RESEARCH ARTICLE OPEN ACCESS

Digital Watermarking Classification : A Survey

Jaishri Guru[1], Hemant Damecha[2]
Research Scholar M.E[1], Assistent professor[2]
Software Systems - Department of Computer Science and Engineering
Shri Ram Institute of Technology, Jabalpur
R.G.P.V University
Bhopal - India

ABSTRACT

One of most significant property of digital information is that it is in principle extremely easy to produce and distribute unlimited number of its copies. The actuality that an unlimited number of perfect copies of text, audio and video data can be illegally produced and distributed requires to study ways embedding copyright information and serial number in audio and video data Now a day's internet is an essential channel for digital assest, but it has been noticed that someone are misusing by building illegal copies and leaking the information which creates a bad environment in the field of software industry .It can be avoided by doing most excellent efforts using digital watermarking . As we have witnessed in the past few months, the problem of protecting multimedia information becomes more necessary and a lot of copyright owners are concerned about protecting any illegal duplication of their data or work. Some serious work needs to be performing in order to maintain the availability of multimedia information but, in the meantime the industry must come up with ways to guard intellectual property of makers, distributors or simple owners of such data [1]. Many approaches possible to protect visual data, digital watermarking is probably the one that has received nearly all interest. We know that stenography and watermarking are main facts of quick developing area in case of information hiding. Generally Watermarks are used where authentication or ownership is required. Watermarks are a good way by which anyone can confirm the ownership of multimedia. This paper attempts to first introduce digital watermarking as well as some of its necessary notions. It is followed by describing some applications of watermarking techniques.

Keywords:- WaterMarking, Copyright Protection, DCT, LSB, URL

I. INTRODUCTION

It is the age of computers and network technologies. Progress in these has increases to massive scopes for develop and distribution of digital media theme. Digital data is easy to be edited and irregular transcribe, thus we need a technology to obviate such issues [2].The spell "Digital watermarking" was first emerged in 1993.The Digital watermarking is a technology that organizes and assigns security, data certification, publishing protection to the digital media theme. Watermarking is the embedding of allude, watermarks in to the digital media theme like as portrait, audio and film. Then later embedded data is searched and pointed out to exhibit actual identity of digital media contents. Digital watermarking is used for various purposes such as proof of identity, copying deterrence, diastole monitoring, data hiding and certification[2]. one of the greatest technological advancements to change people's lives in the past decade or so has been the Internet. The growth of high speed computer networks and that of Internet, in particular, has explored means of new business, scientific, entertainment, and social opportunities in the form of electronic publishing and promotion, real-time information delivery, transaction processing, product ordering, digital repositories and libraries, web pages, web newspapers and magazines, network video and audio, personal communication, lots more[3].

Today, the Internet affects all industries as its potential continues to be recognized and explored [4]. The increase in demand has meant great attention has been paid to the evolution of net technology, including increased data transfer speeds. One of the more notable side effects of this evolution has been the volume of data transfer between users, including the trading of pirate material, whether software, video or audio. With high transfer speeds and the ability to communicate with any other user connected to the Internet, piracy has become a serious problem[4]. The ease by which a digital information can be duplicated and distributed has led to the require for effective copyright protection tools. A variety of software products have been just introduced in attempt to address these growing concerns It should be possible to hide data (information) within digital audio, video and images files. The

information is hidden in the sense that it is perceptually and statistically invisible. One way to protect multimedia data beside illegal recording and retransmission is to implant a signal, called digital signature or copyright label or watermark that completely characterizes the person who applies it and, consequently, marks it as being his intellectual property [5]. Digital watermarking stands for embedding a signature signal, called watermark into a digital cover, in order to verify ownership, check authenticity or integrity of the cover, and it may relate to audio, images, video or even text. Digital watermarking is a process of embedding unobtrusive marks or labels into digital content. These implanted marks are typically imperceptible (invisible) that can later be detected or extracted .The concept of digital watermarking is associated with steganography. Steganography is defined as covered writing. It has a long history of being associated with methods of secret communication. Therefore, digital watermarking is a way to hide a secret or personal message to protect a product's copyright or to demonstrate data integrity. Watermark may contain security feature such as document serial number or other information related to data to originator such as date of birth. Watermarked document can give the information about modifications or upgrading, counterfeits by comparing the watermarked data to original data [6]. The watermark content depends upon the originator or requirements to ensure the integrity of the information as well as authentication of the documents. Digital watermarking techniques can be categorized as private and public watermarks[6].

A. Private watermark

A private (secret) watermark may contain information for identifying the licensee or to prove ownership in disputes. Retrieval of secret watermark information requires at least one secret key, known only to the embedder. A private watermark puts heavy demands on a watermarking algorithm regarding robustness, although the demands for ability are relaxed. Embedded information usually includes licensee-identifying hash values or serial numbers. In general, a serial number is just a pointer or link to externally stored information, such as a customer record [7].

B. Public watermark

A public watermark is retrieved by the receiver (licensee) of copyrighted material. It usually contains copyright or licensing information, such as the identifier of the patent or copyright holder, the creator of the material, or a link (Universal Resource Locator) through which to fetch more related information. A public watermark puts heavy demands on a watermarking algorithm regarding capacity. Because a public watermark providesadditional copyright realted information for receivers and doesn't aim to prove ownership or identify licensees,the re the requirements regarding robustness are relaxed[8].

II. WATERMARK FRAMEWORK

Watermarking is the process that embeds data called a watermark or digital signature or tag or label into a multimedia object such that watermark can be detected or extracted later to make an assertion about the object. The object may be an image or audio or video. However the watermark might contain additional information including the identity of the purchaser of a particular copy of the material.[9] In general, any watermarking scheme (algorithm) consists of three parts:

1. The watermark
2. The encoder (marking insertion algorithm)
3. The decoder and comparator (verification or extraction or detection algorithm)

Each owner has a unique watermark or an owner can also put different watermarks in different objects the marking algorithm incorporates the watermark in to the object. The verification algorithm authenticates the object determining both the owner and the integrity of the object.

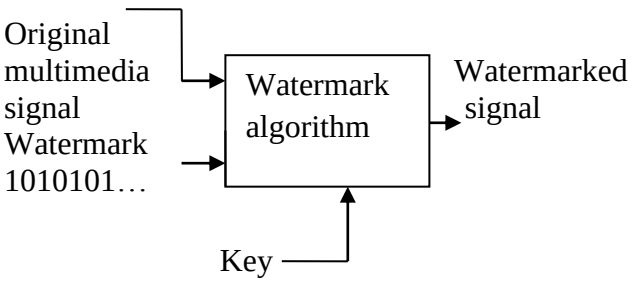


Figure 1: Watermark embedding process

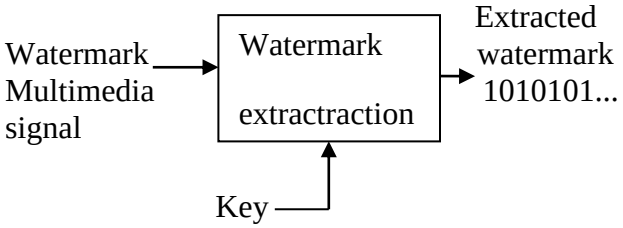


Figure 2: Watermark extraction process

III. PURPOSE OF DIGITAL WATERMARK

Watermarks added to digital content serve a variety of purposes. The following are the purposes of digital watermarking.

A. Ownership Assertion

To establish ownership of the content (i.e image)

B. Fingerprinting

This technique is used and apply for avoid unauthorized duplication and distribution of publicly available multimedia content [9].

C. Authentication and integrity verification

The authenticator is inseparably bound to the content whereby the author has a unique key associated with the content and can verify integrity of that content by extracting the watermark

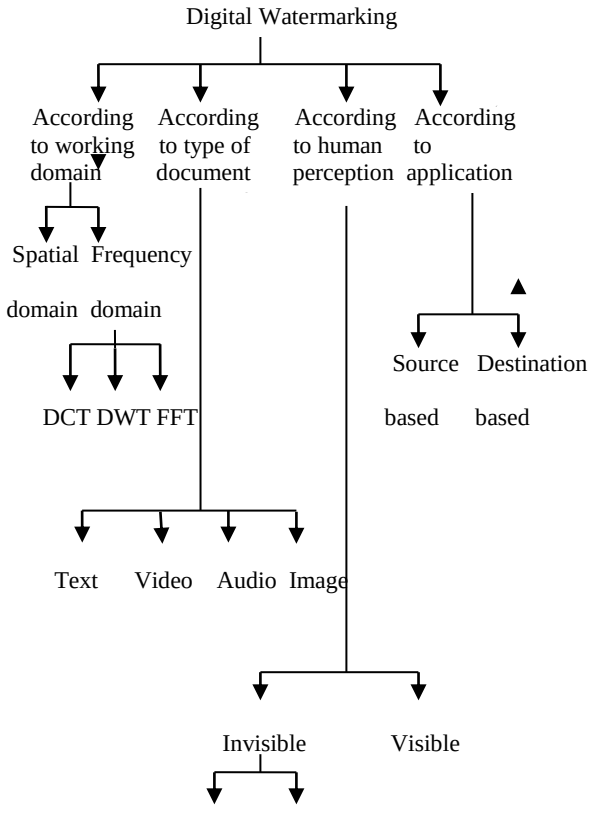
D. Content labeling

Bits embedded into the data that gives further information about the content such as a graphic image with time and place information.

E. Usage control

Added to limit the number of copies created whereas the watermarks are modified by the hardware and at some point would not create any more copies (i.e. DVD)

IV. TYPES OF DIGITAL WATERMARK



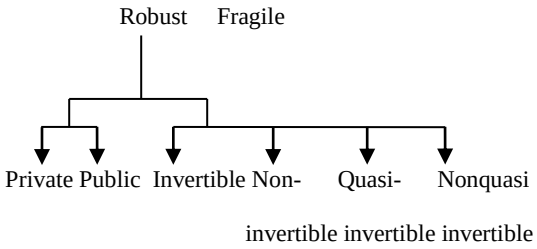


Figure 3: classification of digital watermarking

Watermarks and watermarking techniques can be divided into a variety of categories in various ways [10]. Watermarking techniques can be separated into four categories according to the type of document to be watermarked as follows:

1) Text Watermarking
2) Image Watermarking
3) Audio Watermarking
4) Video Watermarking[5]

In other way, the digital watermarks can be divided into four different types as follows:

I. Visible watermark
II. Invisible watermark
III. Fragile watermark
IV. Robust watermark

V. WATERMARK APPROACHES

There are various approach used for watermarking
Each process and approach is different as compare to others. How the approaches work and it is used is depends upon the application and its requirements.

A. Fragile Watermarking Scheme

Watermark is a visually significant binary logo, which is much smaller than the image to be marked and is used to form a binary image as big as the image. Watermark embedding is performed by scanning each dots or pixel and performing the watermark extraction function based on a lookup table generated with a secret key. If the extracted watermark bit is equal to the valid watermark bit, the pixel or dots is left unchanged otherwise, the gray scale of the pixel or dots is adjusted until the extracted watermark bit is equal to the authentic one. Because of its pixel-wise scanning fashion, local tampering can be localized to pixel accuracy [11]. The pixel-wise watermarking fashion is actually a special case of the block-wise style with block size equal to 1.

B. Reversible Watermarking Schemes:

The reversible watermarking is used for removing the distortion which arrives due to various media sources. One limitation of watermarking based authentication schemes is the distortion inflicted on the host media by the embedding process. Although the distortion is frequently insignificant, it may not be acceptable for some applications, especially in the areas of medical imaging. Therefore, watermarking scheme capable of removing the distortion and recovering the original media after passing the authentication is desirable. Schemes with this capability are often referred to as reversible watermarking schemes also known as invertible or erasable watermarking.

VI. WATERMARKING TECHNIQUES

Digital watermarking is a fairly new research area and combines studies and results from other research areas, such as digital signal processing, communications, compression, information theory, and cryptography . The most important properties of any digital watermarking techniques are robustness, security, imperceptibility, complexity, and verification. Robustness is defined as if the watermark can be detected after media (normal) operations such as filtering, lossy compression, color correction, or geometric modifications. The following sections describe a few of the most common digital watermarking techniques.

A. LSB Watermarking Technique:

LSB watermarking describes a straightforward and basic way to integrate watermark information in digital documents. Considering a basic grey scale image, the pixel and its values can be sliced up into significant and irrelevant levels. Because the significant levels merely represent a digital noise pattern, it could be easily used for digital watermarking. In changing selected pixel values of the noise pattern using a special or key-based algorithm, the watermarking information can be easily integrated. However, such technique is very insecure because the watermark can be easily destroyed. On the other hand, such technique can be useful in copy control and authenticity applications.

B.Robust Watermarking Technique:

Contrary to the LSB approach, the key to making a watermark robust is that it should be embedded in the perceptually significant components of the image. A good watermark is one which takes into account the behavior of human visual system.

C. DCT-based watermarking

The image is first divided into 8 × 8 pixel blocks. After DCT transform and quantization, the mid frequency range DCT coefficients are selected based on a Gaussian network classifier.

The mid-frequency range DCT coefficients are then used for embedding. Those coefficients are modified using linear DCT constraints. It is claimed that the algorithm is resistant to JPEG

Compressions [12].

D. Spatial vs. Frequency Domain

Most watermarking techniques themselves can be distinguished into two approaches, those in the spatial domain and those in the Frequency domain. The main difference between these approaches is their robustness. Spatial techniques were the initial development in the field. Spatial domain watermarks are being developed today, since their techniques are relatively cheap and for more trivial examples they can quickly create a watermark with Little effort. The main area of focus with this form of watermarking is in the randomized key. If the key follows a pattern, then the human mind is more likely to pick up on the imperfection and so it will be easier to notice and therefore remove. Techniques applied in the Frequency domain are more robust than those applied in the spatial domain. This explains in part why the bulk of current research is directed towards the exploration of Frequency based techniques.

E. Blind and Non-blind Techniques

In order to detect the watermark information, blind and non blind techniques are used. If the detection of the digital watermark can be done without the original data, such techniques are called blind. Here, the source document is scanned and the watermark information is extracted. On the other hand, non blind techniques use the original source to extract the watermark by simple comparison and correlation or interconnected procedures. However, it turns out that blind techniques are more insecure than non blind methods[13].

F. Spread Spectrum Watermarking

Spread spectrum techniques are widely used in digital watermarking which is derived from the communication field. The basic idea of spread spectrum is to spread the data across a large frequency band. In the case of audio, it is the whole audible spectrum in the case of images; it is the whole visible spectrum. Spread spectrum is a military

technology designed to handle interferences and disturbances. In most cases, signals that represent the information are modulated at low intensity diagonally the source bandwidth. Spread spectrum techniques used in communication for radar, navigation, and communication applications.

VI. APPLICATIONS

1)Copyright protection: The visible watermarking is used for copyright protection which is the most important digital watermarking application. The copyright protection requires high level of robustness so that the embedded watermark can not be removed without data distortion.then this watermark is extracted to show as proof if someone claims the ownership of the data [14].
Digital watermarking can be used to protecting redistribution of copyrighted material over the untrusted network like Internet[15]. During the sharing of data over the internet we need a protected way for distribution.In this watermarking techniques have various applications [16].

2)Finger Printing:The finger printing is similar to giving serial number to any product.Every spreaded multimedia copy is embedded with a distinct watermark [14]. We can use the concept of fingerprinting to detect the true owner of digital content. Each consumer of digital content has its unique identity as fingerprint[16].

3)Integrity protection:The invisible watermark is a poof of ownership.Objective of this application is to find modification in data.Data watermark is embedded in host data to verify the authenticity of received data.fragile digital watermarking algorithm is required in this case.fragile watermark helps in detecting the tampered regions and estimating by how much and how the data is changed [14].

4)Broadcast Monitoring: Main use of broadcast monitoring is to protecting the valuable TV products like news items from illegal transmission [14]. This refers to the technique of cross-verifying whether the content that was supposed to be broadcasted has actually been broadcasted or not. Digital watermarking can also be used for broadcast monitoring.Broadcast monitoring has major application is commercial advertisement broadcasting where the entity who is advertising wants to monitor whether their advertisement was really broadcasted at the right time and for right duration [15].

5) Indexing: Key information related to the data is inserted as watermark. Now this watermark information is used by a search engine for retrieving the required data quickly and without any ambiguity [14].

6) Medical Applications: In this application patient's information is inserted as watermark in medical images.This helps in avoiding ambiguities in searching the medical records [14].

7) Fraud detection: When consumer use multimedia content for legal purposes then it is important to protect information from being tampered.If receiver discovers the degradation in digital watermark then the document cannot be trusted.The fraud detection is important in terms of the security for some applications for e.g. medical records [16].

8) Id card verification: Data or information on the person photo and at the time of identification the hidden information is compared with the detail present on the id-card.Now it is quite efficient to revel the true identity of a person.Id card verification approach can be used by company to verify its employee, passport authority for the identity of the person and many more[16].

VII. CONCLUSION

Watermark, a recognizable image or pattern in paper used to identify authenticity. Digital watermarking is a technique to embed information into the underlying data. Using digital watermarking techniques the security requirements such as data integrity, data authentication can be met and user can check the validity or authenticity of the received watermarked information with a watermarking extraction process and a watermark key. In this paper, we have reviewed the needs of watermarking, the watermarking technique, watermarking approaches and watermarking purpose and their types.

REFERENCES

[1] Radhika v. Totla, K.S.Bapat(2, February 2013) Comparative Analysis of Watermarking in Digital Images Using DCT & DWT, International Journal of Scientific and Research Publications, Volume 3, Issue 2, ISSN 2250-315

[2] Chan-Il Woo and Seung-Dae Lee , "Digital Watermarking for Image Tamper Detection using Block-

Wise Technique", International Journal of Smart Home Vol.7, No.5 (2013), pp.115-124 http://dx.doi.org/10.14257/ijsh.2013.7.5.12.

[3] Prabhishek Singh, R S Chadha, "A Survey of Digital Watermarking Techniques, Applications and Attacks", International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 9(March 2013).

[4] Mohammad Ibrahim Khan1, Md. Maklachur Rahman2 andMd. Iqbal Hasan Sarker(May 2013) Digital Watermarking for Image Authentication Based on Combined DCT, DWT and SVD Transformation, IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 3, No 1, ISSN (Online): 1694-078

[5] Darshana Mistry(09, 2010) Comparison of Digital Water Marking methods,/ (IJCSE) International Journal on Computer Science and Engineering Vol. 02, No. 09, 2010,ISSN 2905-2909

[6] Jaishree Jain and Vijendra Rai(16, May, 2012) Robust Multiple Image Watermarking Based on Spread Transform,VOL-2, ISBN 978-953-51-0619-7

[7] Madhuri Tonge#1, Praveen kumar Malviya*2, Anshu Gupta(January 2014), Implementation of Digital Watermarking Algorithm based on DWT and DCT, International Journal of Advanced Engineering and Global Technology, Vol-2, Issue-1, January 2014 ISSN No: 2309-4893

[8] Vikas Kumar 1, Ram Lautan 2, MHD Faisal 3, Krishna Mohan Pandey(9, September - 2013) Dwt and Particle Swarm Optimization Based Digital Image Watermarking, International Journal of Engineering Research & Technology (IJERT),Vol. 2 Issue 9,ISSN: 2278-0181

[9] Dilip Kumar Sharma1*, Vinay Kumar Pathak2 and G.P. Sahu-(30 December 2007)

[10] Dr. Ajit Preeti, Kalra Sonia, Dhull (4, April 2013), DIGITALWATERMARKING,International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 4, ISSN: 2277 128X

[11] Preeti Gupta (9, September 2012) Cryptography based digital image watermarking algorithm to increase security of watermark data, International Journal of Scientific & Engineering Research, Volume 3, Issue 9, September 2012 , ISSN 2229-5518

[12] Remya Elizabeth Philip1, Sumithra M.G.2(January - February 2013) Development Of A New Watermarking Algorithm For Telemedicine Applications, Vol. 3, Issue 1, January -February 2013, ISSN: 2248-9622

[13] Ensaf Hussein, Mohamed A. Belal(7, September – 2012) Digital Watermarking Techniques, Applications and Attacks Applied to Digital Media: A Survey, International Journal of Engineering Research & Technology (IJERT), Vol. 1 Issue 7, September – 2012, ISSN: 2278-0181

[14] Dr. Vipula Singh, "Digital Watermarking: A Tutorial", Geethanjali College of Engineering and Technology, Hyderabad India (2011).

[15] Vinita Gupta and Mr. Atul Barve "A Review on Image Watermarking and Its Techniques", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 1, January 2014.

[16] Anupma Yadav, Anju Yadav ,"Comparison of SVD-Watermarking and LSB-Watermarking Techniques", International Journal of Computer Science and Mobile Computing, Vol.3 Issue.5, May- 2014, pg. 495-499.

AUTHOR PROFILE

Miss jaishri guru received her B.E. in CSE from Takshshila institute of engineering and technology (R.G.P.V.Bhopal), Madhya Pradesh, India in 2011.Currently she is pursuing M.E. in Software systems from S.R.I.T (Affiliated to R.G.P.V, Bhopal). She is working on project related to "DIGITAL WATERMARKING". Her interest areas are Digital Image Processing, Network security and Network Management.