iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 4 **Issue:** X **Month of publication:** October 2016

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

A Review on Digital Watermarking, its features, need and various techniques

Manjushree A.Shete[1], Prof.V.S.Kolkure[2]
[1]PG Student of Electronics Department of, B.I.G.C.E., Solapur, Maharashtra, India
[2]Prof. of Electronics Department of, B.I.G.C.E., Solapur, Maharashtra, India

Abstract –The advent of the Internet has resulted in many new opportunities for the creation and delivery of content in digital form. Applications include electronic advertising, real time video and audio delivery, digital repositories and libraries, and Web publishing. An important issue that arises in these applications is the protection of the rights of all participants. Sometimes current copyright laws are not enough for dealing with digital data protection. This has led to an interest towards developing new copy protection techniques. One of such technique is digital watermarking techniques. Digital watermarking is the process of embedding information into digital multimedia content such that the information (which we call the watermark) can later be extracted or detected for a variety of purposes including copy prevention and security. Digital watermarking is the act of hiding a message related to a digital signal (i.e. an image, song, video) within the signal itself. It is a concept closely related to steganography, in that they both hide a message inside a digital signal. However, what separates them is their goal. Watermarking tries to hide a message related to the actual content of the digital signal, while in steganography the digital signal has no relation to the message, and it is merely used as a cover to hide its existence. This paper includes watermarking definition concept and various methods of watermarking process. It starts with overview, techniques, application, challenges and limitations of watermarking.
Keywords: Watermarking, Encryption, Multimedia protection, Digital Watermarking

I. INTRODUCTION

Digital watermarking is the process of adding identifying data -- such as a sequence of characters or code to digital content such as text, images, films, music and software programs. There are two types of digital watermarks: those that are perceptible to the human eye or ear, and those that are imperceptible. Both need to be able to survive intact without affecting the quality of the content during compression and decompression, encryption and decryption, and while it's being used. A watermark is typically used to identify either the originator or authorized user, state usage rights, verify the authenticity or integrity of the data, or control its use and distribution. The Digital Watermarking Alliance, an international group of leading organizations, promotes the advantages of digital watermarking to content owners, industries, policy makers and consumers.

Traditional watermarks, such as those on banknotes, are only perceptible under certain conditions and are difficult to remove. The problem with digital watermarks is that any digital process can be reversed. There is also a problem known as the analog hole: content has to be in analog form for humans to see or hear it, but once digital content is put into analog form, it's no longer protected and can be converted back into digital format, allowing unauthorized copying and redistribution.

Despite these shortcomings, digital watermarking is being used for source tracking. This is where each recipient gets content with its own unique watermark. A watermark embedded into content at each point of distribution can be retrieved from the copy and the source of the distribution can be checked. While watermarks cannot prevent illegal activity, they can alert someone if they receive or access illegally copied or distributed content. It is far from a perfect science, though. False positives often occur when watermarked data is legally restored to a replacement device, or when key files are corrupted or removed by anti-spyware tools.

In terms of a watermark ensuring data is of little value to attackers if stolen, the only type of watermark that would work is a perceptible one, such as big red text over a digital image, a PDF document saying copyrighted material, or a hiss recorded throughout the soundtrack of a video or music file. However, this approach clearly affects the quality of the data and renders the files of little use to the legal owner. So until watermarking techniques are developed that are robust enough to prevent removal, encryption remains the best approach to protecting data.

II. OBJECTIVES

A. To study the basic concept Digital Watermarking System.

B. To study Digital watermarking classifications.
C. To study features of Digital watermarking.
D. Requirements of digital watermarking.
E. To study various techniques of digital watermarking.
F. To study applications of digital watermarking.
G. To take guidelines from these study to analyze best watermarking technique for digital watermarking.

III.DIGITAL WATERMARKING

As an emerging technology, digital watermarking involves the ideas and theories of different subject coverage, such as signal processing, cryptography, probability theory and stochastic theory, network technology, algorithm design, and other techniques [3]. Digital watermarking hides the copyright information into the digital data through certain algorithm. The secret information to be embedded can be some text, author‘s serial number, company logo, images with some special importance. This secret information is embedded to the digital data (images, audio, and video) to ensure the security, data authentication, identification of owner and copyright protection. The watermark can be hidden in the digital data either visibly or invisibly. For a strong watermark embedding, a good watermarking technique is needed to be applied. Watermark can be embedded either in spatial or frequency domain. Both the domains are different and have their own pros and cons and are used in different scenario.

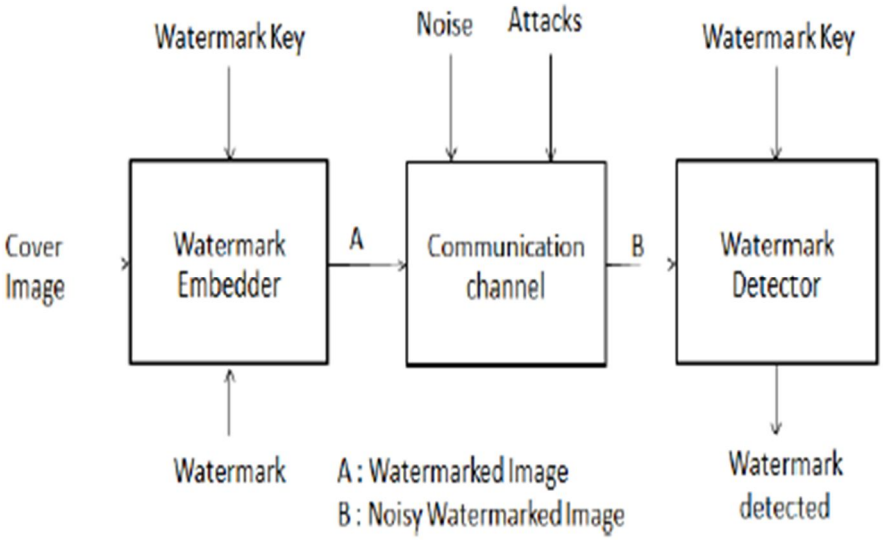


Fig.1 Digital Watermarking process

Simple Digital watermarking is a technology in which a watermark (secret information) is hidden in the digital media using an appropriate algorithm for the authentication and identification of original owner of the product. Outcome we get is watermarked image. Simple digital watermarking technique consists of two modules watermark embedding module and watermark detection and extraction module. Watermark embedding embeds the watermark into the original image using a key. Watermark detection and extraction module is used to determine whether the data contains specified watermark or the watermark can be extracted.

IV. DIGITAL WATERMARKING CLASSIFICATION

A. According to characteristics/robustness

1) *Robust:* Robustness watermarking is mainly used to sign copyright information of the digital works, the embedded watermark can resist the common edit processing, image processing and lossy compression, and the watermark is not destroyed after some attack and can still be detected to provide certification. It resists various attacks, geometrical or non-geometrical without affecting embedded watermark.
2) *Fragile:* Fragile watermarking is mainly used for integrity protection, which must be very sensitive to the changes of signal. We can determine whether the data has been tampered according to the state of fragile watermarking.
3) *Semi fragile:* Semi fragile watermarking is capable of tolerating some degree of the change to a watermarked image, such as the

addition of quantization noise from lossy compression.

B. According to attached media/host signal

1) *Image watermarking:* This is used to hide the special information into the image and to later detect and extract that special information for the author‘s ownership.
2) *Video watermarking:* This adds watermark in the video stream to control video applications. It is the extension of image watermarking. This method requires real time extraction and robustness for compression.
3) *Audio watermarking:* This application area is one of the most popular and hot issue due to internet music, MP3.
4) *Text watermarking:* This adds watermark to the PDF, DOC and other text file to prevent the changes made to text. The watermark is inserted in the font shape and the space between characters and line spaces.
5) *Graphic watermarking:* It embeds the watermark to 2D or 3D computer generated graphics to indicate the copyright.

C. According to perceptivity

1) *Visible watermark:* The watermark that is visible in the digital data like stamping a watermark on paper, (ex.) television channels, like HBO, whose logo is visibly superimposed on the corner of the TV picture.
2) *Invisible watermarking:* There is technology available which can insert information into an image which cannot be seen, but can be interrogated with the right software. You can‘t prevent the theft of your images this way, but you can prove that the image that was stolen was yours, which is almost as good.

D. According to its purpose

1) *Copyright protection watermarking:* This means if the owner want others to see the mark of the image watermark, then the watermark can be seen after adding the watermark to the image, and the watermark still exists even if it is attacked.
2) *Tampering tip watermarking:* It protects the integrity of the image content, labels the modified content and resists the usual lossy compression formats.
3) *Anti-counterfeiting watermarking:* It is added to the building process of the paper notes and can be detected after printing, scanning, and other processes.
4) *Anonymous mark watermarking:* It can hide important annotation of confidential data and restrict the illegal users to get confidential data.

E. According to watermark type

1) *Noise type:* Noise type has pseudo noise, Gaussian random and chaotic sequences.
2) *Image type:* There are binary image, stamp, logo and label.

F. According to domain

1) *Spatial domain:* This domain focuses on modifying the pixels of one or two randomly selected subsets of images. It directly loads the raw data into the image pixels. Some of its algorithms are LSB, SSM Modulation based technique.
2) *Frequency domain:* This technique is also called transform domain. Values of certain frequencies are altered from their original. There are several common used transform domain methods, such as DCT, DWT, and DFT.

G. According to detection process

1) *Visual watermarking:* It needs the original data in the testing course, it has stronger robustness, but its application is limited.
2) *Semi blind watermarking:* It does not require an original media for detection.
3) *Blind watermarking: It* does not need original data, which has wide application field, but requires a higher watermark technology.

V. FEATURES OF DIGITAL WATERMARKING

A. Following features of watermarking

1) *Robustness:* Robustness refers to that the watermark embedded in data has the ability of surviving after a variety of processing

operations and attacks. Then, the watermark must be robust for general signal processing operation, geometric transformation and malicious attack.

2) *Imperceptibility:* Watermark cannot be seen by human eye or not be heard by human ear, only be detected through special processing or dedicated circuits. It can be detected by an authorized agency only. Such watermarks are used for content or author authentication and for detecting unauthorized copier.
3) *Security:* A watermark system is said to be secure, if the hacker cannot remove the watermark without having full knowledge of embedding algorithm, detector and composition of watermark. A watermark should only be accessible by authorized parties. This requirement is regarded as a security and the watermark is usually achieved by the use of cryptographic keys. Watermark information owns the unique correct sign to identify, only the authorized users can legally detect, extract and even modify the watermark, and thus be able to achieve the purpose of copyright protection.
4) *Verifiability:* Watermark should be able to provide full and reliable evidence for the ownership of copyright-protected information products. It can be used to determine whether the object is to be protected and monitor the spread of the data being protected, identify the authenticity, and control illegal copying.
5) *Capacity and data payload:* Capacity of the watermarking system is defined as the maximum amount of information that can be embedded in the cover work. The number of watermark bits in a message in data payload and the maximum repetition of data payload within an image is the watermark capacity. Depending on the application some watermarking methods require a data payload exceeding 10,000 bits. A watermark may have high data capacity but low data payload.
6) *Computational cost:* In order to reduce computational cost, a watermarking method should be less complex. Watermarking methods with high complex algorithms will require more software as well as hardware resources and thus incur more computational cost. Computational simplicity usually preferred in resource-limited environments like mobile devices.

B. Requirements of digital watermarking

There are following requirements of Digital Watermarking:

1) *Robustness:* Robustness means Resistance to ―blind‖, non-targeted modifications, or common media operations. For manipulation recognition the watermark has to be fragile to detect altered media. There are two major problems when trying to guaranty robustness; the watermark must be still present in the media after the transformation or it must be still possible for the watermark detector to detect it.
2) *Security:* Security describes whether the embedded watermarking information cannot be removed beyond reliable detection by targeted attacks based on a full knowledge of the embedding algorithm and the detector, except the key, and the knowledge of at least one watermarked data. Watermarking security implies that the watermark should be difficult to remove or alter without damaging the host signal. As all watermarking systems seek to protect watermark information, without loss of generality, watermarking security can be regarded as the ability to assure secrecy and integrity of the watermark information, and resist malicious attacks.
3) *Capacity:* Capacity describes how many information bits can be embedded. It addresses also the possibility of embedding multiple watermarks in one document in parallel. Capacity requirement always struggle against two other important requirements, that is, imperceptibility and robustness.
4) *Imperceptibility:* The watermark should not be noticeable to the viewer nor should the watermark degrade the quality of the content. The term ―imperceptible‖ is widely used in this case. However, if a signal is truly imperceptible, then perceptually based lossy compression algorithms either introduce further modifications that jointly exceed the visibility threshold or remove such a signal, Gonzalez and Woods (2008). It is then important to develop techniques that can be used to add imperceptible or unnoticeable watermark signals in perceptually significant regions to counter the effects of signal processing.
5) *Modification and Multiple Watermarks:* Changing a watermark can be accomplished by either removing the first watermark or then adding a new one, or Inserting a second watermark. The first alternative goes against the principle of tamper resistance, because it implies that a watermark is easily removable. Allowing multiple watermarks to coexist is the preferred solution. There is however security problem related to the use of multiple watermarks. The basis of watermarking security should lie on Kirchhoff‘s assumption that one should assume that the method used to encrypt the data is known to the unauthorized party. It means that watermarking security can be interpreted as encryption security leading directly to the principle that it must lie mainly in the choice of the embedded key. Allows insertion of multiple, independently detectable watermarks in an Image.

VI. DIFFERENT WATERMARKING TECHNIQUES

A. Spatial domain

Spatial domain digital watermarking algorithms directly load the raw data into the original image. Spatial watermarking can also be applied using color separation. In this way, the watermark appears in only one of the color bands. This renders the watermark visibly subtle such that it is difficult to detect under regular viewing. Spatial domain is manipulating or changing an image representing an object in space to enhance the image for a given application. Techniques are based on direct manipulation of pixels in an image [10]. Some of its main algorithms are as discussed below:

B. Additive Watermarking

The most straightforward method for embedding the watermark in spatial domain is to add pseudo random noise pattern to the intensity of image pixels. The noise signal is usually integers like (-1, 0, 1) or sometimes floating point numbers. To ensure that the watermark can be detected, the noise is generated by a key, such that the correlation between the numbers of different keys will be very low.

C. Least Significant Bit

Old popular technique embeds the watermark in the LSB of pixels. This method is easy to implement and does not generate serious distortion to the image; however, it is not very robust against attacks. The embedding of the watermark is performed choosing a subset of image pixels and substituting the least significant bit of each of the chosen pixels with watermark bits. The watermark may be spread throughout the image or may be in the select locations of the image. But these primitive techniques are vulnerable to attacks and the watermark can be easily destroyed. Such an approach is very sensitive to noise and common signal processing and cannot be used in practical applications.

D. Frequency domain

Compared to spatial-domain methods, frequency-domain methods are more widely applied. The aim is to embed the watermarks in the spectral coefficients of the image. The most commonly used transforms are the Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), Discrete Wavelet Transform (DWT), the reason for watermarking in the frequency domain is that the characteristics of the human visual system (HVS) are better captured by the spectral coefficients. Some of its main algorithms are discussed below:

E. Discrete cosine transforms (DCT)

DCT like a Fourier Transform, it represents data in terms of frequency space rather than an amplitude space. This is useful because that corresponds more to the way humans perceive light, so that the part that are not perceived can be identified and thrown away. DCT based watermarking techniques are robust compared to spatial domain techniques. Such algorithms are robust against simple image processing operations like low pass filtering, brightness and contrast adjustment, blurring etc. However, they are difficult to implement and are computationally more expensive. At the same time they are weak against geometric attacks like rotation, scaling, cropping etc. DCT domain watermarking can be classified into Global DCT watermarking and Block based DCT watermarking. Embedding in the perceptually significant portion of the image has its own advantages because most compression schemes remove the perceptually insignificant portion of the image. Steps in DCT Block Based Watermarking Algorithm 1) Segment the image into non-overlapping blocks of 8x8 2) Apply forward DCT to each of these blocks 3) Apply some block selection criteria (e.g. HVS) 4) Apply coefficient selection criteria (e.g. highest) 5) Embed watermark by modifying the selected coefficients. 6) Apply inverse DCT transform on each block

F. Discrete wavelet transforms (DWT)

Wavelet Transform is a modern technique frequently used in digital image processing, compression, watermarking etc. The transforms are based on small waves, called wavelet, of varying frequency and limited duration. The wavelet transform decomposes the image into three spatial directions, i.e. horizontal, vertical and diagonal. Hence wavelets reflect the anisotropic properties of HVS more precisely. Magnitude of DWT coefficients is larger in the lowest bands (LL) at each level of decomposition and is smaller for other bands (HH, LH, and HL). The Discrete Wavelet Transform (DWT) is currently used in a wide variety of signal processing applications, such as in audio and video compression, removal of noise in audio, and the simulation of wireless antenna distribution. Wavelets have their energy concentrated in time and are well suited for the analysis

of transient, time-varying signals. Since most of the real life signals encountered are time varying in nature, the Wavelet Transform suits many applications very well. One of the main challenges of the watermarking problem is to achieve a better trade off between robustness and perceptivity. Robustness can be achieved by increasing the strength of the embedded watermark, but the visible distortion would be increased as well. However, DWT is much preferred because it provides both a simultaneous spatial localization and a frequency spread of the watermark within the host image. The basic idea of discrete wavelet transform in image process is to multi-differentiated decompose the image into sub-image of different spatial domain and independent frequencies.

VII. APPLICATION OF DIGITAL WATERMARKING

Some important applications of digital watermarking are as below:

A. Copyright protection

Digital watermarking can be used to identify and protect copyright ownership. Digital content can be embedded with watermarks depicting metadata identifying the copyright owners.

B. Copy protection

Digital content can be watermarked to indicate that the digital content cannot be illegally replicated. Devices capable of replication can then detect such watermarks and prevent unauthorized replication of the content.

C. Digital right management

Digital right management (DRM) can be defined as ―the description, identification, trading, protecting, monitoring, and tracking of all forms of usages over tangible and intangible assets‖. It concerns the management of digital rights and the enforcement of rights digitally.

D. Tamper proofing

Digital watermarks which are fragile in nature, can be used for tamper proofing. Digital content can be embedded with fragile watermarks that get destroyed whenever any sort of modification is made to the content. Such watermarks can be used to authenticate the content.

E. Broadcast monitoring

Over the last few years, the number of television and radio channels delivering content has notably expanded. And the amount of content flowing through these media vehicles continues to grow exponentially. In this highly fragmented and fast changing market, knowing the real broadcast reality has become critical for content owners, copyright holders, distributors and broadcasters.

F. Fingerprinting

Fingerprints are the characteristics of an object that tend to distinguish it from other small objects. As in the applications of copyright protection, the watermark for finger printing is used to trace authorized users who violate the license agreement and distribute the copyrighted material illegally. Thus, the information embedded in the content is usually about the customer such as customer's identification number.

G. Access control

Different payment entitles the users to have different privilege (play/copy control) on the object. It is desirable in some systems to have a copy and usage control mechanism to prevent illegal copy of the content or limit the number of times of copying. A robust watermark can be used for such purpose.

H. Medical application

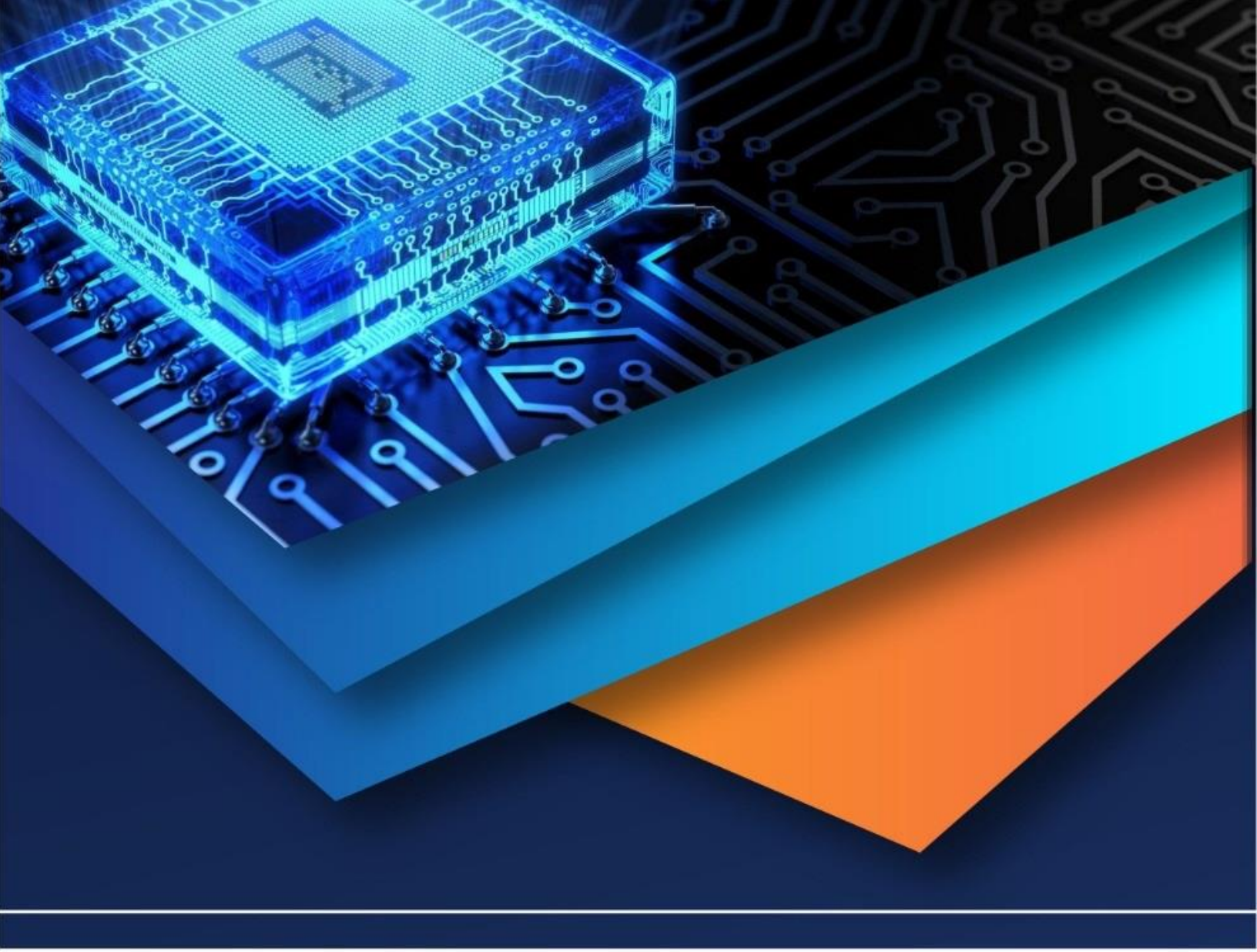
Names of the patients can be printed on the X-ray reports and MRI scans using techniques of visible watermarking. The medical reports play a very important role in the treatment offered to the patient. If there is a mix up in the rep

VIII. CONCLUSION

We have studied need of digital watermarking for multimedia protection and security, its process and different techniques and it's some important application and explored some of the considerations involved. We have tried to establish some guidelines for the analysis of the best digital watermarking technique for respective application.

REFERENCES

[1] R.G. Schyndel, A. Tirkel, and C.F Osborne, ―A Digital Watermark‖, Proceedings of IEEE International conference on Image Processing, ICIP-1994, pp. 86-90, 1994.
[2] Christine I. Podilchuk, Edward J. Delp, ―Digital watermarking: Algorithms and applications‖, IEEE Signal processing Magazine, July 2001.
[3] Jiang Xuehua, ―Digital Watermarking and Its Application in Image Copyright Protection‖, 2010 International Conference on Intelligent Computation Technology and Automation.
[4] Ensaf Hussein, Mohamed A. Belal, ―Digital Watermarking Techniques, Applications and Attacks Applied to Digital Media: A Survey‖, IJERT, ISSN: 2278-0118, Vol. 1 Issue 7, September-2012.
[5] C.-T. Li and F.M. Yang., ―One-dimensional Neighborhood Forming Strategy for Fragile Watermarking‖. In Journal of Electronic Imaging, vol. 12, no. 2, pp. 284-291, 2003.
[6] Rakesh Ahuja, S S Bedi, Himanshu Agarwal, ―A Survey of Digital Watermarking Scheme‖, MIT International Journal of Computer Science and Information Technology, Vol.2, No. 1, Jan. 2012, pp.(52-59)
[7] G. Coatrieux, L. Lecornu, Members, IEEE, Ch. Roux, Fellow, IEEE, B. Sankur, Member, IEEE'‖A Review of digital image watermarking in health care‖.
[8] Edin Muharemagic and Borko Furht ―A Survey of watermarking techniques and applications‖ 2001.
[9] Jahnvi Sen, A.M. Sen, K. Hemachandran,‖ AN ALGORITHM FOR DIGITAL WATERMARKING OF STILL IMAGES FOR COPYRIGHT PROTECTION‖, Jahnvi Sen et al / Indian Journal of Computer Science and Engineering IJCSE).
[10] CHAPTER 2: LITERATURE REVIEW, Source: Internet
[11] http://ippr-practical.blogspot.in
[12] www.scisstudyguides.addr.com
[13] Manpreet kaur, Sonia Jindal, Sunny behal, ―A Study of Digital image watermarking‖, Volume2, Issue 2, Feb 2012.
[14] Evelyn Brannock, Michael Weeks, Robert Harrison, Computer Science Department Georgia State University ―Watermarking with Wavelets: Simplicity Leads to Robustness‖, Southeast on, IEEE, pages 587 – 592, 3-6 April 2008.
[15] D. Kundur, D. Hatzinakos, ―Digital Watermarking for Telltale Tamper Proofing and Authentication‖, in proceeding of the IEEE, (1999), pp. 1167-1180.
[16] G. Bouridane. A, M. K. Ibrahim, ―Digital Image Watermarking Using Balanced Multi wavelets‖, IEEE Transaction on Signal Processing 54(4), (2006), pp. 1519-1536.
[17] Cox, I.J.; Miller, M.L.; Bloom, J.A., ―Digital Watermarking,‖ Morgan Kaufmann, 2001.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY