario.
3. **Embedding and retrieving (watermarking) algorithms:** Two algorithms are required: one to embed the fingerprint into the content and another one to extract a fingerprint from an illegally redistributed content [6]. These two algorithms must fulfill some properties, such as robustness against signal processing operations, transparency, capacity, and security (watermarking keys are required for both embedding and retrieving the fingerprints).
4. **Traitor tracing:** This is an algorithm or a protocol that makes it possible to retrieve the identification that can be linked to at least one buyer involved in illegal redistribution and/or collusion when an unlawful copy of the content is retrieved.
5. **Auxiliary cryptographic protocols:** Well-known cryptographic building blocks, such as zero-knowledge proofs, mix networks, or onion routing, are sometimes used to guarantee some security and privacy properties of these protocols.

Finally, the most typical attack scenarios to consider in fingerprinting applications are the following:

1. **Robustness against signal processing attacks:** These include filters, recompression, resizing, resampling, and other operations, either intended or unintended, which may affect or erase the embedded fingerprint.
2. **Collusion attacks:** This is described above.
3. **De-anonymization attacks:** These are attacks intended to break the anonymity of a buyer (this includes frameproof an innocent buyer, linking different purchases to the same buyer, or associating a real identity with a given buyer).
4. **Communication attacks:** These include man-in-the-middle-attack (a malicious party may try to eavesdrop messages exchanged by any two parties in a given protocol) or replay attack (a malicious party may try to collect proofs from another user and reuse them later on as a false authentication to another party).

Effective fingerprinting protocols must be endowed with mechanisms to overcome the aforementioned types of attacks in order to be used in real-world scenarios.

From a different point of view, the efficiency of the transaction between a merchant and buyer must be considered for a real-time distribution over the network. As the size of multimedia content

is basically very large, an efficient compression tool is used before distribution. This means that robustness against lossy compression is inevitable to embed/extract the fingerprint information. Although complicated cryptographic protocols are required to assure a sufficiently high security level, the computational cost must be reasonably small. In this sense, the reduction of the file size by using lossy compression is one of the important operations for a real-time distribution. It is worth pointing out that the computational costs at the encryption and decryption of public key cryptography is much higher than those of symmetric key cryptography. Therefore, it is desirable to combine different cryptographic techniques to realize a secure and low-cost transaction in a fingerprinting scheme.

3. Review of Digital Fingerprinting Schemes for Peer-to-Peer Systems

The P2P content distribution systems described in the following paragraphs are designed with an intention to satisfy both copyright protection and users' privacy. Hence, they belong to the category of "anonymous fingerprinting".

Domingo-Ferrer and Megías [22] proposed a P2P protocol for distributed multicast of fingerprinted content combining cryptographic primitives and robust watermarking. The proposed scheme takes a game-theoretic approach to ensure that peer buyers cooperate in P2P fashion in both content distribution and fingerprint embedding. However, the system requires an expensive secure multi-party computation protocol between peers for each transaction, which increases the computation and communication demands for buyers. A similar idea was presented by Domingo-Ferrer [23], which includes an expiration date of the contents to enforce digital oblivion.

A completely different approach was suggested by [24,25]. This solution is based on splitting the content into two separate files, a heavy one (supplementary file), containing detail coefficients only, and a very light one (base file) that contains the most relevant coefficients of the multimedia content. The supplementary file, which is completely useless without the base one, is distributed in a purely P2P fashion between peer buyers, whereas the base file is transmitted from vendor to buyer using a standard unicast communication. To ensure the asymmetric property (which guarantees buyer frameproofness), the base file is encrypted using homomorphic encryption (see Section 2) such that only the buyer obtains the decrypted and fingerprinted copy of the content, after combining it with the supplementary file. Homomorphic encryption is used only for a few low-frequency coefficients of the multimedia content (audio, video, or image), which results in lesser data expansion compared with other schemes. The drawbacks of the proposed system are the need of a unicast transmission of the base file for each buyer and the additional overhead for buyers to decrypt the contents once they are received. In addition, this system is conceived only for whole files and is not suitable for streaming applications.

More recently, Qureshi et al. [26] took advantage of some of those ideas, but replaced homomorphic encryption by fragmentation, symmetric encryption, permutation, and distribution of the fragments through a set of proxy peers. The main contribution is to replace the decryption-and-embedding operation that is carried out by the buyers in [24,25] by a pre-computation of all possible fingerprints using a string of all '1's and another one of all '0's. For each transaction, a set of proxy peers select the appropriate version of each coefficient ('0'-embedded or '1'-embedded) according to the specific bit required by a particular buyer. In addition, the sequence of bits and coefficients are previously permuted using a secret key in such a way that only the buyer is able to reverse the permutation and obtain the correct fingerprinted plaintext content. Although this version of the protocol improves the efficiency of the system by preventing homomorphic encryption, it shares most of the drawbacks mentioned above and cannot be used for streaming applications.

Recently, Qureshi and Megías [27] proposed a blockchain-based P2P content distribution system based on the system proposed in [24,25]. The proposed system combines different cryptographic protocols, e.g., collusion-resistant fingerprinting, homomorphic and symmetric encryption schemes, perceptual hash functions, etc., and an Ethereum-based smart contract in a P2P environment (InterPlanetary File System) to provide copyright protection, collusion resistance, atomic payment,

piracy tracing, transparency, proof-of-delivery, revocable privacy (to a buyer), and dispute resolution. Although the system satisfies the privacy and security properties of an anonymous fingerprinting protocol in a P2P network, the computational and communicational costs are not investigated to prove its feasibility. In addition, it shares most of the drawbacks of the systems proposed in [24–26].

The authors of [28,29] presented the novel concept of fingerprinting through a recombination mechanism in a P2P-based distribution scenario. The remarkable advantage of this system is that fingerprint embedding is required only for a few seed buyers, whereas the fingerprint of a non-seed buyer is automatically generated as the recombination of fragments (segments) of the fingerprints of several source buyers. Thus, distinct fingerprints are obtained thanks to combinatorial explosion. This first proposal of the recombination approach requires an expensive graph search for traitor tracing. In addition, to run the traitor-tracing protocol, the participation of trusted and committed proxies are required in the distribution protocol in such a way that valid fingerprints are generated. The fingerprints require a double-layer encoding, with two different collusion-resistant codes. A first layer is required at segment level to ensure that each segment is a codeword of some given collusion-resistant code. The second layer requires that a hash (constructed across the different segments of each fingerprint) is also a codeword of some collusion-resistant code. To construct this hash-level fingerprint codeword, the cooperation of the proxy peers is essential.

Megías [30] proposed an improved version of the recombined fingerprinting mechanism. The improvements are related with a communication protocol that relaxes the need of trusted proxies, since the content fragments are encrypted end-to-end and the intermediate proxies cannot access the plaintext of the fragments. Furthermore, the traitor-tracing algorithm is simplified considerably and the graph search required in [28,29] is replaced by a simple and efficient database search. The proposed scheme, thus, provides a convenient solution for legal multimedia distribution in P2P scenarios preserving both copyright protection and the privacy of (honest) users. Anonymity is only revoked for buyers involved in some illegal redistribution. The main drawback of the improved version is that it still requires the two-layered encoding of the fingerprint, with a segment-level and a hash-level collusion-resistant code. This implies longer fingerprints and also a complex verification protocol during distribution to ensure that valid codewords are generated for each buyer.

The main drawback of recombined fingerprinting was finally overcome by Megías and Qureshi [31]. The requirement of the two-layer encoding of the fingerprinting could be removed by the use of improved Tardos codes [21,32,33] in segment-wise fashion, resulting in remarkably short fingerprints. Apart from using Tardos codes in segment-wise form for the first time, the traitor-tracing protocol is developed in the encrypted domain, protecting the privacy of all users except those who are involved in illegal redistribution. These two non-trivial improvements make recombined fingerprinting a very mature strategy for content distribution in P2P networks. The possibility of moving this technique to the streaming scenario is discussed in Section 6.

Many fingerprinting methods in P2P scenarios only focus on copyright protection (through piracy tracing) and do not consider users privacy. Nevertheless, there are interesting solutions that belong to this category and deserve attention.

Chen and Lian [34] proposed a secure digital content distribution to trace illegal redistributors in P2P e-commerce applications. In this method, the sending peer of a super-node-based P2P network encrypts and distributes the media content, and the receiving peer uses the decryption key together with his/her peer ID (fingerprint) to decrypt the encrypted media content. Each decrypted media copy contains unique information that identifies the peer. Joint decryption and fingerprint embedding operations are performed so as to prevent the leakage of plaintext media content. Upon finding a pirated copy of the content, the fingerprint can be extracted from the decrypted media content to trace the source of redistribution. The proposed scheme has not been analyzed against possible security threats and collusion attacks. In addition, the system does not provide user privacy.

Another asymmetric fingerprinting scheme was proposed by Hu and Li [35]. This method takes a multicast approach to reduce the bandwidth requirements of the vendor. This solution relies on a

concept similar to chameleon encryption such that a decryption key is transmitted and the sender does not know it. However, the sender can guess the key used by the recipient with a non-negligible probability $1/n$ and he/she could also fool the recipient by offering the same key n times. Hence, this proposal does not provide buyer frameproofness. In addition, the scheme does not provide any protection for end users privacy, but it offers collusion resistance.

In the copyright protection system proposed by Gao et al. [36], each user of the P2P system obtains a slightly different version of the same content. The distributor of the system divides the media content into two parts: plaintext content to be used as a demo clip, and an encrypted content. The encrypted key is generated by the distributor by adding a high strength watermarking signal and lower-frequency Discrete Cosine Transformation (DCT) coefficients of the content. Both parts are then published in a P2P system. An AND anti-collusion code is used to represent the corresponding peer ID. Each user is assigned a unique decryption key that is generated from the peer ID and the corresponding watermarking signal. Upon decrypting the same encrypted content with different decryption keys, the result is a slight different fingerprinted copy for each user. If the merchant finds a pirated copy, he/she adopts a hard-detection algorithm based on a correlation method to trace copyright violators. Although the system provides data privacy by employing symmetric cryptography, it does not offer anonymity or revocable privacy to the user.

Terelius [37] proposed an efficient and secure asymmetric fingerprinting protocol that allows distribution of digital content in P2P network to multiple recipients while preserving the merchant's copyright. The protocol allows a buyer to send his/her watermarked content obtained by the merchant to another buyer and, in the process, to change the embedded watermark into the watermark of the receiving buyer. The process requires a limited amount of communication among the buyers and with the merchant and the judge, who acts as a trusted third party and is responsible of generating watermarks and identifying the copyright violator. Although the proposed protocol satisfies a few security requirements of an asymmetric fingerprinting scheme, it is not computationally feasible since the communication complexity of the merchant is proportional to the size of the watermark instead of the size of the content. In addition, the protocol requires at least two of the three parties to be trustworthy. Moreover, it does not consider either collusion resistance or user privacy.

4. Review of Digital Fingerprinting Schemes for Broadcasting Applications

The broadcast content distribution systems are designed to satisfy both access control and traceability from a pirated copy. For the realization of such a system, two major techniques are necessary. One is a cryptographic technique to deliver multimedia content only to legitimate users, and the other is a fingerprinting technique which enables a broadcaster to identify illegal users from a pirated copy as well as the secret keys assigned to the users.

In a broadcast encryption scheme [38], a broadcaster encrypts a message for a subset of buyers who have authorization to receive the message. Each user in a system has a unique decryption key; hence, it is possible to uniquely identify the user from the key [39]. The main goal of a broadcast encryption scheme is to construct efficient schemes that can revoke a set of users with only small size of both the header information and the decryption keys, while the private decryption keys issued to users are fixed. However, the broadcast encryption schemes involve two difficult problems. Once the content is delivered to legitimate users, the broadcaster cannot prevent the users from redistribution. In addition, since the revocation is governed by the broadcaster, he/she must know each user's decryption key. Under such a situation, the asymmetric property cannot be satisfied.

A dynamic traitor-tracing scheme [40,41] allows a broadcaster to trace traitors with a little sacrifice in bandwidth. The basic idea is to break time into consecutive intervals and dynamically modify the watermark inserted during each interval. The traitors can be traced by observing the rebroadcasted content for a long enough time. The sequential traitor-tracing scheme [42] improves upon the dynamic scheme so that the channel feedback is only used for tracing, not for allocating watermarks to users. Unfortunately, the broadcaster knows the content finally distributed to a user. Hence, the asymmetric

property must be considered so that only the user can know the fingerprinted content being decrypted from the broadcasted ciphertext.

Bianchi and Piva [43] proposed an asymmetric fingerprint protocol based on a client-side distribution paradigm. The protocol enables secure distribution of personalized decryption keys containing the buyer's fingerprint by means of existing asymmetric protocols without a trusted third party. Two client-side embedding schemes are proposed to generate a binary fingerprint. In the first scheme, a standard spread spectrum client-side embedding is performed, while the second method performs a novel client-side fingerprint embedding. A look-up table (LUT) is used to encrypt the digital content to be distributed among several users. Then, the server obtains the fingerprints of the users that are encrypted with their public keys. The server sends encrypted LUT to the users, who perform decryption with their secret keys. The scheme effectively solves both customer's rights and scalability problems; however, it is vulnerable to collusion attacks.

The vulnerability of the scheme in [43] was eliminated by the protocol proposed by Bianchi et al. [44]. The proposed protocol adopts two different solutions for generating the fingerprinting codes. The first method is based on generating independent coding matrices for the fingerprint of different users, and is conceptually similar to using near-orthogonal independent Gaussian fingerprints. The second method generates the fingerprint of each user according to Tardos codes. These fingerprints can be securely distributed according to an asymmetric fingerprinting protocol and embedded at the server's side using the homomorphic cryptosystem proposed in [45]. For both methods, correlation-based accusation strategies are developed to evaluate their collusion resistance against the averaging attack. In the schemes proposed in [43,44], the buyers are required to perform complex security actions. Moreover, the scheme in [44] has not been analyzed against the possible collusion attacks on decrypted LUTs (since all the users share the same long term encrypted LUT).

A novel framework called JFDA (joint fingerprinting, decryption and authentication) based on the principle of polynomial secret sharing is proposed in [46] to protect the video streams transmitted via multicasting. The framework is designed to prevent tampering while performing joint fingerprinting and decryption in order to preserve the losslessness of the fingerprint. In addition, it provides a deterrent scheme to prevent dishonest users from illegal redistribution. Fingerprinting is performed in the encrypted domain followed by decryption on the receiver side. Post-authentication method is designed to prevent tampering attack on the decrypted data to ensure the fidelity of the fingerprinted data. The protocol does not provide a traceability protocol and resistance against collusion attacks.

Kuribayashi [47,48] presented a new broadcasting system with tracing capability from both decryption keys and redistributed copies. The multimedia content is broadcasted in such a way that only authorized buyers who have their own decryption key sequence can obtain the content with a distinct fingerprint.

The broadcasting system is based on the following assumptions. Once traitors distribute a pirated copy and they are eventually traced, they must financially compensate to a broadcaster for all content that will be broadcasted in a certain period. It introduces the concept of time-bound key management so that a user key issued at a trusted center will be available before a certain expiration date. The expiration date is hierarchically designed based on the secret information issued to each buyer. As a result, each buyer receives multimedia content containing his/her fingerprint without increasing either the computational costs or the amount of data transmission required for broadcasting. The asymmetric property is satisfied by managing the decryption keys issued to users, which is based on the fingerprinting scheme in [49]. In the case of key leakage, it is possible to identify the users from the keys even if a coalition of users produces a new decryption key by combining the users' keys. The key management cost is reduced by the concept of compensation in a certain period. Once a pirated copy is detected, traitors must pay compensation to the broadcaster for all content in a certain period even if he/she purchased a license to receive the content for a shorter time period. Such a risk is expected to reduce the motivation of traitors to redistribute illegal copies.

The broadcast fingerprinting system is based on the following ideas. A broadcaster commits secret information to a trusted center, and the center partially gives the information to each buyer in a registration. The information gap between broadcaster and buyer plays an important role to assure the asymmetric property, similar to the fingerprinting protocol proposed in [49]. The information at the broadcaster is the entire key sequence while the information at each buyer is interleaved and controlled by the center. At the encryption phase, the content is partitioned into small segments and two versions for each segment are produced by embedding one bit information. Then, each watermarked segment is encrypted by using each element in the key sequence. At the buyer's side, only one of two ciphertexts for each segment can be decrypted by using the buyer's key sequence because it is interleaved from the entire key sequence. By managing the expiration date of the key sequence adaptively, each buyer can receive the content containing his/her unique fingerprint from a broadcast channel during a specified period. In the system, two types of secret keys are used, and each expiration date is designed adaptively considering the amount of information to be transmitted to users.

A broadcaster updates a key sequence by using a current time-bound key which is valid within a certain time slot, and encrypts multimedia content by using the updated key. The time-bound key is committed to a trusted center from the broadcaster to indirectly share the key with buyers. Each buyer must make a registration at the center to obtain the buyer's key sequence which involves a fingerprint, and then, purchase a time-bound key to receive the content from a broadcast channel. Similar to the broadcaster, the buyer's key is updated by using the time-bound key to synchronize the reception time. If the time-bound key is valid at the time, the fingerprinted content can be decrypted by the buyer.

In the broadcast fingerprinting system, the use of a fingerprinting code is easy because a trusted center can encode a user's identity information at the generation of his/her secret key. In other words, the fingerprint is the codeword assigned to a buyer. Different from the procedure introduced by Charpentier et al. [45], the trusted center can directly produce the codeword using its secret information required for encoding/decoding.

5. Review of Decentralized Tracing Protocols

Generally, the operations of tracing protocol require heavy computational resources for the trusted center. When a pirated copy is discovered, a merchant first extracts the fingerprint, and then requests the center to identify colluders. If the fingerprint is encoded as a codeword of a fingerprinting code, the center needs to calculate a level of suspicion for each user by means of correlation of codewords. Among the correlation scores of all users registered in a system, the users whose score exceeds a threshold are judged guilty. Due to the secrecy of the parameters of the fingerprinting code, the calculation of the score is considered to be the center's task. Specifically, secret weighting parameters derived from bias probabilities of symbols in the codeword are necessary to calculate the score in bias-based fingerprinting codes (see, e.g., [21,32,33]).

Different from the study of asymmetric protocol at the time of content delivery, the tracing protocol was investigated by Kuribayashi and Funabiki [50], who introduced the idea of a delegated server. In this protocol, a trusted center is responsible to select secret parameters of a fingerprinting code and to issue a unique codeword to each user. The delegated server helps a merchant to identify illegal redistributors when a pirated copy is found while a trusted center works only at the time of registration phase. Upon finding a pirated copy, the merchant extracts a codeword from the pirated copy, and calculates the correlation of codewords in an encrypted domain by using encrypted weighting parameters. Then, the merchant sends the ciphertexts of these scores to the delegated server, who decrypts the ciphertext of correlation scores and returns a binary decision for each ciphertext.

The advantages of the decentralized system are the followings: (1) A trusted center's task is to issue secret parameters at the initialization phase. (2) The trusted center and illegal users do not need to participate in the tracing protocol. After the identification of illegal users, the merchant can claim the fact to a judge by showing collected proofs.

For the dispersion of the task, the secrecy of parameters in a fingerprinting code must be considered in the protocol. Once a list of users' codewords are leaked to a malicious merchant, innocent users may be accused from fake content distributed by the merchant because he/she can produce a specific fingerprinted version of content by his/her choice. A delegated server generates a public key and secret key pair of the public-key cryptosystem, and registers the public key at a public key infrastructure (PKI). To ensure its independence, the trusted center does not know the secret key. The trusted center allows the server to check a correlation score whether it exceeds the threshold determined by the center. The server is blind to the setting of fingerprinting code except for the threshold and the number of allowable colluders which is assumed at the setting. The server's task is to decrypt a ciphertext received from a merchant and return a binary decision.

The role of server is regarded as a decryption oracle that receives a ciphertext and returns the decryption result. As discussed in the cryptographic community, the number of queries to the server should be limited for security reasons. The more queries a merchant requests, the more information about the codeword bias probability he/she obtains. As there are many users, the merchant requests multiple ciphertexts simultaneously to find suspicious users whose score exceeds the threshold. To manage the information leakage, three restrictions are introduced into the check at the server: (1) The number of ciphertexts at each request must be equal to the number of users in a system, (2) Due to the limitation of traceability in a fingerprinting code, the number of suspicious users must be lower than the number of allowable colluders. If the number of the scores exceeding the threshold is larger than the number of allowable colluders, the server rejects the request, (3) The statistical distribution of scores: It is known that the scores of innocent users follow a Gaussian distribution with zero mean [51,52]. Except for a few scores of colluders, the scores observed after the decryption of requested ciphertexts must follow the distribution. Hence, a server checks the soundness of the request by the above three restrictions.

Although the protocol requires no participation of the trusted center and the users in tracing protocol, the communication costs for the merchant are considerably high due to the use of the database encrypted with Paillier's cryptosystem [53]. Recently, Kuribayashi and Funabiki [54] proposed an improved version of the scheme in [50] by introducing the lifted Elliptic Curve-ElGamal cryptosystem [55,56] into the tracing protocol. This lifted ElGamal cryptosystem over Elliptic Curve (EC) results in reduction in the size of the encrypted database as well as the computational complexity. The size of encrypted database can be further reduced by introducing an index table under the characteristics of discretized bias distribution of Nuida codes [32,33].

The scores calculated in the above protocol are independent from the collusion strategy and the number of colluders, which is said to be non-informed. If the information about the collusion attack is available at the detector side, an optimal scoring function can be employed to discriminate colluders' scores from innocents' ones as much as possible [57]. Because of the difficulty in the realization of an optimal scoring function, the scoring function has been adjusted for a certain fixed collusion strategy to achieve better performance [58–61].

In binary fingerprinting codes, the number of symbols '0' and '1' is generally balanced because of the design of the codeword. After a collusion attack, the number of symbols is not always balanced in a pirated codeword. Such a bias of symbols is utilized to calculate weights for correlation scores in [62,63], which provide traceability close to the optimal scoring function. Yasui et al. [64] proposed an accurate estimation of collusion attack and the traceability is much close to the optimal detector.

Although the employment of complicated scoring functions is difficult in the encrypted domain, the idea of bias equalizer presented in [63] can be used because the bias of the number of symbols '1' and '0' can be measured from the observation of the codeword extracted from a pirated copy.

6. Analysis and Discussion

Almost all the schemes presented in the previous sections guarantee piracy tracing, but there are differences between them regarding privacy, collusion resistance, resilience against communication attacks, and applicability in real-time streaming scenarios. These differences are discussed below.

Regarding privacy and anonymity, the following considerations can be made:

- The schemes in [22,24–31] provide revocable privacy. These systems hide the real identity of the buyers that is only revealed by a trusted third party in case of illegal redistribution. On the other hand, the schemes in [34–37] do not consider buyers' privacy. In the broadcasting system [47,48], a broadcaster cannot obtain any information about users who receive the broadcasted content unless an illegal redistribution is detected. In this sense, the trusted third party should securely manage the anonymity of users in the system. The systems proposed in [43,44,46] have not addressed users' privacy concerns.
- The schemes in [22,24–31] also provide mutual anonymity between the users of the distribution system, using pseudonyms, and anonymous authentication and communication techniques. Again, mutual anonymity is not discussed in [34–37]. On the other hand, the broadcasting system [47,48] offers the anonymity of users, but the users know who broadcasts the content. None of the systems proposed in [43,44,46] provide mutual anonymity.
- Furthermore, in the P2P distribution systems proposed by the authors of [22,24–31], the privacy of the users is preserved against malicious or coalition attacks that attempt to deanonymize the users. Although the systems in [34–37] provide copyright protection through asymmetric fingerprinting protocols, the privacy of the users is not preserved against any type of malicious attack. Since the private information about users is managed by the trusted third party, the privacy of the users is preserved in the broadcasting system [47,48].
- The schemes in [22,24–31,34–37] guarantee data protection through the use of different cryptographic solutions (either symmetric, public key or hybrid). Similarly, the data are protected against eavesdropping of broadcast channel because of the enciphering before the broadcasting in [43,44,46–48].
- The P2P distribution systems proposed by the authors of [22,24–31,34–37] guarantee the traceability of copyright violators through either a tracing function of employed collusion-resistant codes or proposed detection/tracing algorithms and/or protocols. The scheme in [47,48] provides the traceability from a user's decryption keys as well as a pirated copy. It means the fingerprint is insulated into the decryption key. On the other hand, the schemes in [38,39] cannot trace illegal users from a pirated copy. Although the traceability from a pirated copy is possible in [40–42], the asymmetric property is not satisfied. The system proposed by Bianchi and Piva [43] detects copyright violators by means of blind decoding, whereas, in the improved version [44], the traceability from a pirated copy is performed through Tardos's tracing algorithm [21]. Although the system in [46] is based on anti-collusion codes, the traceability mechanism is not provided.

As security against collusion and communication attacks are concerned, the following differences must be taken into account:

- In the methods proposed by the authors of [22,25–31,35,36,44,47,48], collusion-resistant fingerprinting codes are used, whereas the schemes in [34,37,43,46] do not provide security against collusion attacks.
- The communication channel for transferring the content between users of the systems in [25–31, 47,48] are secure against communication attacks. In the other systems, the protection against communication attacks is either not provided or not discussed.

A collusion attack may be performed at secret keys issued to buyers as well as fingerprinted copies. In a broadcasting system [47,48], there are two kinds of keys: one is a time-bound key and

the other is a decryption key, which is updated by using the time-bound key at the reception of content in a certain time. Due to the characteristics of the time-bound key management scheme, a coalition of buyers can share their keys. Although it is difficult to restrict the sharing of time periods, the production of time-bound keys at the expired period can be prohibited. On the other hand, the decryption key is produced at a trusted center by interleaving a key sequence of the broadcaster according to a fingerprint. Basically, the tolerance against collusion attacks is considered to encode a fingerprint by a collusion-resistant fingerprinting code.

To identify illegal users, a tracing algorithm tries to find suspicious users by calculating the similarity between the codeword extracted from a pirated copy and the user's codeword [21,32,33]. The tracing algorithm can be classified into three types: catch-one, catch-many, and catch-all [65]. In the case of catch-one, the most suspicious user whose similarity score becomes maximum is detected as guilty. All illegal users can be identified from a pirated copy in the case of catch-all, although the false-negative rate that no illegal user is detected becomes larger. A catch-many type can identify as many illegal users as possible while the false-positive detection is controlled to be negligibly small. According to an information theoretical analysis, an optimal-tracing algorithm is investigated in [57,58] to discriminate illegal users from innocents as much as possible. For both P2P-based and broadcasting schemes, there is no restriction regarding the use of such a tracing algorithm.

In a real environment, the communication and computational costs should be kept as small as possible. In a broadcasting system [47,48], two differently watermarked segments are produced for each partitioned segment of content. Thus, the size of data becomes double from the original. Generally, a watermarking method is robust against lossy compression, and the watermarked segments must be compressed before transmission. Therefore, a broadcaster can produce the watermarked segments and compress them in advance, which enables reduction in both computational costs for encryption and amount of data for transmission. Only the enciphering operation is carried out by a broadcaster during the on-line protocol; hence, real-time streaming is possible.

Regarding the use for real-time streaming (broadcasting) applications, the P2P-based systems proposed in [26,28,29,31] may also be used in a broadcasting scenarios, since fingerprint embedding is either pre-computed or carried out for a small number of seed buyers and, thus, is not required to be carried out during transmission. In this case, the cryptographic protocols should be revised in order to include the requirements for key distribution in broadcasting scenarios. In other P2P systems [34–36], the encrypted content embedded with a watermark is sent to the peers, which upon decryption by using the private keys and/or peer IDs generate the fingerprinted content. Thus, by incorporation of secure key management schemes within these systems, the merchants can use them in broadcasting scenarios.

A comparison of the reviewed methods is provided in Table 1. The systems proposed in [34–36] are P2P-based distribution systems, which can be improved to be used in broadcasting scenarios. However, these schemes do not fully satisfy the required properties of an asymmetric fingerprinting protocol. Although the P2P distribution system proposed in [37] provides buyer frameproofness, the high communication complexity at the merchant's end makes it impractical to be used for real-time streaming applications. The systems in [22,23] in principle satisfy all the requirements, but the P2P distribution is tree-like and requires that the complete file is distributed from a single node. Hence, the applicability of the technique is somewhat limited, and the properties of full P2P distribution are not exploited. The systems in [24–26] also provide a good solution for P2P distribution, but they still require the unicast transmission of the base file from the merchant to each buyer. Only the supplementary file is transmitted in P2P fashion. The methods in [28–30] also have good performance and exploit the P2P network fully, but offer limited collusion resistance due to the need of the "two-layer" encoding of the fingerprint. The broadcasting systems in [43,44,46] satisfy requirements of an asymmetric fingerprinting protocol, but fail to provide user privacy. In addition, the security of the key management protocol has not been addressed in these systems.

Table 1. Comparative analysis.

Scheme	P2P	Broadcasting	Collusion Resistance	Buyer Frameproofness	Privacy
Chen and Lian [34]	Yes (super-node)	Maybe	No	No	No
Hu and Li [35]	Yes	Maybe	Limited	Yes	No
Gao et al. [36]	Yes	Maybe	Limited	No	No
Domingo-Ferrer [23]	Yes (Tree)	No	Yes	Yes	Yes (Revocable)
Terelius [37]	Yes	No	No	Yes	No
Domingo-Ferrer and Megías [22]	Yes (Tree)	No	Yes	Yes	Yes (Revocable)
Megías and Domingo-Ferrer [28,29]	Yes	Maybe	Limited	Yes	Yes (Revocable)
Megías [30]	Yes	Maybe	Limited	Yes	Yes (Revocable)
Qureshi et al. [24,25]	Yes (Supl. file)	No	Yes	Yes	Yes (Revocable)
Bianchi and Piva [43]	No	Yes	No	Yes	No
Bianchi et al. [44]	No	Yes	Yes	Yes	No
Kuribayashi [47,48]	No	Yes	Yes	Yes	Yes (Revocable)
Qureshi et al. [26]	Yes (Supl. file)	Maybe	Yes	Yes	Yes (Revocable)
Megías and Qureshi [31]	Yes	Maybe	Yes	Yes	Yes (Revocable)
Qureshi and Megías [27]	Yes	No	Yes	Yes	Yes (Revocable)

Table 1 shows that the systems in [26,31] and those in [47,48] can be applied successfully for P2P distribution and broadcasting, respectively. These systems take quite a different approach in each case, although they share a few similar characteristics. In their domain of application, the systems in [26,31,47,48] stand out among the best technologies available for solving the anonymous fingerprinting problem. It is worth analyzing whether the properties of these different approaches could be incorporated into each other to improve the solutions in their respective domains (P2P and broadcasting) or, even better, yield a new solution that can be applied in a more general scenario.

In the light of the analysis provided above, we consider that the most relevant open challenge of fingerprinting applications is concerned with the streaming of live events (such as sports). Such a challenge requires, first, a robust watermarking scheme for video that can resist strong attacks (such as using a capturing device to record the video from a TV and then streaming the captured video). Second, embedding should be carried out in real time, and the fingerprinting solution should provide collusion resistance, buyer frameproofness, traceability, and revocable privacy to the end users. The efficiency of the distribution can be attained if P2P protocols are used and, hence, the combination of the technologies surveyed in this paper can be a promising research area that can contribute to the technological solution of the most difficult open problems in copyright protection during the decentralized distribution of multimedia contents.

7. Conclusions

Copyright infringement of multimedia contents is a relevant research topic from both the legal and the technological points of view. Digital fingerprinting consists of embedding an identification sequence into a content in such a way that each receiver obtains a slightly different copy that can be traced back to him/her. In this way, an illegal redistributor can be identified and legal action can be taken against him/her. In addition, the anonymous property guarantees that the identity of the buyer is not known during distribution as per the requirement of GDPR. However, if a buyer is found to be involved in copyright infringement, his/her privacy can be revoked.

This paper focuses on anonymous fingerprinting solutions that have been proposed for the two most challenging scenarios of multimedia distribution: P2P networks and broadcasting. While the distribution of multimedia contents preserving copyright in unicast contexts (from merchant to buyer) has been deeply investigated in the last few decades, decentralized and broadcast scenarios require more research in order to attain solutions that can be deployed in real-life applications.

This work reviews the most relevant recent schemes that have been proposed in both broadcasting and P2P distribution contexts. Some recent works seem to provide quite effective and efficient methods for each case, but, after some analysis, it becomes apparent that fingerprinting schemes for the broadcasting of live events (e.g., sports) is still an open research challenge due to the extreme requirements of such applications. The paper also reviews solutions for the decentralization of the tracing protocol, which is a convenient approach for the proposed scenario. Real-time embedding of the fingerprints, collusion resistance, efficient distribution without delay, traceability, and time-bound cryptographic keys are, among others, the most relevant issues to be tackled in such case. Combining the properties of recent schemes that address the P2P and the broadcasting problems, together with decentralized tracing, seems to be a convenient research direction for the academic community focused on copyright protection. Consequently, we invite the data hiding and the multimedia security research communities to address this research topic and explore new solutions to face this very demanding challenge.

Author Contributions: D.M., M.K. and A.Q. commonly finished the manuscript. Conceptualization, D.M. and M.K.; Original draft preparation, D.M. and M.K.; Comparative analysis, A.Q.; and Writing—review and editing, all authors. All authors have read and agreed to the published version of the manuscript.

Funding: The first and third authors acknowledge the financial support received from the Spanish Government through grant RTI2018-095094-B-C22 “CONSENT”. The research of the second author was partially supported by JSPS KAKENHI Grant Number JP16K00185.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Flores-Vergara, A.; García-Guerrero, E.E.; Inzunza-González, E.; López-Bonilla, O.R.; Rodríguez-Orozco, E.; Cárdenas-Valdez, J.R.; Tlelo-Cuautle, E. Implementing a chaotic cryptosystem in a 64-bit embedded system by using multiple-precision arithmetic. *Nonlinear Dyn.* **2019**, *96*, 497–516. doi:10.1007/s11071-019-04802-3. [[CrossRef](#)]
2. García-Guerrero, E.; Inzunza-González, E.; López-Bonilla, O.; Cárdenas-Valdez, J.; Tlelo-Cuautle, E. Randomness improvement of chaotic maps for image encryption in a wireless communication scheme using PIC-microcontroller via Zigbee channels. *Chaos Solitons Fractals* **2020**, *133*, 109646. doi:10.1016/j.chaos.2020.109646. [[CrossRef](#)]
3. Liu, H.; Kadir, A.; Li, Y. Audio encryption scheme by confusion and diffusion based on multi-scroll chaotic system and one-time keys. *Optik* **2016**, *127*, 7431–7438. doi:10.1016/j.ijleo.2016.05.073. [[CrossRef](#)]
4. Ballesteros, L.D.M.; Moreno, A.J.M. Speech Scrambling Based on Imitation of a Target Speech Signal with Non-confidential Content. *Circuits Syst. Signal Process.* **2014**, *33*, 3475–3498. doi:10.1007/s00034-014-9810-9. [[CrossRef](#)]
5. Hamidouche, W.; Farajallah, M.; Sidaty, N.; Assad, S.E.; Deforges, O. Real-time selective video encryption based on the chaos system in scalable HEVC extension. *Signal Process. Image Commun.* **2017**, *58*, 73–86. doi:10.1016/j.image.2017.06.007. [[CrossRef](#)]
6. Cox, I.; Miller, M.; Bloom, J.; Fridrich, J.; Kalker, T. *Digital Watermarking and Steganography*, 2nd ed.; Morgan Kaufmann Publishers Inc.: San Francisco, CA, USA, 2007.
7. Pizzolante, R.; Castiglione, A.; Carpentieri, B.; Santis, A.D.; Castiglione, A. Reversible Copyright Protection for DNA Microarray Images. In Proceedings of the 10th International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), Krakow, Poland, 4–6 November 2015; pp. 707–712. doi:10.1109/3PGCIC.2015.139. [[CrossRef](#)]

8. Hou, R.; Xian, H.; Wang, X.; Li, J. A Robust Reversible Watermarking Scheme for Relational Data. In *Security and Privacy in New Computing Environments*; Li, J., Liu, Z., Peng, H., Eds.; Springer International Publishing: Basel, Switzerland, 2019; pp. 545–550. doi:10.1007/978-3-030-21373-2_44. [CrossRef]
9. Blakley, G.R.; Meadows, C.; Purdy, G.B. Fingerprinting Long Forgiving Messages. In *Advances in Cryptology—CRYPTO '85 Proceedings*; Williams, H.C., Ed.; Springer: Berlin/Heidelberg, Germany, 1986; pp. 180–189. doi:10.1007/3-540-39799-X_15. [CrossRef]
10. Boneh, D.; Shaw, J. Collusion Secure Fingerprinting for Digital Data. *IEEE Trans. Inf. Theory* **1999**, *44*, 1897–1905. doi:10.1109/18.705568. [CrossRef]
11. Pizzolante, R.; Castiglione, A.; Carpentieri, B.; Santis, A.D.; Palmieri, F.; Castiglione, A. On the protection of consumer genomic data in the Internet of Living Things. *Comput. Secur.* **2018**, *74*, 384–400. doi:10.1016/j.cose.2017.06.003. [CrossRef]
12. Walters, T.C.; Ross, D.A.; Lyon, R.F. The Intervalgram: An Audio Feature for Large-Scale Cover-Song Recognition. In *From Sounds to Music and Emotions*; Aramaki, M., Barthet, M., Kronland-Martinet, R., Ystad, S., Eds.; Springer: Berlin/Heidelberg, Germany, 2013; pp. 197–213. doi:10.1007/978-3-642-41248-6_11. [CrossRef]
13. Faundez-Zanuy, M.; Hagsmüller, M.; Kubin, G. Speaker identification security improvement by means of speech watermarking. *Pattern Recognit.* **2007**, *40*, 3027–3034. doi:10.1016/j.patcog.2007.02.016. [CrossRef]
14. Qiu, Y.; Gu, H.; Sun, J. Reversible watermarking algorithm of vector maps based on ECC. *Multimed. Tools Appl.* **2018**, *77*, 23651–23672. doi:10.1007/s11042-018-5680-7. [CrossRef]
15. Pfitzmann, B.; Schunter, M. Asymmetric Fingerprinting. In Proceedings of the International Conference on the Theory and Application of Cryptographic Techniques, EUROCRYPT'96, Saragossa, Spain, 12–16 May 1996; pp. 84–95. doi:10.1007/3-540-68339-9_8. [CrossRef]
16. Zoethout, T. GDPR: A Fateful Course for Smart Buildings? *Elektor* **2019**. Available online: <https://www.elektormagazine.com/news/gdpr-a-fateful-course-for-smart-buildings> (accessed on 3 April 2020).
17. Pfitzmann, B.; Waidner, M. Anonymous Fingerprinting. In Proceedings of the International Conference on the Theory and Application of Cryptographic Techniques, EUROCRYPT'97, Konstanz, Germany, 11–15 May 1997; pp. 88–102. doi:10.1007/3-540-69053-0_8. [CrossRef]
18. Dittmann, J.; Megías, D.; Lang, A.; Herrera-Joancomartí, J. Theoretical Framework for a Practical Evaluation and Comparison of Audio Watermarking Schemes in the Triangle of Robustness, Transparency and Capacity. In *Transactions on Data Hiding and Multimedia Security I*; Shi, Y.Q., Ed.; Springer: Berlin/Heidelberg, Germany, 2006; pp. 1–40. doi:10.1007/11926214_1. [CrossRef]
19. Spotify. 2006. Available online: <http://www.spotify.com/> (accessed on 3 April 2020).
20. Netflix. 2007. Available online: <http://www.netflix.com/> (accessed on 3 April 2020).
21. Tardos, G. Optimal Probabilistic Fingerprint Codes. In Proceedings of the 35th Annual ACM Symposium on Theory of Computing, STOC'03, San Diego, CA, USA, 9–11 June 2003; ACM: New York, NY, USA, 2003; pp. 116–125. doi:10.1145/780542.780561. [CrossRef]
22. Domingo-Ferrer, J.; Megías, D. Distributed Multicast of Fingerprinted Content Based on a Rational Peer-to-Peer Community. *Comput. Commun.* **2013**, *36*, 542–550. doi:10.1016/j.comcom.2012.12.005. [CrossRef]
23. Domingo-Ferrer, J. Rational Enforcement of Digital Oblivion. In Proceedings of the Fourth International Workshop on Privacy and Anonymity in the Information Society, Uppsala, Sweden, 25 March 2011; pp. 2:1–2:8. doi:10.1145/1971690.1971692. [CrossRef]
24. Qureshi, A.; Megías, D.; Rifà-Pous, H. Secure and Anonymous Multimedia Content Distribution in Peer-to-Peer Networks. In Proceedings of the 6th International Conference on Advances in Multimedia, Nice, France, 23–27 February 2014; pp. 91–96.
25. Qureshi, A.; Megías, D.; Rifà-Pous, H. Framework for Preserving Security and Privacy in Peer-to-Peer Content Distribution Systems. *Expert Syst. Appl.* **2015**, *42*, 1391–1408. doi:10.1016/j.eswa.2014.08.053. [CrossRef]
26. Qureshi, A.; Megías, D.; Rifà-Pous, H. PSUM: Peer-to-peer multimedia content distribution using collusion-resistant fingerprinting. *J. Netw. Comput. Appl.* **2016**, *66*, 180–197. doi:10.1016/j.jnca.2016.03.007. [CrossRef]

27. Qureshi, A.; Megías, D. Blockchain-based P2P multimedia content distribution using collusion-resistant fingerprinting. In Proceedings of the 11th Asia-Pacific Signal and Information Processing Association (APSIPA) Annual Summit and Conference, Lanzhou, China, 18–21 November 2019; pp. 1606–1615. doi:10.1109/APSIPAASC47483.2019.9023054. [[CrossRef](#)]
28. Megías, D.; Domingo-Ferrer, J. Privacy-aware Peer-to-Peer Content Distribution using Automatically Recombined Fingerprints. *Multimed. Syst.* **2014**, *20*, 105–125. doi:10.1007/s00530-013-0307-3. [[CrossRef](#)]
29. Megías, D.; Domingo-Ferrer, J. DNA-Inspired anonymous Fingerprinting for Efficient Peer-to-Peer Content Distribution. In Proceedings of the IEEE Congress on Evolutionary Computation, 2013, CEC'13, Cancun, Mexico, 20–23 June 2013; pp. 2376–2383. doi:10.1109/CEC.2013.6557853. [[CrossRef](#)]
30. Megías, D. Improved Privacy-Preserving P2P Multimedia Distribution Based on Recombined Fingerprints. *IEEE Trans. Dependable Sec. Comput.* **2015**, *12*, 179–189. doi:10.1109/TDSC.2014.2320712. [[CrossRef](#)]
31. Megías, D.; Qureshi, A. Collusion-resistant and privacy-preserving P2P multimedia distribution based on recombined fingerprinting. *Expert Syst. Appl.* **2017**, *71*, 147–172. doi:10.1016/j.eswa.2016.11.015. [[CrossRef](#)]
32. Nuida, K.; Fujitsu, S.; Hagiwara, M.; Kitagawa, T.; Watanabe, H.; Ogawa, K.; Imai, H. An Improvement of Tardos's Collusion-Secure Fingerprinting Codes with Very Short Lengths. In Proceedings of the 17th International Conference on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAecc'07, Bangalore, India, 16–20 December 2007; Springer: New York, NY, USA, 2007; pp. 80–89. doi:10.1007/978-3-540-77224-8_12. [[CrossRef](#)]
33. Nuida, K.; Fujitsu, S.; Hagiwara, M.; Kitagawa, T.; Watanabe, H.; Ogawa, K.; Imai, H. An improvement of discrete Tardos fingerprinting codes. *Des. Codes Cryptogr.* **2009**, *52*, 339–362. doi:10.1007/s10623-009-9285-z. [[CrossRef](#)]
34. Chen, X.; Lian, S. Research on Secure Digital Content Distribution for Peer to Peer E-commerce Applications. In Proceedings of the International Conference on Multimedia Information Networking and Security, Wuhan, China, 18–20 November 2009; Volume 1, pp. 463–467. doi:10.1109/MINES.2009.242. [[CrossRef](#)]
35. Hu, D.; Li, Q. Asymmetric fingerprinting based on 1-out-of-n oblivious transfer. *IEEE Commun. Lett.* **2010**, *14*, 453–455. doi:10.1109/LCOMM.2010.05.100067. [[CrossRef](#)]
36. Gao, H.; Zeng, W.; Chen, Z. Fingerprinting for Copyright Protection in P2P Context. In Proceedings of the International Symposium on Intelligence Information Processing and Trusted Computing, Wuhan, China, 28–29 October 2010; pp. 114–117. doi:10.1109/IPTC.2010.101. [[CrossRef](#)]
37. Terelius, B. Towards transferable watermarks in buyer-seller watermarking protocols. In Proceedings of the IEEE International Workshop on Information Forensics and Security (WIFS), Guangzhou, China, 18–21 November 2013; pp. 197–202. doi:10.1109/WIFS.2013.6707818. [[CrossRef](#)]
38. Fiat, A.; Naor, M. Broadcast encryption. In *Lecture Notes in Computer Science, Proceedings of the CRYPTO'93, Santa Barbara, CA, USA, 22–26 August 1993*; Springer: Heidelberg, Germany, 1993; Volume 773, pp. 480–491. doi:10.1007/3-540-48329-2_40. [[CrossRef](#)]
39. Chor, B.; Fiat, A.; Naor, M.; Pinkas, B. Tracing Traitors. *IEEE Trans. Inf. Theory* **2000**, *46*, 893–910. doi:10.1007/3-540-48658-5_25. [[CrossRef](#)]
40. Fiat, A.; Tassa, T. Dynamic traitor tracing. *J. Cryptol.* **2001**, *14*, 211–223. doi:10.1007/s00145-001-0006-7. [[CrossRef](#)]
41. Laarhoven, T. Dynamic Tardos traitor tracing schemes. *IEEE Trans. Inform. Theory* **2013**, *59*, 4230–4242. doi:10.1109/TIT.2013.2251756. [[CrossRef](#)]
42. Naini, R.S.; Wang, Y. Sequential tracing traitors. *IEEE Trans. Inform. Theory* **2003**, *49*, 1319–1326. doi:10.1007/3-540-44598-6_20. [[CrossRef](#)]
43. Bianchi, T.; Piva, A. TTP-free asymmetric fingerprinting protocol based on client side embedding. In Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP'14), Florence, Italy, 4–9 May 2014; pp. 3987–3991. doi:10.1109/ICASSP.2014.6854350. [[CrossRef](#)]
44. Bianchi, T.; Piva, A.; Shullani, D. Anticollusion solutions for asymmetric fingerprinting protocols based on client side embedding. *EURASIP J. Inf. Secur.* **2015**, *6*, 1–17. doi:10.1186/s13635-015-0023-y. [[CrossRef](#)]
45. Charpentier, A.; Fontaine, C.; Furon, T.; Cox, I. An Asymmetric Fingerprinting Scheme Based on Tardos Codes. In Proceedings of the 13th International Conference on Information Hiding, IH'11, Prague, Czech Republic, 18–20 May 2011; pp. 43–58. doi:10.1007/978-3-642-24178-9_4. [[CrossRef](#)]

46. Lin, C.Y.; Muchtar, K.; Yeh, C.H.; Lu, C.S. Secure multicasting of images via joint privacy-preserving fingerprinting, decryption, and authentication. *J. Vis. Commun. Image Represent.* **2016**, *38*, 858–871. doi:10.1016/j.jvcir.2016.02.003. [[CrossRef](#)]
47. Kuribayashi, M. Fingerprinting for broadcast content distribution system. In *Lecture Notes in Computer Science, Proceedings of the International Workshop on Digital Watermarking (IWDW'15), Siena, Italy, 15–17 September 2016*; Springer: Heidelberg, Germany, 2016; Volume 9569, pp. 163–175. doi:10.1007/978-3-319-31960-5_14. [[CrossRef](#)]
48. Kuribayashi, M.; Funabiki, N. Fingerprinting for multimedia content broadcasting system. *J. Inf. Secur. Appl.* **2018**, *41*, 52–61. doi:10.1016/j.jisa.2018.06.002. [[CrossRef](#)]
49. Kuribayashi, M.; Tanaka, H. Fingerprinting protocol for on-line trade using information gap between buyer and merchant. *IEICE Trans. Fundam.* **2006**, *E89-A*, 1108–1115. doi:10.1093/ietfec/e89-a.4.1108. [[CrossRef](#)]
50. Kuribayashi, M.; Funabiki, N. Decentralized tracing protocol for fingerprinting system. *APSIPA Trans. Signal Inf. Process.* **2019**, *8*, e2. doi:10.1017/ATSIP.2018.28. [[CrossRef](#)]
51. Škorić, B.; Vladimirova, T.U.; Celik, M.; Talstra, J.C. Tardos fingerprinting is better than we thought. *IEEE Trans. Inform. Theory* **2008**, *54*, 3663–3676. doi:10.1109/TIT.2008.926307. [[CrossRef](#)]
52. Furon, T.; Guyader, A.; Cérrou, F. On the design and optimization of Tardos probabilistic fingerprinting codes. In *Lecture Notes in Computer Science, Proceedings of the Information Hiding (IH'08), Santa Barbara, CA, USA, 19–21 May 2008*; Springer: Heidelberg, Germany, 2008; Volume 5284, pp. 341–356. doi:10.1007/978-3-540-88961-8_24. [[CrossRef](#)]
53. Paillier, P. Public-Key Cryptosystems Based on Composite Degree Residuosity Classes. In *Proceedings of the 17th International Conference on Theory and Application of Cryptographic Techniques, EUROCRYPT'99, Istanbul, Turkey, 13–17 April 1999*; Springer: Heidelberg, Germany, 1999; pp. 223–238. doi:10.1007/3-540-48910-X_16. [[CrossRef](#)]
54. Kuribayashi, M.; Funabiki, N. Efficient Decentralized Tracing Protocol for Fingerprinting System with Index Table. In *Proceedings of the 11th Asia-Pacific Signal and Information Processing Association (APSIPA) Annual Summit and Conference, Lanzhou, China, 18–21 November 2019*; pp. 1595–1601. doi:10.1109/APSIPAASC47483.2019.9023302. [[CrossRef](#)]
55. ElGamal, T. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Trans. Inf. Theory* **1985**, *31*, 469–472. doi:10.1109/TIT.1985.1057074. [[CrossRef](#)]
56. Sakai, Y.; Emura, K.; Hanaoka, G.; Kawai, Y.; Omote, K. Methods for Restricting Message Space in Public-Key Encryption. *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.* **2013**, *E96-A*, 1156–1168. doi:10.1587/transfun.E96.A.1156. [[CrossRef](#)]
57. Furon, T.; Preire, L.P. EM decoding of Tardos traitor tracing codes. In *Proceedings of the 11th ACM Workshop on Multimedia and Security, Princeton, NJ, USA, 7–8 September 2009*; pp. 99–106. doi:10.1145/1597817.1597835. [[CrossRef](#)]
58. Meerwald, P.; Furon, T. Towards practical joint decoding of binary Tardos fingerprinting codes. *IEEE Trans. Inform. Forensics Secur.* **2012**, *7*, 1168–1180. doi:10.1109/TIFS.2012.2195655. [[CrossRef](#)]
59. Desoubreaux, M.; Herzet, C.; Puech, W.; Guelvouit, G.L. Enhanced blind decoding of Tardos codes with new MAP-based functions. In *Proceedings of the 15th International Workshop on Multimedia Signal Processing (MMSP), Sardinia, Italy, 30 September–2 October 2013*; pp. 283–288. doi:10.1109/MMSP.2013.6659302. [[CrossRef](#)]
60. Laarhoven, T. Capacities and capacity-achieving decoders for various fingerprinting games. In *Proceedings of the 2nd ACM Workshop on Information Hiding and Multimedia Security (IH&MMSec'14), Salzburg, Austria, 11–13 June 2014*; pp. 123–134. doi:10.1145/2600918.2600925. [[CrossRef](#)]
61. Oosterwijk, J.J.; Škorić, B.; Doumen, J. A Capacity-Achieving Simple Decoder for Bias-Based Traitor Tracing Schemes. *IEEE Trans. Inf. Theory* **2015**, *61*, 3882–3900. doi:10.1109/TIT.2015.2428250. [[CrossRef](#)]
62. Kuribayashi, M. Bias equalizer for binary probabilistic fingerprinting codes. In *Lecture Notes in Computer Science, Proceedings of the Information Hiding (IH'12), Berkeley, CA, USA, 15–18 May 2012*; Springer: Heidelberg, Germany, 2012; Volume 7692, pp. 269–283. doi:10.1007/978-3-642-36373-3_18. [[CrossRef](#)]
63. Kuribayashi, M.; Funabiki, N. Universal scoring function based on bias equalizer for bias-based fingerprinting codes. *IEICE Trans. Fundam.* **2018**, *E101-A*, 119–128. doi:10.1587/transfun.E101.A.119. [[CrossRef](#)]

64. Yasui, T.; Kuribayashi, M.; N. Funabiki, I.E. Near-optimal detection for binary Tardos code by estimating collusion strategy. *IEEE Trans. Inf. Forensics Secur.* **2020**, *15*, 2069–2080. doi:10.1109/TIFS.2019.2956587. [[CrossRef](#)]
65. Wu, M.; Trappe, W.; Wang, Z.J.; Liu, K.J.R. Collusion resistant fingerprinting for multimedia. *IEEE Signal Process. Mag.* **2004**, 15–27. doi:10.1109/MSP.2004.1276103. [[CrossRef](#)]



© 2020 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).