# Digital Copyright Protection: Focus on Some Relevant Solutions

Franco Frattolillo

Department of Engineering, University of Sannio, Benevento, Italy

***Abstract:*** Copyright protection of digital content is considered a relevant problem of the current Internet since content digitalization and high performance interconnection networks have greatly increased the possibilities to reproduce and distribute digital content. Digital Rights Management (DRM) systems try to prevent the inappropriate or illegal use of copyrighted digital content. They are promoted by the major global media players, but they are also perceived as proprietary solutions that give rise to classic problems of privacy and fair use. On the other hand, watermarking protocols have become a possible solution to the problem of copyright protection. They have evolved during the last decade, and interesting proposals have been designed. This paper first presents current trends concerning the most significant solutions to the problem of copyright protection based on DRM systems and then focuses on the most promising approaches in the field of watermarking protocols. In this regard, the examined protocols are discussed in order to individuate which of them can better represent the right trade-off between opposite goals, such as, for example, security and easy of use, so as to prove that it is possible to implement open solutions compatible with the current web context without resorting to proprietary architectures or impairing the protection of copyrighted digital content.

***Keywords***: digital copyright protection, watermarking protocols, digital rights management.

## 1. Introduction

Content digitalization and high performance interconnection networks have greatly increased the possibilities to reproduce and distribute information on the Internet. Digitalisation allows for copying content without loss of quality, whereas the current Internet makes it possible to easily share and distribute content. However, the ability for anyone to make perfect copies of digital content and the ease by which such copies can be distributed facilitate misuse, illegal distribution, plagiarism, and misappropriation. Such a situation represents an actual threat for the owners of digital content, since they are no longer able to sell their content at a profitable price. In particular, they claim that the access to digital copyrighted content should be enabled under control license, since copyright violations lead to considerable revenue loss to copyright owners.

The need to guarantee the copyright protection of digital content distributed on the Internet just arises from the situation described above. In fact, copyright protection is currently considered as a basic requirement to avoid revenue loss to copyright owners, even though it is often perceived as a use restriction by web users [1]. More precisely, copyright owners aim at a wide dissemination of their digital content which does not compromise the originality and creativity of their intellectual properties. They want both to sell their content at the highest possible price and to reduce the costs of production and distribution. Digital Rights Management (DRM) systems have been developed to prevent the inappropriate or illegal use of copyrighted digital content [2, 3]. They should protect copyrights from infringement as well as be characterized by a use that does not limit a wide dissemination of digital content on the Internet. In this regard, DRM systems exploit security technologies to solve the main problem of preventing who are not provided with valid license from illegally copying or gaining access to copyrighted digital content [4, 5, 6].

DRM systems tend to protect the interests of content owners by maintaining a persistent control of the ownership over digital content distributed on the Internet. A first consequence of such an approach is that most of the DRM systems developed by relevant global media players, such as Sony, Apple, or Microsoft, are typically closed proprietary systems. They operate by packaging digital content in proprietary data containers made accessible only by using proprietary trusted hardware/software. This causes a lack of interoperability between different DRM systems. In addition, this also significantly reduces the ease in accessing digital content, since the restrictions imposed by DRM systems may hamper a number of legitimate uses, such as accessing the digital content on multiple devices or doing backup. Therefore, the adoption of DRM systems to protect copyrights has also caused “unintended” injury. More precisely, some uses of DRM systems have served no lawful purpose. On the contrary they have enforced unlawful agreements in restraining trade or have evaded statutory limits on the copyright. Furthermore, such uses have also given rise to problems concerning with the basic rights of “fair use” and privacy: the former is invoked in order to prevent copyright owners from having the exclusive control over their creations than the copyright law intends, whereas the latter is invoked in order to preserve the ownership and distribution of confidential data [1, 7, 8, 9, 10, 11].

A different approach to the problems reported above is represented by the web systems that employ watermarking based technologies [12] to implement the copyright protection of digital content distributed on the Internet. Such systems do not need to exploit proprietary technologies, but they can be based on open solutions well-documented in the literature. Their core is represented by the “watermark insertion techniques” and by the “watermarking protocols” they adopt: the former define the way in which watermarking information or “fingerprints” are embedded into digital content [12], whereas the latter define the scheme of the interactions that have to take place among the entities involved in the processes of content protection and web-based distribution implemented by such systems [13, 14].

Both watermark insertion techniques and watermarking protocols determine the security level that a web system can achieve in implementing the copyright protection of digital content. They have been characterized by a significant evolution during the last years. In particular, watermark insertion techniques have been designed so as to make watermarks robust against the most common and nonmalevolent manipulations and able to survive the most relevant and intentional attacks, such as signal processing based attacks, geometric attacks, or collusion attacks [12, 15, 16, 17]. Watermarking protocols, in turn, have been designed to be more suited for web context [14]. However, such an evolution has conducted to the development of very different solutions to the problem of digital copyright protection. As a consequence, this paper first presents current solutions to the problem of copyright protection based on DRM systems. Then it examines some of the most promising approaches in the field of watermarking protocols. In this regard, the examined protocols are discussed in order to individuate which of them can better represent the right trade-off between opposite goals, such as, for example, security and easy of use, so as to prove that it is possible to implement open solutions compatible with the current web context without resorting to proprietary architectures or impairing the protection of copyrighted digital content.

The paper is organized as follows. Section 2 describes the approach based on DRM systems to protect digital content. Section 3 reports on the main problems characterizing such systems. Section 4 introduces watermarking protocols and their security problems, together with the most important design challenges that such protocols have to face to be used in the current web context. In Section 5 some of the last and relevant solutions in the field of watermarking protocols are presented. In Section 6 a discussion of the watermarking protocols described in the previous sections is reported. Section 7 concludes the work.

## 2. Approach Based on DRM Systems

Although many different DRM systems have been proposed in the literature, current trends in the field of copyright protection are evolving towards solutions that use standard technologies based on HTML5 and its extensions [18]. The main motivation is that such solutions support interoperability among different DRM systems, since they enable web users provided with last generation internet browsers to access multimedia digital content protected by a proprietary DRM system by employing a different DRM system. This result can be achieved exploiting the Encrypted Media Extensions (EME) [19] of HTML5 together with the Common Encryption (CENC) technique [20].

EME is an extension of HTML5 and can be optionally implemented by a web browser. It provides an application programming interface (API) that enables web applications to interact with content protection systems in order to play encrypted audio and video content. Its peculiarity consists in enabling the same encrypted audio and video files to be played in any browser, regardless of the DRM system used to protect them, provided that these files have been encrypted according to the CENC scheme.

In contrast to legacy solutions proposed in the field of DRM systems, CENC allows content providers to encrypt and package their audio or video digital content once per container/codec and use it with a variety of DRM systems that support CENC.

In Figure 1 the scheme to play a protected digital audio or video content is shown. A web user can use a browser implementing EME to download a protected content from a server. Once the content has been received by the user, the browser invokes the EME API to recognize if the content is encrypted. This task is accomplished by accessing the metadata that are included in the media file container, which can be expressed in a standard format, such as the ISO Base Media File Format (BMFF) [21] or WebM [22].

If the content is encrypted, the browser has to contact a Content Decryption Module (CDM) to decrypt it. The CDM is a software or hardware component that enables playback of encrypted audio or video digital content. In this regard, EME provides an interface to interact with CDMs that are compliant with HTML5 extensions, whereas CDMs can simply decrypt a media content or also decode it, thus passing the decrypted and decoded media content to the browser for rendering.

CDMs can implement proprietary mechanisms to protect digital content. They represent the core of DRM systems. In fact, content protected by a specific and proprietary mechanism implemented by a DRM system can be unprotected only by using the CDM belonging to that DRM system. However, if a content is protected according to the CENC scheme, all the CDMs belonging to DRM systems that are compliant with such a scheme can be used to unprotect the content.

To unprotect content, the user browser creates a session to manage the key and the license that have to be obtained from the license server. Then, the browser contacts the CDM and passes it the metadata included in the media file container.

CDM receives the metadata and generates a request to acquire the key to decrypt the content from a license server. The request is sent to the browser, which takes charge of contacting the license server. Communication in this phase has to pass through the browser even though it is opaque to it. More precisely, the exchanged messages are understood only by the CDM and license server, although the browser can see what types of messages the CDM has sent.

When the browser receives a response from the license server, it passes the received data to the CDM, which can thus decrypt the protected content using the key included in the received license. In particular, the CDM can only decrypt the content, thus enabling playback using the normal media pipeline, for example, via a "<video>" HTML5 element. Otherwise, the CDM can decrypt and decode the content, thus passing content that can be directly rendered by the browser.

Finally, as observed above, a CDM implements a DRM system on a machine. It can be made available on a machine together with the browser or can be installed separately or can be directly supported by the operating system. However, in all cases the browser is responsible for exposing the CDM, and this result can be achieved only if both the browser and the DRM support the EME extensions.

## 3. Considerations

The approach described in Section 2 is characterized by a number of relevant advantages. First, HTML5 technologies, together with EME and CENC, support interoperability among different DRM systems, whereas early DRM systems were mostly based on closed proprietary mechanisms employing proprietary data formats and encryption techniques. Furthermore, they make the retrieval of keys and the playback of protected media files independent of the process of user authentication, which has to be directly managed by the web application before the access to such files.

On the other hand, the DRM systems developed according to the approach reported in Section 2 continue to be based on “black boxes”, that are the CDMs. In fact, even though the support to CENC and HTML5 extensions enables different CDMs to be equivalently used to unprotect media content, CDMs still remain closed proprietary components strictly tied to the underlying hardware/software computing architectures. Moreover, privacy is still a problem, since CDMs, by directly interacting with the user browser and the license server, can easily control who plays what, when, and with which application/software. Finally, the protection model is mainly based on securing the content delivery channel between the content provider and the web user rather than the content itself. More precisely, it requires that the protected audio or video digital content, once downloaded and unlocked by the CDM of the web user, is played by the user player, which is a trusted hardware or software component that has to be employed by the user to access the content. In particular, the user player acts together with the user web browser, and it is the unique component in charge of enforcing the usage rules associated with the protected content. However, this is a crucial aspect concerning the security chain implemented by the DRM systems adhering to the approach reported in Section 2, since adversaries have all the time and resources to attack user players. Furthermore, a protection model mainly based on content encryption can facilitate circumvention attacks such as, for example, those based on sound and video grabbing. In fact, encryption is the unique direct protection applied to audio and video digital content. As a consequence, when content is decrypted to be played, it is no longer protected and can be grabbed and then unlimitedly copied and redistributed. Therefore, persistent content protection is required.

## 4. Approach Based on Watermarking Protocols

To overcome the problems reported above, a different approach to the design of DRM systems has been proposed by the research community. It is based on watermarking protocols used to develop innovative web systems to protect copyrighted digital content.

Watermarking protocols define the schemes of the web transactions by which buyers can purchase protected digital content distributed by content providers (CPs) in a secure manner [13, 14]. They have to ensure both a correct content protection and an easy participation of buyers in the purchase transactions of content distributed on the Internet [23]. In this regard, most of the early experiences documented in the literature were based on the cooperation of entities such as buyers, sellers or CPs, and authorities called “watermark certification authorities” (WCAs), which are trusted third parties (TTPs) able to guarantee the correct execution of the protocols [24, 25, 26, 27, 28, 29].

However, in the last years, new experiences have been conducted in developing watermarking protocols. Most of them are based on the removal of WCAs from the protocols [30, 31, 32, 33, 34], since such authorities could give rise to potential collusion actions with buyers or sellers [35, 36, 37], thus weakening the security of the protocols. Nonetheless, the result of such experiences is often represented by inefficient watermarking protocols unsuited for the current web context, in which buyers are forced to perform complex security actions, if they want to complete their purchase transactions. As a consequence, in order to make watermarking protocols efficient and more suited for web context, new innovative design approaches have been explored [14, 23]. Such approaches are based on the main assumption that the participation of buyers in the protocols has to be simplified, since buyers are the less specialized party among those ones involved in the protocols. In fact, sellers are the main actors of their business, and can perform complex actions as well as equip themselves with specific and sophisticated software solutions. On the contrary, buyers have to be considered occasional customers, and so they should be forced to carry out only simple and intuitive actions to purchase digital content managed by watermarking protocols, just as it commonly happens in the marketplace.

Based on the considerations reported above, the following sections first focus on the main security problems that have to be solved by modern watermarking protocols. Then, they discuss the most relevant challenges posed by the design of such protocols.

### 4.1 Security Problems

This section enumerates the main security problems that are expected to be solved by modern watermarking protocols according to what is documented in recent studies conducted in the field of digital copyright protection [25, 26, 27, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47].

- *The piracy tracing problem*. The problem occurs when a watermarking protocol does not allow a CP to determine whether a user illegally possesses a digital content as well as who has appropriately purchased a content and then illegally shared it via, for example, peer-to-peer network applications. In this regard, the protocol should make it possible to collect undeniable proofs against a malicious buyer who has illegally redistributed pirated copies of a digital content and tries to deny this fact [17, 43].

- *The customer’s right problem.* The problem occurs when a watermarking protocol does not prevent a malicious CP from fabricating piracy to frame a honest buyer. In fact, a CP could make and distribute a protected copy of a digital content purchased by a buyer and then accuse the buyer of illegal distribution [25].

- *The unbinding problem.* The problem occurs when a watermarking protocol does not allow a dishonest CP to frame an innocent buyer by transplanting the buyer’s watermark into a copy of higher-priced digital content which the buyer never bought. In fact, a CP might accuse the buyer of illegal distribution as well as obtain a compensatory payment [25].

- *The anonymity problem*. The problem occurs when a watermarking protocol does not protect the buyer's privacy against CPs during the web transactions needed to purchase digital content. In fact, a CP could collect sensitive data about buyers and benefit from reselling them to other parties or exploiting them to do criminal actions [25].

- *The dispute resolution problem*. The "dispute resolution protocol" has to be run when a pirated copy is found in the market, and it is used to identify the "traitor", i.e. the buyer who distributed illegal replicas. Therefore, the dispute resolution problem occurs when such a protocol: (1) does not enable a CP to make appropriate adjudications without involving the suspected buyer, since, in actuality, such a buyer is very unlikely to cooperate; (2) is based on the disposition of presuming the guilt of an uncooperative buyer, because, in the general practice of law, it is the responsibility of the accuser to prove the guilt of the defendant, not the reverse; (3) depends on the cooperation between the buyer and the CP, because this could enable a malicious CP to easily harass an innocent buyer by repeatedly requiring cooperation [25].

- *The conspiracy problem*. The problem occurs when a watermarking protocol cannot nullify the effects of a collusion to fabricate piracy between a dishonest CP and a malicious buyer or between these two entities and an untrustworthy third party. In fact, a CP could attempt to cause the effects of the unbinding problem or of the customer's right problem, whereas the buyer could confound the tracing of piracy by obtaining the discredit or the removal of the watermark from the purchased content [17, 28, 40, 49, 50, 51].

- *The ambiguity problem*. The problem occurs when a watermarking protocol needs multiple watermark insertions to guarantee the protection of digital content. In fact, such insertions do not take into account that a digital content, when coded in a compressed format, has a limited capacity of including hidden information without suffering either a deterioration in its perceptual quality or a weakness in the information hiding scheme [52, 53]. Therefore, when applied independently, a second watermark could confuse or discredit the authority of the first watermark, and this can act as an actual "ambiguity attack" [12, 52, 53]. On the contrary, a single watermark insertion can be secure and robust [54], and enables the insertion of long fingerprinting codes particularly useful to exploit "anti-collusion" techniques [16, 17, 37, 55].

### 4.2Design Challenges

Even if a watermarking protocol solves the problems reported above, it has also to face the challenges posed by the current trends in the field of copyright protection of digital content distributed on the Internet [23, 30, 32, 33, 34, 40, 41, 42, 43, 45, 46, 47, 56, 57, 58].

The first relevant challenge deals with the negotiation mechanism supported by a watermarking protocol. It defines the method adopted by the protocol to identify buyers in the web transactions needed to purchase a digital content distributed by a CP [14]. In this regard, buyers should not be forced to adhere to a unique and rigid identification method when they want to buy digital content. On the contrary, they should be able to choose among different and usable identification methods, thus being able both to benefit from real purchase options and to accept the right trade-off between some of their goals, such as simplicity and anonymity [7, 59]. However, most of the watermarking protocols proposed in the literature adopt a unique negotiation mechanism mainly based on digital certificates issued by CAs. This is an actual problem, since digital certificates are widely used within Western Europe, the U.S., and Japan, but their spread within other geographical areas is still a slow and difficult process. Furthermore, it is unthinkable in the current web context that a buyer, for example, should possess and use a digital certificate even to purchase a single mp3 file. In fact, such protocols end up limiting the sale possibilities of CPs on the Internet.

The second relevant challenge concerns with the participation of buyers in watermarking protocols, which should be maximally simplified. In fact, while it is reasonable to assume that a TTP or a CP can perform complex security actions, it appears to be questionable to make the same assumptions for buyers, who should not be forced to perform actions that cannot be automatically carried out by plugins installed in their web browsers without a competent intervention. In particular, buyers should not be considered able to generate one-time anonymous public and private key pairs based on specific security parameters, or participate in group signature schemes and in interactive zero-knowledge proofs, or generate valid watermarks, or digitally sign or encrypt specific messages [30, 50, 60, 61]. Such an assumption represents a necessary condition to consider a watermarking protocol suited for the current web context, because it is unthinkable that buyers have to do one of the complex actions reported above, if they want to purchase content on the Internet. On the contrary, buyers can establish SSL (Secure Sockets Layer)/TLS (Transport Layer Security) connections to web sites that do not demand users for digital certificates, or can download and execute mobile code fragments, such as Javascript code or Java bytecode [14, 23].

Another relevant challenge concerns with the possible role of TTPs in watermarking protocols. In fact, such parties are often employed as WCAs, Arbitrators, or Judges, to guarantee the security of the protocols. However, in the real world, third parties could collude with the other parties involved in the protocols, thus impairing security. Furthermore, if a TTP is actively involved in the protocol, mostly acting as an entity that gathers inputs from buyer and seller and produces the outputs for them, the protocol ends up lacking theoretical interest, since it is well-known that any cryptographic task can be securely realized in an ideal world where a trusted party gets inputs from the other parties, computes the outputs and sends each party its corresponding output [62]. Therefore, protocols should not be based on such parties or, at most, should strongly limit the role played by them [30, 60]. However, the protocols that try not to employ TTPs need al least one TTP to validate specific data, or a crucial phase of their transaction schemes, or the plugins that have to be downloaded and installed in the buyers' web browsers. This demonstrates that TTPs, at the state of the art, cannot be completely eliminated from watermarking protocols, even though their role can be limited [40, 48]. Furthermore, the protocols that assume the untrusted behaviour or the limited role of TTPs end up adopting protection schemes that force buyers to perform complex security actions if they want to participate in purchase transactions, and this makes such protocols impractical and unsuited for the web context [30, 50, 60, 61]. As a consequence, if TTPs can neither be completely eliminated from watermarking protocols nor play fundamental roles, it is better to carefully exploit them [63, 64, 65] in order both to simplify the buyer participation in the protocols and to limit their role. In fact, the real challenge in designing a practical watermarking protocol suited for the web context consists in adopting a "buyer centric" approach based on striking a fair balance between a simple participation of buyers and a limited, but necessary, role of TTPs [23].

The last relevant challenge deals with the efficiency characterizing a watermarking protocol. It depends on the amount of computing, memory and communication resources that a protocol requires, and it determines the practicability of the protocol since the smaller amount of resources a protocol needs, the more feasible it is. Furthermore, since the tracing mechanism implemented by a watermarking protocol requires that a unique identification, i.e. the fingerprint, is embedded into each content distributed on the Internet, the time needed to apply the protection to a content and the size of the protected content become two crucial aspects of the protocol practicability. Finally, protocol scalability is another significant aspect of practicability, since it measures the capability of a protocol to adequately support the protection process in the presence of an increasing number of buyers.

## 5. Current Trends in Watermarking Protocols

In the following sections some of the most challenging watermarking protocols proposed in the last few years are described and discussed on the basis of what is reported above. The main aim is to realize if such protocols can be actually adopted to develop DRM systems suited for the current web context without resorting to proprietary solutions that do not correctly balance the opposite goals that characterize the problem of digital copyright protection in Internet.

### 5.1TTP-Free Watermarking Protocol

The proposal described in [30] is a TTP-free, "anonymous buyer and seller watermarking protocol". Similar to public key cryptography, it uses a private key to embed a watermark in a content, whereas the presence of the watermark can be verified using a public key. Both the keys are employed within an insertion scheme based on an interactive protocol between the buyer and the seller. The protocol ensures that the buyer is the sole entity able to obtain the content in its final watermarked form. Consequently, if the seller finds a watermarked copy of content in the market, it can identify the "traitor", that is who has initially obtained such a copy and then illegally shared it on the Internet [13, 14], and prove it to a third party [66]. Moreover, such a watermarking protocol enables both buyers to purchase watermarked content without informing their identities to sellers and sellers to identify traitors by employing a specific "dispute resolution protocol" [17, 66].

More precisely, according to what is reported in Figure 2, the buyer *B* generates a one-time key pair $(pk_B,sk_B)$, which has to be used in the public key cryptosystem that is "privacy homomorphic" with respect to the watermark insertion [67]. Homomorphic encryption enables buyer and seller to jointly compute the encryption of a watermark and to embed it directly in the encrypted content in such a way that none of the parties knows the inserted watermark. Then, *B* picks a random watermark $W_B$, and encrypts it bitwise with $pk_B$. *B* sets a request message that includes the identifier of the content to buy, the bitwise encryption of $W_B$, the public key $pk_B$, and further complementary information. Finally, *B* signs the request message, sends it to the seller *S*, and proves in "zero-knowledge" that the request is correctly computed by exploiting the complementary information included in the message. This means that *B*, i.e. the prover, can prove to *S*, i.e. the verifier, knowledge of some secret input that fulfils some statement by exploiting an interactive two-party protocol and without disclosing this input to the verifier.

After the zero-knowledge proof, *S* picks a unique random watermark $W_S$ and encrypts it bitwise with $pk_B$. Then, *S* computes the concatenation of the two encrypted watermarks $W_B$ and $W_S$, thus generating the watermark that can be embedded into the content to protect by using the homomorphic property of the encryption scheme. This means that the concatenation of the two encrypted watermarks can be embedded in the original content by running the watermark embedding algorithm directly in the encrypted domain. Finally, *S* sends the encrypted and watermarked content to *B*, who can decrypt it to obtain the final watermarked content.

The protocol described above is characterized by a simple and secure scheme. It solves all the problems reported in Section 4.1, particularly the conspiracy problem, without resorting to a TTP. However, buyers are required to perform complex security actions which cannot be carried out without specific competence. They have to perform encryptions and watermark generations, and they can purchase digital content on the Internet only if they are provided with digital certificates and are able to participate in interactive zero-knowledge proofs and group signature transaction schemes, without having further alternatives. Furthermore, the protocol is based on an additive homomorphic public key encryption scheme, which enables encrypted watermarks to be embedded directly into the encrypted content without prior decryption. However, such a scheme is very inefficient in practice, since it encrypts the samples of the content to be watermarked individually, and this causes a high computational overhead. Moreover, the protocol expands the size of the protected content due to the use of public-key encryption, and this requires a high communication bandwidth whenever the protected contents are sent to buyers. Therefore, the watermarking protocol is not scalable in the presence of an increasing number of buyers wanting to obtain protected contents, since each buyer has to receive a content protected by a personalised watermark.

### 5.2 Client-Side Embedding Watermarking Protocols

The watermarking protocol described in Section 5.1 does not properly take into account the demands of buyers for a transaction scheme that does not force them to carry out complex security actions. Moreover, it is affected by efficiency and scalability problems when the seller receives many purchase requests: the former are caused by watermark insertions in digital contents, which are heavy operations and are carried out solely by the seller; the latter are induced by the high communication overhead that occurs whenever the copy of a content, whose size is expanded by the insertion of a personalised watermark, is sent to a buyer.

Considerations about efficiency and scalability motivate the design of "client-side embedding watermarking protocols", which are characterized by protection schemes that adopt symmetric ciphers and "partial encryption" [33, 34, 39, 58] (see Figure 3). In such schemes, watermark insertion is carried out by sellers, which employ algorithms that additively distort selected transform coefficients of digital content with a noise sequence, thus making the distorted copy of content unusable. Then, the same distorted copy, which can be considered as encrypted content because of the embedded noise, is sent to all the buyer who wish to buy it, together with specific information needed to partially remove the embedded noise sequence. Such information is different for each buyer and enables buyers to leave an imperceptible fraction of noise representing the watermark. Consequently, each buyer can obtain a slightly different version of content, which thus ends up bearing a different watermark.

Client-side embedding watermarking protocols can achieve a high level of efficiency in applying the watermark protection, since they adopt an enciphering scheme that only requires computations of modular additions, whereas the other schemes based on homomorphic encryption often require computations of modular exponentiations, which are much more expensive than modular additions. However, they usually suffer a number of security problems, the most important of which are: the customer's rights problem and collusion problem.

The former is caused by the fact that the seller knows the information to partially remove the noise sequence embedded into the digital content sent to buyers and so it can have access to the decryption keys that carry the client-specific watermarks. Consequently, the seller can fabricate piracy to frame an innocent buyer, since it can make and distribute copy of digital content purchased by a buyer, then accuse the buyer of illegal distribution.

The latter depends on the watermarking insertion scheme and occurs when a coalition of buyers combine their differently watermarked copies in order to obtain a new copy in which the watermark is much harder to be detected. In fact, the watermark insertion scheme based on the distribution of the same distorted copy of digital content to all buyers is characterized by a documented vulnerability to collusion attacks [34].

To solve such problems, two relevant protocols have been proposed. The former [33] solves the customer's rights problem by modifying the original protection scheme to prevent the seller from accessing the decryption keys sent to buyers. Furthermore, the protection scheme makes it also possible to embed a personalized binary fingerprint in digital content as a result of the decryption operations. Consequently, digital content distributed on the Internet ends up being watermarked by personalized fingerprints that are unknown to the seller.

The latter [34] makes the proposal documented in [33] resistant to collusion attacks by adopting two different solutions for generating the fingerprinting codes to be embedded in the decryption keys sent to buyers: the former exploits a generation strategy conceptually similar to using near orthogonal independent Gaussian fingerprints, whereas the latter consists in generating the fingerprint of each user according to a Tardos code.

Even though the last developments of client-side embedding watermarking protocols make them secure, efficient and scalable without resorting to TTPs, they force buyers to perform complex security actions, such as the decryption of slightly different versions of the received content, thus generating copies protected by different watermarks. In fact, such a peculiarity makes them unsuited to web context [23].

### 5.3 Buyer-Friendly Watermarking Protocols

The main aim of buyer-friendly watermarking protocols is to overcome the problems that affect the protocols presented above by correctly balancing opposite goals, such as security and ease of the participation of buyers in the protocol. To this end, these new protocols try to carefully employ TTPs in order to make the participation of buyers in the protocols simple and intuitive without impairing security. In particular, in the buyer-friendly watermarking protocol documented in [23], the TTP is employed in the role of "security delegate", which is a common web entity specialized in supplying secure and reliable web services to buyers. More precisely, the TTP acts as a "registration authority", which is involved only in the initial phase of the proposed protocol. It can be implemented with a conventional Certication Authority (CA) that takes charge of generating "tokens" and information to be used to unambiguously identify the buyer, the seller, the purchased content, and the purchase transaction. It is not a WCA, even though it has to behave as a TTP in the sense of a common CA. Moreover, it cannot be considered as an actual "online" TTP, since it only intervenes in the initial, registration phase of the protocol, while it does not take part in the subsequent, core, protection phase.

In Figure 4, a buyer *B* wishing to purchase digital content from a seller *S* contacts the registration authority *RA* and communicates his/her personal and payment credentials. *RA*, which manages such credentials according to the widely accepted concept of "multilateral security" [7, 59], generates a "nonce" *N* and a one-time public and private key pair ($pk_B$,$sk_B$) linked to the *B*'s identity, the seller, the content, and the purchase transaction. Then, it generates further security tokens. Finally, it encrypts *N* with $pk_B$ and signs all the generated information and tokens, which are returned to *B*.

*B* forwards the encrypted nonce, the key $pk_B$, and some of the received information to *S*, which can thus use it to generate the watermark to be inserted into the chosen digital content directly in the encrypted domain, since the protocol is based on a privacy-homomorphic cryptosystem. In fact, the watermark is the concatenation of the encrypted nonce *N* and of an encrypted watermark picked by *S*. Then, *S* sends the encrypted and watermarked content to *B*, who can decrypts it, thus obtaining the final watermarked content.

The introduction of the registration authority in the role of security delegate makes it possible to strongly simplify the participation of buyers in the protection scheme without impairing security, thus achieving an actual buyer-friendly solution. In fact, a buyer has solely to interact with the seller and the registration authority: the interaction with the seller is "natural", whereas the interaction with the registration authority is needed to relieve the buyer of complex actions and to generate tokens able to make the protection transaction secure. Moreover, the protocol is characterized by a reduced number of interactions among the involved parties, even though it cannot be considered scalable, since its transaction scheme is similar to that one characterizing the protocol described in Section 5.1. However, the design approach adopted by the protocol makes it very promising, since buyers not provided with specific competences or digital certificates can purchase copyrighted digital content in a secure way.

**Table 1.** The main design characteristics of the watermarking protocols described in Section 5

| **Problems and Challenges** | **Comments** | | |
|---|---|---|---|
| | *TTP-free* wat. prot. | *Client-side embedding* wat. prot. | *Buyer-friendly* wat. prot. |
| Security problems | all solved | all solved | all solved |
| Negotiation mechanism | only one based on digital certificate | only one based on digital certificate | multiple |
| Participation of buyers | complex | complex | simple |
| Role of TTP | no TTP | no TTP | limited |
| Efficiency | low due to additive homomorphic encryption | medium due to partial encryption | low due to additive homomorphic encryption |
| Scalability | low | high | low |

**Table 2.** Pros and cons of the watermarking protocols described in Section 5

| ***Watermarking Protocols*** | ***Pros*** | ***Cons*** |
|---|---|---|
| *TTP-free* | simple transaction scheme<br>no TTP and collusion problems | complex actions in charge of buyers<br>limited efficiency and scalability |
| *Client-side embedding* | high efficiency and scalability | complex actions in charge of buyers |
| *Buyer-friendly* | no collusion problems<br>no complex actions in charge of buyers | limited efficiency and scalability |

## 6. Discussion

The watermarking protocols described in the previous sections are based on very different design approaches. Their main characteristics, together with pros and cons, are summarised in Table 1 and Table 2.

The protocol presented in Section 5.1 is based on the key idea of eliminating the TTP so as to restrict the transaction scheme to the sole interaction between buyer and seller. This enables the protocol to be secure and to solve the conspiracy problems through an interaction scheme that consists of a limited number of steps. However, such a design solution makes the interaction scheme unusable in the web context, since buyer (1) cannot take advantage of multiple negotiation mechanisms, (2) has to participate in an interactive zero-knowledge proof, and (3) has to generate the watermark to be inserted into the content to protect. To this end, it is worth noting that a watermark should be generated as a fingerprinting code [16, 17, 37, 55] in order not to reduce the effectiveness of the applied protection, and this cannot be considered as a competence of buyers. Finally, the protection scheme adopted by the protocol tends to enlarge the size of watermarked content, and requires that each content watermarked by a personalised fingerprinting code is directly transferred by the seller to each buyer. As a consequence, the protocol is characterized by a not scalable service model, since the seller is burdened by a huge amount of computation and communications when the number of content purchase requests increases.

In contrast to the solution referred above, client-side embedding watermarking protocols are characterized by a scalable service model, which is obtained by directly involving buyers in the protection process of digital content. In fact, as reported in Section 5.2, buyers have to take charge of partially removing the noise sequence previously embedded by the seller from the purchased content, thus obtaining a content watermarked by a personalised watermark. This also means that the scalability of the protocol is achieved at the expense of buyers, who have to perform complex actions to generate the final version of the purchased protected content.

The protocol presented in Section 5.3 represents an attempt to balance opposite design goals, such as security, easy of use, and efficiency. The key idea is to resort to a careful and restricted employ of a TTP in order to make the participation of buyers in the protocol easy. Therefore, the protocol adopts a simple protection scheme similar to that one implemented by the proposal documented in Section 5.1, but, at the same time, it avoids complex operations for buyers, such as participation in group signature scheme, watermark generation, participation in interactive zero-knowledge proofs, and signature checks. Nonetheless, the protocol is affected by the same efficiency and scalability problems that characterize the protocol described in Section 5.1.

## 7. Final Remarks

Digital copyright protection is a relevant problem for global media players and for web users. The former wish to adequately protect their digital content without incurring in problems of misuse, illegal distribution, plagiarism, and misappropriation, which cause considerable revenue loss. The latter wish to buy digital content without being forced to carry out complex security actions or to use proprietary DRM systems that can give rise to problems of privacy and fair use.

Although global media players promote software solutions based on HTML5 and its extensions, other solutions based on watermarking protocols appear to be very promising. They exploit watermarking techniques applied in the context of secure transactions to protect digital content distributed on the Internet. They have evolved over the last decade according to different design approaches, which have determined the points of strength and weakness of the major protocols. In this regard, the most recent solutions try to address the problem of achieving efficiency in applying protection and tend to eliminate TTPs, since such parties can give rise to collusive behaviors. However, when the TTPs are eliminated, the protocols end up requiring a complex participation of buyers in the purchase transactions of digital content, thus making the protocols unsuited for the current web context. On the contrary, buyer-friendly solutions are possible if, for example, “mediated” approaches are adopted. Such approaches are based on the introduction of security delegates, which can relieve buyers of the burden of carrying out complex security actions by generating specific security tokens during limited phases of protocols.

Security delegates behave like common CAs and their role can be carefully designed so as to prevent collusive behaviors. In this regard, future challenges to meet in designing buyer-friendly watermarking protocols concern the simplification of the transaction schemes, so as to makes the protocols scalable, and the reconsideration of the role of security delegates, which could be further limited.

## References

[1] E. W. Felten, “A skeptical view of DRM and fair use,” Communications of the ACM, Vol. 46, No. 4, pp. 57–59, 2004.

[2] W. Ku, C.-H. Chi, “Survey on the technological aspects of digital rights management,” Proc. 7th Int. Information Security Conf., K. Zhang and Y. Zheng, Eds., Palo Alto, CA, USA, September 27–29, 2004, Vol. 3225 of Lecture Notes in Computer Science, pp. 391–403, Springer-Verlag, Berlin, Germany.

[3] Z. Zhang, Q. Pei, J. Ma, L. Yang, “Security and trust in digital rights management: A survey,” Int. Journal of Network Security, Vol. 9, No. 3, pp. 247–263, 2009.

[4] F. Frattolillo, F. Landolfi, “A Cluster Grids Based Platform for Digital Copyright Protection,” Proc. 12th IEEE Int. Symp. on Web Systems Evolution, Timisoara, Romania, September 17–18, 2010, pp. 83–87, IEEE Computer Society, Washington, DC, USA.

[5] F. Frattolillo, F. Landolfi, F. Marulli, “A novel approach to DRM systems,” Proc. 12th IEEE Int. Conf. on Computational Science and Engineering, Vancouver, Canada, August 29–31, 2009, pp. 492–497, IEEE Computer Society, Washington, DC, USA.

[6] F. Frattolillo, F. Landolfi, “Designing a DRM system,” Proc. 4th Int. Conf. on Information Assurance and Security, Naples, Italy, September 8–10, 2008, pp. 221–226, IEEE Computer Society, Washington, DC, USA.

[7] K. Rannenberg, D. Royer, A. Deuker, “The Future of Identity in the Information Society - Challenges and Opportunities”, Springer, Berlin, Germany, 2009.

[8] A. Rehman, S. Rehman, I. U. Khan, M. Moiz, S. Hasan, “Security and Privacy Issues in IoT,” International Journal of Communication Networks and Information Security, Vol. 8, No. 3, pp. 147–157, 2016.

[9] J. Sen, “A secure and user privacy-preserving searching protocol for peer-to-peer networks,” International Journal of Communication Networks and Information Security, Vol. 4, No. 1, pp. 29–40, 2012.

[10] M. Backes, N. Grimm, A. Kate, “Data Lineage in Malicious Environments,” IEEE Transactions on Dependable and Secure Computing, Vol. 13, No. 2, pp. 178–191, 2016.

[11] K. Fan, X. Yao, X. Fan, Y. Wang, M. Chen, “A new usage control protocol for data protection of cloud environment,” EURASIP Journal on Information Security, Vol. 2016, No. 1, pp. 1–7, 2016.

[12] I. Cox, M. Miller, J. Bloom, J. Fridrich, T. Kalker, “Digital Watermarking and Steganography”, Morgan Kaufmann, Burlington, MA, USA, 2007.

[13] K. Gopalakrishnan, N. Memon, P. L. Vora, “Protocols for watermark verification,” IEEE Multimedia, Vol. 8, No. 4, pp. 66–70, 2001.

[14] F. Frattolillo, “Watermarking protocols: Problems, challenges and a possible solution,” The Computer Journal, Vol. 58, No. 4, pp. 944–960, 2015.

[15] F. A. P. Petitcolas et al., “A public automated web-based evaluation service for watermarking schemes: StirMark benchmark,” in Electronic Imaging 2001, Security and Watermarking of Multimedia Contents, P. W. Wong and E. J. Delp, Eds., S. Jose, CA, USA, Jan. 2001, Vol. 4314 of Proc. of SPIE, pp. 575–584, SPIE, Bellingham WA, USA.

[16] W. Trappe, M. Wu, Z. J. Wang, K. J. R. Liu, “Anti-collusion fingerprinting for multimedia,” IEEE Trans. Signal Process., Vol. 41, No. 4, pp. 1069–1087, 2003.

[17] K. J. R. Liu, W. Trappe, Z. J. Wang, M. Wu, H. Zhao, “Multimedia Fingerprinting Forensics for Traitor Tracing”, Hindawi Publishing Corporation, New York, NY, USA, 2005.

[18] I. Hickson et al., “HTML5: A vocabulary and associated APIs for HTML and XHTML”, W3C, `https://www.w3.org/TR/html5/`, october 2014.

[19] D. Dorwin et al., “Encrypted Media Extensions”, W3C, https://www.w3.org/TR/encrypted-media/, February 2016.

[20] H. W. Barz, G. A. Bassett, “Multimedia Networks: Protocols, Design and Applications”, Wiley, 2016.

[21] A. Colwell, A. Bateman, M. Watson, “ISO BMFF Byte Stream Format”, W3C, https://w3c.github.io/media-source/isobmff-byte-stream-format.html, March 2015.

[22] The WebM Project, http://www.webmproject.org/, “WebM: an open web media project”, 2016.

[23] F. Frattolillo, “A buyer–friendly and mediated watermarking protocol for web context,” ACM Transactions on the Web, Vol. 10, No. 2, article no. 9, April 2016.

[24] N. Memon, P. W. Wong, “A buyer-seller watermarking protocol,” IEEE Trans. Image Process., Vol. 10, No. 4, pp. 643–649, 2001.

[25] C. L. Lei, P. L. Yu, P. L. Tsai, M. H. Chan, “An efficient and anonymous buyer-seller watermarking protocol,” IEEE Trans. Image Process., Vol. 13, No. 12, pp. 1618–1626, 2004.

[26] C. I. Fan, M. T. Chen, W. Z. Sun, “Buyer-seller watermarking protocols with off-line trusted parties,” Proc. IEEE Int. Conf. on Multimedia and Ubiquitous Engineering, Seul, South Korea, April 26–28, 2007, pp. 1035–1040, IEEE Computer Society, Washington, DC, USA.

[27] V. V. Das, “Buyer-seller watermarking protocol for an anonymous network transaction,” Proc. 1st Int. Conf. on Emerging Trends in Engineering and Technology, Nagpur, Maharashtra, India, July 16–18, 2008, pp. 807–812, IEEE Computer Society, Washington, DC, USA.

[28] V. Laxmi, M. N. Khan, S. Sarath, M. S. Gaur, “Buyer seller watermarking protocol for digital rights management,” Proc. 2nd Int. Conf. on Security of information and networks, Famagusta, North Cyprus, October 6–10, 2009, pp. 298–301, ACM, New York, NY, USA.

[29] D. Hu, Q. Li, “A secure and practical buyer-seller watermarking protocol,” Proc. Int. Conf. on Multimedia Information Networking and Security, Wuhan, China, November 18–20, 2009, pp. 105–108, IEEE Computer Society, Washington, DC, USA.

[30] A. Rial, M. Deng, T. Bianchi, A. Piva, B. Preneel, “A provably secure anonymous buyer—seller watermarking protocol,” IEEE Trans. Inf. Forensics Security, Vol. 5, No. 4, pp. 920–931, 2010.

[31] A. Rial, J. Balasch, B. Preneel, “A privacy-preserving buyer—seller watermarking protocol based on priced oblivious transfer,” IEEE Trans. Inf. Forensics Security, Vol. 6, No. 1, pp. 202–212, 2011.

[32] Z. Xu, L. Li, H. Gao, “Bandwidth efficient buyer-seller watermarking protocol,” Int. Journal of Information and Computer Security, Vol. 5, No. 1, pp. 1–10, 2012.

[33] T. Bianchi, A. Piva, “TTP-free asymmetric fingerprinting based on client side embedding,” IEEE Trans. Inf. Forensics Security, Vol. 9, No. 10, pp. 1557–1568, 2014.

[34] T. Bianchi, A. Piva, D. Shullani, “Anticollusion solutions for asymmetric fingerprinting protocols based on client side embedding,” Eurasip Journal on Information Security, Vol. 2015, No. 6, 2015.

[35] M. Barni, F. Bartolini, “Watermarking Systems Engineering: Enabling Digital Assets Security and Other Applications”, CRC Press, Boca Raton, FL, USA, 2004.

[36] M. Wu, W. Trappe, Z. J. Wang, K. J. R. Liu, “Collusion-resistant fingerprinting for multimedia,” IEEE Signal Process. Mag., Vol. 21, No. 2, pp. 15–27, 2004.

[37] H. V. Zhao, K. J. R. Liu, “Traitor-within-traitor behavior forensics: Strategy and risk minimization,” IEEE Trans. Inf. Forensics Security, Vol. 1, No. 4, pp. 440–456, 2006.

[38] I. M. Ibrahim, S. H. N. El-Din, A. F. A. Hegazy, “An effective and secure buyer-seller watermarking protocol,” Proc. 3rd Int. Symp. on Information Assurance and Security, Manchester, United Kingdom, August 29–31, 2007, pp. 21–28, IEEE Computer Society, Washington, DC, USA.

[39] S. Katzenbeisser, A. Lemma, M. U. Celik, M. van der Veen, M. Maas, “A buyer—seller watermarking protocol based on secure embedding,” IEEE Trans. Inf. Forensics Security, Vol. 3, No. 4, pp. 783–786, 2008.

[40] G. S. Poh, K. M. Martin, “Classification framework for fair content tracing protocols,” in Proc. 8th Int. Workshop on Digital Watermarking, A. T. S. Ho, Y. Q. Shi, H. J. Kim, and M. Barni, Eds., Guildford, UK, August 24–26, 2009, Vol. 5703 of Lecture Notes in Computer Science, pp. 252–267, Springer-Verlag, Berlin, Germany.

[41] C.-C. Chang, H.-C. Tsai, Y.-P. Hsieh, “An efficient and fair buyer-seller fingerprinting scheme for large scale networks,” Computers and Security, Vol. 29, No. 2, pp. 269–277, 2010.

[42] J. Zhang, Y. Xiang, W. Zhou, L. Ye, Y. Mu, “Secure image retrieval based on visual content and watermarking protocol,” The Computer Journal, Vol. 54, No. 10, pp. 1661–1674, 2011.

[43] S.-H. Lee, S.-G. Kwon, K.-R. Kwon, “Mobile 3d secure transmission based on anonymous buyer-seller watermarking protocol,” Recent Advances in Communications and Networking Technology, Vol. 3, No. 1, pp. 33–43, 2014.

[44] F. Frattolillo, “A Digital Rights Management System Based on Cloud,” Telkomnika, Vol. 15, No. 2, pp. 671–677, 2017.

[45] F.-G. Jeng, J.-C. Huang, T.-H. Chen, “An Improved Anonymous Buyer-Reseller Watermarking Protocol,” International Journal of Network Security, Vol. 18, No. 4, pp. 728–735, 2016.

[46] A. Qureshi, D. Megías, H. Rifà-Pous, “PSUM: Peer-to-peer multimedia content distribution using collusion-resistant fingerprinting,” Journal of Network and Computer Applications, Vol. 66, pp. 180-197, 2016.

[47] J-C. Huang, F.-G. Jeng, T.-H. Chen, “A new buyer-seller watermarking protocol without multiple watermarks

insertion," Multimedia Tools and Applications, Vol. 76, No, 7, pp. 9667–9679, 2017.

[48] G. S. Poh, "Design and Analysis of Fair Content Tracing Protocols", Ph.D. thesis, Department of Mathematics, Royal Holloway, University of London, Egham, Surrey, England, 2009.

[49] J. Zhang, W. Kou, K. Fan, "Secure buyer-seller watermarking protocol," IEE Proc. Inf. Secur., Vol. 153, No. 1, pp. 15–18, 2006.

[50] M. Deng, B. Preneel, "On secure and anonymous buyer-seller watermarking protocol," Proc. 3rd Int. Conf. on Internet and Web Applications and Services, Athens, Greece, June 8–13, 2008, pp. 524–529, IEEE Computer Society, Washington, DC, USA.

[51] Y. Hu, J. Zhang, "A secure and efficient buyer-seller watermarking protocol," Journal of Multimedia, Vol. 4, No. 3, pp. 161–168, 2009.

[52] F. Hartung, J. K. Su, B. Girod, "Spread spectrum watermarking: Malicious attacks and counterattacks," in Security and Watermarking of Multimedia Contents, E. J. Delp and P. W. Wong, Eds., San Jose, CA, USA, April 9, 1999, Vol. 3657 of Proc. of SPIE, pp. 147–158, SPIE, Bellingham WA, USA.

[53] S. Katzenbeisser, H. Veith, "Securing symmetric watermarking schemes against protocol attacks," in Security and Watermarking of Multimedia Contents IV, E. J. Delp, P. W. Wong, Eds., S. Jose, CA, USA, April 29, 2002, Vol. 4675 of Proc. of SPIE, pp. 260–268, SPIE, Bellingham WA, USA.

[54] B. Chen, G. Wornell, "Quantization index modulation: a class of provably good methods for digital watermarking and information embedding," IEEE Trans. Inf. Theory, Vol. 47, No. 4, pp. 1423–1443, 2001.

[55] S. Pehlivanoglu, "An asymmetric fingerprinting code for collusion-resistant buyer-seller watermarking," Proc. 1st ACM Workshop on Information Hiding and Multimedia Security, Montpellier, France, June 17–19, 2013, pp. 35–44, ACM, New York, NY, USA.

[56] T. Bianchi, A. Piva, "Secure watermarking for multimedia content protection: A review of its benefits and open issues," IEEE Signal Process. Mag., Vol. 30, No. 2, pp. 87–96, 2013.

[57] X. Cui, G. Sheng, F. Li, X. Liu, "An efficient and impartial buyer-seller watermarking protocol," Journal of Communications, Vol. 10, No. 5, pp. 339–344, 2015.

[58] J.-H. Sun, Y.-H. Lin, J.-L. Wu, "Secure client side watermarking with limited key size," in Proc. MultiMedia Modeling: 21st Int. Conf., X. He, S. Luo, D. Tao, C. Xu, J. Yang, and M. A. Hasan, Eds., Sydney, Australia, January 2015, Vol. 8935 of Lecture Notes in Computer Science, pp. 13–24, Springer Int. Publishing.

[59] K. Rannenberg, "Multilateral security. A concept and examples for balanced security," Proc. 9th ACM Workshop on New Security Paradigms, Cork, Ireland, September 18–21, 2000, pp. 151–162, ACM, New York, NY, USA.

[60] M. Deng, B. Preneel, "Attacks on two buyer-seller watermarking protocols and an improvement for revocable anonymity," Proc. IEEE Int. Symp. on Electronic Commerce and Security, Guangzhou, China, August 3–5, 2008, pp. 923–929, IEEE Computer Society, Washington, DC, USA.

[61] M. Deng, T. Bianchi, A. Piva, B. Preneel, "An efficient buyer-seller watermarking protocol based on composite signal representation," Proc. 11th ACM Workshop on Multimedia and Security, Princeton, NJ, USA, September 7–8, 2009, pp. 9–18, ACM, New York, NY, USA.

[62] R. Canetti, "Universally composable security: A new paradigm for cryptographic protocols," Proc. 42nd IEEE Int. Symp. on Foundations of Computer Science, Las Vegas, NV, USA, October 2001, pp. 136–145, IEEE Computer Society, Washington, DC, USA.

[63] D. Boneh, X. Ding, G. Tsudik, C. M. Wong, "A method for fast revocation of public key certificates and security capabilities," Proc. 10th USENIX Security Symposium, Washington, D.C., USA, Aug. 2001, pp. 297–308, The USENIX Association.

[64] X. Ding, G. Tsudik, "Simple identity-based cryptography with mediated RSA," in The Cryptographers' Track at the RSA Conference 2003, M. Joye, Ed., San Francisco, CA, USA, Apr. 2003, Vol. 2612 of Lecture Notes in Computer Science, pp. 193–210, Springer-Verlag, Berlin, Germany.

[65] F. W. C. Yang, X. Wang, "Efficient mediated certificates public-key encryption scheme without pairings," Proc. 21st Int. Conf. on Advanced Information Networking and Applications Workshops, Niagara Falls, Ontario, Canada, May 21–23, 2007, pp. 109–112, IEEE Computer Society, Washington, DC, USA.

[66] M. Kuribayashy, H. Tanaka, "Fingerprinting protocol for images based on additive homomorphic property," IEEE Trans. Image Process., Vol. 14, No. 12, pp. 2129–2139, 2005.

[67] C. Fontaine, F. Galand, "A survey of homomorphic encryption for nonspecialists," EURASIP Journal on Information Security, Vol. 2007, 2007.

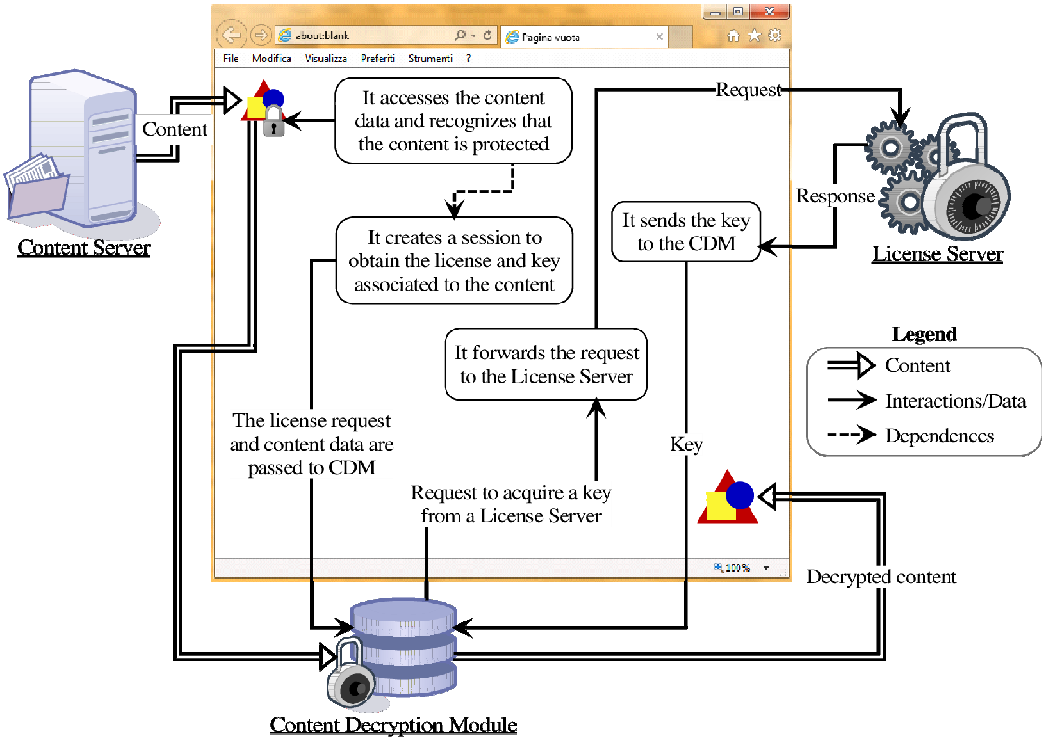
File Modifica Visualizza Preferiti Strumenti ?
about:blank
Pagina vuota
Content
Content Server
It accesses the content data and recognizes that the content is protected
It creates a session to obtain the license and key associated to the content
Request
Response
License Server
It sends the key to the CDM
It forwards the request to the License Server
The license request and content data are passed to CDM
Request to acquire a key from a License Server
Key
Decrypted content
100%
Legend
Content
Interactions/Data
Dependences
Content Decryption Module

**Figure 1.** DRM system based on HTML5 and its extensions

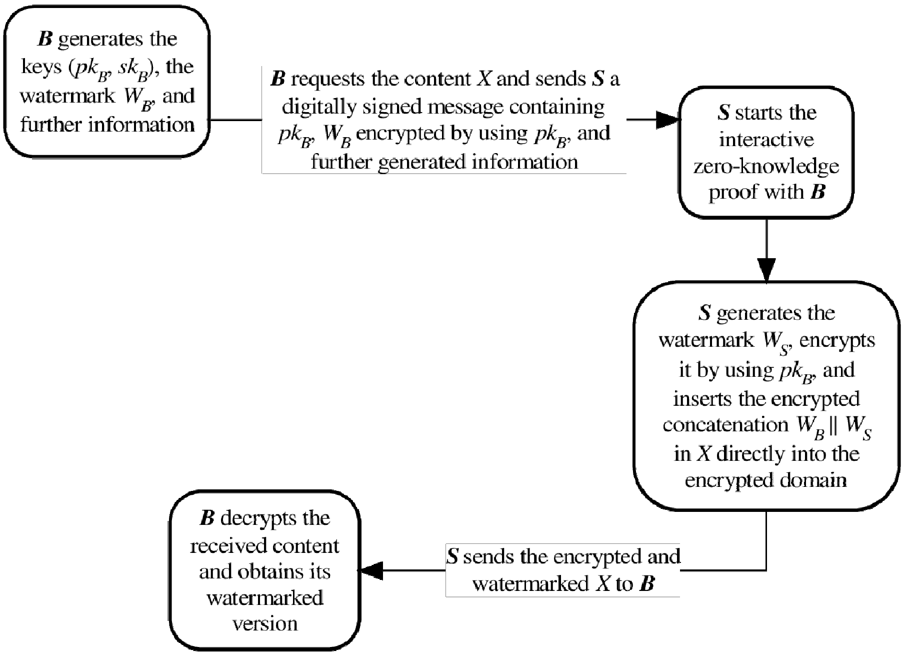
*B* generates the keys ($pk_B$, $sk_B$), the watermark $W_B$, and further information
*B* requests the content *X* and sends *S* a digitally signed message containing $pk_B$, $W_B$ encrypted by using $pk_B$, and further generated information
*S* starts the interactive zero-knowledge proof with *B*
*S* generates the watermark $W_S$, encrypts it by using $pk_B$, and inserts the encrypted concatenation $W_B \| W_S$ in *X* directly into the encrypted domain
*S* sends the encrypted and watermarked *X* to *B*
*B* decrypts the received content and obtains its watermarked version

**Figure 2.** The scheme of a TTP-free watermarking protocol

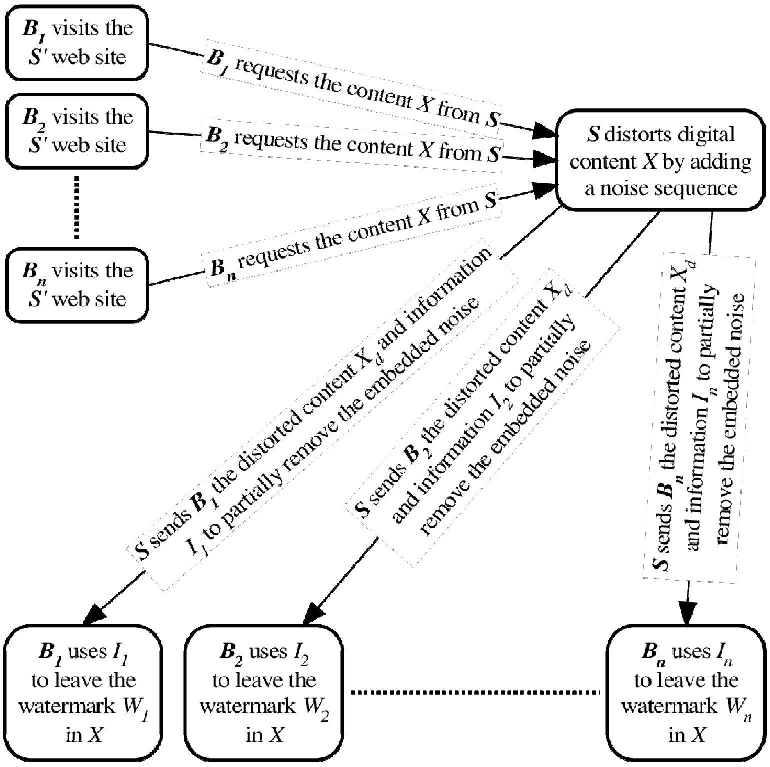
B1 visits the S' web site
B2 visits the S' web site
Bn visits the S' web site
B1 requests the content X from S
B2 requests the content X from S
Bn requests the content X from S
S distorts digital content X by adding a noise sequence
S sends B1 the distorted content Xd and information I1 to partially remove the embedded noise
S sends B2 the distorted content Xd and information I2 to partially remove the embedded noise
S sends Bn the distorted content Xd and information In to partially remove the embedded noise
B1 uses I1 to leave the watermark W1 in X
B2 uses I2 to leave the watermark W2 in X
Bn uses In to leave the watermark Wn in X

**Figure 3.** The scheme of a client-side embedding watermarking protocol

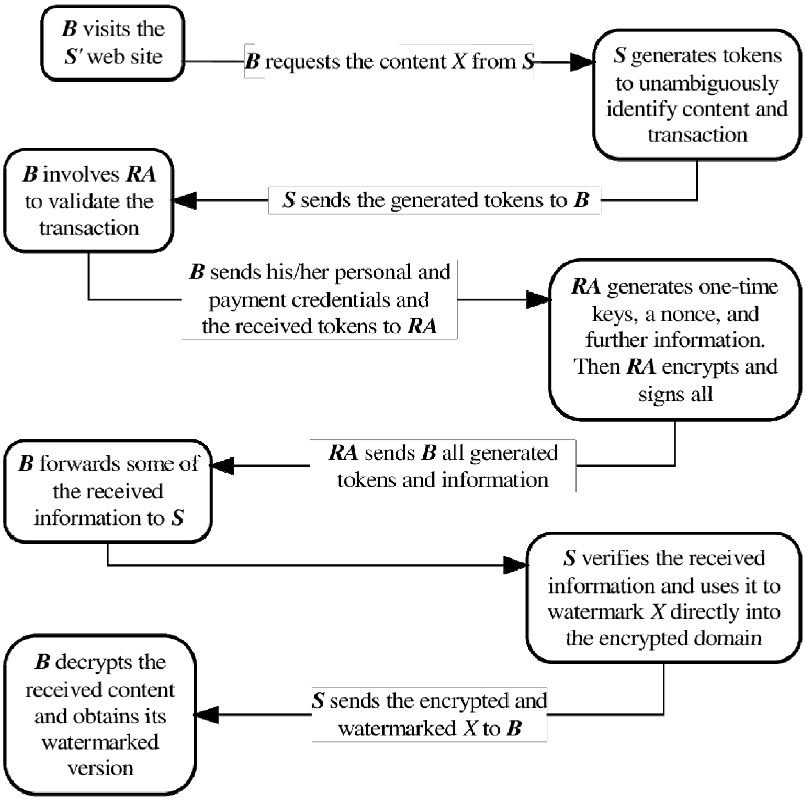
B visits the S' web site
B requests the content X from S
S generates tokens to unambiguously identify content and transaction
S sends the generated tokens to B
B involves RA to validate the transaction
B sends his/her personal and payment credentials and the received tokens to RA
RA generates one-time keys, a nonce, and further information. Then RA encrypts and signs all
RA sends B all generated tokens and information
B forwards some of the received information to S
S verifies the received information and uses it to watermark X directly into the encrypted domain
S sends the encrypted and watermarked X to B
B decrypts the received content and obtains its watermarked version

**Figure 4.** The scheme of a buyer-friendly watermarking protocol