Existing Trends of Digital Watermarking and its Significant Impact on Multimedia Streaming: A Survey

R. Radha Kumari[1]
Research Scholar
JNT University, Ananthpuramu, India

V. Vijaya Kumar[2]
Dean, Department of CSE & IT and Director CACR, Anurag Group of Institutions, Hyderabad, India

K.Rama Naidu[3]
Professor, Department of ECE, Jawaharlal Nehru Technological University, Ananthpuramu, India

***Abstract*—Nowadays digital media has reached the general level of resource sharing system and become a convenient way for sharing lots of information among various individuals. However, these digital data are stored and shared over an internet which is an entirely unsecured and most frequently attacked by several attackers, resulting in a massive loss at various parameters and creates severe issues of copyright protection, ownership protection, authentication, secure communication, etc. In recent years, digital watermarking technology has received extensive attention from users and researchers for content protection and digital data authentication. However, before implementing digital watermarking techniques in practical applications, there are still many problems that need to be solved technically and efficiently. The purpose of this manuscript is to provide a detailed survey on current research techniques of digital watermarking techniques for all media formats with their applications and operational process. The prime objective of this manuscript is to reveal the research problem and the efficient requirement to implement robust watermarking technique after analyzing the progress of watermarking schemes and current research trend.**

***Keywords*—Authentication; copyright-protection; digital information; digital watermark; robustness, security**

I. Introduction

The emerging trends in digital computing and network technologies have become an area of research interest owing to its potential and vast applicability. The increasing growth of digital technology provides massive scope for development and sharing of digital data information over an open platform. The term ‘open platform' refers to internet services which provide the data sharing facilities effortlessly and cost-effectively. The internet has explored a comprehensive means of entertainment, social interaction, scientific work, education, business and lot more in the form of electronic publishing, real-time delivery, web pages, transaction processing, audio, and video communication. However, this growth of technology has created various challenging issues such as copyright and some other security problems for both user & the provider. Most of the time owner of the data is not aware that the data is being used illegally by some unauthorized persons. The internet is a wide accessing and open communication medium where the digital data can be quickly interrupted for malicious purpose and also can be attacked by different kinds of unwanted attempts during the data distribution process over the internet networks. One such type of attack is Modification where anyone can insert or delete content from the data. Piracy, this is the act of copying the contents of the original digital data and distributing the file without the permission of the content owner. The copyright protection for the digital-data has turned into a severe issue. For reliable communication process, the security of the digital data is the prime concern [1]. Traditionally various methods such as cryptographic, steganography and their combinational approaches were used for preserving the digital information secure, but these all methods have its limitation to handle which mainly work on the nature of application type in which the digital data is being used and modified. To resolve the problem of the traditional techniques, [2][3] researchers have come up with the concept of digital signatures and digital watermarking which increases the security by providing integrity and confidentiality properties to digital-data and protects the content from the unauthorized access. The digital signature and Watermarking techniques are quite similar to each other. A digital signature is used for validating the authenticity of the digital data content, and it can be performed into an encrypted form or in the signed hash value of data characteristic. However, the digital signature has its limitation, i.e., it can identify the changes made in the digital data, but it cannot find the region where the data has been altered. The digital watermarking technique is introduced to provide some additional features which overcome the limitation and issues of digital signature method [4] [5].

A Digital watermarking (DWM) is a class of information hiding technique which is designed to recognize the identity of content owners by embedding some impalpable signals like sound, pictures, and videos into the digital-data content [6]. The watermarking technique serves to preserve ownership of the digital data content in which the owner uses a private key to embed the watermark to protect the information against tampering and detection attacks. The watermarking technique requirements are application dependent and can be utilized for various purposes such as hiding information, source tracking, broadcast tracking, and also for Copyright protection. Digital watermarking is classified as visible watermarking and invisible watermarking [7-10]. In visible watermarking, the data is embedded into visible water-markers which can be text or labels that refer to the content owner. The invisible

watermarking methodology is used in such a direction where data gets implanted into the invisible form like as in case of audio content. Fig. 1 demonstrates the basic representation of the original image (a) and a watermarked image (b).

Fig. 1. Sample of Watermarking.

Therefore, the current manuscript represents the domain concept of digital watermarking (DWM). The paper focuses on various aspects of digital data watermarking and considers the application of existing technologies in multimedia data formats. The purpose of the present manuscript is specified as follows:

- The purpose of the study is to represent detailed reviews on requirements and applications for the digital watermarking technique for multimedia application;
- To identify the critical trends in the watermarking technique;
- To explore the knowledge about the current development of data hidden technique and the open research challenges.

The flow of the presented manuscript is segregated into various sections as follows: Section II presents a discussion on existing watermarking tools. Section III describes the classification of watermarking schemes. Section IV discusses the fundamentals and application of DWM and its techniques in Section V. Section VI presents the research pattern towards DWM. Section VII carries a brief review of existing research works towards watermarking. The open research problem is discussed in Section VIII followed by the conclusion in Section IX.

II. An Existing Digital Watermarking Tools

Various watermarking tools can be accessed through web services based on data types such as images, text, audio, and video. These tools have a variety of features that allow watermark creation and extraction as well as a modification on the host content or to the watermarked content. Therefore, this section presents different existing tools to provide a secure mechanism to protect the originality of the content by embedding a watermark in it. The following are the few popular tools which are described as below:

A. UMark- Free

It is a free version tool available for both Windows and MAC system. It has five distinct features that allow a user to set watermark in the form of text or logo with customizable features including style, color, font, font size, and also set transparency level according to user interest. The advantage of this tool is that it facilitates batch watermarking that supports processing of 100 photos in one-time execution.

B. Water Marquee-Free

It is an entirely free online tool and does not come with any download option. In this tool, text, and logos are used as watermarks. It also allows the user to configure the font, style, color, and region of the watermark as per the demand of interest. The advantage of this tool is that it supports both Windows and MAC OS. The watermark applied to the content is protected, and users can add up to 5 watermarks at the same time.

C. Alamoon-Paid

It is the premium version of the app with the Professional Edition download option. It provides a powerful watermarking mechanism for digital images and allows users to enhance their images before or after watermarking. It can also perform watermark operations on thousands of images at a time.

D. WatermarkLib-Free

It is also a free version of the watermarking tool with text and logo feature. It supports custom feature with various image formats (JPEG, BMP, PNG, and JPG). It offers robust mechanism with the time stamp and date adding functionality and also supports multi-data processing where the user can upload as many image data at a time for watermarking.

E. VisualWatermark-Free

It can be used both online and on an application. It has several built-in templates and style features and also supports batch watermarking with very high processing and execution speed. Here, the user can apply any form of a watermark on the image and video data. Its advantageous feature is that it ensures users security and privacy.

F. Video Watermark Maker-Paid

It is a paid version video watermarking tool and can be accessed on PC and MAC OS. This tool supports a variety of features that give users the flexibility to add watermarks to their videos using custom support and batch processing features. Here, users can create their watermarks and set the interval at which watermark appears.

G. Digital Audio Watermarking-Free

This is a free audio watermarking tool available only for windows platform working with MatLab software. This tool offers a robust watermark mechanism with good custom feature support for the digital audio file format.

H. JACO Watermark Tool-Free

It provides an effective user interface for image watermarking with lots of custom features.

I. TSR Watermark-Paid

It is a simple user-interactive watermarking tool which has robust protection mechanism; once the image is watermarked, it is challenging to remove. It enables batch processing feature

for performing a watermarking operation on several images with a single click.

III. Classification of Watermarking

This section discusses variants of the digital-watermarking scheme based on a variety of information and various parameters.

A. Classification of Digital Watermarking based on Applications

- *Intellectual-property-rights protection:* In this watermarking operation is performed for copyright protection, piracy tracking, finger-printing and to express knowledge about the content owners and their IP rights [11].
- *Data hiding:* Here watermarking techniques are used for secure communication process where the digital data is watermarked into relevant or non-relevant cover.
- *Content verification:* The watermarking is used for ensuring integrity, content verification and to analyze either the digital-data is modified or not and if any modification has made then it locates the region.

B. Classification of Digital Watermarking According to Human Perception

- *Visible watermark:* The Watermark is noticeable through eyes such as watermark label or stamping on paper, or logo on any individual product.
- *Invisible watermark:* In this, the watermark label is performed through the computational mechanism and is not noticeable to the human eye. This approach does not prevent the data from getting stolen, but it allows the owner to claim that he is the authorized person of the data that was attacked [12].

C. Classification of Digital Watermarking based on Characteristics

- *Fragile:* A fragile watermark is a marker which is destroyed when the data gets altered via linear or non-linear transformation concept. It is used for image authentication temper detection and integrity protection [13].
- *Semi-fragile:* Semi-fragile watermarks are used to tackle some common types of image attacks, and quality degradation factors [14].

D. Classification of Digital Watermarking According to the Domain

- *Spatial domain:* In this, the bits of the watermark get inserted to the pixels of the cover image. The embedded signal of the watermark can be damaged without difficulty or eliminated by signal processing attacks because it is effortless to analyze the structure of the spatial domain by performing mathematical modeling and analysis [15].
- *Frequency domain:* Here, the embedding of the watermark signal is performed using the modified image coefficients based on the image transformation. The frequency domain-based watermarking scheme offers a robust and efficient secure mechanism against image processing attacks.

IV. Basic Approaches of Digital Watermarking

This section discusses the fundamental concept of Digital Watermarking along with architectural description with scope and advantages.

In the area of digital-multimedia applications, watermarking is a significant method mainly utilized to hide the content of the data or file (i.e., text, picture, audio or video file format). The hidden information contains data with a carrier signal (ΔSignal), i.e. IP [16]. The digital watermarking includes the concepts and theories of stochastic and probability, signal processing, networking, cryptography, and other approaches. The digital watermarking embed the copyright data into the multimedia format information with the help of specific algorithms. The multimedia information could be in a symbolic format, special characters or serial number and other formats. The function of a given approach is to serve secure communication, owner authentication and integrity of data files [17]. The watermarking method is a particular representation of multimedia files security. A digital watermark is a pattern or digital signature which gets implanted into digital information. It can also call as digital-signature. The watermarking keyword comes from the hidden link used to write secure information. The benefit of this approach is that attackers can never decimate the embedded watermark information into the data. The embedded watermark cannot remove until cover information is unusable. Initially, there are four types of watermarking methods such as 1) Public, 2) Fragile, 3) Visible and 4) Invisible. The digital watermarking life cycle levels are shown below.

A. Life-Cycle of Digital Watermarking (DWM)

The embedded information in a signal is familiar as a "Digital Watermark" while in some theories the Digital Watermark called the difference between the cover and watermarked signal. The place at which the watermark is hidden is identified as a host-signal. The process of watermarking will be carried out into three different phases; Embedding (Ef), Attacking (A) and Identifying Retrieval (IR) operation is shown in below Fig. 2.

- *Embedding Function (E_f):* It is an algorithmic approach which takes the data or information and the host to be embedded and generates a watermarked signal.
- *Attacking Operation (A):* The digital signal is transmitted from one person to another person, or it is stored. If this person changes the embedded files, it is called "Attack." The attack generates from piracy prevention application, where attackers try to remove or delete watermark through the transformation process. Some transformation schemes like cropping pictures or video files, lossy compression or deliberately adding noise.

- *IR Operation:* This is also an algorithmic approach which is used to get rid of the watermark from the attacked signal. When the signal is unchanged during transmission, then the digital watermark still present or it may be removed. The IR algorithm should be capable of generating the digital watermark appropriately, even if the transformation were substantial in the robust watermarking application. In Fragile watermarking technique, the IR algorithmic approach would fail if any modification formed to the signal.

B. Procedural Architecture of DWM

Fig. 3 exhibits the formulation of the watermarking process where the raw image data is processed into the covered image to get digitally watermarked image. For originality authentication and content verification, a suitable algorithmic approach is used as shown in Fig. 2 where the input takes an original picture and after that embeds a secret key into the original image. Then the result shows a digitally watermarked image.

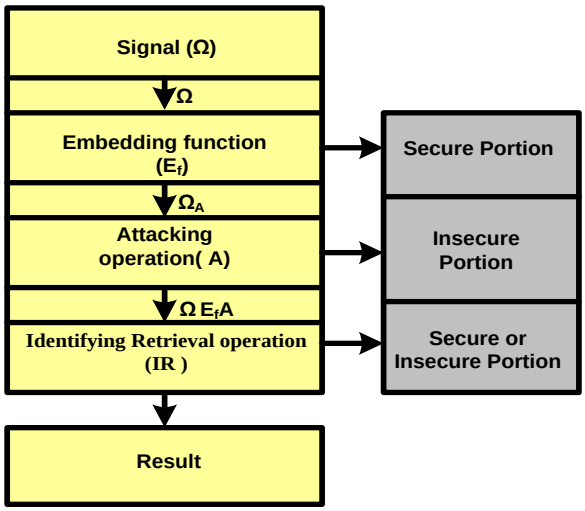


Fig. 2. Life Cycle of Digital Watermarking [18].

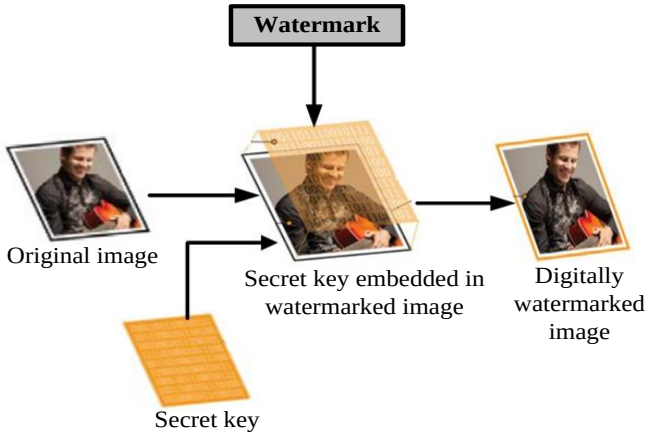


Fig. 3. Basic structure of Digital Watermarking.

C. Flow Process of DWM

The watermark process contains two essential modules which are as discussed as follows:

- *Embedding:* In this, the watermarking is achieved at the source end. The watermark inserts into the original picture by the use of a secret key. The systematic process of Embedding watermark segment is shown in Fig. 4 [19].
- *Detection and Extraction:* In this, the detection and extraction method are used to define whether the information consists in a particular watermark or the DWM can be removed. The watermark detection and extraction are shown below in Fig. 5.

D. Applications of DWM

The Digital watermarks are useful in various applications which are discussed as follows [20] [21]:

- *Broadcast Monitoring:* The broadcast application provides an active role for detecting unauthorized broadcast station. The broadcast monitoring can identify whether the information is broadcasted or not.
- *Copyright Security:* The copyright information implanted in a network as a watermark. The provided copyright information is beneficial in case of any controversy in product ownership. It can deliver as proof.
- *Secret Communication:* The secret communication communicates embedded messages within pictures securely. In this process, the invisible information should not increase any suspicion when a secure signal is being transmitted.

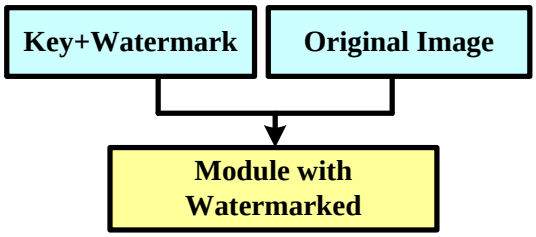


Fig. 4. Watermark Embedded Module.

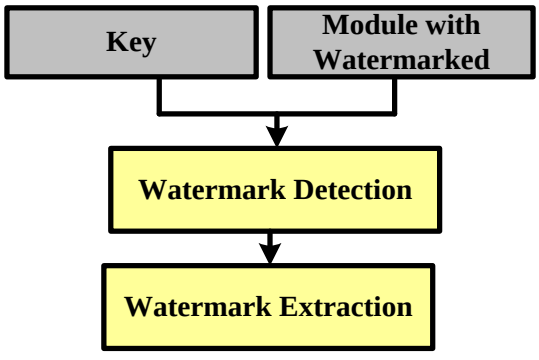


Fig. 5. Watermark Ddetection and Extraction.

- *Content Description:* This watermark consist of some comprehensive data of the host picture like captioning and labeling. For that type of application, the capacity of watermark should be quite large.
- *Fingerprinting:* The fingerprint approaches are exclusive to the owner of digital data. It also provides the facility to notify when a prohibited copy appears. In fingerprinting application, every copy of the work is recognized uniquely.
- *Authentication:* The data authentication is capable of identifying any modification in digital data. It can complete the process by the use of the semi-fragile or fragile watermark, which has the low robustness to change in a picture. It contains two approaches: Fragile and robust watermarking.
- *Airline Traffic Monitoring:* The airline monitoring provides communication between the pilots with the ground monitoring system through end to end voice communication on a specific frequency.
- *Medical application:* The unique name of the patient can be written on MRI or X-Ray report with the help of watermark. It is an essential application to avoid misplacement of the patient report which is critical in treatment.
- *Content Filtering:* Nowadays people want to watch serials, videos or movies in their location and time. The propagation of Set Top Boxes (STB) in homes proof of this, as people want to watch their content on demand. The STB is a useful device which provides various services.

E. Classifications of Different Types of Digital Watermarking Attacks

The different types of DWM attacks are divided into four categories which are illustrated below in Fig. 6 [22];

- *Removal Attacks:* The primary goal of the removal attacks is complete removal of the unique watermark signal without trying to break the watermark algorithm security. This category contains quantization, de-noising, collusion, and re-modulation attacks. All of these techniques, seldom come close to their destiny of complete watermark signal removing, but they never destruct the watermark signal information.

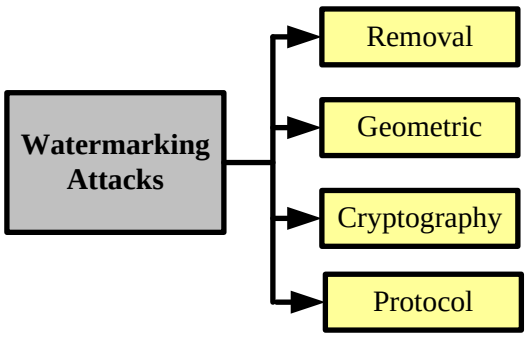


Fig. 6. Types of Watermarking Attacks.

- *Geometric Attacks:* It doesn't remove the embedded sign of watermark but intends to change or distort the watermark detector with the inserted information. The detector could retrieve the added information when active synchronization is getting back. In spite of present watermarking techniques, the information survives these attacks with the help of unique synchronization methods.
- *Cryptography Attacks:* The Cryptography attack attempts to crack the security technique in watermarking methods and thus search a way to delete the inserted watermark content or information. The brute-force method is used for finding the embedded secret information. In this attack, one more sub-category comes which is called Oracle attack. The Oracle attack helps to generate non-watermarked information when a detector device of the watermark is available. The applications of cryptography stacks are limited because of its computational difficulties.
- *Protocol Attacks:* In the protocol attack, the intruder subtracts his watermark sign from the embedded information and claims to be the actual owner of the embedded data. A signal-dependent watermark is generated to avoid this problem with the help of one-way functions. The one more protocol attack is Copy Attack. In copy attack, the aim is not to dissipate the embedded watermark but to assess watermark from the embedded watermarked information and copy it to target data. The signal-dependent watermarks may obstruct the copy attack.

V. Digital Watermarking Techniques

Security and privacy are the essential concerns in the current digital computing world. Millions of data bits are transformed from one place to another place via internet access. The main concern for the transmitter is the reliability of the data file being forwarded securely to its destination. The only authorized user should decrypt the data file. For that reason, steganography and watermarking are the two critical techniques which are mainly responsible for the transmission of data in a secured by hiding the data information in any other digital file format.

Steganography is the technique which hides the textual information in image or text format whereas the watermarking method hides the data in the digital data file, i.e., watermarking hides the digital file behind the other data (e.g., image, video or audio data). In this approach, both source image, as well as hidden images, has the highest preference. This technique is highly secure as the data information is encrypted more accurately in image format. In the following subsection, four important watermarking methods are discussed:

A. Text Watermarking (TWM)

"Text watermarking" is a technique to protect the integrity and authenticity of the text data by inserting a watermark into a text file. It ensures that a text file carries a hidden or secret data content which contains all the copyright information [23]. For the protection of such material, it is essential in solving the difficulty of duplicating unauthorized access, and security.

Various researchers have found different approaches to address this kind of problems. In the process of text watermarking, the first system will discriminate content that has to hide the data information regarding sign or sentence. Here, the information is not embedded with existing information instead of it the information is covered by misleading data information. If the watermark is in the correct format, then it can be removed by retyping the whole text using the new format. Specifically, this approach is utilized for embedding data information into document files which have been used for an extensive duration by secret services.

B. Classification Map for Text Watermarking

Fig. 7 represents the classification map for TWM, which is classified based on the techniques and attacks. There are different types of methods used, i.e., image-based approach, text content, structural based approach, hybrid approach, and an object-based approach.

Furthermore, the text-content based approach is divided into the semantic and syntactic approach. Similarly, the structurally based approach is classified as text, line and word-shift coding. These methods apply to the bitmap of a page image or format data file of a document. Among these methods, the line-shift approach is easily defeated, but it is highly robust in the presence of noise.

C. Flow Process of TWM

The working process of Text watermarking is shown in Fig. 8. Initially, the text watermarking system removes all the inappropriate elements from the original file then sentence preprocessor forward that content for a watermarking process. The system then uses the syntactic tool list, WordNet and dictionary and generates the proper watermarked sentence with the help of secret-key [24].

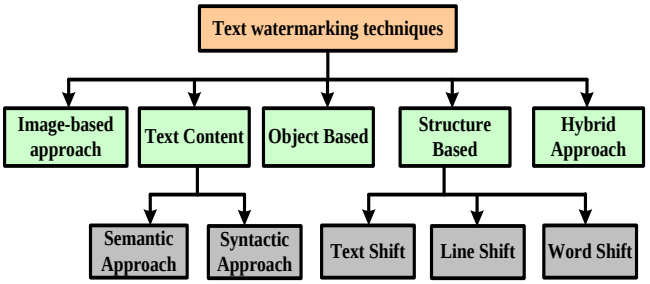


Fig. 7. Classification Map for Text Watermarking.

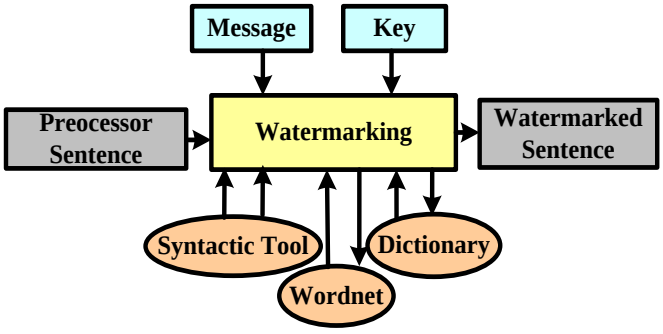


Fig. 8. The Working Process of TWM.

D. Digital Image Watermarking (DIWM)

Most of the watermarking scheme is focused on images. The reason behind that is there is a high demand for image watermarking because of so many images are freely available at World Wide Web which needs to be protected. A watermark is an identifying pattern or design in the paper that may have shades of darkness or lightness. It is viewed by transmitting the light that appears as different shades of lightness/darkness when looked by transmitted light. Image watermarks have been used on currency, stamps and other government documents. The dandy roll process and cylinder mould process are the two main ways of producing image watermarks in the paper. An example of DIWM is given in Fig. 9.

E. The Process of Digital Image Watermarking

Fig. 10 represents the schematic process flow of DIWM technique. In this, the system considered the original image with the removal of unwanted data and forwarded it to DCT (Discrete Cosine Transform) [25]. Here, the system contains the usable hidden information which then embedded with DCT coefficients. The purpose of choosing DCT is that the block transformer can calculate efficiently and also for image-compression. The watermark embedder and detector have to select at same points for further processing. Using sorting and embedded algorithm system generates the watermarked image using PN sequence & secret-key [26]. The original size of the image IDCT (Inverse Discrete Cosine Transform) is used.

The above section discussed the text and image watermarking methodology. Similarly, in a digital data security system, audio and video watermarking mechanisms are an also important method, which allows embedding the data information with the same optimized length of audio or video. It is also responsible for enhancing the quality level of audio/video up to a great extent. Thus, in the next sections, a detailed study is carried out for two of the most important watermarking techniques, i.e., Audio Watermarking and Video Watermarking.

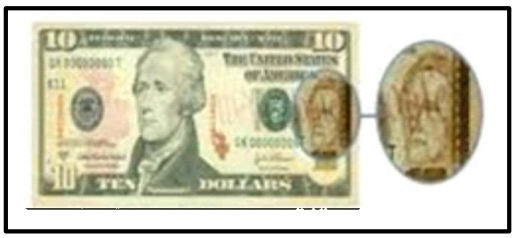


Fig. 9. Example of DIWM.

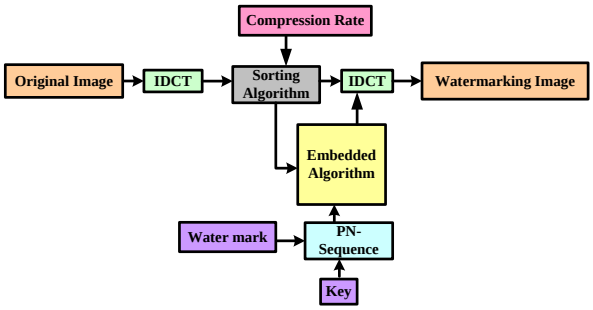


Fig. 10. Schematic Representation of DIWM Process.

F. Digital Audio Watermarking (DAWM)

The representation of digitally copyrighted audio-data, for example, radio songs, telephone calls, air-traffic communication and call recordings, etc. provides several opportunities and applications over the analog system. Therefore, audio editing is a straightforward approach, since a person can access the exact locations that should be changed and replicate it very easy with no loss of fidelity. In the current scenario, digital audio files are commonly transmitted over several social websites with a quick and inexpensive medium. This kind of development results from unauthorized access provided by the digital techniques, specifically highly scaled unauthorized replicating, downloading, and distributing medium over the multimedia channels. As a result, the significance of authenticity, data verification, authorized replication, and data security in digital audio files has become a problem. These challenges have encouraged the researchers to implement an efficient technique to secure the copyrights messages in digital audios to protect forgery and impersonation. The DAWM is the process of converting audio-signals into embed message which could be identified or extracted later to create an assertion about actual audio being communicated is the host signal, and the watermark offers an additional knowledge about the host signal [27]. Examples of digital audio data are: songs are the most applicable to copyright the data because of conditions attached to it.

G. Classifications of DAWM

Several audio watermarking methods have been introduced, which are mainly classified into three categories (as given in Fig. 11) like 1) Temporal domain, 2) Frequency domain, and 3) Coded domain.

It is found that the DAWM is relatively lower in percentage compared with image and video watermarking method owing to the sensitivity of HAS (i.e., human auditory system). Additionally, an amount of data which is implanted into the digital audio file is lesser than image/video files, because audio signals are single dimensional signals.

H. Module Design of DAWM System

The typical module design of DAWM system contains two significant sub-modules; 1) Embedding module and 2) Recovery module also named as Extractor. The schematic view of DAWM scheme is shown in below Fig. 12.

First, the system inserts the watermark information into an audio signal via the embedding module, and then the recovery module extracts or predicts the watermarked information as presented in the processing scheme. In a few systems, the prediction can be made with the availability of real signal called Non-Blind detection [28]. Generally, there are two significant watermarking embedding schemes based on time domain and transformation domain. Currently, engineers have been utilizing a combined approach to increases the robustness of DAWM algorithms. Time domain approach was an initial watermarking method introduced by researchers. In the temporal domain, watermark file is embedded directly with host file (i.e., audio) by changing attributes or inserting pseudo-random noise pattern into an audio file. Transform domain audio watermarking scheme works on a frequency domain, which considers the characteristics of HAS system and embeds the inaudible watermark data into digital audio signals. Transformation of audio files from time-to-frequency domain enables the system to integrate the watermark file into perceptually significant components which offer the efficient watermark system with high-level of in-audibleness and robustness.

I. Applications of DAWM

Copyright defense applications have been the brainchild behind the audio watermarking. Some useful applications like; broadcast-monitoring and fingerprinting are rapidly increasing in demand for audio watermarking. Nowadays, DAWM scheme has considered a new dimension, which is mainly utilized to stop music writers from piracy or to leak the audio copies on the internet or other sites. Audio watermarking has been used to prevent the audio plagiarism which presents a severe threat to the music industries to generate profits. In music studios, watermarks are utilized in sounds track of theatrical releases, and when plagiarized recording appears it is easy to determine place, date and time of its creation. Such type of watermark will assure the modification that has made. Nowadays, watermarks are integrated in such a way that it functions similar to the telephonic system where identification of caller gets confirmed.

J. Digital Video Water Marking (DVWM)

It is a series of video files that contains a sequence of consecutive & equal time spaced images. Therefore, the primary method of watermarking is simple for images and videos. The image watermarking technique can be directly applied to video watermarking. There are lots of things in image watermarking which is also applicable to videos. However, such methods are highly suitable for utilizing watermarking, e.g. the, increasing digital versatile disk (i.e., DVD) standard which contains the copyright prevention system. The initial objective is to mark the copyrighted video files (i.e., DVDs, recorders) and refuses to record pirated digital files. The classification of DVWM is given in Fig. 13.

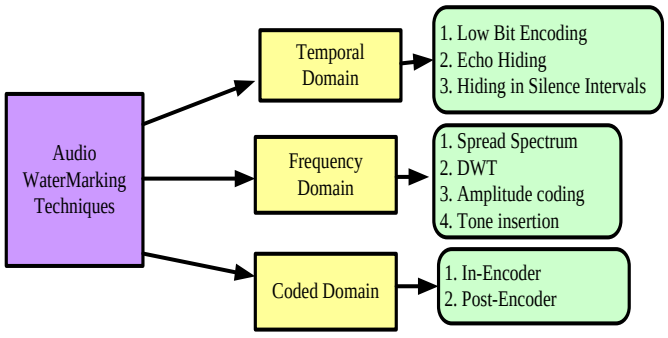


Fig. 11. Classifications of Audio Watermarking Methods.

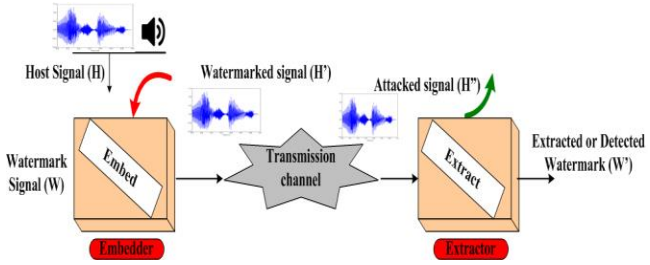


Fig. 12. Schematic Views of DAWM Scheme.

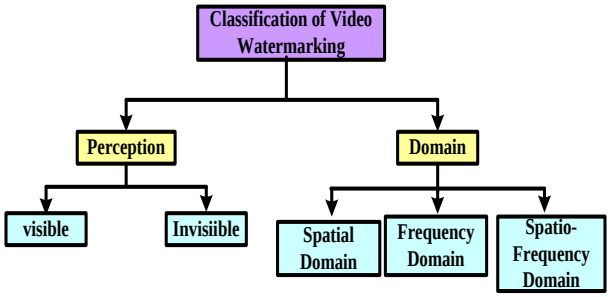


Fig. 13. Classification Map for DVWM Techniques.

K. Classification of DVWM

However, based on the working domain, the DVWM techniques are categorized as 1) Spatial-Domain, 2) Frequency-Domain and 3) Format-Specific. That is those classification based on watermarking algorithms according to the type of video, considering motion sensitivity and type of embedding domain. The following figure schematically represents the classification of DVWM based on working domain [29].

L. Spatial Domain Digital Video Watermarking

The spatial domain DVWM is a simple approach which is able to embed the watermark with host-signal by modifying the pixel rates of actual video. This approach is nearly associated to frequency domain approach which contains lower computational complexity. This scheme has low-pass filtering, low robustness and less resistance to noise.

M. LSB Modification

"Least Significant Bit" modification technique is utilized to add a watermark into LSB pixels which are allocated in the image vicinity counter. That is watermark is embedded by changing the lower range bits of every single pixel. The overall payload of LSB is very low and restricted.

N. Correlation-Based Method

It is another form of watermarking embedding technique which uses the correlation attributes of pseudo-random noise-patterns (PRNP), and those attributes are adding with the luminance of video pixel values. Basically, PRNP is 2-D signals and transformed into the DCT domain, the generated new bit value is compared with the initial value and based on bit value, the original DCT block is elected.

O. Frequency Domain Digital Video Watermarking

The frequency domain is an alternative process of spatial-domain. In this water, the mark is spread out over the image, and it is very complex to be removed after embedding. The major drawback of this approach requires higher computation. But it is more secure, robust and efficient compared to another domain.

P. Discrete Fourier Transformation (DFT)

The primary purpose of this DFT technique is to search the frame to be watermarked and calculates the magnitude coefficients. In this process, watermark image is embedded only into the first frame of video sequence frame by modifying the positions of DFT coefficients. This technique is more reliable than DCT. Additionally, it allows us to exploit more energy watermarks in places where HVS is to be low sensitive.

Q. Discrete Cosine Transformation (DCT)

The DCT method allows an image file to be split up into several frequency bands and making it easier to be embed watermark image into middle-frequency bands. The frequency of middle bands is selected and ignores the low-frequency image parts without overexposing which removes the noisy threats and compression. The DCT watermarking approach is highly robust to lossy-compression.

R. SVD Watermarking Method

SVD (i.e., Singular Value Decomposition) is a numerical approach which is specifically exploiting to obtain zed-matrix diagonal elements from the original matrix. In this watermarking approach, a single image is taken as matrix and decomposed by SVD into three different matrices (like X, Y, and Z) and transpose into an orthogonal matrix. The SVD watermarking method adds the watermark data into singular values of the diagonal matrix to meet the requirement of imperceptibility and robustness of digital watermarking algorithms.

S. Format-Specific Video Watermarking

It is an MPEG based watermarking method which uses the MPEG -1, -2 and -4 coding procedure in terms of primitive components which are initially motivated for embedding watermarking and compression to minimize the complexity of live video processing. The most prominent drawback of this method totally depends upon MPEG coding which could be more susceptible to recompression with other attributes.

T. Detection and Extraction Process

The following Fig. 14 illustrates about the overall process of detection of video watermark file. In the initial step, a sample testifying video file is divided into video and audio frames, and watermarks are responsible for extracting the audio and video frames separately by watermark extraction.

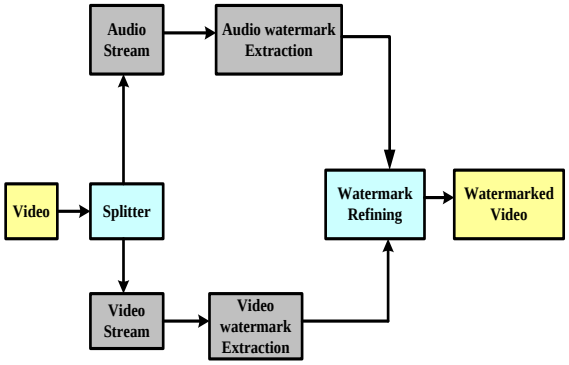


Fig. 14. Flow Process of Video Watermarking.

After the watermark extraction, the extracted file is undergoing for refining operation. The video frame is processed to obtain video-watermark. During this phase, image scene modifies are detected from sample tested video file, and every single video frame is transformed into discrete wavelet domain with four-levels. After the extraction and refining of the watermark, the user can contrast the outcome files with referenced watermark file. Finally, the system will generate the resultant watermark video file.

U. Application of DVWM

Some significant applications of digital video watermarking over different domain are briefly explained as below [30]:

1) Finger-printing policy: There are mainly two kinds of video streaming applications such as 1) Pay-Per-View and 2) Video on Demand. In such a video streaming application, the fingerprinting technique is utilized for video watermarking. Through finger-printing of any user's information which is an image or video file and can easily detect that user over the worldwide if they are breaking the policy.

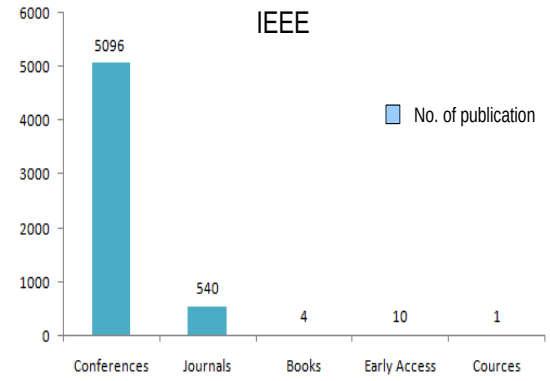
2) Authentication of the video file: From the authentication, can save the watermark signature into a header file, but header file still is a leak to tempering. So that the system can easily embed this kind of authentication video data directly as a watermark.

3) Content or copyrights prevention: Content or copyright prevention is an essential application is video watermarking approach. To detect the real content owner in watermarking for copyright prevention on the internet.

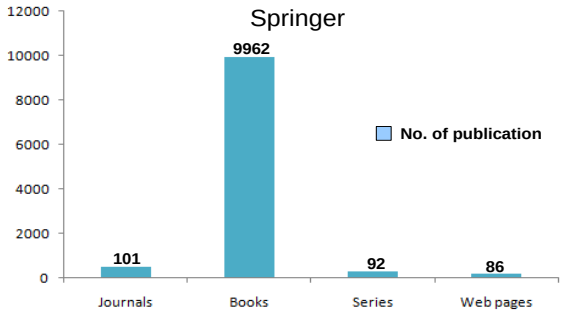
4) Monitoring of broadcast video files: Broadcasting is mainly related to the television world where numerous types of videos, images and other broadcast products are there. In the watermarking process, the system put the watermark on every single video sequence.

VI. Research Pattern

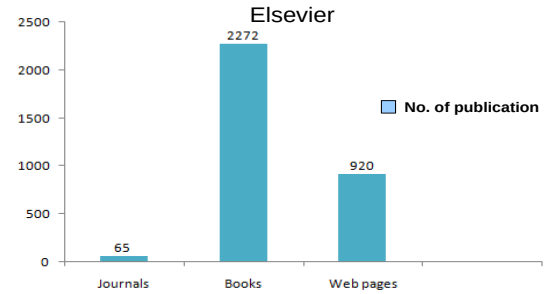
The digital watermarking has been evolved very progressively, and we find that there are more than 5,000 research publications are available till date that focuses on the digital watermarking. Thus, Fig. 15 shows the research trends of digital watermarking from three different popular publications.



(a) Number of Total Publication form IEEE.



(b) Number of Total Publication form Springer.



(c) Number of Total Publications from Elsevier.

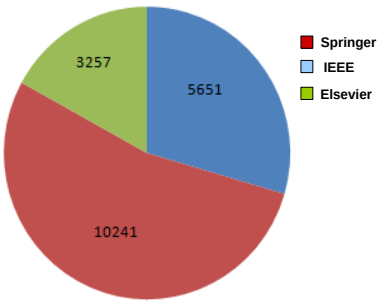


Fig. 15. (d) Analysis of IEEE, Springer, and Elsevier.

VII. Existing Research Studies Carried in Domain Digital Watermarking

This section presents a summarized review of last 5 years existing research works i.e from 2013 to 2018 towards addressing the privacy issue of digital content and ownership authentication issue. There are also lots of research efforts that have been made to provide an efficient solution for content and ownership protection. Therefore, Table 1 represents a brief review of digital watermarking research works in tabular form.

TABLE I. SUMMARIZED REVIEW REPRESENTATION OF EXISTING WORKS

Author	Problem	Methodology	Result
Xiang and He [31]	Content privacy in the cloud database	Authentication algorithm based on watermarking scheme	Achieves efficient preserving capacity to keep data content safe in the cloud
Liu et al. [32]	Copyright and piracy problem	fractal encoding method and the discrete cosine transform	Obtains robustness and effective property for copyright protection
Mohanty et al. [33]	The biomedical image communication process	Hardware architecture with the compression algorithm	Good performance in compression quality
Kamaruddin et al. [34]	Security issues in text watermarking	Model for evaluating the watermarking technique	Point out requirements for text watermarking technique
Shehab et al. [35]	Unsecured image authentication for the medical application	Singular value decomposition and a least significant bit	Achieves high accuracy in temper detection and recovery of the original image
Ishtiaq et al. [36]	Image distortion	Reversible watermarking and predictor concept	Lower distortion of the watermarked image
Liang et al. [37]	Big Data utilization and data protection	Carried a survey on the life cycle of data and data trading	Reveal challenges in big data lifecycle
Su et al. [38]	Software protection	Mathematical model	Achieves good performance than traditional methods in terms of software protection
Zhaofeng Ma [39]	Content copying issue	digital rights management Security Infrastructure	Provides a flexible solution to control content copying
Ahmaderaghi et al. [40]	Issues of payload and imperceptibility in blind image watermarking	Discrete Shearlet Transformation	Achieves windowing flexibility
Hou et al. [41]	The gray image in Reversible Data Hiding	Unchanged gray version	Obtains Reversibility and invariance
Hua et al. [42]	Security issues in the linear system	Greedy algorithms and the random matching pursuit	Performs forward and inverse transforms before and after watermark embedding
Nie et al. [43]	Limitation of feature points distribution	quantization of local feature and global feature point based on Laplacian matrix and unsupervised learning approach	obtains good performance under common Alteration
Guo et al. [44]	Identification of colorized Image	Histogram and Feature Encoding for Fake Colorized Image identification	Achieves higher performance in detecting Colorized Image then existing approach
Amanpour and Ghaemmaghami [45]	Detecting Localization of tampering and recovery of original content	content Reconstruction algorithm	Efficiency in reconstruction property about 67% with improved quality
Wang et al. [46]	Design issue of spread spectrum watermarking method	Secure spherical watermarking technique	Obtains robustness property
Guo et al. [47]	Impractical performance of error diffusion-based halftone visual watermarking approach (EDHVW)	An improved model of EDHVW	Achieves superior performances in terms of data content security
Chen et al. [48]	The issue of copyright protection and image content integrity	Matrix factorization technique	Tackle various attacks and modification
Su et al. [49]	The issue of balancing between robustness and imperceptibility in audio marking method	optimization model with binary search algorithm and heuristic Search algorithm	Maintains a good balance between imperceptibility and robustness and provides copyright protection.
Amini et al. [50]	Limited watermarking design using hidden Markov model	Vector-based hidden Markov watermarking model	Robustness and can resist various attacks
Chang and Shen [51]	To improve blind watermarking methods.	Features Classification Forest (FCF)	Larger capacity, robust, more practical.
Hou et al. [52]	Low content protection.	Blind 3D mesh watermarking, Blind estimation algorithm.	Dose, not a loose embedded pattern.

Iftikhar et al. [53]	To increase data recovery.	Reversible watermarking method, decoding mechanism, a formal specification architecture.	Robust, actual data retrieval after decoding.
Imran et al. [54]	Tampering in digital audio.	Copy-move Forgery detection (CFD) system.	Doesn't need any threshold to make decisions, low detection error.
Mohanty et al. [55]	Watermarking mechanism,	Comparative analysis with steganography.	Insight into different watermarking approaches.
Parikh et al. [56]	Medical image compression.	High-Efficiency Video Coding (HEVC)	Enhance compression performance, low complexity.
Sengupta et al. [57]	Piracy and un-authorized claim of ownership.	Seven-variable signature encoding.	Cost reduction, low delay and minimal hardware in the embedding process.
Xie et al. [58]	Channel capacity.	No Methodology.	Investigational approach.
Piper and Safavi-Naini [59]	Image authentication.	Scalable Fragile Watermarking (SFW) algorithm.	Protects data, provide security against attackers.
Golestani and Ghanbari [60]	Side effect minimization in image.	Structural Similarity Index (SSI) model.	Low computational complexity.
Hamghalam et al. [61]	Theoretical analysis.	Robust picture Watermarking (RPW) method based on geometric modeling.	High robustness.
Su et al. [62]	Geometricla transformations.	Feature-based Digital Picture Watermarking (FDPW) method.	More effective against intruders, signal detection efficiency.
Zareian and tohidypour [63]	Scaling and rotation attack.	Quantisation Index Modulation (QIM) technique.	Optimal performance.
Khalili and Asatrayan [64]	Ownership authentication, image authentication.	Code Division Multiple Access (CDMA) method.	More imperceptibility, robustness, and security.
Coatrieux et al. [65]	Identifying medical picture integrity.	Integrity Control (IC) system, L1 or L2-Signatures.	Detect picture tampering.
Vargas and Vera [66]	To implement the watermark for still pictures.	Reversible Information-hiding (RI) algorithm.	Provide more Security, adding metadata and integrity control.
Coatrieux et al. [67]	To detect watermarked in image pixels.	Dynamic Prediction Error Histogram Shifting (DPEHS) method and Pixel Histogram Shifting (PHS) technique.	In lower distortion can add more data and can get PSNR about 1-2 decibel (dB) greater.
Naskar and Chakraborty [68]	To modify the cover picture components.	Histogram-bin-Shifting (HS) based reversible watermarking algorithm.	High embedding capacity with minimum distortion.
Walia and Suneja [69]	Authentication of medical pictures.	Spatial Domain Watermarking (SDW) method based on Weber's law.	Highly imperceptible, increase capacity for high-contrast pictures.
Bian and Liang [70]	To detect the embedded image watermark.	Locally Optimum-Bessel K Form (LO-BKF) Model.	More appropriate, provide effective performance in the weak strength of watermark.

VIII. Open Research Issues in Digital Watermarking Approach

Digital watermarking is still a highly popular topic among the researchers where it is observed that issue related to image security was given much priority in existing research work. The existing watermarking techniques have been mainly concentrated on the protecting content of the image for secure communication, privacy preservation, and content ownership protection, etc. By surveying existing research work it has been analyzed that there are extremely few efforts have been made that considers video and audio watermarking schemes. Though the presented manuscript also discusses a few popular existing watermarking tools and there we observed that very few watermarking tools have good supportability features which are not cost effective. Tools available for video and audio watermarks do not appear to be sufficient to provide advanced security mechanisms for video content protection. Majority of the research work that has focused on securing image and text digital data suffers from cost complexity, computational complexity and robust security mechanism against geometric attacks. The followings are some points that will reflect more loopholes in existing digital watermarking schemes. The existing research works have not considered other types of attacks such as watermark hiding attacks, ad hoc attacks, random geometric transformations attacks, etc. Therefore, researchers should also focus on other types of attacks and their possible solution because efficient security mechanism against these attacks plays a crucial role act to protecting content from being stolen and misuse. Till now there are few issues and approaches that have been raised in concern of practical watermarking implementation for the full copyright protection. However, this is probably the most important problem in the watermarking field.

Digital video watermarking (DVWM) mechanism introduces some challenges which are not yet presented in image watermarking. Owing to the massive amount of data and redundancy among video frames, video signals are more susceptible to plagiarize attacks, containing frame dropping, swapping, and statistical analysis.

Exploiting fixed image watermark scheme to individual frame in video stream leads a challenge of handling statistical invisibility. Applying fixed and independent watermark on each video frame is also a big challenge for the researchers.

DVWM approaches must not exploit the original video frame during the detection of the watermark as the video normally is large and it is an inconvenience to save it twice. Thus, to solve such problem researchers should try to introduce a new digital watermarking approach.

- Basically, there are four performance parameters, has to consider for the computation and evaluation of the performance of a data hiding system such as computational cost, robustness/security, invisibility, and payload. Based on these performance parameters it can be analyzed that few of watermarking scheme is less efficient than others.
- Robust and secure watermarking methods are expected to support several kinds of attacks. Image-compression, cropping, rescaling, and low-pass filtering are the types of watermark attacks which are not addressed in the prior research studies.
- Most watermarking methods were developed with the purpose of information hiding within large data patterns. Despite this, the discussion and work of watermarking using digital file compression techniques are rare. Digital images/videos are continuously transmitted or uploaded over the World Wide Web in a compressed format. Developing the ability to incorporate watermarking schemes into digital image/video compression technology is also one of the challenging tasks that the researchers are facing.
- With the development of more and more watermarking algorithms, an unbiased benchmarking technique is required to evaluate the effectiveness of different techniques from special viewpoints, including robustness, quality, clarity, and computational complexity. However, there is very little work towards developing an effective benchmarking system. Therefore, more research efforts are required for performing a complete watermark effectiveness assessment process.

IX. Conclusion

The image processing attacks and piracy problems on digital media are a big concern, and it is reasonable to expect that it will grow more as many digital data travels over the internet, and as the technology advances. Therefore, digital watermarking has become a vibrant topic of the research area in recent years. In this paper, we have surveyed existing research efforts and watermarking tools that were designed to secure and address the problem related to data content from piracy and content ownership. However, it is found that there is a considerable gap between the practical implementation of watermarking tools and the approach given in the existing system. After reviewing the existing works of literature, it can be analyzed that further research into effective watermarking schemes is needed, which has received less attention in video and audio digital formats. Although digital images and text data have good numbers of research techniques, there is still a lack of optimization methods on it. The study also found that watermark designed for image integrity, content originality and ownership authentication needs to be enhanced. A benchmarking platform is required to measure the overall performance of new upcoming watermark techniques. Finally, future work should put more concern on all the digital formats and bring some innovative, cost-effective and secure mechanism.

References

[1] Panchal UH, Srivastava R. A comprehensive survey on digital image watermarking techniques. InCommunication Systems and Network Technologies (CSNT), 2015 Fifth International Conference on 2015 Apr 4 (pp. 591-595). IEEE.

[2] Jiang Xuehua,―Digital Watermarking and Its Application in Image Copyright Protection‖, 2010 International Conference on Intelligent Computation Technology and Automation

[3] C. H. Lu, Multimedia Security: Steganography and Digital Watermarking Techniques for Protection of Intellectual Property. Hershey, PA: Idea Group Publishing, 2005

[4] S. P. Mohanty. (2012, May 22). ISWAR: An imaging system with watermarking and attack resilience. [Online]. Available: https://arxiv.org/ pdf/1205.4489.pdf

[5] G. Voyatzis and I. Pitas, "The use of watermarks in the protection of digital multimedia products," Proc. IEEE, vol. 87, no. 7, pp. 1197–1207, July 1999.

[6] Cox I, Miller M, Bloom J, Fridrich J, Kalker T (2008) Digital Watermarking and Steganography Second Edition. Elsevier, 2008

[7] Rakesh Ahuja, S. S. Bedi,‖ All Aspects of Digital Video Watermarking Under an Umbrella‖, Ijigsp, Vol 12, Pp 54-73, 2015 [8] T.R. Singh, "Image Watermarking Scheme based on Visual Cryptography in Discrete Wavelet Transform," International Journal of Computer Applications, vol. 39, pp. 18-24, 2012.

[8] R. Jain and J. Boaddh, "Advances in digital image steganography," 2016 International Conference on Innovation and Challenges in Cyber Security (ICICCS-INBUSH), Noida, 2016, pp. 163-171.

[9] Cox, Ingemar, et al. Digital watermarking and steganography. Morgan Kaufmann, 2007.

[10] Macq, Benoît, Patrice Rondao Alface, and Mireia Montanola. "Applicability of watermarking for intellectual property rights protection in a 3D printing scenario." Proceedings of the 20th International Conference on 3D Web Technology. ACM, 2015.

[11] T. M. Thanh and P. T. Hiep, "Frame background influence based invisible watermarking to visible video watermarking," 2013 International Conference on Advanced Technologies for Communications (ATC 2013), Ho Chi Minh City, 2013, pp. 563-568.

[12] W. C. Ku, T. C. Chou, H. L. Wu, and J. C. Chang, "A Fragile Watermarking Scheme for Image Authentication with Tamper Detection and Localization," 2010 Fourth International Conference on Genetic and Evolutionary Computing, Shenzhen, 2010, pp. 638-641.

[13] K. L. Prasad, T. C. M. Rao and V. Kannan, "A Hybrid Semi-fragile Image Watermarking Technique Using SVD-BND Scheme for Tampering Detection with Dual Authentication," 2016 IEEE 6th International Conference on Advanced Computing (IACC), Bhimavaram, 2016, pp. 517-523.

[14] Boreiry, Mahsa, and Mohammad-Reza Keyvanpour. "Classification of watermarking methods based on watermarking approaches." Artificial Intelligence and Robotics (IRANOPEN), 2017. IEEE, 2017.

[15] "Digital Watermarking", https://www.cl.cam.ac.uk/teaching/0910/R08/work/essay-ma485-watermarking.pdf, Retrieved on 09th Nov, 2018

[16] Xuehua, Jiang. "Digital watermarking and its application in image copyright protection." Intelligent Computation Technology and Automation (ICICTA), 2010 International Conference on. Vol. 2. IEEE, 2010.

[17] "Digital watermarking", http://adigitalwatermarking.blogspot.in/2011/08/digital-watermarking-life-cycle-phases.html, Retrieved on 09th Nov, 2018

[18] Singh, Prabhishek, and R. S. Chadha. "A survey of digital watermarking techniques, applications and attacks." International Journal of Engineering and Innovative Technology (IJEIT) 2.9 (2013): 165-175.

[19] Rashid, Aaqib. "Digital Watermarking Applications and Techniques: A Brief Review." International Journal of Computer Applications Technology and Research 5.3 (2016): 147-150.

[20] S. Liu, K. Yue, H. Yang, L. Liu, X. Duan and T. Guo, "Digital watermarking technology and its application in information security," 2017 IEEE 3rd Information Technology and Mechatronics Engineering Conference (ITOEC), Chongqing, 2017, pp. 786-789.

[21] S. Kumar and A. Dutta, "A study on the robustness of block entropy based digital image watermarking techniques concerning various attacks," 2016 IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), Bangalore, 2016, pp. 1802-1806.

[22] N. S. Kamaruddin, A. Kamsin, L. Y. Por and H. Rahman, "A Review of Text Watermarking: Theory, Methods, and Applications," in IEEE Access, vol. 6, pp. 8011-8028, 2018.

[23] S. G. Rizzo, F. Bertini, and D. Montesi, "Text Authorship Verification through Watermarking," 2016 European Intelligence and Security Informatics Conference (EISIC), Uppsala, 2016, pp. 168-171.

[24] M. Islam, G. Mallikharjunudu, A. S. Parmar, A. Kumar, and R. H. Laskar, "SVM regression based robust image watermarking technique in the joint DWT-DCT domain," 2017 International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT), Kerala State,Kannur, India, 2017, pp. 1426-1433.

[25] P. C. Su, Y. C. Chang and C. Y. Wu, "Geometrically Resilient Digital Image Watermarking by Using Interest Point Extraction and Extended Pilot Signals," in IEEE Transactions on Information Forensics and Security, vol. 8, no. 12, pp. 1897-1908, Dec. 2013.

[26] B. A. F. Agradriya, F. K. Perdana, I. Safitri and L. Novamizanti, "Audio watermarking technique based on Arnold transform," 2017 2nd International Conference on Automation, Cognitive Science, Optics, Micro Electro-Mechanical System, and Information Technology (ICACOMIT), Jakarta,

[27] Olanrewaju, R. F., and Othman Khalifa. "Digital audio watermarking; techniques and applications." Computer and Communication Engineering (ICCCE), 2012 International Conference on. IEEE, 2012.

[28] Rini T Paul, "Review of Robust Video Watermarking Techniques," IJCA Special Issue on "Computational Science - New Dimensions & Perspectives" NCCSE, 2011

[29] M. A. Gangarde and J. S. Chitode, "Application of the crypto-video watermarking technique to improve robustness and imperceptibility of secret data," 2017 Fourth International Conference on Image Information Processing (ICIIP), Shimla, 2017, pp. 1-6.

[30] Xiang, Shijun, and Jiayong He. "Database authentication watermarking scheme in encrypted domain." IET Information Security (2017).

[31] Liu, Shuai, Zheng Pan, and Housbing Song. "Digital image watermarking method based on DCT and fractal encoding." IET Image Processing 11.10 (2017): 815-821.

[32] Mohanty, Saraju P., Elias Kougianos, and Parthasarathy Guturu. "SBPG: Secure Better Portable Graphics for Trustworthy Media Communications in the IoT." IEEE Access6 (2018): 5939-5953.

[33] Kamaruddin, Nurul Shamimi, et al. "A Review of Text Watermarking: Theory, Methods, and Applications." IEEE Access 6 (2018): 8011-8028.

[34] Shehab, Abdulaziz, et al. "Secure and Robust Fragile Watermarking Scheme for Medical Images." IEEE Access 6 (2018): 10269-10278.

[35] Ishtiaq, M. U. H. A. M. M. A. D., et al. "Hybrid predictor based four-phase adaptive reversible watermarking." IEEE Access(2018).

[36] Liang, Fan, et al. "A Survey on Big Data Market: Pricing, Trading, and Protection." IEEE Access (2018).

[37] Su, Qing, et al. "A Method for Construction of Software Protection Technology Application Sequence based on Petri Net with Inhibitor Arcs." IEEE Access (2018).

[38] Ma, Zhaofeng. "Digital rights management: Model, technology, and application." China Communications 14.6 (2017): 156-167.

[39] Ahmaderaghi, Baharak, et al. "Blind Image Watermark Detection Algorithm based on Discrete Shearlet Transform Using Statistical Decision Theory." IEEE Transactions on Computational Imaging (2018).

[40] Hou, Dongdong, et al. "Reversible Data Hiding in Color Image with Grayscale Invariance." IEEE Transactions on Circuits and Systems for Video Technology (2018).

[41] Hua, Guang, et al. "Random Matching Pursuit for Image Watermarking." IEEE Transactions on Circuits and Systems for Video Technology (2018).

[42] Nie, Xiushan, et al. "Robust Image Fingerprinting Based on Feature Point Relationship Mining." IEEE Transactions on Information Forensics and Security (2018).

[43] Guo, Yuanfang, et al. "Fake Colorized Image Detection." arXiv preprint arXiv:1801.02768 (2018).

[44] Amanipour, Vahideh, and Shahrokh Ghaemmaghami. "Video-Tampering Detection and Content Reconstruction via Self-Embedding." IEEE Transactions on Instrumentation and Measurement 67.3 (2018): 505-515.

[45] Wang, Yuan-Gen, Guopu Zhu, and Yun-Qing Shi. "Transportation spherical watermarking." IEEE Transactions on Image Processing 27.4 (2018): 2063-2077.

[46] Guo, Yuanfang, et al. "Halftone Image Watermarking by Content Aware Double-sided Embedding Error Diffusion." IEEE Transactions on Image Processing (2018).

[47] Chen, Zigang, et al. "A novel digital watermarking based on General non-negative matrix factorization." IEEE Transactions on Multimedia (2018).

[48] Su, Zhaopin, et al. "SNR-Constrained Heuristics for Optimizing the Scaling Parameter of Robust Audio Watermarking." IEEE Transactions on Multimedia (2018).

[49] Amini, Marzieh, M. Ahmad, and M. Swamy. "A robust multibit multiplicative watermark decoder using vector-based hidden Markov model in Wavelet Domain." IEEE Transactions on Circuits and Systems for Video Technology (2016).

[50] Chang, Chia-Sung, and Jau-JiShen. "Features classification Forest: a novel development that is adaptable to robust blind watermarking techniques." IEEE Transactions on Image Processing 26.8 (2017): 3921-3935.

[51] Hou, Jong-Uk, Do-Gon Kim, and Heung-Kyu Lee. "Blind 3D Mesh Watermarking for 3D Printed Model by Analyzing Layering Artifact." IEEE Transactions on Information Forensics and Security 12.11 (2017): 2712-2725.

[52] Iftikhar, Saman, et al. "A reversible watermarking technique for social network data sets for enabling data trust in cyber, physical, and social computing." IEEE Systems Journal 11.1 (2017): 197-206.

[53] Imran, Muhammad, et al. "Blind detection of copy-move forgery in digital audio forensics." IEEE Access 5 (2017): 12843-12855.

[54] Mohanty, Saraju P., et al. "Everything You Want to Know About Watermarking."

[55] Parikh, Saurin S., et al. "High Bit-Depth Medical Image Compression with HEVC." IEEE Journal of biomedical and health informatics 22.2 (2018): 552-560.

[56] Sengupta, Anirban, Dipanjan Roy, and Saraju P. Mohanty. "Triple-Phase Watermarking for Reusable IP Core Protection During

Architecture Synthesis." IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems37.4 (2018): 742-755.

[57] Xie, Xu, ZhengguangXu, and HuiXie. "Channel Capacity Analysis of Spread Spectrum Watermarking in Radio Frequency Signals." IEEE Access 5 (2017): 14749-14756.

[58] A. Piper and R. Safavi-Naini, "Scalable fragile watermarking for image authentication," in IET Information Security, vol. 7, no. 4, pp. 300-311, December 2013.

[59] H. B. Golestani and M. Ghanbari, "Minimisation of image watermarking side effects through subjective optimization," in IET Image Processing, vol. 7, no. 8, pp. 733-741, November 2013.

[60] M. Hamghalam, S. Mirzakuchaki, and M. A. Akhaee, "Robust image watermarking using dihedral angle based on the maximum-likelihood detector," in IET Image Processing, vol. 7, no. 5, pp. 451-463, July 2013.

[61] P. C. Su, Y. C. Chang and C. Y. Wu, "Geometrically Resilient Digital Image Watermarking by Using Interest Point Extraction and Extended Pilot Signals," in IEEE Transactions on Information Forensics and Security, vol. 8, no. 12, pp. 1897-1908, Dec. 2013

[62] M. Zareian and H. R. Tohidypour, "Robust quantization index modulation-based approach for image watermarking," in IET Image Processing, vol. 7, no. 5, pp. 432-441, July 2013

[63] M. Khalili and D. Asatryan, "Colour spaces effects on improved discrete wavelet transform-based digital image watermarking using Arnold transform map," in IET Signal Processing, vol. 7, no. 3, pp. 177-187, May 2013

[64] G. Coatrieux, H. Huang, H. Shu, L. Luo and C. Roux, "A Watermarking-Based Medical Image Integrity Control System and an Image Moment Signature for Tampering Characterization," in IEEE Journal of Biomedical and Health Informatics, vol. 17, no. 6, pp. 1057-1067, Nov. 2013

[65] L. Vargas and E. Vera, "An Implementation of Reversible Watermarking for Still Images," in IEEE Latin America Transactions, vol. 11, no. 1, pp. 54-59, Feb. 2013.

[66] G. Coatrieux, W. Pan, N. Cuppens-Boulahia, F. Cuppens and C. Roux, "Reversible Watermarking Based on Invariant Image Classification and Dynamic Histogram Shifting," in IEEE Transactions on Information Forensics and Security, vol. 8, no. 1, pp. 111-120, Jan. 2013

[67] R. Naskar and R. S. Chakraborty, "Histogram-bin-shifting-based reversible watermarking for color images," in IET Image Processing, vol. 7, no. 2, pp. 99-110, March 2013

[68] E. Walia and A. Suneja, "Fragile and blind watermarking technique based on Weber's law for medical image authentication," in IET Computer Vision, vol. 7, no. 1, pp. 9-19, February 2013

[69] Y. Bian and S. Liang, "Locally Optimal Detection of Image Watermarks in the Wavelet Domain Using Bessel K Form Distribution," in IEEE Transactions on Image Processing, vol. 22, no. 6, pp. 2372-2384, June 2013