Indian Journal of Science and Technology, Vol 9(35), DOI: 10.17485/ijst/2016/v9i35/101778, September 2016
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

The Collective Copyright Authentication Scheme Merging Collaborators' Rights on the Wisdom Contents

Sunghyun Yun[1*], Keun-Ho Lee[1], Heuiseok Lim[2] and Daeryong Kim[3]

[1*]Division of Information and Communication Engineering, Baekseok University, South Korea; shyoon@bu.ac.kr, root1004@bu.ac.kr
[2]Department of Computer Science and Engineering, Korea University, South Korea; limhseok@korea.ac.kr
[3] Department of Business, Delaware State University, USA; dkim@desu.edu

Abstract

Objectives: As wisdom contents are themselves the thought of people, the contents are made through collaboration of many authors in common, and there exists many duplicated or similar contents also. **Methods/Statistical Analysis:** Existing copyright authentication schemes mainly focus on the protection of primary author's right. The collaborators' rights are subordinated to the primary author. Thus, there needs to be a new scheme that could represent multiple rights on the wisdom contents. We propose the copyright protection scheme suitable for the wisdom contents. The proposed scheme consists of copyright registration, copyright creation and copyright add protocols. The primary author requests the center to do registration of the copyright. The center verifies the primary author's signature, and if it is valid, the center registers the copyright to the DB. **Findings:** In this study, we propose the collective copyright authentication scheme. It can merge collaborators' rights to the existing primary author's right. It is consisted of collective copyright registration, generation, add and verification protocols. We prove that our scheme is secure against masquerade attack, and the primary author and collaborators cannot deny multiple authorship. The proposed scheme could be extended to make multiple rights by combining each right of similar contents also. In Information Society, as the people's thoughts are varying each other, the types of software contents are much more various compared to the hardware based products. In this paper, we propose the dynamic copyright protection scheme in which creating and combining multiple authors' rights are possible. The proposed scheme ensures the right of the primary author and can add the select collaborator's right. It also could make the business model flexible to provide weighted profit distribution according to the level of developers. **Application/Improvements:** Due to these properties of our scheme, it's possible to create or extend the business model which is suitable for trading contents of Collective Intelligence.

Keywords: Authentication, Collaboration, Collective Copyright, Collective Intelligence, Copyright Protection

1. Introduction

In Industrial Society, a company secures competitive price by turning out goods on a mass production basis, and promotes and sales them to get more profits. In this case, customers can not get a choice but to accept the standardized goods. The company cannot produce customized goods satisfying various needs of customers. On the contrary, in Information Society, personal experiences or creative ideas are essential elements to create value-added contents. Especially, as the demands for mobile apps growing rapidly, the digital contents businesses are getting more attention nowadays[1,2]. The Apple's App Store is a typical leading platform in the area of digital contents business. It takes business transactions such as marketing, sales, and accounting from the individual developers. Thus, the developers have only to focus on making their own contents. They could make the profits at ease just by uploading their apps to the App Store. Due to these properties, ordinary persons could take part in the con-

*Author for correspondence

tents business. As a result, the small business is getting easier and popular these days[3], and it seems it's necessary to have a platform like App Store to success the business in Information Society[4]. The Wisdom Market is the hub to create and trade value added contents composed of persons' ideas and experiences. To be successful, the participation rate of ordinary persons should be raised high. To promote the rate, the Wisdom Market should provide easy to use authoring tools, and distribute profits fairly to the copyright holders. The wisdom contents are made with collaboration tools shared by multiple authors. Generally, the main author provides the concept of the contents to the social collaboration network. The concepts are made up with the feedbacks of collaborators. In a typical contents business model such as the App Store, the sales profits are distributed to the main author by rate fixed. In case of Wisdom Market where many authors are co-worked, the collaborators are also being considered for the distribution of profits. The researches on the copyright protection are classified into two major area, those are tag insertion and DRM (Digital Right Management). In tag insertion, the watermarking technique is the most common, and its role is to insert the copyright data into the contents transparently[5]. The DRM (Digital Right Management) includes contents distribution and profit sharing as well as authorship management on the contents[6,7]. The existing copyright protection schemes are mainly focus on how to protect the authorship of the primary author, the single entity. Thus, it's not appropriate to apply for the wisdom contents those are required to represent and authenticate authorships of many authors. In this paper, we propose the collective copyright authentication scheme suitable for the contents of Collective Intelligence such as wisdom contents. The proposed scheme consists of copyright generation, verification and update protocols. In section 2, we define wisdom contents and review reference models. In section 3, we present the proposed scheme. In section 4, we analyze the security of our scheme and discuss applications of it. Finally, we make a conclusion in section 5.

2. Research Background

2.1 Wisdom Contents

The high quality contents are made by professional authors who have specialized skills to develop apps, games, movies, and etc. As the ordinary persons cannot make such contents, the high quality contents types are restrictive, and the numbers of developers are also a little. Since wisdom contents are composed of persons' ideas and experiences, the professional skills are not required to make it. Anyone can do it as like we make YouTube contents to upload to the Internet. Thus, wisdom contents can be represented with various forms. Existing contents distribution models is developed to handle the standardized contents in common. It's not appropriate to distribute wisdom contents which are representable with various forms. As the human thoughts could be imagined voluntarily by anyone, there exist many similar and duplicated wisdom contents. Thus, it's more reasonable to define the author's copyright as a right to get profit rather than to acquire exclusive use on it. The copyright management scheme should be more flexible to satisfy various requirements of wisdom contents. The author should be able to combine the copyright with other authors' copyrights, and also represent multiple authorships on the same contents.

2.2 Business Model Requirements

We define following requirements to build the Wisdom Market.

A. An ordinary person should be able to participate in contents production and sales.

B. There should exist a system that takes part in sales, distribution and accounting of contents on behalf of authors.

C. The collaborators should be able to represent the multiple authorships on the primary author's contents

We review and analyze the App Store model satisfying both A and B, and quirky. Commode l satisfying C[8].

2.2.1 App Store Model

The App Store is the contents server and its role is to sale and distribute apps for mobile devices. It's a very big store in which many developers are participating. App developers should make contents with the standardized tool, Xcode, and the other things such as packaging, sales, distribution and accountings are to be done by the App Store. Due to these properties, the small companies including an ordinary person could get a chance to business with their contents. Before the advent of the App Store, it's not easy for them to participate in even though they have sufficient skills to build their contents, because they have not enough money to pay for the business transactions of sales, distribution, promotion, accounting, etc. Considering wisdom

contents, as we have already mentioned, there exists various similar and duplicate contents. They are represented with various forms which are not standardized. Thus it's not appropriate to apply App Store model to sale and distribute wisdom contents in direct. The business model for the wisdom contents should be dynamic and extensible to accommodate various types of it.

2.2.2 Quirky.com Model

The Figure 1 shows the profit distribution model of quirky.com company. The primary author gets 30% of sales profit, and the community who worked together are also get 30% of it. This means quirky.com model agrees on the partial rights of collaborators[8]. In the model; the primary author designs the product with his or her own ideas. The role of quirky.com is to help the author to implement the concept to the product and to get the profit. In general, ordinary consumers have many good ideas on the product, but it's not easy to make their ideas in to business because it requires too many costs to set up business transactions. Therefore, many good ideas of consumers are being disappeared. The quirky.com shows the answer how to connect ordinary persons' ideas to the business. The user should subscribe to the quirky.com and submit the product concept online. The user's proposal is completed with feedbacks of existing subscribers, the community shown in Figure 1. The board of committee, the expert group of quirky.com, decides if the modified proposal is worth to produce. Once the proposal is accepted, quirky.com takes parts of doing the product production, distribution and sales. The sales profits are distributed to the members according to the participation rates each. In the Wisdom Market, all transactions related to the contents are made online which is not mandatory in quirky.com model. Thus, we need a new method that could represent and authenticate the collective copyright online to ensure the rights of community.

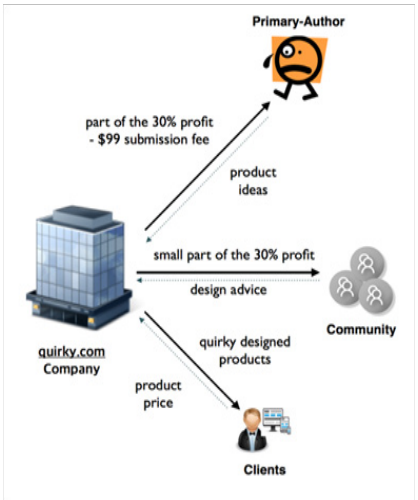

Figure 1. Quirky.com profit distribution model

3. Collective Copyright Protection Model

In this paper, we propose the copyright protection scheme suitable for the wisdom contents. The proposed scheme consists of copyright registration, copyright creation and copyright add protocols.

3.1 Copyright Registration

A primary author, collaborators and a registration center is the components of our scheme. The primary author is the creator of the contents, and collaborators are the group co-worked with. The primary author has the right of adding copyright of the select collaborators on the contents. The center registers and manages the collective copyright. Figure 2 shows the registration process of the collective copyright. The contents are made with co-operation of the primary author and collaborators. The primary author requests the center to do copyright registration and the collaborators to do copyright add. Then, collaborators request the center to generate the collective copyright. The center generates the watermark and the collective copyright, and signs on them to represent multiple authorships. The watermark is encrypted with center's secret key. Then, the center watermarks it to the contents invisibly. Finally, the center registers and saves the collective copyright to the DB. Figure 3 shows the verification process of the collective copyright. The user

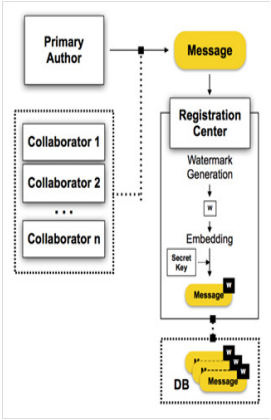

Figure 2. The registration process of collective copyright

who wants to verify the copyright sends the watermarked contents to the center. Then, the center extracts the watermark and compares it with the one registered previously. If two values are equal, the center confirms the integrity of the collective copyright. Otherwise, the center sends failure notice to the user.

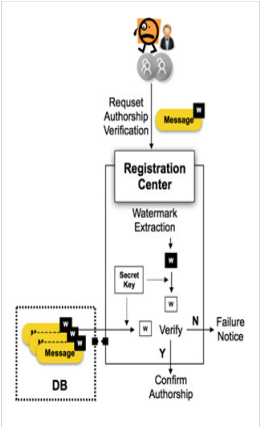

Figure 3. Verification process of collective copyright

Assumption 1. There exists a trustful registration center.

Assumption 2. The primary author, collaborators and the center have respective certificates issued by PKI authentication center that has legal binding forces. Thus, the certificates are legally bound. The key generation and encryption algorithms are cryptographically secure[9,10].

Assumption 3. The watermarking method is used to insert and extract the copyright. The conventional encryption algorithm is used to encrypt the watermark. We assume that both schemes are cryptographically secure[11-13].

3.2 Copyright Creation

The primary author requests the center to do registration of the copyright. The center verifies the primary author's signature, and if it is valid, the center registers the copyright to the DB. The terms and definitions used here are shown in Table 1.

Step 1: The PA hashes the message and signs on it to make the signature, $sig_{PA}(msg)$. The PA generates the copyright request message, $reqMsg_{PA}$, and makes the signature, $sig_{PA}(reqMsg_{PA})$. The $reqMsg_{PA}$ is composed of msg , $cInfo_{PA}$ and $cert_{PA}$. The $cInfo_{PA}$ $cInfo_{PA}$ is composed of copyright data such as the PA's name, contents ID, publication date, etc.

Table 1. Terms and definitions

Term	Definition	Term	Definition
PA	Primary Author	$cInfo_{RC}$	copyright Information of Center
CA	Collaborator	$reqMsg_{PA}$	PA's Request for copyright
RC	Registration Center	$reqMsg_{CA}$	CA's Request for Co-authorship
$cert_{PA}$	PA's PKI Certificate	$EN_{key}(\square)$	RSA Encryption with the key
$cert_{CA}$	CA's PKI Certificate	$DE_{key}(\square)$	RSA Decryption with the key
$cert_{RC}$	RC's PKI Certificate	$sig_{USER}(\square)$	USER's Digital Signature
pk_{PA}	PA's Public Key	msg	Digital Contents
pk_{CA}	CA's Public Key	msg_{w*}	Watermarked Digital Contents, *=[0…]
pk_{RC}	RC's Public Key	$H(\square)$	MD5 or SHA-1 Hash Function
sk_{PA}	PA's Private Key	$SC(\square)$	Scramble with RC's master key
sk_{CA}	CA's Private Key	$DESC(\square)$	Descramble with RC's master key
sk_{RC}	RC's Private Key	$EB(w^* \rightarrow msg)$	Embed Watermark w* to the msg
$cInfo_{USER}$	copyright Information of USER	$ET(w^* \leftarrow msg_{w^*})$	Extract Watermark w* from the msg_{w^*}

$$reqMsg_{PA} = \{msg, cInfo_{PA}, cert_{PA}\}$$
$$sig_{PA}(msg) = EN_{sk_{PA}}(H(msg))$$
$$sig_{PA}(reqMsg_{PA}) = EN_{sk_{PA}}(H(reqMsg_{PA}))$$

Step 2: The PA sends $reqMsg_{PA}$, $sig_{PA}(reqMsg_{PA})$ and $sig_{PA}(msg)$ to the RC.

Step 3: The RC verifies the PA's copyright request as follows. The RC verifies the signature in the $cert_{PA}$. If it is valid, the RC extracts the PA's public key, pk_{PA}, from the $cert_{PA}$. Then, the RC uses pk_{PA} to verify the signature on the PA's copyright request, $sig_{PA}(reqMsg_{PA})$. If $H(reqMsg_{PA})$ is not equal to the decrypted result of $sig_{PA}(reqMsg_{PA})$, the RC sends failure notice to the PA and terminates the protocol. Otherwise, the RC advances to the step 4.

Step 4: The RC creates the PA's copyright, $cRight_{PA}$, and signs on it.

$$cRight_{PA} = \{cInfo_{PA}, issuer_{RC}, sig_{PA}(msg), cert_{PA}\}$$
$$sig_{RC}(cRight_{PA}) = EN_{sk_{RC}}(cRight_{PA})$$

Step 5: The RC scrambles the $cRight_{PA}$ with its own secret key.

$$SC(cRight_{PA})$$

Step 6: The RC watermarks the signature of step 4 and the encrypted copyright of step 5 as follows.

$$w0 = \{SC(cRight_{PA}), sig_{RC}(cRight_{PA})\}$$
$$msg_{w0} = EB(w0 \rightarrow msg)$$

Step 7: The RC registers $cRight_{PA}$, $sig_{RC}(cRight_{PA})$, msg, and msg_{w0} to the DB and sends them to the PA also.

3.3 Copyright Add

The primary author requests the collaborator to do adding his or her own copyright. Then, the collaborator requests the center for adding its copyright to the primary author's one. The center verifies the signatures of the primary author and the collaborator respectively. If it succeeds, the center creates the collective copyright and registers it to the DB.

Step 1: The PA generates the add request, $reqAdd_{CA}$, to add the authorship of the CA. Then, the PA signs on the add request to make the signature, $sig_{PA}(reqAdd_{CA})$. The $req\ Add_{CA}$ is composed of the PA's contents, certificate and the CA's certificate.

Step 2: The PA sends $reqAdd_{CA}$, $sig_{PA}(reqAdd_{CA})$, $sig_{PA}(msg)$ to the CA.

Step 3: If the PA's certificate, $cert_{PA}$, is verified as authentic, the CA extracts the PA's public key, pk_{PA}. Then, the CA uses pk_{PA} to verify the signatures, $sig_{PA}(reqAdd_{CA})$ and $sig_{PA}(msg)$. If the hash result of $reqAdd_{CA}$ is not equal to the decrypted result of $sig_{PA}(reqAdd_{CA})$, the CA sends failure notice to the PA. Otherwise, the CA compares the hash result of msg with the decrypted result of $sig_{PA}(msg)$. If two values are not equal, the CA sends failure notice to the PA and terminates the protocol. Otherwise, the CA advances to the step 4.

Step 4: The CA generates $reqMsg_{CA}$ composed of the PA's add request, the PA's signature and the CA's copyright data. Then, the CA signs on the $reqMsg_{CA}$, and makes the multi-signature on the contents, $sig_{CA}(sig_{PA}(msg))$.

$$reqMsg_{CA} = \{reqAdd_{CA}, sig_{PA}(reqAdd_{CA}), cInfo_{CA}\}$$
$$sig_{CA}(reqMsgc_{CA}) = EN_{sk_{CA}}(H(reqMsg_{CA}))$$
$$sig_{CA}(sig_{PA}(msg)) = EN_{sk_{CA}}(sig_{PA}(msg))$$

Step 5: The CA sends $reqMsg_{CA}$, $sig_{CA}(reqMsgc_{CA})$ and $sig_{CA}(sig_{PA}(msg))$ to the RC.

Step 6: The RC verifies the CA's certificate. If it is verified as authentic, the RC extracts the CA's public key. Then, the RC uses pk_{PA} and pk_{CA} to verify the CA's signatures, $sig_{CA}(reqMsgc_{CA})$ and $sig_{CA}(sig_{PA}(msg))$. If verifications are failed, the RC sends failure notice to the CA and terminates the protocol. Otherwise, the RC advances to the step 7.

Step 7: The RC makes the collective copyright, $\square cRight\square_{\downarrow}(PA||CA)$, and signs on it as follows.

$$\square cRight\square_{\downarrow}(PA||CA) = \{\square cInfo\square_{\downarrow}PA\ ||\square cInfo\square_{\downarrow}CA, \square issuer\square_{\downarrow}RC, \square sig\square_{\downarrow}CA\ (\square sig\square_{\downarrow}PA\ (msg)), \square cert\square_{\downarrow}PA\ ||\square cert\square_{\downarrow}CA\}$$
$$cRight_{(PA||CA))}$$

$$\square cRight\square_{\downarrow}(PA||CA) = \{\square cInfo\square_{\downarrow}PA\ ||\square cInfo\square_{\downarrow}CA, \square issuer\square_{\downarrow}RC\}$$

Step 8: The RC scrambles the $\square cRight\square_{\downarrow}(PA||CA)$ with its own secret key.

$$cRight_{(PA||CA))}$$

Step 9: The RC watermarks the signature of step 7 and the encrypted copyright of step 8 as follows.

$$w1 = \{SC(\square cRight\square_{\downarrow}(PA||CA)), \square sig\square_{\downarrow}RC\ (\square cRight\square_{\downarrow}(PA||CA))\}$$

$$msg_{w1} = EB(w1 \rightarrow msg)$$

Step 10: The RC registers $\square cRight\square_{\downarrow}(PA||CA)$, $^{cRight_{(PA||CA))}}$, msg, and msg_{w1} to the DB and sends them to the PA and CA also.

3.4 Collective Copyright Verification

The center extracts the watermark from the contents, and decrypts it to get the collective copyright and the corresponding multi-signature. Then, the center uses them to authenticate copyright holders.

Step 1: The RC extracts the watermark from the contents, msg_{w1}, as follows.

$$w1 = ET(w1 \leftarrow msg_{w1})$$

$$w1 = \{SC(\square cRight\square_{\downarrow}(PA||CA)), \square sig\square_{\downarrow}RC\ (\square cRight\square_{\downarrow}(PA||CA))\}$$

Step 2: The RC descrambles the watermarks with the secret key of its own.

$$\square cRight\square_{\downarrow}(PA||CA) = DESC(SC(\square cRight\square_{\downarrow}(PA||CA)))$$

Step 3: The RC verifies the signature on the collective copyright as follows. If the equation 3.4.1 holds, the RC advances to the step 4. Otherwise, the RC sends failure notice to the verifier, and terminates the protocol.

$$\square cRight\square_{\downarrow}(PA||CA) = \square DE\square_{\downarrow}(\square pk\square_{\downarrow}RC)\ (\square sig\square_{\downarrow}RC\ (\square cRight\square_{\downarrow}(PA||CA))) \quad (3.4.1)$$

Step 4: The RC authenticates the certificates of the PA and the CA respectively. If those are verified as authentic, the RC advances to the step 5. Otherwise, the RC terminates the protocol. Step 5: The RC decrypts the multi-signature with the public keys of the PA and the CA. Then, the RC compares the decrypted result with the hash result of the contents as follows. If two values are equal, the collective copyright is verified as valid. Otherwise, the RC notifies the verifier of the failure on authentication.

$$H(msg) = DE_{\downarrow}(pk_{\downarrow}PA)\ (DE_{\downarrow}(pk_{\downarrow}CA)\ (sig_{\downarrow}CA\ (sig_{\downarrow}PA\ (msg))))$$

4. Security Analysis and Discussion

We analyze the security of the proposed scheme in section 4.1, and discuss its applications in section 4.2.

4.1 Security Analysis

Theorem 1: The collective copyright is safe against masquerade attacks.

(Proof) In section 3.2, the primary author hashes the contents and signs on it. In section 3.3, the collaborator creates the multi-signature with the private key of its own. To forge the multi-signature, the attacker needs the private keys of both the primary author and the collaborator. If it is not available, the attacker should be able to make the key to impersonate the copyright holders. The security of the private key is based on the security of the corresponding public key encryption algorithm. From the assumption 2, the public and private key pairs are generated with a cryptographically secure crypto algorithm, and the key pairs are authenticated by the PKI centers having legal binding forces. The attacker could not extract and make the private key from the data open to the public. Thus, the proposed scheme is safe against masquerade attacks. Q.E.D.

Theorem 2: The multiple authorships on the collective copyright cannot be denied. (Proof) In section 3.4, the center verifies the group signature with the PKI certificates of copyright holders. To deny the signature, the user must prove that the corresponding public key is not belonging to himself or herself. From the assumption 2, the primary author and the collaborator's public keys are authenticated by the PKI center. Thus, those keys are legally bound. In addition, from the assumption 3, the watermarking scheme is also cryptographically secure to insert and extract the copyright. Therefore, the multiple authorships on the collective copyright cannot be repudiated. Q.E.D.

4.2 Discussion

In DRM business models, the specific policies and implementations are varied according to the various business conditions[14]. The proposed collective copyright protection scheme could be best suited to the model like Wisdom Market in which ordinary persons could participate and do business. Our scheme could be used to extend the model and control specific. Existing copyright protection schemes are mainly focusing on the primary author's authorship[15]. But operations of it, with the development of Internet and social network services, co-worked products are growing rapidly today. Thus, we should also consider joint copyright to upgrade and protect the existing business models. The wisdom contents are made of person's ideas and experiences. As these are come from human thoughts, it's not easy to make it a patent. From the result, there exist a lot of contents duplicated or similar. Especially, if the customers prefer to buy the professional contents, the participating rate of ordi-

nary persons would be dropped, because they are lack of capacities to make the professional contents. To promote the Wisdom Market, it's necessary to provide the method of combining other person's copyright to upgrade the contents and extend the sales opportunity. In Information Society, as the people's thoughts are varying each other, the types of software contents are much more various compared to the hardware based products. In this paper, we propose the dynamic copyright protection scheme in which creating and combining multiple authors' rights are possible. The proposed scheme ensures the right of the primary author and can add the select collaborator's right. It also could make the business model flexible to provide weighted profit distribution according to the level of developers.

5. Conclusion

In this paper, the collective copyright protection scheme is proposed suitable for the contents of Collective Intelligence. The proposed scheme is composed of copyright registration, add and verification protocols. We provide the proof of security on our scheme, and discuss the applications. As the proposed scheme could provide to make the joint copyright and combine the existing ones, it's possible to create the new model or extend the existing model suitable for trading contents made of Collective Intelligence

6. Acknowledgment

This work was supported by the ICT R&D program of MSIP/IITP. [2014, Development of distribution and diffusion service technology through individual and collective Intelligence to digital contents]

7. References

1. A Comparative Analysis of Learning Factors through Online Learning and Social Learning. https://www.researchgate.net/publication/301513849_A_Comparative_Analysis_of_Learning_Factors_through_Online_Learning_and_Social_Learning. Date Accessed: 19/10/2015.
2. Want R. iPhone: Smarter than the Average Phone. *IEEE Pervasive Computing*. 2010 Jul-Sep; 9(3):6-9.
3. The app store: The new "must-have" digital business model. http://www.zdnet.com/article/the-app-store-the-new-must-have-digital-business-model/. Date Accessed: 21/01/2010.
4. How Media Companies Can Make Multichannel Networks Profitable. http://www.forbes.com/sites/strategyand/2014/12/19/how-media-companies-can-make-multichannel-networks-profitable/#1a32a1a66876. Date Accessed: 19/12/2014.
5. Zhao J. A WWW service to embed and prove digital copyright watermarks. *Proceeding of the European Conference on Multimedia Application, Services and Techniques*.1996 May, p.1-15.
6. Mason A, Salmon RA, Devlin J. User requirements for watermarking in broadcast applications. *International broadcasting convention (IBC 2000)*, 2000.
7. Piva A, Bartolini F, Barni M. Managing copyright in open networks. *IEEE Internet Computing*. 2002 May-Jun; 6(3):18-26.
8. Business Model Breakdown - Quirky.com. http://www.lumosforbusiness.com/blog/722/28-06-2010/Business+Model+Breakdown++Quirkycom. Date Accessed: 28/06/2010.
9. Rivest R, Shamir A, Adleman L. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM*. 1978 Feb; 21(2):120-26.
10. Taher El Gamal. A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. *IEEE Transactions on Information Theory*. 1985 Jul; 31(4):469-72.
11. Samtani R. Ongoing innovation in digital watermarking. *IEEE Computer Society*. 2009 Mar; 42(3):92-4.
12. Beyond traditional DRM: moving to digital watermarking and fingerprinting in media. http://www.businesswire.com/news/home/20080219005764/en/Traditional-DRM-Moving-Digital-Watermarking-Fingerprinting-Media. Date Accessed: 19/02/1008.
13. Announcing the Advanced Encryption Standard (AES). http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf. Date Accessed: 26/11/2001.
14. Rosenblatt William, Trippe William, Mooney Stephen. Digital Right Management: Business and Technology. John Wiley & Sons, Inc. New York, NY, USA. 2001.
15. Eric Diehl. Securing Digital Video: Techniques for DRM and Content Protection. Springer, 2012 Ed., 2012 Jun.