Reihaneh Safavi-Naini
Moti Yung (Eds.)

Digital Rights Management
Technologies, Issues, Challenges and Systems

LNCS 3919

First International Conference, DRMTICS 2005
Sydney, Australia, October/November 2005
Revised Selected Papers

Springer

Reihaneh Safavi-Naini Moti Yung (Eds.)

Digital Rights Management

Technologies, Issues Challenges and Systems

First International Conference, DRMTICS 2005
Sydney, Australia, October 31 – November 2, 2005
Revised Selected Papers

Springer

Volume Editors

Reihaneh Safavi-Naini
University of Wollongong, School of IT and CS
Northfields Avenue, Wollongong 2522, Australia
E-mail: rei@uow.edu.au

Moti Yung
RSA Laboratories
and
Columbia University, Department of Computer Science
450 Computer Science Building, New York, NY 10027, USA
E-mail: moti@cs.columbia.edu

Library of Congress Control Number: 2006928038

CR Subject Classification (1998): E.3, D.4.6, F.2.1, C.2, J.1, C.3, K.4.4, K.6.5

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-540-35998-2 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-35998-2 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11787952 06/3142 5 4 3 2 1 0

Lecture Notes in Computer Science 3919

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

Lecture Notes in Computer Science

For information about Vols. 1–3975

please contact your bookseller or Springer

Vol. 4068: H. Schärfe, P. Hitzler (Eds.), Conceptual Structures: Inspiration and Application. XI, 455 pages. 2006. (Sublibrary LNAI).

Vol. 4067: D. Thomas (Ed.), ECOOP 2006 – Object-Oriented Programming. XIV, 527 pages. 2006.

Vol. 4063: I. Gorton, G.T. Heineman, I. Crnkovic, H.W. Schmidt, J.A. Stafford, C.A. Szyperski, K. Wallnau (Eds.), Component-Based Software Engineering. XI, 394 pages. 2006.

Vol. 4060: K. Futatsugi, J.-P. Jouannaud, J. Meseguer (Eds.), Algebra, Meaning and Computation. XXXVIII, 643 pages. 2006.

Vol. 4059: L. Arge, R. Freivalds (Eds.), Algorithm Theory – SWAT 2006. XII, 436 pages. 2006.

Vol. 4058: L.M. Batten, R. Safavi-Naini (Eds.), Information Security and Privacy. XII, 446 pages. 2006.

Vol. 4057: J.P. W. Pluim, B. Likar, F.A. Gerritsen (Eds.), Biomedical Image Registration. XII, 324 pages. 2006.

Vol. 4056: P. Flocchini, L. Gąsieniec (Eds.), Structural Information and Communication Complexity. X, 357 pages. 2006.

Vol. 4055: J. Lee, J. Shim, S.-g. Lee, C. Bussler, S. Shim (Eds.), Data Engineering Issues in E-Commerce and Services. IX, 290 pages. 2006.

Vol. 4054: A. Horváth, M. Telek (Eds.), Formal Methods and Stochastic Models for Performance Evaluation. VIII, 239 pages. 2006.

Vol. 4053: M. Ikeda, K.D. Ashley, T.-W. Chan (Eds.), Intelligent Tutoring Systems. XXVI, 821 pages. 2006.

Vol. 4052: M. Bugliesi, B. Preneel, V. Sassone, I. Wegener (Eds.), Automata, Languages and Programming, Part II. XVIII, 602 pages. 2006.

Vol. 4048: L. Goble, J.-J.C.. Meyer (Eds.), Deontic Logic and Artificial Normative Systems. X, 273 pages. 2006. (Sublibrary LNAI).

Vol. 4046: S.M. Astley, M. Brady, C. Rose, R. Zwiggelaar (Eds.), Digital Mammography. XVI, 654 pages. 2006.

Vol. 4045: D. Barker-Plummer, R. Cox, N. Swoboda (Eds.), Diagrammatic Representation and Inference. XII, 301 pages. 2006. (Sublibrary LNAI).

Vol. 4044: P. Abrahamsson, M. Marchesi, G. Succi (Eds.), Extreme Programming and Agile Processes in Software Engineering. XII, 230 pages. 2006.

Vol. 4043: A.S. Atzeni, A. Lioy (Eds.), Public Key Infrastructure. XI, 261 pages. 2006.

Vol. 4041: S.-W. Cheng, C.K. Poon (Eds.), Algorithmic Aspects in Information and Management. XI, 395 pages. 2006.

Vol. 4040: R. Reulke, U. Eckardt, B. Flach, U. Knauer, K. Polthier (Eds.), Combinatorial Image Analysis. XII, 482 pages. 2006.

Vol. 4039: M. Morisio (Ed.), Reuse of Off-the-Shelf Components. XIII, 444 pages. 2006.

Vol. 4038: P. Ciancarini, H. Wiklicky (Eds.), Coordination Models and Languages. VIII, 299 pages. 2006.

Vol. 4037: R. Gorrieri, H. Wehrheim (Eds.), Formal Methods for Open Object-Based Distributed Systems. XVII, 474 pages. 2006.

Vol. 4036: O. H. Ibarra, Z. Dang (Eds.), Developments in Language Theory. XII, 456 pages. 2006.

Vol. 4035: H.-P. Seidel, T. Nishita, Q. Peng (Eds.), Advances in Computer Graphics. XX, 771 pages. 2006.

Vol. 4034: J. Münch, M. Vierimaa (Eds.), Product-Focused Software Process Improvement. XVII, 474 pages. 2006.

Vol. 4033: B. Stiller, P. Reichl, B. Tuffin (Eds.), Performability Has its Price. X, 103 pages. 2006.

Vol. 4032: O. Etzion, T. Kuflik, A. Motro (Eds.), Next Generation Information Technologies and Systems. XIII, 365 pages. 2006.

Vol. 4031: M. Ali, R. Dapoigny (Eds.), Innovations in Applied Artificial Intelligence. XXIII, 1353 pages. 2006. (Sublibrary LNAI).

Vol. 4029: L. Rutkowski, R. Tadeusiewicz, L.A. Zadeh, J. Zurada (Eds.), Artificial Intelligence and Soft Computing – ICAISC 2006. XXI, 1235 pages. 2006. (Sublibrary LNAI).

Vol. 4027: H.L. Larsen, G. Pasi, D. Ortiz-Arroyo, T. Andreasen, H. Christiansen (Eds.), Flexible Query Answering Systems. XVIII, 714 pages. 2006. (Sublibrary LNAI).

Vol. 4026: P.B. Gibbons, T. Abdelzaher, J. Aspnes, R. Rao (Eds.), Distributed Computing in Sensor Systems. XIV, 566 pages. 2006.

Vol. 4025: F. Eliassen, A. Montresor (Eds.), Distributed Applications and Interoperable Systems. XI, 355 pages. 2006.

Vol. 4024: S. Donatelli, P. S. Thiagarajan (Eds.), Petri Nets and Other Models of Concurrency - ICATPN 2006. XI, 441 pages. 2006.

Vol. 4021: E. André, L. Dybkjær, W. Minker, H. Neumann, M. Weber (Eds.), Perception and Interactive Technologies. XI, 217 pages. 2006. (Sublibrary LNAI).

Vol. 4020: A. Bredenfeld, A. Jacoff, I. Noda, Y. Takahashi (Eds.), RoboCup 2005: Robot Soccer World Cup IX. XVII, 727 pages. 2006. (Sublibrary LNAI).

Vol. 4019: M. Johnson, V. Vene (Eds.), Algebraic Methodology and Software Technology. XI, 389 pages. 2006.

Vol. 4018: V. Wade, H. Ashman, B. Smyth (Eds.), Adaptive Hypermedia and Adaptive Web-Based Systems. XVI, 474 pages. 2006.

Vol. 4016: J.X. Yu, M. Kitsuregawa, H.V. Leong (Eds.), Advances in Web-Age Information Management. XVII, 606 pages. 2006.

Vol. 4014: T. Uustalu (Ed.), Mathematics of Program Construction. X, 455 pages. 2006.

Vol. 4013: L. Lamontagne, M. Marchand (Eds.), Advances in Artificial Intelligence. XIII, 564 pages. 2006. (Sublibrary LNAI).

Vol. 4012: T. Washio, A. Sakurai, K. Nakajima, H. Takeda, S. Tojo, M. Yokoo (Eds.), New Frontiers in Artificial Intelligence. XIII, 484 pages. 2006. (Sublibrary LNAI).

Vol. 4011: Y. Sure, J. Domingue (Eds.), The Semantic Web: Research and Applications. XIX, 726 pages. 2006.

Vol. 4010: S. Dunne, B. Stoddart (Eds.), Unifying Theories of Programming. VIII, 257 pages. 2006.

Vol. 4009: M. Lewenstein, G. Valiente (Eds.), Combinatorial Pattern Matching. XII, 414 pages. 2006.

Vol. 4008: J.C. Augusto, C.D. Nugent (Eds.), Designing Smart Homes. XI, 183 pages. 2006. (Sublibrary LNAI).

Vol. 4007: C. Àlvarez, M. Serna (Eds.), Experimental Algorithms. XI, 329 pages. 2006.

Vol. 4006: L.M. Pinho, M. González Harbour (Eds.), Reliable Software Technologies – Ada-Europe 2006. XII, 241 pages. 2006.

Vol. 4005: G. Lugosi, H.U. Simon (Eds.), Learning Theory. XI, 656 pages. 2006. (Sublibrary LNAI).

Vol. 4004: S. Vaudenay (Ed.), Advances in Cryptology - EUROCRYPT 2006. XIV, 613 pages. 2006.

Vol. 4003: Y. Koucheryavy, J. Harju, V.B. Iversen (Eds.), Next Generation Teletraffic and Wired/Wireless Advanced Networking. XVI, 582 pages. 2006.

Vol. 4001: E. Dubois, K. Pohl (Eds.), Advanced Information Systems Engineering. XVI, 560 pages. 2006.

Vol. 3999: C. Kop, G. Fliedl, H.C. Mayr, E. Métais (Eds.), Natural Language Processing and Information Systems. XIII, 227 pages. 2006.

Vol. 3998: T. Calamoneri, I. Finocchi, G.F. Italiano (Eds.), Algorithms and Complexity. XII, 394 pages. 2006.

Vol. 3997: W. Grieskamp, C. Weise (Eds.), Formal Approaches to Software Testing. XII, 219 pages. 2006.

Vol. 3996: A. Keller, J.-P. Martin-Flatin (Eds.), Self-Managed Networks, Systems, and Services. X, 185 pages. 2006.

Vol. 3995: G. Müller (Ed.), Emerging Trends in Information and Communication Security. XX, 524 pages. 2006.

Vol. 3994: V.N. Alexandrov, G.D. van Albada, P.M.A. Sloot, J. Dongarra (Eds.), Computational Science – ICCS 2006, Part IV. XXXV, 1096 pages. 2006.

Vol. 3993: V.N. Alexandrov, G.D. van Albada, P.M.A. Sloot, J. Dongarra (Eds.), Computational Science – ICCS 2006, Part III. XXXVI, 1136 pages. 2006.

Vol. 3992: V.N. Alexandrov, G.D. van Albada, P.M.A. Sloot, J. Dongarra (Eds.), Computational Science – ICCS 2006, Part II. XXXV, 1122 pages. 2006.

Vol. 3991: V.N. Alexandrov, G.D. van Albada, P.M.A. Sloot, J. Dongarra (Eds.), Computational Science – ICCS 2006, Part I. LXXXI, 1096 pages. 2006.

Vol. 3990: J. C. Beck, B.M. Smith (Eds.), Integration of AI and OR Techniques in Constraint Programming for Combinatorial Optimization Problems. X, 301 pages. 2006.

Vol. 3989: J. Zhou, M. Yung, F. Bao, Applied Cryptography and Network Security. XIV, 488 pages. 2006.

Vol. 3988: A. Beckmann, U. Berger, B. Löwe, J.V. Tucker (Eds.), Logical Approaches to Computational Barriers. XV, 608 pages. 2006.

Vol. 3987: M. Hazas, J. Krumm, T. Strang (Eds.), Location- and Context-Awareness. X, 289 pages. 2006.

Vol. 3986: K. Stølen, W.H. Winsborough, F. Martinelli, F. Massacci (Eds.), Trust Management. XIV, 474 pages. 2006.

Vol. 3984: M. Gavrilova, O. Gervasi, V. Kumar, C.J. K. Tan, D. Taniar, A. Laganà, Y. Mun, H. Choo (Eds.), Computational Science and Its Applications - ICCSA 2006, Part V. XXV, 1045 pages. 2006.

Vol. 3983: M. Gavrilova, O. Gervasi, V. Kumar, C.J. K. Tan, D. Taniar, A. Laganà, Y. Mun, H. Choo (Eds.), Computational Science and Its Applications - ICCSA 2006, Part IV. XXVI, 1191 pages. 2006.

Vol. 3982: M. Gavrilova, O. Gervasi, V. Kumar, C.J. K. Tan, D. Taniar, A. Laganà, Y. Mun, H. Choo (Eds.), Computational Science and Its Applications - ICCSA 2006, Part III. XXV, 1243 pages. 2006.

Vol. 3981: M. Gavrilova, O. Gervasi, V. Kumar, C.J. K. Tan, D. Taniar, A. Laganà, Y. Mun, H. Choo (Eds.), Computational Science and Its Applications - ICCSA 2006, Part II. XXVI, 1255 pages. 2006.

Vol. 3980: M. Gavrilova, O. Gervasi, V. Kumar, C.J. K. Tan, D. Taniar, A. Laganà, Y. Mun, H. Choo (Eds.), Computational Science and Its Applications - ICCSA 2006, Part I. LXXV, 1199 pages. 2006.

Vol. 3979: T.S. Huang, N. Sebe, M.S. Lew, V. Pavlović, M. Kölsch, A. Galata, B. Kisačanin (Eds.), Computer Vision in Human-Computer Interaction. XII, 121 pages. 2006.

Vol. 3978: B. Hnich, M. Carlsson, F. Fages, F. Rossi (Eds.), Recent Advances in Constraints. VIII, 179 pages. 2006. (Sublibrary LNAI).

Vol. 3977: N. Fuhr, M. Lalmas, S. Malik, G. Kazai (Eds.), Advances in XML Information Retrieval and Evaluation. XII, 556 pages. 2006.

Vol. 3976: F. Boavida, T. Plagemann, B. Stiller, C. Westphal, E. Monteiro (Eds.), NETWORKING 2006. Networking Technologies, Services, and Protocols; Performance of Computer and Communication Networks; Mobile and Wireless Communications Systems. XXVI, 1276 pages. 2006.

Preface

The First International Conference on Digital Rights Management: Technology, Issues, Challenges and Systems (DRMTICS – pronounced 'dramatics'), took place in Sydney, Australia on 31st October - 2nd November, 2005. It was organized by the Centre for Information Security of the University of Wollongong and in cooperation with the International Association of Cryptologic Research (IACR) and IEEE Computer Society's Task Force on Information Assurance.

DRMTICS is an international conference series that covers the area of digital rights management, including research advancements of an applied and theoretical nature. The goal is to have a broad coverage of the field and related issues and subjects as the area evolves. Since the Internet and the computing infrastructure has turned into a marketplace for content where information goods of various kinds are exchanged, this area is expected to grow and be part of the ongoing evolution of the information society. The DRM area is a unique blend of many diverse disciplines that include mathematics and cryptography, legal and social aspects, signal processing and watermarking, game theory, information theory, software and systems design and business analysis, and DRMTICS attempts to cover as much ground as possible, and to cover new results that will further spur new investigations on the foundations and practices of DRM. We hope that this first conference marks the beginning of a fruitful and useful series of future conferences.

This year, the conference received 57 submissions out of which 26 were accepted for presentation after a rigorous refereeing process. In addition to the regular program, the program also included invited talks and a panel discussion. Renato Ianella gave an invited talk describing "A Brief History of Right Expression Languages," Moni Naor gave a talk entitled "Humans, Computers and Cryptography," and Karen Gettens gave a talk on "DRM– the Legal Issues." The panel was chaired by Bill Caelli and was entitled "Is Reliable and Trusted DRM Enforcement Realistic or Even Possible?"

We wish to thank all the authors of submitted papers for providing the content of this year's workshop; their high quality submissions made the task of selecting a program hard. We would also like to thank the program committee members as well as the external reviewers, who helped in the refereeing process. We wish to thank our sponsors: Smart Internet Technology CRC, Motorola, DigiSensory Technologies, The Telecommunications and Information Technology Research Institute of the University of Wollongong, Research Network for a Secure Australia, Infosys and Markany. We further wish to thank the attendees, speakers and the participants, as well as Susan Branch, Debbie Farrelly, Harikrishna Vasanta, Wenming Lu, Liang Lu, Rungrat Wiangsripanawan, Siamak Fayyaz-Shahandashti, Angela Piper and Martin Surminem, who helped with the organization of the conference.

Last but not least, we would like to thank Wanqing Li and Nicholas Sheppard, general co-chairs of the conference, for their relentless effort in organizing the event and paying attention to every detail, which made DRMTICS a good drama, but one without unnecessary, unexpected dramatic moments! Without the help of the above bodies and individuals this inaugural conference would not have been a possibility.

November 2005

Rei Safavi-Naini
Moti Yung

Organization

General Chairs

Wanqing Li	University of Wollongong, Australia
Nicholas Sheppard	University of Wollongong, Australia

Program Chairs

Rei Safavi-Naini	University of Wollongong, Australia
Moti Yung	Columbia University and RSA Security, USA

Program Committee

Feng Bao	Institute for Infocomm Research, Singapore
Stefan Bechtold	Max Planck Institute for Collective Goods, Germany
Jong Uk Choi	MarkAny, Korea
Christian S. Collberg	University of Arizona, USA
Ingemar Cox	University of London, UK
Ezzy Dabbish	Motorola Labs, USA
Jana Dittmann	University of Magdeburg, Germany
Yevgeniy Dodis	New York University, USA
Brian Fitzgerald	Queensland University of Technology, Australia
Susanne Guth	ODRL Initiative, Austria
Greg Heileman	University of New Mexico, USA
HweeHwa Pang	Singapore Management University, Singapore
Hideki Imai	University of Tokyo, Japan
Sushil Jajodia	George Mason University, USA
Ton Kalker	Hewlett-Packard Labs, USA
Stefan Katzenbeisser	Technical University of Munich, Germany
Aggelos Kiayias	University of Connecticut, USA
Kwangjo Kim	Information and Communication University, Korea
Kaoru Kurosawa	Ibaraki University, Japan
Jeff Lotspiech	IBM Almaden, USA
Stefan Nusser	IBM Almaden, USA
Josef Pieprzyk	Macquarie University, Australia
Bin Zhu	Microsoft Research Asia, China

External Reviewers

Yongdong Wu
Yuichi Kaji
Takao Nishizeki
Tomoyuki Asano
Katsunari Yoshioka
Goichiro Hanaoka
Carl Bosley
Nelly Fazio
Christopher Peikert
Prashant Puniya
Kevin Kloker
David Kravitz
Tom Messerges
Kohich Kamijoh
Deepa Kundur
Jong W. Kim
Dinesh Dhanekula
Pramod Jamkhedkar
Fabricio Ourique
Angela Piper
Wenming Lu
Nicholas Sheppard
Harikrishna Vasanta

Sponsoring Institutions

DigiSensory Technologies, Australia
Infosys, India
MarkAny, Korea
Motorola, USA
Research Network for a Secure Australia, Australia
Smart Internet CRC, Australia
Telecommunications and Information Technology Research Institute, University of Wollongong, Australia

Table of Contents

Assurance and Authentication Issues

Legal and Related Issues

Expressing Rights and Management

Watermarking

Software Issues

Fingerprinting and Image Authentication

Supporting Cryptographic Technology

P2P Issues

Implementations and Architectures

A Novel Framework for Multiple Creatorship Protection of Digital Movies

Yu-Quan Zhang and Sabu Emmanuel

School of Computer Engineering,
Nanyang Technological University
{zh0004an, asemmanuel}@ntu.edu.sg

Abstract. A digital movie can be created jointly under the cooperation of many creators. It is then necessary to provide protection to the creatorship of each participating creator. In this paper, we propose a framework for providing the creatorship protection of multiple creators involved in creating the object-based digital movie. The proposed framework makes use of digital watermarking techniques and cryptographic protocols to achieve the creatorship protection purpose. Object-based movie may consist of several audio and video objects, which may be created by different creators. The proposed framework embeds different watermarks in different video/audio objects in such a way that each creator can show the joint-creatorship of the movie; as well as each creator can prove his/her creatorship of video/audio object he/she created.

1 Introduction

Nowadays, digital rights management (DRM) issue is discussed more and more since a large amount of digital assets involving media such as text, audio, video etc. are being created. The parties involved in the digital asset creation and transaction are creators, owners, distributors and consumers. Creators have creator rights, owners have owner rights, distributors have distributor rights and consumers have consumer rights. DRM refers to a set of technologies and approaches that establish a trust relationship among the parties involved in a digital asset creation and transaction [16]. Cryptographic techniques and watermarking techniques are important tools in DRM. Cryptographic techniques provide confidentiality, authentication, data integrity, and non-repudiation functions. Watermarking techniques are usually preferred for copyright ownership declaration, creator/authorship declaration, copyright violation detection, copyright violation deterrence, copy control, media authentication, and media data integrity functions. Our proposed framework employs both cryptographic and watermarking techniques to protect the creatorship of multiple creators involved in the creation of object-based digital movie.

The creator has creatorship of digital assets. Many digital media are very complex and almost impossible to be created by single creator. For example, in an image creation, some creators may be good at drawing the plants; some may be good at drawing animals and some may be good at drawing human beings; or in another way, some may do well in sketching the skeleton of the images and others may be good at coloring. Therefore, to create a good complex image, which contains lots of contents

R. Safavi-Naini and M. Yung (Eds.): DRMTICS 2005, LNCS 3919, pp. 1 – 12, 2006.

inside, the whole creation process needs the cooperation of many creators. Another example, in a cartoon movie, different cartoon characters may be created by different video creators and the associated audio dialogues may be dubbed by many audio dubbers. In addition the background music including special effects and foreground music may be created by many creators. Therefore creating a complex cartoon movie may involve many creators from video and audio domains.

In the case of joint creation of digital media by multiple creators, there are some concerns for each of the participating creators. Firstly, it is possible that a creator disowns his/her object at a later stage due to the malpractices (copying from someone else's work etc.) he/she has done during the creation. This disowning may cause unnecessary hardships for the good creators. Secondly, a creator may pose as the sole creator and sell the product to a buyer. These concerns arise mainly due to the mistrust among the creators. Our proposed framework intends to build the trust relationship among the creators involved in joint creations.

There are different kinds of digital media such as image, video, movie etc. In this paper, we focus on the creatorship protection of multiple creators of object-based digital movies. The digital graphics (cartoon) movies may be an example. The creation process of an object-based movie consists of video creation process and audio creation/dubbing process. In the video creation process, each video creator works on one or more video objects and then they refine their creations through several iterations. Usually the audio dubbing is carried out after the video creation process. The background and foreground musics are created by audio creators and are then dubbed along with the dialogs of characters into the movie. The audio dubbing also employs iterative procedures to refine the audio part of the movie.

We in this paper propose a novel framework to address the creatorship concerns of multiple creators of object-based movies (such as digital graphics/cartoon movies). We make use of watermarking techniques and cryptographic protocols for the framework. The watermarking scheme that the framework employs has certain requirements such as robustness, imperceptibility, asymmetric and non-invertibility. So that it can perform well under the complex joint creation situation to achieve the creatorship protection purpose. Cryptographic protocols require the use of digital signature algorithms.

The remainder of the paper is structured as follows: Section 2 discusses related watermarking and cryptographic schemes. Our proposed framework is presented in Section 3. Section 4 lists some application of our framework. Section 5 presents discussion and Section 6 concludes the paper.

2 Related Watermarking and Cryptographic Schemes

So far, there are quite few watermarking schemes considering the joint-creatorship protection problem. Guo and Georganas [8] introduce a digital image watermarking scheme for joint-ownership verification. The scheme that they used embeds a combined watermark of the creators' individual watermarks and a jointly created watermark, and then verifies the partial ownership and full ownership by setting different levels of thresholds in the detector. This scheme is not suitable for protecting the creatorship of multiple creators in a joint creation environment. It does not provide

the protection during the creation process, and each creator cannot specify which video/audio object is created by him/her. For joint-creatorship protection, the scheme needs to provide the protection during the creation process, so it can take care of the two concerns we mentioned in the introduction, which may occur in the creation process. At the same time, single creator should have the ability to show which video/audio object was created by him/her. Our framework gives a solution to this type of problem for object-based movie creation.

Our framework employs both watermarking scheme and cryptographic protocol. The watermarking scheme is mainly used for creatorship protection and the cryptographic protocol is mainly used for digital signature purpose. Some research work on watermarking and digital signature scheme are reviewed below.

There have been many researches done in watermarking area [1][2]. The work by Cox et. al. [3] is spread spectrum based watermark, which is robust and invisible. Being robust watermark, it would be hard for the attackers to make undetectable or remove the watermark. The watermarking techniques proposed in [4] and [5] are asymmetric. The asymmetric watermarks make use of another key for embedding other than the detection key. Thus it would be hard for the watermark verifier to perform watermarking but can detect the watermark. Craver et.al. [6], Qiao and Nahrstedt [7], give a non-invertible watermarking scheme. In order to prove the rightful owner unambiguously, the watermarking scheme should be non-invertible.

Many audio and speech watermarking schemes have been proposed. The dialog in the movie can be seen as speech; the background music and foreground music can be seen as audio. Bassia et. al. [9] applies a straightforward time-domain spread-spectrum watermarking method to audio signals. An audio watermarking technique based on correlation detection is introduced in [13], where high-frequency chaotic watermarks are multiplicatively embedded in the low frequencies of the DFT domain.Wu et.al. [10] propose a low complexity speech-Watermarking scheme as an effective way to detect malicious content alterations while tolerating content preserving operations. The proposed scheme is based on the modified odd/even modulation scheme with exponential scale quantization and a localized frequency-masking model while assuring no mismatch between quantization steps used in watermark embedding and detection. Cheng et. al. [12] propose a speech watermarking technique in which maximum possible watermark signal energy is added to the speech signal satisfying the constraint that the added signal is not audible. Additional watermark energy is embedded into the portions of the speech that have white spectrum, fricative sounds and rapidly changing plosives sounds.

There are many digital signature schemes available such as RSA [14], Digital Signature Algorithm (DSA) and Elliptic Curve Digital Signature Algorithm (ECDSA). Recent years, some new schemes have been proposed. Elkamchouchi et. al. [11] have developed a digital signature scheme with appendix and message recovery in the real and Gaussian integers' domains. The proposed scheme employs the idea of combining the integer factorization, and the Generalized Discrete Logarithm problems. Chang et. al. [15] have proposed a secure digital signature scheme, where neither one-way hash functions nor message redundancy schemes are employed. We can apply any digital signature scheme in our framework as far as it can perform the digital signature safely.

3 Our Proposed Framework

In our proposed framework, a digital movie creation has two stages: video creation process and audio creation/dubbing process. Fig. 1 gives the flowchart of the whole digital movie creation process.

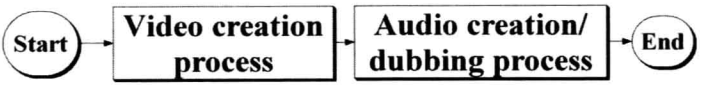

Fig. 1. The digital movie creation process

***Brief Description*:** In the proposed framework the movie creation begins with a video creation process. First, each video creator creates his/her video object. The created video object is then watermarked and signed by the creator and transmitted over the network to other participating video creators. On receiving every others signed watermarked video objects, each video creator then assembles a local video part of the movie by combining every others watermarked video objects and own watermarked video object. The video creators then carry out refinement iterations on their video objects until all the video creators are satisfied with the video part of the movie. The video creators can create their video objects in their own local machine as shown in Fig. 2 and they exchange their creations through the network to every other creators.

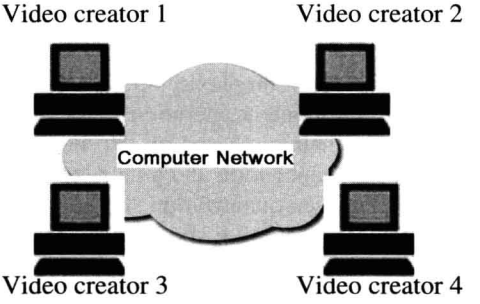

Fig. 2. Hardware infrastructure of the video creation process

Once the video part of the movie is completed, the audio creation/dubbing process begins. Some audio components such as background and foreground music may be created beforehand by some audio creators. Dubbing of all the audio components such as background music, foreground music and the dialogs of characters on to the movie usually will be done in real time while the video is playing. Different audio components can be recorded on different tracks and can be treated as different audio objects. For example, the background music can be one audio object, the dialogs of each character can be considered as individual audio objects. Each audio creator also gets a signed watermarked copy of every audio object. The audio dubbing is also done in