ADDIS ABABA UNIVERSITY
COLLEGE OF NATURAL SCIENCES
DEPARTMENT OF COMPUTER SCIENCE

PIRATES' ACTIVITY DETECTION TOWARDS PROTECTION OF DIGITAL COPYRIGHTS

By

KURIBACHEW GIZAW

A THESIS SUBMITTED TO THE SCHOOL OF GRADUATE STUDIES
OF
ADDIS ABABA UNIVERSITY
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE DEGREE OF MASTERS OF SCIENCE IN COMPUTER SCIENCE

MARCH, 2014

ADDIS ABABA UNIVERSITY
COLLEGE OF NATURAL SCIENCES
DEPARTMENT OF COMPUTER SCIENCE

PIRATES' ACTIVITY DETECTION TOWARDS PROTECTION OF DIGITAL COPYRIGHTS

By

KURIBACHEW GIZAW

Approved by:
Examining Board:

1. DejeneEjigu (Ph. D.), Advisor _____
2. Mulugeta Libsie(Ph. D), Examiner_____
3. Dida Midekso(Ph. D), Examiner_____
4. Yaregal Assabie(Ph. D), Examiner_____

Table of contents

Chapter Three

Chapter Four

Chapter Five

Chapter Six

List of Tables

Tables Page

List of Figures

Figures Page

Acknowledgement

I would also like to acknowledge my husband Ayalew Belay for incessant support. All your supports and encouragement starting my MSc lesson and throughout my thesis work is remarkable. God bless you!

Abstract

The economic importance of copyright law for the copyright owner is unquestionable. The copyright owners have been abused their right of using their intellectual property as they deserve. Looking their right is violated copyright owners didn't sit idle; actions have been taken by the owners unity starting from the establishment of the copyright law article and enforcing the law to be realized. Nevertheless, there is a big gap between the copyright law and realizing it, because of reasons like: the technology and the digital nature of the works, the understanding of copyright law by the public, the difficulty of finding forensic to accuse someone violating the rule, and so on. The struggle to keep the copyright protected has been tried indifferent ways: by creating awareness sessions with the public, by putting technical mechanisms to stop illegal copies, by producing forensic evidence to ask violators, and other solutions which are considered as beneficiary by the copy owners. But still there is a need of copy protection schemes to limit the access of the copyrighted works to legitimate customers and reduce piracies.

This research deals with pirates' activity detection and protection of digital copyright law. By predicting out all the possible ways through which pirate got a chance to copy and redistribute the works. The basic pirates' acts are copying, burning and sharing; in this research all the possibilities of the above acts are well identified,a mechanism to detect and prevent the pirates' acts is proposed and the proposed technique is conceptualized by developing a prototype. Regarding copying; pirates' acts to copy an entire CD/DVD with copyrighted content are listed out. Copying is detected by comparing the system clipboard content with digital content. The burning acts are traced in two ways: firstby looking the most widely used burners/authoring applications from the process table of the operating system and second for pirates expected burners a way to prevent burning is proposed by disabling the burning functionality at CD/DVD entrance and enabling it at CD eject.Finallyan algorithm to detect and prevent sharing is proposed by comparing the first and later IP addressof the digital content.

Keywords: *Piracy, Copyright law, Digital content, system clipboard.*

Chapter One

1. Introduction

1.1 Background

Digital Piracy has become a big concern for music, film, software and game industries. These industries are putting their much effort that consumes a lot of time and money on their product. Their hard work and investment will be rewarded by the money received from legitimate customer but what they get back in return is unsatisfactory because of piracy since the products they create are digital in nature, they can be easily copied and redistributed with minimal effort. The BSA (Business Software Alliance) claims that it results in a loss of revenue of tens billions of dollars per year and that it also destroys jobs, impairs computer security and hinders innovation [1]. Many developers have placed security mechanisms in their software, on the game discs or the original album of music. These security features are often effective but can have unintended consequences which end up hurting legitimate customers [2]. Moreover the pirates can easily examine exactly how the security mechanisms work and find ways to trick the system into validating an illegitimate copy [3]. The digital piracy impact on different categories of digital works is discussed below.

Music Piracy

Music piracy is the copying and distributing of copies of a piece of music for which the composer, recording artist, or copyright-holding record company did not give consent. For the copyright holder in music industry which may be the artist or the recording company piracy is a big head ache. If the recording company buys the copyright from the artist by expecting a profit it may finally result with a loss; hence illegal copies will be distributed to the fans of the artist. The same loss will be true with the artist too. As a result of music piracy now days recording companies will not agree to pay for the artist for the recordings only they need live concert or other stage performance in addition to compensate what they loss. This will be an economic loss crisis for the artist should be beneficiary from both the recordings and the live concert.

Video/film piracy

Video piracy is unauthorized and illegal production and sale of copies of commercial video films.As far as this study is concerned the film piracy intended to mention in this section is the VCD distribution of music, documentary films, and other VCDs for children or other not the one which is shown in cinema.

Video piracy is discouraging professional cameraman who are talented to make documentaries, they are may be interested and gifted on birds, animals, aquatic animals, historical heritages and historical events.

Software Piracy

Software piracy is an act of pirating software/computer programs by copying and redistributing off-the-shelf application programs in violation of the copyright law; which costs software vendors many millions of dollars.

Copyright of software can be owned starting from a single individual who developed certain type of application to big international companies and software piracy will result a loss of revenue for both. As the price of software is too much as compared to other digital contents software piracy is more controversial. Many people believe genuine software is unaffordable to pay for, so they prefer to use pirated software. It is very common to use pirated software and no one consider it as a crime. Nevertheless software piracy is violating the economic right of the copyright owner.

Game piracy

Computer/video game piracy is an illegal act of distributing the copyrighted game. Computer professional, individuals or a company can be the copyright owner in game industry. The copyrighted game will be pirated and distributed which results with a lot of economic crisis for the right owners. Game piracy hinders innovation and discourages young creative computer talented individuals who have a potential to come up with entertain games.

1.2 Statement of the problem

Violation of Copyright became a major problem for the music, film, software and game industries as the materials are digital in nature. Companies are losing more of their revenue because of copyright violation and it is said to be a global pricing problem. The algorithms and the security techniques are revealed by the pirates and these days it seems no more protection for Digital copies from being pirated. Even though the computer technology and scholars in the field are coming up with a new way for securing the copyright which is helpful for protecting the materials the pirates are tricking the security and still there is a need to have trusted distribution of the copyright materials. And the need for securing the copy right raises as the music, software and game industry grows up. The question how we can protect digital rights, how can individuals and organization get their revenue as a reward for their labor need to be answered, hence a better approach for Anti-piracy security mechanism is indeed required.

1.3 Research questions

The following lists of questions are the basic which initiates the start of this research work.

1. From a technical standpoint, it would seem theoretically impossible to completely prevent users from making copies of the media they purchase, is there any means to at least make the copying activity difficult?
2. Is it possible to create copy protection software that can protect unauthorized copying?
3. Copy protection schemes are criticized in harming or led to inconvenience legitimate users is it possible to develop copy protection software that do not harm legitimate users?
4. Is it possible to make a copy protection scheme that do not interfere users' privacy?

1.4 Scope of the study

The scope of this research work is explained in terms of three dimensions:

I. From works which are subject to copyright

Copyright law is envisioned to grant different intangible works. Copyright is to give an exclusive right to authorship for the owner of works like Musical works ,Dramatic works, Pantomimes and choreographic works, Pictorial, graphic, and sculptural works, Motion pictures and other audiovisual works, Sound recordings and Architectural works. This thesis work deals on works that reach to audience with distribution of digital copies which includes:

- Music
- Film/ video
- Software/computer program
- Game

Hence the other ways of violating copyright of original works will not be considered in this study for example: translating the original language of a dramatic work and presenting in a stage is a type of copyright infringing, but out of the scope of this study.

II. From operating system used in the thesis

This study is limited to Window operating system; hence Window is the most widely used operating system. All the models and the prototype are done in Window operating system.

III. From the degree to what extent the protection of digital copyright is done

Regarding this issue all pirates' activities which can be done using computer, in other words computer piracy on the digital copies are considered. It is out of the scope of this thesis to help protection of all pirates' activity that is done not by using computer like: audio/video recording of the copyrighted digital content is not granted in this study.

1.5 Objective

General Objective

The objective of this thesis work is to develop pirates' activity detections towards protection of digital copyright.

Specific Objective

- ✓ Develop tracer model: a Model to trace all the pirates' activities.
- ✓ Develop a prototype: Anti-piracy software that shows the proposed tracer model.
- ✓ Test the prototype: The developed anti-piracy software will be tested.

1.6 Methodology for detecting pirates' activity

The following show the detail methodology for developing pirates' activity detection towards protection of digital copyright:-

Developing tracer model

A model to trace all pirates' activity will be developed. The model will trace what the possible users' acts will be after inserting the copyrighted digital content in CD/DVD drive of their computer system. The question are the users are going to use the copyrighted digital content as intended by the copyright law or are they going to use it pirate it will be assessed. If users are going to pirate; what will they do and how to capture that act will be modeled in the tracer model.

Developing a prototype

A prototype will be developed which shows the tracer model and the action generated when piracy is found.

Testing the prototype

The prototype will be tested whether it is working as planned or not.

1.7 Significance of the study

The following are the major significance of the study

- This study helps to give a new insight to the field of computer science by letting the idea of detecting pirates' activity towards protection of digital copyright to cross researchers' mind, which will give a full-fledged solution from computer science to the problem domain in the real world.
- The study provides a new security mechanism for Anti-piracy security by detecting user activity through identifying the different user actions that might be used by the pirates.
- Helps to reduce Computer piracy against copyright of digital copies.
- The industries which are more affected by Piracy like Music, film, Software and r game will be rewarded as the new security mechanism will help towards protection their product from being pirated.
- The study will motivate copyright owners by having hope on computer science with a better solution and their economic right will be protected soon.
- For Copyright owners of Ethiopia this is a great prize that will encourage innovation in the field of application software and game, it also will be beneficiary for the Ethiopian musicians in reducing illegal copies of their product.
- The study will be initial stand for other security issues in distributed and networked system in detection of threats and attacks by diverting the focus on the attacker and the actions that might be done by the attacker.

Chapter Two

2. Literature Review

This literature review chapter is intended to give a general overview of the scholarly articles related to copy right protection. In this chapter there are three sections the Copy right low, the digital piracy, and the related work. First one deals with the general overview about copyright; it includes definition, importance, draw back, history of copyright low. The second one includes definition, history, and protection mechanism of digital piracy.

2.1 Copyright

2.1.1 Definition

In this digital age as the concern in copyright touches its peak, so many writers defined Copyright and described it in a different ways. The dictionary definition of copyright is the exclusive right to make copies, license, and otherwise exploit a literary, musical, or artistic work, whether printed, audio, video, etc.: works granted such right by law on or after January 1, 1978, are protected for the lifetime of the author or creator and for a period of 50 years after his or her death[4].

Copyright is one of the classifications under Intellectual property together with trade mark, patent t, and design right. The intellectual property office defines copyright as follows, Copyright gives the creators of a wide range of material, such as literature, art, music, sound recordings, films and broadcasts, economic rights enabling them to control use of their material in a number of ways, such as by making copies, issuing copies to the public, performing in public, broadcasting and use on-line. It also gives moral rights to be identified as the creator of certain kinds of material, and to object to distortion or mutilation of it [5].

Copyright can be defined as a person's exclusive right to authorize certain acts (such as reproduction, publication, public performance, adaptation etc.) in relation to his or her original work of authorship. The creator of the work typically owns the copyright, at least initially. However, copyright is often sold or assigned, in whole or in part, to a commercial

publisher, a filmmaker, a recording studio or to someone else who will exploit the work commercially [6].

In short copyright can be defined as: Copyright is restricting the right to copy and distribute content exclusively to the intellectual owner.

2.1.2 The importance of copyright

According to WIPO (World Intellectual property Organization) the importance of copyright can be listed as follows:-

- ✓ **Exclusivity** – authors or rights holders have the right to decide whether to authorize or prohibit certain use of a copyright work by a third party,
- ✓ **No formalities for establishment** – ownership of copyright exists from the time of creation and does not require any formal registration,
- ✓ **Contractual freedom** – authors or rights holders can define the terms and conditions, under which they will grant exploitation rights to their work,
- ✓ **Remuneration** – the rationale behind copyright law is to stimulate artistic creation by providing equitable remuneration and acknowledging creators' efforts to produce literary, dramatic, musical and artistic works, including films,
- ✓ **Territoriality** – the author or rights holder decides on the geographic scope of a license,
- ✓ **Enforcement** – the author or rights holder can enforce her rights against any un-authorized use of the work. [7].

So by having copyright, copyright owners have the exclusive right to do (and authorize others to do) certain things with respect to their copyrighted work, including: make copies of the work, distribute copies of the work, display or perform the work publicly, make derivative works, and transmit the work electronically [8].

2.1.3 The Draw backs of copyright

There are no actual disadvantages to copyright registration. Registration conveys additional rights and benefits, making it easier for the owner of an original work to protect it against infringers. Registration does not take any rights away from the creator of the work. Perceived disadvantages can only be viewed from a functional or theoretical perspective. Functionally, the need to complete a registration takes time and costs money. Theoretically, some activists think copyrights stifle the creative landscape, preventing people from taking works and using them to make new works that will further contribute to society [9].

According to an attorney who specialized in copyright law, copyright that spans for a longer period doesn't benefits society at large. Although it is important to incentivize artists or intellectual owners, the goals of the copyright system are constantly undermined by continually expanding the length of copyright protection. Those in favor of shorter copyright validity periods argue that term as long as seventy years plus the life of the author do not create further incentive because the author does not have any need to collect royalties beyond his own lifetime. Critics further argue that this structure only benefits large businesses that hold copyrights rather than individual artists. Finally, a major disadvantage of a longer copyright validity period is that this structure makes it take longer for works to enter the public domain thereby depriving the public of the ability to enjoy older copyrighted material without restriction [10].

Therefore the importance of having copyright for the society at large really outweighs the drawback.

2.1.4 Types of work subject to copyright

Copyright law protects "original works of authorship," that are fixed in a tangible medium. This protection is available for both published and unpublished works. Copyrightable works include the following categories:

- ✓ **Literary works**: are works, other than audiovisual works, expressed in words, numbers, or other verbal or numerical symbols or indicia, regardless of the nature of the material objects, such as books, periodicals, manuscripts, phonorecords, film, tapes, disks, or cards, in which they are embodied, including software and compilations.
- ✓ **Musical works** including any accompanying words
- ✓ **Dramatic works** including any accompanying music
- ✓ **Pantomimes and choreographic works:** Pantomimes is a play, dance, or other theatrical performance characterized by wordless storytelling. Choreographic is the art of designing sequences of movements in which motion, form, or both are specified.
- ✓ **Pictorial, graphic, and sculptural works** including architectural plans
- ✓ **Motion pictures and other audiovisual works**
- ✓ **Sound recordings**
- ✓ **Architectural works**: is the design of a building as embodied in any tangible medium of expression, including a building, architectural plans, or drawings. The work includes the overall form as well as the arrangement and composition of spaces and elements in the design, but does not include individual standard features [11].

Copyright laws and Fair Use principles also apply to Online and Distance Learning Courses. However, a newer law called the TEACH Act also applies to such courses, but for slightly different uses of copyrighted materials [7].

According to a research conducted by British media regulator Ofcom on Mid-January of 2013 from 380 million piracies tracked:

1. **Music** is the most pirated entertainment content with 280 million piracies
2. **TV show** the second most pirated digital content with 52 million piracies
3. **Films** the third most pirated with 29 million piracies
4. **Computer software and video games** lies in fourth place with 7 million piracies.
5. **E-book** is also tracked as frequently pirated digital content but the number of piracy is not specifically mentioned I the research hence the piracy was very minimal [12].

2.1.5 Usage of Copyrighted works

Copyrighted works can be used legally by:

- ✓ Obtaining the Right to Use Material by Proper Purchase
- ✓ Obtaining Permission of the Owner
- ✓ Face-to-Face Teaching Exemption

Fair Use: The fair use of a copyrighted work is including such use by reproduction in copies or phonorecords or by any other means specified by that section, for purposes such as criticism, comment, news reporting, teaching (including multiple copies for classroom use), scholarship, or research, is not an infringement of copyright. In determining whether the use made of a work in any particular case is a fair use the factors to be considered shall include:

(1) The purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes;

(2) The nature of the copyrighted work;

(3) The amount and substantiality of the portion used in relation to the copyrighted work as a whole; and

(4) The effect of the use upon the potential market for or value of the copyrighted work.

The fact that a work is unpublished shall not itself bar a finding of fair use if such finding is made upon consideration of all the above factors [11].

2.1.6 History of Copyright Low

Copyright came about with the invention of the printing press and with wider public literacy. As a legal concept, its origins in Britain were from a reaction to printers' monopolies at the beginning of the 18th century. Printers, Booksellers, and other Persons, have taken the Liberty of Printing Books, and other Writings, without the Consent of the Authors.

Initially copyright law only applied to the copying of books. Over time other uses such as translations and derivative works were made subject to copyright and copyright now covers a wide range of works, including maps, performances, paintings, photographs, sound recordings, motion pictures and computer programs.

Today national copyright laws have been standardized to some extent through international and regional agreements. Although there are consistencies among nations' copyright laws, each jurisdiction has separate and distinct laws and regulations about copyright.

Copyright are exclusive rights granted to the author or creator of an original work, including the right to copy, distribute and adapt the work. Copyright does not protect ideas, only their expression or fixation. In most jurisdictions copyright arises upon fixation and does not need to be registered. Copyright owners have the exclusive statutory right to exercise control over copying and other exploitation of the works for a specific period of time, after which the work is said to enter the public domain. Uses which are covered under limitations and exceptions to copyright, such as fair use, do not require permission from the copyright owner. All other uses require permission and copyright owners can license or permanently transfer or assign their exclusive rights to others [12].

2.2 Digital piracy

2.2.1 Definition

There are terms that are most frequently used synonymy with digital piracy; some among these words are: infringing copyright low, Internet piracy, computer piracy, illegal recordings, and so on.

Piracy: - Illegal and unauthorized copying or distributing materials protected under copyright, trademark, or patent law[13].

Digital piracy: - The illegal trade in software, videos, digital video devices (DVDs), and music. Piracy occurs when someone other than the copyright holder copies the product and resells it for a fraction of the cost that the legitimate producer charges [13].

Copyright Infringement: -Copyright infringement involves any violation of the exclusive rights of the copyright owner. It may be unintentional or intentional. When unintentional, it is called innocent infringement [14].

Digital piracy is the illegal act of copying digital goods software, digital documents, digital audio (including music and voice) and digital video for any reason other than backup, without explicit permission from and compensation to the copyright holder [16].

2.2.2 Digital Piracy Earlier

In the earlier time when VHS recorder was used as a storage digital piracy was not a problem because the blank VHS cassette was relatively more expensive than the cassette with the content. Piracy became a problem starting the creation of floppy disk; in case of floppy disk the copier need to have the same sequence for reading data as the original. The back and forth struggle between copy protection engineers and nibble copiers to make the read sequence of the track in floppy disk secrete and to reveal that secrete continued until the Apple II became obsolete and was replaced by the IBM PC and its clones. The replacement of the floppy disk with CD and DVD creates a total new era in the history of copy right hence CD/DVD make copying very easy and there is still cat and rat fight between the creators of copy protection scheme and those who make the reverse engineering to make the copyrighted work free from protection[16].

Digital piracy is influenced by economic, technological and ethical considerations. Key technological factors include the growing pervasiveness of the Internet, rapid adoption of broadband technology; write able CD technology, and the emergence of better compression technology highly accelerate the wide spread of digital piracy.

2.2.3 Controversial issue about digital piracy

Digital piracy has been a controversial issues hence its spread over the world. Some people claim that it is unnecessary to have copy right; there reason is sharing should be considered as the right of individual towards free speech and liberty; anyone can't forbid the right of sharing by putting copyright low. And many agree with having copy right to keep the exclusive right of the intellectual property owner to distribute and use the fruit of his/her labor.

Intellectual owners have been heard that they loss most of their revenue because of piracy. To the other side there is an argument that piracy doesn't cost them much. For those who believe Piracy really matters with the revenue of the intellectual owner; they argue that when a consumer makes an illegal copy of an original work, there is typically one less potential sale that the original producer can make. This way if there is reseller who illegally reproduce and sell for the market, this will be robbery or piracy which can make the owner of the copyright empty hand. Others claim that those who got a free copy or a copy with

fewer prices they have it only hence they got it for free or for less price they don't want buy it if they have no chance to get it for free, in this case they argue they can't be claimed as a potential customer.

Some would argue that the methods used to calculate the revenue loss caused by piracy are unreliable. Some claim that piracy has not hurt the copyright owners, only helped, since users are more likely to buy a product after they've tried it.

This all ideas were aroused before and they continue to be controversial, but in this research there is a strong belief as mentioned in the motivation part of chapter one that intellectual owners should get what they deserve and their economic right should be respected.

2.2.4 Protection against digital piracy

In this section all the possible solutions for digital piracy that are tried till this research is done are incorporated. The protection mechanisms lie in three broad categories:

- ✓ Psychological protection
- ✓ Legal protection
- ✓ Technical protection

2.2.4.1 Psychological protection

To protect the copyright low of digital products owners and vendors try psychological protection way by creating awareness with the public. The first attempt was teaching consumers to be moral or ethical and to tell them it is immoral to use a copied product. Telling for users how much the intellectual owner invest his labor, money and time on the product and how much of it will be lost because of the illegal distribution of their product will raise customers' moral and initiate them to buy the original copy.

Warning people on usage of copied product was the other trial. Warning is done in two ways one using copied product will create another undesired result let say if the copied product is software it may have application that report some personal files to third party or it may have bug or virus that can scan the hard disk, in the same way if the product is come with a digital media it will have such tricky software. the other warning is piracy will be reported and you will be asked for committing white collar crime which will sentences you for some defined years in jail. And many vendors announces for piracy reporting which encourages audiences to report piracy for getting some commission.

Reporting Software Piracy

As mentioned above in relation to psychological protection copyright owners use reporting software piracy which helps in minimizing piracy rate by creating awareness with the public that piracy will be reported. The success or failure depends on the common users of the software is 'software piracy reporting' approach. Most of the big software organizations have started a system through which any user can report a piracy against any individual or organization that is using pirated software. After reporting, the software organization verifies complains and then takes legal action against violators. Depending on whom you report the piracy to; you may be able to report anonymously [17].

Summary for the benefit and pitfall of Psychological Copyright protection

The psychological copyright protection mechanism has its own pros and cons.

As a pro there is a chance to decrease the piracy rate, if the people addressed to create awareness have voluntarily changed their attitude after they heard about copyright low and if those people are potential customers. This might work specially for spiritual digital contents as most audience may relate the situation with the religion, but doesn't mean they are fully guaranteed.

As a con it is hard to bring attitude change after awareness creation sessions. Most people stay on their prior belief regarding copyright low. People don't consider their single piracy hurt the copyright owner or the artist, or they don't mind whether the artist is hurt or not. Even if they are fan of the artist, they will prefer to get a copy either from their friends, download it from website, or got it from some file sharing mechanism for a free or they will use the copy with minimal cost.

Hence this way of protecting copyright by making people to be aware on copyright low falls in the hand of the customer; it will be very difficult to assure the protection of the copyright low. It depends on individual attitude whether to use the original or the duplicated copy. Therefore to assure the copyright protection another way of protection is needed.

2.2.4.2 Legal protection

Legally intellectual owners and vendors try to protect their products from being pirated. Different countries use Article in their constitution to protect Copyright low anyone found violating these articles will be bring in front of court and will be sentenced to some years which depends according to the countries.

One of the most famous treaties regarding this issue is the WIPO copyright treaty (WCT) which is special agreement enacted by a consensus of over 100 member states of the European Union (EU). Adopted in Geneva, Switzerland on December 20, 1996, WCT supplements the Berne Convention for the Protection of Literary and Artistic Works (Berne Convention) and the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organizations (Rome Convention). At that time, the Berne and Rome Convention had not been modified for 25 years.

WIPO copyright treaty was created to address changes in digital technology and communications, particularly the distribution of digitally protected works over the Internet. Known as the "Internet treaties," WCT was enacted along with the WIPO Performances and Phonograms Treaty (WPPT) to respond to new marketplace and technology developments. [18]

Legal protection of Copyright in Ethiopia

For Instance in Ethiopia, intellectual property in general and copyright in particular is a very recent development compared to other countries. GetachewMengistie, the former Director General of Ethiopian Intellectual Property Office, confirms that the introduction of policy, legal and institutional framework with regard to intellectual property is a recent phenomenon.

The 1960 Civil Code is the first law that deals with copyright issues in Ethiopia. The Code discusses about protection Literary and Artistic ownership. However, the laws were not sufficient to cover all issues relating to copyright and to effectively protect the right of authors and owners of copyrightable material. As time goes, the need for a specific law dealing with copyright has become crucial.

The Federal Constitution recognizes the protection of intellectual property in general. The Constitution under its cultural objectives provision (Article 91(3)) states that the "Government shall have the duty to the extent its resources permit to support the development of the arts, science and technology." Pertinent to that the Ethiopian Intellectual Property Office (EIPO) was established as an autonomous institution in 2003. Copyright and Neighboring Rights Protection Proclamation No.410/2004 was also enacted in 2004. This new proclamation has introduced new concepts and rights, widened the scope of copyright and related rights, and provided a better mechanism of enforcement and protection of copyright.

According to a prominent person in the entertainment industry, more than 95% of music and 98% of locally made movies on the market are illegal copies. Due to the rampant copyright infringement, publishers are paying less money for movies. The constitution has every provision unambiguously but like most things, lack of enforcement remains the main challenge. Intellectual property, like any other tangible property should be given adequate attention by the law enforcement organs mainly the police and courts [19].

Legal protection of Copyright in USA

United States Copyright Law has its origins in the Constitution, which secures exclusive rights to authors for their writings for a limited time. The copyright law has been updated over the years to reflect new technology.

Another major and relatively recent (1978) development in the copyright law provides copyright protection for any completed work. The copyright notice (+ your name + year of creation) was required on all works and it is still recommended, but not mandatory. You are also strongly encouraged to register your work in the Copyright Office, but that action is also not required, unless you intend to enforce your rights in court. For information about copyright registration, access the Library of Congress and the Copyright Office Web site www.lcweb.loc.gov/copyright or contact an intellectual property attorney.

The law is specific about what constitutes copyright infringement. Except for unusual and egregious situations, the government doesn't normally police and enforce copyright law. It is up to the copyright holder to find copyright violations and bring a lawsuit against the

infringers. Songwriters routinely use certain societies or guilds, such as ASCAP and BMI, to find violations. These organizations send undercover representatives to random nightclubs, restaurants and catering halls to police their members' works. If the establishment does not have a license to play or broadcast the musical work, it may be fined or it may become the defendant in a lawsuit. As a videographer, you may need to get copyright permission even for live or recorded music played at an event you videotape. Ask the musicians or disc jockeys whether they obtained a license to play such music at the event.

If someone found guilty of copyright infringement, under the criminal portion of the law, or liable, under the civil portion, you may face a penalty of five years imprisonment and up to $250,000 in damages. Willful infringement is clearly more serious than unintentional infringement. Once again, as video producers, even if the law weren't so serious, we have an ethical duty to respect people who create original works. Stealing another artist's work is tantamount to stealing their car, their instruments and, literally, their livelihood [20].

Summary for the benefit and pitfall of Legal Copyright protection

The pros: - having the article that state the copyright law in a country constitution will bring confidence for the intellectual owner as their right of reproducing and distributing is exclusively guaranteed for them legally. It may minimize piracy rate hence violating copyright law will accuse a person for committing the so called white collar crime or cybercrime.

The Cons: As mentioned above in Ethiopia and USA case, Ethiopia a country where copyright law is just in the beginning stage and USA where the copyright law was conceived and brought up more than any country ;having the copyright law is a plus but the law alone doesn’t stop digital piracy. The real situation of the world today indicates piracy is increasing dramatically than the year when the law was adopted. Hence the technological changes are helping the piracy world more.

In legal protection the big doubt is having an evidence to bring in front of a court to judge somebody is a pirate which it too controversial. Obviously it needs paramount time to get evidence, to bring the suspect to the court; to hold jury sessions; after all the decision that is given from the court may end up by hurting innocent people.

2.2.4.3 Technical protection

Technically starting from the creation of floppy disk the diskette owners try to protect from being copied which at that time was nibble copier by creating a new sequence of writing order of the floppy track and by keeping the secrecy of the sequence from the attackers. As CD/DVD take place of storage from floppy companies try another technical protection scheme by creating CDs read only CD-R. As software became more dominant than the hardware the chase between the protectors and pirates became more of creating application software. Owners try some activation methods which ask the customer to answer some questions from the manual, secondly using serial numbers or CD key was used as a means of protection, on-line verification and activation was tried even by the most popular software companies like Microsoft.

In this section the most widely used digital piracy protection mechanisms are discussed in the flow of their usage time from past to present.

Using Serial Numbers or CD-keys**:** Some anti-piracy security utilizes unique CD-keys or serials that are distributed with legitimate copies of the product [21]. Obviously it was very simple to share the same CD-key or serial with multiple people, since one serial usually works for multiple copies of a product.

On-line Verification**:**Some of security mechanism needs having the CD to communicate with an online server to validate CD-key information. This ensures that a unique and legitimate CD-key is used, rather than allowing the same key to work with multiple copies of the CD. Although this is effective method to fight back piracy this can also frustrate the genuine users of the software. These systems can be pirated by modifying the program and removing that code that makes it check with the server [22].

Blocking Misused ID or Registration Code**:**There are many software/ programs that require only user name and password or the registration code for full version installation. Sometimes a working password or registration code gets circulated among a number of people and these unauthorized people use them without purchasing a new license. In this case software organization can block or black list the particular registration code or password that is compromised [23].

Product Activation**:**It is a system through which a single software license is tied to a single computer. Many organizations including Microsoft are adapting a product activation system to enforce license agreement. Product activation system is most convenient and easy from both the user's and vendor's view. It allows the user to easily transfer his/her software license from one computer to another. On the other hand it allows vendor to easily extend or modify the license, without bothering the user [24]. Product activation is not completely effective in stopping copyright infringement of software, as these keys can be distributed. The overall effectiveness of product keys in enforcing software copyrights requires further study. In addition, with improved communication from the rise of the Internet, more sophisticated attacks on Keys such as cracks (removing the need for a key) and CD key generators have become common [25].

Digital Rights Management

Digital Rights Management (DRM) is one of the major technologies for protecting and distributing intellectual property assets in the Digital Age. It is a system to protect high-value digital assets and control the distribution and usage of those digital assets.

Windows Media DRM:Window Media DRM is the digital rights management system developed by Microsoft Corporation to provide delivery of audio and/or video content over an IP network to a PC or other playback device in such a way that the distributor can control how that content is used. Windows Media DRM uses Windows Media Format to distribute the protected content. In this format allows storing rights management information in the media file [26]. Attempts to crack the Window media DRM have been made with a varying degree of success like DRM removal and others.

Fair Play:Fair Play is the control mechanism used in Apple iTunes, iPod and QuickTime. Fair Play provides fixed set of conditions. Protected files may be copied to any number of portable music players.They may also be used on five authorized computers simultaneously. To authorize a computer,

iTunes sends a unique machine identifier to Apples servers. In return the computer is provided with all of the users keys needed to unlock the protected files. The protection that Fair lay provides is very limited. Since neither the audio tracks are protected nor the quality is reduced, it is easy to re-encode the CD and generate unprotected copies of the music files [27].

Helix DRM:Like Fair Play, Helix uses advanced Audio Codec Format. The architecture of Helix DRM is similar to WM DRM. The Helix DRM Packager encrypts the source media file. Helix DRM License Server receives the licensing requests, issues content licenses to end-user clients and provides auditing information for royalty payments. As WM DRM Helix provides flexible licensing options, in which the content owner can also revoke licenses, if terms of use were violated [28].

Protection mechanisms in DRM system

Digital cryptographic technologies, digital water mark and digital fingerprinting are some of the common protection mechanism in DRM system.

Digital cryptographic technologies:DRM Systems use different cryptographic algorithms to secure the content. The most manufacturers keep information about used algorithms confidential. However, since standard algorithms are more efficient, a standard symmetric key algorithm such as Advanced Encryption Standard (AES) or CR4 might be used to protect the content in the most digital rights management systems [29].

Digital Watermarking:A digital watermark is an imperceptible sign inserted into digital content. A Watermark should be robust against common signal transformations such as filtering or compression. Watermarks can be used for identifying copyrighted material, using special search robots the rights owner can determine if his marked content is illegally distributed through the World Wide Web or file sharing networks. Watermarks can be also used for try-before-buy models. In this model, the watermark affects the quality of the content [30].

Digital Fingerprinting:Digital fingerprinting is an enhancement of watermarking technology. They do not only identify if the content is copyrighted and who is the owner, but also have identification information, which allows distinguishing between different instances of the same copyrighted content. Fingerprinting helps the forensics to find out which consumer has spread the copyrighted material [31].

Summary for the benefit and pitfall of Digital Right management system

The Pros: Content producers use DRM protections to limit copyright infringement and theft of intellectual property. DRM technology is used to protect artists and other content producers from copyright infringement and theft of intellectual property. Therefore digital

right management system can limit the unauthorized sharing and unpaid usage of the contents.

The cons: DRM system has certain critics' raised from consumers. Critics claim that Digital Rights Management technology can limit even legal usage of media purchased by consumers. This usage may include creating backup copies and lending by libraries, which are considered fair use under copyright law. Other critics of DRM usage claim that there is a chance that some media may become totally unusable with changes in technology. Another problem they find is that may be an anti-competitive practice to include DRM technology in products.

Other cons

- It affects eBook sales, many people refuse to buy digital products that have DRM in place and/or objections to it on principle. Secured formats also cause ten times the number of customer service calls, when compared to unsecured formats. A customer who has a problem with a secured file is less likely to purchase DRM formats again.
- bugs in the DRM software
- The inability to use a file they paid for across multiple operating systems they own personally. Secured formats are difficult or impossible to pass from device to device.
- The inability to back up and safeguard files.
- Limit the ability of the legal purchaser to fully use the content, such as printing locked PDF files, citing material in a scholarly study, or when using a recipe from an e-book version of a cookbook. Some might argue that you have to hand type in from a paper book, but the fact is the unique advantages of e-books are stripped away by DRM.
- The inability to make the e-book into an audio book.
- The inability to print and read on the go from paper.
- The added expense of DRM, which is passed along to the reader, in the form of higher prices.
- DRM punishes honest purchasers, in a vain attempt to stop criminals. There is currently no DRM that cannot be broken. When a new form comes out, it is usually broken within a number of weeks and the hack…or the unlocked copy of the file is passed around[31].

Chapter Three

3. Related Work

In this section research works done so far related to this research work idea regarding protection of copyright in digital media will be discussed.Research works that have been done to stop or reduced digital piracy using computer technology will be discussed.

Research works regarding digital piracy lies into two groups:

- ✓ Piracy detection
- ✓ Piracy prevention

3.1 Research works in Detecting piracy

3.1.1 Software/Application piracy detection research works

HIDDEN MARKOV MODELS FOR SOFTWARE PIRACY DETECTION

In this research work a method for detecting software piracy is presented. The researchers develop and test a tool that can be used to detect pirated software. The technique can be used if a company suspects that their copy- righted software has been illegally copied. This tool based on hidden Markov models, the original software is scored against the suspected pirated copy. A high score indicates that further investigation is warranted, while a low score indicates that the two pieces of software are almost certainly distinct. No source code is required, executable software can be used to detect piracy. In addition, only statistical analysis is used neither the original nor the suspect code is executed [32].

The research work contributes a lot for software companies in getting evidence after suspecting somebody or some organization in pirating their software by using hidden Markov model for this domain. The above common limitations of detecting piracies works is shared in this research too.

Method Based Static Software Birthmarks: A New Approach to Derogate Software Piracy

In this research work a 'method based' software birthmark technique targeting the distributed piracy threats is proposed. The researchers found the intrinsic properties in software methods by locating their code attributes, elements, and relation among code elements. The proposed approach identifies similarity of programs and detects program transformation as well. Moreover, the technique can spot out method as well as class theft while assuring the credibility and resilience properties of birthmarks [33].

This research work contributes in differentiating the original copyrighted software from the copied one by using powerful method based software birthmark technique. Moreover the method can pick out which class or method is plagiarized from the original one. The above common limitations of detecting piracies works is shared in this research too.

Survey of Feature Extraction Techniques to detect the Theft of Windows applications

In this research a method to extract the feature information from the binary codes of the executable files on MS Windows systems in order to determine whether software is pirated or core modules of a program are stolen is presented. The researchers perform a small experiment to detect program similarity and plagiarism by comparing the statically extracted features of target programs.

In this research work, the researchers have compared static and dynamic software birthmarks and studied the methods to calculate similarity between two programs using the birthmarks. They have proposed several techniques to extract birthmarks form Windows executable to detect software theft. Then, they have performed a simple experiment to measure similarity between small programs using static kgram based birthmark which was a sequence of k contiguous opcodes in an executable [34].

The contribution of the work is the researchers proposed that the possibility of detecting software piracy especially window applications by measuring the similarity of the birthmarks of the original and the suspected executable applications. The same limitations will be inherited as of the other piracy detection research works.

A Method for Detecting Illegally Copied Apk Files on the Network

In this research work a method of detecting illegally copied Android applications targeting at the APK (Android application package) files is presented. The data objects being transmitted from the network were extracted through the process of sniffing, analyzing, and assembling packets. Then, an analysis on the features of APK files is made to judge whether the extracted data object is an APK file or not. The researchers claimed that they were able to achieve a success rate of 95.5% in detecting illegally copied applications by identifying them through APK feature points and forensic technologies [35].

The contribution of the research work is the proposed method helps in detecting illegally copied application distribution in the network. Identify the illegality of applications by judging based on APK feature points and forensic watermarking information will contribute a lot in decreasing piracy in the Android application market. The other advantage is of minimizing the slowdown of operating systems due to illegally copied applications detection, as it performs packet sniffing on the network driver level.

The limitation is the scope of the work is limited to Android applications, which is a common limitation for the other works too. The other limitation is the proposed approach needs reporting the result to other central server which has IP address and other information to reach to the IP address which use illegal copied Android application, but here finding the IP address doesn't always mean finding a person to be accused of digital piracy. Moreover it is expensive to build such central server system, which handles much IP addresses and routers information.

3.1.2 Video Piracy detection research works

A Hierarchical Scheme for Rapid Video Copy Detection

This research work presents a hierarchical scheme to detect video copies, especially the temporal attacked and re-encoded ones. The researchers articulate algorithm which is based on the ordinal signature of intra frames and effective R*-Tree indexing structure archives real time performance. This is to detect a query video is a copy or not and has two steps:

1. Off-line step to collect copyrighted videos to build a DB which maintains extracted features.

2. On-line step the classifier process the query video and determine which query is a copy.

The contribution of the work is the proposed approach to detect video copies enables to distinguish whether a query video is a copy or not. This will definitely help to differentiate the original copyrighted video from the copied one, as forensic evidence.

The same limitation will be shared here with the other piracy detection mechanism. The other limitation that is specific to this work is; it is not simple to continuously feed new copyrighted videos to the database as thousands of videos will be created per day [36].

Novel Framework for Video Content Infringement Detection and Prevention

This research work presents a technique which aims to detect and prevent a replicated video from being uploaded into the web. The technique can serve as a standard at the server end, verifying for the authenticity of a video.

The entire technique is composed of two levels: the first level deals with extraction of feature set from the video and the second level deals with embedding of secret information into the same video from which the features are extracted.

The feature set of the video for which the legitimacy is to be tested is also obtained by mapping against the reference feature set that has already been obtained and stored. This mapping is done based on the faces that are present in the feature set in accordance with the time of occurrence constraint.The video to be checked for piracy will be checked for if it has the bits that are embedded at pixel level in the original video. The bits that are obtained from the video are compared with those that are present in the reference set. If both the bit streams match, then it is certain that the video currently tested is authentic and can be uploaded into the server. In cases of any inconsistency between the bit stream obtained and the reference set, corresponding action like blocking the video from being uploaded or an alarm being raised can be taken[37].

The contribution of this research work is the proposed technique presented by the researchers really helps in differentiating the original copyrighted video from the copied one.

The same limitation will be inherited together with piracy detection mechanisms in this research work too. The specific limitation for this research work is the researchers feel uploading only copyrighted videos on the server prevent video piracy. But uploading could be another piracy by itself. There is no prevention mechanism as the researchers thought for video piracy in their proposed technique, it is only detection.

3.1.3 Research works in piracy detection in Peer-to-peer network

There are many research works in detecting illegal file sharing, in this section only few of them will be discussed.

Detecting Illegal File Sharing in Peer-to-Peer Networks using Fuzzy Queries

In this research architecture that integrates fuzzy queries and an inference process with a P2P protocol called Localized Fuzzy Search Protocol (LFSP) is proposed. This will help in reducing much of the P2P query traffic which is caused by the keyword search method; a typical P2P network uses query broadcast to enable keyword search and are not able to express impreciseness. These protocols and mechanisms can be reinforced by the use of fuzzy logic. The LFSP decreases P2P traffic and enables the discovering possible sources of illegal file sharing by querying directly the P2P sources. The researchers claimed that their proposed architecture can be used by organizations wishing to detect possible sources of illegal file sharing and that are willing to take the corresponding actions [38].

The contribution of the research work istwofold; the first one is application architecture that incorporates fuzzy queries and an inference process with a P2P protocol in order to detect possible sources of piracy and take the corresponding actions. Additionally, the fuzzy query is translated and executed over a set of distributed hosts in the network. The second is an application layer P2P query broadcast protocol called Localized Fuzzy Search Protocol (LFSP). LFSP decreases traffic from searches in P2P, is space efficient, and reduces the processing time of discovering possible sources of illegal file sharing.

The limitation of this research work is detecting illegal file sharing is not taken as a major task in this work it is seen as a byproduct while making an architecture which is space efficient. It do nothing special towards detecting illegal copy only providing a means to reduce the processing time of discovering possible sources of illegal file sharing.

3.2 Research works in piracy prevention

3.2.1 Piracy prevention in peer-to-peer network

Collusive Piracy Prevention in P2P Content Delivery Networks

In this research work a proactive content poisoning scheme to stop colluders and pirates from alleged copyright infringements in P2P file sharing is proposed. The basic idea is to detect pirates timely with identity-based signatures and time stamped tokens. The scheme stops collusive piracy without hurting legitimate P2P clients by targeting poisoning on detected violators, exclusively. Researchers developed a new peer authorization protocol (PAP) to distinguish pirates from legitimate clients. Detected pirates will receive poisoned chunks in their repeated attempts. Pirates are thus severely penalized with no chance to download successfully in tolerable time [39].

The contribution of this research work is presenting a new protocol that helps to distinguish pirates from legitimate customers and making trusted zone of file sharing.

The limitation lies on the proposed protocol which uses identity-based signature from the file index, a peer authentication is done in the protocol to establish the legitimacy of a peer when it downloads and uploads the file. But the protocol is in questioned; hence it is very difficult to create identity-based signature for peers based on the files they share.

PPBD: A Piracy Preventing System for BT DHT Networks

In this research work a system called PPBD to stop pirated content propagation by utilizing several attacking methods is designed. First, the system can efficiently deal with massive concurrent connections to reduce bandwidth consumption, schedule peers to cooperate and optimize the protection methods according to clients. Second, two mathematical models for BT DHT attacks are constructed, and the system performance is theoretically analyzed. Third, the researchers take into account some countermeasures of different BT clients and make corresponding optimizations of our PPBD system. The real world experiments show that: The system can extend the download duration at least three times by the fake-block attacking method and it is more effective in a small swarm; (2) DHT index poison and routing pollution methods can limit the sharing swarm to a small swarm [40].

The contribution of the work is: the PPBD system that is designed by the researchers can delay the propagation of piracy contents in BT DHT network without modifying the existing network architectures and protocols. Secondly a mathematical model for the fake-block method and a polar coordinate ID space model for the DHT pollution methods are constructed. These models are used to analyze the effectiveness and efficiency of PPBD. The protection mechanism is optimized for popular BT clients by considering their different implementations. The optimization can significantly improve system performance and reduce resource consumption.

The limitation of this research work lies on the scope which is fixed with the BitTorrent

(BT) distributed hash-tables (DHT) network types.

3.2.2 Software Piracy prevention

A Robust Approach to Prevent Software Piracy

In this research work the researchers refines their earlier proposed technique "Software Piracy Prevention through SMS Gateway" to make it more stable and effective against piracy. The targeted approach is based on SMS gateway service to install software on a system, but the technique left some problems untouched i.e. issues related to MAC address, time offset and Man in the middle attack. In refined approach the server will initiate authentication process instead of client at regular time intervals, and this facility increase the effectiveness of the technique.

In proposed technique, at the time of purchasing software, authentication server maintains serial number SN and a mobile number MN association. Server starts the process by sending periodic challenge to each of its client on registered mobile number by sending server time stamp along with hash of time stamp which is encrypted by private key of server which provides integrity with authentication and then server waits for response from client. Client receives challenge and compare received hash of time stamp with the integrated or decrypted hash of server timestamp with public key of server. Otherwise, if client will not receive challenge at fix period or received hash is not equal to calculated hash i.e. challenge is tempered, software Uninstallation process starts [41].

The contribution of the work is the proposed new approach helps in software piracy prevention. Checking the authenticity of the Software at every fixed time interval gives it advantage to identify fake unauthorized users. And then blocking such installed software save software companies from huge loss because of software piracy.

The limitation of the research work is using SMS gateway as dependable means in authentication software will have its own problem, what if the mobile owner loss his cell phone by chance this means he will no longer use that copyrighted software. Genuine users may be hurt if there is connection problem in their cell phone hence the client expect a SMS message to receive from the authentication server to authenticate the software. The other limitation is the scope of the work is limited to software as of the other works.

Software Piracy Prevention: Splitting on Client

This research work proposes a software-splitting technique in which the split contents are put on the client instead of the remote trust server. Unlike traditional static client identification techniques, this new technique would encrypt the extracted contents from the software by a key relating to the hardware characteristics, and then decrypt them dynamically during the main program running. This method not only makes it harder to create an additional available copy based on diversity, but also prevents illegal uses on the copy [42].

Contribution of the work is this new technique approves the communication latency which was in the former software splitting technique; a technique for protecting software from piracy by removing code fragments from an application and placing them on a remote trusted server. Moreover it may overcome the weakness of classical client-side static registration techniques as the split contents are on the client side itself.

The limitation of this work is the scope is limited to software piracy. The other limitation is related to computer resource consumption; it needs extensive processor speed in the client side.

Software Piracy Prevention through Diversity

In this research paper the researchers claimed that the weaknesses of existing piracy preventions approaches, is resulting from the static nature of defense and the impossibility to prevent the duplication of digital data. They present a new scheme that enables a more dynamic nature of defense and makes it harder to create an additional, equally useful copy. Furthermore it enables a fine-grained control over the distributed software. Its strength is based on diversity: each installed copy is unique and updates are tailored to work for one installed copy only. Each installed copy differs enough from all other installed copies to guarantee that successful attacks on its embedded copyright protection mechanism cannot be generalized successfully to other installed copies [43].

The contribution of the work is the researchers try to model a dynamic defense scheme obviously it will help more than the static one. The dynamic nature is possible through updates. Software updates are used for other purposes too other than the piracy prevention like: to fix bugs; to add security patches; to support new hardware and new file formats; to keep a program compatible with other programs; to add new functionality.

The limitation of the work is as the other work is the scope is limited to software piracy. The other limitation is the automatic update cannot be considered as the only means to prevent piracy. This way of prevention needs to establish a system like digital right management system which needs all software vendors and users to be a partner; such a system is more ideal and very difficult to realize it.

3.3 Summary of Related Works

Research has been done both in preventing and detecting digital piracy. Detecting digital piracy is used to get evidence for forensic case after a suspect pirate is brought to a court. The detecting mechanism helps to differentiate the pirated copy from the original one. The contribution is detecting piracy will help as forensic evidence, this is a great contribution hence most of the time after suspecting a piracy it will be very difficult to get a confidential evidence to bring the pirate to the court. The limitation that all piracy detection works share is the suspected digital content should be caught in order to check it with the original copyrighted work. To get somebody with the pirated digital content at hand it should be sudden investigation which is forbidden according to any country constitution without the order paper from the court. Therefore there is a chance that the suspected body can change the copied digital content to the original one after receiving court order paper.

Preventing piracy is better than detecting after it happened. Researches which try to prevent piracy have greater contribution towards minimizing digital piracy. The limitation shared by almost all this kind of research work is there scope is limited to one type of digital content either for software, video, computer game or music they don't consider all at once.

This research proposed a way in preventing digital piracy which can be applied to almost all types of the digital contents. As piracy is a common problem for all digital works which are subject to copyright because of their nature, hence they are digital they can be easily copied and distributed.

Chapter Four

4. Proposed Model

4.1 Overview of the proposed Model

This research is engrossed on the possible ways of protection of infringing copyright law. The user/consumer who bought the original copyrighted digital content may apply various techniques to get more free copies, to share it with friends, or at worst case to distribute the illegal copies to the public with a free or minimal cost. The likely techniques that could be applied are studied and all user activities are identified based on the copyright law which states the right to copy/distribute is only for the copyright owner whereas activities that lead to copy and distribute are categorized as pirates' acts but other activities like opening areconsidered genuine use. Therefore this research work deals with identification of user action on copyrighted digital content, designing tracing model to catch up the user actions, developing prototype for the modeland testing it using test cases considering different user actions.

The proposed model traces users' activities which are considered as pirates' acts at the operating system level.The operating system that is considered in this research work is Window operating system as it has 90.6% of the total market share for desktop applications[44].

4.2 Technique to hide the proposed anti-piracy software

This section briefly describes how the copyrighted data together with the anti-piracy software which use the proposed predicting model can be burn in a CD/DVD for distributing the copyrighted content. Hence, if the anti-piracy software and the copyrighted file simply stored in a CD/DVD, it will be very easy for pirates to cut the anti-piracy software and to get the copyrighted file for free in order to copy and share it as they like. There for data soring technique is needed to avoid this problem and steganography is one to apply.

Steganography

Steganography is the art and science of encoding hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message. It is a form of security through obscurity. The word steganography is of Greek origin and means "concealed writing". It combines the Greek words steganos meaning "covered or protected", and graphei meaning "writing". Generally, the hidden messages will appear to be (or be part of) something else: images, articles, shopping lists, or some other cover text [45]

In this case the hidden part will be the anti-piracy software which uses the proposed model and the copyrighted file will be the visible one. There are steganography tools to hide applications inside other digital data. Most of the tools accept single files for both the hidden and host file; there for the application software in this case which is built by java needs to be a single JAR file (Java Archive file). This is because a JAR (Java ARchive) file contains the class, image, and sound files for the developed Java application which is gathered into a single file and possibly compressed. And to use this Anti-piracy softwareJava runtime platform is required.

4.3 Proposed Model

To design the tracer model first we tried to answer the question what a user do? Or what is the user act as she/he purchases a copyrighted digital content after she/he inserted the digital content in the CD/DVD drive? By analyzing this question all the possible user acts were identified. Table 4.1 shows the list of all identified user acts.

Table 4.1List of identified user acts

No	Acts
1	Open
2	Play
3	install
4	Upload
5	Share
6	Copy
7	burn

According to the copyright law which states the one who purchase the copyrighted digital content is legible only to use the content for herself /himself, users' activities can be either piracy act or genuine act. Activities like copying, sharing are piracy acts whereas playing, installing and opening are considered to be genuine acts.

Based on this classification it is possible to predict users' activities as piracy or genuine action and its description is presented in Figure 4.1.

No	Acts
1	Open
2	Play
3	install
4	Copy
5	Burn
6	Share
7	Upload

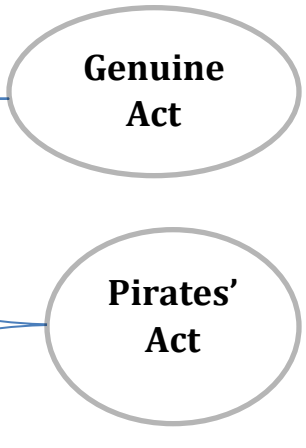

Figure 4.1 Categorizing user acts based on copyrightlaw

In building the proposed model the following tasks are accomplished.

- Tracer model design
- Prototype development for the Tracer model
- Testing the prototype based on scenarios representing users' actions.

4.3.1 Tracer Model

Regarding tracing users' activities, the question to be raised is users' privacy. In the Tracer model to keep users privacy the actions that will be emphasized are only pirates' act. Actions that will be done on other applications or to manage the working environment will not be tracked by the tracer model. The tracer model represents tracing of user activities. All user activities upon the digital content are traced by tracking all the events and processes at the operating system level. To trace the user activities, first it is important to realize all the potential actions through which a user pirates a digital content.

In order to do piracies a consumer, the one with the original copyrighted work can do one or more of the following listed actions listed in table 4.1 and thisis the first input to the tracer model and should be traced as events and processes at the operating system level.

The whole actions that the user can do arecategorized into three groups:

1. Reproducing the original work
2. Sharing the original work
3. Using the original work genuinely as intended in the copyright law

Table 4.2 Possible actions through which a user pirates a digital copyrighted content

Case	Action	Description
1	Copy	Copying the original work to other secondary storage devices like: CD, DVD, Blue Ray, Flash disk, external hard disk or the computer hard disk (Copy then Paste or cut then paste), [for Music]Copy the original work using Media players to library files.
2	Burn	Burningthe original work to a CD/DVD using special burning/authoring applications.
3	share	• Sharing in P2P file sharing system. • Sharing through FTP File Transfers • Attaching to Email • Uploading to Web

4.3.1.1 Case 1:copy

The following cases show the possible activities of a user in using the copyrighted original work in MS Windows operating system and solutions proposed to trace the activities.

The user tries to copy the original content using one of the following ways:

- The key board shortcuts: Using Keyboard shortcuts **Ctrl + C** or **Ctrl + Ins** to Copy then Paste in the intended location with **Ctrl + V** or **Shift + Ins**
- The **copy** function: of the same application in which the content is played or another application used to read copyrighted content.
- Using shortcut: to get the **Copy** command like: Right click then from the short cut menu select Copy, Shift + Right click then from the short cut menu Copy, Shift + F10 then from the short cut menu Copy, Application key then from the short cut menu Copy, Alt + Down Arrow then from the drop down list box copy
- Dragging: to another location or hold down the CTRL key while dragging to another location, this activity is to create a copy of the file therefore the drag action can be taken as Copy and the drop is the same as paste in Windows operating system.

Through any of the above methods in Window operating system, the copied content is copied to the system Clipboard for temporary usage and then in pasting it is pasted to the destination location which can be hard disk, Floppy disk, CD, DVD, flash etc. Therefore it is possible to trace the copying activity of a user or anapplication from the clipboard as depicted in Figure 4.2.

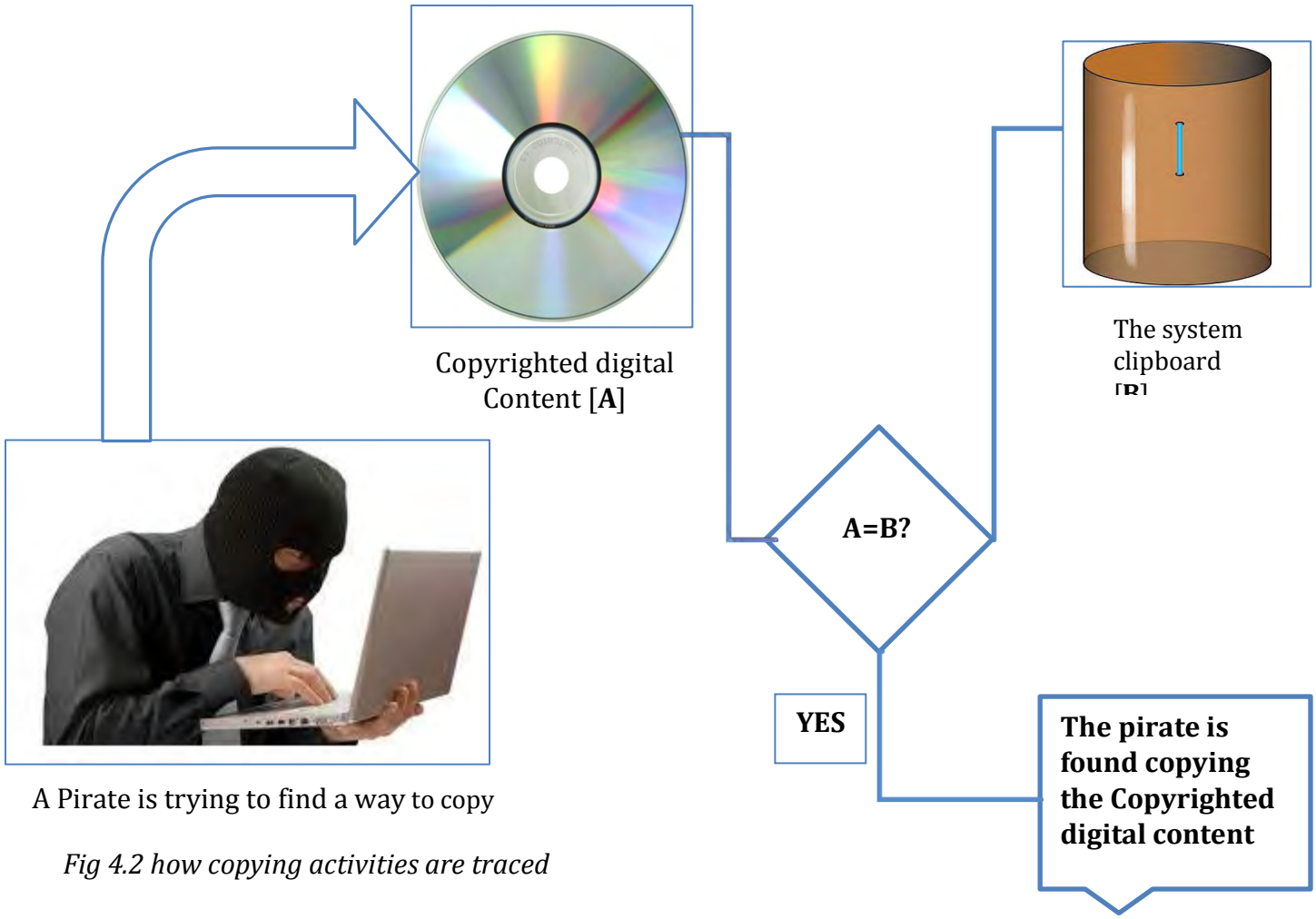

Fig 4.2 how copying activities are traced

Windows has a feature called the Windows Clipboard which is available in almost all other operating systems too.The clipboard is a set of functions and messages that enable applications to transfer data. Because all applications have access to the clipboard, data can be easily transferred between applications or within an application [46].

Finding the filename of the copyrighted file

To find the filename of the copyrighted file the following technique is used.The copyrighted file is expected to come with CD/DVD copy as it is a digital copy distribution. Getting the file lists inside the CD/DVD means getting the copyrighted file as most computers comes with only one CD/DVD drive. Differentiating drives of a computer system in order to identify the CD/DVD drive path is mandatory. After getting the right CD/DVD drive it is possible to list all the files inside the CD/DVD filename that is considered as the copyrighted filename.

Finding the filename of the current file inside the system clipboard

To find the filename of the current file inside the system clipboard the following technique is used. First the system clipboard will be known then the data flavor in order to get only file types will be set, finally the filename of the current file inside the system clipboard is found.

Comparing the two filenames (filename of the copyrighted file and filename of the current file in the system clipboard)

The algorithm presented in Figure 4.3 shows comparing files from clipboard and CD.

```
1. Start
2. Compare the file name of the copyrighted file andthe
   current file inside the system clipboard
3. If the two filenames from step2 are the same
4. Display Copyright  law is violated  and eject the CD
5. Else
6. Go to step 3
7.  End
```

Fig 4.3 Algorithm comparing clipboard and CD file

The flow chart representation of tracing users' action while copying is depicted in Figure 4.4.

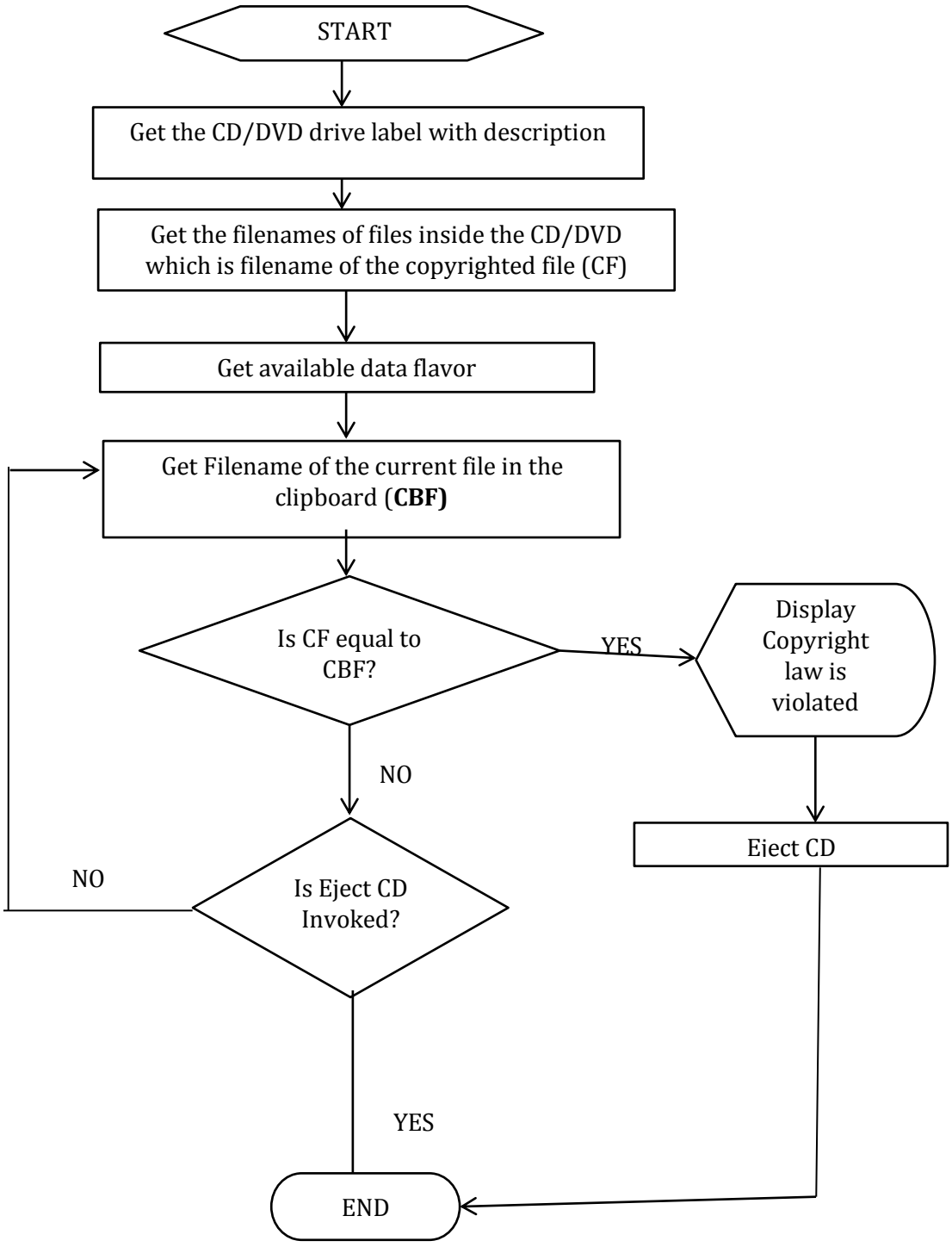

Figure 4.4 Flowchart representing algorithm for tracing of copying

4.3.1.2 Case 2:Burn

Burning a CD/DVD means putting or entering data on a blank CD using burner/authoring software. To trace burning activity different options for tracing and stopping has been observed and the following solutions are settled out.

Tracing Most Widely used Burning and Authoring Software

Among all the burning and authoring applications those which could be challenging for the copyright law are only those which allow users to copy the entire CD/DVD. In this research work the possible and the most widely used burning/authoring applications which are available at the time of this research done with entire CD copy options are tracked by checking from the operating system process table. Hence in order to use burner software a blank CD/DVD is inserted; while using the copyrighted digital content which is in a CD/DVD if such kinds of burners are started to the entire CD/DVD, soit is considered as trying to violate copyright law.

Pirates' Expected Burners

It is expected that pirates' may try to do their own burner software which can't be tracked by the tracer model in the above case. To trace such burners and grant the tracing of burning activities, the general behavior to create burner software is studied. Two types of burners are exhibited. The first type of burners use buffer, the common characteristic that such applications have is they rely on internal buffer to store the copied data temporarilyuntil burn. To get the internal buffer and knowing the data content inside is a must. The second type is using direct Read/write option without buffering.

Tracing buffered Burning activity

Buffer: A buffer is memory area that stores data being transferred between two devices or between a device and an application. Buffer is a pre allocated area of the physical memory where data can be stored while processing [48].

Methods for Accessing Data Buffers

One of the primary responsibilities of driver stacks is transferring data between user-mode applications and a system's devices. Window Operating system provides three methods for accessing data buffers: Buffered I/O, Direct I/O, Neither Buffered nor Direct I/O. Among the three the one that is useful for accessing data buffer is Buffered I/O

Buffered I/O

Window operating system creates a non-paged system buffer, equal in size to the applications' buffer. For write operations, the I/O manager copies user data into the system buffer before calling the driver stack. For read operations, the I/O manager copies data from the system buffer into the application's buffer after the driver stack completes the requested operation. [48]

Tracing both buffered and un-buffered Burners

To trace burners which use both buffered and un-buffered burners the general solution which is used is disabling and enabling the CD burner functionality technique. The CD burner functionality is expected to be enabled at first in any computer system. Disabling the burning functionality by program and enable it just before CD-Eject is called is a general solution for both buffered and un-buffered burners.The algorithm representing Cd/DVD-ROM disabling is depicted in Figure 4.5.

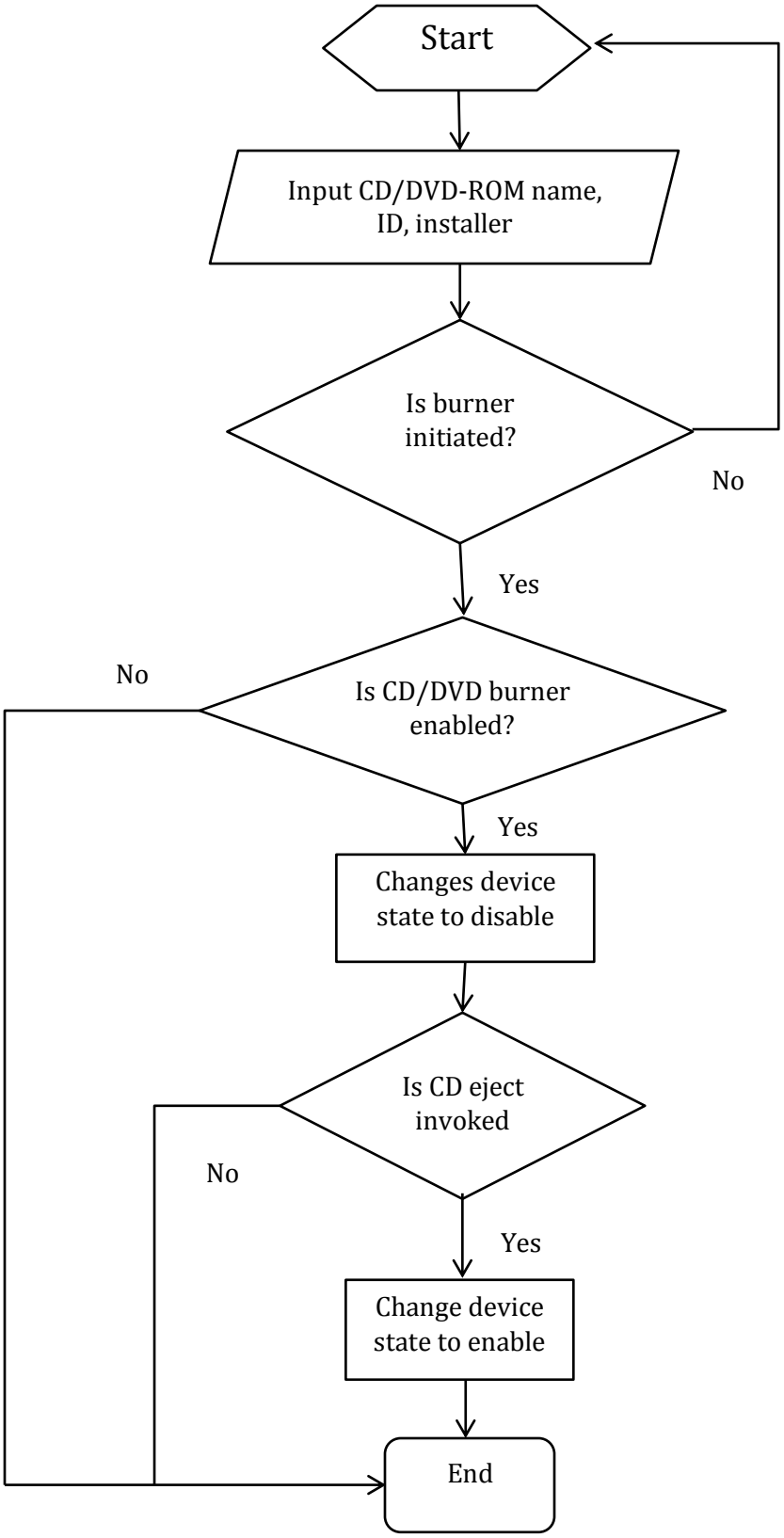

Figure 4.5 Flow chart to disable CD/DVD Burner and enable at CD eject

4.3.1.3 Case 3: Share

The third case that the user may do is sharing the copyrighted content. Sharing copyrighted content illegally is act of piracy as it may give illegal access for all users withinin the connection.A file can be shared by different methods like:-Peer to Peer File Sharing, FTP File Transfers, attach to Email, and Online Sharing Services.

How to trace file sharing in a network connection in Window Operating system

The algorithm to trace file sharing in a peer-to-peer system, FTP file transfer, e-mail attachment and uploading is as follows:

Figure 4.6 depicts the algorithm that tracesfile sharing activity

```
1. Get the local host IP address for the copyrighted file
2. Buffer the result  from 1 in temporary basis
3. Check the  host IP address for the copyrighted file
4. Compare the result from 2 and 3
5. If 2 not equals3
6. Buffer the difference host IP address
7. Make the sharing unsuccessful by deleting the copied data in
   the result from 6
8. Go to step 1-4 recursively
9. Delete the temporarily stored host IP address at CD eject
   invoking.
```

Figure 4.6Algorithm to trace file sharing

Description Algorithm:

Get the Local host IP address for the copyrighted file is used toreturn the address of the local host, which is the first original computer system. This is achieved by retrieving the name of the host from the system.

Buffer the host IP address temporarily

Storing the local host IP address for temporarily and delete it on CD eject helps in avoiding a problem that hurts genuine users by restricting to use only one computer. Users might use the same CD of the copyrighted file in different computers; at home, in office or other place. The

proposed algorithm for tracing file sharing tracks only when a user tries to share a file and not affect legitimate users.

Get the host IP address for the copyrighted fileisamethod which returns the IP address of the host computer at any time.

Compare the result from 2 and 3

Comparing the first local host IP address with host IP address is needed to see the change in the IP address which host the copyrighted file. If the two IP are the same it shows the copyright file is still on the first computer so it is not shared, otherwise a change on the two IP addresses indicates the copyright file is shared to other computer(s). The host IP address which is different from the first local host is buffered and the sharing is made unsuccessful by corrupting the copied data on the second host IP. The flow chart on Figure 4.7shows the step by step activities to trace the user action in case 3 sharing.

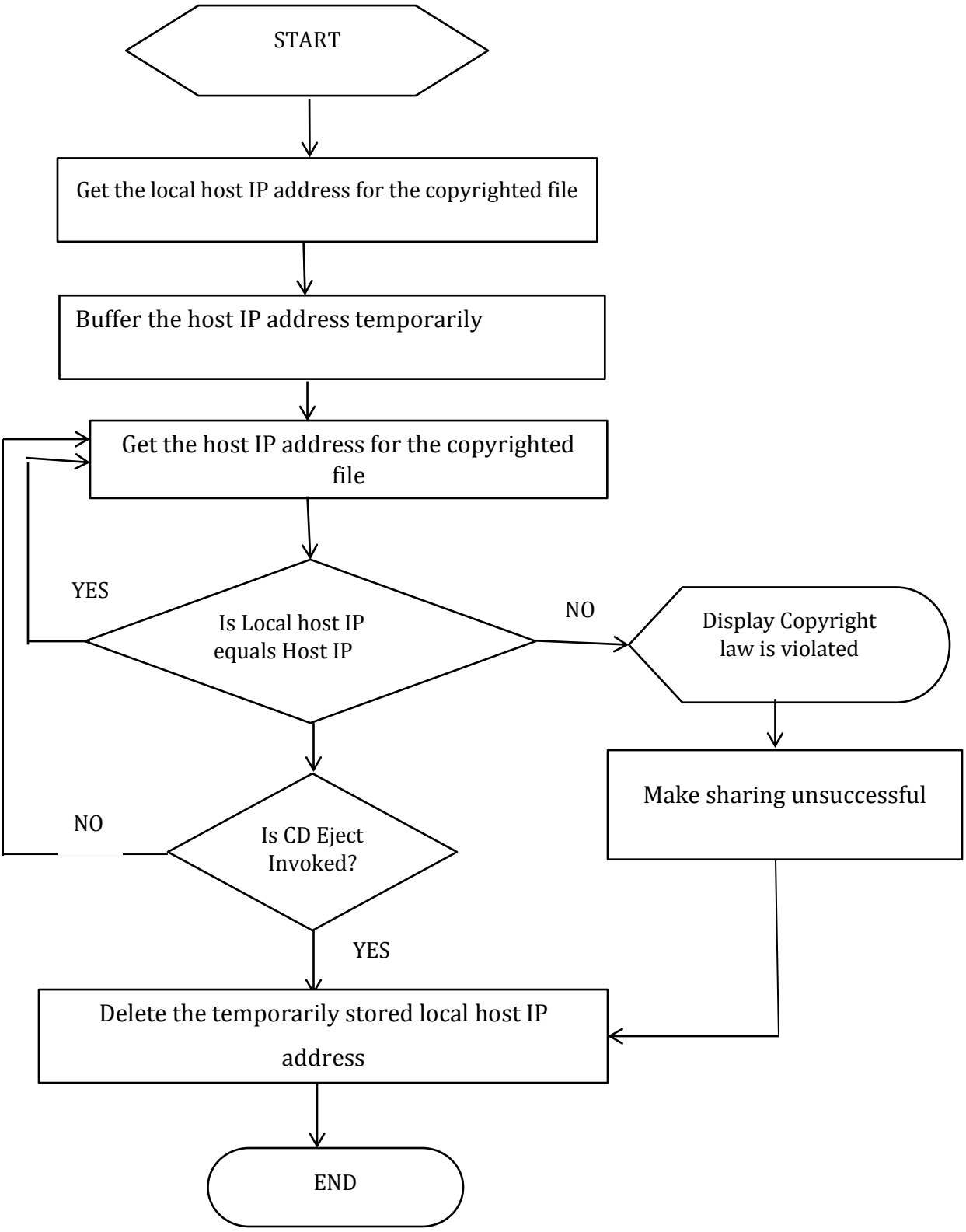

Figure4.7 Flow chart to trace users' activity in file sharing

Chapter Five

5. Implementation

5.1 Prototype for the Tracer Model

To demonstrate the effectiveness of the tracer model, a prototype is developed using java programming language on NetBeans IDE. Java is selected because of its interoperability featuresand ease of use to trace events and processes. The piracy acts addressed in the prototype include copying, burning and sharing. When any one of the piracy acts is performed, the prototype displays copyright law violation pop up message and it action is triggered to prevent the execution of the operation on the copyrighted digital content.

5.1.1 Tracing copy

Java source code compares the CD/DVD content with the Clipboard content

Getting the CD/DVD content

To get the CD/DVD content, the path for CD/DVD drive in that specific computer system should be known. The following code is used to get the CD/DVD drive path.

```
File[] paths;

FileSystemViewfsv = FileSystemView.getFileSystemView();

paths = File.listRoots();

for(File path:paths)

{

if("CD Drive".equals(fsv.getSystemTypeDescription(path)))

JOptionPane.showMessageDialog(null, "The CD Drive is: "+path,"Message",
JOptionPane.OK_OPTION);

 }
```

Figure 5.1 CD/DVD path accessing java program.

The source code in figure 5.1 returns the CD/DVD drive in any computer system like E/: F/: G/: or other which depends in the computer system drive usage.(See the screen shot depicted on Figure 5.2.)

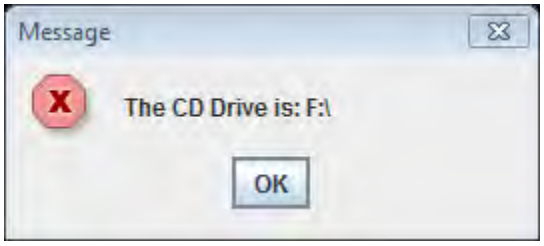

Figure 5.2 Screen shot showing CD/DVD path while the java code in Figure 5.1 is run.

Once having the CD/DVD drive path the method in Figure 5.3 is used to read the files in the drive if not empty. The java source code in Figure 5.3returns names of files, directors read from the specified CD/DVD found in the CD/DVD drive. This is the first activity required to trace copying.The second one is getting the copied file inside the system clipboard. The java code that is used to get the clipboard content is presented in Figure 5.2.

```
Clipboard clip = Toolkit.getDefaultToolkit().getSystemClipboard();
DataFlavor[] flavors = clip.getAvailableDataFlavors();
    String disp="";
for (DataFlavor f: flavors)
        {
          Try  {       disp=clip.getData(f)+"\n"; }
catch (Exception e1)
            {       }
JOptionPane.showMessageDialog(null, "The file copied is: "+disp,"Message",
JOptionPane.OK_OPTION);
          }
```

Figure 5.3 java Code to get current file in the clipboard.

The java source code in Figure 5.2 accesses the system clipboard and reads the copied file from the clipboard (see the screen shot in Figure 5.4).

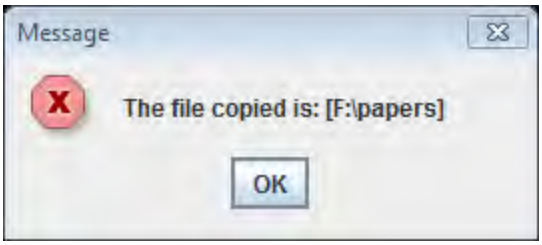

Figure 5.4 Screen shot displaying the copied file from CD/DVD path while the java code in Figure 5.3 is run.

After reading files from the CD/DVD and from the system clipboard to check whether the copyrighted digital content is copied or not is just to compare the two. The prototype developed to trace copying (the complete java program is found in **Appendix A**) compares the two files and if they are the same the CD/DVD is ejected automatically with popping message that shows the copyright rule is violated. (See the screen shot depicted in Figure 5.5). And if they are not the same the system takes no action.

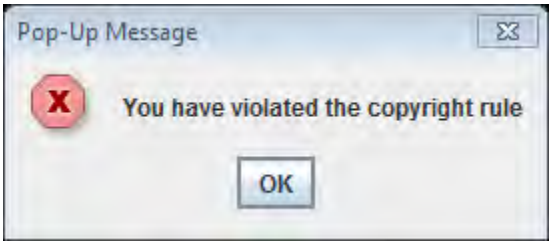

Figure 5.5 Screen shot of pop-up message due to the user copyright violation and it results automatic CDEject.

5.1.2 Tracing burn

The burning activity is tracked in two ways: The first is tracking the most common burner applications is done by tracking these applications from operating system process tableof windows operating system.The implementation is done using Java programming language and while one of the common burner applications listed and stored in an array (See the complete java program on **Appendix B**) are opened, the java program checks the existence of the burner application name in the list and if so a pop-up message which says "You have violated the copyright rule" is displayed and automatically the CD is ejected. The screen shot depicted in Figure 5.6 is displayed while trying to burn using Nero burner.

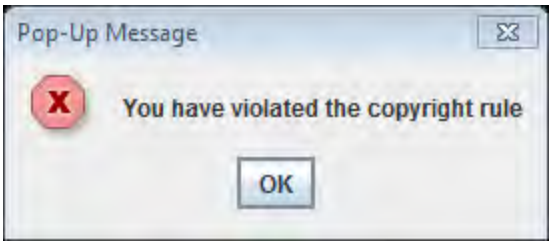

Figure 5.6 Screen shot of pop-up message while trying to use Nero burner and it results automatic CD eject.

The second tracing burner activity is done for pirates' expected burners. The implementation of this part is done using Visual basic in opposition to the so far implementation which is done using java; java is used for the sake of familiarity and ease of use in that specific condition. Visual basic is selected in this case as both Window operating system and Visual basic are from the same Microsoft company and accessing the window components is more easy and there is a help guideline from Microsoft to use Window components in programming languages like C, C++, C#, and Visual basic. Visual basic is selected for the sake of familiarity from the other three. Because pirates' can use third party burning software which is not listed in **Appendix B**, to trace burring, disabling the CD/DVDburning functionality based on the registry key located in the device manager in windows operating system supporting this activity is a solution. While the burner application is opened,the VB program searches CD/DVD burn supporting registrykey 4D36E965-E325-11CE-BFC1-08002BE10318 [51]from the device manager and when found disables the Cd/DVD burning functionality and when CD/DVD door is openedit will be enabled back. (See the complete program presented in**Appendix C)**

5.2 Testing the Prototype

In the prototype algorithms to trace users' actions while executing the piracy acts discussed in section 5.2 on the copyrighted content are developed.To test the performance of the prototype in generating actions based on the users' piracy acts, different test cases are designed considering the piracy acts done on the copyrighted digital content and the expected test result and true result are presented in table 5.2.

Table5.1 Test result on the prototype based on the test cases identified using Users'piracy act.

No	Case	Expected result	True result
1	Copying using • keyboard shortcuts • copy function • By drag and drop • Copy Code	A pop up message that shows piracy is tried is displayed and the Cd is ejected.	As expected
2	Burning Using • Known burning/ authoring applications • Pirates' expected burners	A pop up message that shows piracy is tried is displayed and the Cd is ejected.	As expected
3	Sharing using • a peer-to-peer network • FTP File transfer network • Attach the copyright file in an e-mail • Uploading the copyright file in a Web.	A pop up message that shows piracy is tried is displayed and the Cd is ejected.	Hence the algorithm is done and the prototype is left for future work, yet it is not as expected.

5.3 Discussion

This research questions initiated this study basically were to get a means that at least make copying activity on copyright protected digital content difficult. Hence from a technical point of view it would seem theoretically impossible to completely prevent users from making copies of the media they purchase. And the other question is developing copy protection software that doesn't harm legitimate users.

Consideringthese research questions the research aimed to develop pirates' activity detection model that helps to prevent digital copyright. As it is depicted in table 3.3 of section 3.3.3, the test result done on the developed prototype for the tracer model showed that the expected result and the true result while a user perform piracy acts are the same. And from this we can say the goal of the research which was set in the proposal is achieved and the result found is pleasing.

When we evaluate the research we may need to consider certain criteria. The first one is the activities the tracer model can properly trace and generate action of to defend copyright law. There are basically two pirates' activities that the model can defend:

- Reproducing (Copy and Burn)
- Sharing(within a LAN and Web)

Regarding copy, all the copying activities are articulated by the tracer model, the prototype developed shows the tracer model while copying, generates an action to display message and eject CD. Regarding burn, if pirates' burn using known burners/authoring applications the developed model tracedthis activity and generating an action by popping a message and ejecting the CD . And the other issue if the pirates developed third party burner application. For this also the model traces this act and disable the Cd/DVD ROM and enable back at CD eject.Finally for the piracy act sharing for both within the LAN and at the Web, flowchart representing the algorithm to combat this activity is developed but not implemented in the prototype because of resource limitation.

The second one is the influence the model can have on legitimate customers.This can be evaluated whether the Copy protection software create some sort of limitations on users while opening the CD/ DVD. The proposed anti-piracy software doesn't let the user to any sort of problem; the user can copy another text to the clipboard.During burning users shouldejectthe CD/DVD to insert blank CD/DVD.If the CD/DVD with copyrighted digital

content is playing, the users can't open any burner/authoring software. Therefore it is possible to say this research work doesn't hurt legitimate users; hence from the start of the work this was the big intention all actions have been done considering this issues.

The last one is related to users'privacy. Concerning users' privacy even the code is back door. None of the users' information are traced while using the developed anti-piracy software. Therefore users are free from being a victim of their data theft. Hence this work defends copyright law of digital data and never affectsprivacies users.

Chapter six

6. Conclusion, Recommendation and Future Work

6.1 Conclusion

Enjoying the fruit of a labor will make happy and prosperous, for the intellectual owners this can't be realized because of digital world. Pirates' have been taking advantage over the copyright owners and no one stop them. This research work can help copyright owners protecting their work by detecting pirates' activity. The result of this research will help to prevent Pirates'from reproducing and distributing copyrighted contents freely. The solution how to stop pirates' from making their own copies and share it with people is already set out. Now the one which seems impossible to stop pirates is changed to be possible by using this research work. Especially for software and Games that need to be installed for use, the work gives a full solution from piracy acts. For audio music and videos a tape/video recording may cause piracy but still the major problem that worries the music and film industry is computer piracy; so for this industry too it is a great relief to use the developed solution.

6.2 Recommendation

From the literature review section it is understood that there were more research works and application software to stop piracies against copyright, but these security features were analyzed by the pirates and they try to find away by studying the features of the security mechanism to bypass it. Therefore, this anti-piracy software to be useful for the copyright owners it should be kept safe from pirates activities. The possible ways to bypass the anti-piracy software and how to trace the bypassing activity is presented as possible potential risks and risk monitoring and controlling activities.

As Bernd bruegge[50] defines, risk is future uncertain events with a probability of occurrence and a potential for loss. In this thesis work there is a proposed model to detect copyright violation and prototype software is developed. There might be unpredicted risks in

developing and specially implementing the software. Identifying, analyzing and monitoring the possible risk is a mandatory section for the research work.The risk expected to happen in implementing and using the proposed anti-piracy software comes from two angles.

1. From the pirates angle
2. From the intellectual owner angle, the potential end user of the software.

All identified risks are documented in a table 4.5 with the following information:

- Risk ID: Number that identifies the risk
- Description: The description of what the risk is. The Cause or Event statement.
- Potential outcome (Impact): The loss that will happen due to the risk. It is expressed in degree from lower to higher as: Minimal, Moderate, and Significant.
- Recommended Risk Mitigation strategy: strategy to mitigate the risk.

Table 6.1**Risk analysis of the proposed anti-piracy software**

Risk ID	**Description**	**Potential Outcome (Impact)**	**Recommended risk Mitigating strategy**
R01	The pirate may tries to identify the data storage technique of the media to differentiate the copyrighted digital content and the proposed anti-piracy software then tries to get the content alone.	Significant	The proposed anti-piracy software will be hiding inside the copyrighted digital content using steganography tools.
R02	The pirate may use different cracking software/ brute force attack to get the password to unhide the anti-piracy software.	Significant	Make the password strong by increasing the length and the complexity of the password.
R03	Copyright owners may worry that they will not get much Consumers of their work if they put the anti-piracy software, thinking: Consumers may feel inconvenience regarding their privacy.	Moderate	Having awareness session with copyright owners that this proposed anti-piracy software doesn't cost any hurt on legitimate users.

	Consumers may think the software may be incompatible with different platform & operating system. The anti-piracy software doesn't protect their work from illegal copying in think of stopping copying is impossible		

From the table 4.5, the recommendation is that in using such Anti-piracy software, pirates will never accept it and sit idle they will dig a lot to get any hole in order to find the copyrighted digital content alone. Considering pirates', it is recommended to use steganography tools to hide the anti-piracy software inside the copyrighted digital content with a strong password protection for hiding. To mitigate the other risk of being unacceptable by copyright owners' awareness creating sessions are a must.

6.2 Future Work

I. Incorporating other operating systemlike: Linux, UNIX, Mac, Dos will be included in future work. In this research Window Operating system is selected because of the familiarity widely used type of operating system especially for desktop applications.

II. From users' acts that are categorized as genuine, Installing software/game since it needs verification whether the same copy is installed more than one time or not, this will be a future work to grant one machine(number of installation as intended by the copyright owner) installation

III. Algorithm to trace sharing activity is already included in this study but showing the proposed algorithm in a prototype is a future work.

Reference

1. Ignou,S., A. (2009) "Security Threats Due to Software Piracy",a report by the Business Software Alliance .
2. The Linux Information Project (2007), "The Software Piracy Controversy", http://www.linfo.org/software_piracy.html, Retrieved on Nov. 2013.
3. Belousov, A. (2004), "Definition of Computer Piracy, Carrying Out Expert Examination".Computer Crime Research Center.
4. World English Dictionary , http://dictionary.reference.com/browse/copyright , "Copyright", Retrieved on November ,2013
5. Intellectual Property Office , http://www.ipo.gov.uk, "about copyright " Retrieved on October 20, 2013
6. FLA CLM ,(2004). "Limitations and Exceptions to Copyright and Neighboring Rights in the Digital Environment", Netherland.
7. WIPO. (2010). "The importance of copyright in the distribution of films", www.wipo.int/freepublications/en/**copyright**/950/wipo_pub_950.pdf, Retrieved Sept, 2013
8. Terry, M. "Copyright Registration Advantages and Disadvantages", http://smallbusiness.chron.com/copyright-registration-advantages-disadvantages-12029.html , Retrieved on Sep 12, 2013.
9. Kroeck, L. (2012). "What Are the Advantages & Disadvantages of a Longer Copyright Validity Period? Balancing Public Interests with Artist Incentive".
10. United States Code, "Copyright Law of the United States of Americaand Related Laws Contained in Title 17 of the United States Code, Circular 92, Chapter 1 Subject Matter and Scope of Copyright", http://www.copyright.gov/title17/92chap1.html, Retrieved on August. 2013
11. Donaldson, B. "The history of copyright", http://www. Copyrighthistory.com, Retrieved on August 08, 2013.
12. MacQueen, H. L., Charlotte W. and Graeme T. (2007). *Contemporary Intellectual Property: Law and Policy*. Oxford University Press. p. 34. Retrieved on August 12, 2013.
13. World Dictionary, "Definition for digital piracy",http://www.yourdictionary.com, Retrieved Sep 10,2013
14. Farlex," Copyright infringement", www.thefreedictionary.com,Retrieved on 2013-10-10.
15. George, S. (2013) "U.K. Digital Content Piracy Rises Slightly",Holly Wood Reporter
16. Gopal, S., Bahatta C. and Agrawal, W. (2004)."Digital piracy".

17. OZ, S. (1986). “A Strategic Approach to Software Protection”, University of Haifa, Israel and Stockholm School of Computerworld.
18. World Intellectual Property Organization“WIPO Copyright Treaty (WCT)”, http://www.techopedia.com/definition/26952/wipo-copyright-treaty-wct, Retrieved Nov. 2013.
19. Kiya, T. (2012).“Copyright protection in Ethiopia: Shining law, zero effect”, http://addisstandard.com/copyright-protection-in-ethiopia-shining-law-zero-effect/ , Retrieved on Nov, 2013.
20. Videomaker Magazine, (2003). “Copyright: Legal Issues You Need to Know”,http://www.videomaker.com/article/9195-copyright-legal-issues-you-need-to-know, Retrieved on Nov.2013.
21. Esoteric (2008), “Anti-Piracy Security Mechanisms in PC Games”, UW computer security Research and course Blog, https://cubist.cs.washington.edu/Security/2008/01/11/anti-piracy-security-mechanisms-in-pc-games/ Retrieved on Nov. 2013.
22. Dominic, H. (2010)."Copy protection on virtual systems", www.docstoc.com/docs/71510891/Softwarecopyprotection, Retrieved on Jan 2014.
23. Goel, S., Meseing, P. and Chandra. U. (2010), “The impact of illegal peer-to-peer file sharing on the media industry” http://cmr.berkeley.edu/ Retrieved on Jan. 2014.
24. Aladdin Knowledge Systems Ltd, (2009), “safe Word Products Activation”, https://portal.aladdin.com/ Retrieved on Jan, 2014.
25. Goldstein, M. “Product key”,http://en.wikipedia.org/wiki/Product_key#cite_note-1 Retrieved on August 12, 2012.
26. Spiridonov, D. “Digital Rights Management, Digital Entertainment Security Mechanisms”, www.ipvs.uni-stuttgart.de Retrieved on Jan 2014.
27. Schuetz, F. (2006) “Taxonomy of Control Mechanisms”, Alexander Pretschner Information Security, ETH Zurich, Switzerland.
28. Helix Community, (2008), “Helix Device DRM”,Retrived on July 2012.
29. Wolak, M.C, (2001). “Digital Watermarking”, School of Computer and Information Sciences Nova Southeastern University.
30. Mediahedge (20100). “Digital Fingerprinting White Paper”,http://www.mediahedge.com/fileadmin/bestanden/pdf/White_Paper_-_Digital_Fingerprinting_by_Mediahedge_01-2010.pdfRetrieved on August 2012.
31. Beman, S. (2011). “Question on Digital Rights Management or DRM”, http://selfpubauthors.com/2011/01/09/question-on-digital-rights-management-or-drm/, Retrived on Feb. 2014.

32. Kazi, S., (2012)." Hidden Markov Models for Software Piracy Detection", San Jose State University SJSU Scholar Works.
33. Kim,S., Kim, E. and Choi,L. "Method Based Static Software Birthmarks: A New Approach to Derogate Software Piracy", National University of Science and Technology, Islamabad, Pakistan.
34. Choi, J., Han, Y., Cho, S., Park, M., Han, S., You, I. and Song, I. (2013) ."A Survey of Feature Extraction Techniques to Detect the Theft of Windows Applications". In Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), Seventh International Conference on (pp. 723-728). IEEE.
35. Kim, S., Kim, E., & Choi, J. (2012). "A method for detecting illegally copied APK files on the network." In Proceedings of the 2012 ACM Research in Applied Computation Symposium (pp. 253-256). ACM.
36. Wu, X., Zhang, Y., Tang, S., Xia, T., & Li, J. (2008). "A hierarchical scheme for rapid video copy detection." In Applications of Computer Vision, 2008. WACV 2008. IEEE Workshop on (pp. 1-6). IEEE.
37. Kumar, G. S., Manikanta, G., &Srinivas, B. (2013). "A novel framework for video content infringement detection and prevention." In Advances in Computing, Communications and Informatics (ICACCI), 2013 International Conference on (pp. 424-429). IEEE.
38. Goncalves, M., Perera, G., &Rodabaugh, S. (2010). "Detecting illegal file sharing in Peer-to-Peer networks using fuzzy queries." In Fuzzy Systems (FUZZ), 2010 IEEE International Conference on (pp. 1-7). IEEE.
39. Lou, X., & Hwang, K. (2009). "Collusive piracy prevention in P2P content delivery networks." Computers, IEEE Transactions on, 58(7), 970-983
40. Zhang, H., Shi, J., Ye, L., & Du, X. (2013). PPBD: "A piracy preventing system for BT DHT networks." In INFOCOM, 2013 Proceedings IEEE (pp. 1806-1814). IEEE.
41. Nehra, A., Meena, R., Sohu, D., & Rishi, O. P. (2012). "A robust approach to prevent software piracy. " In Engineering and Systems (SCES), 2012 Students Conference on (pp. 1-3). IEEE.
42. Zhang, Y., Jin, L., Ye, X., & Chen, D. (2008). "Software Piracy Prevention: Splitting on Client." In Security Technology, 2008. SECTECH'08. International Conference on (pp. 62-65). IEEE.
43. Anckaert, B., De Sutter, B., & De Bosschere, K. (2004). "Software piracy prevention through diversity. " In Proceedings of the 4th ACM workshop on Digital rights management (pp. 63-71). ACM.
44. NETMARKETSHARE, "Desktop Operating System Market Share"http://www.netmarketshare.com/operating-system-market-share.aspx?qprid=10&qpcustomd=0,Retrieved on Feb , 2014

45. Fridrich, J., Goljan, M., &Soukal, D. (2004, June). Searching for the stego-key. In Electronic Imaging 2004 (pp. 70-82). International Society for Optics and Photonics.
46. Microsoft, "The clipboard", http://msdn.microsoft.com, Retrieved on Dec 02, 2013.
47. Silberschatz, A. (2008)."Operating System Concepts ." Yale University, JOHN WILEY & SONS. INC
48. Microsoft, "Methods for Accessing Data Buffers"; http://msdn.microsoft.com, Retrieved on Feb 20, 2014.
49. Microsoft Community, "Using Buffered I/O", http://msdn.microsoft.com, Retrieved on Feb, 2014.
50. Bernd,B. and Allen H. D. (2004)"*Object-Oriented Software Engineering Using UML", Patterns and Java-(Required)*. Prentice Hall,
51. Microsoft Community, "CD/DVD registry Key",http://answers.microsoft.com/en-us/windows/forum/windows_7-hardware/cddvd-registry-key, Retrieved on Feb, 2014.

```
packagecopypack;
importjava.awt.Toolkit;
importjava.awt.datatransfer.Clipboard;
importjava.awt.datatransfer.DataFlavor;
importjava.io.File;
importjava.io.FileWriter;
importjava.util.regex.Matcher;
importjava.util.regex.Pattern;
importjavax.swing.JOptionPane;

/**
 *
 * @author Kuribachew
 */

public class Copyright

{

public String[] CopiedFile()
             {
              String copied="";

               Clipboard clip = Toolkit.getDefaultToolkit().getSystemClipboard();
DataFlavor[] flavors = clip.getAvailableDataFlavors();
String[] splitcopied=new String[flavors.length];
for (DataFlavor f: flavors)
              {
try
                 {

copied=clip.getData(f).toString();
splitcopied=copied.split(",");

                  }
catch (Exception e1)
                  {
                  }
                 }
return (splitcopied);
              }

public String[] ReadFileFolder(String path)
               {

                File folder = new File(path);
File[] listOfFiles = folder.listFiles();
               String [] fileNames =new String[listOfFiles.length];
for (int i = 0; i <listOfFiles.length; i++)
                       {

if (listOfFiles[i].isFile())
                                  {
fileNames[i]=(listOfFiles[i].getName());
                                   }
else if (listOfFiles[i].isDirectory())
                                 {
fileNames[i]=(listOfFiles[i].getAbsolutePath());
ReadFileFolder(listOfFiles[i].getAbsolutePath());
                                 }
                           }
     return (fileNames);
```

```
                    }


publicbooleancontainsIgnoreCase(  String drivefile, String copied )
                     {
if(drivefile == null || copied == null || copied == null || drivefile .equals(""))
                     {
JOptionPane.showMessageDialog(null, "The drive/clipboard is empty","Pop-Up Message",
JOptionPane.OK_OPTION);
return false;
                     }

               Pattern                                  p                                    =
Pattern.compile(drivefile,Pattern.CASE_INSENSITIVE+Pattern.LITERAL);
               Matcher m = p.matcher(copied);
returnm.find();
                    }

public static void Checkcddrive(String drive)
                {

try {
                        File file = File.createTempFile("realhowto",".vbs");
file.deleteOnExit();
FileWriterfw = new java.io.FileWriter(file);
 String vbs = "Set wmp = CreateObject(\"WMPlayer.OCX\") \n"
                                    +              "Set              cd              =
wmp.cdromCollection.getByDriveSpecifier(\""
                                    + drive + "\") \n"
                                    + "cd.Eject";
fw.write(vbs);
fw.close();
Runtime.getRuntime().exec("wscript " + file.getPath()).waitFor();
                    }
catch(Exception e)
                    {
System.out.println("ERROR"+e);
                    }
                 }

public static void main( String [] args)
                {

                    String cdpath="f:/";
                    File deviceFile = new File(cdpath);
                    Copyright copyobject=new Copyright();
String[] copyfile= copyobject.CopiedFile();
if (copyfile.length>0 )
                   {
if (deviceFile.exists())
                     {
                      String [] drivefile =copyobject.ReadFileFolder(cdpath);
for (int i=0;i<drivefile.length;i++)
                            {
                            String dfile=drivefile[i];
for (int j=0;j<copyfile.length;j++)
                              {
                              String cfile= copyfile[j];
if (copyobject.containsIgnoreCase(dfile, cfile))
                               {
JOptionPane.showMessageDialog(null,  "You  have  violated  the  copyright  rule","Pop-Up
Message", JOptionPane.OK_OPTION);
Copyright.Checkcddrive(cdpath);
                               }

                               }
```

```
                                }

                            }

        }
else
                        {
JOptionPane.showMessageDialog(null,  "The  clipboard  is  empty","Pop-Up  Message",
JOptionPane.OK_OPTION);

                        }
                    }
}
```

Appendix B: Java code used to trace burning using most common burner applications

```
packagecopypack;
importjava.io.BufferedReader;
importjava.io.File;
importjava.io.FileWriter;
importjava.io.IOException;
importjava.io.InputStreamReader;
importjava.util.regex.Matcher;
importjava.util.regex.Pattern;
importjavax.swing.filechooser.FileSystemView;
importjavax.swing.JOptionPane;
/**
 *
 * @author Kuribachew
 */
public class Burner
{
publicbooleancontainsIgnoreCase(  String drivefile, String copied )
        {
   Pattern p = Pattern.compile(drivefile,Pattern.CASE_INSENSITIVE+Pattern.LITERAL);
              Matcher m = p.matcher(copied);
returnm.find();
              }
public static void Ejectcd(String drive)
                {
try {
                   File file = File.createTempFile("realhowto",".vbs");
file.deleteOnExit();
try (FileWriterfw = new java.io.FileWriter(file))
                    {
              String vbs = "Set wmp = CreateObject(\"WMPlayer.OCX\") \n"
                                  + "Set cd = wmp.cdromCollection.getByDriveSpecifier(\""
```

```
                                + drive + "\") \n"
                                + "cd.Eject";
fw.write(vbs);
                    }
Runtime.getRuntime().exec("wscript " + file.getPath()).waitFor();
                    }
catch(IOException | InterruptedException e)
                    {
                   }
                }
public static void main(String[] args) throws IOException {
File[] drives;
FileSystemViewfsv = FileSystemView.getFileSystemView();
drives= File.listRoots();
for(File path:drives)
{
if("CD Drive".equals(fsv.getSystemTypeDescription(path)))
   {
       String cdpath=path.toString();
       String line;
       String pidInfo ="";
String[] burners={"NeroStartSmart,     ImgBurn\n" +
        "    Ashampoo Burning Studio (version 6 only)\n" +
        "    DeepBurner Free\n" +
        "    DVD Decrypter\n" +
        "    DVD Shrink\n" +
        "    DVD Styler\n" +
" Alcohol 120%\n" +
        "Ashampoo Burning Studio\n" +
        "AVS Video Editor\n" +
        "Blindwrite\n" +
        "CDRWIN\n" +
        "CloneCD\n" +
        "CloneDVD\n" +
```

```
        "DeepBurner\n" +
        "DiscJuggler\n" +
        "Easy CD Creator (now obsolete)\n" +
        "Easy Media Creator (now renamed as Roxio Creator)\n" +
        "MagicISO\n" +
        "Nero Burning ROM\n" +
        "Netblender\n" +
        "PowerISO\n" +
        "Ulead/Corel DVD MovieFactory\n" +
        "UltraISO\n" +
        "Winiso \n"+
        ""};
      Process p = Runtime.getRuntime().exec
      (System.getenv("windir") +"\\system32\\"+"tasklist.exe");
try (BufferedReader input = new BufferedReader(new
InputStreamReader(p.getInputStream()))) {
while ((line = input.readLine()) != null) {
pidInfo+=line;
         }    }
     Burner burnobject=new Burner();
for (String burner : burners) {
if (  burnobject.containsIgnoreCase(burner,line)) {
JOptionPane.showMessageDialog(null, "You have violated the copyright rule","Pop-Up
Message", JOptionPane.OK_OPTION);


Burner.Ejectcd(cdpath);
         } else {
         }
     }
   }
}
}
}
```

Appendix C: VB code to enable and disable CD/DVD burning functionality

```
Imports System.Management
Public Class Burner
    Dim blReady As Boolean

Private Sub btnEnable_Click(ByVal sender As System.Object, ByVal e As System.EventArgs)
Handles btnEnable.Click
getCdDrives("Enable")
    End Sub
    Private Sub btnDisable_Click(ByVal sender As System.Object, ByVal e As
System.EventArgs) Handles btnDisable.Click
getCdDrives("Diable")
    End Sub
    Public Function getCdDrives(ByValEnableOrDisable As String) As Boolean
        If InputBox("password") = "password" Then
            Try
                Dim info As System.Management.ManagementObject
                Dim search As System.Management.ManagementObjectSearcher
                Dim deviceGuid As String
                Dim deviceType As String
                Dim cameraIsSeenByWindows As Boolean = False
                Dim showDebugPrompts As Boolean = False
                Dim actualGuid As Guid
             search = New System.Management.ManagementObjectSearcher("SELECT * From
Win32_PnPEntity")
                For Each info In search.Get()
' Go through each device detected.
deviceType = CType(info("DeviceID"), String)
deviceGuid = CType(info("ClassGuid"), String)
                    If deviceGuid = "{4D36E965-E325-11CE-BFC1-08002BE10318}" Then
actualGuid = New Guid(deviceGuid)

blReady = GetDrive(actualGuid).IsReady

                        If AppActivate("burner.exe”) And blReady = True Then
EnableOrDisable = "Disable"
                        Else
EnableOrDisable = "Enable"
                        End If

                        If EnableOrDisable = "Enable" Then
DeviceHelper.SetDeviceEnabled(actualGuid, deviceType, True)
                        Else
DeviceHelper.SetDeviceEnabled(actualGuid, deviceType, False)
                        End If
                    End If
                Next
                If EnableOrDisable = "Enable" Then
btnDisable.Enabled = True
btnEnable.Enabled = False
                Else
btnDisable.Enabled = False
btnEnable.Enabled = True
                End If
            Catch ex As Exception
MsgBox(ex.Message)
            End Try

        End If
    End Function
End Class
```