Journal of Information Systems Engineering and Management
2025, 10(56s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Digital Watermarking Systems: A Study of Resilience and Applications

Leena Amol Deshmukh[1], Dr. Maithili Arjuwadkar[2]
[1]Progressive Education Society's Modern Institute of Business Studies, Nigdi, Pune, Maharashtra India
[2]Progressive Education Society's Modern Institute of Business Studies, Nigdi, Pune, Maharashtra India

ARTICLE INFO

Received: 15 Jan 2025
Revised: 27 Feb 2025
Accepted: 17 Mar 2025

ABSTRACT

In the digital world, security of digital documents is a big challenge. Digital documents can be in any form, like images, word files or PDF. Digital watermark is used to secure copyright ownership. Also, it is used to validate the ownership of the digital document. This paper gives a detailed literature review of digital watermark types and applications. Also enlighten different attacks on digital watermarks.

Keywords: Digital watermark, attacks on digital watermark, Applications

Introduction

With the help of the internet, it is very easy and time saving to send important electronic documents such as identity proof, address proof, bills, and images from one place to another. As the internet is not providing any security to digital content, it is important to provide security to these digital documents. For example, an image in healthcare sector holds significant value in shaping treatment choices. If the image is tempered by an attacker, then there is high risk as the patient's life is in danger. To avoid such situations, security is provided to digital documents.

Authentication, confidentiality, authorization, integrity, accountability, and non-repudiation are criteria for digital document security [1].

As the internet is growing fast, digital content can be reproduced very easily. So, there is a strong need to provide security to digital content. Digital watermark is a solution for content protection.

Digital watermark

Digital watermarking is the branch of information hiding. Digital watermarking is the process of incorporating identification or reorganization information into multimedia content that are readily apparent. It protects the copyright information of the owner. Also, it is used for safeguarding intellectual property rights, recognizing ownership, and ensuring authentication and security of digital content.

As per definition digital watermarking is the process of incorporating digital information known as watermark into in the form of text, image or video on the digital media.

Characteristics of digital watermark

Evaluation of watermark is done based on these characteristics [2][3].

1) **Robustness:** watermark must be robust. Robustness means if there is any attack on watermark, watermark is expected to be intact, and there is no change in watermark data. Integrity of the watermark remains as it is after attending several watermark attacks. Also, if an unauthorized user tries to manipulate the watermark, then the watermark remains unchanged.
2) **Imperceptibility**: Imperceptibility means unnoticed. Watermarks should be hard to detect or it cannot be easily apparent to the viewer. Such a watermark is used for content or owner

Journal of Information Systems Engineering and Management
2025, 10(56s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

authentication. However, digital watermarks are classified as visible and invisible. Visible watermarks are visible to the human eye. Examples are logos used in news channels at the time of broadcasting news. Invisible watermark is helpful for text documents as it can be modified or copied easily. Invisible watermark is not visible easily but it can be extracted using a certain algorithm.

3) **Security:** Digital watermark is said to be secure if watermarked data is unchanged irrespective of various attacks on it. It signifies the ability to prevent any unauthorized manipulation of the digital watermark.
4) **Capacity:** Capacity is stated as the maximum amount information can be inserted into a cover object. Cover objects can be text, image, audio or video.
5) **Verifiability:** Watermark should be able to confirm the ownership of copyright protected information.

Process of Digital Watermark

Digital watermarking is used to hide copyright information into cover media such as text, image, audio or video. If any modification is done with watermark or in case of any attack on watermark or any changes made in the digital data, then this watermarked data is extracted to validate ownership.

Digital Watermark embedding and extracting process is as follows [4].

Digital watermark Embedding Process:

a. Let X is digital data on which digital watermark (W) is embedded.
b. Digital watermark (W) may contain copyright information.
c. Generate key (K) which is required to embed a watermark on digital data.
d. Apply algorithm with key (K) to embed digital watermark (W) on Data (X).
e. The output of successful watermark embedding Process is watermarked data (X`)

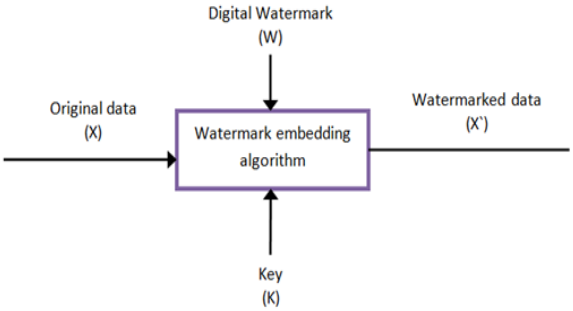

Figure (a): Watermark embedding process

The watermark extraction process is as follows

a. Watermarked data (X`) is input to extract original data and digital watermark
b. Another input is Key (K) of the watermark extraction algorithm.
c. Apply algorithm with key (K)on watermarked data (X`) to get output as Original Data (X) and Digital watermark (W)

Journal of Information Systems Engineering and Management
2025, 10(56s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

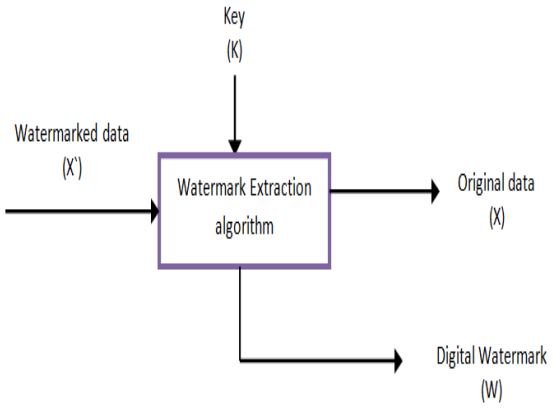

Figure (b): Watermark Extraction process

Digital watermark is grouped into different categories based on their features, type and applications [5] [6][7][8].

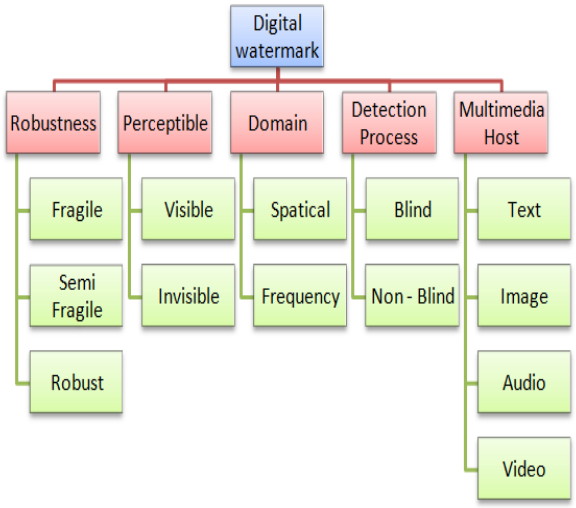

Figure 1 : Classification of Digital Watermarking

Parameter	Watermark and Description
Data for Extraction or Detection Process	**Blind**: These watermarks find out watermarked data without knowing the original signal. Here Original document is not required during watermark extraction. These watermarks are not much robust.
	Informed: To know watermarked data, these watermarks require an original signal. Original document is required during watermark extraction. This type of watermarks more tough to any attack.
Robustnes	**Fragile**: These watermarks are very

Journal of Information Systems Engineering and Management
2025, 10(56s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

s	sensitive. Watermark will be destroyed immediately if any small modification is done with watermark. Such a watermark will be used in authentication and verification of integrity purposes.
	Semi: This type of watermark presents itself like fragile watermark but they are much robust to handle minimal alteration such as adding noise. Such watermarks will use in authentication and tamper control of images.
	Robust: Robust watermark can survive itself after multiple attacks on the watermark. Also, in robust watermark watermarked data is extracted successfully by authorized users though watermark has gone through multiple signals processing to manipulate watermark and watermark attack. Such watermarks will be used for duplication control also known as copy control and e-monitoring purposes.
Perceptivity	**Visible**: Visible watermarks can be clearly visible to the human eye.
	Invisible: Invisible watermark is not visible to the human eye. This type of watermarks is stronger as compared to visible watermark.
Domain	**Spatial**: It is watermarking technique where watermarked data is embedded by modifying pixel value of an image, audio or video.
	Transform: It is watermarking technique where watermarked data is inserted in the frequency domain. For example, Fourier Transform, Discrete Cosine Transform
Host Media	**Text**: In text watermark, Watermark data is embedded into text then it is called Text Watermark.
	Image: Watermarked data is embedded inside image is called image watermark. It is visible or invisible.
	Audio: Watermarked data is embedded inside audio signal is called audio watermark. It is imperceptible to human ear and can store copy right information.
	Video: Video is sequence of images and audio signal. When watermarked data is embedded into video signal, it is called video watermarking.

Table 1: Classification of watermark

Journal of Information Systems Engineering and Management
2025, 10(56s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Applications of Digital Watermark

Digital watermarking is used in various applications [9].

1. **Broadcast monitoring**: The aim of broadcast monitoring is to check when and where content was broadcast via satellite transmission and generate tracking reports for content owners. Here watermark is embedded in content data such as music, video etc. [10].
2. **Copyright protection**: owner`s copyright information is embedded in a digital watermark to prove his ownership. For this, an invisible watermark is used. If there is any controversy or dispute about ownership of the data, this watermarked information is extracted to prove the ownership [11].
3. **Copy Protection**: digital watermark is used to avoid replication of digital content. If an unauthorized user tried to copy digital content, then digital watermark embedded on digital content does not allow making a replica of the same [11].
4. **Medical applications**: Digital watermark is used in the medical field. In this, medical information of patients and other details such as prescriptions, reports is stored in digital format. This document contains digital watermarks either in visible or invisible format. This digital watermark helps doctors and medical applications to verify the authenticity of documents. Here digital watermark ensures that medical documents are not tampered [12].
5. **Fingerprinting:** Fingerprints are used in identification. Watermarking technique is used for fingerprinting. In fingerprinting hidden data is known as fingerprint which is unique and used for identification purposes. For example, a unique watermark is embedded on each license document. When a buyer purchased a copy of a licensed document, a unique watermark owner can identify buyer information. This will help to prevent illegal copying of licensed documents [12].
6. **Captioning**: Captioning means title or explanation. For example, an image with a caption means brief information about the image. Similarly, a watermark is also used as a caption which provides identification information of the owner [12].
7. **Data Authentication**: Authentication is the process of verifying the identity. Data authentication is the process of verifying the identity of data received. Digital watermark is used in the data authentication process. Digital watermark helps to verify data received is original and no tampering is done with data. Here Sender sends data with a digital watermark embedded on it. On the receiver side, when data is received, digital watermark is extracted to check authenticity of data [13].

Attacks on digital watermark

In terms of watermark, detecting watermark or watermarked data by unauthorized users is called an attack on watermark. Detecting and manipulating watermark is the major in copyright protection, fingerprinting or copy control applications. Watermark attack is partitioned into four categories namely Removal attack, geometric attack, cryptographic attack and protocol attack [14].

a. **Removal attack:** it tries to remove watermark information without knowing the watermarking algorithm [15].
b. **Cryptographic attack**: These attacks target the security methods in the watermarking system and try to remove embedded watermark information or it simply adds fake watermark information into it. This can be done with a technique called brute force search. Another technique used in Cryptographic attack is called **Oracle attack**. This technique is used to create non-watermarked signals and when this signal traverses watermark detector, it fails to recognize [16].
c. **Protocol attack:** In Protocol attack, attacker tries to prevent watermark to do its intended functions. Attacker removes watermark from watermarked data and claims ownership of the watermarked data. This creates ambiguity between the genuine owner and fake owner. This type of protocol attack is called Ambiguity attack. Another form of protocol attack is copy attack where watermark is neither destroyed nor changed, only identify and extract watermark, copy it and paste

Journal of Information Systems Engineering and Management
2025, 10(56s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

it into another data called target data. The attack is called copy attack when a valid watermark (Copy of original watermark) is generated on target data without any watermark algorithm [17].

d. **Geometric attack:** it tries to modify synchronization between watermark detector and information which is embedded and result in synchronization error. This watermark is neither removed nor changed. Watermark is still present but only its position changed. Once perfect synchronization is achieved watermark detectors detect digital watermark and extract watermark information [18].

Various types of other watermark attacks are as follows [19][20].

1. **Active attacks:** In this type of attack, the attacker removes watermarked data. It tries to make the watermark undetectable.
2. **Passive attacks:** Here the attacker does not remove watermarked data. But it tries to find out whether a watermark is present or not.
3. **Collusion attacks:** Every valid document or image contains valid data and watermark information. This watermark is unique, which is used for identifying a copy of a valid document. In this type of attack, the attacker tries to create a new copy of document or image without any watermark. Collusion attack is a major challenge in fingerprinting applications.
4. **Forgery attacks:** In this type of attack, the attacker does not remove the original watermark. Here hackers add new valid watermarks into data. Once a new valid watermark is inserted into data, hackers in other words, unauthorized users can obtain access and modify document data or images. This will create confusion between original document and fake document. Forgery attacks are a major concern in data authentication.
5. **Detection disabling attacks:** this attack tries to find correlation of watermark. Once correlation is found, it breaks the correlation. As correlation breaks, watermark detection is not possible. Though watermark is present in the data, due to lack of correlation, detection of watermark is not possible. This attack is known as "Synchronization attack".
6. **Ambiguity attacks:** this attack attempts to generate false or fake watermarked data from host data. By generating fake watermarks, it claims ownership of watermarked images or data. For Example, ambiguity attack generates and embed one or multiple fake watermarks into image or document to confuse watermark detector. It makes confusion about the original owner of the document. It misleads here original owner. This attack is also known as "fake watermark attack", "fake-original attack", "deadlock attack" and "inversion attack"
7. **Copy attacks:** The goal of this attack is neither to remove watermark nor to manipulate watermark. It attempts to detect watermarked data and copy it to some other data. The attack is called a copy attack if a valid watermark in other data can be produced without using any algorithm and algorithm key.
8. **Geometric attacks:** Unlike removal attacks, geometric attack does not remove watermarked information but it tries to manipulate watermark detector synchronization with embedded information.

Text vs. image watermark

For document security host media is text and image only. So in this section we will see about text watermarking and image watermarking in detail.

Ref. No	Parameter	Text	Image
[21]	Definition	Text watermarking involves embedding unique	When watermarked data is embedded inside image, it

Journal of Information Systems Engineering and Management
2025, 10(56s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

		watermark inside text.	is called image watermark.
[22] **[23]**	Classification	**image based** - for embedding watermark image of text is used **syntactic** - text is converted into syntactic tree and depending upon bit value from syntactic tree watermark is embedded **semantic**- synonym substitution method is used for semantic content for watermarking	**Spatial domain**: In Spatial domain, watermark is embedded into cover image by just modifying pixel values **Frequency domain**: In Frequency domain, image is first transformed into spectral coefficient and then watermark is added to spectral coefficient.
[5] [21] **[6]**	Attacks	**character-level attack**: altering characters of text without changing original word **Word Level attack**: Adding, replacing word with other word **Deletion attack**: some words of text are deleted which distort watermark **Formatting based attack** like copy and paste, retyping	Geometric attack Image Degradation Image Enhancement Image Compression Image Transformation
[21] **[27]**	Applications	copyright protection fake news detection	Fingerprinting Intellectual property right protection Broadcast monitoring Medical imaginary

Journal of Information Systems Engineering and Management
2025, 10(56s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

			Illegal transaction identification
[28]	Embedding Capacity	Low or Limited to text information such as copyright information	HIGH means can embed comparatively large information into image
[28]	Robustness	HIGH	MEDIUM/LOW
	Visibility	Less Visible or sometimes overlooked	Clearly Visible
	Example	Text, mostly copyright information	Logos and graphics images
	Implementation complexity	Simple	Complex

Table 2: Text vs. Image Watermarking

Combining Hybrid Image Watermark for more Robustness and enhanced Security of digital document

Hybrid image watermarking

Advanced security, imperceptivity and robustness to various attacks (high robustness) are basic characteristics of digital watermark. It is not feasible to any single watermark (Spatial or Frequency domain) to fulfill all these characteristics. Hence to achieve High Robustness, Good Imperceptivity and Advanced Security, hybrid image watermarking is used.

Domains are spatial and frequency. By combining domains for image watermarking, watermark becomes more robust and embedding capacity is also increased which is helpful for adding watermark information.

Watermarks become more robust as spatial domain uses Least Significant Bit (LSB) technique to insert watermarked images into cover images. LSB bits of cover image are modified with watermarked image and frequency domain inserts watermarked information into the low frequency part of cover image. This watermark is more secure and has double layer protection. [10]

Combining multiple frequency domains such as DCT, DWT and SVD provides strong robustness and good imperceptivity

Improved robustness is achieved when DCT-SVD combined method of image watermarking is used. DCT-SVD based watermarking technique is used in fingerprinting, owner identification and tamper detection [27].

Combining DWT, DCT and SVD together provides high robustness in terms of quality and security for medical images. It is used to provide copyright protection to medical images. It ensures Robustness against Gaussian noise, Salt & pepper, Speckle noise and filtering attacks such as Average filter, Median filter and Wiener filter [29].

Hybrid image watermark is used for copyright protection of digital document as it provides high robustness and more imperceptibility.

Conclusion

Digital watermark is used to provide copyright protection to digital documents. It can be visible or invisible. There are various attacks on digital watermark. To provide security of digital document,

digital watermark is more robust. Robustness to digital document is achieved by applying hybrid image watermark in frequency domain. To have better robustness along with digital watermark, steganography or cryptography can also be applied. Steganography, Cryptography and Digital watermarking are branches of information hiding. The main aim of cryptography is to keep messages secret whereas the main aim of steganography is to hide information in such a way that it cannot be easily visible. To make digital documents robust, 11 Steganography and digital watermark are applied together. Combining Steganography with hybrid image watermark will provide double layer security to digital documents.

References

[1] Mr. Parag S.Deshmukh , Mr. Pratik Pande, "A Study of Electronic Document Security", International Journal of Computer Science and Mobile Computing, Vol. 3, Issue. 1, ISSN 2320–088X , January 2014, pg.111 – 117

[2] Nurul Shamimi Kamaruddin, Amirrudin Kamsin, Lip Yee Por, Hameedur Rahman, " A Review of Text Watermarking: Theory, Methods and Applications Article ",in IEEE Access · January 2018

[3] Shraddha S. Katariya , "Digital Watermarking: Review",International Journal of Engineering and Innovative Technology (IJEIT), Volume 1, Issue 2, February 2012, ISSN: 2277-3754,pp:143-153

[4] Ritu Rawat , Nikita Kaushik , Soumya Tiwari, "Digital Watermarking Techniques", International Journal of Advanced Research in Computer and Communication Engineering Vol. 5, Issue 4, April 2016, ISSN (Online) 2278-1021 ISSN (Print) 2319 5940, pp:491-495

[5] Maninder Kaur, Nirvair Neeru, "A Review on Digital Watermarking Using LSB", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 11, November 2015, ISSN: 2277 128X, pp:210-214

[6] Prabhishek Singh, R S Chadha , "A Survey of Digital Watermarking Techniques, Applications and Attacks" ,International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 9, March 2013, ISSN: 2277-3754 ,pp:165-175

[7] Gaurav Chawla, Ravi Saini , Rajkumar Yadav , Kamaldeep , "Classification of Watermarking Based upon Various Parameters", International Journal of Computer Applications & Information Technology , Vol. I, Issue II, September 2012 , ISSN: 2278-7720, pp:16-19

[8] Al. Embaby, Mohamed A. Wahby Shalaby, Khaled Mostafa Elsayed , "Digital Watermarking Properties, Classification and Techniques" , International Journal of Engineering and Advanced Technology (IJEAT), Volume-9 Issue-3, February 2020, ISSN: 2249-8958 (Online),pp:2742-2750

[9] Lalit Kumar Saini1 , Vishal Shrivastava, "A Survey of Digital Watermarking Techniques and its Applications", International Journal of Computer Science Trends and Technology (IJCST) – Volume 2 Issue 3, May-Jun 2014, International Journal of Computer Science Trends and Technology (IJCST) – Volume 2 Issue 3, May-Jun 2014 ISSN: 2347-8578, pp:70-73

[10] Mahbuba Begum ,Mohammad Shorif Uddin , "Digital Image Watermarking Techniques: A Review",MDPI open access, 2020, pp:1-38

[11] Mohammad Abdullatif Akram M. Zeki Jalel Chebil Teddy Surya Gunawan ," Properties of Digital Image Watermarking", 2013 IEEE 9th International Colloquium on Signal Processing and its Applications, 8 - 10 Mac. 2013, Kuala Lumpur, Malaysia, pp:235-240

[12] Jobin Abraham , "Digital Image Watermarking: An Overview", National Seminar on Modern Trends in EC &SP, 3-4 Feb 2011, pp:36-42

[13] Ifra Iqbal Khan, M.A. Rizvi, "Discrete Wavelet Transformation a Method for Digital Watermarking", IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 4 Issue 6, June 2017 ISSN (Online) 2348 – 7968, pp:243-247

[14] Yukti Varshney, "Attacks on Digital Watermarks: Classification, Implications, Benchmarks", International Journal on Emerging Technologies (Special Issue NCETST-2017), ISSN No. (Print) : 0975-8364 ISSN No. (Online) : 2249-3255,pp:229-235

[15] Amy Yang,"A SURVEY OF DIGITAL IMAGE WATERMARKING TECHNIQUES AND ATTACKS",A THESIS Presented to the University Honors Program California State University, Long Beach

[16] Ensaf Hussein , Mohamed A. Belal , "Digital Watermarking Techniques, Applications and Attacks Applied to Digital Media: A Survey ",International Journal of Engineering Research & Technology (IJERT) ,Vol. 1 Issue 7, September - 2012 ,ISSN: 2278-0181, pp:1-8

[17] Sunesh, Harish Kumar, "Watermark Attacks And Applications in Watermarking", International Journal of Engineering Research & Technology (IJERT), Vol. 1 Issue 7, September – 2012, ISSN: 2278-0181,pp:1-8

[18] Gangadhar Tiwari , Debashis Nandi, Madhusudhan Mishra , "Digital Watermarking and Attacks: A Review" , International Journal of Engineering Research & Technology (IJERT), Vol. 2 Issue 10, October – 2013, ISSN: 2278-0181, pp:1144-1149

[19] Dr. Sanyam Agarwal , Priyanka ,Usha Pal, "Different Types of Attack in Image Watermarking including 2D, 3D Images", International Journal of Scientific & Engineering Research, Volume 6, Issue 1, January-2015, ISSN 2229-5518, pp: 841-845

[20] Jordi Nin and Sergio Ricciardi , "Digital watermarking techniques and security issues in the information and communication society", 2013 27th International Conference on Advanced Information Networking and Applications Workshops, IEEE, pp:1553-1558

[21] Aiwei Liu, Leyi Pan, Yijian Lu, Jingjing Li, Xuming Hu, Lijie Wen, Irwin King, Philip S. Yu, "A Survey of Text Watermarking in the Era of Large Language Models" , Vol. 1, No. 1

[22] Zunera Jalil, Anwar M. Mirza, and Hajira Jabeen , "Word Length Based Zero-Watermarking Algorithm for Tamper Detection in Text Documents", 2010 2nd International Conference on Computer Engineering and Technology, pp:378-382

[23] Vidyasagar M. Potdar, SongHan,Elizabeth Chang , "A Survey of Digital Image Watermarking Techniques", 2005 3rd IEEE International Conference on Industrial Informatics (INDIN) , pp:709-716

[24] L. Robert , T.Shanmugapriya , "A Study on Digital Watermarking Techniques ",International Journal of Recent Trends in Engineering, Vol. 1, No. 2, May 2009, pp:223-225

[25] J.T. Brassil, Steven Low, N.F. Maxemchuk, Lawrence O'Gorman , "Electronic Marking and Identification Techniques to Discourage Document Copying", IEEE Journal on Selected Areas in Communications pp:1495 – 1504

[26] Aaqib Rashid, "Digital Watermarking Applications and Techniques: A Brief Review", International Journal of Computer Applications Technology and Research , Volume 5–Issue 3, 2016, ISSN:2319–8656 , pp: 147-150

[27] Vassilis E. Fotopoulos and Athanassios N. Skodras , "Digital Image Watermarking: An Overview" , EURASIP NEWS LETTER, European Association for Signal, Speech, and Image Processing, ISSN 1687-1421, Volume 14, Number 4, December 2003, pp:10-19

[28] Sulong Ge, Zhihua Xia, Jianwei Fei, Xingming Sun, and Jian Weng , "A Robust Document Image Watermarking Scheme using Deep Neural Network" , JOURNAL OF LATEX CLASS FILES, VOL. 18, NO. 9, SEPTEMBER 2020, pp:1-20

[29] Imane Assini, Abdelmajid Badri, Khadija Safi, Aicha Sahel, Abdennaceur Baghdad , "A Robust Hybrid Watermarking Technique for Securing Medical Image" , International Journal of Intelligent Engineering and Systems , Vol.11, No.3, pp:169-176