future internet

MDPI

Article

Watermarking Protocols: A Short Guide for Beginners

Franco Frattolillo

Department of Engineering, University of Sannio, Corso Garibaldi 107, 82100 Benevento, Italy; frattolillo@unisannio.it; Tel.: +39-0824305806

Abstract: Watermarking protocols, in conjunction with digital watermarking technologies, make it possible to trace back digital copyright infringers by identifying who has legitimately purchased digital content and then illegally shared it on the Internet. Although they can act as an effective deterrent against copyright violations, their adoption in the current web context is made difficult due to unresolved usability and performance issues. This paper aims at providing researchers with the basics needed to design watermarking protocols suited to the web context. It is focused on two important aspects. The first concerns the basic requirements that make a protocol usable by both web users and content providers, whereas the second concerns the security primitives and how they have been used to implement the most relevant examples of watermarking protocols documented in the literature. In this way, researchers can rely on a quick guide to getting started in the field of watermarking protocols.

Keywords: watermarking protocols; digital copyright protection; digital rights management

Citation: Frattolillo , F. Watermarking Protocols: A Short Guide for Beginners. *Future Internet* **2023**, *15*, 163. https://doi.org/10.3390/fi15050163

Academic Editor: Michael Sheng

Received: 30 March 2023
Revised: 23 April 2023
Accepted: 26 April 2023
Published: 28 April 2023

1. Introduction and Motivations

Digital copyright protection is one of the relevant problems of the current Internet because anyone can legitimately purchase digital contents from content providers and then illegally share them by means of peer-to-peer network applications. In fact, the current network and multimedia technologies make it easy to duplicate, modify, and re-distribute digital contents without reducing their perceptual quality. As a consequence, content providers endure heavy economic losses because they cannot adequately protect their digital contents.

Although the problem of copyright protection is widely recognized, its solution is hard to find since it has to take into account the conflicting interests of content providers and web users wanting to enjoy digital contents. The former want to sell as many contents as possible at the highest possible price without incurring high protection and distribution costs; the latter, on the contrary, want to purchase contents at the lowest possible price. They want to follow the "fair use" doctrine, which guarantees legitimate buyers dominion over reproduction, public performance and display, and distribution of the purchased content. Moreover, web users want to keep control over the ownership and the spreading of their personal data, thus preserving privacy and opposing protection mechanisms that tend to identify them.

In the past, the research community has been very active in proposing solutions to the copyright protection problem. Some of them are based on financial incentives that attempt to make the copyrighted versions of contents more desirable and useful than copies. Others adopt punitive approaches that force third parties, such as Internet Service Providers (ISP), to prevent web users from performing illegal content sharing. Still others exploit the so-called Digital Rights Management (DRM) systems [1–3], which are web platforms aiming at enforcing the legal rights associated with the use of copyrighted digital contents by implementing specific services. They usually keep track of content modifications or manage copyright transfers and other transactions related to digital contents distributed on the Internet. However, all these solutions have revealed specific shortcomings. For

example, financial incentives have reduced the earning capacity of content providers. ISPs have often been accused of privacy violation in monitoring the data traffic of web users with the aim of preventing illegal content sharing. DRM systems, for their part, cannot counter the illegal sharing of contents legitimately bought by web users. They cannot legally prove the ownership of content that has been downloaded and tampered as well as identify those responsible for copyright infringement. Moreover, DRM systems have been often accused of having too much control over the protected contents compared to what the copyright law intends.

A different approach to protecting digital copyright is represented by solutions based on digital watermarking [4]. They make it possible to embed hidden "fingerprints", in the form of "watermarks", into the contents sold on the Internet [5]. In this way, if watermarks are generated so as to identify buyers, and if the watermarked contents are released according to interaction schemes specified by "watermarking protocols", the embedded watermarks can be used as a proof of ownership to identify the web users who have legitimately purchased contents and then illegally shared them on the Internet [6].

The capacity to identify initial copyright "infringers" by examining one of the copies of content illegally shared on the Internet makes watermarking protocols an effective solution to the digital copyright problem. The basic idea consists of a simple consideration: the more a web user illegally shares a legitimately purchased content, the greater the likelihood that the copyright infringement will be picked up and punished. This represents an effective deterrent against copyright violations.

A consequence of what is reported above is that the scientific literature on the watermarking protocols of the last two decades is characterized by a wide variety of proposals. The proposed protocols mainly differ in the requirements they meet and in the security primitives they exploit, thus achieving very different results in terms of security and practicability for the web context.

This paper proposes a systematization of preliminary knowledge needed to design innovative watermarking protocols, particularly those based on the popular "buyer–seller" scheme [7,8]. Therefore, the paper firstly specifies and discusses the basic requirements that make a protocol usable by both web users and content providers. Then, it lists the security primitives used to implement the most relevant examples of watermarking protocols documented in the literature. In this way, researchers can rely on a short guide to design watermarking protocols without making the classic errors characterizing many of the previous protocols proposed by the scientific community.

2. Requirements

Watermarking protocols can be effective only if two basic requirements are met. The first concerns the watermark embedding algorithm, which has to be both robust against non-intentional manipulations and secure against intentional attacks. Thus, the watermark extracted from a content can unambiguously identify its original buyer. The second involves the watermarking protocol, which has to ensure that only the original buyer of a content has access to it in its final, protected form.

However, the nature of the requirements reported above has usually led researchers to focus on the security design of watermarking protocols, thus overlooking their practicality for the current web context. Hence, there is a need to revise the set of the classic requirements documented in the literature on watermarking protocols. The main aim is to mainly differentiate "practicality" requirements from security requirements. The former, also named "usability" requirements, deal with the participation of buyers and sellers in the interaction schemes defined by the protocols; the latter specify the conditions that have to be ensured by the protocols in order to be considered secure. Both are usually described in terms of problems that the protocols have to solve.

2.1. Usability Requirements

The studies conducted in the past few years show that usability requirements must be given priority over security requirements in designing modern watermarking protocols. In fact, if a protocol makes the involvement of buyers in the interaction scheme difficult, or if it does not meet the actual service needs of content providers, the distribution of protected contents on the Internet can be seriously hampered. This harms the business interests of content providers, thus making the security capacities of the protocol useless [9].

2.1.1. Buyer Problem

E-commerce has become a consolidated reality in the current Internet. Web users purchase goods online by simply using credit or pre-paid cards. They are not required to have specific competence to participate in the purchase transactions. They only need to know how to use modern web browsers supporting HTML5 and scripts. As a consequence, such ease must also be ensured when web users purchase copyrighted digital content. This means that watermarking protocols have to be designed so as not to force buyers to carry out complex actions such as, for example, participating in zero-knowledge proof or group signature schemes, generating one-time anonymous public and private key pairs based on specific security parameters, creating valid watermarks based on fingerprinting codes, or digitally signing or encrypting messages or tokens. Such actions are permitted only if they can be automatically supported by web browsers [9].

2.1.2. Content Provider Problem

Initially, content providers were web entities specialized in producing and distributing paid digital contents. However, in the last few years, the rise of social networks has turned many common web users into actual content producers wanting to distribute their creations on the Internet. Such users have no skills to protect and distribute their contents, and so they have to resort to specific web entities to implement such functions. They are not different from professional content producers that do not want to directly protect and/or distribute their contents. As a consequence, watermarking protocols have to be designed so as to enable such new categories of content providers to outsource the burdensome activities of digital content protection and distribution according to the new web service models characterizing the current Internet. In fact, the need to involve web entities different from buyers and content providers, such as, for example, cloud computing platforms, poses further security problems for watermarking protocols, since such entities have to be considered "honest-but-curious", with all that this entails [10–14].

2.1.3. Multiple Negotiation Problem

Web users usually purchase goods online without having to disclose their identities. All that matters is that buyers can pay what they purchase. On the contrary, copyright protection systems need to unambiguously link buyers to the contents they purchase, since, as reported in Section 1, they have to track down the infringers once illegal copies of contents have been found in the market. However, web users wish to remain anonymous during purchases. They fear that content providers may gather sensitive data about buyers and may benefit from reselling those data to other parties which can misuse it. As a consequence, to reach a good compromise between anonymity and tracing, most watermarking protocols implement identification systems based on anonymous digital certificates issued by certification authorities (CAs) [8]. However, such systems are usually considered acceptable to web users residing within geographical areas such as Western Europe, the USA and Japan, but they cannot be adopted outside these areas, where the spread of digital certificates is still rather limited.

The considerations reported above suggest that watermarking protocols have to support multiple negotiation mechanisms so as not to force buyers to adhere to a unique and rigid identification method when they want to buy digital contents [15]. Such mechanisms can also identify the buyers by exploiting the information normally used to purchase digital

contents, such as credit card numbers, since a credit card is always associated with a unique identity. The ultimate goal is to make the purchase of copyrighted contents as similar as possible to the purchase of any other good online.

2.2. Security Requirements

The security requirements are needed to design watermarking protocols able to resist increasingly dangerous attacks. However, the search for security has led to less usable and complex protocols, which, for example, often involve trusted third parties (TTPs) acting as watermark certification authorities (WCAs) [8] to manage the implemented protection schemes. As a consequence, the key challenge in designing modern watermarking protocols consists of finding the right balance between conflicting requirements, such as simplicity and usability on the one hand and security on the other hand.

2.2.1. Piracy Tracing Problem

As reported in Section 1, the deterrent action characterizing watermarking protocols strictly depends on their capacity to correctly track down copyright infringers starting from copies of contents illegally owned or shared by web users. More precisely, when such a copy is found in the market, a watermarking protocol should make it possible to trace it back to the user who initially purchased the original content and then illegally shared the copy on the Internet. In this regard, the protocol should be based on a protection scheme that permits gathering undeniable proof against the infringer so as to prevent any form of repudiation [8,9].

2.2.2. Customer's Right Problem

This problem arises when a content provider can have access to the final form of a protected digital content sold to a buyer. In this case, the content provider can fabricate piracy to frame the innocent and unwitting buyer, since they can make and distribute a copy of the digital content purchased by the buyer and then accuse the buyer of illegal distribution [8].

2.2.3. Unbinding Problem

This problem occurs whenever a watermarking protocol does not implement mechanisms to uniquely bind a given watermark identifying a buyer to both the purchased digital content and the corresponding purchase transaction. In this case, a dishonest content provider can frame the buyer by transplanting his/her watermark into a copy of higher priced digital content that the buyer never bought in order to obtain a compensatory payment. A similar situation may also occur when a content provider can, more simply, know the watermark embedded in a digital content purchased by a buyer. This fact enables the content provider to insert the same watermark into further copies of the content bought by the buyer so as to unjustly accuse him/her of illegal distribution [8].

2.2.4. Dispute Resolution Problem

The dispute resolution protocol is a sub-protocol of watermarking protocols. It is run by the content provider whenever a pirated copy of a copyrighted content is found in the market. Its task is to identify the "traitor", that is, the buyer who distributed illegal replicas of the protected content. In this regard, it is worth noting that, in the general practice of law, it is the accuser who has to prove the guilt of the defendant, not the reverse. Therefore, the sub-protocol should provide the content provider with the evidence necessary to make appropriate adjudications without involving the suspected buyer, and this is because of two main reasons: the first is that a suspected buyer is very unlikely to cooperate since he/she is presumed innocent until proved guilty; the second is that a malicious content provider could easily harass an innocent buyer by repeatedly requiring cooperation [8].

2.2.5. Conspiracy Problem

As reported above, many watermarking protocols need TTPs to ensure the correct execution of the protection scheme. However, the presence of a TTP may cause conspiracy or collusion problems. More specifically, a TTP, particularly if it is a WCA, might behave dishonestly and collude (1) with a fraudulent content provider or (2) with a malicious buyer to fabricate piracy. In the former case, the collusion could cause the same effects of the unbinding problem or the customer's right problem. In the latter case, the buyer could remove or partially corrupt the watermark embedded into the purchased content, thus cheating the tracing mechanism implemented by the watermarking protocol [16].

Even though the watermarking protocols that do without TTPs appear to be more secure [13,14,17], they are often affected by usability problems. Indeed, the absence of TTPs ends up complicating the participation of buyers in the protocols, forcing buyers to carry out complex actions.

2.2.6. Ambiguity Problem

To solve the problems reported above, a number of watermarking protocols need a double watermark insertion carried out by distinct web entities, such as, for example, content providers and WCAs. Such solutions, however, may give rise to a further problem caused by the fact that, when embedded independently, the second watermark insertion can impair the previously inserted watermark, thus discrediting its authority. In addition to confusing the copyright information embedded in digital contents, a double watermark insertion may also impair the final quality of the protected contents, thus reducing their commercial value. As a consequence, a double watermark insertion ends up behaving as an "ambiguity attack" on watermarks, and this strongly reduces the security performance of protocols [18,19].

3. Security Primitives

The watermarking protocols documented in the literature exploit a wide variety of security primitives. However, the focus is on the primitives used in "buyer and seller" watermarking protocols based on the "asymmetric fingerprinting" protection scheme [7,8,20]. According to such a scheme, the buyer and seller can jointly protect digital content in such a way that only the buyer receives the final version of the content watermarked by using a fingerprint that unambiguously binds the buyer, the content, and the purchase transaction. As a consequence, if a copy of the protected content is illegally distributed and found in the market, the seller can run a proper dispute resolution protocol to prove the guilt of the buyer. Moreover, asymmetric fingerprinting schemes can also involve TTPs, which usually assist buyers in performing the most complex actions required by joint protections.

Accordingly, the basic primitives employed in the asymmetric fingerprinting schemes are presented in the following. They are described also in relation to the goals that they make it possible to achieve. In fact, their knowledge can be considered sufficient to understand the basics to design modern watermarking protocols.

3.1. Zero-Knowledge Proof

Zero-knowledge proof of knowledge is a basic technique that can be used by a party, called the "prover", to prove to another party, called the "verifier", that a given statement is true without providing any additional information besides the fact that the statement is indeed true [21]. This technique results in a two-party protocol involving a prover and a verifier. The protocol enables the prover to prove to the verifier knowledge of a secret about a statement without disclosing anything about the secret to the verifier. This also means that a prover without the knowledge of the secret can convince the verifier with negligible probability. Moreover, the verifier cannot learn any information about the secret during the execution of the protocol.

More formally, the notation

$$\mathsf{PK}\{(x) : y = f(x)\}$$

represents a zero-knowledge proof of knowledge of the secret x such that $y = f(x)$. In particular, in the notation, the letter x in round brackets represents the secret, whereas the result y and the function f are known to the verifier [22].

Zero-knowledge proof of knowledge has found many applications in watermarking protocols. One of the most frequent uses concerns the verification of public–private key pairs in public key infrastructures (PKIs). For example, the notation

$$\mathsf{PK}\{(sk') : (pk', sk') \leftarrow C \leftarrow \mathsf{Enc}(pk, sk')\}$$

denotes a proof that C is the encryption of the secret key sk', corresponding to the public key pk', carried out using the public key pk and the encryption algorithm Enc. As a consequence, a party who possesses the secret key sk, corresponding to pk, can retrieve sk' from C. In this regard, to instantiate the proof, the encryption algorithms described in [23,24] can be used.

Other relevant uses of zero-knowledge proof of knowledge concern the need to prove that a content is the encrypted version of a binary string usually representing a fingerprint or watermark information. For example, the notation

$$\mathsf{PK}\{(b) : C \leftarrow \mathsf{Enc}(pk, b) \wedge b \in \{0, 1\}\}$$

denotes the proof that C is the encrypted version of the bit b under the public key pk [25].

Zero-knowledge proofs of knowledge can be considered very useful for watermarking protocols since they make it possible to convince a party of something without revealing any secret information. However, they force the prover and the verifier to execute complex protocols. Therefore, according to what is reported in Section 2.1.1, these two specific roles should never be assigned to the buyers, whose involvement should be as simplified as possible. In fact, protocols such as the one proposed in [26] are characterized by security schemes that are simple but impractical in the current web context.

3.2. Homomorphic Encryption

Homomorphic encryption is defined as follows. Let $\mathcal{M}$ be a set of plaintexts, and let $\mathcal{C}$ be a set of ciphertexts corresponding to $\mathcal{M}$. An encryption scheme E is said to be *homomorphic* if it satisfies the following condition for any encryption key k:

$$\forall m_1, m_2 \in \mathcal{M}, \quad E(m_1 \odot_{\mathcal{M}} m_2) \leftarrow E(m_1) \odot_{\mathcal{C}} (m_2)$$

where $\odot_{\mathcal{M}}$ and $\odot_{\mathcal{C}}$ denote some operators in $\mathcal{M}$ and in $\mathcal{C}$, respectively, and $\leftarrow$ means "can be directly computed from", that is, without any intermediate decryption [27].

The homomorphic encryption schemes used in watermarking protocols usually assume that both content and watermark can be represented in a block-wise form, $X = \{x_1, x_2, \ldots x_l\}$ and $W = \{w_1, w_2, \ldots w_t\}$, respectively. In particular, the elements of X can be either the original host signal samples or the features of the host signal computed by transforms such as, for instance, the discrete Fourier transform or the discrete cosine transform (DCT). The elements of W are usually binary values representing a fingerprinting anti-collusion code [5,28–31].

The watermarking protocols also assume that the encryption is a block-wise function E so that the encryption of a content $X = \{x_1, x_2 \ldots x_l\}$ under the key k can be calculated as [7,8]:

$$E_k(X) = E_k(x_1, x_2 \ldots x_l) = (E_k(x_1), E_k(x_2) \ldots E_k(x_l))$$

Likewise, they assume that watermark insertion can be expressed in the form:

$$X \oplus W = \{x_1 \oplus w_1, x_2 \oplus w_2, \ldots x_l \oplus w_l\} = \bar{X}$$

in which the symbol $\oplus$ represents, in principle, an arbitrary function [4]. However, in practice, it is sufficient to consider only the asymmetric homomorphic encryption schemes that support addition and multiplication operations since such operations are functionally complete sets over finite sets [32]. In addition, such schemes also have to be "probabilistic" and "semantically secure". This ensures that the knowledge of a ciphertext does not provide any useful information on the plaintext to an adversary having only a reasonably restricted computational power represented by polynomial resources [27,32].

The result is, therefore, represented by the so-called multiplicatively and additively homomorphic encryption schemes. The former ensure that [33]

$$\forall m_1, m_2 \in \mathcal{M}, \quad E(m_1 \cdot m_2) = E(m_1) \cdot E(m_2)$$

whereas the latter ensure that [34,35]

$$\forall m_1, m_2 \in \mathcal{M}, \quad E(m_1 + m_2) = E(m_1) \cdot E(m_2)$$

Such schemes can be used to apply a watermark, for a fixed key k, according to the following expression:

$$E_k(X \oplus W) = E_k(X) \oplus E_k(W) = E_k(\bar{X})$$

Homomorphic encryption schemes have changed the way watermarking protocols are designed. They have been used to prevent content providers from having exclusive rights on their contents sold to buyers since, in the early watermarking protocols, content providers took charge of embedding watermarks into the distributed contents. On the contrary, homomorphic encryption schemes enable all the parties involved in the protocols to directly operate on the encrypted contents. More precisely, performing operations on the plaintexts before encryption is equivalent, for a fixed key, to carrying out operations on the corresponding ciphertexts after encryption.

For example, consider the watermark insertion algorithm based on the spread spectrum technique described in [4] and represented by the formula:

$$\bar{x} = x + \alpha(2b - 1)s$$

where x is a host signal feature obtained by calculating the cosine discrete transform (DCT), $\bar{x}$ is the corresponding watermarked feature, $b \in \{0, 1\}$ is the bit to embed, s is the component of a spreading sequence, and α is a scaling factor that controls the watermark's strength. The watermark insertion can be directly carried out into the encrypted domain by exploiting an additively homomorphic cryptosystem, thus obtaining [36,37]

$$E[\bar{x}] = E[x] \cdot E[b]^{2\alpha s} \cdot E[\alpha s]^{-1} \tag{1}$$

Homomorphic encryption can also be applied to the class of data hiding schemes defined as "informed embedding". Such schemes hide signal-dependent watermarks using as embedding rules the quantization of some content features. For example, consider a watermark insertion based on quantization index modulation (QIM) [38]. It is carried out according to the following expression [37]:

$$\bar{x} = f(x) + b\Delta(x)$$

where x, $\bar{x}$, and b maintain the signification reported above, while $f(x)$ and $\Delta(x)$ denote a function of the original signal features and a signal-dependent quantization step, respectively. In particular, $f(x)$ and $\Delta(x)$ can be expressed as:

$$f(x) = Q^{2\Delta}_{\delta,0}(x) \qquad \Delta(x) = \Delta \cdot sgn(x - Q^{2\Delta}_{\delta,0}(x))$$

where

$$Q^{\Delta}_{\delta,0}(x) = arg \min_{u_{0,k} \in U^{\Delta}_{\delta,0}} |u_{0,k} - x| \qquad \text{and} \qquad sgn(x) = x/|x|$$

In particular, Q is a quantizer associated with the following codebook:

$$U^{\Delta}_{\delta,0} = \{u_{0,k}\} = \{k\Delta + \delta,\ k \in \mathbb{Z}\}$$

where Δ is the quantization step and δ is the dithering value. In fact, both parameters are specific to a binary dither modulation with uniform scalar quantizers, such as the QIM modulation [38].

By directly operating in the encrypted domain and by assuming an additively homomorphic cryptosystem, the watermark insertion based on QIM can be obtained by applying the following expression [37,39,40]:

$$E[\bar{x}] = E[f(x)] \cdot E[b]^{\Delta(x)} \tag{2}$$

The two examples reported above show that homomorphic encryption results in a kind of commutativity between encryption and some data-processing operations, such as those concerning watermark insertions. This makes it possible to decouple content encryption from watermark insertion: a party involved in a watermarking protocol can receive an encrypted watermark and can directly insert it into an encrypted content without knowing anything about it. Such a property is crucial in the development of protocols able to meet the security requirements reported in the previous sections.

3.3. Commutative Encryption

An encryption scheme E is *commutative* if it satisfies the following properties [41–44]:

$$E_{k_1}(E_{k_2}(m)) = E_{k_2}(E_{k_1}(m)) \quad \text{and} \quad D_{k_1}(D_{k_2}(E_{k_1}(E_{k_2}(m)))) = m$$

with D representing the decryption function corresponding to E for any two keys k_1 and k_2 and any message m.

The above properties mean that a message m can be encrypted more than once using different public keys; that is, there is no need to decrypt m before re-encrypting it. Moreover, m can be recovered from the corresponding ciphertext without having to take into account the order of the public keys used in encrypting it. More precisely, m can be decrypted by applying the private keys in any order. In practice, the results achieved by applying a commutative encryption scheme are not affected by the order of keys used in encryption and in decryption.

The properties of commutative encryption schemes can be very useful to implement a wide variety of applications [45–49]. However, they are particularly suitable for watermarking protocols that enable content providers to exploit "security delegates", such as cloud computing platforms, to apply protections to digital contents distributed on the Internet [10,11]. In such cases, the protection schemes are based on double encryption. More in detail, content providers apply a first encryption to their digital contents so as to release them in a protected form to cloud platforms. Then, cloud platforms can re-encrypt the received contents without having to first decrypt them. At this point, it is possible to embed watermarks directly into the encrypted domain even in the presence of a double encryption, thus supporting the protection schemes based on security intermediaries [50–52].

3.4. Joint Watermarking

Joint watermarking proposes a different approach to designing watermarking protocols. Its main aim is to distribute the computing load to protect contents among buyers and content providers. It operates in two phases. The former enables a content provider to encrypt multimedia digital content by heavily distorting some of its perceptually significant parts. In particular, distortion is obtained by adding a specific noise signal to the

content. The latter enables a buyer to decrypt such content by partially removing the noise signal added to it, thus introducing changes in the content, which can be considered as a detectable watermark.

A significant example of joint watermarking based on the spread spectrum embedding technique is described in [53,54]. The example shows how a content X can be encrypted and distributed to N buyers by employing a long-term master encryption look-up table (LUT) $\mathbf{E}$ whose size is T. The entries of $\mathbf{E}$ are denoted as $\mathbf{E}(0)$, $\mathbf{E}(1), \ldots,$ $\mathbf{E}(T-1)$, and represent independent and identically distributed (i.i.d.) random variables characterized by a Gaussian distribution with variance σ_E^2. In particular, to encrypt the copy of X for the k-th buyer, the content provider has to generate two LUTs, denoted as $\mathbf{W}_k$ and $\mathbf{D}_k$, personalized for that buyer. The former represents a watermark LUT whose entries are i.i.d. random variables following a Gaussian distribution with variance σ_W^2. The latter represents the personalized decryption LUT built by combining componentwise the encryption and watermark LUTs according to the following expression:

$$\mathbf{D}_k(t) = -\mathbf{E}(t) + \mathbf{W}_k(t)$$

for $t = 0, 1, \ldots, T-1$.

Then, the content provider creates a content-dependent key, denoted as sk_X, and encrypts X by applying the following procedure. Firstly, it uses sk_X to generate a set of pseudo-random $M \times R$ values in the range $[0; T-1]$, each denoted as t_{ih} and with $0 \leq i \leq M-1$ and $0 \leq h \leq R-1$. Then, M significant content features of X, each denoted as x_i, are encrypted by employing the encryption LUT $\mathbf{E}$. In particular, the encrypted value of x_i, denoted as c_i, is obtained by adding R entries of $\mathbf{E}$ identified by the indexes $(t_{i0}, \ldots, t_{i(R-1)})$ included in the set of $M \times R$ values according to the following expression:

$$c_i = x_i + \sum_{h=0}^{R-1} \mathbf{E}(t_{ih}) \tag{3}$$

Once encryption of X is completed, the content can be sent to the N buyers together with the key sk_X. Moreover, each buyer also receives the personalized decryption LUT. This means that the k-th buyer receives $\mathbf{D}_k$ for $k = 1, 2, \ldots, N$.

Joint watermarking is carried out by each of the N buyers in two phases: in the former, the k-th buyer has to reconstruct the same sequence of indexes t_{ih} by employing the content-dependent key sk_X; in the latter, the k-th buyer adds R entries of the decryption LUT $\mathbf{D}_k$ to each encrypted feature c_i according to the following expression, thus obtaining the decrypted and watermarked content feature $y_{k,i}$ corresponding to x_i:

$$y_{k,i} = c_i + \sum_{h=0}^{R-1} \mathbf{D}_k(t_{ih}) = x_i + \sum_{h=0}^{R-1} \mathbf{W}_k(t_{ih}) = x_i + w_{k,i} \tag{4}$$

$w_{k,i}$ represents the i-th watermark component of the k-th copy of X. It is calculated as the sum of the R entries of the k-th watermark LUT $\mathbf{W}_k$. As a result, the k-th buyer can receive a personalized watermarked copy of X, denoted as $Y_k = X + W_k$.

Joint watermarking is characterized by computational simplicity since it makes it possible, in the first instance, to watermark digital content without resorting to complex homomorphic public-key encryption operations. However, its use in watermarking protocols has to be accompanied by specific solutions to solve the following problem: the content-dependent keys and personalized decryption LUTs are both created and distributed by content providers, which end up fully controlling the protocols. In fact, this prevents protocols from matching some of the requirements reported in the previous sections. In this regard, the solutions proposed in the literature, such as, for example, those described in [55,56], implement specific variants in order to enable the generation of the personalized decryption LUTs in such a way that content providers cannot know or access them. Such a result is achieved by applying the following procedure.

Firstly, proper watermarking LUTs $\mathbf{W}_k$ are generated by buyers or TTPs in the form $\mathbf{W}_k = \mathbb{G}\mathbf{m}_k$, where $\mathbf{m}_k$ is obtained by coding the L-bit fingerprint identifying the k-th buyer using a binary antipodal modulation, while $\mathbb{G}$ represents a generator matrix of a linear block code over the set of real numbers [57,58].

The personalized watermarking LUTs $\mathbf{W}_k$ are then encrypted using an additively homomorphic cryptosystem, thus obtaining

$$[|\mathbf{W}_k(t)|] = [|\mathbb{G}\mathbf{m}_k(t)|] = \prod_{l=0}^{L-1} [|\mathbf{m}_{k,l}|]^{\mathbb{G}(t,l)}$$

where homomorphic encryption is denoted as $[|\ \ |]$. The encrypted LUTs are sent to the content provider, which can generate the personalized decryption LUTs $\mathbf{D}_k$ by exploiting the same homomorphic cryptosystem since all the operations to be performed are linear. Therefore, each entry of the decryption LUT $\mathbf{D}_k$ can be calculated directly into the encrypted domain as follows:

$$[|\mathbf{D}_k(t)|] = [|\mathbf{E}_k(t)|]^{-1} \prod_{l=0}^{L-1} [|\mathbf{m}_{k,l}|]^{\mathbb{G}(t,l)}$$

Once the personalized encrypted LUT $[|\mathbf{D}_k|]$ is received, the k-th buyer can perform the decryption, thus obtaining

$$\mathbf{D}_k = -\mathbf{E}_k + \mathbb{G}\mathbf{m}_k$$

The k-th buyer can therefore use $\mathbf{D}_k$ to operate the joint watermarking on the previously received encrypted version of X and obtain the personalized, final watermarked copy of X, which is unknown to the content provider.

4. Performance Issues

The requirements listed in Section 2 provide researchers with a guide to designing watermarking protocols able to protect the copyrights of digital content distributed on the web. The protocols are implemented as web applications that embed personalized protections into distributed content [1], as reported in Section 1. This means that protections are applied "on-the-fly" when contents are purchased by buyers (see Figures 1 and 2). Therefore, such applications have to be run by systems provided with adequate resources if they want to implement competitive, real-time services in the current web context.

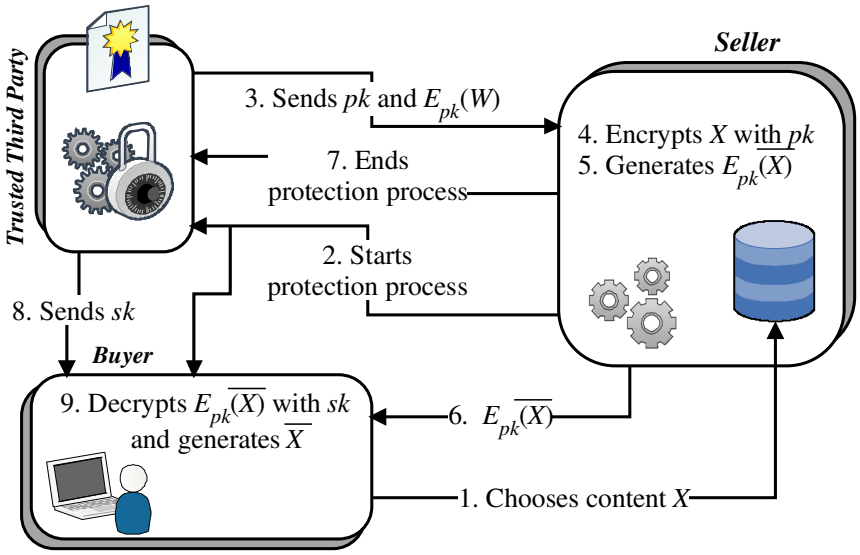

Figure 1. Buyer and seller watermarking protocol based on asymmetric fingerprinting and homomorphic encryption.

More precisely, the computing and memory resources needed to implement a watermarking protocol determine its efficiency and scalability; the former mainly depends on the processing time taken to protect content, whereas the latter depends on how such a time increase is related to the increment in the number of the buyers purchasing content.

Efficiency should be maximized so as to achieve a near-linear growth of scalability. In this regard, it is worth noting that, in past years, searching for secure watermarking protocols led researchers to design protection schemes mainly based on homomorphic primitives (see Figures 1 and 2). This resulted in rather inefficient protocols, since homomorphic primitives require that each sample of protected content is individually encrypted. In fact, the public-key individual encryption of samples causes a high computing overhead as well as an expansion of data, which also has a specific impact on communication bandwidth.

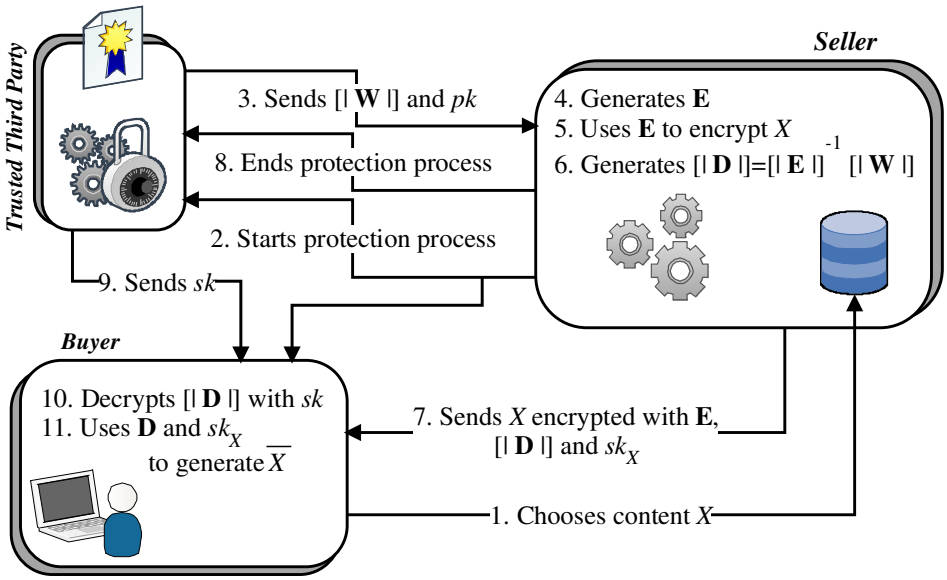

Figure 2. Buyer and seller watermarking protocol based on asymmetric fingerprinting and joint watermarking.

The performance problems caused by homomorphic public-key encryption algorithms particularly affect watermarking protocols based on the interaction scheme shown in Figure 1, in which sellers implement the most resource-intensive and time-consuming operations.

For example, consider the tests conducted in [26,59] on images of 1024 × 1024 pixels. Each image is watermarked by applying the QIM algorithm reported in Section 3.2. The watermarked features are extracted by the lowest frequency DCT coefficients, excluding the DC value, of the 8 × 8 DCT blocks composing the images. The embedded watermarks are 128-bit strings. Each image is encrypted using the Paillier cryptosystem with a public key size of 1024 bits [35]. Therefore, in an image of 1024 × 1024 pixels, the size of the host signal is 1,048,576 DCT coefficients. This means that the Paillier cryptosystem requires 1,048,576 multiplication exponentiations on a 2048 bit group to protect an image according to the expression (2). However, by adopting the optimization strategy called "composite-embedding strategy" [26,59], it is possible to group several signal features into a single 2048-bit group and to perform basic linear operations on them. As a consequence, the number of multiplication exponentiations can be reduced by a factor of about 100 in the tests documented in [26,59].

Under the above assumptions, let T^1_{sel} denote the computing time spent by the seller to protect a digital content. Let T^1_{buy} denote the computing time spent by the buyer to obtain the same content in its final protected form. According to the scheme in Figure 1, the total computation cost T^1_{total} needed to protect a content can be expressed as $T^1_{total} \approx T^1_{sel} + T^1_{buy}$ since it can be approximated by the sum of three main contributions corresponding to the phases 4, 5, and 9 indicated in Figure 1. These phases consist of public key encryption,

watermark insertion, and public key decryption. In fact, the remaining computation costs to complete content protection can be ignored since they are related to operations on short bit strings [26,59]. Therefore, the tests mentioned above show that the major contribution is T^1_{sel} (phases 4 and 5 in Figure 1) and is less than 2 min on an Intel Core 2 Quad CPU at 2.40 GHz, used as a single processor. The remaining contribution T^1_{buy} (phase 9 in Figure 1) is about 30 s on the same computing system.

The results achieved by the QIM watermarking algorithm are essentially similar to those obtained by the spread spectrum watermarking algorithm since the two expressions (1) and (2) require a similar number of multiplication exponentiations in the case of the use of the same homomorphic cryptosystem.

On the contrary, a scheme based on joint watermarking requires a reduced computational load. In the tests documented in [53,60,61], images of 1024×1024 pixels were watermarked by applying the expressions (3) and (4). The watermarked features were extracted by choosing 4 frequency DCT coefficients, excluding the DC value, from the 8×8 DCT blocks composing the images. This results in $M = 2^{16}$ content features to watermark. In all experiments, the LUT size was set to $T = 2^{16}$, and $R = 4$ LUT entries were added to encrypt each content feature. The embedded watermarks were 128-bit strings.

Under the above assumptions, the total computation cost T^2_{total} can be approximated by the sum of two similar contributions, denoted as T^2_{sel} and T^2_{buy}, respectively: the former corresponds to the evaluation of (3), whereas the latter corresponds to the evaluation of (3). This is because the remaining computation costs concern the generation of LUTs, which are long-term encryption/decryption tables used to protect a single content distributed to multiple buyers (see Section 3.4). Therefore, $T^2_{total} \approx T^2_{sel} + T^2_{buy}$ is about 9 s on an Intel Core 2 Quad CPU at 2.40 GHz used as a single processor. Moreover, T^2_{total} is split between the buyer and seller.

The experiences documented above show that the protection schemes based on homomorphic encryption perform worse than joint-watermarking-based schemes since they require heavy multiplication exponentiations. On the contrary, the schemes based on joint watermarking mostly require sums. Moreover, they make it possible to distribute the computational costs of the protocols between buyers and sellers, thus improving scalability.

5. Conclusions

Buyer and seller watermarking protocols based on asymmetric fingerprinting have proven to be effective tools to protect digital copyright. They are mainly based on the primitives documented in Section 3, which can be assumed to be building blocks to design secure interaction schemes able to meet the requirements reported in Section 2. However, such primitives are often characterized by high computational costs, which make their use in the current web context rather difficult.

On the other hand, attempts to develop watermarking protocols that do not use the primitives described above have often resulted in solutions that are not able to achieve sufficient levels of usability and security. As a consequence, a first key challenge in the next few years consists of designing new and more efficient homomorphic encryption schemes since such new schemes can increase the efficiency of buyer and seller watermarking protocols based on asymmetric fingerprinting, which remain the most promising solutions to the problem of digital copyright protection.

Funding: This research received no external funding.

Data Availability Statement: Not applicable.

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

Abbreviations

The following abbreviations are used in this manuscript:

DRM	Digital Rights Management
TTP	Trusted Third Party
CA	Certification Authority
WCA	Watermark Certification Authority
LUT	Look-Up Table
DCT	Cosine Discrete Transform
QIM	Quantization Index Modulation

References

1. Frattolillo, F.; Landolfi, F. Designing a DRM System. In Proceedings of the 4th International Conference on Information Assurance and Security, Naples, Italy, 8–10 September 2008; pp. 221–226.
2. Zhang, Z.; Pei, Q.; Ma, J.; Yang, L. Security and Trust in Digital Rights Management: A Survey. *Int. J. Netw. Secur.* **2009**, *9*, 247–263.
3. Srinivas, T.; Narasimha, V.; Puroshothammam, M. Survey on design challenges and analysis of service architecture of DRM. In Proceedings of the 2017 International Conference on Trends in Electronics and Informatics, Tirunelveli, India, 11–12 May 2017; pp. 682–686. [CrossRef]
4. Cox, I.; Miller, M.; Bloom, J.; Fridrich, J.; Kalker, T. *Digital Watermarking and Steganography*; Morgan Kaufmann: Burlington, MA, USA, 2007.
5. Liu, K.J.R.; Trappe, W.; Wang, Z.J.; Wu, M.; Zhao, H. *Multimedia Fingerprinting Forensics for Traitor Tracing*; Hindawi Publishing Corporation: New York, NY, USA, 2005.
6. Gopalakrishnan, K.; Memon, N.; Vora, P.L. Protocols for watermark verification. *IEEE Multimed.* **2001**, *8*, 66–70. [CrossRef] [PubMed]
7. Memon, N.; Wong, P.W. A buyer-seller watermarking protocol. *IEEE Trans. Image Process.* **2001**, *10*, 643–649. [CrossRef]
8. Lei, C.L.; Yu, P.L.; Tsai, P.L.; Chan, M.H. An Efficient and Anonymous Buyer-Seller Watermarking Protocol. *IEEE Trans. Image Process.* **2004**, *13*, 1618–1626. [CrossRef] [PubMed]
9. Frattolillo, F. Watermarking protocols: An excursus to motivate a new approach. *Int. J. Inf. Secur.* **2018**, *17*, 587–601. [CrossRef]
10. Frattolillo, F. A multiparty watermarking protocol for cloud environments. *J. Inf. Secur. Appl.* **2019**, *47*, 246–257. [CrossRef]
11. Frattolillo, F. Blockchain and Cloud to Overcome the Problems of Buyer and Seller Watermarking Protocols. *Appl. Sci.* **2021**, *11*, 12028. [CrossRef]
12. Dong, X.; Zhang, W.; Hu, X.; Liu, K. A Cloud-User Watermarking Protocol Protecting the Right to Be Forgotten for the Outsourced Plain Images. *Int. J. Digit. Crime Forensics* **2018**, *10*, 118–139. [CrossRef]
13. Kumar, A. A cloud-based buyer-seller watermarking protocol (CB-BSWP) using semi–trusted third party for copy deterrence and privacy preserving. *Multimed. Tools Appl.* **2022**, *81*, 21417–21448. [CrossRef]
14. Kumar, A.; Kumar, M.; Verma, S.; Kavita.; Jhanjhi, N.; Ghoniem, R. Vbswp-CeaH: Vigorous Buyer-Seller Watermarking Protocol without Trusted Certificate Authority for Copyright Protection in Cloud Environment through Additive Homomorphism. *Symmetry* **2022**, *14*, 2441. [CrossRef]
15. Rannenberg, K.; Royer, D.; Deuker, A. *The Future of Identity in the Information Society—Challenges and Opportunities*; Springer: Berlin, Germany, 2009.
16. Barni, M.; Bartolini, F. Data Hiding for Fighting Piracy. *IEEE Signal Process. Mag.* **2004**, *21*, 28–39. [CrossRef]
17. Song, C.; Wang, H.; Zhang, W.; Sudirman, S.; Zhu, H. A Blockchain Based Buyer-seller Watermark Protocol with Trustless Third Party. *Recent Adv. Electr. Electron. Eng.* **2020**, *13*, 942–950. [CrossRef]
18. Hartung, F.; Su, J.K.; Girod, B. Spread Spectrum Watermarking: Malicious Attacks and Counterattacks. In *Security and Watermarking of Multimedia Contents, Proceedings of the Electronic Imaging '99, San Jose, CA, USA, 23–29 January 1999*; Delp, E.J., Wong, P.W., Eds.; SPIE: Bellingham WA, USA, 1999; Volume 3657, pp. 147–158.
19. Katzenbeisser, S.; Veith, H. Securing Symmetric Watermarking Schemes Against Protocol Attacks. In *Security and Watermarking of Multimedia Contents IV, Proceedings of the Electronic Imaging, 2002, San Jose, CA, USA, 19–25 January 2002*; Delp, E.J., Wong, P.W., Eds.; SPIE: Bellingham WA, USA, 2002; Volume 4675, pp. 260–268.
20. Pfitzmann, B.; Waidner, M. Anonymous fingerprinting. In *Advances in Cryptology–Eurocrypt '97, Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques, Konstanz, Germany, 11–15 May 1997*; Lecture Notes in Computer Science; Fumy, W., Ed.; Springer: Berlin/Heidelberg, Germany, 1997; Volume 1233, pp. 88–102.
21. Bellare, M.; Goldreich, O. On defining proofs of knowledge. In *Advances in Cryptology—CRYPTO' 92, Proceedings of the 12th Annual International Cryptology Conference, Santa Barbara, CA, USA, 16–20 August 1992*; Lecture Notes in Computer Science; Brickell, E.F., Ed.; Springer: Berlin/Heidelberg, Germany, 1992; Volume 740, pp. 390–420.
22. Camenisch, J.; Stadler, M. *Proof Systems for General Statements about Discrete Logarithms*; Technical Report TR 260; Institute for Theoretical Computer Science, ETH: Zurich, Switzerland, 1997.

23. Poupard, G.; Stern, J. Fair Encryption of RSA Keys. In *Advances in Cryptology—EUROCRYPT 2000, Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques, Bruges, Belgium, 14–18 May 2000*; Lecture Notes in Computer Science; Preneel, B., Ed.; Springer: Berlin/Heidelberg, Germany, 2000; Volume 1807, pp. 172–189.
24. Camenisch, J.; Shoup, V. Practical verifiable encryption and decryption of discrete logarithms. In *Advances in Cryptology—CRYPTO 2003, Proceedings of the Annual International Cryptology Conference, Santa Barbara, CA, USA, 17–21 August 2003*; Lecture Notes in Computer Science; Boneh, D., Ed.; Springer: Berlin/Heidelberg, Germany, 2003; Volume 2729, pp. 126–144.
25. Damgård, I.; Jurik, M. A generalisation, a simplification and some applications of Paillier's probabilistic public-key system. In *Public Key Cryptography, Proceedings of the 4th International Workshop on Practice and Theory in Public Key Cryptography, Cheju Island, Republic of Korea, 13–15 February 2001*; Lecture Notes in Computer Science; Kim, K., Ed.; Springer: Berlin/Heidelberg, Germany, 2001; Volume 1992, pp. 119–136.
26. Rial, A.; Deng, M.; Bianchi, T.; Piva, A.; Preneel, B. A Provably Secure Anonymous Buyer—Seller Watermarking Protocol. *IEEE Trans. Inf. Forensics Secur.* **2010**, *5*, 920–931. [CrossRef]
27. Fontaine, C.; Galand, F. A Survey of Homomorphic Encryption for Nonspecialists. *Eurasip J. Inf. Secur.* **2007**, *2007*, 013801. [CrossRef]
28. Boneh, D.; Shaw, J. Collusion-secure fingerprinting for digital data. *IEEE Trans. Inf. Theory* **1998**, *44*, 1897–1905. [CrossRef]
29. Trappe, W.; Wu, M.; Wang, Z.J.; Liu, K.J.R. Anti-collusion fingerprinting for multimedia. *IEEE Trans. Signal Process.* **2003**, *41*, 1069–1087. [CrossRef]
30. Zhao, H.V.; Liu, K.J.R. Traitor-Within-Traitor Behavior Forensics: Strategy and Risk Minimization. *IEEE Trans. Inf. Forensics Secur.* **2006**, *1*, 440–456. [CrossRef]
31. Pehlivanoglu, S. An Asymmetric Fingerprinting Code for Collusion-resistant Buyer-seller Watermarking. In *IH&MMSec '13: Proceedings of the First ACM Workshop on Information Hiding and Multimedia Security, Proceedings of the 1st ACM Workshop on Information Hiding and Multimedia Security, Montpellier, France, 17–19 June 2013*; Association for Computing Machinery: New York, NY, USA, 2013; pp. 35–44.
32. Acar, A.; Aksu, H.; Uluagac, A.S.; Conti, M. A Survey on Homomorphic Encryption Schemes: Theory and Implementation. *ACM Comput. Surv.* **2019**, *51*, 79. [CrossRef]
33. ElGamal, T. A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. *IEEE Trans. Inf. Theory* **1985**, *31*, 469–472. [CrossRef]
34. Goldwasser, S.; Micali, S. Probabilistic encryption & how to play mental poker keeping secret all partial information. In Proceedings of the 14th Annual ACM Symposium on Theory of Computing, San Francisco, CA, USA, 5–7 May 1982; pp. 365–377.
35. Paillier, P. Public-key Cryptosystems Based on Composite Degree Residuosity Classes. In *Advances in Cryptology—EUROCRYPT '99, Proceedings of the Eurocrypt '99, International Conference on the Theory and Applications of Cryptographic Techniques, Prague, Czech Republic, 2–6 May 1999*; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 1999; Volume 1592, pp. 223–238.
36. Kuribayashi, M. On the Implementation of Spread Spectrum Fingerprinting in Asymmetric Cryptographic Protocol. *EURASIP J. Info. Security* **2010**, *2010*, 694797. [CrossRef]
37. Bianchi, T.; Piva, A. Secure Watermarking for Multimedia Content Protection: A Review of its Benefits and Open Issues. *IEEE Signal Process. Mag.* **2013**, *30*, 87–96. [CrossRef]
38. Chen, B.; Wornell, G. Quantization index modulation: A class of provably good methods for digital watermarking and information embedding. *IEEE Trans. Inf. Theory* **2001**, *47*, 1423–1443. [CrossRef]
39. Kuribayashy, M.; Tanaka, H. Fingerprinting Protocol for Images Based on Additive Homomorphic Property. *IEEE Trans. Image Process.* **2005**, *14*, 2129–2139. [CrossRef]
40. Prins, J.P.; Erkin, Z.; Lagendijk, R.L. Anonymous fingerprinting with robust QIM watermarking techniques. *EURASIP J. Inf. Secur.* **2007**, *2007*, 031340. [CrossRef]
41. Shamir, A.; Rivest, R.L.; Adleman, L.M. Mental Poker. In *The Mathematical Gardner*; Klarner, D.A., Ed.; Springer: Boston, MA, USA, 1981; pp. 37–43.
42. Zhao, W.; Varadharajan, V.; Mu, Y. A Secure Mental Poker Protocol over the Internet. In Proceedings of the Australasian Information Security Workshop Conference on ACSW Frontiers 2003, Adelaide, Australia, 1 February 2003; pp. 105–109.
43. Huang, K.; Tso, R. A Commutative Encryption Scheme based on ElGamal Encryption. In Proceedings of the International Conference on Information Security and Intelligent Control, Yunlin, Taiwan, 14–16 August 2012; pp. 156–159.
44. Huang, K.; Tso, R.; Chen, Y.C. One-time-commutative public key encryption. In Proceedings of the Computing Conference 2017, London, UK, 18–20 July 2017; pp. 814–818.
45. Samanthula, B.K.; Elmehdwi, Y.; Howser, G.; Madria, S. A secure data sharing and query processing framework via federation of cloud computing. *Inf. Syst.* **2015**, *48*, 196–212. [CrossRef]
46. Shafagh, H.; Hithnawi, A.; Burkhalter, L.; Fischli, P.; Duquennoy, S. Secure sharing of partially homomorphic encrypted IOT data. In Proceedings of the 15th ACM Conference on Embedded Networked Sensor Systems, Delft, The Netherlands, 5–8 November 2017; pp. 1–14.
47. Derler, D.; Ramacher, S.; Slamanig, D. Homomorphic proxy reauthenticators and applications to verifiable multi-user data aggregation. In Proceedings of the International Conference on Financial Cryptography and Data Security, Sliema, Malta, 3–7 April 2017; pp. 124–142.

48. Gao, C.; Cheng, Q.; Li, X.; Xia, S. Cloud-assisted privacy-preserving profile-matching scheme under multiple keys in mobile social network. *Clust. Comput.* **2019**, *22*, 1655–1663. [CrossRef]
49. Yu, B.; Zhang, C.; Li, W. File matching based on secure authentication and proxy homomorphic re-encryption. In Proceedings of the 11th International Conference on Machine Learning and Computing, Zhuhai, China, 22–24 February 2019; pp. 472–476.
50. Choi, J.G.; Sakurai, K.; Park, J.H. Does It Need Trusted Third Party? Design of Buyer-Seller Watermarking Protocol without Trusted Third Party. In *Applied Cryptography and Network Security, Proceedings of the 1st International Conference on Applied Cryptography and Network Security, Kunming, China, 16–19 October 2003*; Lecture Notes in Computer Science; Zhou, J., Yung, M., Han, Y., Eds.; Springer: Berlin/Heidelberg, Germany, 2003; Volume 2846, pp. 265–279.
51. Wang, C.; Leung, H.F.; Cheung, S.C.; Wang, Y. Use of Cryptographic Technologies for Privacy Protection of Watermarks in Internet Retails of Digital Contents. In Proceedings of the 18th International Conference on Advanced Information Networking and Application, Fukuoka, Japan, 29–31 March 2004.
52. Jeng, F.J.; Huang, J.C.; Chen, T.H. An Improved Anonymous Buyer-Reseller Watermarking Protocol. *Int. J. Netw. Secur.* **2016**, *18*, 728–735.
53. Celik, M.U.; Lemma, A.N.; Katzenbeisser, S.; van der Veen, M. Lookup table based secure client-side embedding for spread-spectrum watermarks. *IEEE Trans. Inf. Forensics Secur.* **2008**, *3*, 475–487. [CrossRef]
54. Katzenbeisser, S.; Lemma, A.; Celik, M.U.; van der Veen, M.; Maas, M. A Buyer—Seller Watermarking Protocol Based on Secure Embedding. *IEEE Trans. Inf. Forensics Secur.* **2008**, *3*, 783–786. [CrossRef]
55. Bianchi, T.; Piva, A. TTP-free asymmetric fingerprinting based on client side embedding. *IEEE Trans. Inf. Forensics Secur.* **2014**, *9*, 1557–1568. [CrossRef]
56. Bianchi, T.; Piva, A.; Shullani, D. Anticollusion solutions for asymmetric fingerprinting protocols based on client side embedding. *Eurasip J. Inf. Secur.* **2015**, *2015*, 6. [CrossRef]
57. Marshall, T., Jr. Coding of real-number sequences for error correction: A digital signal processing problem. *IEEE J. Sel. Areas Commun.* **1984**, *2*, 381–392. [CrossRef]
58. Wang, Z.; Giannakis, G.B. Complex-field coding for OFDM over fading wireless channels. *IEEE Trans. Inf. Theory* **2003**, *49*, 707–720. [CrossRef]
59. Deng, M.; Bianchi, T.; Piva, A.; Preneel, B. An efficient buyer-seller watermarking protocol based on composite signal representation. In Proceedings of the 11th ACM Workshop on Multimedia and Security, Princeton, NJ, USA, 7–8 September 2009; pp. 9–18.
60. Celik, M.U.; Lemma, A.N.; Katzenbeisser, S.; van der Veen, M. Secure Embedding of Spread Spectrum Watermarks using Look-up-Tables. In Proceedings of the 2007 IEEE International Conference on Acoustics, Speech and Signal Processing, Honolulu, HI, USA, 15–20 April 2007; Volume 2, pp. II–153–II–156.
61. 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, Florence, Italy, 4–9 May 2014; pp. 3987–3991.