

# Anonymous Authorship Control for User-Generated Content

Suk-Bong LEE\*

Telecommunication R&D Center, Samsung Electronics, 416, Maetan-3Dong, Yeongtong-gu,  
Suwon-Si, Gyeonggi-Do, 443-742, Republic of Korea

Sang-Gyoo SIM

WIDI Lab, 748-28 Yeoksam-Dong, Gangnam-Gu,  
Seoul, 139-925, Republic of Korea

Yeo-Jin KIM

Samsung Advanced Institute of Technology Nongseo-dong, Giheung-gu,  
Yongin-Si, Gyeonggi-Do, 446-712, Republic of Korea

Yun-Sang OH

Telecommunication R&D Center, Samsung Electronics, 416, Maetan-3Dong, Yeongtong-Gu,  
Suwon-City, 443-742, Republic of Korea

Kyung-Im JUNG

Samsung Advanced Institute of Technology Nongseo-dong, Giheung-gu,  
Yongin-Si, Gyeonggi-Do, 446-712, Republic of Korea

Bong-Nam NOH\*

Div. of Electronics Computer Eng., Chonnam National University, Gwangju, R.O.Korea

## ABSTRACT

User-Generated Content (UGC) is opening up new large market in content services, and more and more people are visiting web sites to share and enjoy UGCs. These trends make many authors to move into online. Authors want to conserve their authorship and expect to publish their UGC anonymously in cases. To meet the requirements, we propose a new authorship control model based on watermarking and metadata. Authors can embed their authorship into their UGC with identities or with anonym. Even though an author publishes his UGC anonymously, he can prove his authorship without unveiling his identity via 5 methods utilizing the proposed authorship model. The proposed model and methods need no TTP and are robust even based on fragile underlying watermarking scheme.

**Keywords:** User-Generated Content, Authorship Control, Anonymous Author and Authorship Proof

## 1. INTRODUCTION

With wide spread of mobile devices having multimedia content generation function, it has been possible the device user to generate multimedia content anywhere and anytime. Also sharing of the UGC (User-Generated Content) is increasing explosively through online content sharing sites such as YouTube (<http://www.youtube.com>). Through these sites, one can be a famous star if his UGC wins popularity among other

people [1]. In other case, someone become a target of criticism if his immoral conduct was taken by someone's lens. Also, there are people who earn money using the popularity of their distributed UGC containing an accident scene, a terror scene, or other impressively noble picture.

In proportion to explosive spread of UGC, preservation and proof of authorship of the author have become more important. A user wants his copyright to be preserved even in cases out of his control or consent. If there happens a dispute between the author and other persons about UGC, it is required to prove the authorship of the author. In addition, the anonymity of author is an additional but critical feature. Authors want to remain anonymous for their safety if their UGC contain some clues or evidences of criminals. The authors of the UGC may be a victim of another crime. Other authors want anonymity for privacy rather than safety because he does not want to be bothered by the public. Though an author generates and then shares his UGC anonymously, he may want to unveil his anonymity some time later. If his content becomes very popular, the author may want to reveal his authorship to boast his work or to earn some money, royalty fee. Consequently, we need the means to support author's anonymity for the various usage of the UGC.

This paper proposes an authorship control model which is based on digital watermarking schemes and the corresponding metadata of content. The metadata contains information about author and the media. And watermarking schemes are used to guarantee the integrity of the metadata. By utilizing the authorship control model, an author can share his UGC anonymously, and prove his authorship if he determines some time later. This paper proposes 5 methods to do it.

This paper is organized as follows. Section 2 introduces a user scenario where anonymous authorship is needed, and Section 3 reviews previous works. The proposed authorship control model is described in Section 4, and the 5 methods to support author's

\* The authors were partially supported by the MIC (Ministry of Information and Communication), Korea, under the ITRC (Information Technology Research Center) support program supervised by the IITA (Institute of Information Technology Advancement) (IITA-2006-C1090-0603-0027).

anonymity are proposed in section 5. Finally Section 6 discusses more issues and concludes.

## 2. MOTIVATION

Figure 1 illustrates a feasible user scenario representing the necessity of author's anonymity.

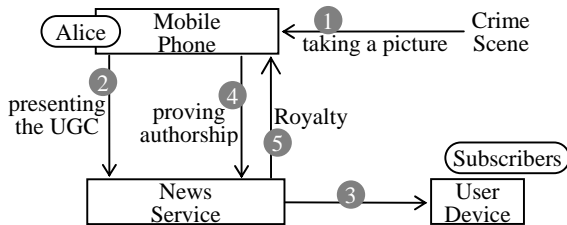


Figure 1. User Scenario

### 2.1 Generating UGC and setting attributes

In Step 1, Alice sees that some bank robbers are getting out of the bank on her way. Alice takes a moving picture of the robbers stealthily via her mobile phone. In this time, her mobile phone may ask some questions of her to select some options about the attributes of the UGC. The attributes are configured according to Alice's selection. If Alice selects 'To Hide My Identification' option for her anonymity, then, the UGC is stored including an attribute for anonymous author. This attribute setting may be done during either generation step (Step 1) or distribution step (Step 2).

### 2.2 Distribution of UGC

In Step 2, Alice is going to present the UGC to a news service such as a broadcasting station and a newspaper. Since she is afraid of revenge from the robbers, she determines to hide her identification. If she did not select 'To Hide My Identification' option in Step 1, she selects the option in this step. Before transmitting her UGC out, her mobile phone hide her identification information and inserts authorship proof information in her UGC. On receiving her contents, the news service broadcasts this scene of crime as their clear scoop to subscribers in Step 3. Now the robbers become notorious criminals because of Alice's moving picture.

### 2.3 Unveiling anonymity

The news service wants to give the royalty to the author of the UGC, since they have got much benefit by using the UGC. But the news service doesn't know who the author is because the UGC was presented anonymously. Thus, the news service announces to give the author some royalty.

In Step 4, Alice decides to unveil the anonymity and proves her authorship of the content. After her proving, Alice can get some royalty in Step 5.

## 3. RELATED WORKS

### 3.1 Proving authorship with watermarking

There are several approaches to prove authorship using digital watermarking method against infringement actions. [2, 3, 4] These approaches embed author's identity directly into author's digital work using digital watermarking schemes before

distribution of the digital works. The author can prove his authorship by presenting his identity which is embedded in the work. This proof is done by verifying the presented identity is the same as the mark embedded in the distributed digital works. In general watermarking schemes, embedded mark may be distorted or deleted by the various modification of content such as editing, appending etc. Since the embedded mark is the only evidence to prove the authorship, these approaches requires robustness of digital watermarking schemes. However, it is an open problem to design a digital watermarking scheme which defends all possible attacks. This is a drawback of these approaches.

### 3.2 Anonymous fingerprinting

A kind of fingerprinting technique is thought to be used to anonymize sender's identity. [5, 6] In fingerprinting techniques, there are content buyers who consume contents and senders who sell contents. Seller makes fingerprint for each buyer and embeds it into contents before transmitting contents to buyer. Since the fingerprint contains identification information of buyer, it varies on buyers. Using this property, content seller can identify his buyers. That is, when a buyer infringes the seller's authorship, seller can identify the traitor among his buyers and prove the infringement with the embedded fingerprint. These techniques cause privacy issue that seller can collect buyer personal information such as identity, preference, etc. It contradicts 'fairness'. To support buyer's anonymity, some researches adopted TTP (Trusted Third Party) [7]. TTP hides identities of buyers from seller, and reveals them to seller when a buyer makes infringement of authorship.

### 3.3 Embedding metadata into multimedia content

According to growth of market of digital works, the formalized expression of data corresponding to digital works has been needed. As a candidate, DCMI (Dublin Core Metadata Initiative) [8] has been established as a basis for modular and interoperable metadata for distributed resources and digital works. ISO MPEG-21 [9] supports an environment under which all content types from different categories can be delivered and used over various applications. JPEG2000 [10] supports metadata with 64 bits corresponding to image works.

## 4. AUTHORSHIP CONTROL MODEL

### 4.1. Generation of digital works

This paper proposes a new authorship control model based on digital watermarking schemes and metadata expression. Conventional digital watermarking schemes have a drawback that these cannot embed a vast amount of data in digital works because the embedded mark does a role of noise. To prevent the quality decline of digital work from 'watermark noise', the amount of data to be embedded cannot help being restricted. In addition, the embedded watermark is fragile from distortion of media affected by transformation between formats, loss of data during transfer, etc. Unfortunately, it is remained as a open problem to make a robust watermark standing all distortion. The proposed authorship control model resolves the aforementioned drawbacks.

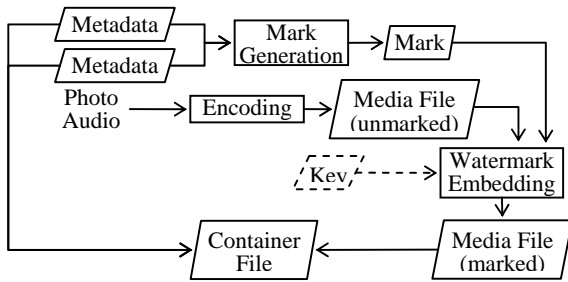


Figure 2. Watermark Generation and Embedding

Figure 2 shows the overall model of the proposed. If an author takes a photo or records an audio, the photo or the audio encoded as a media file, which does not contain any watermark – that is, which is an ‘unmarked’ media file. The media file has metadata corresponding to it. For one media file, there may be more than one metadata. The corresponding metadata are digested as a mark through mark generation process. This process may have a key depending on the method of mark generation. Underlying watermarking scheme embeds the computed mark into the media file, which results in the new ‘marked’ media file. According to the underlying watermarking scheme, watermark embedding process may have a key. The marked media file and the corresponding metadata are packaged within a container file. Consequently, the container file is the final result of UGC generation by the author.

The metadata possibly includes three kinds of data: media information, author information and media attribute. See Figure 3. Media information can be the image resolution, the number of frame, the color encoding method, the used codec, the date when the media was created or modified, the title information, the information of tracks, etc. Author information is the information about the authors who are either creators or modifiers. This includes the identity, the contact information, and other information which is dependent on authors. Media attribute means either conditions which the environment of the user or device using the media meets, or constraints under which the media should be used. Media attributes possibly consist of predefined attribute, user-defined attribute and previously used attribute. Predefined attribute is a set of attributes defined either by manufacturers during manufacturing or by service providers before selling devices, or loaded from publicly agreed standards. User-defined attribute is the user’s preferred set of attributes. It is built by users, whereas predefined attribute cannot be edited by users. If a user selects a set of attributes from predefined attributes or user-defined attribute, and he applies the attribute into the media with editing the attributes, then the applied set of attributes is stored as previously used attribute in the device. This functionality expands user experience by reducing user’s tedious input for customizing the attributes.

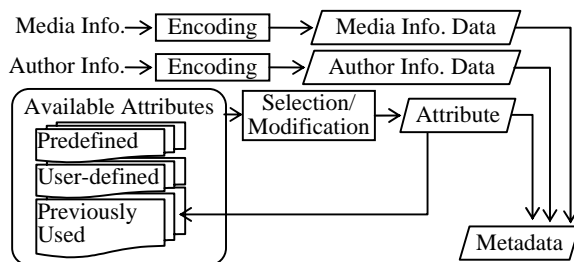


Figure 3. Metadata Generation

In the proposed model, a container file consists of media file and metadata describing the media file.

By embedding the mark computed from metadata into media file, the media file and its metadata are bind to each other. It provides integrity and authenticity of the container file. And embedding the mark rather than the metadata allows to deliver a vast amount of information about the media file.

#### 4.2. Insertion of authorship information

Insertion of authorship information is performed by three steps: metadata generation, digital watermarking and content packaging.

Metadata generation step makes metadata. As describing above, the metadata includes the information of author, media and attributes. The authorship information is described mainly in author information data, but possibly in media information data. For more understand, see Section 5.

Digital watermarking step generates a mark from the metadata and embeds it into the media file. The mark can be computed using a hash function or a MAC (Message Authentication Code) function. For some cases, a MAC can be replaced with a digital signature scheme. If a MAC function is used to compute the mark, the key of MAC is available to verifiers also when to validate the integrity of digital work. The watermarking scheme is used to embed the computed mark into the media file. According to the used scheme, it may need a key. [11]

Content packaging step generates a container file by packaging the ‘marked’ media file and the metadata according to a given specific format of container file. After packaging, the container file may be distributed to some other users or to public.

#### 4.3. Validation of authorship information

Validation of authorship information is done by validating the integrity of container file. Firstly, verifier re-computes a mark from the metadata contained in the container file. And then, he verifies integrity of the container file using the re-computed mark and ‘marked’ media file. According to the kind of underlying watermarking scheme, two types of validation are possible for the re-computed mark.

If the underlying watermarking scheme is a semi-private marking [11], verifier knows whether the re-computed mark is the same as the embedded mark of ‘marked’ media file or not. See Figure 4.

If the underlying watermarking scheme is a public marking [11], verifier can retract the embedded mark from ‘marked’ media file and know whether the retracted mark and the re-computed mark are the same or not. See Figure 5.

As a result, the proposed digital watermarking model makes it possible to distribute the metadata with integrity of it.

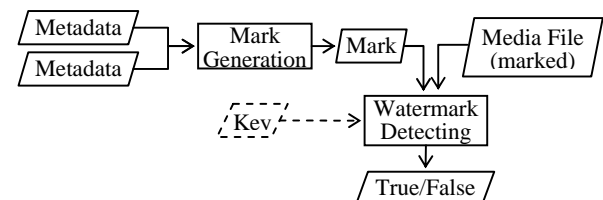


Figure 4. Watermark Detection (for Semi-Private Marking)

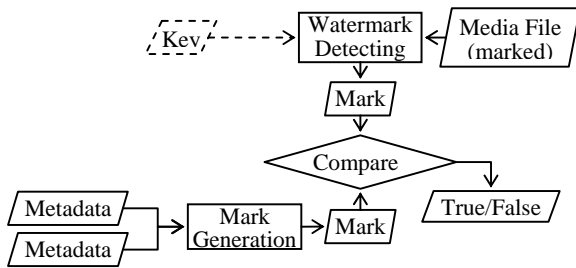


Figure 5. Watermark Retraction (for Public Marking)

## 5. HOW TO SUPPORT ANONYMOUS AUTHORS

### 5.1. Requirements and Assumptions

There are some requirements to design methods which supports anonymous authors based on the proposed authorship control model, so that the methods are suitable to recent P2P content delivery model and UGC service.

First, Author can veil or unveil his identity without interactive protocols. Contrastively, anonymous fingerprinting techniques use interactive protocols between sender (seller) and receivers (buyers) to hide receivers' identity. When an author 'A' delivers his UGC to other users via P2P connection, there are two possible connections: transient connection and radiant connection. In transient connection, 'A' sends the UGC to 'B', 'B' sends it to 'C', and so on. In this case, the author 'A' cannot keep the connection with all the receivers (for example, 'C') through interactive protocols. On the other side, radiant connection makes 'A' send his UGC to 'B', 'C', 'D', and so on. It causes that the author 'A' has too much load to maintain interactive protocol with all receivers.

Second, any TTP (Trusted Third Party) should not be used. If a TTP takes part in hiding the author's identity, it can become a kind of big brother to control the user ID and anonymity. It is impossible to share UGC between users freely without the TTP involvement. Moreover, the existence of TTP increases management cost and causes risk for centralized information gathering.

Third, only author has the information that proves authorship of the content. It may be possible to imagine an escrow system like as a key recovery system, which escrows the user identities and opens them under user agreement. However, since the escrow system is also another kind of TTP, the unveiling information for user anonym should be kept by the anonymous user himself. Last, the identity of author should be kept anonymously even after proving the authorship of his UGC. If not, the safety of the author will be fallen and he will enter an unwanted situation. To solve this last requirement, this paper replaces authorship proof with ownership proof.

### 5.2. Proposed Methods

Under aforementioned requirements new five methods are designed to support anonymous authors based on the proposed authorship control model.

#### A. Method 1: Using Pseudonym

Author information data of metadata have information about author such as author identity. Let assume a user inserts the author identity as pseudonym rather than his real identity. The pseudonym of the author is given by Pseudonym Management Authority (PMA) which generates and interprets pseudonym for one's real ID. Since the UGC is published with pseudonym

rather than the author identity, it can be distributed anonymously. That is, any receiver of the UGC cannot retrieve the real ID of the author from the UGC.

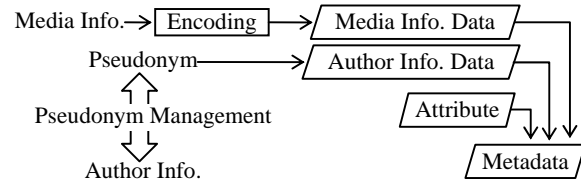


Figure 6. Using Pseudonym

Only when the author wants to unveil his pseudonym, he is able to prove his real ID with help of Pseudonym Management Authority. Sender submits a confidential check value which is given by PMA when generating his pseudonym to Verifier. The verifier can verify the sender is the only one who owns the credential. This verification can be processed via online or via offline. If the credential has no real identity of the author, the author identity can be kept anonymously after proving the authorship.

Here, PMA looks like another kind of TTP. However, PMA works only on generation of pseudonym but not on distributing the UGC. In addition, it is possible not to use real identity in generating pseudonym, which can, moreover, be performed inside of author's device.

#### B. Method 2: Using Media Integrity

Recall that watermarking scheme embeds a mark into given unmarked media file, which results in marked media file. The marked media file is slightly different from the unmarked media file because of the embedded mark. And recall that the retracting/detection process does not need the unmarked media file in semi-private or public marking [11].

Let assume metadata (especially, media information data) includes the media integrity code of the unmarked media file. In addition, it is supposed that author information data does not contains any real id of author. Then, no receiver of the marked media can retrieve the real ID of the author in absence of the author ID.

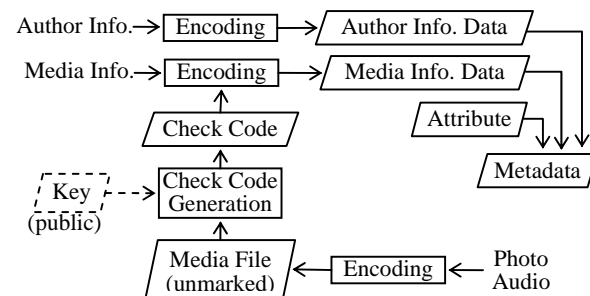


Figure 7. Using Media Integrity

When the author determines to prove his authorship, he does it by giving out the unmarked media file. From the unmarked media file, the metadata (including the media information data) and the mark can be computed. The retracting/detection process of watermarking scheme is able to verify either whether the marked media contains the computed mark (see Figure 4) or whether the computed mark is the same as the embedded mark (see Figure 5). Thus, the unmarked media file proves that it is

the original one of the marked media file. It is a proof of ownership for the original media rather than authorship. In this method, the media authentication code is either of a check code (i.e., a hash code) or a MAC (message authentication code). When a MAC is used, the key of MAC may be fixed.

**C. Method 3: Using Media Authenticity Key**

Let assume that a MAC is used for media authentication codes in Method 2. Method 3 is the same with Method 2 except that the key of MAC is not fixed.

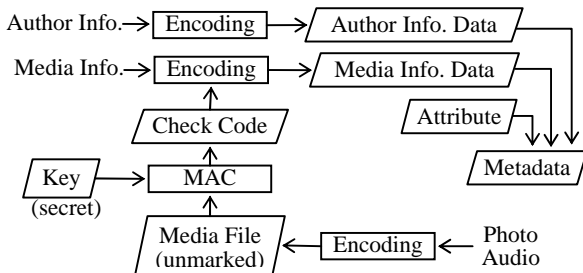


Figure 8. Using Media Authenticity Key

The anonymity unveiling process is done by submitting the key of MAC as well as the original unmarked media file. This feature can improve the usability of service and its security. Moreover, this method is very effective against weak watermarking schemes. Suppose that the watermarking scheme is so fragile, that it is feasible to obtain the original media with ‘innegligibly high’ probability. In case that an attacker tries to assert his illegitimate ownership by showing the obtained original media, Method 2 cannot prevent confirming the ownership. However, if the key is neither fixed nor public, the attacker should find out the secret key of MAC as well as the original media file. Thus, Method 3 provides a simple but strong countermeasure for fragile watermarking scheme not being sufficiently robust.

**D. Method 4: Using Metadata Authentication Key**

To embed metadata into media file, the set of metadata is compressed as mark. That is, the mark is computed via one-way function (such as hash) or MAC. Let assume that MAC is used for mark generation. When an author publishes his UGC anonymously, he omits his identity in author information and keeps the MAC key secret. Then, any receiver cannot find out the author identity in absence of it. Some time later, if he wants to prove the authorship of his UGC, what to do is only to make the MAC key open. Others are able to compute the mark and to verify the authorship through checking whether the computed mark is embedded in the marked media.

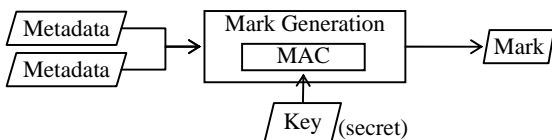


Figure 9. Using Metadata Authentication Key

This method has the same feature with Method 3. That is, their hypotheses to prove authorship go well even though the underlying watermarking scheme is so weak that attackers are able to obtain unmarked media file with ‘good’ probability.

**E. Method 5: Using Watermarking Key**

Some watermarking schemes use a key to embed the mark into unmarked media file and a retraction/detection key is used to recover or detect the mark from the marked media file. The two keys are different for public key marking but they are the same for other watermarking model [11]. In public key marking, the retraction process uses a key available to public and the embedding process uses a private key of user. This feature is very hard to support the anonymity of author because the retraction uses publicly available keys which are coupled with user identities. In other marking schemes, the retraction and embedding use a same key.

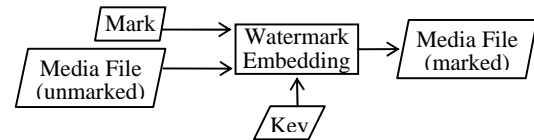


Figure 10. Using Watermarking Key

Let assume that user builds metadata without his real ID and embeds the mark using a secret key. Then, any one cannot retract the embedded mark from the marked media file nor verify the authorship of the author. If a proof is needed for authorship, the author opens the secret key used in watermark embedding and others can verify the media file was watermarked with the key. Since the needed evidence of authorship is only the secret key, this method also keeps the anonymity even after proving the authorship.

**6. DISCUSSION AND CONCLUSION**

This paper built an authorship control model based on watermarking scheme using metadata, which consists of author information, media information and attributes. This metadata can cover rich additional information flexibly. Since the metadata is computed as an authentication code and then watermarked into media, the rich additional information of metadata can be bind to the media file.

Based on the authorship control model, this paper proposed five methods to support anonymous author who hides his identity and some time later unveils his anonym when needed. The proposed methods use no TTP – in Method 1, pseudonym can be computed inside of author’s device. So there is no management cost or risk for a centralized big brother. Moreover, the proposed methods have very good features: they preserve the user anonymity even after proving the authorship through replacing authorship with ownership. The method 3 and 4 preserve author’s anonymity even though the underlying watermarking scheme is so fragile that the unmarked media can be obtained feasibly.

The proposed authorship control model and methods are suitable to P2P and UGC environments where users can generate and deliver their own content freely. The model is simple but provides rich information about media, and meets with requirements about media author’s privacy preservation.

## REFERENCES

- [1] Associated Press, “Now Starring on the Web: YouTube”, **Wired News**, April 9, 2006.
- [2] E. Koch and J. Zhao, “Towards robust and hidden image copyright labeling”, **Proceedings of 1995 IEEE Workshop on Nonlinear Signal and Image Processing**, 1995, pp. 452-455
- [3] N. Nikolaidis and I. Pitas, “Copyright protection of images using robust digital signatures”, **IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP-96)**, 4, 1996, pp. 2168–2171.
- [4] I. Pitas and G. Voyatzis, “Applications of toral automorphisms in image watermarking”, **IEEE Signal Processing Society**, 1996.
- [5] Birgit Pfitzmann, Michael Waidner, “Anonymous Fingerprinting”, **Lecture Notes in Computer Science**, Vol. 1233, 1997.
- [6] N. Memon and P.W. Wong, “A buyer–seller watermarking protocol”, **IEEE Transactions on Image Processing**, 2001, pp. 643-649.
- [7] Chin-Laung Lei Pei-Ling Yu Pan-Lung Tsai Ming-Hwa Chan, “An efficient and anonymous buyer-seller watermarking protocol”, **Image Processing, IEEE Transactions on**, Vol. 13, 2004, pp. 1618- 1626.
- [8] Dublin Core Metadata Initiative, <http://dublincore.org>, 2007
- [9] Joint Photographic Experts Group, <http://www.jpeg.org>, 2007
- [10] ISO/IEC JTC1/SC29/WG11, TR 18034-1, Information Technology - Multimedia Framework (MPEG21) - Part 1., September 2000.
- [11] Fabien A. P. Petitcolas, Ross J. Anderson and Markus G. Kuhn, “Information Hiding – A Survey”, **Proceeding of the IEEE, special issue on protection of multimedia content**, Vol. 87, No. 7, 1999, pp. 1062-1078.