Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 5, May 2015, pg.859 – 870

REVIEW ARTICLE

Protecting Digital Images by Wavelet Based Watermarking Method in Network Environment – Articles Review

HAMID SADEQ MAHDI

University of Diyala / Basic Education College / Computer Science Department, Iraq

hamidalsultani81@gmail.com

ABSTRACT

Contemporary networks environment has become and will be more multimedia based data communications. The growing popularity of this new trend of internetworking communications data goes along with the need for protection of transmitted data. Many methods are developed to deal with this issue, typically about copyright protected security, digital image, audio and video products concerns (e.g. control of copies pirating, illegal broadcast use, sales) [1][4]. And since past years, digital watermarking (DWM) is one of the most used of such data protection security methods. Protecting digital images by wavelet based watermarking is the aim for this papers review. It presents an analysis on common watermarking schemes for Digital images protection in network environment. The paper closes up after discussing also about the DWM applications, core properties and the concept of best in DWM.

Keywords:

Network environment, wavelet, digital images/signals, watermarking, communications, geometric, copyrights, security, Transform spatial, frequency domain, DWL, WM

1. INTRODUCTION

Networking computers system has rendered fast, easier and cheap the communications data. However, multimedia based communications data (e.g. digital data –i.e. video, voice/audio and images) are still posing significant challenges to networks despite the advancement of technologies for their production (i.e. digitized format, compression, and tech-convergence). Such challenges are in matters of copyright protected security questions; because they get disclosed in transmission throughout the network communication environments [1][2][4]. However, to solve for raised issues, some techniques have been developed and are usually implemented under appropriate schemes, depending on the method. And watermarking or digital water marking (DWM – as short form throughout this review) is one the most applied scheme and will be here the focus of discussions

This article's sections are intended to explore in three stages the process of protecting digital images by wavelet based watermarking in network environment. First is introduced an overview of digital watermarking as a process for digital protection; and finally some application/implementation methods. The overall sections will

close up with an attempt of presenting the efficiency of each DWM method, including the notion best of schemes, techniques/ methods.

1.1 Background and WM Importance

Historically, the need for DWM goes back to the implementation on the networks of multimedia data improved design quality (e.g. digital media --audio and videos) of which copyright security was then threatened of corrupt [1] [17]. And considerable efforts for protecting transmitted data over networks have emerged since several years ago with the oldest and one of the popular solutions for this purpose – cryptography [1] [5] especially for multimedia data by 1990s. But, this security method, was less affordable to every users due to additional costs (hardware & necessary software), including its unavoidable vulnerability after decryption [1][2], which happened to be a significant limitations with modern media development. However, digital information age has only much improved greatly both the information quality and it transmission process (i.e. Speed). Yet, its features were and are making it easier copying, duplicating, pirating with untraceable manipulations: all these became a threat and bitter challenge to legally preserve the right of ownership [1].

1.1.1 Concepts & Principle Of DWM

Literally, DWM refers to the process of caching, sinking details of a digitized information (e.g. audio/visual information, pictures) inside the same signal carrying that information [1][4]. According to [1], for need in audio, video and unanimated pictures' authentication and copyright protection, and digital watermarks technique has been developed as a solution. It consists of planting this technology inside a digital material (e.g. for an image, audio sequence or video frame: a piece of itself) having the intelligence of detecting any user's attempts of manipulation [1][2][4] [17]. One can figure out that the process works somehow like in a document's electronic text protected from modification, whereby a refusal message pops up, or related warning signal anytime an editing process is being signalled through the word processor.

1.1.2 Watermarking (WM) Concept

Technically, the DWM principle is learned or borrowed from steganography. For, either technique refers to a process of keeping information by hiding its details inside the cover of the data [1].

1.2 WAVELET BASED WATERMARKING PROTECTION

Wavelets are known broadly as a mathematical function in digital signal processing and image compression, And the principles applied are similar to those of Fourier analysis in use since early 19th century [9][10].

1.2.1 Digital WM (DWM) Proprieties

According to literatures these are overlapping in list and thus, depend on the network system implementing watermarking. However, the most significant ones free from confusing, [4] mentioned:

Robustness: propriety that crucially set for DWM a true difference with cryptography as explained early in background section[4] [13/14]. In general DWM is known more robust for being stronger in protection contrary to cryptography for its potential features to oppose better any attempt of stealing of altering the hidden watermarks. This includes withstanding compression, scaling, noise, Gaussian, printing and scanning, rotation,, cropping and etc.

Fidelity of original image: -i.e. restoring to the nearest possible quality an image after undergoing watermarking process, by keeping lower the incurred degradation effect on the original image's quality.

Effectiveness: - refers to the possible greater chance level for the hidden information to remain sensible and thus fairly detectable in watermarked media (audio/video, images); and it considered also as important as robustness [1], or even more due to the required fidelity over time.

Payload size: - that is about how big enough (the better) is the (allocated) size for the hidden DWM data, even though it is true for every application.

False Positive Rate: -i.e. a perceived amount of wrongly accounted or identified (e.g. the lower number the better) as quantity of digital works containing digital watermarks. This can be thought also of the level of errors rate associated with the watermarks system.

Many applied research works have deployed important efforts studying this method to enable its use to best of its regular proprieties despite some limitations. Thus, [12] [15] has identified as factors characterizing watermarking effectiveness: Validation, invisibility, Capacity and Robustness; these are known particularly as DWM factors of quality [17] and, are slightly named differently in many other study papers – For instance robustness, imperceptibility, capacity, and blindness.

1.2.1. **Application Motivation Fact**

The huge amount and motivation for research study in past and recent years on DWM are merely proven as due to its great efficiency at the face of many achievements in digital copyrights management and protection [4] [12] [15][17].

1.2.1.2 Digital WM (DWM) Use

Examples of common use or implementations of these techniques are just many and some of them include:

- ✓ Ownership identifying: DWM makes it easier to differentiate between and mainly to avoid involvement into copyright infringement disputes by burying it into digital material.
- ✓ **Broadcast** monitoring: useful for tracking video use (i.e. Advertisement application) and free play (i.e. Entertainment) on radio or TV broadcast program. Both video and music's owners and business services appreciate this DWM feature applied respectively to control the use of the media and the execution of contract by agencies to which are outsourced business' products advertisements.
- ✓ Piracy acts' control: implemented watermarks into picture/video/song/music digital data are detectable by watermarking- compatible CD/DVD writer through a warning message to its fraudulent users.
- ✓ Transaction tracking this feature enables recording every recipient over all legal transactions involved onto a digital art's history, making easier to trace the originator of any leak.

2. DWM IMPLEMENTATION

2.1 Life-Cycle Phases for DWM Implementation

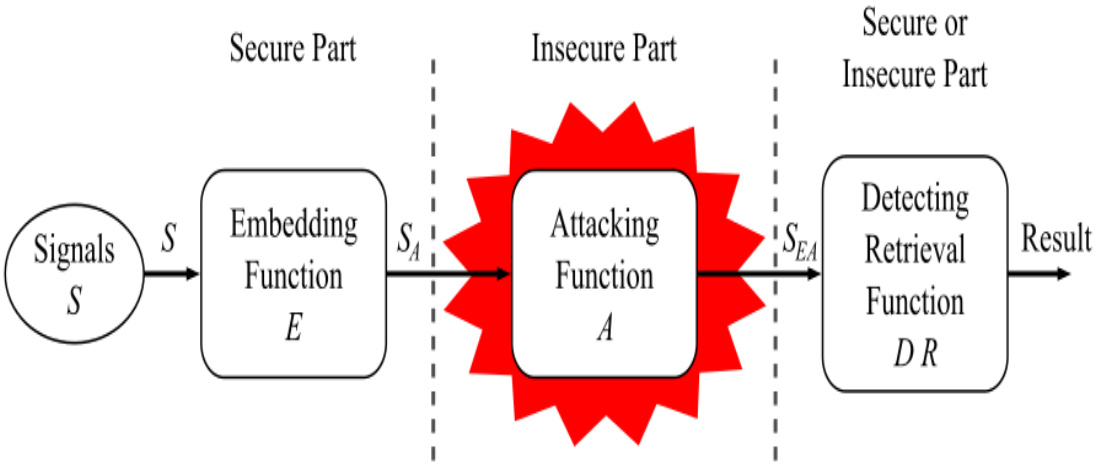


Figure 2.1 General digital watermark life-cycles

3. DWM PERFORMANCE QUALITIES AND EVALUATION

3.1 Metrics and Evaluation

DWM technique's performance evaluation/assessment is basically carried out according to the level of security it can provide against possible attacks. The well-known DWM attacks include noise addition, rotation, cropping, scaling, resizing and compression [17]. However, there are two specific metrics for this evaluation, which consist of Perceptual transparency (i.e. image observed quality)

Practically, PSNR (Peak signal to Noise Ratio), measures the image quality and, the Mean Square Error *(MSE)* between original & watermarked image, respectively determined for a picture of size (M) as:

$$PSNR = 10\ log_{10} \frac{(255 \times 255)}{MSE}$$

with:
$X\ i,j$: Original image,
$X'\ i,j$: Watermarked image, and
Nt: Size of image

$$MSE = \frac{1}{Nt} \sum_{i,j} \left(X(i,j) - X^{'}(i,j)\right)^2$$

With f (i, j) being pixel grey values of original image.

- **Image Fidelity (IF)**

It is a measure of imperceptibility or transparency of watermarked image [13]; functionally this encompasses its Robustness and calculated as follows

$$IF = 1 - \frac{\sum_{i,j}(X(i,j) - X'(i,j))^2}{\sum_{i,j}(X(i,j))^2}$$

Other commonly used metrics for robustness verifications include: Mean Average Error (MAE), Signal to Noise Ratio (SNR), Bit Error Ratio (BER), Universal Image Quality Index (UIQI), Mutual Information (MAE) and Structural Content (SC), and Normalized Absolute Error (NAE) [21].

The main goal of watermarking is to resist both geometric distortion and signal processing attacks [21].

3.2 Important Fact about Performance Assessment

In overall cases, attackers' effort is always about either 'nullifying, modifying the structural design, or changing watermark data covering technique; etc. Therefore, performance considerations must more look into how much robust is a watermarking technique against such threats. This has confirmed once again why robustness is the most important of parameters with respect to DWM quality.

4. DWM Scheme Classification & Comparison

A critical observation from different studies shows strong hold and consistent outcome for DWM. For instance [4] and [12] lightly differ only on wording about its properties' analysis, but for a same meaning.

4.1. Scheme Classification

In matter of scheme classes, they are defined according to the nature of signal (i.e. data) available on the terminal to be watermarked. Hence, based on [1], there are almost four groups in classification namely, digital image watermark, digital video watermark, digital audio watermark, and '3D' multimedia based watermark. However, other study like [17] has gone further for this by accounting various criteria underlining each of the above four groups – though [17] still categorizing all into broadly four groups (Figure 4.2-a)

4.1.1 Brief Overview

4.1.1.1 Digital image Watermark

Digital image watermark can be made visible or invisible [1]. The popularity of Watermarking image technique goes back to its closer look alike with human counterpart visual system [11].With respect to digital property's security or protection watermark is contemporary method to implement an invisible signature embedded inside a digital image/video/song for authenticity or ownership proof verification/control/monitoring.

Examples of DWM important contributive support to authorship include discouraging fraudulent duplication, use on the communication networks, including any initiatives of changing these applications' contents.

However, the growth of computer literacy based community, availability and widespread of more computer scientists can be seen as source of many attempt of intentional attacks to DWM or other digital protection methods.

4.1.1.2 Digital video Watermark

Because a video materials are made up of successive pictures moving in frames sequence manner, the principles for image WM (watermark) are then applicable by oriented reuse in video and audio DWM (digital watermarking).

- **DWM Execution./Implementation Process**

DWM implementation process is performed (Figure 2.1) in three basic steps – embedding, attack and extraction [20][21].

Respectively the first is about insertion of the referential image/video/audio signal into its intended referential host prior to use (i.e. release to public); the next activity refers to any attempts (intentionally or not) to corrupt or change the watermark data; and the last operation is about the necessary of applying relevant detection algorithm to verify the status of watermark. Additionally, this last operation is aimed at either proving the authenticity/ownership or the safe status of the of the digital material [14] [15][17][20]

4.1.1.3 Digital audio Watermark

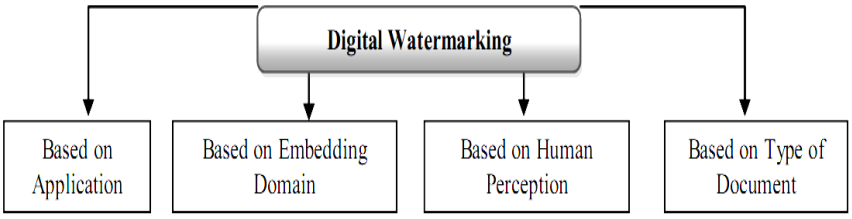
As mentioned earlier, the principles for image WM can apply by extension for audio as well as also for video cases. Therefore, digitized and distributed medias (e.g. audio, images and videos) can be also protected similarly from networker's user attack on the copyright owner embedded watermarks. Like in image and video security process, digital audio watermarking technique follow the same three steps mentioned earlier; this remark include all other aspect of studies (e.g. performance evaluation, applications, etc.;) performed on digital data.

4.1.1.4 Watermarking 3D Multimedia

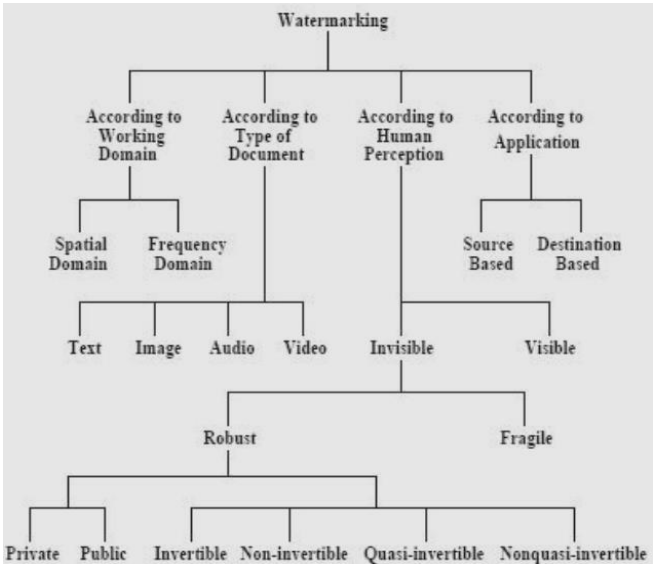
Watermarking "3D Multimedia", initiated and first published in 1997, has two models of algorithms: spatial domain methods and frequency domain methods. The first is implemented by altering some of its relevant factors like vertices' positions, texture point's appearance and any others. The second is done through changing some of the transformation coefficients [12].

4.2 – **DWM Insertion Method Based Technique Classification**

Among existing WM (Watermarking) techniques the two following are likely the most applicable: spatial domain and transform domain watermarking [15][20]. How each basically performs /operates?



[a]



[b]

Figure 4.2 DWM domains based classification

[a] Narrowed & [b] Detailed categorization of WM techniques

4.2.1 **Spatial Domain** Watermarking

Refer to Figure 4.2 for detail on WM techniques categorization broad presentation

The design of Watermark in the spatial domain is executed by altering the intensity applied randomly to a selection of the digital picture pixels. And the process does not need the presence of the initial picture for verification, but instead a quick statistical check.—marked pixels' is evaluated against the non-marked ones relatively to their mean intensity [11].

4.2.1.1 Algorithm Example

There is a great number of WM techniques implementing spatial domain, of which many could not resists from purposely led frequency domain based attacks. However, this section based on [15] is a brief introduction, presenting how watermarking can designed to face some manipulations in the frequency domain.

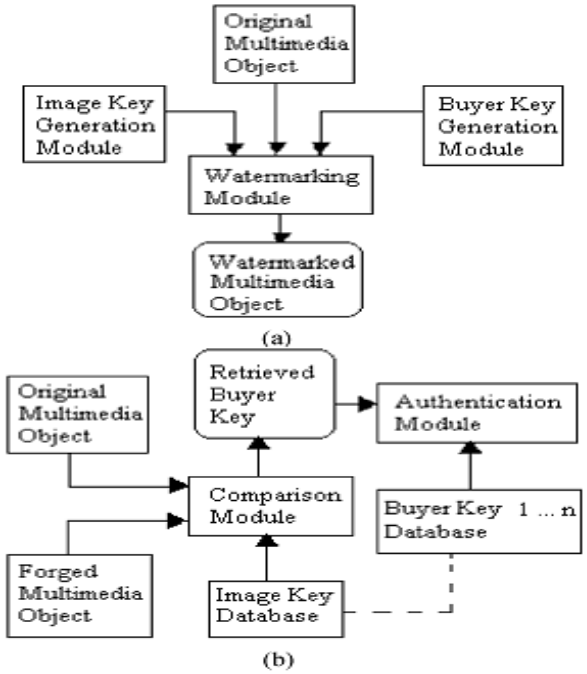


Figure4.2.1.1 Algorithm Example for Spatial Domain DWM

(a) Watermarking process; (b) Watermark retrieval process

4.2.1.2 Spatial Domain Watermarking Processes Summary

The referential image is split into small sections (Respective matrices and overall algorithm omitted). Then, when the image intensity is applied each section get modulated according to its bit value (Figure 4.2.1.2) to produce a watermarked image [15][2].

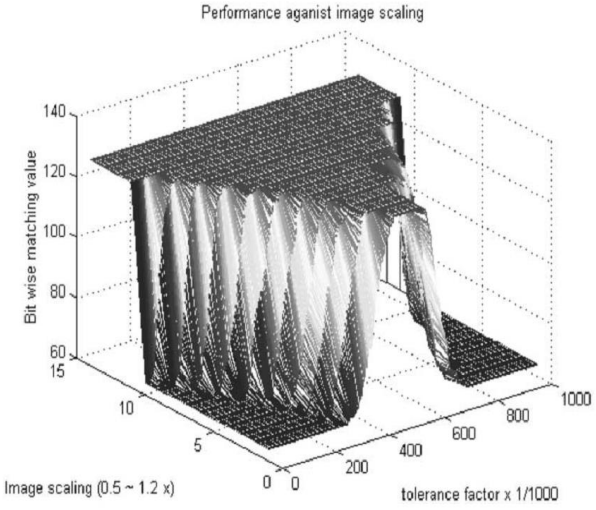


Figure 4.2.1.2 Performance against image scaling –

In spatial domain based watermarking process, the change performed on the image pixels ensures that the watermark remains infallible to the modification of the picture texture. Hence, use of low power during watermarking is one of the strategic methods [11][17].

4.2.2 Transform Domain Watermarking

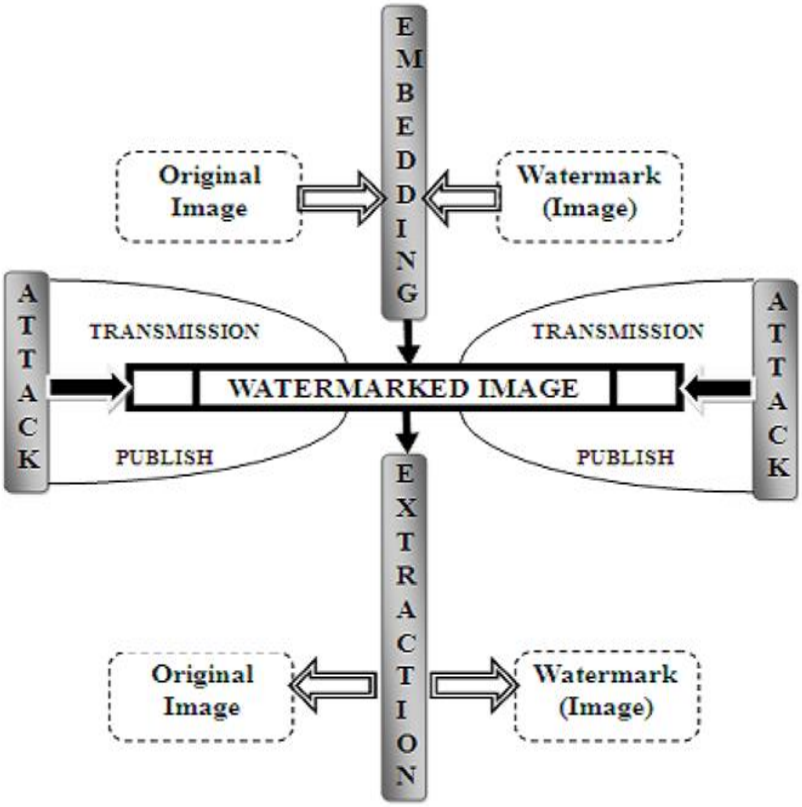
Besides existing DWM techniques, transform domain watermarking is a model that associates some mathematical model (Algorithms), whose formulae express the various factors involved in the watermarking processes (Figure 2.1 & 4.2.1.1) to either insert or extract a watermark. This technique algorithm models include DWT, CDMA based, DCT-DWT combined approach [17].

In fact, according to [17] and related works, watermark will be set onto the image/video signal transformed coefficients as to increase its capacity and robustness. And because transform domain WM is a frequency domain based model, for watermarking algorithm, the following transforms are different options: Fourier Transform (FT), Short Time Fourier Transform (STFT), and Continuous Wavelet Transform (CWT), Discrete Wavelet Transform (DWT), Discrete Cosine Transform (DCT) or Combination of DCT and DWT. In quick conclusion, the above [17] source showed a strong recommendation of this DWM techniques as proven good enough for robust watermarks.

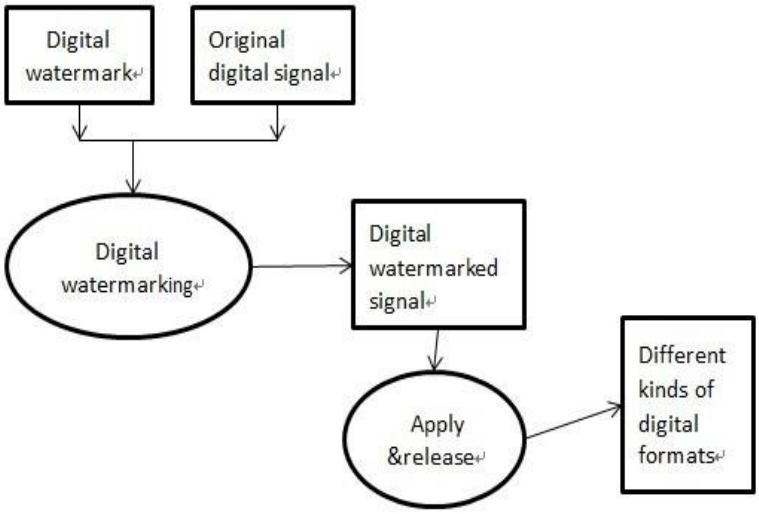
4.3 DWM Techniques Categorization Summary

According to [17] study, WM (watermarking /watermark) techniques are classifiable broadly into four categories, and each made of subgroups, which are mapped so based on the criteria characterizing WM techniques operation or mode of implementation.

Briefly, these watermarking methods/techniques are grouped based on either WM perceptibility level (i.e. no/less or fully visibility enabled), detection/Extraction (i.e. blind /non-bling watermarking), insertion domain (i.e. spatial, transform/frequency): and WM potential to resist attack (i.e. weak/lossy/fragile, semi-strong). Even though, some studies may differ with some of the listed subgroup criteria depending of the available study facility, however this [17] & [20] proposed classification so far is the most comprehensible among contemporary accessed papers for this review.



[a]



[b]

Figure 4.3 DWM General Process

4.4 Comparisons to Digital Watermarking

Relatively to networking communications data protection, DWM potential outperforms most similar methods (e.g. stenography. encryption) as these latter fail to compete DWM in matter digital data security and control. Here is some justification under the following comparisons with some existing data security techniques.

4.4.1 DWM Proprieties & Features

`In literatures, robustness is classified the most important MW/DWM characteristic [1][3][4][12]; whereas few studies diverged on this point. However, considering the purpose, which made up the design objective of WM technique and thus its application preference against other securities methods for communications data on multimedia based networks robustness and transparency can be seen as the most important

4.4.1.1 Encrypting vs. Watermarking

Encryption is another potential protection technology for communications data, facing some challenges as to its effectiveness as according to [18][19], no single algorithm is ideal for all situations, and guidance on the merits of each is beyond the scope of SQL Server Books Online.

4.4.1.2 Stenography vs. Digital Watermarking

Relatively to the aim, DWM is a similar technology (i.e. hiding information onto its signal) to stenography despite divergence in target – Stenography is broadly about covering and rendering the whole content invisible; whereas in DWM instead hidden details are only those about the information [1][4].Therefore, watermarking can be thought of /interpreted as sinking (i.e. for marking) something (made invisible) besides an object (e.g. a ship and control-box/black-box both carried by water but only the black-box is made invisible even though attached/embedded to the ship by whatever means)altogether sharing the same water environment. Thus water-marking since only the expert knows about the existence of the mark existing around there. Furthermore, according to [1]**,** watermark can be made either visible or invisible; and the most important fact is that the watermarked element in either case remains invulnerable from fraudulent users of the digital information carrying it from its inside.

Based on the literatures and relatively to their features' efficiency with respect to the digital materials protection concern, DWM anyhow outperforms the stenography in robustness. Stenography is known less resistant to the content of information data manipulation; whereas DWM is expected to remain more invulnerable to hidden info removal.

5. WAVELETS BASED DWM LITERATURE REVIEW

This article's section review objective: is to produce shortly a useful analysis on watermarks design techniques for digital image, video, audio protection on networks /multimedia base networks / watermarking based networks.

5.1 Wavelet DWM Applications on Data Networks

5.1.1 Objective in Networking Communication Data

An importantly particular DWM application is on the proof of ownership monitoring/tracking [1][2][6][7][17][23]. Some other internetworking communications data protection's schemes are widespread under the internet data dispatching management's convenience and not legally by world's countries consent [3]. For instance, encryption enables millions of emails messages to reach their intended recipients and this invisibly across various public and private networks. But, how much those contents remain secure once opened up on any host computer, voila the limitation. Wavelet based DWM does better from controlling to monitoring (i.e. reporting, helping track the leaking source) the movements and use of the digital data on DWM networks [1][2][3][5][9][10] [17][20]

5.1.2 Digital Watermark's Performance over Years

A creativity of Andrew Tirkel and Charles Osborne (1992) digital watermark was intended to identifying marks in paper in manufacturing process. Then, it formerly helped distinguish between papermaker. In today's applications, DWM encompasses above statements and helps under all the following areas: Copyright protection, source tracking (using various watermarks), TV Broadcasting Medias control (Televisions watermarked video for advertisements) and videos authors' authentication [1][2][3][5] [6] [9][10] [23]

5.2 Applications Preference or Convenience

Wavelet based application in DWM network is far convenience since its application conceptual target gives it more legal acceptance for usage in all applicable level without restriction [3]. This is compared to the limited legal grant of usage to cryptography [3] and stenography [3][4] .

5.2.1 Technologies Progress Problem Solved with DWM

Digitization of information on media support and its implementation on the internet protocol IP have respectively eased much its production/reproduction and the transport/transmission. However such easiness has brought about illegal use issue against the proprietorship rights. Hence, DWM development has come as solution for copyright protection to image, video and audio/song by hiding particular data inside the original image ones for originality check or rightful ownership tracking [17]. And this is the one of the most commonly applications of watermarking. It is used in business communications and mainly for over networking communications data related various security purposes ---namely in media authentication control, tamper-proofing (i.e. checking if or not a digital content is corrupted by a third party [14]. By reuse or extension of principles, other digital communications data (e.g. video, audio/voice applications) are able to receive similar protection. And, it is done with just some modifications on the set of proprieties that more relevant to each data type for watermarks embedment requirements [1][13][14].

5.2.2 Challenge with Spatial domain WM Techniques Use

As critical challenges to DWM (digital watermarking) efforts for securing data protection, threats to break spatial and frequency domains based watermarks are ranked among the most happening figures. However a study conducted by [15] has proven that watermarking scheme still can achieve great successes by implementing bit wise matching values as high as possible beyond the indicated/recommended average, whilst maintaining the image distortion bellow Weber ratio. Furthermore, considering these threats as related to DWM robustness characteristic, alternative solutions consist of applying transforms such as DFT, DCT, or DWT in frequency domain watermarking [16].

5.3 Which of DWM Models Is The Best?

5.3.1 A Convenient Alternative?

Referring to the background section, DWM based wavelet application was originally designed in imitation of stenography in both principle and purpose, but having a different target with respect to its specific features [1]. Therefore, DWM has been developed as suitable solution to switch from invisible to visible security marks embedment – even though now the two forms are applicable in DWL (See Figure 4.2). Otherwise, this condition (DWM ability) made it preferable to other competing techniques. Otherwise, it is more preferred than other related techniques firstly for this unique characteristic. And secondly follow its robustness ds another distinctive characteristic [1] [2] [4].

5.3.2 Best Fit on All Security?

On typical research works, which have involved designing and testing algorithms based DWM, it is quite hard to get consensus for the said-best as a model fit for security of all communications data as shown in the following statement. Based on such a work conducted by [12], there is no unified standard to test which algorithm is better. But, some great applications are performing wonderfully and thus considered as getting the best of protection using this method, compared to any others [12].

In digital data security matters**,** studies have proved that **no watermarking algorithm resists all the attacks. And** even so, it **is still great method for digital data publication and distribution over networks just at the cost of performing some further computations on failing points** [21].

5.3.3 Limitation Point

In general, the main goals and aims for Digital watermarks for whatever purposes (e.g. authentication control, distribution monitoring, tamper-proofing; etc.;), share almost the following characteristics as criteria for security role that they can provide undeletable by an attacker. For instance a DWM is expected to be friendly verifiable by the authors, visible but not statistically; invulnerable to content attacks and filtering including and deleting embed mark and any related harmful processing [1] [2] [3] [4] [12] [13][14][15].

However, according to [14][15] despite the complexity of the task, some great theories and thus algorithms have been developed with hopes to fairly tackle almost the majority of threats, which face digital applications; but unfortunately, for instance "research on copyright protection of images is still in its early stages and none of the existing methods is totally effective against attacks". In fact, similarly to any scientific researches and innovation works, enhancement for performance improvement is a fundamental part of such an activity.

6. CONCLUSIONS

This review has gone through various aspect of wavelets based watermarking as a great method in contemporary protection of digital images in network environment. Its most important aspects such DWM characteristics, quality parameters, realization or implementation processes have been analysed as based on recent researches literatures. An overview on wavelets mathematical perspectives in watermarking has been covered. And finally, some critical comparisons regarding watermarking various techniques' potential and limitation based on researchers' opinions. Probably, this review intends to serve its readers as quick reference in original research works or a knowledge review.

REFERENCES

1. Bibi Isac & V. Santhi, 2011 *A Study on Digital Image and Video Watermarking Schemes using Neural Networks*; International Journal of Computer Applications (0975 – 8887) Volume 12– No.9; 2011
2. Cox I, Miller M, Bloom J, Fridrich J, Kalker T , 2008 *Digital Watermarking and Steganography Second Edition. Elsevier, 2008; ISBN 978-0-12-372585-1; Library of Congress Cataloging-in-Publication Data, Digital watermarking and steganography/Ingemar J. Cox ... [et al.]*.
3. Techtarget.com, Margaret Rouse & Borys Pawliw, 2014 *Cryptography;* [http://searchsoftwarequality.techtarget.com/definition/cryptography]
4. Melinos Avertkiou, *Digital Watermarking*
5. I. Daubechies *Basics of Wavelets; (Ten Lectures on wavelets; Orthonormal Bases of Compactly Supported Wavelets).*

6. Bangxi Yu & Raj Jain, 2011 *A Quick Glance at Digital Watermarking*; Academic Project Report [www.cse.wustl.edu].
7. CSP Research and & Development, 2015 *Embedding Interactive Data into an Audio-visual Content by Watermarking*, [www.iitg.ernet.in]
8. Ingemar J. Cox, MatthewL.Miller, Jeffrey A. Bloom, Jessica Fridrich and Ton Kalker, *Digital Watermarking and Steganography Second Edition*; The Morgan Kaufmann Series in Multimedia Information and Systems Series Editor, Edward A. Fox, Virginia Poytechnic University; Elsevier.
9. Amara Graps, 1995 *Introduction to Wavelets*, IEEE Computational Science and Engineering, Summer 1995, vol. 2, num. 2, IEEE Computer Society, 10662 Los Vaqueros Circle, Los Alamitos, CA 90720, ©1995
10. Brani Vidakovic and Peter Mueller, 1991, *Wavelets for Kids*: A Tutorial Introduction; AMS Subject Classification: 42A06, 41A05, 65D05.
11. Vaishali S. Jabade & Dr. Sachin R. Gengaje, 2011 *Literature Review of Wavelet Based Digital Image Watermarking Techniques; International Journal of Computer Applications (0975 – 8887) Volume 31– No.1; 2011*.
12. Yu-Ping Wang and Shi-Min Hu, *A new watermarking method for 3D model based on integral invariant*; Department of Computer Science and Technology, Tsinghua University.
13. Giorgos Louizis, Anastasios Tefas and Ioannis Pitas, 1999 *Copyright Protection Of 3D Images Using watermarks Of Specific Spatial Structure*; Department of Informatics, Aristotle University of Thessaloniki; Box 451, Thessaloniki 54006.
14. N. Nikolaidis!, I. Pitas, 1998 *Robust image watermarking in the spatial domain*; Elsevier, Signal Processing 66 (1998) 385Ð403; 0165-1684/98/$19.00 (1998 Elsevier Science B.V. All rights reserved. PII S0165-1684(98)00017-6
15. Dipti Prasad Mukherjee, Subhamoy Maitra, and Scott T., 2004 *Spatial Domain Digital Watermarking of Multimedia Objects for Buyer Authentication*; IEEE Transactions On Multimedia, Vol. 6, No. 1, February 2004
16. Jamal A. Hussein; 2010 *Spatial Domain Watermarking Scheme for Colored Images Based on Log-average Luminance*; Journal of Computing, Volume 2, Issue-1, 2010, ISSN 2151-9617 [Https://Sites.Google.Com/Site/Journalofcomputing/]
17. Baisa L. Gunjal & R.R. Manthalkar 2010 *An Overview Of Transform Domain Robust Digital Image Watermarking Algorithms*; Journal of Emerging Trends in Computing and Information Sciences; Volume 2 No. 1; ISSN 2079-8407; ©2010-11 CIS Journal, All rights reserved.
18. MSDN – Microsoft, 2014 *Choose an Encryption Algorithm – SQL Server 2014;* Microsoft Developer Network; © 2015 Microsoft;
19. Gary C. Kessler, 2015 *An Overview of Cryptography;* 1999 Edition of *Handbook on Local Area Networks*, published by Auerbach in September 1998© 1998-2015
20. Pooja Dabas & Kavita Khanna, 2013 *Efficient Performance of Transform Domain Digital Image Watermarking Technique over Spatial Domain*; International Journal of Advanced Research in Computer Science and Software Engineering; Volume 3, Issue 6, 2013; ISSN: 2277 128X
21. Pooja Dabas & Kavita Khanna, 2013 *A Study on Spatial and Transform Domain Watermarking Techniques;* International Journal of Computer Applications © 2013 by IJCA Journal, Volume 71 - Number 14 , Publication: 2013 Authors:, DOI: 10.5120/12429-9124
22. Kamran Hameed, Adeel Mumtaz, and S.A.M. Gilani, *2006 Digital Image Watermarking in the Wavelet Transform Domain*; World Academic of Science, Engineering and Technology 13 2006
23. Digital Watermarking – [http://en.wikipedia.org/wiki/Digital_watermarking]
24. Jung-Hee Seo, and Hung-Bog Park, 2006 *Data-Hiding Method using Digital Watermark in the Public Multimedia Network*; International Journal of Information Processing Systems, Vol.2, No.2, June 2006; Copyright Ⓒ 2006 KIPS (ISSN 1738-8899)
25. Demin Wang, Liang Zhang, Robert Klepko, and André Vincent *A Wavelet-Based Video Codec And Its Performance;* Communications Research Centre, Canada

