Digital rights management for multimedia in a collaborative environment

Zhang, Yuquan

2006

Zhang, Y. (2006). Digital rights management for multimedia in a collaborative environment. Master's thesis, Nanyang Technological University, Singapore.

<https://hdl.handle.net/10356/35723>

<https://doi.org/10.32657/10356/35723>

9455755

Digital Rights Management for Multimedia in a Collaborative Environment

Zhang Yuquan

School of Computer Engineering

A thesis submitted to the Nanyang Technological University
in fulfilment of the requirement for the degree of
Master of Engineering

2006

Acknowledgement

I would like to express sincere appreciation to my supervisor, Assistant Professor Sabu Emmanuel, for his patient and altruistic assistance throughout my research.

I would give my thankfulness to Dr. Tzeng Jengnan for his kindly help.

Last but not least, I wish to say thanks to my family and all the people who provided me with continued support and understanding.

Abstract

With the increase in complexity of multimedia data, digital media creation is often carried out jointly. It is then necessary to provide protection to the creatorship of each participating creator. We call this a joint creatorship protection problem. Digital watermarking technology proposed in recent years is a new technology for copyright protection and authentication of digital contents. But there are very few watermarking frameworks for the joint creatorship protection problem.

Our research mainly focuses on the joint-creatorship protection for digital multimedia. We reviewed recent years development of watermarking techniques. Then, we developed three novel digital watermarking frameworks to address the problem of joint-creatorship protection of images, object-based videos and object-based movies. We have also developed a watermarking scheme which can be employed by the watermarking framework.

In our frameworks, the multimedia products are produced in an iterative manner, since it is difficult to finish the whole product in single iteration. Our framework is also suitable for the situation where the co-operating creators are located far from each other but connected through the network. I.e., the co-operating creators need not necessarily come together to produce a digital multimedia product; instead they can sit before their own workstations to work, then transmit and discuss the product over the network. The proposed frameworks make use of digital watermarking techniques and cryptographic protocols. All the three frameworks embed multiple watermarks in a non-overlapping manner in the multimedia data during the creation process. We have developed the watermarking schemes for the frameworks. The watermarking schemes have the

properties of robustness, imperceptibility, asymmetry and non-invertibility. The complexities of the frameworks are analyzed by calculating the data transmission and storage requirements, and the results show that all the three frameworks can solve the joint-creatorship protection problem with reasonable storage and transmission requirements.

Table of Contents

Acknowledgement	i
Abstract	ii
Table of Contents	iv
List of Figures	vii
List of Publications	ix
CHAPTER 1 INTRODUCTION.....	1
1.1 An Overview of DRM in Digital Multimedia	1
1.2 Motivation and Objective.....	2
1.3 Our Contributions.....	3
1.3.1 Framework for Jointly Created Image	3
1.3.2 Framework for Jointly Created Object-Based Video.....	4
1.3.3 Framework for Jointly Created Digital Movie.....	5
1.3.4 Our Designed Watermarking Scheme.....	6
1.4 Organization of the Thesis	6
CHAPTER 2 LITERATURE REVIEW AND BACKGROUND THEORY	7
2.1 Multimedia Watermarking Techniques.....	7
2.1.1 Background	7
2.1.2 Overview	7
2.1.3 Digital Watermarking	8
2.1.4 Some Watermarking Techniques	11
2.1.5 Watermark Applications and Robustness	12
2.1.6 Future of Digital Watermarking.....	15
2.2 Literature Review of Related Work.....	17
2.2.1 Image Watermarking Schemes	17
2.2.2 Video Watermarking Schemes.....	18
2.2.3 Watermarking Schemes Related to our Work.....	19
2.3 Digital Signature Schemes.....	21
2.3.1 Background Theory.....	21
2.3.2 Related Digital Signature Schemes.....	22
CHAPTER 3 JOINT-CREATORSHIP PROTECTION FOR DIGITAL IMAGES ..	23
3.1 Introduction.....	24

3.2 Risks in Joint Creation 25

3.3 Framework for Parallel Process 26

3.4 Framework for Sequential Process 34

3.5 Applications of our Framework 37

 3.5.1 Creatorship Verification by Judge 37

 3.5.2 Creatorship Verification by Buyer 37

3.6 Complexity Analysis of Parallel Process 38

 3.6.1 Data Transmission Complexity 38

 3.6.2 Storage Complexity 39

3.7 Complexity Analysis of the Sequential Process 40

 3.7.1 Transmission Complexity 40

 3.7.2 Storage Complexity 41

3.8 Experimental Results 42

 3.8.1 Number of Bytes Transmitted 42

 3.8.2 Storage requirements 43

3.9 Conclusion 44

CHAPTER 4 JOINT-CREATORSHIP PROTECTION FOR DIGITAL VIDEOS .. 45

4.1 Introduction 45

4.2 Risks in Joint Creation 46

4.3 Our Proposed Watermarking Framework 47

 Video Creation Process 48

4.4 Complexity Analysis of our Framework 55

 4.4.1 Transmission Complexity 55

 4.4.2 Storage Complexity 58

4.5 Application of our Framework 59

 4.5.1 Rightful Creatorship Dispute Resolution 59

 4.5.2 Creatorship Purchasing Situation 60

 4.5.3 Creatorship Replacement Dispute Resolution 60

4.6 Conclusion 61

CHAPTER 5 JOINT-CREATORSHIP PROTECTION FOR DIGITAL MOVIES.. 62

5.1 Introduction 62

5.2 Our Proposed Framework 64

5.2.1 Initialization Process	66
5.2.2 The Video Creation Process.....	67
5.2.3 The Audio Creation/Dubbing Process	71
5.2.4 Registration Process.....	74
5.3 Applications of the Proposed Framework	75
5.3.1 Rightful Creatorship Dispute Resolution.....	75
5.3.2 Creatorship Purchasing Situation.....	76
5.3.3 Creatorship Replacement Dispute Resolution	76
5.4 Complexity Analysis of the Proposed Framework.....	77
5.4.1 Complexity in Video Creation	77
5.4.1.1 Transmission Complexity for Video.....	78
5.4.1.2 Storage Complexity for Video	80
5.4.2 Complexity in Audio Creation.....	82
5.4.2.1 Transmission Complexity for Audio.....	82
5.4.2.2 Storage Complexity for Audio	82
5.4.3 Total Complexity	83
5.4.3.1 Total Transmission Complexity.....	83
5.4.3.2 Total Storage Complexity	83
5.5 Experimental Results.....	84
5.5.1 Number of Bytes Transmitted.....	84
5.5.2 Storage Requirements	85
5.6 Discussion.....	86
5.7 Conclusion.....	86
 CHAPTER 6 OUR WATERMARKING SCHEME.....	 88
6.1 Watermark Construction	89
6.2 Watermark Embedding.....	90
6.3 Watermark Detection	91
6.4 Discussion.....	92
6.5 Testing Results.....	92
 CHAPTER 7 CONCLUSION AND FUTURE WORK	 95
7.1 Our Achievements.....	96
7.2 Future Work.....	98
 References	 xi

List of Figures

Figure 2.1: Generic digital watermarking scheme	10
Figure 2.2: Generic watermark recovery/detection scheme	11
Figure 3.1: the infrastructure of the proposed framework	27
Figure 3.2: The whole creation process	28
Figure 3.3 (a): the whole area is divided into N sub-areas.....	28
(b): watermarked image I_1^w after first iteration	28
Figure 3.4: Step 1 of parallel process.....	29
Figure 3.5: Step 2 of parallel process.....	30
Figure 3.6: Step 3 of parallel process.....	31
Figure 3.7 (a): whole area before j^{th} iteration	31
(b): watermarked image I_j^w after j^{th} iteration	31
Figure 3.8: Step 4 of parallel process.....	32
Figure 3.9: Step 5 of parallel process.....	32
Figure 3.10: Registration step	33
Figure 3.11: First iteration of sequential process.....	35
Figure 3.12: Refinement iterations of sequential process	35
Figure 3.13: Data transmitted against iteration number.....	39
Figure 3.14: Storage requirement against number of iterations.....	40
Figure 3.15: Transmitted bytes of 100 random modification rate	43
Figure 3.16: Storage requirements of 100 random modification rate.....	43
Figure 4.1: Physical infrastructure of the framework	49
Figure 4.2: Flowchart of initialization step.....	50
Figure 4.3: Flowchart of step 1	51
Figure 4.4: n^{th} frame after first iteration.....	51
Figure 4.5: Flowchart of step 2	52
Figure 4.6: Flowchart of step 3	52
Figure 4.7: Flowchart of step 4	53
Figure 4.8: Flowchart of step 5	53
Figure 4.9: The flowchart of Registration Step	54
Figure 4.10: n^{th} frame of final video after J^{th} iteration.....	55
Figure 4.11: Total data transmitted for $f_{ij}=1$	57
Figure 4.12: Total data transmitted for $f_a = 1/2$	57
Figure 4.13: Total storage requirement against the number of iterations	59
Figure 5.1: The digital movie creation process.....	64
Figure 5.2: Hardware infrastructure of the video creation process.....	65
Figure 5.3: Hardware infrastructure of audio creation process.....	66
Figure 5.4: Initialization process.....	67
Figure 5.5: First iteration of video creation process	69
Figure 5.6: The n^{th} frame after first iteration	69
Figure 5.7: Refinement iterations of video creation process	71

Figure 5.8: The n^{th} frame of the final video after J^{th} iteration..... 71

Figure 5.9: The first iteration in the audio creation process 73

Figure 5.10: Refinement iterations of audio creation process 74

Figure 5.11: Registration step 75

Figure 5.12: Total data transmitted against iteration number ($f_{ij} = 1$)..... 79

Figure 5.13: Total data transmitted against the iteration number ($f_{ij} < 1$)..... 80

Figure 5.14: Storage requirement for single video creator 81

Figure 5.15: Total system-wide storage requirements 83

Figure 5.16: Total data transmitted of 100 Experiments 84

Figure 5.17: Total storage requirements of 100 experiments 85

Figure 6.1: (a) Original image (b) Watermarked image ($\beta=4$) 93

Figure 6.2: PSNR under different scaling factor β 93

List of Publications

Journal paper:

Yu-Quan Zhang, Sabu Emmanuel, "A Novel Creatorship Protection Framework for Digital Images", in Journal of Ubiquitous Computing and Intelligence, issue 3, 2006

Conference paper:

Yu-Quan Zhang, Sabu Emmanuel, "A Novel Framework for Object-Based Video Multiple Creatorship Protection", in the Proceedings of the 4th Int'l Symposium on Image and Signal Processing and Analysis, Zagreb, Croatia, 2005, pp. 227-232

Yu-Quan Zhang, Sabu Emmanuel, "A Novel Watermarking Framework for Joint-Creatorship Protection", in the Proceedings of International conference on CYBERWORLDS, Singapore, Nov 2005, pp. 109-116

Yu-Quan Zhang, Sabu Emmanuel, "A Novel Framework for Multiple Creatorship Protection of Digital Movies", in proceedings of first international conference on DRMTICS, Sydney, Australia, Oct 2005, pp. 1-12

Chapter 1

Introduction

The topic of this thesis is the digital rights management (DRM) for digital multimedia in a collaborative environment. The research focuses on the digital rights of the creators in a jointly/collaboratively created digital media.

This chapter provides a general introduction of this thesis. In section 1.1, we will briefly introduce the concept of digital rights management in digital multimedia. Then, we explain the motivations and objectives in this research topic in section 1.2. Section 1.3 presents the major contributions of our research work. Finally, section 1.4 gives the organization of the whole thesis.

1.1 An Overview of DRM in Digital Multimedia

As more and more digital assets containing multimedia are being produced, the digital rights management for digital multimedia becomes a big issue. The parties involved in the digital multimedia product creation and transaction are creators, owners, distributors and consumers. Each of these parties has their own rights namely, creators have creator rights, owners have owner rights, distributors have distributor rights and consumers have consumer rights. It is to be noted that there can be multiple creators jointly creating a digital asset and likewise, multiple owners jointly owning a digital asset. 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 [52]. Cryptographic techniques and

CHAPTER 1 INTRODUCTION

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.

During past decades, there are lots of cryptographic protocols [52][53][54] and watermarking schemes [1][2][3] developed and the researchers are still improving them and developing new schemes nowadays.

1.2 Motivation and Objective

The research work presented in this thesis focuses on the joint-creatorship protection problem for the jointly/collaboratively created digital multimedia products. With the rapid development in the digital creation and delivery technologies, lots of digital multimedia data are created and transacted everyday. The contents of the digital multimedia are more and more complex, and another fact is that different creators are good at different techniques. So instead of creating everything by single creator, the digital multimedia are often created jointly in order to maximally utilize the strongpoint of different creators. But at the same time, new problems rise up with the joint creation of digital multimedia. In the scenario of joint creation, it is possible that a group of creators (or a creator) can connive to remove another creator (or another group of creators) from creatorship of the final product. If one of the creators creates his/her creation illegally (copying from someone else's copyrighted work etc.), the rest innocent creators are not supposed to take responsibility. Thus, each creator is concerned about his/her rightful share of creatorship of the final product. How to protect each creator's creatorship in a collaborative environment becomes a big challenge.

CHAPTER 1 INTRODUCTION

In this thesis, we address this kind of joint-creatorship protection problem by designing novel watermarking frameworks, which employ both cryptographic protocol and watermarking scheme. With the help of our watermarking frameworks, the creators of an image are able to establish and prove their contributions and amount of contribution to buyers of jointly created image; the creators of an object-based video are able to establish the creatorship of specific video object and joint-creatorship for the whole video. We have also designed framework for object-based digital movies, where video creators and audio creators can protect their creatorship for their objects. In one word, our framework builds up the trust relationship among the creators involved in a joint creation. The cryptographic protocol used in the frameworks is asymmetric and any secure asymmetric digital signature scheme can be used. The watermarking technique employed by the framework is robust, invisible, non-invertible and asymmetric. With these properties, the creators can successfully protect their creatorship without affecting the quality of the digital multimedia.

1.3 Our Contributions

This thesis presents frameworks for creatorship protection for digital multimedia. We designed three frameworks which are for jointly created image, jointly created object-based video and jointly created digital movie respectively. We have also developed a watermarking scheme which is robust, imperceptible, asymmetric and non-invertible. The watermarking scheme can be applied to the three frameworks mentioned above in order to achieve creatorship protection.

1.3.1 Framework for Jointly Created Image

We have developed a watermarking framework for jointly created digital images. The digital images can be created in either parallel process or sequential process. Our

CHAPTER 1 INTRODUCTION

framework embeds multiple watermarks into the images in a non-overlapping manner to ensure imperceptibility. And from distinct watermarks of different creators, people can know each creator's contribution. The framework is applied during the image creation process for both parallel process and sequential process. The framework supports the following. First, a creator or a group of creators are not able to connive to remove the creatorship of another creator. Second, a creator cannot disown his/her own part of the joint creation. Third, a creator cannot pose as the sole creator and sell the product to a buyer.

We have also developed a watermarking scheme for our designed framework for images. The watermarking scheme has the properties of non-invertibility, asymmetry, robustness and invisibility. Our framework requires the watermarking scheme to have these properties in order to protect the creators' creatorship in a collaborative environment. The watermarking framework can be applied in rightful creatorship resolution and image purchasing situation. The complexity of the framework is analyzed by calculating the data transmission and storage requirements, and the experimental results show that the framework can address the joint-creatorship protection problem with low storage and transmission requirements.

1.3.2 Framework for Jointly Created Object-Based Video

We also developed a framework for object-based video joint-creatorship protection. Object-based video may contain many video objects, which are created by different creators. The framework first embeds a jointly created watermark into the background object. Then the framework embeds different watermarks in different video objects in such a way that each creator can show the joint-creatorship of the whole video; as well as each creator can prove his/her creatorship of video object he/she created. The

CHAPTER 1 INTRODUCTION

complexities of the frameworks are analyzed by calculating the amount of data transmission and storage requirements.

The framework requires a watermarking scheme with the properties of non-invertibility, asymmetry, robustness and imperceptibility. We have developed a watermarking scheme which satisfies all the above requirements. By employing this watermarking scheme and a secure digital signature scheme, the framework can help to protect the creatorship without the degradation of the video quality.

1.3.3 Framework for Jointly Created Digital Movie

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 creators. 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 watermarks are embedded in a non-overlapping manner in order to not degrade the visual and audio quality of the movie. Each creator can show his/her creatorship on his/her object since they will use their own watermarks. Different creators will use different watermarks. The creators also can together show the full creatorship of the movie. We have also developed a watermarking scheme with the properties of robustness, imperceptibility, asymmetry and non-invertibility. The watermarking scheme satisfies all the requirements of our watermarking framework. The watermarking scheme can be applied in the rightful creatorship dispute resolution, movie purchase situation and creatorship replacement dispute resolution. The complexity of the framework is analyzed by calculating the amount of data transmission

CHAPTER 1 INTRODUCTION

and storage requirements. Experiments were conducted to study the effectiveness of the framework.

1.3.4 Our Designed Watermarking Scheme

The designed frameworks require a robust, imperceptible, asymmetric and non-invertible watermarking scheme. Therefore, we have built a watermarking scheme that satisfies all the above requirements. The watermarking scheme can be applied to all of the three watermarking frameworks.

1.4 Organization of the Thesis

The remainder of this thesis is organized as follow: Chapter 2 gives the review of watermarking scheme development and some related works. Chapter 3 introduces framework for joint-creatorship protection for digital images. In chapter 4, the framework for object-based videos joint-creatorship protection is presented. The framework for jointly created object-based digital movies is given in chapter 5. Chapter 6 presents the watermarking scheme and chapter 7 concludes this thesis.

Chapter 2

Literature Review and Background Theory

In this chapter, we first discuss the background theory on multimedia watermarking technology in section 2.1; then we introduce the watermarking schemes related to our framework in section 2.2. In section 2.3, we present the cryptographic protocols suitable for our framework.

2.1 Multimedia Watermarking Techniques

2.1.1 Background

Multimedia watermarking technology has evolved very quickly during the last few years [1]. A digital watermark is information embedded in the host media data. A watermark typically contains information about the origin, status, or recipient of the host data. Applications of watermark include copyright protection, data monitoring, and data tracking, data authentication etc.

2.1.2 Overview

The advantages of digital processing and distribution, like noise-free transmission, software instead of hardware processing, and improved reconfigurability of systems, are all well known and obvious. But, the possibility for unlimited copying of digital data without loss of fidelity is undesirable because it may cause considerable financial loss.

One method for the protection of intellectual property rights (IPR) is the embedding of digital watermarks into multimedia data. The watermark is a digital code embedded in

CHAPTER 2. BACKGROUNDS AND RELATED WORKS

the host data and typically contains information about origin, status, and/or destination of the data. Although not directly used for copy protection, it can at least help identifying source and destination of multimedia data and, as a “last line of defense,” enable appropriate follow-up actions in case of suspected copyright violations.

While copyright protection is the most prominent application of watermarking techniques, others exist, including data authentication by means of fragile watermarks which are impaired or destroyed by manipulations, embedded transmission of value added services within multimedia data, and embedded data labeling for other purposes than copyright protection, such as data monitoring. An example for a data-monitoring system is the automatic registration and monitoring of broadcasted radio programs such that royalties are automatically paid to the IPR owners of the broadcast data.

2.1.3 Digital Watermarking

A. Requirements

The basic requirements in watermarking that apply to all media are very intuitive [1].

1) A watermark shall convey as much information as possible, which means the watermark information rate should be high.

2) A watermark should in general be secret and should only be accessible by authorized parties. This requirement is referred to as security of the watermark and is usually achieved by the use of cryptographic keys. With the development of the asymmetric watermarking techniques, the watermark embedding key can be different from extraction key.

3) A robust watermark should be detectable from the host data even after the attacks, including all possible signals processing that may occur, and including all hostile attacks that unauthorized parties may attempt. This requirement is referred to as robustness of the watermark. It is a key requirement for copyright protection or conditional access

CHAPTER 2. BACKGROUNDS AND RELATED WORKS

applications, but less important for applications where the watermarks are not required to be cryptographically secure, for example, for applications where watermarks convey public information.

4) A watermark should, though being unremovable, be imperceptible. There is always a tradeoff between robustness and imperceptibility. The more robust, the more information is required to be embedded into host data. The increase of amount of the information may affect the imperceptibility.

Depending on the media to be watermarked and the application, this basic set of requirements may be supplemented by additional requirements.

1) Watermark recovery may or may not use the original, unwatermarked host data. The detection system which is required to use the original host data are called “non-blind”, and the one which is not required to use the original host data are referred as “blind”.

2) Depending on the application, watermark embedding may be required in real time, e.g., for video fingerprinting. Real-time embedding again may, for complexity reasons, require compressed-domain embedding methods. The limited bandwidth is also an issue.

3) Depending on the application, the watermark may be required to be able to convey arbitrary information. For other applications, only a few predefined watermarks may have to be embedded, and for the decoder it may be sufficient to check for the presence of one of the predefined watermarks (hypothesis testing).

B. Basic watermarking principles

The basic idea in watermarking is to add a watermark signal to the host data to be watermarked such that the watermark signal is unobtrusive and secure in the signal mixture but can partly or fully be recovered from the signal mixture later on if the correct cryptographically secure key needed for recovery is used.

There are three main issues in the design of a watermarking system.

CHAPTER 2. BACKGROUNDS AND RELATED WORKS

1) Design of the watermark signal W to be embedded to the host signal. Typically, the watermark signal depends on a key K_1 and watermark information I

$$W = f_o(I, K_1) \quad (2.1)$$

Possibly, it may also depend on the host data X into which it is embedded

$$W = f_o(I, K_1, X) \quad (2.2)$$

2) Design of the embedding method itself that incorporates the watermark signal W into the host data X with an embedding key K_2 yielding watermarked data Y

$$Y = f_1(X, K_2, W) \quad (2.3)$$

3) Design of the corresponding extraction method that recovers the watermark information from the signal mixture using the keys and with help of the original

$$\hat{I} = g(X, Y, K_1, K_2) \quad (2.4)$$

or without the original

$$\hat{I} = g(Y, K_1, K_2) \quad (2.5)$$

Sometime a confidence measure is computed instead of extracting the watermark. For this purpose the original watermark may be required. The first two issues, watermark signal design and watermark signal embedding, are often regarded as one, specifically for methods where the embedded watermark is host signal adaptive. Figure 2.1 shows the generic watermark embedding scheme (without the watermark signal design). Generic watermark recovery/detection process is depicted in Figure 2.2.

Figure 2.1: Generic digital watermarking scheme

CHAPTER 2. BACKGROUNDS AND RELATED WORKS

Figure 2.2: Generic watermark recovery/detection scheme

2.1.4 Some Watermarking Techniques

A. Image Watermarking

Most watermarking research and publications are focused on images. The reason might be that there is a large demand for image watermarking products due to the fact that there are so many images available on the World Wide Web, which need to be protected.

A DCT-based watermarking scheme is introduced in [20], the watermarking scheme inserts the watermark in subimages obtained through subsampling, and the original image is not required for watermark recovery process. But the robustness of this scheme is a little weak under lowpass filtering and JPEG coding, which is due to the fact that a crucial portion of the watermark energy is located in the high frequency region.

B. Video Watermarking

Video Sequences consist of a series of consecutive and equally time-spaced still images. Thus, the general problem of watermarking seems very similar for images and video sequences, and the idea that image watermarking techniques are directly applicable to video sequences is obvious. This is partly true, and there are a lot of publications on image watermarking which conclude with the remark that the proposed approach is also applicable to video. However, there are also some important differences.

One important difference is the available signal space. For images, the signal space is very limited. This motivates many researchers to employ implicit or explicit models of

CHAPTER 2. BACKGROUNDS AND RELATED WORKS

the human visual system (HVS), in order to reach the threshold of visibility and to embed a watermark as robust as possible without sacrificing image quality.

A watermarking scheme which enables public decoding and verification of the watermark without giving the possibility of removing the watermark is presented in [23], the basic idea is to make only parts of pseudo-noise signal used for modulation public. One advantage of this watermarking scheme is that it can be combined with some fast compressed-domain algorithm. Hsu [24] embeds watermarks into both intraframe and non-intraframe with different residual marks, the watermarking scheme is invisible and robust.

C. Audio Watermarking

Compared to images and video, audio signals are represented by much less samples per time interval. This alone indicates that the amount of information that can be embedded robustly and inaudibly is much lower than for visual media. An additional problem in audio watermarking is that the human audible system is much more sensitive than the human visual system, and that inaudibility is much more difficult to achieve than invisibility for images.

An audio watermarking technique introduced by Lemma et. al. [21] gives a system called modified audio signal keying(MASK). The short-time envelope of the audio signal is modified in such a way that the change is imperceptible to the human listener. The Modified Patchwork Algorithm [22] is a statistical technique for audio watermarking algorithm in the transform domain.

2.1.5 Watermark Applications and Robustness

A. Application

Although watermarking methods have to be robust in general, different levels of required robustness can be identified depending on the specific application-driven requirements.

CHAPTER 2. BACKGROUNDS AND RELATED WORKS

In authentication applications, the watermarks have to resist only certain attacks. Among all possible watermarking applications, authentication watermarks require the lowest level of robustness. The purpose of such watermarks is to authenticate the data content. For example, data can be watermarked such that the watermark can accommodate lossy compression, but they are destroyed as soon as the data are manipulated in a different way.

Applications such as data monitoring and tracking require a higher level of robustness. The main purpose is to detect or identify stored or transmitted data. Examples are automatic monitoring of radio broadcast for billing purposes or identification of images on the World Wide Web with the help of web crawlers. For such applications, the watermarks have to be easily extractable and must be reasonably robust, for example, against standard data processing like format conversion and compression. In fingerprinting applications, watermarks are embedded that identify the recipient of each individual distributed copy. The purpose is to have a means to trace back pirated copies to the recipient who pirated it. Fingerprinting applications require a very high level of robustness against data processing and malicious attacks. Watermarking for copyright protection is used to resolve rightful ownership and requires the highest level of robustness.

However, robustness alone is not sufficient for such applications. For example, if different watermarks are embedded in the same data, it must still be possible to identify the first, authoritative, watermark. Hence, additional design requirements besides mere robustness apply. In the following, we go into more details on how to resist malicious attacks and elaborate on design constraints for copyright protection applications of watermarking.

CHAPTER 2. BACKGROUNDS AND RELATED WORKS

B. Watermark robustness

Robustness against attacks is a major watermarking requirement. Absolute robustness against all possible attacks and their combinations may be impossible to achieve. Thus, the practical requirement is that a successful attack must impair the host data to the point of significantly reducing its commercial value before the watermark is impaired so much that it cannot be recovered. In fact, with appropriate design, fairly high robustness can be achieved, but it should be pointed out that robustness always has to be traded against watermark data rate and imperceptibility, and the optimum tradeoff depends on the application.

Classification of Attacks: Following the classification in [12], four different types of attacks can be identified.

1) “Simple attacks” (other possible names include “waveform attacks” and “noise attacks”) are conceptually simple attacks that attempt to impair the embedded watermark by manipulations of the whole watermarked data (host data plus watermark) without an attempt to identify and isolate the watermark. Examples include linear and general nonlinear filtering, waveform-based compression (JPEG, MPEG), addition of noise, addition of an offset, cropping, quantization in the pixel domain, conversion to analog, and gamma correction.

2) “Detection-disabling attacks” (other possible names include “synchronization attacks”) are attacks that attempt to break the correlation and to make the recovery of the watermark impossible or infeasible for a watermark detector, mostly by geometric distortion like zooming, shift in spatial or temporal (for video) direction, rotation, shear, cropping, pixel permutations, subsampling, removal or insertion of pixels or pixel clusters, or any other geometric transformation of the data.

CHAPTER 2. BACKGROUNDS AND RELATED WORKS

3) “Ambiguity attacks” (other possible names include “deadlock attacks”, “inversion attacks”, “fake-watermark attacks” and “fake-original attacks”) are attacks that attempt to confuse by producing fake original data or fake watermarked data [13].

An example is an inversion attack [14] - [16] that attempts to discredit the authority of the watermark by embedding one or several additional watermarks such that it is unclear which was the first, authoritative watermark.

4) “Removal attacks” are attacks that attempt to analyze the watermarked data, estimate the watermark or the host data, separate the watermarked data into host data and watermark, and discard only the watermark. Examples are collusion attacks [18]; denoising, certain nonlinear filter operations [17], or compression attacks using synthetic modeling of the image (e.g., using texture models or 3-D models). Also included in this group are attacks that are tailored to a specific watermarking scheme and combat it by exploiting conceptual cryptographic weaknesses of the scheme that make it vulnerable to a specific attack. The conceptual cryptographic weakness means the weakness in the cryptographic protocols used in the watermarking scheme. It should be noted that the transitions between the groups are sometimes fuzzy and that some attacks do not clearly belong to one group. Collusion attacks could be argued to be a group of its own, since they require, unlike the other attacks, more than one differently watermarked copy of the data. However, since they attempt to reconstruct the unwatermarked original host data, and thus remove the watermark(s), the classification as a “removal attack” holds.

2.1.6 Future of Digital Watermarking

The interest in watermarking technology is high, both from academia and industry. The interest from academia is reflected in the number of publications on watermarking and the number of conferences on watermarking and data hiding are being held. The interest from

CHAPTER 2. BACKGROUNDS AND RELATED WORKS

industry is evident in the number of companies in this field that have been founded within the past few years.

Besides research activities in universities and industry, several international research projects funded by the European Community have the goal to develop practical watermarking techniques.

Despite the many efforts that are underway to develop and establish watermarking technology, watermarking is still not a fully mature and understood technology, and a lot of questions are not answered yet. Also, the theoretical fundamentals are still weak, and most systems are designed heuristically.

Another drawback is that fair comparisons between watermarking systems are difficult [19]. As long as methods and system implementations are not evaluated in a consistent manner using sophisticated benchmarking methods, the danger exists that weak and vulnerable systems and *de facto* standards are produced that result in spectacular failures and discredit the entire concept.

Thus, the expectations into watermarking should be realistic. It should always be kept in mind that every watermarking system involves a tradeoff between robustness, watermark data rate (payload), and imperceptibility. The invisible 10000-bit-per-image watermark that resists all attacks whatsoever is an illusion (realistic numbers are approximately two orders of magnitude lower). Even when designed under realistic expectations, watermarks offer robustness against non-experts but may still be vulnerable to attacks by experts. Although proof of ownership was the initial thrust for the technology, it seems that there is a long way to go before watermarking will be accepted as a proof in court. In copyright-related applications, watermarking must be combined with other mechanisms like encryption to offer reliable protection. Still, there exist enough applications where watermarking can provide working and successful solutions.

CHAPTER 2. BACKGROUNDS AND RELATED WORKS

Specifically for audio and video it seems that watermarking technology will become widely deployed. The DVD industry standard, as an example, uses watermarking for the copy protection system. Similarly, there exist plans to use watermarking for copy protection for Internet audio distribution. Broadcast monitoring using watermarking is another application that will probably widely be deployed for both audio and video.

Although working systems are already available, research in digital watermarking has to continue. There is a huge demand from content providers. Watermarking technology will evolve, as well as attacks on watermarks. Careful overall system design under realistic expectations is crucial for successful applications.

2.2 Literature Review of Related Work

Our watermarking frameworks protect the joint-creatorship for images, videos and movies. In this section, after reviewing some general image and video watermarking schemes, we emphasize on those related to our research work.

2.2.1 Image Watermarking Schemes

The number of image watermarking publications is very large, however, most techniques share common principles. A lot of watermarking methods are in fact very similar and differ only in parts or single aspects of the three topics: signal design, embedding, and recovery.

The watermark signal is often designed as a white [25] or colored pseudorandom signal with, e.g., Gaussian [26], uniform, or bipolar [28], probability density function. In order to avoid visibility of the embedded watermark, an implicit or explicit spatial [29], [30] or spectral [30], [31] shaping is often applied with the goal to attenuate the watermark in areas of the image where it would otherwise become visible. The watermark signal is often designed in the spatial domain, but sometimes also in a transform domain

CHAPTER 2. BACKGROUNDS AND RELATED WORKS

like the full-image discrete cosine transform (DCT) domain [26] or block-wise DCT domain [32].

The signal embedding is done by addition [33] or signal-adaptive addition [34], mostly to the luminance channel alone, but sometimes also to color channels, or only to color channels [35]. The addition can take place in the spatial domain, or in transform domains such as the Discrete Fourier Transform (DFT) domain [36], the full-image DCT domain [37], [26], the block-wise DCT domain [29], the wavelet domain [38] etc.

Watermark signal generation and watermark embedding are often treated jointly. For some proposed methods, they cannot be regarded separately, especially if the watermark is signal adaptive [37], [39], [40].

The watermark recovery is usually done by some sort of correlation method, like a correlation receiver or a matched filter. Since the watermark signal is often designed without knowledge of the host signal, crosstalk between watermark signal and host data is a common problem in watermarking. In order to suppress the crosstalk, many proposed schemes require the original, unwatermarked data in order to subtract it before watermark extraction. Other proposed methods apply a prefilter [41], [35] instead of subtracting the original.

2.2.2 Video Watermarking Schemes

A lot of research papers have been published on image watermarking; there are fewer publications that deal with video watermarking. However, the interest in such techniques is high.

In the following, some watermarking methods exploiting uncompressed or compressed video for fingerprinting applications are reviewed.

Hartung and Girod [42] - [44] have concentrated on watermarking of compressed video for fingerprinting applications. They employ a straightforward spread-spectrum

CHAPTER 2. BACKGROUNDS AND RELATED WORKS

approach and embed an additive watermark into the video. Jordan et al. [45] have proposed a method for the watermarking of compressed video that embeds information in the motion vectors of motion-compensated prediction schemes.

Many watermarking schemes are designed in compressed domain. Hsu and Wu present a watermarking method [46], [47] for compressed video which is an extension of their method for images [48] and which modifies middle-frequency DCT coefficients in relation to spatially or temporally neighboring blocks. Simitopoulos et al. [27] propose to embed the copyright information in compressed domain. The watermarking scheme is robust to filtering attacks, clipping attacks etc and the watermark is invisible, but the invertibility is a weakness.

Some are designed for the uncompressed video. Swanson et al. [49], [50] propose a multi-scale watermarking method working on uncompressed video, which has some interesting properties. Lancini et al. [51] have developed a video watermarking method. It works in the uncompressed image domain and robust to a large set of possible attacks. It is also invisible.

2.2.3 Watermarking Schemes Related to our Work

There have been many researches done in watermarking area [1][2][70][71]. The work by Cox et. al. [3] is spread spectrum based watermarks, which are robust and invisible. Being robust watermarks, it would be hard for the attackers to make undetectable or remove the watermarks. The watermarking techniques proposed in [4] and [5] are asymmetric. The asymmetric watermarks make use of another key for detection other than the embedding 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], Li and Chang [69], give a non-invertible watermarking scheme. In order to prove the rightful owner unambiguously, the watermarking scheme should be non-invertible.

CHAPTER 2. BACKGROUNDS AND RELATED WORKS

With the concept of object-based video coming out, certain watermarking schemes are specifically designed to support object based coding standard MPEG-4. Alattar et. al. [8] proposed a MPEG-4 compressed domain video watermarking method. A watermark signal is inserted directly into the MPEG-4 compressed bit stream while detection is performed using the uncompressed video. This method allows detection if video has been manipulated or its format changed, without writing a detector to interpret new formats. Lancini et. al.[9] developed a robust video watermarking technique in the spatial domain. The scheme worked in uncompressed spatial domain. A DWT-based watermarking scheme for MPEG-4 video streams is introduced in [10].

Watermarking technology is a solution for establishing the ownership. Many watermarking schemes related to ownership are published [63].

The non-invertibility is an essential requirement for ownership proof. In order to achieve non-invertibility, Craver et al. [57] proposed to include one-way functions along the path of watermark generation, so that it is not possible to reverse the process. Qiao et al. [58] proposed the use of standard encryption functions for watermark generation. In their constructions, the watermark is created by encrypting some information derived from transform coefficients of the cover-object under a predetermined key selected by the owner, and ownership verification requires both the original and the key. In [60] and [61], Ramkumar et al. showed that if the false-positive rate of the underlying embedding/detection scheme is high, the cryptographic constructions deployed in watermark generation does not provide a basis for establishing ownership because the pirate does not need to reverse engineer the watermark generation process to obtain a valid watermark to claim counterfeit ownership. Katzenbeisser et al. [62] proposed an alternate approach which has been further developed by Adelsbach et al. [59]. In their construction, the computation of the watermark is hardened by incorporating digital

CHAPTER 2. BACKGROUNDS AND RELATED WORKS

signatures of a trusted party rather than deploying mechanisms to achieve the non-invertibility. In [56], a cryptographic time-stamping service is used to certify the creation time of an object due to its security properties.

Although there are many papers related to the ownership, very few of them considered joint-ownership protection and even less the joint-creatorship (different from ownership) protection.

Guo and Georganas [11] introduce a digital image-watermarking scheme for joint-ownership verification. For N owners, this scheme needs to embed a combined watermark of N individual watermarks and one joint watermark, and prove the partial and full ownership by setting different thresholds in the detector. This scheme does not provide the protection during the creation process, so there is no hard trust relationship among creators during creation process. And the creator cannot specify which part of the product was created by him/her. A new method should be developed to solve these problems.

2.3 Digital Signature Schemes

Digital signature is data appended to or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery. [68]

2.3.1 Background Theory

The digital signature is analogous to the handwritten signature. It must have the following properties;

- It must verify the author and the date and time of the signature.
- It must authenticate the contents at the time of the signature.
- It must be verifiable by third parties, to resolve disputes.

CHAPTER 2. BACKGROUNDS AND RELATED WORKS

On the basis of these properties, we can formulate the following requirements for a digital signature:

- The signature must be a bit pattern that depends on the message being signed.
- The signature must use some information unique to the sender, to prevent both forgery and denial.
- It must be relatively easy to produce the digital signature.
- It must be relatively easy to recognize and verify the digital signature.
- It must be computationally infeasible to forge a digital signature, either by constructing a new message for an existing digital signature or by constructing a fraudulent digital signature for a given message.
- It must be practical to retain a copy of the digital signature in storage.

A variety of approaches have been proposed for the digital signature function.

2.3.2 Related Digital Signature Schemes

There are many digital signature schemes available such as RSA [53], Digital Signature Algorithm (DSA) and Elliptic Curve Digital Signature Algorithm (ECDSA). Recent years, some new schemes have been proposed. Elkamchouchi et. al. [54] 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. [55] 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 secure digital signature.

Chapter 3

Joint-Creatorship Protection for Digital Images

In this chapter, we will present our framework for joint-creatorship protection for images. Digital image creations are sometimes carried out jointly. It is then necessary to provide protection to the creatorship of each participating creator. This chapter introduces a novel digital watermarking framework to solve the problem of joint-creatorship protection for digital images. The images can be created in parallel process or sequential process. The designed framework makes use of digital watermarking techniques and cryptographic protocols to achieve creatorship protection in jointly created digital images. The framework embeds multiple watermarks in a spatially non-overlapping manner during the creation process and thus obtains a high visual quality for the watermarked digital image. We have also developed a watermarking scheme with the properties of robustness, imperceptibility, asymmetry and non-invertibility, which is required by the framework for joint-creatorship protection. The watermarking framework can be applied in the rightful creatorship resolution and creatorship purchase situation. The complexity of the framework is analyzed by calculating the data transmission and storage requirements, and the experimental results show that the framework can address the joint-creatorship protection problem with low storage and transmission requirements.

CHAPTER 3. JOINT-CREATORSHIP PROTECTION FOR DIGITAL IMAGES

3.1 Introduction

With the rapid development in the digital creation and delivery technologies, lots of digital multimedia data are created and transacted everyday. Nowadays, the digital image creation sometimes needs the cooperation of many creators. Some creators may be only good at sketching the skeleton of the object, and others may be very good at coloring; some may be good at drawing animals, and others may be perfect in drawing plants. To create a complex image, there will be lots of contents inside; single creator may not be able to do a very good job. So the cooperation is necessary. In such a case, the protection of each creator's creatorship becomes a big issue. In this scenario of joint creation, it is possible that a group of creators (or a creator) can connive to remove another creator (or another group of creators) from creatorship of the final product. Thus, each creator is concerned about his/her rightful share of creatorship of the final product. In this chapter we address the joint-creatorship protection problem for digital images. In addition, the creators should be able to establish and prove their contributions and amount of contributions to buyers of the jointly created image. The designed framework elegantly addresses this requirement as well. We make use of watermarking techniques and cryptographic protocols for the framework. We in this chapter describe the framework for the jointly created image creatorship protection in detail.

The remainder of this chapter is structured as follows: section 3.2 introduces the risks in joint creation. The developed frameworks for parallel process and sequential process are presented in section 3.3 and 3.4 respectively. Section 3.5 gives some application of our framework. We analyze the complexity of the parallel framework and sequential framework in section 3.6. Section 3.7 gives some applications of our framework. The experimental results are shown in section 3.8 and section 3.9 concludes this chapter.

CHAPTER 3. JOINT-CREATORSHIP PROTECTION FOR DIGITAL IMAGES

3.2 Risks in Joint Creation

In a joint-creatorship situation, to protect the creatorship, the creators can place their own watermarks on their own sub-creations. When and how these watermarks should be embedded into the image is the major consideration during this process. If the watermark is embedded too early, it cannot protect the future creation and modification. If the watermark is embedded after the creation of the whole image, some creator may take the whole unwatermarked image and watermark it with his/her own watermark to claim the creatorship of the whole image. So, the watermark should be embedded during the whole creation process, and in a spatially non-overlapping manner in order to avoid the quality degradation.

The watermarking scheme should be robust for the reason that others (including other creators) should not be able to remove the placed watermark. The watermark should be invisible in order to have a high visual quality. It is possible that a conniving creator(s) can place a second watermark on the creation of the creator whom the conniving creator(s) wants to deny creatorship and claim the creatorship of that part. In order to safely guard against such attacks the watermarking scheme used must be non-invertible. The buyer of the jointly created image should be able to verify the existence of the watermark (without the capability to remove it or embed it), which requires the watermarking technique to be asymmetric as well. Each creator should watermark his/her contribution completely. This requirement will help assess the amount of contribution by each creator. Thus the watermarking technique employed in the framework should have the following properties: robust, invisible, asymmetric and non-invertible.

It is possible that a creator wants to disown his/her contribution at a later stage due to the malpractices (copying from someone else's work etc.) he/she has done during the

CHAPTER 3. JOINT-CREATORSHIP PROTECTION FOR DIGITAL IMAGES

creation. In order to solve this problem, the framework employs cryptographic protocols. The creators are requested to sign on their creations.

We have designed frameworks for parallel and sequential creation process. We next discuss the framework for parallel process.

3.3 Framework for Parallel Process

Our framework provides joint-creatorship protection and also creatorship proving capability. The scheme makes use of a robust, invisible, asymmetric and non-invertible watermarking technique and digital signature scheme.

Let N be the number of creators jointly creating a digital image in an iterative manner. The creation area A is divided into N non-overlapping areas for every iteration. Let a_{ij} be the creation area of i^{th} creator in j^{th} iteration and then $A = a_{1j} \cup a_{2j} \cup \dots \cup a_{Nj}$ for any j . The a_{ij} can be arbitrary shaped as in figure 3.1(a) represented by number of pixels occupied. Let the whole created watermarked image at the end of j^{th} iteration be I_j^w and it occupies the entire area A . Let c_{ij} be the i^{th} creator's contribution (creation/modification) during j^{th} iteration. And c_{ij}^w is the watermarked c_{ij} , watermarked by the i^{th} creator using his/her watermark W_i . Let there be M iterations to complete the digital image and the watermarked final image is denoted as I_M^w . The notation $Sign_i\{msg\}$ denotes the digitally signed message msg , signed by i^{th} creator using his/her private key. This signed message can be verified using the corresponding public key known to everyone. The verification of signed message will result in message msg and thus everyone can obtain the message.

The image is created in an iterative manner. It is almost impossible that all the work can be done in single creation and satisfies all the creators. So, creators need to modify

CHAPTER 3. JOINT-CREATORSHIP PROTECTION FOR DIGITAL IMAGES

the image again and again. If we do not provide the protection during the creation process, there will be a big risk to be attacked by an attacker. E.g. if we only watermark the image after the whole creation process, at this time, certain creator can get the whole unwatermarked image and watermark it, then claim the whole creatorship of the image.

Figure 3.1 gives a basic hardware infrastructure of our framework. The creators are connected together by network. So, they can exchange their sub-creations through network, instead of having to come together to create an image, this will benefit the creators that are far from each other.

Figure 3.1: the infrastructure of the proposed framework

Each creator works on his/her own station and the data will be stored in his/her local database. In the first iteration, the whole image area is originally divided to several parts, each of them will work on certain part of the image, after editing, they need to send their sub-creations to all the others, each creator then can assemble the image locally and they can discuss through the network on how to modify the image. In the following iteration, the creators will re-divide the image into several parts; the new part may not be same as in the first iteration. Each creator will work on certain part of the image and modify the image as discussed. In this framework, we allow creators to modify other creator's originally created work, since this will give better final product. But, each creator will only be allowed to watermark the part he/she creates/modifies. The final stage is that all the creators will together go to the Registration Authority (RA) to register the image. The

CHAPTER 3. JOINT-CREATORSHIP PROTECTION FOR DIGITAL IMAGES

whole framework is discussed in detail below. Figure 3.2 shows the whole creation process.

Figure 3.2: The whole creation process

First iteration

Step 1: The image area is divided among all creators in a non-overlapping manner as in figure 3.3(a). Thus, the whole image area $A = a_{11} \cup a_{21} \cup \dots \cup a_{N1}$.

Figure 3.3 (a): the whole area is divided into N sub-areas

(b): watermarked image I_1^w after first iteration

In the first iteration, each creator creates his/her own designated area completely, for example i^{th} creator creates c_{i1} in the entire area a_{i1} . Each creator then embeds a watermark using his/her private embedding key in his/her created area completely. I.e., i^{th} creator embeds his/her watermark W_i using his/her watermark embedding key in his/her creation c_{i1} to obtain c_{i1}^w . Each creator then makes a digitally signed version (using the private key of the creator) of their watermarked creation and then transmits them to all other creators. For example i^{th} creator transmits $Sign_i\{c_{i1}^w\}$ to all the other creators. The creator C_i then stores his/her creation, watermark and embedding key in the local database DB_i . These information are supposed to be presented to a judge in case of the creatorship dispute. This step is illustrated in figure 3.4.

Discussion: Different creators will use different watermarks and hence help to declare the area of creatorship by showing the presence of the watermark. Since the areas

CHAPTER 3. JOINT-CREATORSHIP PROTECTION FOR DIGITAL IMAGES

are arbitrary shaped and also to calculate the amount of contribution done by each creator, the watermarking technique is required to be block-wise. The watermarking scheme should be robust; hence others (including other creators) should not be able to remove the embedded watermark. In addition, the watermark should be invisible in such a way that the watermark embedding will not degrade the visual quality of the original image. In case that some creators disown the creatorship of their created part, other creators can use the digitally signed watermarked sub-creations to prove their creatorship.

Figure 3.4: Step 1 of parallel process

Step 2: On receiving the signed watermarked creations from other creators, the creator first stores them in the local database DB_i (the i^{th} creator's local database). The creator then verifies all the signed watermarked creations received from all other creators using the public keys of the corresponding signatures. If there is no correct signature detected, the creator will ask for a retransmission of the signed watermarked image. After the successful detection of all the signatures, the results of the verifications give the respective watermarked creations. Every creator after the successful signature verification possesses the watermarked creations of all creators (c_{i1}^w for all i 's). All creators then assemble the watermarked image locally. After I^{st} iteration, all the creators will have $I_1^w = c_{11}^w \cup c_{21}^w \cup \dots \cup c_{n1}^w$ in their local database DB_i , which is shown in figure 3.3(b). Figure 3.5 gives the flowchart of this step.

Discussion: The received signed watermarked creations, own creation, own

CHAPTER 3. JOINT-CREATORSHIP PROTECTION FOR DIGITAL IMAGES

watermark and embedding keys are stored locally for checking malpractices by other creators during later iterations and also for reference in dispute resolution which will be discussed in section 3.5.1.

Figure 3.5: Step 2 of parallel process

Refinement iterations

The refinement iterations use the watermarked image of the previous iteration as input. I.e., the j^{th} iteration would use I_{j-1}^w as input. The watermarked image after the j^{th} iteration is I_j^w . We believe that the cooperation of two or more creators can usually produce better images than only one of them create the whole thing from beginning to end. Our framework allows creators to modify others creation, so, the final product will have a better quality. But, the creator is strict to only watermark the parts he/she created in order to avoid the creatorship dispute.

Step 3: The image I_{j-1}^w is divided among all creators in a non-overlapping manner as in figure 3.7(a) for the j^{th} iteration. Thus $A = a_{1j} \cup a_{2j} \cup \dots \cup a_{Nj}$. How to divide the image and which part is assigned to whom are discussed among the creators after the first iteration. And the new division may or may not be the same as in the first iteration. The i^{th} creator gets the area a_{ij} for modification. Though the i^{th} creator can modify the entire area a_{ij} in I_{j-1}^w , the creator may modify only part of it during the j^{th} iteration. Each creator should watermark (with own watermark) only that area which is modified by

CHAPTER 3. JOINT-CREATORSHIP PROTECTION FOR DIGITAL IMAGES

him/her during j^{th} iteration, so we can calculate the percentage of contributions of every creator by calculating his/her watermarked area. Each creator then generates a signed version of watermarked contribution (modification), for example i^{th} creator generates $Sign_i\{c_{ij}^w\}$. The signed contribution (modification) is required to be transmitted to all the other creators. Only the modified part is transmitted in order to reduce the transmission and storage complexity. Each creator then stores his/her contribution during j^{th} iteration into the database DB_i . This process is shown in figure 3.6.

Figure 3.6: Step 3 of parallel process

Discussion: Any modification assumes that the modifying action removes the previous image data and the watermark in the modified area completely. Thus, the creator who carries out the modification has the creatorship of the modified area.

Figure 3.7 (a): whole area before j^{th} iteration

(b): watermarked image I_j^w after j^{th} iteration

Step 4: On receiving the signed watermarked contributions (modifications) from other creators, the creator first stores them in the database DB_i . The creator then verifies the signature of received signed watermarked modifications. If there is no correct signature detected, the creator will ask for a retransmission. After the successful signature verification, the creator obtains the watermarked modifications. Each creator then checks whether its watermark is present in the claimed modified area by others, for example, i^{th}

CHAPTER 3. JOINT-CREATORSHIP PROTECTION FOR DIGITAL IMAGES

creator checks for the existence of its watermark W_i in all received watermarked modifications from other creators. If W_i is detected, He can conclude that some creator want to claim the creatorship of his creation without any modification. If there is no W_i detected, each creator then uses the received watermarked modifications to overwrite the respective area in I_{j-1}^w to obtain the I_j^w . The figure 3.7(b) depicts I_j^w at the end of j^{th} iteration and figure 3.8 gives the flowchart of this process.

Figure 3.8: Step 4 of parallel process

Discussion: Sometimes it is possible that a creator can cheat another joint creator by merely placing his/her watermark on the area without doing any modification. This action would cause both watermark to be detected from the same area. In order to defeat this kind of attack the watermarking technique should be non-invertible which would identify the original creator unambiguously even though two watermarks are detected from the same area.

Step 5: Refinement iterations (step 3 and 4) are repeated again and again until all the creators are satisfied with the image. I.e. the final image is created. Figure 3.9 is the flowchart of step 5.

Figure 3.9: Step 5 of parallel process

CHAPTER 3. JOINT-CREATORSHIP PROTECTION FOR DIGITAL IMAGES

Now, the image creation process is completed. We also need a registration to give an overall view of how many creators are involved in the creation process and who they are. This can help the buyers to know who are the creators.

Registration step

All the creators then jointly submit the I_M^w and their watermark detection keys to a registration authority (RA) for registration. We assume the watermarking technique to be asymmetric and hence the watermark detection key is different from embedding key. Therefore the RA cannot perform the watermarking but can detect the watermarks. The RA first checks whether an identical/mostly similar I_M^w is already present in its database. If not present; the RA then calculates the percentage of contribution by each creator by calculating the area where individual watermark is present. The total watermarked area in the watermarked image should be the area A . The RA then issues a digitally signed (signed by RA) creatorship certificate which contains the authors identity, percentage of contribution and identity of the watermarked image to all the creators. If there is an identical/mostly similar I_M^w already present in its database, the RA does not issue a creatorship certificate until the creatorship is resolved among the creators of old and new watermarked images, themselves or with the help of a judge. The RA stores the watermarked images and the creatorship-certificates in its database Y . The digitally signed creatorship certificate helps buyers to identify the creators and their percentage of contribution. Figure 3.10 gives the flowchart of registration step.

Figure 3.10: Registration step

CHAPTER 3. JOINT-CREATORSHIP PROTECTION FOR DIGITAL IMAGES

Once the final watermarked image I_M^w and the creatorship are obtained, the joint creation phase is completed.

3.4 Framework for Sequential Process

Above we have described our framework for the parallel process. Now consider the following scenario: a few creators try to create a complex digital image, the creator with good overall view can be the first creator to sketch the skeleton of the image; the one with good painting skills can do some coloring job; and the one better in detail drawing can do the further refinement and so on. This will make the image to look better under the cooperation of several creators rather than only one of them. Our framework for parallel process is not suitable for this sequential scenario. Instead, we have designed another framework for this sequential process. Similarly, we assume that there will be N creators totally. And there will be M iterations. Here, we will use the same notations as in the parallel process. The sequential process is also carried out in an iterative manner (including a first iteration and several refinement iterations) and a registration process.

First iteration

First, the first creator C_1 will create an image of pre-determined resolution. Here we assume that C_1 will only create the background of the image. After the creation, C_1 will watermark the image with a non-invertible robust watermark to get I_1^w . Then signs the watermarked image using a digital signature algorithm (any digital signature algorithm can be used such as RSA and [54]) to get the signed watermarked image $Sign_{\{I_1^w\}}$. Finally, C_1 will send the signed watermarked image to all the other creators, so all the creators can discuss on how to modify the image. First iteration is shown in figure 3.11.

CHAPTER 3. JOINT-CREATORSHIP PROTECTION FOR DIGITAL IMAGES

Figure 3.11: First iteration of sequential process

Refinement iterations

The refinement steps will use the image of previous iteration as input. Figure 3.12 shows the flowchart of this process.

Figure 3.12: Refinement iterations of sequential process

After all the creators receive the signed watermarked image, first, they will use the public key to verify that the image is signed by C_1 , this will prevent C_1 disowning his/her ownership at a later time. After the successful verification, the creators will discuss how to modify the image on the network. Then, the second creator, C_2 , will modify certain part of the image in a pre-determined way. For example, if all the creators decide to add one dog at certain position, and C_2 is good at drawing a dog, then, C_2 will draw a dog there. C_2 may modify the shape and color of certain object in the image created by creator C_1 , or may totally create a new object. The modification done by creator C_2 will improve the image. When C_2 finishes editing, he will also watermark and sign on his creation using his private key, then send the whole image to all the other creators. The creators will again decide how to modify the image further and who is the next one to do the

CHAPTER 3. JOINT-CREATORSHIP PROTECTION FOR DIGITAL IMAGES

modification.

This process repeats for a few times, until all the creators are satisfied with the image. And during this process, any creator can edit the image for any number of times. Once the refinement iterations are over and the final image is created, all the creators together carry out the registration as explained in the registration step.

Registration step

After the whole image is finished, all the creators will together go to the RA for product registration. All the creators then jointly submit the final watermarked image I_M^w and their *watermark detection keys* to a registration authority (RA) for registration. We assume the watermarking technique to be asymmetric and hence the watermark detection key is different from embedding key. Therefore the RA cannot perform the watermarking but can detect the watermarks. The RA first checks whether an identical/mostly similar I_M^w is already present in its database. If not present; the RA then calculates the percentage of contribution by each creator by calculating the area where individual watermark is present. The total watermarked area in the watermarked image should be the area A . The RA then issues a digitally signed (signed by RA) creatorship certificate which contains the authors identity, percentage of contribution and identity of the watermarked image to all the creators. If there is an identical/mostly similar I_M^w is already present in its database, the RA does not issue a creatorship certificate until the creatorships are resolved among the creators of old and new watermarked images, themselves or with the help of a judge. The RA stores the watermarked image and the creatorship-certificate in its database Y . The digitally signed creatorship certificate helps buyers to identify the creators and their percentage of contribution.

Once the final watermarked image I_M^w and the creatorship certificate are obtained, the joint creation phase is completed.

CHAPTER 3. JOINT-CREATORSHIP PROTECTION FOR DIGITAL IMAGES

We have developed a watermarking scheme suitable for our framework which is introduced in chapter 6.

3.5 Applications of our Framework

Our framework for both parallel and sequential process can be applied in two scenarios: creatorship verification by judge and creatorship verification by buyer.

3.5.1 Creatorship Verification by Judge

In the event of creatorship dispute among creators, the judge asks for the watermarks, watermark detection key, contributions and the area of dispute in the final watermarked image from the disputing creators. The judge then verifies the existence of watermarks in the disputed area of the watermarked image. If there is more than one watermark found in the same area, the judge uses non-invertible property (using contributions) of the watermark to prove the rightful creator. For resolving the dispute, the asymmetric property of the watermarking technique is not useful, thus the original unwatermarked data is necessary for using the non-invertibility property for proving the rightful creator. However for creatorship verification by buyer, the asymmetric property is useful.

3.5.2 Creatorship Verification by Buyer

When a buyer wants to buy the entire jointly created watermarked image, the buyer identifies all the creators associated with the watermarked image from the RA signed creatorship certificate associated with the watermarked image. The buyer can then approach all the creators for purchase of the jointly created image. In the event the buyer is interested in only part of the jointly created image, the buyer can use the watermark detection key to identify the creators of the area that he/she is interested in and then contact those creators for their parts individually.

CHAPTER 3. JOINT-CREATORSHIP PROTECTION FOR DIGITAL IMAGES

3.6 Complexity Analysis of Parallel Process

Suppose that the image has the dimension K pixels by L pixels and each pixel needs 3 bytes (one byte for each color). The whole creation process contains M iterations, and there are N creators jointly creating the image.

3.6.1 Data Transmission Complexity

Number of Messages Transmitted: At any iteration, every creator must send his/her creation to the other $N-1$ creators. So, there will be $N*(N-1)$ sub-creations transmitted. For M iterations, there are $M*N*(N-1)$ sub-creations transmitted.

Number of Bytes Transmitted: Normally, each creator will not modify the whole area allocated to him/her except in the first iteration. Let p_{ij} be the proportion modified by i^{th} creator in the area a_{ij} . So, the modified pixels for i^{th} creator in j^{th} iteration are $p_{ij} * a_{ij}$, I.e., $3*p_{ij} * a_{ij}$ bytes will be transmitted to each of the rest of creators. For M iterations the total number of bytes transmitted will be

$$\sum_{j=1}^M \sum_{i=1}^N (N-1) * 3 * p_{ij} * a_{ij} \quad (3.1)$$

In the first iteration, every creator creates the entire allocated area, i.e., $p_{i1} = 1, \forall i$. Assume $p_{ij} = (1/r) * p_{i(j-1)}, \forall i, j = 2..M \& r \geq 1$. In the case of $r = 1$, any iteration needs to transmit $3*(N-1)*K*L$ bytes. So, there will be $3*M*(N-1)*K*L$ bytes transmitted in total. For $r > 1$, in the j^{th} iteration, there will be $3*(1/r^{j-1})*(N-1)*K*L$ bytes transmitted. For M iterations, the total data transmitted is calculated by

$$\sum_{j=1}^M 3*(1/r^{j-1})*(N-1)*K*L = 3*(r/r-1)*(N-1)*K*L*(1-1/r^M) \quad (3.2)$$

As M tends to infinity, the total data transmitted are $3*(r/r-1)*(N-1)*K*L$ bytes.

Figure 3.13 plots the number of iterations versus the total data transmitted in bytes with $r = 2, K = 512, L = 512$. And can be seen that the total data transmitted increases slowly

CHAPTER 3. JOINT-CREATORSHIP PROTECTION FOR DIGITAL IMAGES

with increasing M . This is due to r factor.

Figure 3.13: Data transmitted against iteration number

3.6.2 Storage Complexity

In the first iteration, each creator need to store his/her creation, and all other creators' signed creations. Thus, the total storage requirement of first creator in first iteration is $c_{11} + c_{21}^w + c_{31}^w + \dots + c_{N1}^w$. We can see that the size of c_{ij} and c_{ij}^w is equal to $3 * p_{ij} * a_{ij}$. After M iterations, the total bytes required for storage of each creator is

$$\sum_{j=1}^M \sum_{i=1}^N 3 * p_{ij} * a_{ij} \quad (3.3)$$

Again, assume that $p_{ij} = (1/r) * p_{i(j-1)}$, for $r=1$, there will be $3 * M * K * L$ bytes stored.

For $r > 1$, the total number of storage requirements is

$$\sum_{j=1}^M 3 * (1/r^{j-1}) * K * L = 3 * (r/r - 1) * K * L * (1 - 1/r^M) \quad (3.4)$$

We can see that the total number of the creators N does not affect the storage requirement for each creator. With $K=512, L=512$, the relationship between storage required and number of iterations is shown in figure 3.14 and can be seen that, when $M=1$, i.e. only one iteration required, $3 * K * L$ bytes needs to be stored by every creator, i.e., the whole image. With the increasing of M , the storage requirement is asymptotic to $3 * (r/r - 1) * K * L$ bytes. Another thing which can be observed is that the bigger the r , i.e.

CHAPTER 3. JOINT-CREATORSHIP PROTECTION FOR DIGITAL IMAGES

the smaller the $1/r$, the less storage is required.

Figure 3.14: Storage requirement against number of iterations

3.7 Complexity Analysis of the Sequential Process

In this section we analyze the complexity of sequential process in two aspects:

transmission complexity and storage complexity.

We assume that there will be N creators totally. And there will be M iterations. The image has the dimension K pixels by L pixels and each pixel needs 3 bytes to represent (one byte for each color).

3.7.1 Transmission Complexity

Number of message transmitted: let us define the message as an image created or part of the image created. The creator needs to transmit the signed watermarked image to all the other creators. For N creators, there will be $(N-1)$ messages transmitted in every iteration. So, if there are M modifications of the image, there will be $M*(N-1)$ message transmissions.

Number of Bytes transmitted: Suppose that the image has the dimension K pixels by L pixels and each pixel needs 3 bytes (one byte for each color). So, $3*K*L$ bytes needs to

CHAPTER 3. JOINT-CREATORSHIP PROTECTION FOR DIGITAL IMAGES

be transmitted to all the else creators after each modification. Again, it is usually a creator will not totally modify the whole image created by the previous creator. We assume that each iteration will modify the image less than the previous iteration. The percentage of modification is p_j in j th iteration, $p_j = (\text{Bytes modified in the } j^{\text{th}} \text{ modification})/(\text{Bytes of the whole image})$. Let $p_j = (1/r_j) * p_{j-1}$. In the first iteration, C_1 creates the whole part of the image, so $p_1 = 1$, i.e. there are $3 * K * L$ bytes created. As a result, there will be totally $(N-1) * 3 * K * L$ bytes transmitted. In the second creation, there will be $p_2 * 3 * K * L$ bytes modified and $(N-1) * p_2 * 3 * K * L = (N-1) * (1/r_2) * 3 * K * L$ bytes transmitted. In the third creation, there will be $p_3 * 3 * K * L$ and $(N-1) * p_3 * 3 * K * L = (N-1) * (1/r_2) * (1/r_3) * 3 * K * L$ bytes transmitted. So, for M iterations, there needs

$$\sum_{j=1}^M (N-1) * 3 * K * L * \prod_{i=1}^j (1/r_i) \text{ bytes transmitted during the whole creation process.}$$

Suppose that for all $1 \leq j \leq M$, $r_j = r$. then, the expression becomes the

$$\sum_{j=1}^M (N-1) * 3 * K * L * (1/r)^{j-1} = (N-1) * 3 * K * L * \sum_{j=1}^M (1/r)^{j-1} = (N-1) * 3 * K * L * (1 - (1/r)^M) / (1 - 1/r). \quad (3.5)$$

This equation is same as the one in the parallel process in section 3.7. For j tends to infinity, it becomes $(r/(r-1)) * (N-1) * 3 * K * L$.

3.7.2 Storage Complexity

The creator needs to store the watermark, the watermark embedding key, the original of his creation, the signed watermarked image from previous creator. We ignore the watermark and the keys since they are deducible from the original image in our designed watermarking scheme, which is presented in chapter 6. In the first iteration, each creator need to save the whole image, so $3 * K * L$ bytes required. In the second iteration, it requires

$$(1/r_2) * 3 * K * L. \text{ For } M \text{ iterations, each creator needs } \sum_{j=1}^M 3 * K * L * \prod_{i=1}^j (1/r_i) \text{ bytes.}$$

CHAPTER 3. JOINT-CREATORSHIP PROTECTION FOR DIGITAL IMAGES

Suppose that for all $1 \leq j \leq M$, $r_j = r$. then, the expression becomes the

$$\sum_{j=1}^M 3 * K * L * (1/r)^{j-1} = 3 * K * L * \sum_{j=1}^M (1/r)^{j-1} = 3 * K * L * (1 - (1/r)^M) / (1 - 1/r). \quad (3.6)$$

This equation is same as the parallel process described in section 3.7. As j tends to infinity, there will be $3 * K * L * r / (r - 1)$ bytes stored for each creator.

3.8 Experimental Results

In this section, we will discuss the experimental results. We use matlab to simulate our framework environment. We make use of the equations from section 3.7 and section 3.8. And assign those variables certain value. For the dimensions K , L , and the number of creators N , we assign them constant values. For the modification rate, we assign them a random value for different iteration during the creation process. And we assume the number of iterations is infinity, which is the worst case that gives the most complex result. From the complexity analysis in section 3.7 and section 3.8, we can see that the total bytes transmitted on the network and storage requirement for single creator is the same in the two frameworks.

3.8.1 Number of Bytes Transmitted

From the equation (3.2) & (3.5), we can see that the total data transmitted is

$$(N-1) * 3 * K * L * (1 - (1/r)^M) / (1 - 1/r).$$

Here, we set $1/r$ is a random number from 0 to 1 with an assumption that $K = 512$, $L = 512$, $N = 10$ and $M = 10000$. We can calculate out the image size is $3 * 512 * 512 = 0.7864$ Megabytes. We repeated this equation for 100 times, and the result of the calculation is shown in the figure 3.15.

From figure 3.15, we can see from this table, the largest value is 30.3747 Megabytes, which is about 38.625 times of the image size. The smallest value is 7.1652 Megabytes,

CHAPTER 3. JOINT-CREATORSHIP PROTECTION FOR DIGITAL IMAGES

which is about 9.1114 times of the original image size. And the average value is 14.2077, which is about 18.0668 times of the original image.

Figure 3.15: Transmitted bytes of 100 random modification rate

3.8.2 Storage requirements

From the equation (3.4) & (3.6), we can see that the storage requirement is the same for all the creators, which is $3 * K * L * (1 - (1/r)^M) / (1 - 1/r)$.

Here, we set $1/r$ is a random number from 0 to 1 with an assumption that $K = 512$, $L = 512$, $N = 10$ and $M = 10000$. We can calculate out the image size is $3 * 512 * 512 = 0.7864$ Megabytes. We repeated this equation for 100 times, and the result of the calculation is shown in the figure 3.16.

Figure 3.16: Storage requirements of 100 random modification rate.

CHAPTER 3. JOINT-CREATORSHIP PROTECTION FOR DIGITAL IMAGES

From figure 3.16, we can see that the largest value is 3.2800, which is about 4.1709 times of image. The smallest value is 0.8436, which is about 1.0727 times of the image size. And the average is 1.5850, which is about 2.0155 times of the image size.

3.9 Conclusion

We proposed a watermarking framework that solves the joint-creatorship protection problem. The framework is applied during the image creation process. The framework can perform well in both parallel process and sequential process. The framework makes use of both watermarking scheme and cryptographic algorithm. The cryptographic algorithm is mainly used for digital signature purpose. The watermarking scheme is mainly used for creatorship protection. We have developed a robust, imperceptible, asymmetric and non-invertible watermarking scheme to implement our watermarking framework which is explained in chapter 6. The framework successfully handles the creatorship dispute among creators. And is also capable of proving the creatorship and amount of creation to a buyer. The watermark is embedded in a non-overlapping manner, so the quality of the watermarked image is maximized. The research work in this chapter has been published in the paper [66].

Chapter 4

Joint-Creatorship Protection for Digital Videos

This chapter presents the framework for video joint-creatorship protection. Digital videos are always being created jointly. It is then necessary to provide protection to the creatorship of each participating creator. This chapter presents a novel digital watermarking framework to address the problem of joint-creatorship protection for object-based video. The proposed framework makes use of digital watermarking techniques and cryptographic protocols to achieve the creatorship protection purpose. Video objects in the object-based video can be created separately. The framework embeds different watermarks in different video objects in such a way that each creator can show the joint-creatorship of the whole video; as well as each creator can prove his/her creatorship of video object he/she created. We have designed a watermarking scheme, which is suitable for our watermarking framework. The watermarking scheme has the properties of robustness, imperceptibility, asymmetry and non-invertibility. The complexity of the framework is analyzed by calculating the amount of data transmission and storage requirements.

4.1 Introduction

Object-based digital creation of video is gaining ground due to the easy processing

CHAPTER 4. JOINT-CREATORSHIP PROTECTION FOR DIGITAL VIDEOS

capability of digital video objects, reusability of video objects and the popularity of object-based compression standard such as MPEG-4. It is possible that the individual video objects are created individually by different creators and are then assembled jointly to obtain a jointly created video. For example, in a jointly created cartoon movie, each cartoon character may be created (as video objects) by an individual creator, and then all the characters can be assembled together to form a jointly created cartoon movie.

In the case of joint creation, it is possible that a group of creators (or a creator) can connive to remove another creator (or another group of creators) from creatorship of the final digital video. Thus, each creator is concerned about his/her rightful share of creatorship of the final video. They need to protect their joint-creatorship on the final video.

In this chapter, we address this joint-creatorship protection problem for object-based video by adopting a novel watermarking framework during the video creation process. 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, asymmetry, imperceptibility and non-invertibility. So that it can perform well under the complex joint creation situation.

The remainder of the chapter is structured as follows: section 4.2 introduces the risks in joint creation. Our proposed framework is presented in section 4.3. Section 4.4 analyses the framework's complexity. Some applications of our framework are shown in section 4.5 and section 4.6 concludes this chapter.

4.2 Risks in Joint Creation

In a joint-creatorship, all creators can iteratively create a video and in every iteration, each creator works on his/her own video object(s). To protect the creatorship, the creators

CHAPTER 4. JOINT-CREATORSHIP PROTECTION FOR DIGITAL VIDEOS

can place their own watermarks on their own video object(s). The creatorship protection under the jointly creation situation is more complex because that attacks may not only come from non-creators, but also from creators.

So, the watermarking scheme used in the joint-creatorship protection needs following requirements. First, the watermarking scheme should be robust for the reason that others (including other creators) should not be able to remove the placed watermark. Second, the watermark should be invisible in order to have a high visual quality. Third, It is possible that a conniving creator(s) can place a second watermark on the creation of the creator whom conniving creator(s) wants to get rid of creatorship and claim for the creatorship of that part. In order to safe guard against such attacks the watermarking scheme used must be non-invertible. Fourth, The buyer of the jointly created video should be able to verify the existence of the watermark (without the capability to remove it or embed it), which requires the watermarking technique to be asymmetric as well. Each creator should watermark his/her video object completely. This will help to identify the creator of the video object. Thus the watermarking technique employed in the framework should have the following properties: robust, invisible, asymmetric and non-invertible. It is possible that a creator disowns his/her video object at a later stage due to the malpractices (copying from someone else's work etc.) he/she has done during the creation. In order to defeat this problem, the framework employs cryptographic protocols.

4.3 Our Proposed Watermarking Framework

Our framework provides joint-creatorship protection for object-based video. Each creator can show the creatorship of the object he/she created, as well as all the creators can show their joint-creatorship of the whole video. The scheme employs a robust, invisible, asymmetric and non-invertible watermarking scheme and digital signature method.

CHAPTER 4. JOINT-CREATORSHIP PROTECTION FOR DIGITAL VIDEOS

Let N be the number of creators jointly creating an object-based video in an iterative manner. The video contains one background object (BGO) and a few video objects (VO). The background object is made up of several consecutive background object planes (BGOPs) and the video object is made up of several consecutive video object planes (VOPs). Let VO_{ij} be the video object created or modified by the i^{th} creator in the j^{th} iteration, and VO_{ij}^w is the watermarked VO_{ij} using W_i . The VOP_{ijn} is the n^{th} VOP of VO_{ij} , and VOP_{ijn}^w is the watermarked VOP_{ijn} using W_i . Let the W_i embedding key be K_{W_i} and the corresponding asymmetric detection key be $K_{W_i}^*$. $BGOP_n$ is the n^{th} BGOP of BGO and $BGOP_n^w$ is the watermarked $BGOP_n$ using the joint-watermark JW. The joint-watermark JW embedding/detection key be K_{JW} which is created from the participating creators' individual joint-watermark embedding/detection keys, denoted by K_{JW_i} for the i^{th} creator. Thus for creators C_1 , C_2 and C_3 , the individual joint-watermark embedding/detection keys are $K_{JW_{C_1}}$, $K_{JW_{C_2}}$ and $K_{JW_{C_3}}$ respectively. Let there be J iterations to complete the video creation.

The notation $Sign_i\{m\}$ denotes the digitally signed message m signed by the i^{th} creator using his/her private key. This signed message can be verified by everyone using the corresponding public key. The verification of signed message will result in message m , thus anyone can obtain the message from $Sign_i\{m\}$.

Video Creation Process

The video is created in an iterative manner after an initialization step. The initialization step is done on the background object; the iteration steps focus on the video objects created by the creators.

Brief description: The creators are connected together by a computer network which could be the Internet. So, they can exchange their created objects through network.

CHAPTER 4. JOINT-CREATORSHIP PROTECTION FOR DIGITAL VIDEOS

instead of having to come together physically to create a video, this will greatly benefit the creators that are far from each other. Each creator works on his/her own computer and the data will be stored in his/her local database. The creators need not share a common database or a server for creation.

In the initialization step, the creators create a watermark jointly and embed it into background object. In the following iterations, each creator will create his/her own object and modify the object after discussion with other creators. Each creator will only be allowed to watermark his/her own object. The final stage is that all the creators will go to the Registration Authority (RA) together to register the video. The whole framework is discussed in detail below. The hardware infrastructure is shown in figure 4.1.

Initialization step

Assuming the background object is a natural video object. In the beginning, each participating creator should have a copy of this original unwatermarked background object. All the creators should together create a joint non-invertible watermark JW . Then, the watermark is embedded into the background object using the joint-watermark embedding key K_{jw} , which is created from the participating creators individual joint-watermark embedding/detection keys, denoted by K_{jw_i} for the i^{th} creator. The joint-watermark detection key is same as that of embedding key. Each creator keeps a copy of the watermarked background object as well as original background object and their

CHAPTER 4. JOINT-CREATORSHIP PROTECTION FOR DIGITAL VIDEOS

Kjw_i 's.

Discussion: Each creator needs to keep a copy of the watermarked background object in addition to original background object and their Kjw_i 's for solving the creatorship replacement dispute as discussed in section 4.6.3. The initialization step is illustrated in figure 4.2.

Figure 4.2: Flowchart of initialization step

First iteration

In this chapter, we make an assumption that there are totally N video objects in the video to be created. For N creators, each creator creates one video object. The watermarking technique we employed is VOP/BGOP wised.

Step 1: Each creator creates his/her own video object. For example, the i^{th} creator creates VO_{i1} , and then embeds his/her watermark w_i using his/her watermark embedding key Kw_i into his/her creation VO_{i1} to obtain VO_{i1}^w . Each creator then makes a digitally signed version (using the private key of the creator) of their watermarked creation. The creator then stores his/her video object VO_{i1} , watermark w_i and embedding key Kw_i in a database DB_i . These information are needed to be presented to a judge in case of a creatorship dispute which is discussed in section 4.6.1. Finally, each creator will transmit the signed watermarked video object to all other creators. For example, the i^{th} creator transmits $Sign_i\{VO_{i1}^w\}$ to all other creators. Figure 4.3 gives the flowchart of step 1.

CHAPTER 4. JOINT-CREATORSHIP PROTECTION FOR DIGITAL VIDEOS

Figure 4.3: Flowchart of step 1

Discussion: We use different watermarks W_i for different creators and hence help to declare the full creatorship of their video objects. The watermarking scheme should be robust since others (including other creators) should not be able to remove the embedded watermark. In addition, the watermark should be invisible in such a way that the high visual quality of the watermarked video object is preserved. The transmitted digitally signed watermarked video objects prevent the creators from disowning their own video objects at a later stage. In the case that some creator try to disown the creatorship, the rest of the creators can show the signed version of the person's video object to establish the person's creatorship.

Step 2: On receiving the signed watermarked objects from other creators, the creator first stores them locally. The creator then verifies all the signed watermarked objects from all other creators, using the public keys of the corresponding signatures and obtains the respective watermarked objects. After the successful signature verification, every creator possesses his/her original video object and the watermarked video objects of all creators (VO_{i1}^w for all i 's). All creators then assemble the watermarked objects individually, and then discuss on how the video objects should be modified. Figure 4.4 illustrates the n^{th} frame of the video after the first iteration.

Figure 4.4: n^{th} frame after first iteration

Discussion: The received signed watermarked objects, own object, own watermark W_i , embedding key K_{W_i} and detection key $K_{W_i}^*$ are stored locally for checking malpractices by other creators during later iterations and also for reference in dispute

CHAPTER 4. JOINT-CREATORSHIP PROTECTION FOR DIGITAL VIDEOS

resolution which is discussed in section 4.6.1. Figure 4.5 shows the flowchart of Step 2.

Figure 4.5: Flowchart of step 2

Refinement iterations

Step 3: After all the creators agree on how to modify the video objects, the original creator will only modify the VOPs that need to be modified, and just rewatermark those modified VOPs. Each creator then makes a digitally signed version (using the private key of the creator) of their modified watermarked VOPs. The creator then stores his/her modified VOPs into database DB_i for solving the creatorship dispute. Finally, each creator will transmit the signed watermarked VOPs to all other creators. For example the i^{th} creator transmits $Sign_i \{ \text{all watermarked modified VOPs} \}$ to all other creators. The flowchart of step 3 is shown in figure 4.6.

Figure 4.6: Flowchart of step 3

Discussion: Normally, the creator does not need to modify all the VOPs of the video object in the second iteration and following iterations. So, they will also transmit only the watermarked modified VOPs of the video object to the rest of the creators. This will reduce the size of data transmission and storage requirement in the database.

Step 4: On receiving the signed watermarked modified VOPs from other creators, the creator first stores them locally. The creator then verifies all the signed watermarked VOPs from all other creators using the public keys of the corresponding signatures and

CHAPTER 4. JOINT-CREATORSHIP PROTECTION FOR DIGITAL VIDEOS

obtains the respective watermarked VOPs. Every creator after the successful signature verification possesses the watermarked modifications of all creators. Then, each creator uses the all modified VOPs to replace the corresponding VOPs in the corresponding stored watermarked video object. After that, all creators assemble the watermarked objects and again discuss how to modify the video objects. The figure 4.7 illustrates the process of this step.

Figure 4.7: Flowchart of step 4

Step 5: Iterations (step 3 and 4) are carried out until J^{th} iteration, i.e. the final video is obtained. The flowchart of Step 5 is shown in figure 4.8.

Figure 4.8: Flowchart of step 5

Discussion: Since all the creators have the watermarked video objects of the whole video, sometimes it is possible that a single creator or a group of creators may cheat another creator by putting a second watermark on the person’s video object. This action would cause both watermark to be detected from the same video object. In order to defeat this kind of attack, the watermarking technique should be non-invertible which would identify the original creator unambiguously even though two watermarks are detected from the same video object, which is illustrated in section 4.6.1.

Now, the image creation process is completed. We also need a registration to give an

CHAPTER 4. JOINT-CREATORSHIP PROTECTION FOR DIGITAL VIDEOS

overall view that how many creators are involved in the creation process and who they are. This can help the buyers to know who are the creators.

Registration step

All the creators then jointly submit the final video and their watermark detection keys Kw_i^* to a registration authority for registration. We assume the watermarking technique to be asymmetric and hence the watermark detection key is different from embedding key. Therefore the RA cannot perform the watermarking but can detect the watermarks. The RA first checks whether an identical/mostly similar video is already present in its database. If not present, the RA then checks the watermarks in the video objects. Each video object should have a watermark w_i . The RA then issues a digitally signed (signed by RA) creatorship certificate that contains the every creator's identities and his/her corresponding watermark detection key and identity of the watermarked video. If there is an identical/mostly similar video already existing in its database, the RA does not issue a creatorship certificate until the creatorships are resolved among the creators of old and new watermarked videos themselves or with the help of a judge. The RA stores the watermarked video and the creatorship-certificates in its database Y . The digitally signed creatorship certificate helps buyers to identify the creators. Figure 4.9 illustrates the whole registration process.

Figure 4.9: The flowchart of Registration Step

Once the final watermarked video and the creatorship is obtained, the joint creation phase is completed. Figure 4.10 describes the n^{th} frame of the final video.

CHAPTER 4. JOINT-CREATORSHIP PROTECTION FOR DIGITAL VIDEOS

Figure 4.10: n^{th} frame of final video after J^{th} iteration

We have developed a watermarking scheme suitable for our framework which is introduced in chapter 6.

4.4 Complexity Analysis of our Framework

We analyze the complexity from two aspects: transmission complexity and storage complexity. We do not count the background object in this analysis since the background object is only watermarked and stored at the beginning of creation process. No further transmission or storage of the background object is required. For the easiness of analysis, we assume uncompressed video objects rather than compressed video objects.

Suppose that the whole creation process contains J iterations, and there are N creators jointly creating the video. The i^{th} creator creates the video object VO_{ij} in the j^{th} iteration. The video object VO_{ij} contains arbitrary number of VOPs and takes up A_{ij} bytes. The whole video excluding the background object has a size of U bytes.

4.4.1 Transmission Complexity

Number of messages transmitted: the message is defined as the video object created or a set of VOPs modified by the i^{th} creator in the j^{th} iteration. In the first iteration, every creator must send his/her created video object to the other $N-1$ creators. So, there will be $N*(N-1)$ messages transmitted. In the next iteration, each creator still needs to transmit a set of modified VOPs to the other $(N-1)$ creators. So, for J iterations, there are $J*N*(N-1)$

CHAPTER 4. JOINT-CREATORSHIP PROTECTION FOR DIGITAL VIDEOS

messages transmitted.

Number of bytes transmitted: In the first iteration, the i^{th} creator sends the whole watermarked VO_{i1}^w to the other $N-1$ creators, i.e. $(N-1) * A_{i1}$ bytes are transmitted. So for N creators there will be $\sum_{i=1}^N (N-1) * A_{i1} = (N-1) * U$ bytes transmitted.

Normally, each creator will not modify the whole VO in the second and following iterations. For the i^{th} creator, let f_{ij} = (number of bytes of modified VOPs in the j^{th} iteration)/(number of bytes of the whole VO). In the first iteration, the whole video object will be created, so $f_{i1} = 1$ for all i 's. In the j^{th} iteration, each creator will transmit f_{ij} fraction of his/her VO. The creator may have different f_{ij} 's in different iterations, and different creators may have different f_{ij} 's. In the j^{th} iteration, the i^{th} creator modifies only $f_{ij} * A_{i1}$ bytes, and sends this to all the other $N-1$ creators, so totally $f_{ij} * A_{i1} * (N-1)$ bytes will be sent from the i^{th} creator. For N creators,

$$\sum_{i=1}^N f_{ij} * A_{i1} * (N-1)$$

bytes transmitted in j^{th} iteration.

It needs J iterations to complete the creation, so the total number of bytes transmitted will be $TDT = \sum_{j=1}^J \sum_{i=1}^N f_{ij} * A_{i1} * (N-1)$.

If all $f_{ij} = 1$, that means in every iteration, the i^{th} creator will transmit A_{i1} bytes to all the other $N-1$ creators. So,

$$TDT = \sum_{j=1}^J \sum_{i=1}^N A_{i1} * (N-1) = (N-1) * \sum_{j=1}^J \sum_{i=1}^N A_{i1} = (N-1) * \sum_{j=1}^J U = (N-1) * J * U \text{ bytes will be transmitted.}$$

Suppose that $U = 10$ Megabytes, figure 4.11 illustrates the total data transmitted against iteration numbers. We can see that this is a linear function and there are quite

CHAPTER 4. JOINT-CREATORSHIP PROTECTION FOR DIGITAL VIDEOS

large amount of information transmitted during the creation. Fortunately, this does not always happen. Most of the time, we will have a situation that $f_{ij} < 1$.

Figure 4.11: Total data transmitted for $f_{ij} = 1$

If $f_{ij} < 1$, for easy discussion, we assume that $f_{ij} / f_{i(j-1)} = f_a$, $\forall i \& j = 2 \dots J$. So, the total number of bytes transmitted will be

$$\text{TDT} = \sum_{j=1}^J \sum_{i=1}^N f_{ij} * A_{i1} * (N-1) = (N-1) \sum_{j=1}^J f_a^{j-1} * U = (N-1) * U * (1 - f_a^J) / (1 - f_a).$$

Figure 4.12 plots the total data transmitted against the iteration number with $f_a = 1/2$, and $U = 10$ Megabytes, and can be seen that with the increasing of iteration number J , the total data transmitted increases slower than the previous case where all $f_{ij} = 1$. This is due to f_a factor. In this case, Each iteration will only transmit f_a of previous iteration. As J tends to infinity, the upper bound of the data transmission is $(N-1) * U / (1 - f_a)$ bytes.

Figure 4.12: Total data transmitted for $f_a = 1/2$.

CHAPTER 4. JOINT-CREATORSHIP PROTECTION FOR DIGITAL VIDEOS

4.4.2 Storage Complexity

Here, also we ignore the background object since it only needs to store once at the beginning of the creation process. In the first iteration, the i^{th} creator needs to store his/her video object as well as all other creators' signed watermarked video objects. We neglect the watermarks and keys since they are small comparing to the video objects. Thus the total storage required for the first creator is $VO_{11} + VO_{21}^w + VO_{31}^w + \dots + VO_{N1}^w$ in the first iteration. VO_{ij} has the same size with VO_{ij}^w that both are A_{ij} bytes. So, in the first

iteration, any creator needs to store $\sum_{i=1}^N A_{i1} = U$ bytes.

In the following iterations, since all the creators will only modify parts of the video object, every creator will only store the modified VOPs of his/her created object and the VOPs that other creators send to him. Again, let f_{ij} =(number of bytes of modified VOPs in the j^{th} iteration)/(number of bytes of the whole VO). In the first iteration, the whole video object will be created, so $f_{i1} = 1$ for all i 's.

In the following iterations, if $f_{ij} = 1$, that means in every iteration, the creator will transmit A_{i1} bytes to all the other $N-1$ creators. It also means that in every iteration, the i^{th} creator needs to store U bytes. Totally, each creator needs to store $J*U$ bytes for J iterations.

If $f_{ij} < 1$, for easy discussion, here we still make the assumption that $f_{ij} / f_{i(j-1)} = f_a, \forall i \& j = 2 \dots J$. So, the total size of storage requirements is

$$TSR = \sum_{j=1}^J \sum_{i=1}^N f_{ij} * A_{i1} = \sum_{j=1}^J f_a^{j-1} * U = U * (1 - f_a^J) / (1 - f_a) \text{ bytes.}$$

We can see that the total number of the creators N does not affect the storage requirement for single creator. As J tends to infinity, the storage requirement is

CHAPTER 4. JOINT-CREATORSHIP PROTECTION FOR DIGITAL VIDEOS

asymptotic to $U/(1-f_a)$ bytes.

Figure 4.13 plots the total storage requirements against the number of iterations with $U = 10$ Megabytes, and can be seen that the smaller the f_a , the smaller storage is required.

Figure 4.13: Total storage requirement against the number of iterations

4.5 Application of our Framework

4.5.1 Rightful Creatorship Dispute Resolution

In the event of creatorship dispute among creators, the judge asks for the watermarks W_i , watermark detection key $K_{W_i}^*$ and the video object of dispute in the final watermarked video from the disputing creators. The judge then verifies the existence of watermarks in the disputed video object of the watermarked video. If there is more than one watermark found in the same video object, the judge uses non-invertible property (which needs to use the embedding key K_{W_i}) of the watermark to prove the rightful creator. For resolving the rightful creatorship dispute, the asymmetric property of the watermarking technique is not useful, thus the original unwatermarked object is necessary for using the non-invertibility property to prove the rightful creator. However, for creatorship verification by buyer, the asymmetric property is useful.

CHAPTER 4. JOINT-CREATORSHIP PROTECTION FOR DIGITAL VIDEOS

4.5.2 Creatorship Purchasing Situation

When a buyer wants to buy the entire jointly created video, the buyer identifies all the creators associated with the watermarked video from the RA signed creatorship certificate associated with the watermarked video. The buyer can then approach all the creators for purchase of the jointly created video. In the event that the buyer is interested in only part of the jointly created video, such as certain video object(s), the buyer can use the watermark detection key to identify the creators of the video objects that he/she is interested in and then contact those creators to purchase their video objects individually.

4.5.3 Creatorship Replacement Dispute Resolution

In the case of creatorship replacement dispute, suppose originally, there are only three creators, C_1 , C_2 , and C_3 . But later, C_1 and C_2 try to replace C_3 's creatorship with C_4 's creatorship by replacing C_3 's video object with C_4 's video object. And also replace the background object with a C_1 , C_2 and C_4 joint-watermarked background object. If this happens, C_3 can use the original background to claim that he is one of original creators of the video. The judge will then ask the watermarked background object from the disputed video, also the RA signed creatorship certificate of the disputed video to obtain the identities of the creators C_1 , C_2 and C_4 . The judge then asks C_1 , C_2 and C_4 for their original background object and Kjw_{C_1} , Kjw_{C_2} and Kjw_{C_4} of the disputed video. Using the non-invertible property, and the watermarked background from C_1 , C_2 and C_4 , judge verifies authenticity of the C_1 , C_2 and C_4 given background object. If this background is authentic, the C_1 , C_2 and C_4 given background object is then compared with C_3 given background object. If they are the same, the judge declares C_3 is the original creator who is replaced by C_4 .

CHAPTER 4. JOINT-CREATORSHIP PROTECTION FOR DIGITAL VIDEOS

4.6 Conclusion

We proposed a watermarking framework that solves the joint-creatorship protection problem in object-based video. The framework is applied during the video creation process. By employing the digital signature scheme and our designed watermarking scheme, the framework successfully handles the creatorship dispute problem among creators. And is also capable of proving the creatorship of the specified video object to a buyer. We have designed a watermarking scheme which is robust, imperceptible, asymmetric and non-invertible, which is explained in chapter 6. The research work in this chapter has been published in the paper [65].

Chapter 5

Joint-Creatorship Protection for Digital

Movies

This chapter presents the framework for movie joint-creatorship protection. 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 creators. In this chapter, we propose a framework for providing the creatorship protection of multiple creators involved in creating the object-based digital movies. 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. The complexity of the framework is analyzed by calculating the amount of data transmission and storage requirements. Experiments were conducted to study the effectiveness of the framework.

5.1 Introduction

The creator has creatorship of digital assets. Nowadays, many digital media are very complex and difficult to be created by a single creator.

CHAPTER 5. JOINT-CREATORSHIP PROTECTION FOR DIGITAL MOVIES

In the case of joint creation of digital media by multiple creators, there are some concerns for each of the participating creators. Firstly, each of the creators is concerned about his/her rightful share of creatorship of the final media product. It is possible that a group of creators (or a creator) can connive to remove another creator (or another group of creators) from creatorship of the final digital product. Therefore each of the creators wants to protect their own creatorship from the creatorship removal attack by other creators. Secondly, 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. Thirdly, 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 chapter, 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 music 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 chapter 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.

CHAPTER 5. JOINT-CREATORSHIP PROTECTION FOR DIGITAL MOVIES

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 chapter is structured as follows: Our proposed framework is presented in section 5.2. Section 5.3 lists some application of our framework. The complexity of our framework is analyzed in section 5.4. Section 5.5 shows the experimental results. Section 5.6 presents some discussions on the framework and section 5.7 concludes this chapter.

5.2 Our Proposed Framework

In our proposed framework, a digital movie creation has four stages: initialization process, video creation process, audio creation/dubbing process and registration process. Figure 5.1 gives the flowchart of the whole digital movie creation process.

Figure 5.1: The digital movie creation process

Brief Description: In the proposed framework the movie creation begins with an initialization process where all the creators (including audio and video creators) jointly create a watermark and then watermark the video background with the jointly created watermark. Once the initialization process is over, the video creation process begins with each video creator creating his/her video object. Created video objects are then watermarked and signed by respective creators. And are then transmitted over the network to every other participating video creators. On receiving every others signed watermarked video objects, each video creator then assembles a local video part of the

CHAPTER 5. JOINT-CREATORSHIP PROTECTION FOR DIGITAL MOVIES

movie by combining every others watermarked video objects, background object 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 figure 5.2 and they exchange their creations through the network to every other creators, which are then assembled locally by every creators. Thus, the video creators necessarily need not be connected to a single computer.

Figure 5.2: 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 iterative manner until all the creators are satisfied with the audio part. And the dubbing is usually done in single computer as shown in figure 5.3.

CHAPTER 5. JOINT-CREATORSHIP PROTECTION FOR DIGITAL MOVIES

Figure 5.3: Hardware infrastructure of audio creation process

Finally in the registration process, all the creators including video creators and audio creators will together go to the Registration Authority (RA) to register the created digital movie. After the registration, the whole movie creation process is finished.

Let N_v be the number of video creators, N_a be the number of audio creators and $N = N_v + N_a$ be the total number of creators jointly creating an object-based movie. Let there be J iterations to complete the video creation process and J iterations to complete the audio creation process.

Notation: The notation $Sign_i\{m\}$ denotes the digitally signed message m signed by the i^{th} creator using his/her private key. This signed message can be verified by everyone using the corresponding public key. The verification of signed message will result in message m , thus anyone can obtain the message from $Sign_i\{m\}$.

The four processes are discussed in detail below.

5.2.1 Initialization Process

The video contains one background object (BGO) and a few video objects (VOs). The background object is made up of several consecutive background object planes (BGOPs) and the video object is made up of several consecutive video object planes (VOPs).

Assuming the background object (BGO) is a natural video object. In the beginning, each participating creator should have a copy of this original unwatermarked background object. All the creators should together create a joint non-invertible watermark JW . Then,

CHAPTER 5. JOINT-CREATORSHIP PROTECTION FOR DIGITAL MOVIES

the watermark W is embedded into BGO in BGOP wise. That is the watermark W is embedded into each BGOP using the joint-watermark embedding key K_{jw} , which is generated from the participating creators individual joint-watermark embedding/detection keys, denoted by K_{jw_i} for the i^{th} creator. The joint-watermark detection key is same as that of embedding key. Each creator keeps a copy of the watermarked BGO in addition to original background object and their K_{jw_i} . Guo's scheme [8] can be used in this process. Figure 5.4 gives the flowchart of the whole initialization process.

Figure 5.4: Initialization process

Discussion: Each creator needs to keep a copy of the watermarked BGO in addition to original BGO and their K_{jw_i} 's for solving the creatorship replacement dispute as discussed in section 5.3.3.

5.2.2 The Video Creation Process

After the initialization process, which is carried out on the background object (BGO), the video is created in an iterative manner. The iteration steps focus on the video objects (VOs) created by the video creators. Let VO_{ij} be the video object created or modified by the i^{th} creator in the j^{th} iteration and VO_{ij}^w be the watermarked VO_{ij} using W_i . Each VO is made up of several consecutive video object planes (VOPs). Let VOP_{ijn} be the n^{th} VOP of VO_{ij} and VOP_{ijn}^w be the watermarked VOP_{ijn} using W_i .

First iteration

For easiness of explanation, let there be N_v video creators and each video creator creates one VO each.

Step 1: Each video creator creates his/her own VO. For example, the i^{th} creator creates VO_{i1} in the first iteration. Then embeds his/ her watermark W_i using his/her

CHAPTER 5. JOINT-CREATORSHIP PROTECTION FOR DIGITAL MOVIES

watermark embedding key K_{w_v} into his/her creation VO_{i1} to obtain VO_{i1}^w . The watermarking technique employed is asymmetric and hence the corresponding asymmetric detection key is $K_{w_v}^*$. The watermarking is carried out VOP wise, i.e. the watermark w_i is embedded into each VOP using the watermark embedding key K_{w_i} . Thus watermarked n^{th} VOP of VO_{i1} would be denoted as VO_{i1n}^w .

Each video creator then makes a digitally signed version (using the private key of the creator) of their watermarked creation and transmits them to all other video creators. For example, the i^{th} creator transmits $Sign_i\{VO_{i1}^w\}$ to all other creators. The creator then stores his/her video object VO_{i1} , watermark w_i , embedding key K_{w_v} and detection key $K_{w_v}^*$ in a database DB_i . These information are needed to be presented to a judge in case of a creatorship dispute which is discussed in section 5.3.1.

Discussion: We use different watermarks w_i for different creators and hence help to declare the full creatorship of their video objects. The watermarking scheme should be robust since others (including other creators) should not be able to remove the embedded watermark. In addition, the watermark should be invisible in such a way that the high visual quality of the watermarked video object is preserved. In order the buyer to buy a particular video object, the buyer should be able to verify the existence of the watermark in that object without the capability to remove or embed the watermark, which requires the watermarking technique to be asymmetric as well. The transmitted digitally signed watermarked video objects prevent the creators from disowning their own video objects at a later stage. In the case that certain creator tries to disown the creatorship, the rest creators can show the signed version of the person's video object to establish the person's creatorship.

Step 2: On receiving the signed watermarked objects from other creators, the video

CHAPTER 5. JOINT-CREATORSHIP PROTECTION FOR DIGITAL MOVIES

creator first stores them locally. The creator then verifies all the signed watermarked objects from all other creators, using the public keys of the corresponding signatures and obtains the respective watermarked objects. If there is no signature detected, the video creator will ask for the retransmission of that particular video object. After the successful signature verification, every creator possesses his/her original video object and the watermarked video objects of all creators (VO_i^* for all i 's). All creators then assemble the watermarked objects individually, and then discuss on how the video objects should be modified. Figure 5.5 gives the flowchart of first iteration. Figure 5.6 illustrates the n^{th} frame of the video after the first iteration.

Figure 5.5: First iteration of video creation process

Figure 5.6: The n^{th} frame after first iteration

Discussion: The received signed watermarked objects, own object VO_i , own watermark W_i , embedding key $K_{W_{iv}}$ and detection key $K_{W_{iv}}^*$ are stored locally for checking malpractices by other creators during later iterations and also for reference in dispute resolution which is discussed in section 5.3.1.

CHAPTER 5. JOINT-CREATORSHIP PROTECTION FOR DIGITAL MOVIES

Refinement iterations

Step 3: After all the video creators agree on how to modify the video objects, the original creator will only modify the VOPs that need to be modified, and just rewatermark those modified VOPs. Each creator then makes a digitally signed version (using the private key of the creator) of their modified watermarked VOPs and then transmits them to all other video creators. For example the i^{th} creator transmits $Sign_i \{ \text{all watermarked modified VOPs} \}$ to all other video creators. The video creator then stores his/her modified VOPs into database DB_i for solving the creatorship dispute.

Discussion: Normally, the creator does not need to modify all the VOPs of the video object in the second iteration and following iterations. So, they will also transmit only the watermarked modified VOPs of the video object to the rest of the creators. This will reduce the size of data transmission and storage requirement in the database.

Step 4: On receiving the signed watermarked modified VOPs from other video creators, the creator first stores them locally. The creator then verifies all the signed watermarked VOPs from all other video creators using the public keys of the corresponding signatures and obtains the respective watermarked VOPs. If no correct signature is detected, the creator will ask for the retransmission of that object. Every video creator after the successful signature verification possesses the watermarked modifications of all creators. Then, each creator uses all the modified VOPs to replace the corresponding VOPs in the corresponding stored watermarked video object. After that, all video creators assemble the watermarked objects and again discuss how to modify the video objects. The iteration is shown in figure 5.7.

CHAPTER 5. JOINT-CREATORSHIP PROTECTION FOR DIGITAL MOVIES

Figure 5.7: Refinement iterations of video creation process

Step 5: Iterations (step 3 and 4) are carried out until J^{th} iteration, i.e. the final video is obtained. Figure 5.8 describes the n^{th} frame of the final video.

Discussion: Since all the creators have the watermarked video objects of the whole video, sometimes it is possible that a single creator or a group of creators may cheat another creator by putting a second watermark on the person's video object. This action would cause both watermark to be detected from the same video object. In order to defeat this kind of attack, the watermarking technique should be non-invertible which would identify the original creator unambiguously even though two watermarks are detected from the same video object, which is illustrated in section 5.3.1.

Figure 5.8: The n^{th} frame of the final video after J^{th} iteration

5.2.3 The Audio Creation/Dubbing Process

After the video creation process, a complete video with all the watermarks and without any audio is produced. This video will be signed by all the video creators and then passed to the audio creators. The subsequent audio dubbing process will add all the audio tracks to the video to complete the whole movie. The audio tracks can be dialogs of characters,

CHAPTER 5. JOINT-CREATORSHIP PROTECTION FOR DIGITAL MOVIES

background music (including special effects such as thunder, car engine sounds etc.) and foreground music. The background and foreground music tracks may be created beforehand but dubbed along with the dialogs on to the movie. In audio creation process, different audio tracks will be considered as different audio objects. For easiness of discussion, we consider only one background music object (BO) created by one creator, one foreground music object (FO) created by another creator and several audio dubbers dubbing the dialog objects (DOs) of characters in the movie.

Discussion: The audio creators will request the video creators to send a signed version of the video. So, in the case that the video creators replace the original audio objects by new set of audio objects which are created by another set of audio creators, the original set of audio creators can show the signed version to claim that in fact they also participated in the creation of the movie.

The audio creation/dubbing process is also conducted in an iterative manner. But for the easiness of explanation, we assume that the background and foreground music are perfect so they will not be modified during the iteration process. The audio creation/dubbing is usually carried out in one single computer.

First iteration

Let there be N_a audio creators and each audio creator creates one Audio Object (AO) each. For dialog of characters, each character's voice will be treated as one dialog object DO_i , which is dubbed by i^{th} creator in the 1st iteration. Then, the audio object created by the i^{th} creator will be watermarked with a watermark embedding key Kw_{ia} which is only known to him/her (the corresponding detection key is Kw_{ia}^*). Let FO_i be the foreground music object created by i^{th} creator and BO_i be the background music object created by i^{th} creator. FO_i and BO_i are also watermarked with watermark embedding key Kw_{ia} to obtain

CHAPTER 5. JOINT-CREATORSHIP PROTECTION FOR DIGITAL MOVIES

FO_i^w and BO_i^w . The watermarking scheme employed here needs to be asymmetric. The asymmetry property can help in the registration process which is discussed in section 5.2.4.

Then, the watermarked audio objects will be signed by their respective audio creators. Each audio creator then makes copies of their signed watermarked audio object which are then passed to all the other creators. All the audio creators store the received audio objects and multiplex the watermarked audio objects together with the watermarked video objects. At this stage, the first draft of audio dubbing is produced. The first iteration is illustrated in figure 5.9.

Figure 5.9: The first iteration in the audio creation process

Discussion: The watermarking scheme used here must be robust, imperceptible, asymmetric and non-invertible. First, to protect the audio creator's creatorship, the watermarking scheme must be robust so the attackers cannot remove the watermark easily. Second, the human audible system is quite sensitive to the audio, so the watermarking scheme must be imperceptible to keep a good quality of audio. Third, the buyer of the movie may use the watermark to identify the creator of certain audio object, so the watermarking scheme is required to be asymmetric. Fourth, sometimes, attackers may put another watermark on a watermarked audio object. In the detection process, usually two watermarks will be detected; the non-invertibility will help to resolve this problem. For any audio object, if it is found to be illegal in a later time, the creator cannot disown his/her creatorship since all the other creators have his/her signed object. The signature can also prove the creator's joint creatorship. If some audio creators want to remove one audio creator's creatorship by removing his/her object, this creator can show all the other creators' signed version of the object to prove that he is one of the creators.

CHAPTER 5. JOINT-CREATORSHIP PROTECTION FOR DIGITAL MOVIES

Refinement iterations

The first draft of the audio dubbing may not satisfy all the people. This requires the audio creators to do some modification on the audio objects. So, the audio creators will modify the parts which are not good enough and rewatermark that part. After the watermarking, the modified parts will be signed by the audio creators and passed to all the audio creators. Then again all the audio creators multiplex the audio and video objects for further evaluation. This process may repeat several times until all the creators (video creators and audio creators) are satisfied with the audio objects. The process is shown in figure 5.10.

Figure 5.10: Refinement iterations of audio creation process

Now, the movie creation process is completed, we also need a registration process to give an overall idea that how many creators are involved in the creation process and who they are. This can help the buyers to know who are the creators and single creator cannot sell the movie individually.

5.2.4 Registration Process

All the creators (including video and audio creators) then jointly submit the final movie product and their watermark detection keys K_{W_i} to a registration authority (RA) for registration. We assume the watermarking technique to be asymmetric and hence the watermark detection key is different from embedding key. Therefore the RA cannot perform the watermarking but can detect the watermarks. The RA first checks whether an identical/mostly similar movie is already present in its database. If not present, the RA then checks the watermarks in the video/audio objects. Each video/audio object should

CHAPTER 5. JOINT-CREATORSHIP PROTECTION FOR DIGITAL MOVIES

have a watermark w_i . The RA then issues a digitally signed (signed by RA) creatorship certificate that contains the every creator's identities and his/her corresponding watermark detection key and identity of the watermarked movie. If there is an identical/mostly similar movie already existing in its database, the RA does not issue a creatorship certificate until the creatorships are resolved among the creators of old and new watermarked movies themselves or with the help of a judge. The RA stores the watermarked movie and the creatorship certificate in its database Y . The digitally signed creatorship certificate helps buyers to identify the creators. Once the final watermarked movie and the digitally signed creatorship certificate are obtained, the whole joint creation process is completed. Figure 5.11 shows the flowchart of the registration step

Figure 5.11: Registration step

5.3 Applications of the Proposed Framework

In this section, we will give some applications of the proposed framework. Section 5.3.1 and 5.3.3 tell that how our framework works for creatorship dispute resolution, and 5.3.2 is for creatorship purchasing under the framework. These three situations are discussed in detail below and our framework can successfully handle the three situations.

5.3.1 Rightful Creatorship Dispute Resolution

In the event of creatorship dispute among creators, the judge asks for the watermarks w_i ,

CHAPTER 5. JOINT-CREATORSHIP PROTECTION FOR DIGITAL MOVIES

watermark detection key κ_{w_i} and the video/audio object of dispute in the final watermarked movie from the disputing creators. The judge then verifies the existence of watermarks in the disputed video/audio object of the watermarked movie. If there is more than one watermark found in the same video/audio object, the judge uses non-invertible property (which needs to use the embedding key κ_{w_i}) of the watermark to prove the rightful creator. For resolving the rightful creatorship dispute, the asymmetric property of the watermarking technique is not useful, thus the original unwatermarked object is necessary for using the non-invertibility property to prove the rightful creator. However, for creatorship verification by buyer, the asymmetric property is useful.

5.3.2 Creatorship Purchasing Situation

When a buyer wants to buy the entire jointly created movie, the buyer identifies all the creators associated with the watermarked movie from the RA signed 'creatorship certificate associated with the watermarked movie. The buyer can then approach all the creators for purchase of the jointly created movie. In the event that the buyer is interested in only part of the jointly created movie, such as certain video object(s), the buyer can use the watermark detection key to identify the creators of the video objects that he/she is interested in and then contact those creators to purchase their video objects individually. Because of the asymmetric property, the buyer can detect the watermark without knowing the embedding key. Once the buyer buys the movie, one question raised is that how the buyer can protect his/her ownership. This is a problem regarding to ownership protection, which will not be discussed in this multiple creatorship protection problem.

5.3.3 Creatorship Replacement Dispute Resolution

In the case of creatorship replacement dispute, suppose originally, there are only three creators, C_1 , C_2 , and C_3 . But later, C_1 and C_2 try to replace C_3 's creatorship with C_4 's creatorship by replacing the background object with a C_1 , C_2 and C_4 joint-watermarked

CHAPTER 5. JOINT-CREATORSHIP PROTECTION FOR DIGITAL MOVIES

background object. If this happens, C_3 can use the original background to claim that he is one of original creators of the movie. To prove the involvement, besides the unwatermarked background object, C_3 also need to provide a key to the judge, which can do the successful joint watermark detection together with C_1 and C_2 's keys $K_{jw_{C_1}}$, $K_{jw_{C_2}}$. Besides the background, the judge also asks C_3 to show his/her object in the disputed movie. In case that C_4 's watermark is also appearing in that object (put a second watermark), Judge can use the non-invertible property to show who is the true creator of that object. The one create that object is the original creator who is replaced.

5.4 Complexity Analysis of the Proposed Framework

So far, there are no other frameworks proposed to solve this kind of multiple creatorship protection problems. So we cannot compare the efficiency with others. We will analyze the complexity of our framework.

We will discuss the complexity in video creation process and audio creation process separately. We analyze the complexity from two aspects: transmission complexity and storage complexity for both video creation and audio creation. We do not calculate the complexity of initialization process since it is very straightforward where the background object is just watermarked and stored once. There is no further transmission or storage is required. For easiness of discussion, we assume uncompressed data rather than compressed data in this analysis.

5.4.1 Complexity in Video Creation

In the video creation complexity analysis, suppose that the whole creation process contains J iterations, and there are N_v video creators jointly creating the video part. The i^{th} creator C_i creates the video object VO_{ij} in the j^{th} iteration. The video object VO_{ij} contains

CHAPTER 5. JOINT-CREATORSHIP PROTECTION FOR DIGITAL MOVIES

arbitrary number of VOPs and takes up A_{ij} bytes. Let the integer set $CV = \{i \mid C_i \text{ is a video creator and } i \text{ is an integer and } 0 < i \leq N\}$. All the video objects have a total size of U bytes.

5.4.1.1 Transmission Complexity for Video

Number of Messages Transmitted: the message is defined as the video object created or a set of VOPs modified by the i^{th} creator in the j^{th} iteration. In the first iteration, every video creator must send his/her created video object to the other $N_v - 1$ video creators. So, there will be $N_v * (N_v - 1)$ messages transmitted. In the next iteration, each creator still needs to transmit a set of modified VOPs to the other $(N_v - 1)$ creators. So, for J iterations, there are $J * N_v * (N_v - 1)$ messages transmitted.

Number of Bytes Transmitted: In the first iteration, the i^{th} creator sends the whole watermarked VO_{i1}^w to the other $N_v - 1$ video creators, i.e. $(N_v - 1) * A_{i1}$ bytes are transmitted. So for N_v video creators there will be

$$\sum_{i \in CV} (N_v - 1) * A_{i1} = (N_v - 1) * U \text{ bytes transmitted.}$$

Normally, each video creator will not modify the whole VO in the refinement iterations. For the i^{th} creator, let $f_{ij} = (\text{number of bytes of modified VOPs in the } j^{th} \text{ iteration}) / (\text{number of bytes of the whole VO})$. In the first iteration, the whole video object will be created, so $f_{i1} = 1$ for all i 's. In the j^{th} iteration, each video creator will transmit f_{ij} fraction of his/her VO. The video creators may have different f_{ij} 's in different iterations, and in any iteration, different creators may have different f_{ij} 's. In the j^{th} iteration, the i^{th} creator modifies only $f_{ij} * A_{i1}$ bytes, and sends this to all the other $N_v - 1$ video creators, so totally $f_{ij} * A_{i1} * (N_v - 1)$ bytes will be sent from the i^{th} creator. For N_v video creators, $\sum_{i \in CV} f_{ij} * A_{i1} * (N_v - 1)$ bytes transmitted in j^{th} iteration.

CHAPTER 5. JOINT-CREATORSHIP PROTECTION FOR DIGITAL MOVIES

It needs J iterations to complete the creation, so the total number of bytes transmitted will be

$$\text{TDTv} = \sum_{j=1}^J \sum_{i \in C^j} f_{ij} * A_{i1} * (N_v - 1) \quad (5.1)$$

If all $f_{ij} = 1$, that means in every iteration, the i^{th} creator will transmit A_{i1} bytes to all the other $N_v - 1$ video creators. So,

$$\text{TDTv} = \sum_{j=1}^J \sum_{i \in C^j} A_{i1} * (N_v - 1) = (N_v - 1) * \sum_{j=1}^J \sum_{i \in C^j} A_{i1} = (N_v - 1) * \sum_{j=1}^J U = (N_v - 1) * J * U \text{ bytes will be transmitted.}$$

Suppose that $U = 10$ Megabytes, figure 5.12 illustrates the total data transmitted against iteration numbers. We can see that this is a linear function and there are quite large amount of data transmitted during the creation. Fortunately, this does not always happen. Most of the time, we will have a situation that $f_{ij} < 1$.

Figure 5.12: Total data transmitted against iteration number ($f_{ij} = 1$)

If $f_{ij} < 1$, for easy discussion, we assume that $f_{ij} / f_{i(j-1)} = f_a, \forall i \& j = 2 \dots J$. So, the total number of bytes transmitted will be

$$\text{TDTv} = \sum_{j=1}^J \sum_{i \in C^j} f_{ij} * A_{i1} * (N_v - 1) = (N_v - 1) \sum_{j=1}^J f_a^{j-1} * U = (N_v - 1) * U * (1 - f_a^J) / (1 - f_a).$$

Figure 5.13 plots the total data transmitted against the iteration number with $f_a = 1/2$, and $U = 10$ Megabytes, and can be seen that with increasing J , the total data transmitted

CHAPTER 5. JOINT-CREATORSHIP PROTECTION FOR DIGITAL MOVIES

increases slower than the previous case where all $f_{ij} = 1$. Here we take the average value that $f_a = 1/2$, which gives the general case. As an average value, $1/2$ is chosen for f_a . This is due to f_a factor. Each iteration will only transmit f_a of previous iteration. As J tends to infinity, the upper bound of the data transmission is $(N_v - 1) * U / (1 - f_a)$ bytes. For $f_a = 1/2$, $U = 10$ Megabytes and $N_v = 10$, the value will be 180 Megabytes.

Figure 5.13: Total data transmitted against the iteration number ($f_{ij} < 1$)

5.4.1.2 Storage Complexity for Video

Here, also we ignore the background object since it only needs to store once at the beginning of the creation process. We neglect the watermarks and keys since they are deducible from the original video object. In the first iteration, the i^{th} creator needs to store his/her video object as well as all other creators' signed watermarked video objects. Thus the total storage required for the any video creator is his/her VO and watermarked VO of all the other video creators. VO_{ij} has the same size with VO_{ij}^* that both are A_{ij} bytes. So, in the first iteration, any creator needs to store $\sum_{i \in C \setminus V} A_{i1} = U$ bytes.

In all the refinement iterations, since all the creators will only modify parts of the video object, every creator will only store the modified VOPs of his/her created object and the VOPs that other creators send to him. Again, let f_{ij} = (number of bytes of modified VOPs in the j^{th} iteration) / (number of bytes of the whole VO). In the first iteration, the

CHAPTER 5. JOINT-CREATORSHIP PROTECTION FOR DIGITAL MOVIES

whole video object will be created, so $f_{i1}=1$ for all i 's.

If $f_{ij}=1$ for all the refinement iterations, then the video creator would transmit A_{i1} to all other video creators in every refinement iteration. It also means that in every iteration, the i^{th} creator needs to store U bytes. Totally, each creator needs to store $J \cdot U$ bytes for J iterations.

If $f_{ij} < 1$, for easy discussion, here we still make the assumption that $f_{ij}/f_{i(j-1)} = f_a, \forall i \text{ \& } j = 2 \dots J$. So, the total bytes of storage requirements for each single video creator is

$$\text{SSR}_v = \sum_{j=1}^J \sum_{i \in C \setminus i'} f_{ij} \cdot A_{i1} = \sum_{j=1}^J f_a^{j-1} \cdot U = U \cdot (1 - f_a^J) / (1 - f_a) \quad (5.2)$$

We can see that the total number of the video creators N_v does not affect the storage requirement for single video creator. As J tends to infinity, the storage requirement is asymptotic to $U/(1-f_a)$ bytes.

Figure 5.14 plots the total storage requirements against the number of iterations with $U = 10$ Megabytes, and can be seen that the smaller the f_a , the smaller storage is required, if we make $f_a = 1/2$, i.e. each iteration will only modify half of previous iteration, the total storage requirement will be $10/(1-(1/2)) = 20$ Megabytes which is twice of the total video size for infinite number of iterations.

Figure 5.14: Storage requirement for single video creator

CHAPTER 5. JOINT-CREATORSHIP PROTECTION FOR DIGITAL MOVIES

For N_v video creators, the system-wide total storage requirement $TSR_v = N_v * SSR_v$.

5.4.2 Complexity in Audio Creation

We assume the i^{th} creator will create B_{ij} bytes of audio objects in j^{th} iteration. And the sum of all the audio objects has a size of S bytes. Let the integer set $CA = \{i \mid C_i \text{ is an audio creator and } i \text{ is an integer and } 0 < i \leq N\}$.

5.4.2.1 Transmission Complexity for Audio

We can see from the audio creation process, the audio is dubbed in a single computer. Hence, there is no data transmission. The transmission complexity of audio creation process is negligible.

5.4.2.2 Storage Complexity for Audio

Before the first iteration of audio creation process, every audio creator needs to store the video which is signed by all the video creators which is U bytes.

In the first iteration, all the audio objects have been created. Each audio creator will store his/her own object and others watermarked object. In the refinement iterations, they need to store the modified parts of objects. $f_{ij} = B_{ij} / B_{i1}$. Comparing the creation process of video and audio, we can conclude that the expressions of storage requirement for video and audio has similar manner except that the audio creator need to store additional U bytes. So, the storage requirement for each single audio creator is

$$SSRa = \sum_{j=1}^J \sum_{i \in CA} f_{ij} * B_{i1} + U = \sum_{j=1}^J f_a^{j-1} * S + U = S * (1 - f_a^J) / (1 - f_a) + U \text{ bytes.}$$

For N_a audio creators, the system wide storage requirement is $TSRa = N_a * SSRa$ (5.3)

CHAPTER 5. JOINT-CREATORSHIP PROTECTION FOR DIGITAL MOVIES

5.4.3 Total Complexity

5.4.3.1 Total Transmission Complexity

This is the same as the transmission complexity in the video creation process since the audio part is dubbed in a single computer where there is no data transmission. If we assume in every iteration, all creator will modify the same percentage of previous iteration, and define $r_j = f_{ij} / f_{i(j-1)}$, the total data transmission is

$$TDT = TDT_v = \sum_{j=1}^J \sum_{i \in CV} f_{ij} * A_{i1} * (N_v - 1) = (N_v - 1) * U * \sum_{j=1}^J \prod_{t=1}^j r_t \quad (5.4)$$

5.4.3.2 Total Storage Complexity

So, for $N = N_v + N_a$ creators, the system-wide total storage requirement is $TSR_v + TSR_a$.

$$\begin{aligned} TSR &= TSR_v + TSR_a = N_v * \sum_{j=1}^J \sum_{i \in CV} f_{ij} * A_{i1} + N_a * (\sum_{j=1}^J \sum_{i \in CA} f_{ij} * B_{i1} + U) \\ &= N_v * U * \sum_{j=1}^J \prod_{t=1}^j r_t + N_a * S * \sum_{j=1}^J \prod_{t=1}^j r_t + N_a * U \quad (5.5) \end{aligned}$$

If we assume that $f_{ij} / f_{i(j-1)} = f_a, \forall i \& j = 2 \dots J$. So, the total data transmission will be

$$TSR = N_v * U * (1 - f_a^J) / (1 - f_a) + N_a * S * (1 - f_a^J) / (1 - f_a) + N_a * U.$$

Figure 5.15: Total system-wide storage requirements

If we use $N_v = N_a = 10$, $f_a = 1/2$, J is infinity, $U = 10$ Megabytes and $S = 1$

CHAPTER 5. JOINT-CREATORSHIP PROTECTION FOR DIGITAL MOVIES

Megabytes, the result will be 320 Megabytes. Figure 5.15 shows the curve of TSR for J from 1 to 10.

After analyzing the complexity, we can conclude that on average, each video creator needs to store only twice of the original video size, and each audio creator needs to store the sum of video size and twice of audio size. This is very low cost. The transmission complexity in the network is also acceptable.

No specific watermarking algorithm has been considered in this analysis. Any watermarking scheme satisfies those requirements, which are robustness, imperceptibility, asymmetry and non-invertibility can be applied.

5.5 Experimental Results

In this section, we will give an experiment. We use matlab to simulate our framework environment. And we assume the numbers of iterations in video creation process and audio creation process are both 10000, which is large.

5.5.1 Number of Bytes Transmitted

The total data transmitted can be calculated from equation (5.4),

$$\text{TDT} = \text{TDT}_v = (N_v - 1) * U * \sum_{j=1}^J \prod_{i=1}^J r_i$$

Figure 5.16: Total data transmitted of 100 Experiments

CHAPTER 5. JOINT-CREATORSHIP PROTECTION FOR DIGITAL MOVIES

We use $N_v = 10$, $U = 10$ Megabytes, $J = 10000$ and r_t 's are uniformly distributed from 0 to 1. We carried out 100 experiments of movie creations; the result of TDT for each movie creation is plotted in figure 5.16. We can see that the largest value is 386.2344 Megabytes, which is 38.62344 times of the original movie size. The smallest value 91.1099 Megabytes, which is about 9.11099 times of the original movie size. And the average value is 180.6606 Megabytes, which is about 18.06606 times of the original movie. And the value 180.6606 is very similar to the theoretical value we calculate in Section 5.5.3.1 above, where $f_a = 1/2$ for every iteration.

5.5.2 Storage Requirements

Equation (5.5) gives the expression of total storage requirement.

$$\text{TSR} = N_v * U * \sum_{j=1}^J \prod_{t=1}^J r_t + N_a * S * \sum_{j=1}^J \prod_{t=1}^J r_t$$

We use that $U = 10$ Megabytes, $S = 1$ Megabytes, $N_v = N_a = 10$, $J = 10000$ and r_t 's are uniformly distributed from 0 to 1. We carried out 100 experiments of movie creations; the result of TSR for each movie creation is plotted in figure 5.17.

Figure 5.17: Total storage requirements of 100 experiments

From figure 5.17, we can see that the largest value is 544.7230 Megabytes, which is about 49.5203 times of the movie. The smallest value is 218.0937 Megabytes, which is about 19.8267 times of the movie size. And the average is 323.4743 Megabytes, which is

CHAPTER 5. JOINT-CREATORSHIP PROTECTION FOR DIGITAL MOVIES

about 29.4068 times of the movie size. The average value of the total storage requirement is quite similar to the theoretical value calculated in section 5.5.3.2 where $f_a = 1/2$.

5.6 Discussion

The watermarking scheme used in the creatorship protection for multiple creators has the following requirements. First, the watermarking scheme should be robust for the reason that others (including other creators) should not be able to remove the placed watermark. Second, the watermark should be imperceptible in order to have a high quality of video or audio object. Third, it is possible that a conniving creator(s) can place a second watermark on the creation of the creator whom conniving creator(s) wants to get rid of creatorship and claim for the creatorship of that part. In order to safe guard against such attacks the watermarking scheme used must be non-invertible. Fourth, the buyer of the jointly created movie should be able to verify the existence of the watermark (without the capability to remove it or embed it), which requires the watermarking technique to be asymmetric as well. Each creator should watermark his/her video/audio object completely. This will help to identify the creator of the video/audio object. Thus the watermarking technique employed in the framework should have the following properties: robust, invisible, asymmetric and non-invertible. It is possible that a creator disowns his/her video object at a later stage due to the malpractices (copying from someone else's work etc.) he/she has done during the creation. In order to defeat this problem, the framework employs cryptographic protocols in the video creation process.

5.7 Conclusion

We proposed a novel watermarking framework that solves the creatorship protection problem in the creation of multiple creators, object-based digital movie. The framework

CHAPTER 5. JOINT-CREATORSHIP PROTECTION FOR DIGITAL MOVIES

employs the watermarking and digital signature scheme and is applied during the video creation and audio creation/dubbing process. The framework successfully handles the creatorship dispute problem among creators; the creatorship replacement problem is also solved. At the same time, the single creator cannot disown his/her creatorship of the object he created. By applying the framework, the creator also has the capability to prove the creatorship of his/her video/audio object to a buyer. The research work in this chapter has been published in the paper [67].

Chapter 6

Our Watermarking Scheme

In this chapter, we will present our watermarking scheme in detail. The watermarking scheme is for digital image creatorship protection framework, but it can be easily extended to video and audio by changing the dimension of watermark, embedding keys and extraction keys.

The designed frameworks shown in previous three chapters require a robust, imperceptible, asymmetric and non-invertible watermarking scheme. Therefore, we build a watermarking scheme that satisfies all the above requirements.

Notations: Following notations are used for describing the algorithm:

IMG	original image
img	image element
w	watermark element
W	watermark
IMG^w	watermarked image
G	watermark embedding key
E	watermark extraction key
W^E	extracted watermark
KEY	DES key of the of the original creator
G'	fake watermark embedding key
W'	fake watermark

CHAPTER 6. OUR WATERMARKING SCHEME

IMG' fake original image

KEY' fake DES key

The purpose of watermark in our watermarking framework is to protect the creator's creatorship as explained in chapter 3, 4 and 5. If there is no careful scheme design and proper requirements on the watermark, an attacker can manipulate the watermarked image and claim he/she is also an original creator.

After studying Qiao [7] and Tzeng [64]'s watermarking method, we combine the strongpoint of the two methods, and modify it to make it suitable for our framework.

6.1 Watermark Construction

First, the watermark to be embedded into the image is constructed. Non-invertibility is a must to solve the "rightful creatorship" problem. In order to make the watermark non-invertible, we make a strict requirement on the construction of the watermark. We bind the watermark to the original image. Given an original image *IMG* with dimension $N*M$, we create the watermark $W = \{w_1 w_2 w_3 \dots w_{N*M}\}$ by applying a standard encryption function such as DES with an encryption key *KEY*. The watermark will have the same size as the original image. We construct our watermark in the following procedure.

1. Present the original image in a set format. The elements are the pixels of the original image. I.e., $IMG = \{img_1 img_2 img_3 \dots img_{N*M}\}$.
2. Group each 8 pixels of the original image. The original $N*M$ 8-bit elements will be changed to $N*M/8$ 64-bit elements. $GI = \{gi_1 gi_2 gi_3 \dots gi_{N*M/8}\}$, where $gi_j = \{img_{(j-1)*8+1} img_{(j-1)*8+2} img_{(j-1)*8+3} \dots img_{j*8}\}$
3. Combine the 8 8-bit binary into a 64-bit binary number. $NGI = \{ngi_1 ngi_2 ngi_3 \dots ngi_{N*M/8}\}$, where ngi_j is a 64-bit number made up of 8 8-bit number of gi_j .

CHAPTER 6. OUR WATERMARKING SCHEME

4. Use this 64-bit binary as the input of the DES system. $GW = \{gw_1 gw_2 gw_3 \dots gw_{N*M/8}\}$, where $gw_j = \text{DES}_{KEY}(ngi_j)$
5. Divide the 64-bit output into 8 8-bit binary number. $FW = \{fw_1 fw_2 fw_3 \dots fw_{N*M}\}$, where $wf_{8(j-1)+k}$ is the k^{th} 8 bit of gw_j , $1 \leq j \leq N*M/8$ and $1 \leq k \leq 8$.
6. Find out the large number in FW . Let the mfw be the largest number of FW . $mfw = \max\{fw_1 fw_2 fw_3 \dots fw_{N*M}\}$.
7. Let $W = \{w_1 w_2 w_3 \dots w_{N*M}\}$, where $w_j = fw_j/mfw$. W is the watermark that we are going to embedded into the original image.

By applying the DES encryption method, we have achieved the prerequisite of the non-invertibility of the watermark, we will prove this in section 6.4. After the construction of the watermark, now we need to design a way to embed the watermark into the original image to make the watermark robust, imperceptible and asymmetric.

6.2 Watermark Embedding

The watermark is embedded in the spatial domain. In our watermarking scheme, we use key G to embed the watermark. The key G will be kept secret from others. Only the person who embeds the watermark will know the key. We embed the watermark into the original image on a block-basis. For the first block of the original image, we select first 64 elements from the watermark W to form an 8 by 8 matrix W_1 , and then embed these elements into the first block of the image. Then, the second 64 elements W_2 are chosen for the second block and so on.

We embed our watermark W into the image IMG by the function

$$IMG_j^w = IMG_j + \beta * G_j * W_j \quad (6.1)$$

CHAPTER 6. OUR WATERMARKING SCHEME

Where IMG_j is the j^{th} block of the original image IMG and IMG_j^w is the watermarked IMG_j . G_j is the watermark embedding key and W_j is the j^{th} set of 64 elements of the watermark. β is the scaling factor, which can control the watermarking strength. By applying the Gram-Schmidt orthogonalization principle [26], we can choose G_j such that $G_j^T * IMG_j = 0$, so the method does not need a reference image to extract the watermark.

The watermark strength should be as large as possible, in order to obtain a high robustness. However, it should not affect the perceptual quality.

6.3 Watermark Detection

In our watermarking scheme, we use key $E = (G_j^T + \alpha * H_j^T)/\beta$ to extract the watermark from the watermarked image. The extraction key E is different from embedding key G , which makes the watermarking scheme asymmetric.

$$\text{The watermark extraction key } E_j = (G_j^T + \alpha * H_j^T)/\beta \quad (6.2)$$

Where α is a scaling factor to control the accuracy of the watermark extraction, H is a matrix and $H_j^T * G_j = 0$. To make the watermarking scheme blind, we choose $H_j^T * G_j = 0$. This can be achieved by applying the Gram-Schmidt orthogonalization principle.

The detection is a hard decision function δ with a threshold ε . The detection function applies the extraction key E to the watermarked image IMG^w and then uses the *sim* function to measure the similarity between real watermark W and watermark extracted W^E . The watermark is extracted block by block. I.e., $W^E = \{W_1^E \ W_2^E \ W_3^E \ \dots \ W_{N*M/64}^E\}$

Where

$$\begin{aligned} W_j^E &= E_j * IMG_j^w = ((G_j^T + \alpha * H_j^T)/\beta) * (IMG_j + \beta * G_j * W_j) \\ &= G_j^T * IMG_j / \beta + G_j^T * \beta * G_j * W_j / \beta + \alpha * H_j^T * IMG_j / \beta + \alpha * H_j^T * \beta * G_j * W_j / \beta \end{aligned}$$

CHAPTER 6. OUR WATERMARKING SCHEME

$$= W_j + \alpha * H_j^T * IMG_j / \beta \quad (6.3)$$

$$\text{The detector function is } \delta(I^w) = \begin{cases} 1, & \text{if } |sim(W, E * I^w)| \geq \varepsilon \\ 0, & \text{otherwise} \end{cases} \quad (6.4)$$

$$\text{where } sim(W, W_E) = \frac{W^T W_E}{\|W\| \|W_E\|} \quad (6.5)$$

By selecting proper α and threshold ε , we can justify whether the watermark exists in the image.

6.4 Discussion

Now, we can prove the non-invertibility of our watermarking scheme by contradiction. First, we assume that the watermarking scheme is invertible. Then, according the definition in [7], we can find IMG' and W' that

$$IMG^w = IMG' + \beta' * G' * W'. \quad (6.6)$$

$$\text{And } DES_{KEY'}(IMG') = W'. \quad (6.7)$$

Combine formulas (6.6) and (6.7),

$$\text{we can get } DES_{KEY'}(IMG') = (IMG^w - IMG') / (G' * \beta'). \quad (6.8)$$

At the right hand side, IMG^w is publicly known, G' is related to IMG' and β' is a constant. So, the right hand side can be regularly derived. That means, without knowing the KEY' , we can predict the result of DES. This contradicts with the fact that so far there is no such an attack on DES known. Therefore, as long as DES is safe, the above scheme is non-invertible.

6.5 Testing Results

We have tested several images with our designed watermarking scheme. Here we use image “Lena” which is shown in figure 6.1(a) to demonstrate the testing result. To test the

CHAPTER 6. OUR WATERMARKING SCHEME

imperceptibility and robustness property, applying our watermarking scheme with scaling factor $\beta = 4$, we can get the watermarked image which is shown in figure 6.1(b). We can see that the watermark is imperceptible.

Figure 6.1: (a) Original image (b) Watermarked image ($\beta=4$)

The quantitative measure of degradation was based on objective analysis using Peak Signal-to-Noise Ratio (PSNR),

$$PSNR_{dB} = 20 \log_{10} \left\{ 255 / \sqrt{\sum_{i=1}^N \sum_{j=1}^M [IMG(i,j) - IMG^w(i,j)]^2 / (N \times M)} \right\} \quad (6.9)$$

Where $IMG(i,j)$ is the original image and $IMG^w(i,j)$ is the watermarked image in spatial domain and N, M are image dimension.

Figure 6.2: PSNR under different scaling factor β

Several images were tested using our watermarking scheme under different scaling factors β , which attempted to determine the quantitative measure of degradation. Figure 6.2 shows the PSNR in DB against the scaling factor.

CHAPTER 6. OUR WATERMARKING SCHEME

Our watermarking scheme is also robust under many attacks. Since our watermarking scheme is based on [64], their robustness analysis is also suitable for our watermarking scheme.

Our watermarking scheme can be extended to video and audio. By changing the N and M , we can apply them to video and audio.

Chapter 7

Conclusion and Future Work

The digital multimedia is more and more popular nowadays. The multimedia data can be classified into many categories: image, video, audio and etc. With the development of the Internet, there are more and more multimedia products produced and transacted on the Internet. As a result, the security of the digital multimedia becomes an essential problem. Among all the digital rights management problems, creatorship protection and copyright protection are big issues. In this thesis, we are focusing on the creatorship protection.

We review the watermarking techniques development and some digital signature schemes in chapter 2. From the literature review, we can see that there are lots of watermarking schemes developed during past decades for different multimedia formats. Most of these watermarking schemes are for digital images. The watermarking schemes are proposed for different purposes such as copyright/ownership declaration, creatorship/authorship declaration, copyright violation detection, copyright violation deterrence, copy control, media authentication, and media data integrity functions. Different purposes have the different requirements on the watermarking scheme. For instance, the watermarking scheme for copyright protection must be robust. The watermarking schemes that are aimed for media authentication may be fragile. But we observed that there are very few watermarking frameworks designed for the creatorship protection under joint creation scenerio. The fact is that with the increasing of complexity of digital multimedia, it is difficult to produce the digital multimedia product by single

CHAPTER 7. CONCLUSION

person. Our research work mainly focuses on the protection of the joint creatorship of image, video and movie in a collaborative environment.

7.1 Our Achievements

In this thesis, we have presented three digital watermarking frameworks to protect the joint-creatorship of the multimedia and a watermarking scheme required by these frameworks:

- a.) Framework of joint-creatorship protection for digital images
- b.) Framework of joint-creatorship protection for digital videos
- c.) Framework of joint-creatorship protection for digital movies
- d.) Watermarking framework required by the three frameworks above

We have developed a watermarking framework of creatorship protection for jointly created digital images, which is presented in chapter 3. The framework embedded multiple watermarks into the images in a non-overlapping manner to ensure the perceptibility. And from the watermark, people can know each creator's contribution. The framework is employed during the image creation process. With the framework, first, a creator is not able to remove another creator's watermark. Second, a creator or a group of creators are not able to connive to remove the creatorship of another creator. Third, a creator cannot disown his/her own part of the joint creation. Forth, a creator cannot pause as the sole creator and sell the product to a buyer. The framework employs the cryptographic protocol and watermarking scheme. The cryptographic protocol can be any secure digital signature scheme developed so far. The watermarking scheme must be robust, imperceptible, asymmetric and non-invertible. We have developed a new watermarking scheme, which satisfies all these requirements. A digital signature scheme is required in order to avoid the disowning of the creatorship. The complexity of the

CHAPTER 7. CONCLUSION

transmission and storage requirement is low in our framework.

In chapter 4, we present our framework of creatorship protection for jointly created object-based digital video. The framework embeds different watermarks in different video objects in such a way that each creator can show the joint-creatorship of the whole video; as well as each creator can prove his/her creatorship of video object he/she created. The watermarking framework also employs the cryptographic protocol and watermarking scheme. The cryptographic protocol and watermarking scheme have the same requirements as in the framework for digital images. We have designed a suitable watermarking scheme for this watermarking framework. The complexities of the frameworks are analyzed by calculating the amount of data transmission and storage requirements and it is shown to be low.

We introduce our framework of joint-creatorship protection for digital movies in chapter 5. 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. The complexity of the framework is analyzed by calculating the amount of data transmission and storage requirements. Experiments were conducted to study the effectiveness of the framework.

The watermarking scheme we have designed for the frameworks is presented in chapter 6. The watermarking scheme is robust, imperceptible, asymmetric and non-invertible. These properties are required by our watermarking frameworks.

List of our contributions:

We have designed

- Framework of joint-creatorship protection for digital images
- Framework of joint-creatorship protection for digital videos

CHAPTER 7. CONCLUSION

- Framework of joint-creatorship protection for digital movies
- Watermarking framework required by the three frameworks above

We have published following papers.

Journal paper:

- Yu-Quan Zhang, Sabu Emmanuel, "A Novel Creatorship Protection Framework for Digital Images", in Journal of Ubiquitous Computing and Intelligence, issue 3, 2006

Conference paper:

- Yu-Quan Zhang, Sabu Emmanuel, "A Novel Framework for Object-Based Video Multiple Creatorship Protection", in the Proceedings of the 4th Int'l Symposium on Image and Signal Processing and Analysis, Zagreb, Croatia, 2005, pp. 227-232
- Yu-Quan Zhang, Sabu Emmanuel, "A Novel Watermarking Framework for Joint-Creatorship Protection", in the Proceedings of International conference on CYBERWORLDS, Singapore, Nov 2005, pp. 109-116
- Yu-Quan Zhang, Sabu Emmanuel, "A Novel Framework for Multiple Creatorship Protection of Digital Movies", to appear in proceedings of first international conference on DRMTICS, Sydney, Australia, Oct 2005

7.2 Future Work

We have solved the creatorship protection problem in a collaborative environment. There are three more roles in digital rights management, which are owner, distributor and customer. How to solve the joint ownership protection can be the focus of our future work.

References

- [1] F. Hartung and M. Kutter, "Multimedia Watermarking Techniques", in *Proceedings of the IEEE, Special Issue on Identification and Protection of Multimedia Information* 87, June 1999
- [2] J. J. Eggers, J. K. Su, and B. Girod, "Asymmetric Watermarking Schemes", in *Tagungsband Des GI Workshops Sicherheit in Mediendaten*, Berlin, Germany, Sept. 2000, pp. 107-123
- [3] I. J. Cox, J. Killian, F. T. Leighton, and T. Shamoan, "Secure Spread Spectrum Watermarking for Multimedia", *IEEE Transactions on Image Processing*, vol. 6, no. 12, Dec. 1997, pp. 1673-1687
- [4] B. Pfitzmann and M. Schunfer, "Asymmetric fingerprinting", in *Advances in CryptologyEUROCRYPT 1996*, LNCS 1070, SpringerVerlag, 1996, pp. 84-95
- [5] T. Y. Kim, H. Choi, K. Lee and T. Kim, "An Asymmetric Watermarking System With Many Embedding Watermarks Corresponding to One Detection Watermark", *IEEE Signal Processing Letters*, Vol. 11, No. 3, March 2004
- [6] S. Craver, N. Memon, B. Yeo, and M. Yeung, "Can Invisible Watermarks Resolve Rightful Ownerships?" *Technical Report RC 20509, IBM Research Division*, July 1996
- [7] L. Qiao and K. Nahrstedt "Watermarking Schemes and Protocols For Protecting Rightful Ownership And Customer's Rights", *ICLASS and National Science Foundation Career Grant CCR-96-23867*
- [8] A. M. Alattar, E. T. Lin and M. U. Celik, "Digital Watermarking of low Bit-Rate Advanced Simple Profile MPEG-4 Compressed Video", *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 13, no. 8, August 2003
- [9] R. Lancini, F. Mapelli and S. Tbaro "A Robust Video Watermarking Technique in the Spatial Domain", *IEEE Region 8 International Symposium on Video/Image Processing and Multimedia Communications*, pp. 16-19, June 2002
- [10] A. Piva, R. Caldelli and A. D. Rosa, "A DWT-Based Object Watermarking System for MPEG-4 Video Streams", *IEEE Int. Conference on Image Processing*, 2000, vol. 3, pp. 5-8
- [11] H. Guo and N. D. Georganas, "Digital image watermarking for joint ownership", in *ACM Multimedia 2002*, 362-371, Dec 2002
- [12] F. Hartung, J. K. Su, and B. Girod, "Spread spectrum watermarking: Malicious attacks and counterattacks", in *Proc. SPIE Security and Watermarking of Multimedia Contents 99*, San Jose, CA, Jan, 1999.
- [13] M. Holliman and N. Memon, "Counterfeiting attacks on linear watermarking schemes", in *Proc IEEE Multimedia Systems 98, Workshop Security Issues in Multimedia Systems*, Austin, TX, June 1998.
- [14] S. Crave, N. Memon, B. L. Yeo, and M. Yeung, "Can invisible watermarks resolve rightful ownerships?", *IBM, IBM Res. Rep, RC 20509*, July 1996.

- [15] S.A. Craver, N. Memon, B.-L. Yeo, and M. Yeung, "On the invertibility of invisible watermarking techniques", in *Proc. IEEE Int. Conf. Image Processing 1997(ICIP '97)*, vol. 1, Santa Barbara, CA, Oct. 1997, pp.540-543.
- [16] S. Craver, N. Memon, B. Yeo, and M. Yeung, "Resolving rightful ownerships with invisible watermarking techniques: Limitations, attacks, and implications", *IEEE J. Select. Areas Commun. (Special Issue on Copyright and Privacy Protection)*, vol. 16, pp. 573-586, May 1998.
- [17] G. C. Langelaar, R. L. Lagendijk, and J. Biemond, "Removing spatial spread spectrum watermarks by nonlinear filtering", in *Proc. Europ. Signal Processing Conf. (EUSIPCO '98)*, Rhodes, Greece, Sept. 1998.
- [18] H. S. Stone, "Analysis of attacks on image watermarks with randomized coefficients", *NEC Res. Inst., Princeton, NJ, Tech. Rep.*, May 1996.
- [19] M. Kutter and F. Petitcolas, "A fair benchmark for image watermarking systems", in *Proc. SPIE IS&T/SPIE's 11th Annu. Symp., Electronic Imaging 99:Security and Watermarking of Multimedia Contents*, vol. 3657, Jan. 1999.
- [20] W. C. Chu, "DCT-Based Image Watermarking Using Subsampling", *IEEE Transactions on Multimedia*, vol. 6, No. 1, March 2003.
- [21] A. Lemma, J. Aprea, W. Oomen and L. van de Kerkhof, "A Temporal Domain Audio Watermarking Technique", *IEEE Trans. on SP*, Vol. 51, No. 4, April 2003, pp. 1088--1097.
- [22] I.-K. Yeo, and H. J. Kim, "Modified Patchwork Algorithm: A Novel Audio Watermarking Scheme", *IEEE Transactions on Speech and Audio Processing*, vol. 11, no. 1, 2003
- [23] Frank Hartung, Bernd Girod, "Fast public-key watermarking of compressed video", *IEEE International Conference on Image Processing*, October 26-29, 1997.
- [24] Chiou-Ting Hsu, Ja-Ling Wu, "DCT-based watermarking for video", *IEEE Transactions on Consumer Electronics*, Vol. 44, No. 1, Feb 1998, pp. 206-216
- [25] R. G. van Schyndel, A. Z. Tirkel, and C. F. Osborne, "A digital watermark", in *Proc. Int. Conf. Image Processing (ICIP)*, vol. 2, 1994, pp. 86-89.
- [26] I. Cox, J. Killian, T. Leighton and T. Shamoan, "Secure spread spectrum watermarking for images, audio, and video", *NEC Res. Inst., Princeton, NJ, Tech. Rep.* 95-10, 1995.
- [27] D. Simitopoulos, S. A. Tsaftaris, N. V. Boulgouris and M. G. Strintzis, "Fast MPEG watermarking for copyright protection", in *IEEE International Conference on Electronics, Circuits and Systems (ICECS 2002)*, Dubrovnik, Croatia, Volume 3, pp. 1027-1030, September 2002.
- [28] D. Kundur and D. Hatzinakos, "Digital watermarking using multiresolution wavelet decomposition", in *Proc. IEEE Int. Conf. Acoustics, Speech, and Signal Processing 1998 (ICASSP 98)*, vol. 5, Seattle, WA, May 1998, pp. 2969-2972.
- [29] D. Benham, N. Memon, B.-L. Yeo, and M. Yeung, "Fast watermarking of DCT-based compressed images", in *Proc. Int. Conf. Image Science, Systems, and Technology (CISST '97)*, Las Vegas, NV, June 1997, pp. 243-253.
- [30] M. S. Kankanhalli, Rajmohan, and K. R. Ramakrishnan, "Content-based watermarking of images", in *Proc. ACM Multimedia '98*, Bristol, U.K., Sept. 1998.
- [31] R. B. Wolfgang, C. I. Podilchuk, and E. J. Delp, "Perceptual watermarks for digital images and video", *Proc IEEE*, vol. 87 no. 7, Jul. 1999
- [32] E. Koch and J. Zhao, "Toward robust and hidden image copyright labeling", in *Proc. Workshop Nonlinear Signal and Image Processing*, Marmaros, Greece, June 1995.

- [33] N. Nikolaidis and I. Pitas, "Copyright protection of images using robust digital signatures", in *Proc. ICASSP '96*, Atlanta, GA, May 1996.
- [34] M. Barni, F. Bartolini, V. Cappellini, and A. Piva, "A DCTdomain system for robust image watermarking", *Signal Processing (Special Issue on Watermarking)*, vol. 66, no. 3, pp. 357-372, May 1998.
- [35] M. Kutter, F. Jordan, and F. Bossen, "Digital signature of color images using amplitude modulation", in *Proc. Electronic Imaging 1997 (EI 97)*, San Jose, CA, Feb. 1997.
- [36] J. J. K. 'O Ruanaidh, W. J. Dowling, and F. M. Boland, "Phase watermarking of digital images", in *Proc. Int. Conf. Image Processing (ICIP)*, vol. 3, Sept. 1996, pp. 239-242.
- [37] M. Barni, F. Bartolini, V. Cappellini, A. Piva, and F. Rigacci, "A M.A.P. identification criterion for DCT-based watermarking", in *Proc. Europ. Signal Processing Conf. (EUSIPCO '98)*, Rhodes, Greece, Sept. 1998.
- [38] D. Kundur and D. Hatzinakos, "A robust digital image watermarking method using wavelet-based fusion", in *Proc. IEEE Int. Conf. Image Processing 1997 (ICIP 97)*, vol. 1, Santa Barbara, CA, Oct. 1997, pp. 544-547.
- [39] B. Chen and G. W. Wornell, "Digital watermarking and information embedding using dither modulation", in *Proc. IEEE Workshop Multimedia Signal Processing*, Los Angeles, CA, Dec. 1998.
- [40] B. Chen and GW Wornell, "Dither modulation: A new approach to digital watermarking and information embedding", in *IS&T/SPIE's 11th Annu. Symp., Electronic Imaging 99: Security and Watermarking of Multimedia Contents*, vol. 3657, San Jose, CA, Jan. 1999.
- [41] G. Depovere, T. Kalker, and J.-P. Linnartz, "Improved watermark detection reliability using filtering before correlation", in *Proc. IEEE Int. Conf. Image Processing 1998 (ICIP 98)*, Chicago, IL, Oct. 1998.
- [42] F. Hartung and B. Girod, "Digital watermarking of raw and compressed video", in *Proc. SPIE Digital Compression Technologies and Systems for Video Commun.*, vol. 2952, Oct. 1996, pp. 205-213.
- [43] F. Hartung and B. Girod, "Fast public-key watermarking of compressed video", in *Proc. IEEE Int. Conf. on Image Processing 1997 (ICIP '97)*, vol. 1, Santa Barbara, CA, Oct. 1997, pp. 528-531.
- [44] F. Hartung and B. Girod, "Digital watermarking of uncompressed and compressed video", *Signal Processing (Special Issue on Copyright Protection and Access Control for Multimedia Services)*, vol. 66, no. 3, pp. 283-301, 1998.
- [45] F. Jordan, M. Kutter, and T. Ebrahimi, "Proposal of a watermarking technique for hiding/retrieving data in compressed and decompressed video", *ISO/IEC Doc. JTC1/SC29/WG11 MPEG97/M2281*, July 1997.
- [46] C.-T. Hsu and J.-L. Wu, "Digital watermarking for video", in *Proc. of DSP'97*, Santorini, Greece, July 1997, vol. 1 pp. 217-220.
- [47] C.-T. Hsu, "Digital watermarking for images and videos", *Ph.D. dissertation, Commun. Multimedia Lab.*, National Taiwan Univ., 1997.
- [48] C.-T. Hsu and J.-L. Wu, "Hidden signatures in images", in *Proc. IEEE Int. Conf. Image Processing (ICIP 96)*, Lausanne, Switzerland, Sept. 1996, pp. 223-226.
- [49] M. Swanson, B. Zhu, and A. Tewfik, "Multiresolution video watermarking using perceptual models and scene segmentation", in *Proc. IEEE Int. Conf. Image Processing 1997 (ICIP '97)*, vol. 2, Santa Barbara, CA, Oct. 1997, pp. 558-561.

- [50] M. Swanson, B. Zhu, and A. H. Tewfik, "Multiresolution scenebased video watermarking using perceptual models", *IEEE J. Select. Areas Commun. (Special Issue on Copyright and Privacy Protection)*, vol. 16, pp. 540-550, May 1998.
- [51] R. Lancini, F. Mapelli and S. Tubaro, "A Robust Video Watermarking Technique in the Spatial Domain", in *IEEE Region 8 International Symposium on Video/Image Processing and Multimedia Communications, 16-19 June 2002, Zadar, Croatia*
- [52] S. Emmanuel and M. S. Kankanhalli, "Digital Rights Management Issues for Video", in *Multimedia Security Handbook*, Chapter 26, pp. 759-787, Editors: B. Furht and D. Kirovski, Publisher: CRC Press, 2005
- [53] R.L. Rivest, A. Shamir, and L.M. Adleman, "A Method for Obtaining Digital signatures and public-key cryptosystems", *Communications of the ACM* (2) 21 (1978), 120-126
- [54] H. Elkamchouchi, K. Elshenawy and Heba. A. Shaban, "New digital signature schemes in the real and gaussian integers' domains", in *21st National Radio Science Conference (NRSC2004)* (NTI) March, 2004
- [55] C-C Chang and Y-F Chang, "Signing a Digital Signature Without Using One-Way Hash Functions and Message Redundancy Schemes", *IEEE Communications Letters*, Vol. 8, No.8, August 2004
- [56] A. Adelsbach and A. R. Sadeghi, "Advanced techniques for dispute resolving and authorship proofs on digital works", in *Proc. Of SPIE: Security and Watermarking of Multimedia Contents V*, vol. 5020, 2003
- [57] S. Craver, N. Memon, B. Yeo and M. Yeung, "Resolving rightful ownership with invisible watermarking techniques: limitation, attacks, and implications", *IEEE Journal on Selected Areas in Communications*, vol. 16 no. 4, pp. 573-586, 1998
- [58] L. Qiao and K. Nahrstedt, "Watermarking methods for mpeg encoded video: Towards resolving rightful ownership", in *Proc. of ICMCS*, 1998
- [59] A. Adelsbach, S. Katzenbeisser, and H. Veith, "Watermarking schemes provably secure against copy and ambiguity attacks", in *Proc. of ACM CCS-10 Workshop on Digital Rights Management*, 2003
- [60] M. Ramkumar and A. N. Akansu, "A robust protocol for proving ownership of multimedia content", *IEEE Transactions on Multimedia*, vol. 6, no. 3, pp. 469-478, 2004
- [61] M. Ramkumar and A. N. Akansu, "Image watermarks and counterfeit attacks: Some problems and solutions", in *Proc. of Content Security and Data Hiding in Digital Media*, 1999
- [62] S. Katzenbeisser and H. Veith, "Securing symmetric watermarking schemes against protocol attacks", in *Proc. of SPIE: Security and Watermarking of Multimedia Contents*, vol. 4675, pp. 260-268, 2002
- [63] H. T. Sencar and N. Memon, "Watermarking and ownership problem: a revisit", in *Proceedings of the 5th ACM Workshop on Digital Rights Management* (Alexandria, VA, USA, November 07 - 07, 2005). DRM '05. ACM Press, New York, NY, 93-101.
- [64] J. Tzeng, W.-L. Hwang and I.-L. Chern, "An Asymmetric Subspace Watermarking Method for Copyright Protection", *IEEE transactions on signal processing*, VOL. 53, No. 2 February 2005
- [65] Yu-Quan Zhang, Sabu Emmanuel, "A Novel Framework for Object-Based Video Multiple Creatorship Protection", in the Proceedings of the 4th Int'l Symposium on Image and Signal Processing and Analysis, Zagreb, Croatia, 2005, pp. 227-232

- [66] Yu-Quan Zhang, Sabu Emmanuel, "A Novel Watermarking Framework for Joint-Creatorship Protection", in the Proceedings of International conference on CYBERWORLDS, Singapore, Nov 2005, pp. 109-116
- [67] Yu-Quan Zhang, Sabu Emmanuel, "A Novel Framework for Multiple Creatorship Protection of Digital Movies", to appear in proceedings of first international conference on DRMTICS, Sydney, Australia, Oct 2005
- [68] William Stallings, "Cryptography and Network Security: Principles and Practices", Prentice Hall, 2003
- [69] Qiming Li, Ee-Chien Chang, "On the Possibility of Non-Invertible Watermarking Schemes", 6th International Workshop on Information Hiding, Toronto, Canada, 2004
- [70] Ghouti L., Bouridane A., Ibrahim, M.K., Boussakta S. "Digital image watermarking using balanced multiwavelets" IEEE Transactions on Acoustics, Speech and Signal Processing, Volume 54, Issue 4, April 2006 Page(s):1519-1536
- [71] Hong Yin, Zengqiang Chen, Zhuzhi Yuan, "Multimedia Digital Watermarking Detection System Based on Watermark", First International Conference on Innovative Computing, Information and Control, Volume 3, 30 Aug. 2006 Page 475 - 478