Research on Credible Regulation Mechanism for the Trading of Digital Works

Guozhen Shi[1], Ying Shen[2(✉)], Fenghua Li[3], Mang Su[4], and Dong Liu[2]

[1] Department of Information Security, Beijing Electronic Science and Technology Institute, Beijing 100070, China
sgz@besti.edu.cn
[2] National Key Laboratory of Integrated Services Network Xidian University, Xi'an 710071, Shaanxi, China
{597917153,136560427}@qq.com
[3] Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100195, China
lifenghua@iie.ac.cn
[4] School of Computer Science and Engineering, Nanjing University of Science and Technology, Nanjing 210094, Jiangsu, China
sml222@163.com

Abstract. The digital works, as a particular commodity in the trading process, which faces with difficulties in counting, content providers can not accurately obtain the actual sales data and even more cannot guarantee the integrity of trading data. This paper presents a trading data management model with a trusted third party of copyright protection. The trusted third-party management platform hedge the uploaded data from authority party and seller party to facilitate to supervise the trading, and effectively resolve credibility and non-repudiation of trading, and then providing the basis proof for the trading count to resolve disputes, at the same time, it make these invisible digital products can be measured. For this reason, it can protect the legitimate interests of publishers and copyright owner.

Keywords: Trading of digital works · Trusted counting · Integrality · Non-repudiation · Supervision

1 Introduction

With the development of computer networks, e-commerce has become an indispensable part of our life. Nowadays, digital products have been traded as commodities. It provides the final readers with a variety of reading ways.

Digital works is different from traditional e-commerce. Due to the digital works are virtual goods, so it is difficult to count, content providers cannot guarantee the integrity of trading data. So how to make trading of digital works become a trusted data that must be addressed immediately.

This paper gave a credible regulatory model of Trading Data Management Platform which is based on the analysis of the traditional trading process, this credible

© Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2015
J. Tian et al. (Eds.): SecureComm 2014, Part I, LNICST 152, pp. 519–523, 2015.
DOI: 10.1007/978-3-319-23829-6_36

supervision platform will hedge the trading data and authorization data to record the whole data that would be an important proof when trading disputes occurs, so it can effectively solve disputes to protect the legitimate interests of publishers and copyright holders.

2 Related Work

At present, publishers generally do not directly deal with the trading. But in domestic, the content vendors rarely settled with publishers directly, the credible settlement mechanism has not been established between the content vendors and publishers. In [1], it describes the basic concepts of digital copyright protection technology and system architecture. The basic principles of Digital Rights Management (DRM) technology was presented in [2], the author analyzes the application at home and abroad. So the standardization of digital works transaction data, fair trade agreement [3, 4] is important to achieve fairness and secure transactions. The certification and authorization management protocol of credible digital products based on PKI technology security were proposed in [5], which not only achieved the authentication among content providers, digital entity and CA, but security and authentication mechanisms of CA is failed. Similarly the literature [6] also analyzed the problem of illegal copying and spread of digital content works and its solutions, but the system security and concurrency there are still some flaws.

3 Credible Regulatory Mechanism of Trading Data Management Platform

3.1 Credible Regulatory Model of Trading Data Management Platform

For digital works, it is not easy to count in the process of trading, lacking of supervision. This paper presents a credible regulatory model in Fig. 1. Sellers and authority party will upload the Right Permission Request data (RPR) and the Right Permission data (RP) to the Trading Data Management Platform to record. When the event of copyright disputes occurs, regulatory authorities can obtain information to arbitrate the disputes. In the trading process, if one party uploaded the data to management platform earlier than other party, and then the management platform will ensure to cache the data. Three parties separately embedded trusted counter among the sales system, the authorization system and Trading Data Management Platform, but the counter that embedded in the sales system and authorization system cannot communicate with each other. Sales (authorized) counter is responsible for generating the RPR (Right Permission Request) or RP (Right Permission data) back to sales (authorization) system, while the data is uploaded to the platform to record. The platform is responsible for receiving data from the credible counter to decrypt and verify data or other process, then return the testing results to the sender, and upload the legal trading data to the data matching central to match, last store these data in the corresponding background database.

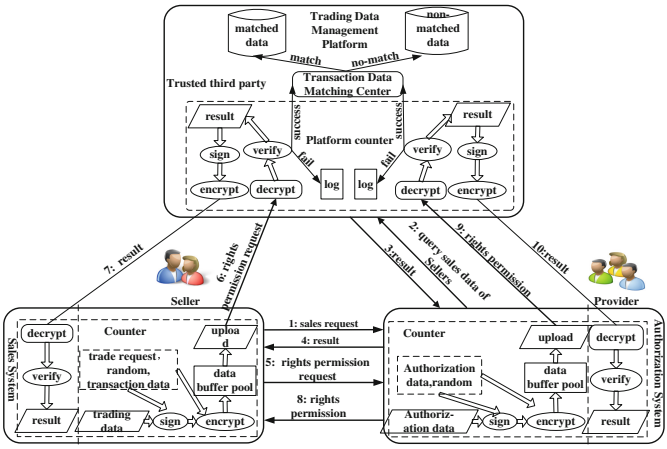

Fig. 1. Credible regulatory model of trading data management platform, it contains three parties, sales system, authorization system and trusted third party.

3.2 Data Upload Protocol

In the process of trading digital works, the premise of purchasing digital works is that consumers have obtained sales permission. Therefore, in order to ensure the integrity, confidentiality and non-repudiation of permission, and the trading metering data is authentic certification and auditable, so the following data upload protocol is designed. The agreement involves the buyers, sellers, authority party, trusted third party that the Trading Data Management Platform and CA. The data upload protocol is shown in Fig. 2:

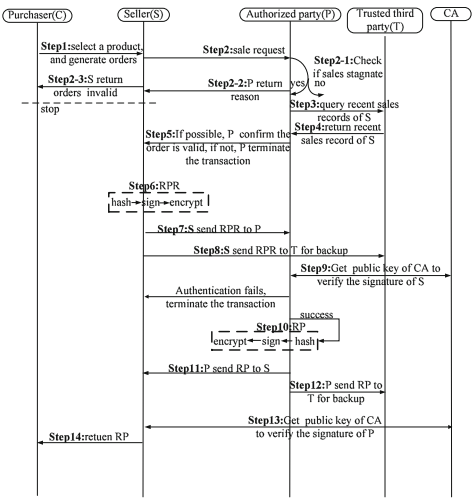

Fig. 2. Data upload protocol process

The data upload protocol during in selling process of digital works is shown in Fig. 2: The procedure described specifically as below:

Step1: A buyer C confirmed the intention to generate purchase orders and send to the seller S.

Step2: After S receives the order, the authority party P asks whether the digital work may sell.

Step3: P sends the seller S's recent sales data to a trusted third party T.

Step4: T queries sales S's recent transaction record, and return to P.

Step5: P can analysis the results returned by T to determine whether sales.

Step6: S processes the basic trade data Ms to Hash, S_RPR_HASH = HASH (Ms, R, Ns), signature processing S_RPR_SIG = ESKs (S_RPR_HASH), after the encryption process MES = EKS ({Ms, R, Ns, S_RPR_SIG}) generated sales request data.

Step7: S send the unencrypted data to P, Mus = {Ms, R, Ns, S_RPR_SIG}.

Step8: S sends the encrypted request data MES to T as a record.

Step9: P gains CA's public key certificate the validity of the content of S certificate; further verify the S's signature S_RPR_SIG.

Step10: P processes the basic authorization data MP, and generates a random number NP to structure authorization data, including {MP, NS, NP}. Then hash processing P_RP_HASH = HASH ({MP, NS, NP}), signature P_RP_SIG = ESKp (P_RP_HASH), encryption MPE = Ekp ({MP, NS, NP, P_RP_SIG}) to generate authorization data.

Step11: P sends unencrypted RP data to S, Mup = {MP, NS, NP, P_RP_SIG}.

Step12: P sends encrypted request permission data MPE to T for the record.

Step13: S verifies the authorization data.

Step14: S will return authorize data to the C.

3.3 Data Hedge

During the trading process, the sales party and authority party were authorized to upload sales data and authorization data to platform. After platform receiving sales data and authorization data, hedging processing and storing the data to the corresponding database. Detailed field contrast shown in Fig. 3:

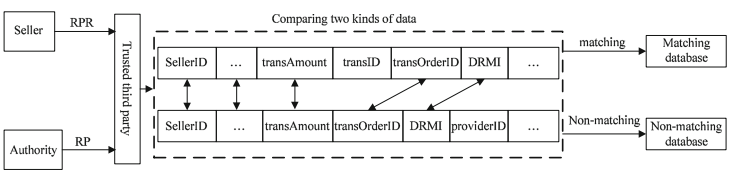

Fig. 3. Data hedging

4 Conclusion

The development of computer network lead to the progress of electronic commerce, such as digital works, however, the special electronic commodity trading faces the reliable counting problems. We present a regulatory model of copyright protection with a trusted third party and use the digital signatures, encryption data of trading process. So we can ensure the transactions and other important data are not tampered, guarantee the transaction data is trusted and reliable, For this reason, copyright legitimate interests of the owner have been fully protected.

Acknowledgement. This work is supported by the National Natural Science Foundation of China (No. 61170251), the Digital Rights Management Technology Research and Development Projects (No. 1681300000119), the Beijing Natural Science Foundation of China (No. 4152048).

References

1. Yu, Y.Y., Tang, Z.: A survey of the research on digital rights management. J. Chin. J. Comput. **28**(12), 1957–1968 (2005)
2. Fan, K.F., Mo, W., Cao, S., Zhao, X.H., Pei, Q.Q.: Advances in digital rights management technology and application. J. Acta Electronica Sinica **35**(6), 1139–1147 (2007)
3. Gao, W., Li, F., Xu, BH.: An abuse-free optimistic fair exchange protocol based on BLS signature. In: Proceedings of the 2008 International Conference on Computational Intelligence and Security (CIS 2008), Suzhou, China, pp. 841–845. IEEE Compute Society (2008)
4. Wang, G.L.: An abuse-fair exchange protocol based on RSA signature. J. IEEE Trans. Inf. Forensics Secur. **05**(1), 158–168 (2009)
5. Xu, L.J., Wang, L.H.: Secure authentication and authorization management protocol for trusted digital content. Appl. Res. Comput. **26**(11), 4325–4328 (2009)
6. Lu, R., Liu, H., Liao, Z.C., Liao, X.H.: Design and implementation of a digital content trading system. J. Comput. Appl. Softw. **28**(8), 135–138 (2011)