International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:1, No:7, 2007

A Web Oriented Watermarking Protocol

Franco Frattolillo, and Salvatore D'Onofrio

Abstract**—** This paper presents a watermarking protocol able to solve the well-known "customer's right problem" and "unbinding problem". In particular, the protocol has been purposely designed to be adopted in a web context, where users wanting to buy digital contents are usually neither provided with digital certificates issued by certification authorities (CAs) nor able to autonomously perform specific security actions. Furthermore, the protocol enables users to keep their identities unexposed during web transactions as well as allows guilty buyers, i.e. who are responsible distributors of illegal replicas, to be unambiguously identified. Finally, the protocol has been designed so that web content providers (CPs) can exploit copyright protection services supplied by web service providers (SPs) in a security context. Thus, CPs can take advantage of complex services without having to directly implement them.

Keywords**—** Copyright protection, digital rights management, watermarking protocols.

I. Introduction and Motivations

Digital watermarking can be considered one of the main technologies to support the copyright protection of digital contents distributed on the Internet [1], [2], [3]. However, a content protection based on watermarking procedures directly implemented by CPs can be affected by the "customer's right problem" [4], [5]. In fact, the applied protection does not take into account the buyers' rights, since the watermark is autonomously inserted by the copyright owner, i.e. the seller, without any control. Thus, a buyer whose watermark is found in an unauthorized copy cannot be legally prosecuted, since he/she can claim that the unauthorized copy was created and distributed by the seller. Furthermore, if a watermarking procedure fails to provide proper mechanisms on binding a chosen watermark to a specific digital content or a specific transaction, the "unbinding problem" can also arise [6]. This because a malicious seller can intentionally transplant a watermark initially embedded in a copy of certain digital content into another copy of a completely different digital content, provided both copies are sold to the same buyer. Finally, it is worth noting that buyers usually wish to keep their identities unexposed during the web transactions by which they purchase digital contents, and this normally contrasts with the need of the sellers, who often want to identify buyers in order to generate "fingerprinting codes" by which to protect the distributed contents [7], [8], [3].

The literature in this field is rich of proposals that attempt to solve the problems reported above by introducing specific watermarking protocols [4], [5], [9], [10]. At the state of the art, one of the most recent and advanced solutions to the reported problems is devised in [6]. In particular, this solution employs a Public-Key Infrastructure to attain several important achievements that are missing in the previously proposed watermarking protocols. Furthermore, it is also based on resorting to trusted watermark certification authorities (WCAs), which are responsible for ensuring a correct watermarking protocol able to take into account the rights of both buyers and sellers. In fact, such authorities take also charge of carrying out the watermark insertions. However, such a solution requires that buyers are provided with digital certificates issued by CAs as well as are able to perform some security actions, such as the generation of the digital signature of messages. Moreover, it also requires a double watermark insertion performed by distinct web entities involved in the watermarking protocol. Therefore, this solution presents some important drawbacks that can be summarized as follows:

- Buyers wishing to buy goods in the Internet are usually not provided with digital certificates and do not know how they can obtain them from CAs. In addition, they are often not able to autonomously perform security actions that cannot be directly and automatically performed by web browsers. Therefore, a CP that requires buyers to have such capabilities ends up strongly limiting its sale possibilities.
- The double watermark insertion requires that more than one trusted web entity is able to carry out a secure and robust watermarking procedure. In fact, a double watermark insertion may impair the final quality of the protected contents, thus ending up reducing their commercial value. Furthermore, the second applied watermark could also confuse or discredit the authority of the first applied watermark, thus acting as an actual "ambiguity attack" [11].
- The involved WCAs implement the "core" of the protection process. Thus, it is not possible to differentiate the generation of the fingerprinting codes and the control activity of the protection process from the watermark insertion. As a consequence, new watermarking procedures cannot be dynamically chosen and applied "on the fly", i.e. during each purchase web transaction, without forcing the involved WCAs to directly implement them.

This paper presents a web oriented and interactive anonymous buyer-seller watermarking protocol able to ensure the copyright protection of digital contents distributed on the Internet. The proposed protocol overcomes the drawbacks affecting the solution presented in [6]. In fact, the protocol allows buyers who are neither able to autonomously perform security actions nor provided with digital certificates issued by CAs

Authors are with the Research Centre on Software Technology, Department of Engineering, University of Sannio, Benevento, Italy (e-mail: frattolillo@unisannio.it).

to participate in the web transactions needed to buy contents distributed by CPs. Furthermore, it also allows guilty buyers, i.e. who are responsible distributors of illegal replicas, to be unambiguously identified without imposing a double watermark insertion in each of the distributed contents. Finally, the proposed protocol also allows the involved WCAs to behave solely as the "guarantors" of the protection process, whereas the watermark insertion is actually carried out by specific SPs whose services can be dynamically invoked during the purchase transactions. Thus, it is possible to differentiate the generation of the fingerprinting codes and the control activity of the protection process from the watermark insertion. As a consequence, particular and new watermarking procedures can be dynamically chosen and applied "on the fly" without forcing the involved WCAs to directly implement them [12], [13], [14].

The idea of designing and adopting watermarking protocols able to exploit distinct web entities, such as CPs, WCAs and SPs, is nowadays considered a clever way to address the problems reported above [4], [6], [10]. In fact, CPs often have neither the technical competence nor the economical advantage to directly apply complex or not certificated watermarking procedures to their distributed contents. They appear to be more involved in improving their specific and consolidated web consumer- or business-focused applications, rather than implementing new services based on advanced technologies that are not part of their original core business. On the other hand, SPs are web entities that have knowledge and expertise in the use of web programming technologies, and their core business is just to supply complex and specialized software services to CPs. On the contrary, WCAs are authorities that usually take charge of implementing and managing watermarking and dispute resolution protocols. Therefore, they are usually specialized in implementing few and specific watermarking procedures. As a consequence, SPs can be considered particularly suited to deploy many and differentiated copyright protection services on behalf of CPs, whereas WCAs can limit their action to the sole role of guarantors of the protection process. In fact, this model has already proven highly successful in the Internet, where SPs enable the building of web applications for CPs with good ideas but little time for technology [13], [14].

The paper is organized as the follows. Section II defines the entities taking part in the proposed watermarking protocol. Section III describes the protocol. Section IV discusses the accomplishment of the main protocol goals. In Section V a brief conclusion is available.

II. Entities and Roles

The proposed watermarking protocol is based on four main web entities: the buyer (B), the content provider or seller (CP), the service provider (SP), and the trusted watermark certification authority (WCA).

B is a web user, who is assumed neither to be provided with any digital certificate issued by a CA nor to know how he/she can obtain it. He/she is not able to autonomously perform any security action that cannot be automatically performed by the web browser he/she uses to purchase copies of digital contents distributed by CPs. Therefore, he/she is assumed to be able to establish SSL connections to web sites which do not demand users for digital certificates, and to pay by credit card, which can be nowadays considered a widely accepted payment method in the Internet.

CP is the seller, i.e. the entity wanting to make a profit on the sales of the digital contents distributed by its web site. It may be the owner of the contents or an authorized reselling agent. CP publishes its contents in catalogues made available on directly managed web servers or within thematic or dynamically built pages hosted by web portals. In fact, it supplies web consumer applications.

SP can implement trusted, advanced security services on behalf of other web entities, such as CPs. In fact, it promotes the integration of its services with web applications implemented by CPs by adopting web oriented technologies [15] and guaranteeing a high level of reliability and security to its services.

WCA is a trusted watermark certification authority, which directly implements two main services: the implementation of the payment process on behalf of CPs, and the generation of the fingerprinting codes able to unambiguously identify buyers. In particular, the payment process allows WCA to identify B on the base of his/her credit card.

III. The Proposed Watermarking Protocol

The proposed watermarking protocol:

- solves both the "customer's right problem" and the "unbinding problem";
- keeps B anonymous during the purchase web transactions;
- enables users who are not provided with digital certificates issued by CAs to purchase protected digital contents;
- does not require B to be able to autonomously perform security actions that are not closely tied to the functionalities implemented by common web browsers;
- does not require a double watermark insertion, thus both avoiding to discredit the embedded protection and a possible degradation of the final quality of the distributed contents.

In the following, the main design choices are reported. Then, the two subprotocols comprising the proposed protocol are presented: the *protection protocol* and the *identification and arbitration protocol*.

A. The Design Choices

In order to meet the requirements reported above, the following choices have been made.

First, B is identified by means of a fingerprinting code associated to his/her credit card, and this allows him/her to purchase digital contents distributed by CPs even though he/she is not provided with a valid digital certificate. However, the implemented identification method could be considered

"weak", since credit cards can be cloned. On the other hand, credit cards are always associated to real identities, and, if not invalidated, they are commonly exploited to implement an actual and widely used payment method in e-commerce transactions. As a consequence, if generated on the basis of information tied to a credit card and if correctly retrieved from a pirated copy, a fingerprinting code always allows for individuating a real identity, and this enables CPs to legally prosecute the identified users whenever they are adjudicated to be guilty.

The choice of relating fingerprinting codes to the identities reported on credit cards, i.e. the adoption of a "weak" identification method, results in being advantageous to users, who can now buy digital contents without having to be provided with digital certificates. However, it forces WCAs to be directly involved in the commercial transactions that take place whenever B wants to buy a digital content distributed by CP. This means that, differently from previous solutions, now WCAs have to behave as web entities able to guarantee the whole commercial and protection process, thus playing a strategic role in the watermarking protocol. However, such a new role avoids a double watermark insertion and enables CPs to take advantage of the services supplied by SPs. This makes the watermarking protocol well suited to be adopted in a web context, where it is important to enable the dynamical composition of complex services implemented by distinct web entities [13], [14], [15], [16].

B. The Protection Protocol

Figure 1 shows the scheme of the interactions taking place during a web transaction by which B purchases a copy of the digital content X distributed by CP. In particular, in the following, the notation N.n denotes the message dispatch from the entity N, at the step n of the protocol. The message is exchanged according to what reported in the legend of the Figure, i.e. through SSL connections characterized by different authentication schemes negotiated at the connection start-up. Furthermore, in Figures 1 and 2 the notation $E_{entity}(data)$ specifies a ciphered token whose $data$ are encrypted with the $entity$'s secret key, whereas the notation $Eph_{entity}(data)$ specifies a ciphered token whose $data$ are encrypted by exploiting a cryptosystem that is "privacy homomorphic" with respect to the watermark insertion [6].

All the ciphered tokens are also assumed to be concatenated to a "hashed token authentication code", which is computed as the SHA-1 hash over the token plus the entity's secret key. In particular, as shown in Figure 1, the ciphered tokens are always exchanged through already protected connections, such as the SSL connections. In addition, such tokens may be deciphered and authenticated solely by the entities that have generated them. Therefore, the exploitation of protected tokens does not intend to increase the security level of communications, but it allows each entity involved in the protocol to validate, by comparing the exchanged ciphered and plaintext information, specific parts of the on going transactions.

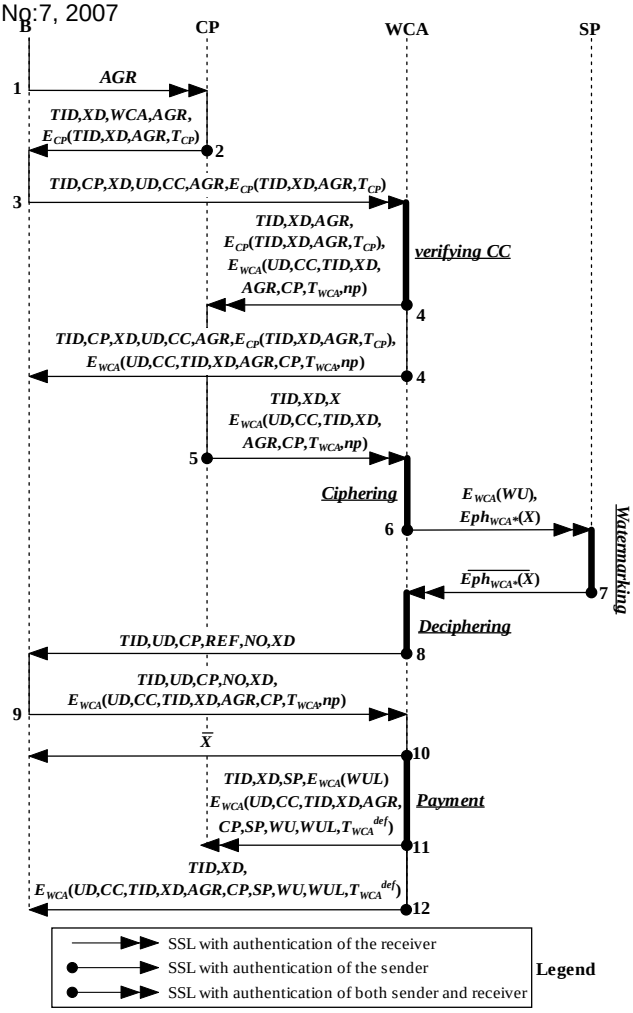

Fig. 1 The protection protocol

B initially visits the CP's web site and, after having chosen X, negotiates with CP to set up a common agreement AGR. AGR states the rights and obligations of both parties as well as specifies the digital content of interest. It can be regarded as a "purchase order" whose generic form can be also published by CP on its web site. During this negotiation phase B may have free access to the CP's web site or use a registered pseudonym, thus keeping his/her identity unexposed.

After the initial negotiation, B communicates his/her will of buying X to CP by sending the negotiated AGR (B.1). In particular, in the SSL session activated between B and CP, CP is the sole entity to be authenticated.

Upon receiving AGR, CP generates the token $E_{CP}(TID, XD, AGR, T_{CP})$ that includes:

- the transaction identifier TID, which is a code used by CP to identify the current transaction;
- the synthetic description of X, denoted as XD;
- the common agreement AGR, which represents the purchase order;

- the timestamp T_{CP}, which is generated by CP in order to make the token's freshness assessable.

The token is sent to B (CP.2) together with plaintext information, such as the reference WCA to the WCA selected by CP.

B receives the message CP.2 and sends WCA the token $E_{CP}(TID, XD, AGR, T_{CP})$ (B.3), previously received from CP, together with further plaintext information, such as:

- TID, XD and AGR, whose definitions are reported above;
- CP, which is the reference to CP;
- UD and CC, which are respectively the identity and the number associated to the B's credit card.

In fact, data exchanged in the message B.3 allow WCA to check if B can pay X and to unambiguously identify B. To this end, it is worth noting that the correct identification of B is based on the validation of the information associated to the B's credit card. Therefore, if data associated to the credit card are incorrect or the credit card turns out to be invalidated, the transaction is interrupted.

B.3 is considered by WCA a purchase order involving B and CP. Therefore, after verifying the B's credit card, WCA generates the token $E_{WCA}(UD, CC, TID, XD, AGR, CP, T_{WCA}, np)$, which includes, among the others, T_{WCA} and np: the former is a timestamp that makes the token's freshness assessable, whereas the latter is a simple flag specifying that the B's credit card has not been charged yet. The token is sent to B as a "temporary" purchase certificate, whereas is sent to CP as a "temporary" sale certificate (WCA.4). In addition, WCA also returns some other information to B and CP in order to enable them to make a check on the current transaction. In fact, B and CP cannot access the information contained in the temporary, ciphered certificates, and this prevents them from maliciously modifying the certificates. However, they can verify the plaintext data exchanged in WCA.4, and so they can abort the transaction if data turn out to be invalid.

After verifying WCA.4, CP can send WCA the watermarking request CP.5, which includes X. After receiving X, WCA encrypts it by exploiting a cryptosystem that has to be "privacy homomorphic" with respect to the subsequent watermark insertion [6]. WCA also generates the fingerprinting code WU, which will have to be embedded in X to identify B. To this end, in order to always associate the same code to the same buyer, WCA exploits two specific functions, Φ and Ψ: the former generates a binary code μ identifying the buyer on the base of CC and UD, whereas the latter generates a bit string τ depending on XD and T_{WCA}. As a consequence, μ is always the same for a given credit card, whereas τ varies under different digital contents and timestamps. WU is the concatenation of μ and τ. In addition, WCA exploits a further function ϵ to generate an extended version of WU, denoted as WUL, whose ciphered form will be used by CP to identify B. Then, WCA selects an SP and sends it the watermarking request (WCA.6), which includes the token $E_{WCA}(WU)$ and the content $Eph_{WCA^*}(X)$, where $*$ denotes that the content has been ciphered with a one-time secret key.

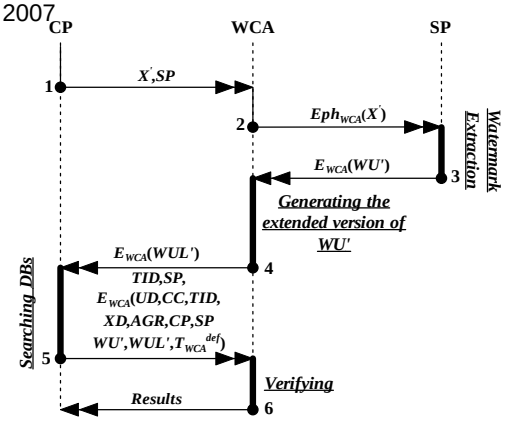

Fig. 2 The identification and arbitration protocol

After receiving WCA.6, SP can directly watermark $Eph_{WCA^*}(X)$. In fact, such an operation is possible because, as reported above, the encryption function applied by WCA is assumed "privacy homomorphic" with respect to the watermark insertion operation. Once $Eph_{WCA^*}(X)$ has been watermarked, SP sends WCA the message SP.7, which contains the new watermarked content $\overline{Eph_{WCA^*}(X)}$ obtained by inserting the watermark in the encryption domain.

Then, WCA can decrypt $\overline{Eph_{WCA^*}(X)}$, thus generating the final version of the watermarked copy of X, denoted as $\bar{X}$. In fact, the privacy homomorphic cryptosystem used by WCA results in the following equalities:

$$\overline{Eph_{WCA^*}(X)} = Eph_{WCA^*}(\bar{X})$$

$$\bar{X} = Dph_{WCA^*}(\overline{Eph_{WCA^*}(X)})$$

where the operator Dph denotes the decryption function corresponding to the encryption function Eph.

Once generated $\bar{X}$, WCA notifies its availability to B. In particular, message WCA.8 also specifies a "nonce" NO and the reference REF to the download server, which can be also distinct from WCA and from which B may download the watermarked content $\bar{X}$. Then, if all data exchanged in B.9 are valid, B can contact the server REF and download $\bar{X}$ (WCA.10). Thus, after the correct download of $\bar{X}$, WCA can charge the B's credit card and generate the token $E_{WCA}(UD, CC, TID, XD, AGR, CP, SP, WU, WUL, T^{def}_{WCA})$, which represents the definitive version of the purchase and sale certificates to be sent to B and CP respectively (WCA.11 and WCA.12). In addition, WCA also sends CP $E_{WCA}(WUL)$, which will be used by CP to refer to the corresponding sale certificate, SP and TID in its databases.

C. The Identification and Arbitration Protocol

The *identification and arbitration protocol*, whose interaction scheme is shown in Figure 2, can be conducted whenever

a pirated copy of a protected digital content owned or distributed by CP is found in the market. The aim is to determine the identity of the responsible distributor, who was the buyer in some earlier transaction, with undeniable evidence. Therefore, when a pirated copy X' is found, CP can ask WCA for starting the *identification and arbitration protocol* by sending it X' and the reference to the SP exploited to protect the original content X (CP.1).

WCA sends SP the ciphered content $Eph_{WCA}(X')$ (WCA.2), and this prevents SP from getting access to the final versions of the protected contents distributed by CP. Then, SP extracts the embedded watermark from $Eph_{WCA}(X')$ and communicates the fingerprinting code $E_{WCA}(WU')$ to WCA (SP.3). WCA takes charge of generating the extended version of WU', denoted as WUL'. Then, WCA sends CP $E_{WCA}(WUL')$ (WCA.4).

CP accesses its databases and uses $E_{WCA}(WUL')$ to search them for a match. When a match is found, CP retrieves the sale certificate $E_{WCA}(UD, CC, TID, XD, AGR, CP, SP, WU', WUL', T^{def}_{WCA})$ as well as the further information associated to $E_{WCA}(WUL')$, and requires the buyer identification by sending these data to WCA (CP.5).

WCA decrypts the sale certificate and verifies all data received from CP. If all data turn out to be correct, the identity of the buyer is revealed, and WCA can adjudicate him/her to be guilty, thus closing the case. Otherwise, the protocol ends without exposing any identity.

Finally, it is worth noting that all the messages shown in Figure 2 are exchanged through SSL connections with authentication of both sender and receiver, according to the legend shown in Figure 1.

IV. Discussion

The proposed protocol has been developed in order to address the "customer's right problem" and the "unbinding problem" as well as to make the devised solution well suited to be exploited in a web context. To this end, it is worth noting that the security level of the protocol essentially corresponds to the one guaranteed by the SSL connections, which can be considered sufficient for a web context, since e-commerce transactions are widely based on SSL.

The proposed protocol is secure and fair to both B and CP. In fact, from B's viewpoint, CP and SP get no access to the final watermarked copy of X, and this prevents them from distributing illegal replicas, thus solving the "customer's right problem". Furthermore, it is impossible for SP to fool B re-using fingerprinting codes taken from previous correct transactions. In fact, the fingerprinting code to be inserted in a content also depends on the content itself. However, the contents to protect are sent by WCA to SP in a ciphered form encrypted with one-time secret keys, and so SP is neither allowed to access contents nor is able to know which CPs are the actual owners of the contents. Therefore, SP cannot collude with CPs in this phase of the protocol, and if it autonomously attempted to re-use a code, it would end up generating a content that would result in being protected by a wrong code. As a consequence, if such a content were found in the market, SP would be adjudicated to be guilty. Again, even if CP and SP were able to collude after a watermark insertion operation so as to correctly bind two corresponding codes $E_{WCA}(WU_\circ)$ and $E_{WCA}(WUL_\circ)$ generated by WCA to protect a content Y previously purchased by B_y, they could not illegally re-use them to protect the content Y purchased by B_z or the content Z purchased by B_y, because they could not generate valid sale and purchase certificates containing $E_{WCA}(WU_\circ)$, $E_{WCA}(WUL_\circ)$, and coherent data about the content description as well as the buyer's identity. In fact, both the sale and purchase certificates bind the fingerprinting code and its extended version to the buyer's identity, the purchased content and the web transaction by which the content is bought, and this because the fingerprinting code is the concatenation of μ and τ. However, both the certificates are stored by B and CP in a ciphered and signed form, and so CP, SP and B cannot generate, access or modify them. As a consequence, running the *identification and arbitration protocol* on a watermarked content illegally generated by SP does not allow CP to adjudicate anybody to be guilty. Therefore, the "unbinding problem" is solved.

From CP's viewpoint, the proposed protocol is secure, because B and SP cannot get access to an original copy of X. In addition, B can neither know which watermarking algorithm has been used to protect X nor calculate the fingerprinting code, because the code is not always the same for a given buyer, being characterized by the varying part determined by τ.

WCA does not carry out the watermark insertion, whereas it is allowed both to get access to X and to know the B's identity derived from his/her credit card. However, WCA is assumed to act as a trusted web entity and as the sale/purchase guarantor. Therefore, as in other watermarking protocols [4], [5], [6], [9], [10], it is assumed not to carry out colluding actions. Moreover, WCA can abort the whole web transaction, if the freshness of the exchanged tokens is violated or the tokens result in being incorrect. Therefore, only if all the phases of the proposed protocol result in being correct, the payment process and the delivery of $\bar{X}$ take place.

SP takes charge of inserting the watermarks. It is not required to manage any database, since it receives the ciphered fingerprinting codes and inserts them into the ciphered contents to protect. However, a problem could arise if SP did not watermark a received content or the applied protection were not effective. In fact, the former situation can be avoided by WCA, which can compare $Eph_{WCA}(X)$ and $\overline{Eph_{WCA}(X)}$, thus aborting the protocol if the two contents result in being equal. On the contrary, in the latter case, an inadequately protected copy of X would end up being delivered to B. However, it is worth noting that SP is directly chosen by WCA as a trusted web service provider, and its business possibilities strongly depend on its capability to effectively protect digital contents on behalf of CPs. In fact, if a content distributed by CP and not adequately protected by SP were found in the

market, WCA could break its relations with SP. Therefore, SP can be assumed to supply trusted, secure and effective services.

B is required to contact CP and WCA. In fact, B performs three distinct actions: the first consists of choosing X; the second consists of sending out the purchase order; the third consists of requiring the download of $\bar{X}$. Even though such a behavior could require B to download and execute some code fragments (such as ActiveX controls or Java bytecode) in order to correctly manage the web transactions, it does not represent an actual problem for users provided with web browsers, such as MS Internet Explorer or Mozilla. Furthermore, B's privacy is protected, since B can purchase a digital content keeping his/her identity unexposed during the web transactions involving CP. His/her identity is known solely by WCA, which acts as a trusted third party and is forced to make the B's identity known only if B is adjudicated to be guilty. Furthermore, B is not required to cooperate in the phase of arbitration, since WCA, CP and SP are capable of making appropriate adjudications collaboratively.

In the proposed protocol web users can purchase digital contents distributed by CPs without having to be provided with digital certificates issued by CAs. This very much resembles what common web users do when shopping in the Internet, and just cannot be any simpler. On the other hand, CPs can achieve an adequate protection of their digital contents without limiting their sale possibilities to the sole users provided with valid digital certificates.

The proposed protocol requires that a content to protect is transferred from CP to WCA and SP, before returning to WCA, i.e. the site which B can download the content from. In fact, this route is characterized by several hops, but avoids a double watermark insertion, which can impair the final quality of the content, thus reducing its commercial value. Furthermore, the second applied watermark could also confuse or discredit the authority of the first applied watermark, thus acting as an "ambiguity attack" [11].

Finally, the proposed protocol assumes that the burden of storing necessary information is put on CPs, and this can be considered reasonable, since CPs are very likely to already have their databases needed to manage their web activities.

V. Conclusions

In this paper a web oriented and interactive anonymous buyer-seller watermarking protocol is presented. The protocol, differently from other relevant solutions previously presented in literature, solves both the "customer's right problem" and the "unbinding problem". Furthermore, it is well suited to be exploited in a web context, since it enables users who are neither provided with digital certificates issued by CAs nor able to autonomously perform any security action to purchase digital contents distributed by CPs while keeping their identities unexposed during web transactions. In addition, the protocol also allows guilty buyers, i.e. who are responsible distributors of illegal replicas, to be unambiguously identified. Finally, the protocol has been designed so that CPs can exploit watermarking services supplied by SPs in a secure context without having to directly implement them, according to a well-known interaction and business model that has already proven to be highly successful in the Internet.

References

[1] I. Cox, J. Bloom, and M. Miller, *Digital Watermarking: Principles & Practice*. Morgan Kaufman, 2001.
[2] F. Bartolini, A. Piva, and M. Barni, "Managing copyright in open networks," *IEEE Internet Computing*, vol. 6, no. 3, pp. 18–26, 2002.
[3] M. Barni and F. Bartolini, "Data hiding for fighting piracy," *IEEE Signal Processing Magazine*, vol. 21, no. 2, pp. 28–39, 2004.
[4] L. Qiao and K. Nahrstedt, "Watermarking schemes and protocols for protecting rightful ownership and customers rights," *Journal of Vis. Commun. Image Representation*, vol. 9, no. 9, pp. 194–210, 1998.
[5] N. Memon and P. W. Wong, "A buyer-seller watermarking protocol," *IEEE Trans. on Image Processing*, vol. 10, no. 4, pp. 643–649, 2001.
[6] C. L. Lei, P. L. Yu, *et al.*, "An efficient and anonymous buyer-seller watermarking protocol," *IEEE Trans. on Image Processing*, vol. 13, no. 12, pp. 1618–1626, 2004.
[7] W. Trappe, M. Wu, *et al.*, "Anti-collusion fingerprinting for multimedia," *IEEE Trans. on Signal Processing*, vol. 41, no. 4, pp. 1069–1087, 2003.
[8] M. Wu, W. Trappe, *et al.*, "Collusion-resistant fingerprinting for multimedia," *IEEE Signal Processing Magazine*, vol. 21, no. 2, pp. 15–27, 2004.
[9] K. Gopalakrishnan, "Protocols for watermark verification," *IEEE Multimedia*, vol. 8, pp. 66–70, 2001.
[10] S. Katzenbeisser, "On the design of copyright protection protocols for multimedia distribution using symmetric and public-keywatermarking," in *Proc. of the 12th Int'l Workshop on Database and Expert Systems Applications*, 2001, pp. 815–819.
[11] F. Hartung, J. K. Su, and B. Girod, "Spread spectrum watermarking: Malicious attacks and counterattacks," in *Security and Watermarking of Multimedia Contents*, ser. Proceedings of SPIE, E. J. Delp and P. W. Wong, Eds., vol. 3657, 1999, pp. 147–158.
[12] F. Frattolillo and S. D'Onofrio, "Applying web oriented technologies to implement an adaptive spread spectrum watermarking procedure and a flexible DRM platform," in *Proc. of the 3rd Australasian Information Security Workshop*, ser. Conferences in Research and Practice in Information Technology, P. Montague, R. Safavi-Naini, R. Buyya, *et al.*, Eds., vol. 44, Newcastle, Australia, Feb. 2005, pp. 159–167.
[13] ——, "Implementing a simple but flexible DRM web platform," in *Proc. of the 3rd Int'l Conference on Computing, Communications and Control Technologies*, Austin, Texas, USA, 2005.
[14] ——, "An effective and dynamically extensible DRM web platform," in *Proc. of the Int'l Conference on High Performance Computing and Communications*, ser. Lecture Notes in Computer Science, L. T. Yang, O. F. Rana, B. Di Martino, and J. Dongarra, Eds., vol. 3726, Sorrento, Italy, Sept. 2005.
[15] R. Brunner, F. Cohen, *et al.*, *Java Web Services Unleashed*. SAMS Publishing, 2001.
[16] M. Ceccarelli, M. Di Santo, S. D'Onofrio, and F. Frattolillo, "A web multi-tier platform for adaptively protecting and securely delivering multimedia contents on the web," in *Proc. of the 5th Int'l Workshop on Image Analysis for Multimedia Interactive Services*, Lisbon, Portugal, 2004.