State-of-the-Art Digital Watermarking Techniques for Content Authentication with a Case Study of eLearning System

Fahd N. Al-Wesabi[1], Kulkarni U. Vasantrao[2]
[1]Department of IT, Faculty of Computing and IT
UST, Sana'a, P.O. Box: 13064, Sana'a, Yemen.
Faculty of Computer Studies
SRTM University, Nanded Maharashtra, India
[2]Department of Comp. Sci. and Engg.
SGGS Institute of Engineering and Techology
Maharashtra, India.
Fwesabi@gmail.com, uvkulkarni@sggs.ac.in

ABSTRACT: *Digital Watermarking (DWM) is a recent technology used to strengthen the security of many applications in different fields. It is a signal which is permanently visible or invisible embedded into digital data called digital cover medium. Content security is one of the fields that are tightly related to digital watermarking. It is usually relevant to the ability of detecting changes in multimedia content, especially in images. However, it remains to examine how applications allow different kinds of users to authenticate e-content and conform its originality, and where the conflicts might be found between the application features and the content authentication. This paper aims to introduce an analytical review for digital watermarking used for authentication in different domains covering state-of-the-art concepts, applications, classifications, and design issues. In this paper, we introduce a new classification for digital watermarking techniques and extract the most important design issues of these techniques depending on our reading in a wide range of digital watermarking literatures. Our new classification for digital watermarking techniques can be considered a contribution of this paper. A recent domain utilizes this technique is eLearning system which is a recent tool that produces a new era of education. It allows student/teacher to learn/teach anywhere at any time. One of the important issues in eLearning environment is content security. The capability to detect changes in eLearning contents has become crucial for many applications in online environment. Thus, we finally present a case study of using digital watermarking techniques for content authentication in eLearning environment taking into account the aspects of our new classification and the design issues extracted for digital watermarking techniques.*

Keywords: Digital Watermarking, Content Authentication, Multimedia Content, eLearning System, DWM Techniques Classification, Design Issues, Soft Computing Tools

Received: 27 May 2012, Revised 12 July 2012, Accepted 20 July 2012

1. Introduction

Currently, there is a massive use of digital contents in most life and business applications either physically or online via Internet such as eCommerce, eLearning, mobile, multimedia, and so many forms of digital information handled on the Internet. On the other hand, there are many challenges encountered by digital information such as security, copyright, content authentication, and owner identification. Digital Watermarking (DWM) is a powerful solution for most of these problems. Digital watermarking is a technology in which various information can be embedded as a watermark in digital content for several applications such as copyright protection, owner identification, content authentication, tamper detection, fingerprinting, access control, and many other applications [1].

There are various techniques that can provide content security. For example, encryption technique provides public or private key in order to encode data.

Site security technique offers firewalls to control the access to digital data. Digital watermarking techniques involve robust features assist preventing illegal attacks [2]. There are many design issues which can be considered in designing systems based on digital watermarking. The most common design issues are security, robustness, capacity, and complexity [1] [6]. The main issue of digital content is content security, especially for online applications. The content security issue in turn includes several aspects such content tampering, authentication, integrity verification, and access authorization [6].

eLearning system is an important application that concerns digital watermarking and its issues. It is referred to as online learning delivered over the World Wide Web (WWW) via the public Internet or private intranet. It is developed as an alternative of the traditional delivery of teaching and learning by electronic service delivery, especially in the sector of higher education. It enables different kinds of users to access different services and materials effectively [3]. There are various issues represent challenges to eLearning environment and its users. Examples of these challenges are the following: what are the main obstacles and opportunities encountered by students when undertaking learning process in an online context? What are the issues of accessibility and usability in eLearning system? How can a student authenticate an online content? How can the administrator or teacher authenticate the originality of an online content? How to resolve the content authentication issues practically? And how to manage the legal legislation of online learning accessibility and content changeability? [4].

Nowadays, most universities and educational institutions use eLearning system to provide their educational materials and services benefiting from the advantages of eLearning system such as the open working hours (24/7 or "*anytime*" feature), and the virtual place of education (Internet space or "*anywhere*" feature). In addition, there are many other advantages such as the use of collaborative tools and support of different styles of learning. However, some eLearning systems do not cover all teaching aspects since they do not usually provide the feature of monitoring and assessing all activities performed by learners. Furthermore, they do not provide the feature of learner's authentication. On the other hand, these systems do not also enable different kinds of learners to authenticate eLearning materials (such as lessons and assignments) and confirm their originality [5] [6] [9] [55].

The significance and motivation of this review paper is that the area is recent and hot. There is a lack in literatures of digital watermarking techniques that collect a wide range and state-of-the-art concepts, applications, classifications, and design issues related to digital watermarking techniques all in one review paper with precise explanation of the effect of application type on the design issue and vise versa. During our reading in literatures of digital watermarking techniques, we feel such lack and then we decided to write up this review paper as an attempt to contribute in reducing that lack.

In addition, this review paper tries to contribute by introducing a new classification for digital watermarking techniques and extracting the most common and important design issues of these techniques depending on our reading in a wide range of digital watermarking literatures are robustness, imperceptibility, security, capacity, complexity, and quality. Furthermore, content security is a most important issue in eLearning environment can effectively utilize these techniques. It concerns to the capability to detect changes in eLearning contents in online environment. Thus, a case study of using digital watermarking techniques has been finally presented in this paper for content authentication in eLearning environment taking into account our new classification and the design issues extracted for digital watermarking techniques.

2. Digital Watermarking Techniques

This section presents a brief overview of digital watermarking concept including its mechanism, history, growing, its applications, and traditional classifications as in literatures. Then, we have introduced our new classification for digital watermarking depending on our literature reading.

2.1 Digital Watermarking Concept and Mechanism

Digital watermarking is an important technology applied to physical objects such as bills, papers, garment labels, and product packing in which physical objects can be watermarked using special dyes and inks or during paper manufacturing. A digital watermarking is a signal which is permanently visible or invisible embedded into digital data called digital cover or host medium. This medium can be audio, image, video, text, or compound medium.

A digital watermark can be detected or extracted later by means of computing operations for the purpose of copyright protection, owner identification, content authentication, tamper detection, data labeling, access control, or other various applications [2]. The information to be embedded in a signal is called a digital watermark and may consist of a various information or meta data such as bit sequence, copyright ownership message, cryptographic keys, biometrics, or content based information. In some contexts, the phrase digital watermark means the difference between the watermarked signal and the cover signal.

The signal where the watermark is to be embedded is called the host signal [8]. The watermarking scheme can be defined as the set of algorithms required for embedding and extraction the watermark [7]. A watermarking mechanism is usually divided into three separate phases that provides a generic approach to watermark any digital media with its related process such as embedding, attacking, and detection as shown in Figure 1. In embedding process, the host and data to be embedded are required as input parameters of an algorithm. In addition, a user key can be required to obtain or produce a watermarked signal. Then the watermarked digital signal is usually stored or transmitted to another person. After that, any modification performed on the signal is considered an attack. While the modification may not be malicious, the term attack appears by copyright protection application, whereas pirates endeavor can remove the digital watermark through modification. Finally, the detection process can be divided into two sub-process, the first one is extracting the watermark by applying special algorithm to the attacked signal to endeavor for extract the watermark from it, this sub-process is called watermark extracting. The second sub-process is to compare the extracted watermark with the original one, this sub-process is called authentication process. The output is Yes or No, depending on the existence of the watermark or not. If the signal is not modified during transmission, then the watermark is still present and it may be extracted and the host signal is authentic, otherwise the host signal is not authentic. [7] [8].

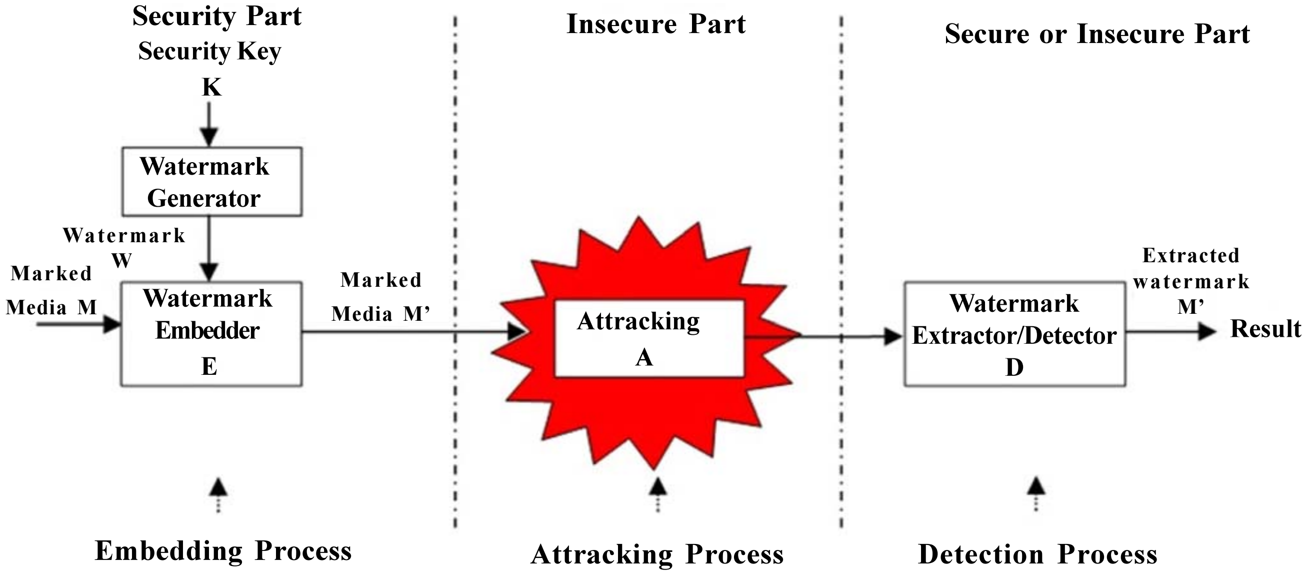


Figure 1. General digital watermark mechanism

2.2 Digital Watermarking History and Growing

The idea of watermarking and hiding data in other media is very old issue. At this time, some techniques such as steganography have been used for practical functions such as mark on the document with invisible secret ink. The basic security of a steganography system is based on a simple procedure because the steganography message is incorporated imperceptibly and covered within other safety sources. Thus, it is very difficult to detect the message without knowing its present and its suitable encoding scheme [9].

Plain watermarking instead is strongly related to the invention of paper making in China as means of guaranteeing quality. After their invention, the water-marking technique extended quickly in America and then in Europe and used in the 18th century for some proposes such as a trademark, quality assessment, dating, and a method against counterfeiting books and money [9] [10].

Regarding the time the term watermark was coined, counterfeiters began developing methods of forging watermarks used to protect paper money. In 1779, Gentle- mans Magazine reported that a man named John Mathison as the first person developed these methods [6]. Regarding the term of digital watermarking, the first example similar to the digital methods nowadays appeared in 1954. The Muzak Corporation filed a patent for watermarking musical work [6]. An identification work was inserted in music by intermittently applying a narrow notch filter centered at 1KH. Such digital watermarking archived by the International Association of Paper Historians and clarifies mainly the historical meaning [10].

In recent years, digital watermarking received considerable attention and has been maturing since an explosion in interest began in the mid 1990's [11]. For some applications, digital watermarking technology has qualified enough to be an interesting tool for developers, along with the development of watermarking techniques, initial application area of content protection was expanded to include authentication, data monitoring, and transmission of value-added services. Up until the early 90's, work in digital watermarking of multimedia was limited to university research labs. And about 1995, interest in digital watermarking began to mushroom. Another example of digital watermarking appeared in 1993 to hide data in images [9]. The first successful commercial venture was Digimarc, founded in 1995 by Geoffrey Rhoads. Digimarc was developing still image watermarking products for the professional photographer to protect against theft.

Around the same time, interest in watermarking had spread to industry research labs including NEC, IBM, and Philips. In 2000, Digimarc started looking at the use of watermarking to create a bridge between the printed page and internet, a theme they continue to press [11]. The most famous watermark can be detected holding a bank note against the light. Later, the digital watermark considers the main principles and practices of its steganographic approach [9]. Nowadays, the initial excitement around digital watermarking becomes a creative new application of a promising technology [11].

2.3 Applications of Digital Watermarking Techniques

Digital watermarking have been broadly and successfully deployed in a wide variety of applications. In this subsection, we examine six proposed or the most common applications that use digital watermarking techniques [6] [7] [9] [10] [12]. We categorize these applications based on the importance in the prevalent real world [7] [9]. The applications have been categorized as the following: content authentication and integrity verification, copyrights protection, signatures, fingerprinting, broadcast monitoring, and data labeling. For each one of these applications, we try to describe in brief how the technology works, and identify what characteristics of the problem make watermarking a suitable solution.

2.3.1 Content Authentication and Integrity Verification

Applications of this type are related to issue of digital content to assure if it is authentic or not. Water-mark consists of information that assists in determining the authentication of content. If the watermark can be extracted and matched to the information representing authenticity of the content, it serves the purpose of content authentication by assuring to the user that the content has not been altered during its passage through a noisy or non-secure communication channel [7]. Digital watermark contains data that can be used later to determine that the contents has been changed or not. Thus, any operation performed on the document will affect or destroy the integrated watermark. If the watermark data can be extracted correctly, the authenticity can be achieved [9].

2.3.2 Copyrights Protection

Copyright protection is one of the main applications that the digital watermarks are often being used for it. Thus, authors can integrate a watermark contains information about the rules of usage and copyright owner- ship or intellectual property signature into the original digital document which the content owner wishes to en- force and distribute it normally. In this case, they can proof their intellectual creation later for a legal proceeding and have the possibility to emphasize claim to the restricted use [9] [7]. The content can utilize devices or some applications that can participate the content that might look for the watermark, extract it, and compare it to original watermark. Example of this utilization is that when the content is on a recordable storage device, we need to identify unlawful copies and disallow to play the content [7].

2.3.3 Signatures

The main usage of a signature with a watermarking techniques is to identify the owner of the content, and to help settle ownership disputes. The signature can be usually used as a fingerprint to identify content consumers [7] [9].

2.3.4 Fingerprinting

Fingerprinting is one of biometric technology that works by extracting attributes of content and storing them in a database as a template and use it later to compare it to new extracted pattern [9]. Fingerprinting can be combined with watermarking techniques to work in security applications in order to restrict unauthorized users when a specific media or digital content is distributed to multiple users. In this case, different watermarks are embedded within the content in which each user is specified by specific watermark. In case the watermarked media is leaked out to unauthorized user, the content is examined for a single watermark to identify the source of leak [7].

2.3.5 Broadcast Monitoring

Broadcast monitoring describes the area of automated systems which automatically monitors distribution channels to track the appearance of distributed material. This technology is usually used by some commercial systems [9]. To monitor the track of distributed digital contents, the content usually requires assistant applications to embed transaction identifiers such as watermark embedding into the content. Transaction identifier is provided as transaction logs and can be detected by automated systems to perform some monitoring operations such as keeping track of when, how, and where the content appears or is being used. This application can use in some areas as monitor television and radio broadcasts, computer networks, and any other distribution channels [7].

2.3.6 Data Labeling

The basic role of digital watermarking techniques in this application is content labeling by embedding different data into a watermark to notify the content consumers for different purposes of usage the same contents [7].

3. Our Classification of Digital Watermarking Techniques

Digital watermarking techniques have been classified by many literatures based on several features and properties that depend on various view points. We have examined briefly some traditional classifications of digital watermarking as in literatures. Some of them have classified digital watermarking techniques based on the basis of their requirements such as robustness, non-perceptibility, non-detectable, security, complexity, and capacity [9]. Other literatures have classified digital watermarking techniques based on scheme such as perceptibility, robustness, embedding method, and retrieval method [7].

A novel aspect of this review paper is that we have classified the digital watermarking techniques into new four paradigms. This classification is figured out based on the most significant aspects and properties of digital watermarking in the most prevalent real world. The four paradigms of our classification are classification based on scheme, classification based on content type, classification based on digital watermarking applications, and finally classification based on the techniques combined with digital watermarking. Figure 2 illustrate our classification of watermarking techniques.

3.1 Classification Based on Scheme

The watermarking scheme represents the core of watermarking systems as the set of algorithms required for insertion and extraction the watermark into or from the host media [7]. We have chosen the scheme as a main category of digital watermarking techniques due to its effect and significance to distinguish between alternatives of watermarking algorithms. There are many parameters that the scheme depends on to determine which watermarking algorithm can be used such as the type of information that can be embedded as a watermark, the place in the host media that the watermark can be embedded, the technique that can be used to embed and extract the watermark data into or from the host media, the way to do the embedding and extracting, and the appropriate capacity of information bits that can be embedded as a watermark. Thus, Watermarking scheme can be classified into four subcategories: scheme according to visibility, scheme according to aims, scheme according to embedding domain, and scheme according to extraction method.

3.1.1 Scheme According to Visibility

In this scheme, the application scenario of a particular digital content determines whether a watermark should be visible or invisible based on the application nature. A visible watermarking refers to the watermark embedded into the digital content which is visual by users. There are three main attributes of this type of watermarking which are first, it is most commonly used for ownership identification and informing users that the content is authentic or not, second it may be a text or a logo, and finally it is easy to remove. On the other hand, invisible watermarking refers to the watermark embedded into the digital content which is not visual by users or invisible due to slight modification on the host signal. The main attributes of this type are that it is typically used for proof of ownership, content labeling, and in validation of intended recipient. Another attribute is that it is difficult to remove [7]. Examples of this scheme are the approaches that have been developed in [13], [14], and [15].

3.1.2 Scheme According to Aims

This scheme defines the strength of the watermark to defend against attacks based on three properties. The first property is the Robustness which refers to the watermark that can resist against different kinds of attacks such as modify and delete attacks. The second property is Fragile which refers to the watermark that is invalidated by slightest modification of the host media. The final property is Semi-Fragile which refers to the watermark that is only destroyed by major changes to the host media [7]. Examples of this scheme are the approaches that have been developed in [16], [17], [18], and [19].

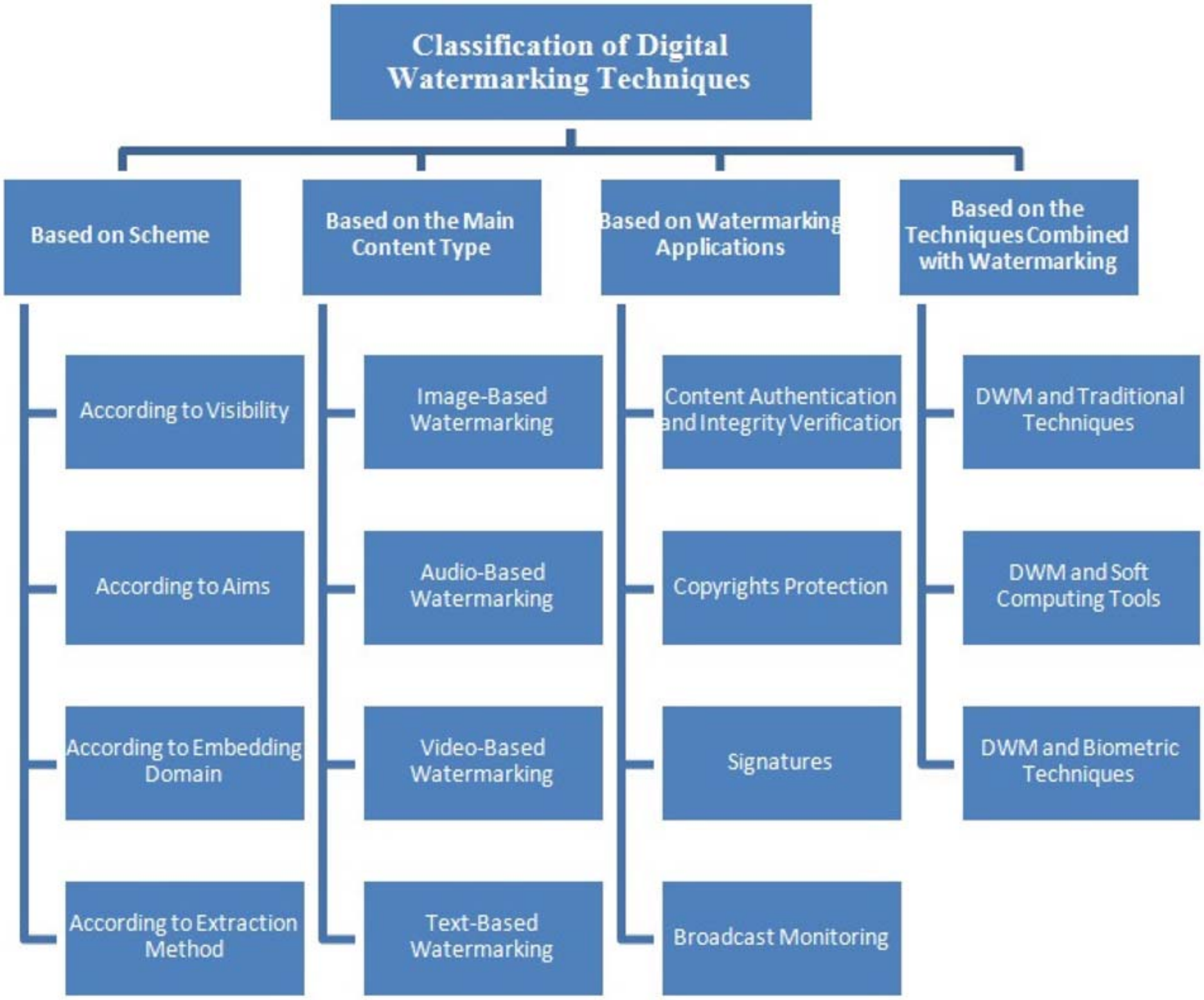

Classification of Digital Watermarking Techniques
Based on Scheme
Based on the Main Content Type
Based on Watermarking Applications
Based on the Techniques Combined with Watermarking
According to Visibility
According to Aims
According to Embedding Domain
According to Extraction Method
Image-Based Watermarking
Audio-Based Watermarking
Video-Based Watermarking
Text-Based Watermarking
Content Authentication and Integrity Verification
Copyrights Protection
Signatures
Broadcast Monitoring
DWM and Traditional Techniques
DWM and Soft Computing Tools
DWM and Biometric Techniques

Figure 2. Our classification of digital watermarking techniques

3.1.3 Scheme According to Embedding Domain

This scheme represents an important property for classification of watermarking schemes by which we can determine the method that can be used for embedding the watermark data into the host media. In addition, this scheme determines the main properties that may affect on it such as embedded effectiveness, fidelity, and capacity. Every host media has different categories that the embedding processes can be classified based on it such as video, audio, images. Also, every host media has watermarking domain such as spatial or transform domain or both [7]. Examples of this scheme are the approach which has been developed for text media in [20], the approach which has been developed for 3D media in [16], and the approaches that have been developed for Video media in [17] and [18].

3.1.4 Scheme According to Extraction Method

This scheme represents another important property for classification of watermarking schemes by which we can determine the method that can be used for extraction or detection a watermark based on the information required to retrieval process, this method can be one of three methods. The first method is called informed method and sometimes is called non-blind method. The idea behind this method is that it depends on retrieval process which requires access to both the original media and the embedded piece of data. The second method is Semi-blind method in which the detector does not require any access to the original media but requires some of original information and/or the watermark itself. The final method is Blind method in which the embedded watermark can be extracted without referring to the original media [7]. Examples of this scheme are the approaches that have been developed using Blind method in [21] and [22], the approach which has been developed using non-blind method in [23], and approach using semi-blind which has been developed in [24].

3.2 Classification Based on the Main Content Type

Digital watermarking techniques can be applied in different types of digital media. The significance of this category is that each type of these media requires different requirements, properties, and methods to perform digital watermarking process. Thus, there are four common types of watermarked media that can be classified: image-based watermarking, audio-based watermarking, video-based watermarking, and text-based watermarking [9]. We have examined briefly each sub-category and described it bellow based on the literatures interesting to each category. A close order has been addressed in the categorization adopted by [26].

3.2.1 Image-Based Watermarking

Most of watermarking literatures have focused on image watermarking for many purposes and applications such as copyright protection, content protection and authentication, and tampering detection. Watermarks can be embedded into images by various mechanisms such as modifying their values and transform domain coefficients. Images can be represented in spatial domain and transform domain. The transform domain image is represented by its frequencies but in spatial domain image represented by pixels [25]. There are three main requirements needed to apply digital watermarking technology to images which are transparency, robustness, and capacity [25]. There are many techniques can be used for digital image watermarking such as Least Significant Bit, Correlation, Frequency Domain, Wavelet Watermarking, and Spread Spectrum Techniques. Examples of these techniques have been used in [21], [30], and [31].

Several executive tools found also that have capability to work with most popular image formats such as jpeg, bmp, tiff, png, gif, etc. [26]. Examples of these tools are Easy Watermark Creator which has been con- ducted by [27], Watermark It which has been conducted by [29] which are able to hide watermark as text beside image, and finally Mytoolsoft Watermark Software which has been conducted by [28].

3.2.2 Audio-Based Watermarking

Digital audio watermarking is a technique for embedding Meta data along with audio signal. Embedded data is used for some purposes such as ownership protection, proof of ownership, authentication and tampering detection. Several audio watermarking techniques have been proposed and used in different ways in order to embed a robust watermark and to maintain the original audio signal fidelity. These techniques include Low-Bit Coding Phase Coding, Direct Sequence Spread Spectrum, Frequency Hopped Spread Spectrum, and Echo Coding [9].

Audio watermarking algorithms can be characterized by six main properties which are perceptual transparency, watermark bit rate, robustness in the presence of attacks, type of watermark detection (blind/informed), security, and computational complexity [9]. Examples of audio watermarking techniques are the approaches that have been used in [32], [33], and [34]. Other examples of some executive tools of digital audio watermarking are that have been developed with capability to work with most audio formats such as WAV, MP3, PCM, and WMA. These tools have been conducted by [35], [36], and [37].

3.2.3 Video-Based Watermarking

Video Watermarking is one of the most popular techniques currently used among the watermarking techniques for many purposes and applications such as security related to copy control, fingerprinting, ownership identification, authentication, and tamper resistance, [38]. Many video watermarking techniques have been proposed and classified based on working domain to pixel domain and transform domain techniques. In pixel domain, the watermark is embedded in the source video by replacement simple addition bits of selected pixel positions.

In transform domain, the host signal is transformed into a different domain and watermark is embedded in selective coefficients [38]. Examples of video watermarking techniques are the approaches that have been used in [17], [18], and [39]. Examples of some executive tools of digital video watermarking are the tools that have been conducted by [40], [41], [42], [43], and [44].

3.2.4 Text-Based Watermarking

Text watermarking is an important area of research. However, the literatures in digital text watermarking is quite scarce and can be classified in the three main categories which are an image based approach, a syntactic approach, and a semantic approach [45]. Text watermarking algorithms are dependent on some properties such as text size, text language, rules, grammar, conventions, and writing styles [45].

Examples of text watermarking techniques are the approaches that have been developed for watermark text document with image-based technique using text-image such as in [46], the approach that has been developed using line-shift algorithm in [47], the approach that has been developed based on word classification and inter-word space statistics in [48], and the approach that has been developed by justified paragraphs and irregular line spacing in [49].

Examples of approaches that have been developed for syntactic technique are the natural language watermarking schemes using the syntactic structure of text such as approach that has been developed by [50], and the approach that has been develope by perform the morpho syntactic alterations on the text in [51]. Finally, examples of approaches that have been developed for semantic techniques are the synonym substitution method that has been proposed in which watermark is embedded by replacing certain words with their synonyms without changing the context of text [52]. Other approaches that have been proposed are firstly noun- verb based on exploits nouns and verbs in a sentence parsed with a grammar parser using semantic networks [53], and secondly the algorithm that has been proposed based on Text Meaning Representation (TMR) strings [54].

3.3 Classification Based on Watermarking Applications

There are many recent digital watermarking techniques that have been considered as application oriented and can be classified into six applications as mentioned in subsection 2.3. Some literatures have begun to examine digital watermarking techniques for various applications in different environments. Examples of using digital watermarking in different applications reviewed by this paper are the approaches that have been proposed in [55], [57], and [58]. These approaches are used for authentication and integrity verification of contents in online environments and digital means. Other copyright protection approaches that have been proposed in [56] and [59]. These approaches are used for content owner identification and verification. Other signature approaches that have been proposed in [61], [62] and [63] which are basically used as watermarks to help settle ownership dispute, identifies the owner of the content, and content authentications. Fingerprint approach has been presented in [60] which used to detect the owner of digital content and security applications. Examples of broadcast monitoring is the approach that has been proposed in [64] which is used to evaluate quality of video tracks, and the approach that has been presented in [65] which is used to add service to radio broadcast music for mobile commerce.

3.4 Classification Based on the Techniques Combined with Watermarking

Digital watermarking techniques can be combined with other techniques to improve its performance based on the application nature. The significance of this category examines the techniques that can be combined with digital watermarking, its applications, strength, and effects. Thus, depending on the literatures which are reviewed in this paper, we can classify it into three sub-categories that are digital watermarking and traditional techniques, digital watermarking and Soft Computing Tools (Artificial Intelligence based), and digital watermarking and biometric techniques.

3.4.1 Digital Watermarking and Traditional Techniques

Many of literatures have been examined and several approaches have been proposed depending on combined digital watermarking as more recent technology along with various traditional techniques such as encryption, checksums, and hash-functions. Examples of these techniques reviewed by this paper is the approach that has been proposed in [66] which use both cryptography and digital watermarking techniques in digital right management model to encrypt digital media with improving the performance, detection copyright of digital media, copyright control and tracking illegal distribution. In [67], a combined method has been proposed using Discrete Wavelet Transformation (DWT), Selected Least Significant Bit (SLSB), and Visual Cryptography (VC) to hide an iris image and a secret message related to the iris stored. The experiment results of this combined techniques show that the recognition rate after dewatermarking is high and resistant to several attacks but the performance slightly decreases with the affine transformation.

In [56], a new method has been presented to resolve copyright problem in eLearning content by inserting a digital logo image as a watermark signals in the audio stream of eLearning material. The proposed method dependents on a combined Modulated Complex Lapped Transform (MCLT) model for watermark embedding and Independent Component Analysis algorithm to watermark extracting. The results show quite good visual and audible quality in watermarked content, as well as a high robustness against common signal processing attacks.

3.4.2 Digital Watermarking and Soft Computing Tools

A more powerful digital watermarking system can be modeled and developed using a combination of digital watermarking along with recent soft computing tools or called artificial intelligent algorithms such as genetic algorithm, neural networks, and fuzzy logic, that based on digital multimedia characteristics and application nature. Although, the main literatures reviewed by this paper focused on improving the system performance, security, and quality.

Examples of these combined techniques are approach which has been proposed in [68] which conduct authentication methods based on combined digital watermarking along with neural networks technique in order to improve authentication process on digital images and video, and to detect if there is a modified malicious tampering on multimedia content. Results of the proposed method show the method's practicality, robust- ness, and efficiency. On the other hand, this method can be applied only to image media.

In [69], a new watermarking method has been proposed so that it combined with genetic algorithm (GA) aimed to adapt high payload watermarking in spatial domain. GA is embedded to find the host region in the cover image for secret image blocks with decreasing effect on visual quality and imperceptibility of the cover image and secret image respectively. In [70], a new watermarking approach has been proposed for audio signal based on genetic algorithm. The main advantages of this approach are determining the optimal localization and intensity of watermark. It is robust against watermarking attacks because GA is used to evaluate selection of the embedding regions. In addition, it improves quality of watermarked image with the aid of GA.

3.4.3 Digital Watermarking and Biometric Techniques

Powerful digital watermarking systems can be modeled and developed using a combination of digital watermarking along with recent biometric techniques such as Iris, Voice, and Signature based on human characteristics and application nature. Although the main literatures reviewed by this paper focused on improving the system performance, robustness, and reliability. In [58], an authentication scheme has been proposed for a DRM system based on integrating a watermarking and a multimodal biometric technique to improve the security and reliability of personal recognition. In the watermarking algorithm, image of face can be selected to be the host image and the iris feature which can be selected to be used as a watermark hidden data in the host image.

In [62], an offline handwritten signature has been used as a watermark for the host image to authenticate the claimed source of the digital image. In [63], the authentication framework has been proposed using Compensated Signature Embedding (CSE) aimed to develop an image authentication system to detect the originality and quality of online multimedia contents. The results of performance evaluation show a successful authentication over a range of robustness. On the other hand, the proposed framework is limited to image multimedia authentication.

In [71], an approach has been proposed to protect the ownership by hiding an iris data into the content digital image for an authentication and ownership identification purposes. In [72], authors have presented a biometric image watermarking method to improve recognition accuracy of face and fingerprint biometric images in addition to protecting these images from tampering. In [73], a handwriting biometric trait has been embedded as a watermark in the form of signatures, pass phrases, and sketches for the purposes of user authentication, ownership identification, and verification of digital content.

4. Design Issues of Digital Watermarking in Content Authentication

This section emphasizes on the most significant design issues of digital watermarking applications, the main concerns addressed by the current literature are Robustness, Security, Imperceptibility, Capacity, Complexity, and Quality [74] [75] [76] [77].

4.1 Digital Watermarking and Security

The security concern of digital watermarking systems assumes that the attacker has full knowledge about the applied watermark procedures. Therefore, an attacker will try to manipulate data in order to destroy the watermark in the content, or sometimes scan to triumph the original multimedia object without a copyright protection note. Non-inevitability of a watermarking system is also one of the important security issues [82].

Different security issues and mechanisms presented in this subsection are mentioned in several literatures reviewed by this paper. In [82], a proposed method has been examined to break the system and perform the collusion attacks by embedding different watermarks to the watermarked data using different keys rather than the original one. In [82], the attackers are also able to estimate the original watermark and to remove it.

In [83], a model of key dependent has been proposed to protect a watermark from attacks. The proposed model improves resistance to attacks by inserting the watermark information into a secret transform domain. In [84] and [85], authors have tried to improve the security of a watermarking algorithm without impacting on watermark robustness. This is done by introducing wavelet filter parameterization for use in the transform domain by the watermarking algorithm. The idea based on protecting the locations of embedded watermark information by keeping the key of WPF secret and using it later as filter to generate and extract the watermark. The experimental results show some robustness reduction when using WPF, however it is not enough to prevent the watermark from being extracted.

In [86], [87], [88], and [89], some approaches recommended providing the security of digital watermarking embedding and extracting mechanisms. The first approach has been proposed to encrypt data in order to be embedded using a secure cipher such as AES and RSA. The second approach aimed to provide security in order to feature extraction such as deriving features through projecting a set of templates/coefficients along a direction specified by a key. The third approach aimed to add security in order to the embed mechanism itself to make it difficult for an adversary embedding any additional bit to watermarked data. Since the first and second approaches involved multiple samples or coefficients, they cannot always allow the localization of tampered regions to fine scale, which is a desirable feature for authentication.

4.2 Digital Watermarking and Robustness

The watermark must be difficult to be removed from the object. So, watermark robustness is typically one of the main issues in the design of any watermarking scheme that should be considered against standard data processing and malicious attacks. Different robustness issues and mechanisms are shown in the literatures reviewed by this paper. In [79], an image watermarking approach has been proposed as a robust approach to geometrical and waveform attacks. This approach primarily based on Radon Transform, which could transform iteration into cyclical shift and supply invariance to scaling. Authors in [79] concluded that the selection of invariant centroid is important. It could promise the robustness of invariant centroid under a variety of attacks.

In [80], a new scheme has been proposed aiming to be adaptive and consider the normal attributes of the host image blocks for providing security issue without impacting on the robustness of the watermark. In [81], a mechanism has been proposed for maximum robustness watermarks in which signal should be embedded adaptively into the same spectral components that the host data already populate. As shown by [81], these are typically the low frequencies for images and videos. In [93], a novel text watermarking scheme has been proposed with good robustness for word document that is based on embedding the secret signals in the particular attributes of word object. The idea is to encrypt the watermarking information, then divide it into some groups, and pack them into a message before embedding it into the word document.

However, the robustness of watermarking methods can be recognized in different levels based on the application requirements. In authentication applications, watermarks have to defend against certain attacks. Thus, authentication watermarks require low level of robustness. Data monitoring and tracking applications require a high level of robustness. Fingerprinting applications require a very high level of robustness to resist data processing and malicious attacks. Finally, watermarking for copyright protection requires the highest level of robustness and is used to resolution equitable ownership [78].

4.3 Digital Watermarking and Perceptibility

Perceptibility issue refers to whether watermark is visible or invisible to human sensor organ. Perceptible watermarks are visible to human while imperceptible are not [91]. Different perceptibility and imperceptibility issues and mechanisms are shown in the literatures reviewed by this paper. In [90] and [91], a new imperceptible wavelet-based watermarking scheme has been pro- posed to find transparent degree of other bands based on the one low pass band which is referred to by the authors as LL, in addition to determining transparent degree of three high-pass bands (horizontal HL3,vertical LH3). Then, the watermark is embedded into those degrees. The proposed method can extract the watermark with or without resorting to the original host image. The experimental results show that the proposed scheme can resist most common attacks, and the watermarked image is highly imperceptible.

In [92], an automatic evaluation method has been presented for image imperceptibility. The idea of the proposed method is the pixel distribution of the differential images between original and watermarked images which are calculated to construct some relative sequences. During analyzing the ultimate pixels distribution, a reference sequence is produced. Then, an overall imperceptibility index is achieved through the grey relational degrees between the two kinds of sequences. Results of evaluation show that not only agree with human visual system, but also basically consist with theoretical analysis. It is necessary to use a perceptibility measure of some sort to ensure imperceptibility of the modification caused by watermark embedding. This can be implicit or explicit, original data adaptive or fixed. As importance of the required imperceptibility, it can modify the individual samples that are used for watermark embedding by an amount relatively small to their average amplitude [78].

4.4 Digital Watermarking and Complexity

Complexity in digital watermarking techniques describes the effort and time needed to embed and recover the watermark information for attacks to be avoided [9]. As importance, the complexity issue is also connected with the security issue of digital watermarking systems. The complexity issue is less important than the other issues of digital watermarking techniques, however the more complex methods seem to embed the watermarks with higher robustness [78]. Thus, it is recommended to design the watermarking procedure and algorithm as complex as possible [97]. There are different recommendations presented in some literatures reviewed by this paper for complexity issue depending on watermarking systems.

In real time applications, the complexity of watermarking systems is relatively low and does not grow with system volume, however fingerprinting systems increase in complexity as the system grows in ways that are difficult to anticipate and have not been investigated in any depth [9]. Many applications even prohibitively complex, complexity in general is a much more importance issue for video watermarking applications than for image watermarking applications [78].

4.5 Digital Watermarking and Capacity

Capacity or payload size refers to the amount of information that can be stored in a data source [9]. Thus, it is an important property that should be considered in the design of a digital watermarking system. Most of literatures reviewed by this paper presented different capacity methods based on multimedia contents and digital watermarking applications. In [94], authors examined the capacity issue under the assumption that attacks can be modeled as additive noise. The authors examination has been depended on embedding a watermark process related to a storing bits in specific devices, and computing the storage capacity of these devices, then, presenting a specific design of a modulator to store information in those devices.

In [95], alternative methods have been proposed to recover the watermark from geometrically distorted image without using the original data. The first method is to preset a part of the watermark to some known values and to use them for spatial resynchronization. This approach decreases the hiding capacity of the useful information, and is also repute very expensive. The second method is to use self reference systems that embed the watermark sometimes at the shifted locations. In [96], a system has been described with a watermark bit rate of 100 kbps, which does not cause distortion of the host audio sequence and it is able to perfectly extract the hidden bits at a signal-to-noise ratio of 15 dB. Authors of [9] and [96] have concluded that depending on the multimedia type, amount of capacity always may be measured in bits for text media, or bits/second/sample for audio, video, and video images media. On the other hand, and depending on watermarking applications, the capacity of one bit to be sufficient in using digital watermarking for simple copy control applications. The have concluded also that the ownership protection and fingerprinting applications require small embedding capacity of the system, because the number of bits that can be embedded and extracted with small probability of error does not have to be large. However, high capacity is required for authentication and tampering applications [9].

Thus, based on all the above, we can differentiate between three classes of digital watermarking systems which are digital watermarking systems with fixed capacity, digital watermarking systems with variable capacity, and digital watermarking systems with size- based capacity which is determined by the embedder. On the other hand and by our reading in literatures, the capacity issue is related to some design issues of digital watermarking system such as robustness, visibility, and complexity more than the other issues.

5. Case Study: A Digital Watermarking for Content Authentication in eLearning Systems

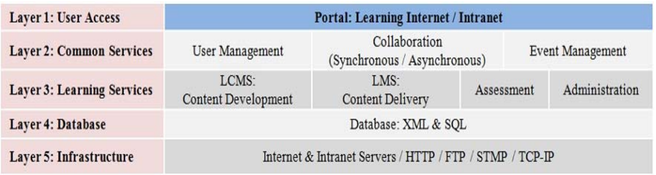
This section presents a brief overview of eLearning systems, including its concept, environment, elements, services, and its components. Then we have introduced a case study on its environment by using digital watermarking for content authentication depending on our reading of the literatures including requirements, design issues, and techniques can be combined with digital watermarking.

5.1 eLearning System Concepts and Environment

5.1.1 eLearning Overview and Infrastructure

eLearning is the idiom used to describe the use of the modern Web and other Internet technologies that aim at improving the teaching and learning experience [98]. It developed as an alternative of the traditional delivery of teaching and learning and it well enable different kind of users to access more services and materials. eLearning system has similar characteristics as several other eApplications such as eCommerce, eBanking and eGovernment.

Nowadays, there are three combination methods of using technology to development of eLearning systems. The first method is using technology asynchronously. In this case, it is only as assistant tool used to enhance a traditional face-to-face learning. The second method is using technology asynchronously and synchronously as assistant tool to enhance a traditional face-to-face learning. The last method is using technology asynchronously and synchronously to deliver a learning material as all online [98]. There are many frameworks have been proposed to work in an eLearning environment, the importance issue to design eLearning architecture must be oriented to eLearning standardization. Figure 3 illustrates the typical logical framework of an eLearning environment [99].



Layer 1: User Access	Portal: Learning Internet / Intranet			
Layer 2: Common Services	User Management	Collaboration (Synchronous / Asynchronous)	Event Management	
Layer 3: Learning Services	LCMS: Content Development	LMS: Content Delivery	Assessment	Administration
Layer 4: Database	Database: XML & SQL			
Layer 5: Infrastructure	Internet & Intranet Servers / HTTP / FTP / STMP / TCP-IP			

Figure 3. eLearning system framework

In this paper, we focus on Layer 3 of Figure 3 namely learning services which involve elements that represent the area which is applied by our case study to examine analytical review of security requirements that facing the challenges addressed in developing the main elements of eLearning system.

5.1.2 eLearning Components and Services

eLearning architecture is usually layered and block-based for easy control and system build, and it must be able to integrate between key components and services. The framework shown in Figure 3 has been modeled as a 5-layer model based on components and services nature as the following:

– Layer 1: User Access: this layer represents the single entry of different kinds of users to access the deeper levels of the portal site in order to participate in eLearning services which is restricted by a login via a standard Web browser.

– Layer 2: Common Services: this layer contains three main components to provide services needed by every user, which are user management, collaboration, and event management. The user management component records and handles all information of different kinds of users. There are many activities of user management such as identifies, tracks and assigns privileges, and conducts the authentication process. Collaboration component provides synchronous or asynchronous communication among all users using virtual classroom, chat, email, white-board resources, instant messaging. Event management component provides some tools such as calendar, scheduling, reminders to learners assistant to view course offerings events.

– Layer 3: Learning Service: this layer contains the core components of eLearning system that provide core functionality for the production and consumption of eLearning resources. These components are LCMS, LMS, assessment, and administration. LCMS component allows author, content experts, reviewers, and administrators. The objectives of these components are to control the backend of learning materials and submit content into the repository for subsequent review, editing and final approval. LMS component allows catalogue review, course selection, enrollment, student tracking, e-commerce automation, and launching the online content. Assessment component allows author/instructors with resources to generate quizzes and tests. Administration component allows backend management of curriculum, resources, instructors, and learners.

– Layer 4: Databases: this layer allows relational databases typically using SQL to be interconnected with new XML database technology.

– Layer 5: Infrastructure: this layer establishes client/server network and physical hardware utilizing standard Internet technologyprotocols as Internet and Intranet servers, HTTP, FTP, TCP/IP, and SMTP [99].

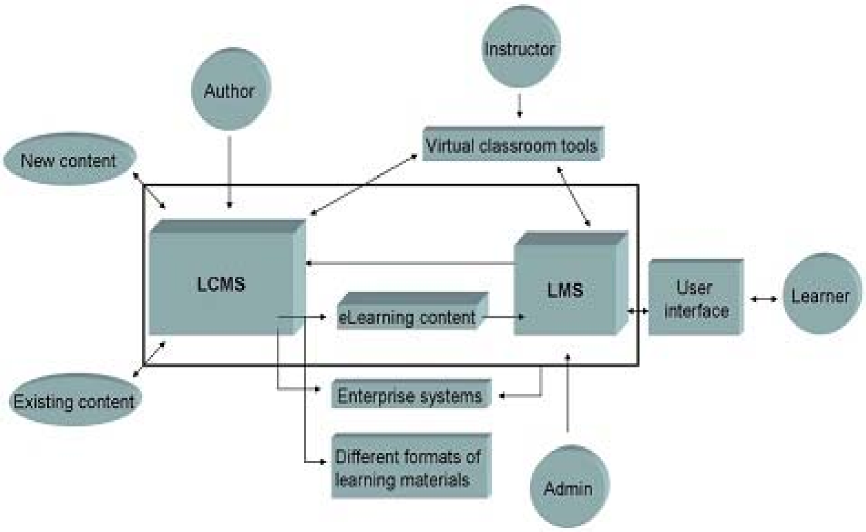
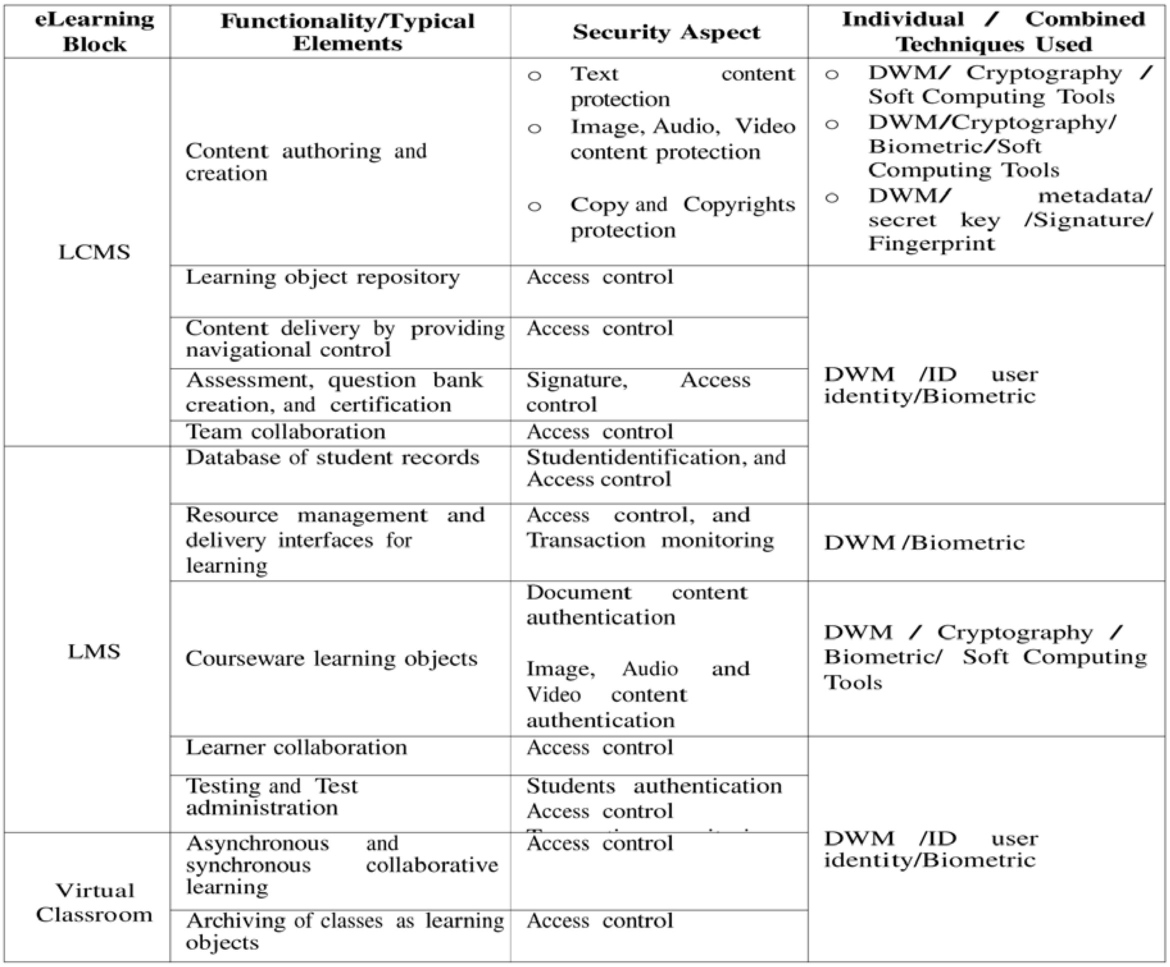


Figure 4. Connection between eLearning elements

eLearning Block	Functionality/Typical Elements	User Nature	Security Aspect
LCMS	Content authoring and creation	Authors Content experts, Reviewers Instructors, and Admin	○ Text content protection ○ Image, Audio and Video content protection ○ Copy and copyrights protection
	Learning object repository	instructors and admin	Access control
	Content delivery by providing navigational control	instructors and admin	
	Assessment, question bank creation, and certification	Authors, Instructors, and admin	Signature, Access control
	Team collaboration	Authors, contentexperts, reviewers, and instructors	Access control
LMS	Database of student records	Students, and admin	Student identification, and Access control
	Resource management and delivery interfaces for learning	Admin, and instructors	Access control, and Transaction monitoring
	Courseware learning objects	Students	Document content authentication, and Image, Audio, Video content authentication
	Learner collaboration	Instructors, and Students	Access control
	Testing and Test administration	Instructors, and Students	Studentsauthentication, Access control, Transaction monitoring
Virtual Classroom	Asynchronous and synchronouscollaborative learning	Instructors, and Students	Access control
	Archiving of classes as learning objects	Instructors, and Students	

Table 1. Analysis security requirements of eLearning elements



eLearning Block	Functionality/Typical Elements	Security Aspect	Individual / Combined Techniques Used
LCMS	Content authoring and creation	○ Text content protection ○ Image, Audio, Video content protection ○ Copy and Copyrights protection	○ DWM/ Cryptography / Soft Computing Tools ○ DWM/Cryptography/ Biometric/Soft Computing Tools ○ DWM/ metadata/ secret key /Signature/ Fingerprint
	Learning object repository	Access control	DWM /ID user identity/Biometric
	Content delivery by providing navigational control	Access control	
	Assessment, question bank creation, and certification	Signature, Access control	
	Team collaboration	Access control	
LMS	Database of student records	Studentidentification, and Access control	
	Resource management and delivery interfaces for learning	Access control, and Transaction monitoring	DWM /Biometric
	Courseware learning objects	Document content authentication Image, Audio and Video content authentication	DWM / Cryptography / Biometric/ Soft Computing Tools
	Learner collaboration	Access control	DWM /ID user identity/Biometric
	Testing and Test administration	Students authentication Access control	
Virtual Classroom	Asynchronous and synchronous collaborative learning	Access control	
	Archiving of classes as learning objects	Access control	

Table 2. Individual or combined common techniques used for improve security in eLearning system

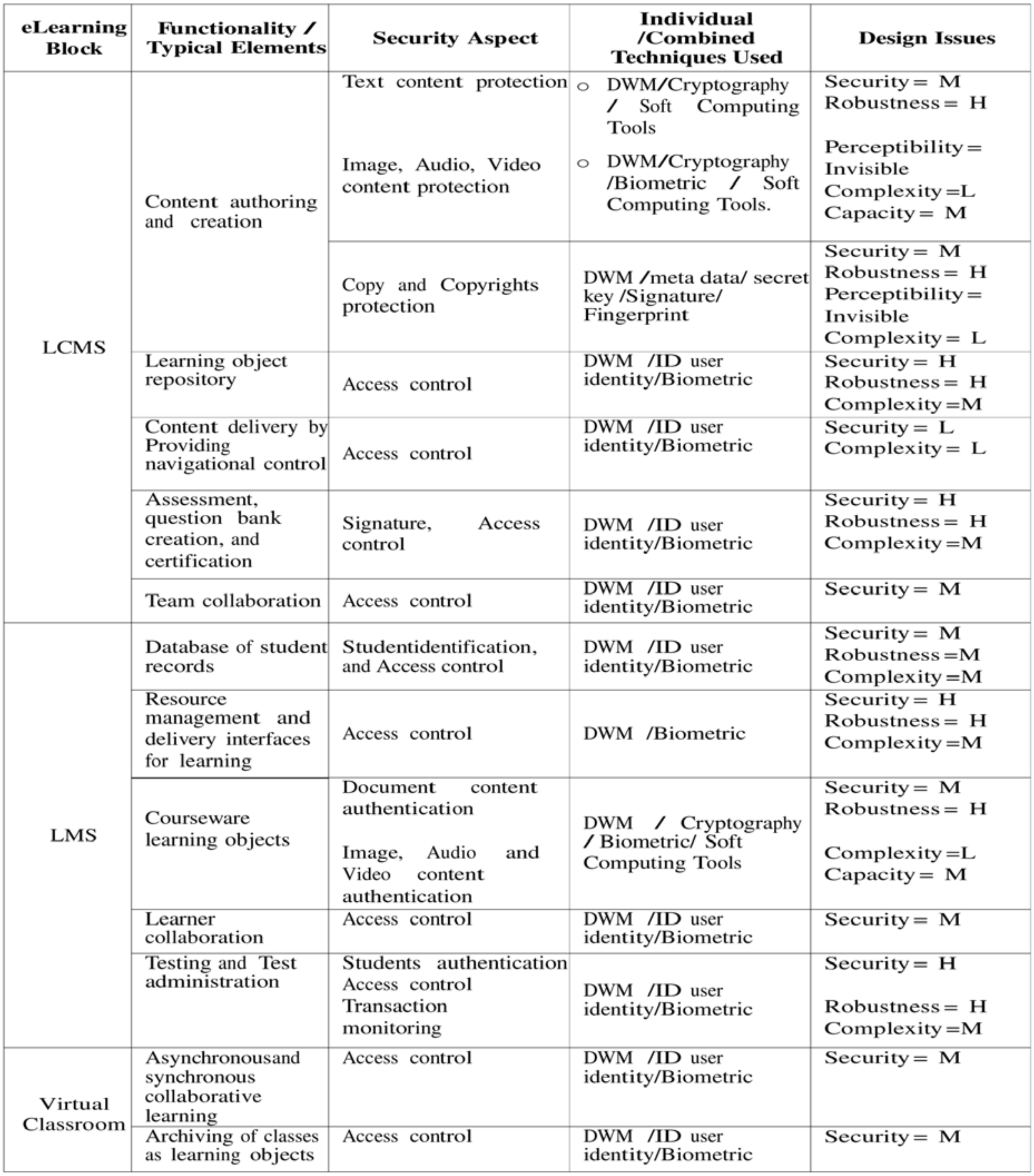
5.1.3 The Main Elements of eLearning Process

In subsection 5.1.1, we have mentioned an eLearning framework which is regarding to standardization on eLearning training materials and depending on literatures reviewed by this paper. We found three primary elements that can be integrated to provide and deliver eLearning services in higher education environment [98] [99] [100]. These elements represent the area which is applied by our case study in this paper. These three elements are: Learning Content Management System (LCMS), Learning Management System (LMS), and Virtual Classroom. In addition to the element represents system users which can be administrators, instructors, students, and content author or developers. Figure 4 illustrates the connection process between these elements [100].

5.2 Security Requirements Analysis of eLearning Elements

One of important requirements for eLearning systems is the information security and security elements such as availability, integrity, access control, contents authentication, user authentication, and confidentiality of material. These requirements contribute to strengthen the security of eLearning environment. Moreover, different kinds of students can have an effective and helpful learning environment and the eLearning users can be comfortable with sustainable institutions [98]. The existing eLearning systems face some security issues that could be lost because a security may not be integrated into the eLearning development process [101].

This subsection examines analytical review of security requirements that are considered challenges addressed in developing the main elements of eLearning system as shown in Layer 3 of Figure 3. In this analytical subsection, we depend on our reading of the literatures reviewed by this paper and based on some other criteria such as functionality of eLearning elements, user nature, and security nature as shown in Table 1. We assume the main eLearning infrastructure so as to include the following



eLearning Block	Functionality / Typical Elements	Security Aspect	Individual /Combined Techniques Used	Design Issues

LCMS	Content authoring and creation	Text content protection
		Image, Audio, Video content protection
			○ DWM/Cryptography / Soft Computing Tools
			○ DWM/Cryptography /Biometric / Soft Computing Tools.
				Security= M
				Robustness= H
				Perceptibility= Invisible
				Complexity =L
				Capacity= M

		Copy and Copyrights protection	DWM /meta data/ secret key /Signature/ Fingerprint	Security= M
				Robustness= H
				Perceptibility= Invisible
				Complexity= L

	Learning object repository	Access control	DWM /ID user identity/Biometric	Security= H
				Robustness= H
				Complexity =M

	Content delivery by Providing navigational control	Access control	DWM /ID user identity/Biometric	Security= L
				Complexity= L

	Assessment, question bank creation, and certification	Signature, Access control	DWM /ID user identity/Biometric	Security= H
				Robustness= H
				Complexity =M

	Team collaboration	Access control	DWM /ID user identity/Biometric	Security= M

LMS	Database of student records	Studentidentification, and Access control	DWM /ID user identity/Biometric	Security= M
				Robustness =M
				Complexity =M

	Resource management and delivery interfaces for learning	Access control	DWM /Biometric	Security= H
				Robustness= H
				Complexity =M

	Courseware learning objects	Document content authentication
		Image, Audio and Video content authentication
			DWM / Cryptography / Biometric/ Soft Computing Tools	Security= M
				Robustness= H
				Complexity =L
				Capacity= M

	Learner collaboration	Access control	DWM /ID user identity/Biometric	Security= M

	Testing and Test administration	Students authentication
		Access control
		Transaction monitoring
			DWM /ID user identity/Biometric	Security= H
				Robustness= H
				Complexity =M

Virtual Classroom	Asynchronousand synchronous collaborative learning	Access control	DWM /ID user identity/Biometric	Security= M
	Archiving of classes as learning objects	Access control	DWM /ID user identity/Biometric	Security= M

Table 3. Design issues of security requirements in eLearning elements

blocks: Learning environment content delivery namely eLearning Management System (LMS), Learning Content Management System (LCMS), and virtual classroom.

Table 1 illustrates the most critical security aspects in eLearning systems that are content authentication and access control. Therefore, eLearning system requires a security management framework which represents helpful guide for eLearning institutions in managing the information security within the eLearning environment.

Furthermore, the combination of information securitymanagement and the existing information security technology used will provide better consequences in the success of security implementation in eLearning environment.

5.3 Techniques Combined with Digital Watermarking

This subsection shows the most common techniques that may be used individually or combined together to improve the security requirements in eLearning environment as illustrated by Table 1. Using one of these techniques is different based on functionality or elements and security nature. Table 2 show samples of using one technique or more than one combined together as shown in bold column of the table 2.

5.4 Design Issues in eLearning System Elements

This section emphasizes on the most significant design issues that mentioned in Section 4 namely security and related issues such as robustness, perceptibility, complexity, and capacity. We classify the levels of the significance for each issue as (high, mid, low) except for Perceptibility levels which are classified as (visible, invisible). In Table 3 we try to apply them approximately to our case study, especially to eLearning elements based on security requirements mentioned in subsections 5.2 and 5.3.

6. Conclusions

In this paper, a literature and analytical review have been presented for state-of-the-art digital watermarking techniques with more emphasizing on the concepts, applications, classifications, design issues, and the relationship with digital content authentication. We have introduced a new classification for digital watermarking techniques and design issues that have been extracted from our reading and literature review. Our new classification for digital watermarking techniques can be considered a contribution of this paper. Finally, this paper introduces a case study in which the requirements analysis of security and other design issues that have been applied to eLearning system using a combination of digital watermarking techniques and other techniques of content authentication in eLearning environment. eLearning system has been segmented into sub-elements, components, and services. On the level of each element or component, digital watermarking techniques have been applied to eLearning system individually or by combining them with other techniques such as biometrics or soft computing tools. We concluded that applying these techniques to each element or component individually based on its content and requirements should take into account keeping the integration between those elements or components and the whole environment. Future work of this paper can be introduced by developing and evaluating a framework for digital content authentication in eLearning system.

7. Acknowledgements

We are grateful to support of Prof. Adnan Zain Al-sakaf and Dr. Ammar T. Zahary who helped us to perform this paper by their invaluable comments and suggestions

References

[1] Suhail, M. A. (2008). Digital Watermarking for Protection of Intellectual Property, A Book Published by University of Bradford, UK.

[2] Chun-Shien, L. (2005). Multimedia Security: Steganography and Digital Watermarking techniques for Protection of Intellectual Property, A Book Published by Idea Group Publishing.

[3] Berman, P., Afaneh, M. (2006). E-Learning Concepts and Techniques, A Book Published by Institute for Interactive technologies, Bloomsburg University of Pennsylvania, USA.

[4] Qing Li et al. (2009). Emerging Internet Technologies for ELearning, *IEEE Internet Computing*, 13 (4) 11-17.

[5] Falakmasir, M., Habibi, J., Moaven, S., Abolhassani, H. (2010). Business Intelligence in E-Learning, 2nd *International Conference on Software Engineering and Data Mining* (SEDM), IEEE, p. 473-477.

[6] Ingemar, C., Matthew, M., Jeffrey, B., Jessica, F., Ton, K. (2008). Digital Watermarking and Steganography, a Book Published by Morgan Kaufmann Publishers.

[7] Rakhi, C., Frederick, C. (2010). A Voice-Based Biometric Watermarking Scheme For Digital Rights Management of 3D Mesh Models, A PhD Dissertation by University of Nevada, Reno.

[8] http://en.wikipedia.org/wiki/Digital watermarking/ Digital watermarking lifecycle phases, last access at 6-5-2011.

[9] Seitz, J. (2005). Digital Watermarking for Digital Media, A Book published by Information Science publishing, USA.

[10] Vielhauer, I. (2006). Steganography and Digital Watermarking, A seminar supported by Christian Krtzer,Otto-von-Guericke University Magdeburg, Germany.

[11] http://www.dialogic.com/den/blogs/corporate/archive/2009/08/21/digital-watermarking.aspx, last access at 6-5-2011, 06:00 PM.

[12] http://www.digitalwatermarkingalliance.org/about.asp, last access at 8-5-2011.

[13] Henrique, S. Malvar, IEEE, M., Dinei, A. (2003). Improved Spread Spectrum: A New Modulation Technique for Robust Watermarking, *Tran. Signal Processing, IEEE*, 51 (4) 898-905.

[14] Kirovski, D., Malvar, H. (2001). Robust spread-spectrum audio watermarking, *International Conference on Acoustics, Speech, and Signal Processing*, IEEE, 3.

[15] Mikhail, A., Victor, R. (2001). Purdue team develops watermark to protect electronic documents, Online on http://news.uns.purdue.edu/html4ever/ 010427. Atal- Iah.watermark.html.

[16] Alface, P. , Macq, B. (2005). Blind watermarking of 3D meshes using robust feature points detection, *In*: Proceedings of International Conference on Image Processing (ICIP), IEEE, 1, 693-696.

[17] Sooyeun, J., Dongeun, L., Seongwon, L., Joonki, P. (2007). Biometric data-based robust watermarking scheme of video streams, *In*: Proceedings of 6th International Conference on Information, *Communications and Signal Processing*, p. 1- 5.

[18] Sooyeun, J., Dongeun, L., Seongwon, L., Joonki, P. (2008). Robust watermarking for compressed video using fingerprints and its applications, *International Journal of Control, Automation and Systems*, 6 (6) 794-799.

[19] Tuan, H., Dat, T., Sharma, D. (2008). Remote multimodal biometric authentication using bit priority-based fragile watermarking, Proceedings of 19th International Conference on Pattern Recognition, p. 1-4.

[20] AbdulQadir, M. (2006). Digital Text Watermarking: Secure Content Delivery and Data Hiding in Digital Documents, *A/E Systems Magazine, IEEE*, p. 18-21.

[21] Eggers, J., Girod, B. (2001). Blind watermarking applied to image authentication, *International Conference on Acoustics, Speech and Signal Processing*, ICASSP, USA, p. 1977-1980,.

[22] Huang, J., Wang, Y., Shi, Y. (2002). A blind audio watermarking algorithm with self-synchronization, *Int. Symp. Circuits and Systems*, *IEEE*, 3, 627-630.

[23] Dazhi , H., Xingqiang, Y., Caiming, Z. (2009). A novel robust 3D mesh watermarking ensuring the human visual system, *In*: Proceedings of Second International Workshop on Knowledge Discovery and Data Mining, p. 705-709.

[24] Suk-Hwan L., Ki-Ryong, K. (2007). A watermarking for 3d mesh using the patch cegis, *Journal of Digital Signal Processing*, 17 (2) 396-413.

[25] Vidyasagar, M., Song, H., Elizabeth, C. (2005). A Survey of Digital Image Watermarking Techniques, 3rd International *Conference on Industrial Informatics*, IEEE, p. 709-716.

[26] Hoang, N., Kim, N., Hoai, B. (2010). Literature Survey on Image Watermarking Tools, Watermark Attacks, and Benchmarking Tools, *Second International Conferences on Advances in Multimedia, IEEE*, p. 67-73.

[27*]* http://www.easyimagetools.com/products/watermark/index.htm, last access at 2-5-2011, 2:00 PM.

[28] http://www.mytoolsoft.com/watermark-software.php, last access at 2-5-2011 04:00 PM.

[29] http://www.watermarksoft.com/watermark-it.htm, last access at 2-5-2011 05:00 PM.

[30] Sudirman, S., Dhiya, A. (2009). Copyright Protection of Digital Images using High Order Polynomial Watermarking, *Second International Conference on Developments in eSystems Engineering, IEEE*, p. 173-180.

[31] Senthil, N., Rajesh, R. (2009). Image Segmentation - A Survey of Soft Computing Approaches, *International Conference on Advances in Recent Technologies in Communication and Computing, IEEE*, p. 844-846.

[32] Cvejic, N., Seppnen, T. (2002). Increasing the capacity of LSB based audio steganography, *In*: Proceedings of the *International Workshop on Multimedia Signal Processing*, *IEEE*, p. 336-338.

[33] Hiujuan, Y., Patra , J., Chan, C. (2002). An artificial neural network- based scheme for robust watermarking of audio signals, *In*: Proceedings of the *International Conference on Acoustics, Speech, and Signal Processing*, *IEEE*, p. I-029 - I-1032.

[34] Kirovski, D., Malvar, H. (2003). Spread-spectrum watermarking of audio signals, *Transactions on Signal Processing*, IEEE, p. 1020-1033.

[35] http://audiowatermarking.info/, last access at 4-5-2011 07:00 PM.

[36] http://research.microsoft.com/enus/downloads/ 885bb5c4-ae6d-418b97f9-adc9da8d48bd/default.aspx, last access at 4-5-201108:30 PM.

[37] http://www.magellanhardware.com/watermarking.asp, last access at 4-5-2011 10:00 PM.

[38] Sourav, B., Chattopadhyay, T., Arpan, P., A Survey on Different Video Watermarking Techniques and Comparative Analysis with Reference to H.264/AVC, *International Symposium on Consumer Electronics*, *IEEE*, p. 1-6.

[39] Saadi, K., Bouridane, A., Gessoum, A. (2010). H.264/AVC Video Authentication Based Video Content, I/V Communications and Mobile Network (ISVC), 2010 5th International Symposium, IEEE, p. 1- 4, 2010.

[40] http://convid.com/la/default.aspx, last access at 5-5- 2011 02:00 PM.

[41] http://www.ease123.com/watermarker/index.htm, last access at 4-5-2011 10:00 PM.

[42] http://www.geovid.com/VidLogo/, last access at 5-5-2011 07:00 PM.

[43] http://www.videocharge.com/Products/wm/main.php, last access at 5-5-2011 07:30 PM.

[44] http://www.videowatermarkfactory.com/, last access at 5-5-2011 09:00 PM.

[45] Zunera, J., Anwar, M., Gessoum, A. (2009). A Review of Digital Watermarking Techniques for Text Documents, *International Conference on Information and Multimedia Technology, IEEE*, p. 230-234.

[46] Brassil, J., Low, S., Maxemchuk, N. (1999). Copyright Protection for the Electronic Distribution of Text Documents, *In*: Proceedings of the IEEE, 87 (7) 1181-1196.

[47] Huang, D., Yan, H., Interword distance changes represented by sine waves for watermarking text images, *IEEE Trans. Circuits and Systems for Video Technology*, 11 (12) 1237-1245.

[48] Youn-Won K., A text watermarking algorithm based on word classification and inter-word space statistics, Proceedings of the Seventh International Conference on Document Analysis and Recognition (ICDAR03), IEEE, p. 775-779.

[49] Alattar A., Alattar O. (2004). Watermarking electronic text documents containing justified paragraphs and irregular line spacing, *In*: Proceedings of SPIE Security, Steganography, and Watermarking of Multimedia Contents SPIE, 5306, 685-695.

[50] Atallah, M., McDonough C., Nirenburg, S., Raskin, V. (2000). Natural Language Processing for Information Assurance and Security: An Overview and Implementations, *In*: Proceedings 9th ACM/SIGSAC New Security Paradigms Work- shop,Ireland, p. 51-65.

[51] Hassan, M. (2009). Natural language watermarking via morphosyntactic alterations, *Computer Speech and language Journal*, 23 (1) 107-125.

[52] Topkara, U., Topkara, M., Atallah, M. (2006). The Hiding Virtues of Ambiguity: Quantifiably Resilient Watermarking of Natural Language Text through Synonym Substitutions, *In*: Proceedings of ACM Multimedia and Security Conference, Geneva, p. 164-174.

[53] Xingming, S., Alex, J. (2005). Noun-Verb Based Technique of Text Watermarking Using Recursive Decent Semantic Net Parsers, Lecture Notes in Computer Science (LNCS), Springer Press, 3612.

[54] Peng, L. (2008). An optimized natural language watermarking algorithm based on TMR, *In*: Proceedings of 9th *International Conference for Young Computer Scientists*, ICYCS, p. 1459-1463.

[55] Sajjadi, Z., Khodami, A., Modiri, N. (2008). Learning Contents integrity verification on E-Learning Systems Using Digital Watermarking Technique, 3rd International *Conference on Information and Communication Technologies: From Theory to Applications*, ICTTA, p. 1-3.

[56] Hanane, H., Hien, D., Zensho, N. (2008). A new intelligent Digital Right Management technique for E-learning content, *International Joint Conference on Neural Networks* (IEEE World Congress on Computational Intelligence), IEEE, p. 3577-3581.

[57] Gulbis, M., Steinebach, M., Muller, E. (2008). Content-Based Authentication Watermarking with Improved Audio Content Feature Extraction, *International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, IEEE, p. 620-623.

[58] De-Song, W., Jian-Ping L., Yue-Hao Y. (2008). A Novel Authentication Scheme of the DRM System based on Multimodal Biometric Verification and Watermarking Technique, *International Conference on Apperceiving Computing and Intelligence Analysis*, IEEE, p. 212-215.

[59] Sudirman S., Al-Jumeily, D. (2009). Copyright Protection of Digital Images Using High Order Polynomial Watermarking, Second International Conference on Digital Object Identifier, IEEE, p. 173-180.

[60] Anil, J., Umut, U. (2002). Hiding Fingerprint minutiae in images, *In*: Proceedings of Third Workshop on Automatic Identification Advanced Technologies (AutoID).

[61] Anoop, N., Anil, J. (2004). Multimedia document authentication using online signatures as watermarks, Security, Steganography, and Watermarking of Multimedia Contents, 6, 5306.

[62] Low, C., Teoh, A., Tee, C. (2007). A preliminary study on biometric watermarking for offline handwritten signature, *In*: Proceedings of International Conference on Telecommunications and Malaysia International Conference on Communications, IEEE, p. 691-696.

[63] Ababneh, S., Ansari, R., Khokhar, A. (2009). Compensated Signature Embedding for Multimedia Content Authentication, *ACM Journal of Data and Information Quality*, USA, 1 (3).

[64] Bossi, S., Mapelli, F., Lancini, R. (2005). Semi-fragile watermarking for video quality evaluation in broadcast scenario, International Conference on Image Processing, IEEE, p. I -4.

[65] Loytynoja, M., Cvejic, N., Keskinarkaus, A., Lahetkangas, E., Seppanen, T. (2006). Mobile Commerce from Watermarked Broadcast Audio, *Digest of Technical Papers International Conference on Consumer Electronics*, p. 5 -6.

[66] Jiaming, H., Hongbin, Z. (2008). Digital Right Management Model Based on Cryptography and Digital Watermarking, *International Conference on Computer Science and Software Engineering*, IEEE, p. 656-660.

[67] Mathivadhani1, D., Meena, C. (2010). Digital Watermarking and Information Hiding Using Wavelets, *SLSB and Visual Cryptography Method*, Image (Rochester, N.Y.), IEEE, p. 1-4.

[68] Shiguo, L. (2007). Image Authentication Based on Neural Networks, SAMI Lab, France Telecom R/D Bejing, Beijing, CoRR, P. R, China.

[69] Anwar, M., Ishtiaq, M., Iqbal, M., Jaffar, M. (2010). Blockbased Digital Image Watermarking using Genetic Algorithm, 6th International Conference on Emerging Technologies (ICET), IEEE, p. 204-209.

[70] Ketcham, M., Vongpradhip, S. (2007). Intelligent Audio Watermarking using Genetic Algorithm in DWT Domain, *World Academy of Science, Engineering and Technology*.

[71] Hassanien, A. (2006). Hiding iris data for authentication of digital images using wavelet theory, Proceedings of Patten Recognition and Image Analysis, Springer Link, 16 (4) 637-643.

[72] Mayank, V., Richa, S., Afzel, N. (2005). Improving biometric recognition accuracy and robustness using DWT and SVM watermarking, *IEICE Electronics Express*, 2 (12) 362-367.

[73] Vielhauer, C., Steinmetz, R. (2001). Approaches to biometric watermarks for owner authentication, security and Watermarking of Multimedia Contents III, 4314.

[74] http://encyclopedia.jrank.org/articles/pages/725/Digital-Watermarking.html, last access at 11-5-2011 08:30 PM.

[75] Qiming, L., Memon, N., Sencar, H. (2006). Security issues in watermarking applications a deeper look, *In*: Proceedings of the 4th international workshop on Contents protection and security, ACM, p. 23-28.

[76] Bojkovic, Z., Milovanovic, D. (2003). Multimedia contents security: watermarking diversity and secure protocols, 6th International Conference on Telecommunications in Modern Satellite, Cable and Broadcasting Service, TELSIKS, p. 377-383.

[77] Zhang, Y. (2009). Digital Watermarking Technology: A Review, *ETP International Conference on Future Computer and Communication, IEEE*, p. 250-252. 2002

[78] Hartung, F., Kutter, M. (1999). Multimedia watermarking techniques, *In*: Proceedings of the IEEE, 87 (7) 1079-1107.

[79] Lian, C., Sidan, D. (2004). Robust Digital Image Watermarking Method Against RST Attacks, *International Conference on Signal Processing and Communications* (SPCOM), IEEE, p. 491-495.

[80] Suhail, M., IEEE, M., Obaidat, M. (2007). Robust Watermarking System Using Security Enhancement on Content Based Image Segmentation, I 14th International Conference on Electronics, Circuits and Systems, IEEE, p. 1252-1255.

[81] Girod, B.,Su, J. (1999). On the imperceptibility and robustness of digital fingerprints, *Multimedia Computing and Systems* (ICMCS) , Italy, 2, 530-535.

[82] Craver, S., Memon, N., Yeo, B., Yeung, M. (1997). Can invisible watermarks resolve rightful ownerships, Technical Report RC 20509, IBM Research Institute.

[83] Fridrich, J. (1999). Key-dependent image transforms and their applications in image watermarking, *In*: Proceeding of International Conference on Image Science, Systems and Technology, CISST, p. 237243.

[84] Meerwald, P., Uhl, A. (2001). Watermark security via wavelet filter parametrization, International Conference on Image Processing, ICIPO, 3, 1027-1030.

[85] Suhail, M., Obaidat, M. (2006). Security Enhancement of Multimedia Copyright Protection, *International Conference on Systems*, *Man, and Cybernetics, IEEE*, 2, 1531- 1535.

[86] Trappe, W., Washington, L. (2001). Introduction to Cryptography with Coding Theory, A Book published by Englewood Cliffs, NJ: Prentice-Hall, 2d edition.

[87] Swanson, M., Zhu, B., Tewfik, A. (1996). Robust data hiding for images, *In*: Proceeding IEEE DSP Workshop, Loen, Norway, p. 3740.

[88] Alghoniemy, M., Tewfik, A. (1999). Self-synchronizing watermarking techniques, *In*: Proceeding Symp. Content Security and Data Hiding in Digital Media: NJ Center for Multimedia Research and IEEE, 4, 2075.

[89] Liu, B.,Wu, M. (1998). Watermarking for image authentication, *In*: Proceeding SIEEE International Conference Image Processing (ICIP98), p. 437-441.

[90] Shu-Fen, T., Ching-Sheng, H. (2008). An Imperceptible Watermarking Scheme Using Variation and Modular Operations, *International Conference on Multimedia and Ubiquitous Engineering*, IEEE, p. 233-237.

[91] Shu-Fen, T., Ching-Sheng H. (2010). An Imperceptible Frequency-Domain Watermarking Scheme without Resorting to the Original Image, *Second International Conference on Communication Software and Networks, IEEE*, p. 360 - 364.

[92] Hongpeng, T., Miao, M. (2007). An Automatic Method to Evaluate the Imperceptibility of Digital Watermark, *International Conference on Control and Automation FrD8-6 Guangzhou, IEEE*, CHINA, p. 3226 - 3229.

[93] Zhang, Y., Qin H., Kong, T. (2010). A Novel Robust Text Watermarking For Word Document, 3rd International Congress on Image and Signal Processing (CISP2010), IEEE, 1, 38-42.

[94] Servettot, S., Podilchuks, C., Ramchandrant, K. (1998). Capacity Issues, *In*: Digital Image Watermarking, *IEEE Journal*, 1, p. 445 - 449.

[95] Kutter, M. (1998). Watermarking resisting to translation, rotation, and scaling, Proceedings of SPIE: Multimedia Systems and Applications, Boston, MA, p. 423-431.

[96] Chou, J., Ramchandran, K., Ortega, A. (2001). High capacity audio data hiding for noisy channels, *In*: Proceedings of the International Conference on Information Technology: Coding and Computing, p. 108-108.

[97] Voyatzis, G., Nikola ides, N., Pitas, I. (1998). Digital watermarking: An overview, *In*: Proceedings of the European Signal Processing Conference (EUSIPCO), p.13 - 16.

[98] Alwi, N., Fan I. (2010). E-Learning and Information Security Management, *International Journal of Digital Society* (IJDS), 1 (2).

[99] http://www.cognitivedesignsolutions.com/ELearning/ Architecture.htm, last access at 17-5-2011 07:30 PM.

[100] Hutter, O., Simonics, I., Szkaliczki, T., Wagner, B. (2006). Standard-Based ELearning Solutions In Higher Education, *Periodica polytechnic Ser.EL.ENG*. 50 (34).

[101] Aljawarneh, S., Muhsin , Z., Nsour, A., Alkhateeb, F., AlMaghayreh, E. (2010).SE-learning Tools and Technologies in Education: A Perspective, LINC 2010 Conference, 20.