# Jurnal Teknologi

## **DIGITAL IMAGE OF WATERMARKING: A SURVEY**

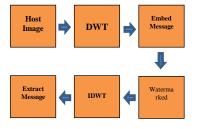
Reza Aghababaeyan<sup>a\*</sup>, Seyed Fariborz Seyed Asrari<sup>b\*</sup>

<sup>a</sup>Department of Computer Engineering, Faculty of Advance Informatics School, University Teknology of Malaysia <sup>b</sup>Department of Computer Engineering, Faculty of Computer Science, Azad University of Dameghan

Article history Received 16 January 2015 Received in revised form 25 June 2015 Accepted 15 December 2015

\*Corresponding author areza26@live.utm.my

## Graphical abstract



## Abstract

This paper reviews the research status of digital image watermarking in the past decade. Considering there are too many publications about the digital image watermarking, we summarize main approaches and point out interesting parts of the researches. Multimedia watermarking technology offers advanced right away throughout the last several years. An electronic watermark is actually facts that are certainly imperceptibly and robustly inserted in the number data in ways that the idea is not taken off. Some sort of watermark commonly consists of information about the foundation, status, or perhaps receiver on the number data. In this review paper, certain requirements and apps intended for watermarking are usually reviewed. Purposes consist of copyright defense, data monitoring, and data pursuing. The fundamental concepts involving watermarking techniques are usually given and highlighted along with offered watermarking options for pictures, movie, audio tracks, text message files, along with advertising. Robustness and safety measures elements are usually mentioned in greater detail. Finally, several remarks are created around the cutting edge and possible potential trends inside watermarking technology.

Keywords: Watermarking, Image, Audio, Video, Multimedia1

© 2016 Penerbit UTM Press. All rights reserved

## **1.0 INTRODUCTION**

Multimedia systems creation in addition to distribution, once we notice these days, will be almost all a digital, in the writing methods connected with information vendors for the receivers. Why people love a digital control in addition to distribution, just like noise-free sign, software program rather than electronics control, in addition to enhanced reconfigurability connected with systems, are all recognized in addition to clear. Not so clear are the negatives connected with a digital media distribution. For instance, in the point of view connected with media producers in addition to information vendors, the possibility intended for limitless duplication connected with digital information without loss of fidelity will be unfavorable

because it might result in sizeable financial loss. A Digital copy defense or copy prevention methods are only of limited value because access to cleartext versions of protected data must at least be granted to paying recipients which can then develop as well as disperse illegitimate copies. Technical attempts to prevent copying have in reality always been circumvented.

Just one staying means for the particular protection involving cerebral property rights [IPR] embeddina involvina would be the digital watermarks directly into multimedia systems information. The watermark is a digital code irremovably, robustly, and imperceptibly embedded in the host data and typically contains information about origin, status, and/or destination of the data. However, not directly used for copy protection, it can

## **Full Paper**

at least help identifying source and destination of multimedia data and, as a "last line of defense," make it possible for appropriate follow-up actions in case there are alleged copyright violations.

Even though copyright protection may be the majority of prominent application of watermarking techniques, some others are present, such as data authentication by means of fragile watermarks which usually are impaired or destroyed by manipulations, embedded transmission of value added services within multimedia data, and embedded data labeling for other purposes than copyright protection, like files monitoring and tracking. A case for a data-monitoring system may be the automatic registration and monitoring of broadcasted radio programs in a way that royalties are automatically paid to the IPR owners of the broadcast data.

The development of watermarking technique involves several pattern tradeoffs. Watermarks should be robust against standard data manipulations, as well as digital-to analog alteration and digital format conversion. Security is a special concern, and watermarks should resist even attempted attacks by knowledgeable individuals. On the other hand, watermarks should be imperceptible and convey as much information as possible. In general, watermark embedding and retrieval should have low complexity because for various applications, real-time watermarking is desirable. Many of these [partly contradicting] requirements and the resulting design constraints will likely be discussed in more detail through the paper [1]

# 2.0 STEGANOGRAPHY AND WATERMARKING HISTORY AND TERMINOLOGY

### 2.1 History

Taking that approach to be able to connect covertly can be as aged as transmission they. Initial reports that are seeing as beginning files involving concealed transmission appear in your aged Language of ancient Greece books, one example is, throughout Homer's Iliad, or throughout reports by Herodotus. The phrase "steganography," which can be even now available currently, derives in the Language of ancient Greece language and suggests concealed transmission. [Kobayashi, 1997] [1] and [Petitcolas, Anderson, & Kuhn, 1999] [2]. Paper watermarks seem in the art of handmade papermaking nearly seven hundred in years past. The actual oldest watermarked paper found in archives dates back to 1292 and contains it is origin in Fabriano, Italy, which in turn is the birthplace of watermarks.

Right at the end from the thirteenth centuries, about forty papers mills were sharing the paper marked in Fabriano and producing papers with different formatting, quality, and cost. After their invention, watermarks rapidly distribute more than Italy and then more than Europe, and although originally used to indicate this papers brand name or even papers generator, they will later serve as indication for papers formatting, high quality, and also strength and were also used to date and authenticate paper. An excellent case illustrating this legitimate power of watermarks is really an even in 1887 in France termed "Des Decorations" [3].

The actual analogy in between report watermarks, steganography, and also digital watermarking is usually obvious, and in fact, report watermarks in money costs or maybe plastic stamps [4] basically influenced the initial usage of the term watermarking in the context of digital files. The concept of digital image watermarking came about separately with 1990 [5-6] and also all around 1993 [7]. Tirkel et al. [8] coined the word "water mark" that started to be "watermark" later on. This got some more many years until eventually 1995/1996 just before watermarking received remarkable interest. Ever Since then, digital watermarking has gained a lot of attention and has evolved very quickly and while there are many topics open up regarding additional investigation, practical working doing the job approaches as well as systems have been developed. In this document, we introduce the concepts and illustrate them with some of the work that has been published. While attempting to be as complete as possible, we can still only supply a hard summary.

Nowadays, we are obviously concerned with digital communication. Like conventional analog communication, furthermore in digital communication there is interest for procedures that allow the transmission of information hidden or embedded in other data.

### 2.2 Steganography

Stands for techniques in generally that make it possible for secret communication, usually through embedding or hiding the secret information in different, unsuspected data. Watermarking, in contrast to steganography, has got the further idea connected with robustness against attacks. Even if the existence of the hidden information is known it is difficult—ideally impossible—for an attacker to destroy the embedded watermark, even if the algorithmic principle of the watermarking method is public. In cryptography, this is known as Kerkhoffs law: some sort of cryptosystem should be secure, even if an attacker knows the cryptographic ideas as well as technique used but does not have the appropriate key. [1]

### 2.3 Watermarking

Watermarking and Steganography are thus more complementary than competitive approaches. Inside the remainder of this research, we focus on watermarking methods and not on steganography methods generally. To have an overview of steganography methods will be described [2-11-12].

### 2.4 Data Hiding and Information Embedding

They are employed throughout numerous contexts, but they do typically give the meaning either steganography or even applications "between" steganography and also watermarking, which means applications the place that the existence of the embedded data are publicly known, but there is no need to protect it. This is typically the case for the embedded transmission of auxiliary information or even products and services [8] that are openly available and do not relate to copyright defense or even conditional access uses.

### 2.5 Fingerprinting and Also Labeling

Fingerprinting and also labeling are terms that denote special applications of watermarking. They relate to copyright defense applications exactly where information about originator and recipient of digital data is embedded as watermarks. The person watermarks, which can be unique codes out of a series of codes, are usually known "fingerprints" or even "labels."

### 2.6 Bit-Stream Watermarking

Bit-stream watermarking is oftentimes used for information hiding or even watermarking of compressed information, an example, compressed online video.

The term embedded signatures has been used instead of "watermarking" throughout earlier publications since it potentially leads to dilemma along with cryptographic digital signatures.14, it is almost always not used longer. Cryptographic signatures assist pertaining to authentication purposes. They may be used to detect alterations of the signed data and to authenticate the sender. Watermarks, however, are only throughout special applications used for authentication and are normally designed to resist alterations and modifications.

Visible watermarks, as the name says, are visual patterns, like logos, which are inserted into or overlaid on images [or video], very similar to visible paper watermarks. However, the name is confusing since visible watermarks are not watermarks in the sense of this paper. Visible watermarks are mainly applied to images, for example, to visibly mark preview images available in image databases or on the World Wide Web in order to prevent people from commercial using these kinds of images. A visible watermarking method devised simply by Braudaway *et al.* [15].

## **3.0 DIGITAL WATERMARKING**

## 3.1 Requirement

The basic demands in watermarking apply to all media and are very intuitive [22].

- i. A watermark should communicate all the information as possible, so this means the particular watermark files rate should be high.
- ii. The watermark ought to normally always be magic formula and should just always be available by means of authorized parties. This demand is referred to as security of the watermark and is usually achieved by the means of cryptographic tips.
- A watermark ought to stay in the particular iii. host files regardless of whatever happens to the host files, in addition all possible signals processing which may occur, in addition all hostile attacks which unauthorized parties may attempt. This requirement is referred to as robustness of the watermark. It is a key requirement for copyright protection or conditional access applications, however a smaller amount of importance to programs where the watermarks will not be forced to always be cryptographically secure, in instance of, for applications where watermarks share general public information.
- iv. Any watermark really should, although staying irremovable, always be imperceptible.

In the following, several of the mentioned requirements plus the resulting design issues are highlighted with much more detail.

### 3.2 Watermark Security and Keys

in the event safety measures, i.e., secrecy of the embedded information, becomes necessary, one or perhaps several secret and cryptographically secure keys need to be useful for the actual embedding and removal extraction process. One example is, in lots of schemes, pseudorandom signs are embedded as watermarks. In this case, the description and the seed of the pseudorandom number generator may be used as key. There are two levels of secrecy. In the first level, an unauthorized user can neither read nor perhaps decode an embedded watermark nor can he detect if a given set of data contains a watermark. The second level allow unauthorized customer to detect when data are generally watermarked, however, the embedded information cannot be read without having the secret key. This kind of schemes can certainly, for example, embed two watermarks, one that has a public key [16] and the other that has a secret key [17].

#### 3.3 Robustness

Inside design of any watermarking scheme, watermark robustness is usually one of the many main issues, since robustness against data distortions introduced through standard data processing and attacks is a major requirement. Standard data processing includes all data manipulation and modification that the data might undergo in the usual distribution chain, for instance of data printing, editing, producing, enhancement [18-19-78] and format conversion. "Attack" means data manipulation with the purpose of impairing, doing damage, or maybe removing the embedded watermarks.

### 3.4 Imperceptibility

One of the main specifications for watermarking is the perceptual transparency. The data embedding process must not bring in any perceptible artifacts into the host data. Alternatively, for high robustness, it is appealing that the watermark amplitude will be up to possible. Thus, the design of any watermarking process always involves a tradeoff between imperceptibility and robustness. It could be maximum to be able to embed a watermark just below the threshold of perception. However, this kind of threshold will be difficult to determine for real-world image, video and audio signs. Various measures to determine objectively identified distortion and the threshold of perception get already been proposed for the mentioned media [20.-21].

# 3.5 Watermark Recovery with or Even Without the Original Data

Watermark recovery is frequently more robust if the original, unwatermarked data can be obtained. Additionally, availability of an original data set in the recovery process makes it detection and inversion of distortions which often alter the data geometry. This can help, for example, when a watermarked image may be rotated by means of an attacker. On the other hand, usage of an original data is not possible in most instances, for example, in applications for instance data monitoring or tracking. In a few publications, this kind of techniques to be named "blind" watermarking techniques [22-23].

# 3.6 Watermark Extraction or Even Verification of Presence for Just a Presented Watermark

In the literature, two various kinds of watermarking systems can be found: systems that embed a selected information or even pattern and also verify the existence of the [known] data later on in the watermark recovery—usually make use of some type of hypothesis testing—and systems that embed arbitrary information into the host data. The primary kind, proof of the presence of a known watermark, is sufficient for many of us copyright-protection applications [24].

The second kind, embedding of arbitrary data, is usually, for example, helpful for image monitoring online the Internet with smart real estate agents where it would not only be of interest to locate images, but to help classify them. In these cases, the embedded watermark could serve as an image recognition amount.

## 4.0 BASIC WATERMARKING PRINCIPLES

The basic notion in watermarking is to add a watermark sign to the host data for being watermarked such that the watermark sign is actually unobtrusive and secure inside signal mixture but can partly or fully be recovered from the signal mixture later on if the correct cryptographically secure key needed for recovery is used. To be sure imperceptibility of the modification caused by watermark embedding, a perceptibility criterion of some sort is used. This is really implicit or even specific, host data adaptive or even fixed, but it is crucial. As a consequence of the required imperceptibility, the individual examples [e.g., pixels or even alter coefficients] that are used for watermark embedding could simply end up being alter by simply an amount relatively small to their average amplitude.

Seeing that claimed prior to, watermark method complete generally speaking use more than one cryptographically secure keys to be sure security against manipulation and erasure on the watermark.

There are three main issues in the design of a watermarking technique.

1. The first two issues, watermark transmission pattern design and watermark signal embedding, can be a single, and specifically for strategies were the embedded watermark are usually host signal adaptive.

Figures 1 and 2 illustrate the theory. Figure 1 indicates the simple watermarking scheme for that embedding process. The input to the scheme is the watermark, the host data, and a suggested general public or even secret key. The host data may, depending on the program, be uncompressed or even pressurized, even so, the majority of recommended strategies work with uncompressed data. The watermark could be of any dynamics, say for example a number, text, or even an image. The secret or even general public key can be used to help enforce security. In the event the watermark isn't being read simple by unauthorized functions, secrets or even general public key can be used to protect the watermark. In the event combination with a secret or a public key, the watermarking techniques are often referred to as secret and general public watermarking techniques, respectively. The output of the watermarking scheme is the modified, i.e., watermarked data. The generic watermark recovery process is depicted

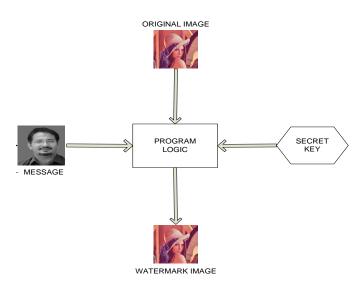
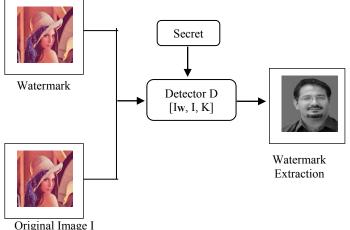


Figure 1 General Watermark embedding process

Figure 2 inputs to the scheme are the watermarked data, the secret or public key and, depending on the method, the original data and the original watermark. The output of the watermark recovery process is usually often the saved watermark or even some sort of assurance determine implying exactly how most likely it is for that given watermark at the input to be contained in the information under examination.



fightar fillage f

Figure 2 General Watermark Extracting process

Design and style of the watermarked sign W for being put into the host signal. Generally, the watermark signal depends on using a key k and also watermarks information [79].

$$W = F0 (I, K)$$
(1)

Possibly, it may also well depend on the host data X into which it is embedded

$$W = F0 (I, K, X)$$
(2)

Design of the embedding process that will include the watermark sign W in to the host data Xcontaining watermarked data Y.

$$Y = F1 (X, W)$$
<sup>(3)</sup>

Design of the corresponding extraction process that will recover the particular watermark information from the signal mixture when using the key with help of the original.

$$\mathbf{I} = \mathbf{g} \ (\mathbf{X}, \mathbf{Y}, \mathbf{K}) \tag{4}$$

Or without the original

$$\mathbf{I}'=\mathbf{g} \ (\mathbf{Y},\mathbf{K}) \tag{5}$$

Numerous proposed watermarking strategies use ideas by spread-spectrum radio communications.25, [26-27] DCT Wavelet watermarking [28-29], FFT Transform [30], text document watermarking [31-32-33].

The watermark signal is usually designed as a white [34-35] or perhaps colored pseudorandom signal having, e.g., Gaussian [36], uniform, or perhaps [37-38-39-40-41], density bipolar likelihood functionality [pdf]. To prevent presence with the embedded watermark, an implicit or perhaps explicit spatial [42-43-44-45] or perhaps spectral [46-47-48-49-50-51] framing is usually applied with the objective to attenuate the watermark throughout parts of image where it would or else come to be visible. The resulting watermark signal will be from time to time sparse as well as actually leaves image pixels unchanged [52-53], although generally it is dense as well as varies pixels with the image to get watermarked. The watermark signal is usually designed within the spatial domain, although sometimes likewise inside a transform domain just like the full-image discrete cosine transforms [DCT] domain [54] or perhaps block-wise DCT domain [55]

The signal embedding is done by addition [56-57-58] or perhaps signal-adaptive [I. at the. scaled] improvement 59, generally on the luminance channel alone, although sometimes also to color channels, or perhaps just to color channels [60] The improvement usually can take place in the spatial domain, or perhaps in transform domains for example the discrete Fourier transform [DFT] domain [61] the wavelet domain [62-63-64] the fractal domain.65, the Hadamard domain [66-67] the Fourier–Mellin domain [68-69] or the Radon domain [70] It is often claimed that embedding within the transform [mostly DCT or wavelet] domain is advantageous in terms of visibility and security [71]

on the other hand, even though some writers argue which the watermarks should be embedded directly into low frequencies [72-73] different argue that they really should rather end up be embedded into the medium [75-74] or high frequencies. The truth is it has been shown [75-76] in which regarding highest robustness watermarks should be embedded signal adaptively into the same spectral components in which the host data already populate. For images and video, most of these can be the low frequencies. Because explain before, watermark signal generation and watermark embedding are sometime treated jointly. For many recommended methods, they can't be regarded independently, especially if the watermark is signaling adaptive [77]

## 5.0 CONCLUSION

Within this overview paper, we reviewed the most important aspects, design specifications, system issues, and techniques for digital watermarking. The historical roots of digital watermarking derive obtain mainly from steganography, the art of data hiding. Though digital watermarking along with steganography has been in a few senses identical, the main change is based on the idea connected with robustness for digital watermarks. Watermark robustness is one of the important design issues, besides imperceptibility.

A number of approaches have been proposed to invertible be able to establish techniques noninvertible, which including hashing and time stamping. Although working programs are already throughout accessible, research а digital watermarking must go on. There is a huge demand from articles services in addition to IPR owners. The market is currently far from being saturated and many more companies are expected to be founded in the near future. The question whether digital watermarks will be used as legal proof in court is not yet decided and difficult to answer. There are, on the other hand, other applications, like multimedia copy protection systems and data broadcast monitoring, in which we will have watermarking functioning.

### References

- [1] M. Kobayashi. 1997. Digital watermarking: *Historical Roots*. IBM Research, Tokyo Res. Lab., Tech. Rep.
- [2] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn. 2001. Information Hiding—A Surveys. 1062–1078.
- [3] O. Emery. 1985. Des filigranes du papier. A. T. I. P. Bull.: Bull. Del' Association Technique de l' Industrie Papetiere. 12(6): 185-188.
- [4] K. Tanaka, Y. Nakamura, and K. Matsui. 1990. Embedding Secret Information into a Dithered Multilevel Image. In Proc. 1990 IEEE Military Commun. Conf. Sept 1990. 216-220.
- [5] A. Tirkel. 1990. Embedding the Attribute Information into a Dithered Image, Syst. Private Communication. Japan. 1990. 21(7).

- [6] G. Caroni. 1993. Remittal un-authorisiertor Verteiler Von Maschinenlesbaren Daten. ETH, Zurich, Switzerland, Tech. Aug 1993.
- [7] A. Tirkel, G. Rankin, R. van Schyndel, W. Ho, N. Mee, and C. Osborne. 1993. Electronic Water Mark. In Proc. (DICTA). 666-672.
- [8] B. Schneider. 1996. Applied Cryptography. New York: Wiley.
- [9] M. Kobayashi. 1997. Digital Watermarking: Historical Roots. IBM Research, Tokyo Res. Lab. Tech. Rep.
- [10] M. D. Swanson, M. Kobayashi, and A. H. Tewfik. 1998. Multimedia Data Embedding and Watermarking Technologies. Proc. IEEE Special Issue on Multimedia Signal Processing. 1064-1087.
- [11] M. Swanson, B. Zhu, and A. Tewfik. 1997. Data Hiding for Video-In Video. In Proc. IEEE Int. Conf. Image Processing 1997 (ICIP). Santa Barbara, CA. 676-679.
- [12] G. W. Braudaway, K. A. Magerlein, and F. C. Mintzer. 1996. Color Correct Digital Watermarking Of Images. U.S. Patent 5 530 759.
- [13] S. Sarbavidya, S. Karform. 2010. Implementation of Security in E-Procurement Environment Using Public Key Digital Watermarking.
- [14] D. V. N. KoteswaraRao. 2012. Robust Image Watermarking using DCT & Wavelet Packet Denoising. International Journal of Scientific & Engineering Research. 3(5): 2229-5518.
- [15] A. Kumar Gupta. 2012. A Robust And Secure Watermarking Scheme Based on Singular Values Replacement. Indian Academy of Sciences. 37(4): 425-440.
- [16] M. Gaata. 2012. Evaluation of Perceptual Quality for Watermarked Images Based on Combination of Fuzzy Similarity Measures Using Neural Network, (IJCSI). International Journal of Computer Science. 9(4): 1694-0814 [Online].
- [17] M. Kutter and F. Petitcolas. 1999. A Fair Benchmark for Image Watermarking Systems. SPIE IS&T/SPIE's 11th Annu. Symp. Electronic Imaging '99: Security and Watermarking of Multimedia Contents. 3657.
- [18] T. Huynh, T. Le Tien. 2013. An Efficient Blind Watermarking Method based on Significant Difference of Wavelet Tree Quantization using Adaptive Threshold. International Journal of Electronics and Electrical Engineering. 1(2).
- [19] M. Baghel, R. Bhardwaj, S. Shivani. 2013. Authenticating Images using Blind Fragile Watermarking Scheme based on LSB Technique. International Journal of Computer Applications. 62(18).
- [20] F. hartung, M. kutter. 1999. Multimedia Watermarking Techniques. Proceedings of the IEEE. 87(7).
- [21] G. Cooper and C. McGillem. 1986. Modern Communications and Spread Spectrum. New York: McGraw-Hill.
- [22] P. G. Flikkema. 1997. Spread-spectrum techniques for wireless communications. *IEEE Signal Processing Mag.* 14: 26-36.
- [23] R. Pickholtz, D. Schilling, and L. Milstein. 1982. Theory of Spread Spectrum Communications—A Tutorial. *IEEE Trans. Common.* 30: 855-884.
- [24] Kobayashi, M. 1997. Digital Watermarking: Historical Roots. IBM Research, Tokyo Res. Lab. Tech. Rep.
- [25] Petitcolas, Fabien AP, Anderson, Ross J, & Kuhn, Markus G. 1999. Information Hiding-A Survey. Proceedings of the IEEE. 87(7): 1062-1078.
- [26] L, Bai Ying. 2011. Blind and Robust Audio Watermarking Scheme Based on SVD-DCT Blind and Robust Audio Watermarking Scheme based on SVD-DCT. 91(8): 1973-1984.
- [27] M. Amit Phadikar. 2011. Region based QIM Digital Watermarking Scheme for Image Database in DCT Domain. 37(3): 339-355.
- [28] V. Kalaskar, R. Jadhav, Y. Kshirsagar. 2011. Application of Adaptive Watermarking for Efficient Image Annotation for

Data Embedding, International Journal of Electronics Communication and Computer Engineering. 2(1).

- [29] A.dnan M. Alattar and Osama M. Alattar. 2004. Watermarking Electronic Text Documents Containing Justified Paragraphs and Irregular Line Spacing (SPIE).
- [30] J. Brassil, S. Low, N. Maxemchuk, and L. O'Gorman. 1995. Electronic Marking and Identification Techniques to Discourage Document Copying. *IEEE J. Select. Areas Commun.* (13): 1495-1504.
- [31] Hiding Information in Document Images. 1995. In Proc. 29th Annu. Conf. Information Sciences and Systems (CISS). Johns Hopkins Univ., Baltimore, MD, Mar. 482-489.
- [32] A. Tirkel, G. Rankin, R. van Schyndel, W. Ho, N. Mee, and C.Osborne. 1993. Electronic Water Mark. In Proc. (DICTA). 666-672.
- [33] R. G. van Schyndel, A. Z. Tirkel, and C. F. Osborne. 1994. A Digital Watermark. In Proc. Int. Conf. Image Processing (ICIP). (2): 86-89.
- [34] Secure spread Spectrum Watermarking for Images. 1995 Audio, and Video, NEC Res. Inst., Princeton, NJ, Tech. Rep. 95-10.
- [35] U, KinTak. 2010. A Robust Image Watermarking Algorithm Based on Non-Uniform Rectangular Partition and DCT-SVD. International Conference on Measuring Technology and Mechatronics Automation. (ICMTMA) 2010, (1): 327-330.
- [36] U, KinTak. 2009. A Robust Image Watermarking Algorithm Based on Non-uniform Rectangular Partition and DWT. 2nd Conference on Power Electronics and Intelligent Transportation System. (PEITS).
- [37] Qi, Dongxu. 2009. A robust Image Watermarking Algorithm Based on Non-Uniform Rectangular Partition and Encryption Scrambling, ICICS 2009. Conference Proceedings of the 7th International Conference on information, Communications and Signal Processing.
- [38] Hu, Shengdun. 2009. A Robust Image Watermarking Algorithm Based on Non-Uniform Rectangular Partition and SVD. Pacific-Asia Conference on Knowledge Engineering and Software Engineering. KESE 2009. 163-166.
- [39] Maeno, Kurato. 2002. New Semi-Fragile Image Authentication Watermarking Techniques Using Random Bias and Non-Uniform Quantization. Proceedings of SPIE-The International Society for Optical Engineering. 4675: 659-670.
- [40] Waltz, Jacob. 2013. Spatial Accuracy and Performance of a Mixed-Order, Explicit Multi-Stage Method for Unsteady Flows. International Journal for Numerical Methods in Fluids. 71(11): 1361-1368.
- [41] Huang, Shengli. 2013. Reconstructing Satellite Images to Quantify Spatially Explicit Land Surface Change Caused by Fires and Succession: A Demonstration in the Yukon River Basin of Interior Alaska, ISPRS Journal of Photogrammetry and Remote Sensing. 79: 94-105.
- [42] Jackson, Bethanna. 2013. Polyscape: A GIS mapping Framework Providing Efficient and Spatially Explicit Landscape-Scale Valuation of Multiple Ecosystem Services. Landscape and Urban Planning. 112(1): 74-88.
- [43] Schädler, Sebastian. 2013. Corrigendum to Spatially explicit computation of Sustainability Indicator Values for the Automated Assessment of Land-Use Options. Landscape and Urban Planning. 114: 113.
- [44] Bellaaj, Maha. 2012. Comparative Analysis of Audio Watermarking Technique in MDCT Domain with Other References in Spectral Domain. International Multi-Conference on Systems, Signals and Devices. (SSD) Summary Proceedings.
- [45] Liu, Yang. 2012. Spectral Watermarking for Parameterized Surfaces. IEEE Transactions on Information Forensics and Security. 7(5): 1459-1471.
- [46] Ma, Long. 2011. Watermarking spectral Images with Three-Dimensional Discrete Wavelet Transform and Singular Value Decomposition Under Various Illumination Conditions, Proceedings of SPIE-The International Society

for Optical Engineering. Multispectral Image Acquisition, Processing, and Analysis. MIPPR 2011.8002.

- [47] Yan, Bin. 2013. Seismic Responses of Railway Track-Bridge System Under Travelling Wave Effect, Zhendong Gongcheng Xuebao. Journal of Vibration Engineering. 26(3): 357-362.
- [48] Yan, Bin. 2013. Quantum correlations are Tightly Bound by the Exclusivity Principle. Physical Review Letters. 110(26).
- [49] Wu, Rina. 2013. Effect of LC molecular Orientation on the Transmission Spectrum of One-dimensional Optics Multilayer Film Photonic Crystal. Hongwai yu Jiguang Gongcheng/Infrared and Laser Engineering. 42(3): 738-741.
- [50] V. Darmstaedter, J.-F. Delaigle, D. Nicholson, and B. Macq. 1998. A block Based Watermarking Technique For MPEG-2 Signals: Optimization and Validation on Real Digital TV Distribution Links. In Proc. European Conf. Multimedia Applications, Services, and Techniques (ECMAST). Berlin, Germany.
- [51] 1998. Digital Signature of Color Images Using Amplitude Modulation. J. Electron. Imaging. 7(2): 326-332.
- [52] Wang, Xin. 2013. Digital Image Hiding Using Iterative Blending in Discrete Cosine Transform Domain. Applied Mechanics and Materials. 318: 63-66.
- [53] E. Koch and J. Zhao. 1995. Toward robust and Hidden Image Copyright Labeling. In Proc. Workshop Nonlinear Signal and Image Processing. Marmaros, Greece.
- [54] C. Langelaar, J. C. A. ven der Lubbe, and R. L. Lagendijk. 1997. Robust labeling Methods for Copy Protection of Images. In Proc. Electronic Imaging, San Jose, CA. 3022: 298–309.
- [55] N. Nikolaidis and I. Pitas. 1996. Copyright Protection Of Images Using Robust Digital Signatures. In Proc. ICASSP '96, Atlanta, GA.
- [56] R. G. van Schyndel, A. Z. Tirkel, and C. F. Osborne. 1994. A Digital Watermark. In Proc. Int. Conf. Image Processing (ICIP). 2: 86-89.
- [57] M. Barni, F. Bartolini, V. Cappellini, and A. Piva. 1998. A DCT Domain System for Robust Image Watermarking. Signal Processing (Special Issue on Watermarking). 66(3): 357-372.
- [58] B.Pradosh. 2012. A New Invisible Color Image Watermarking Framework Through Alpha Channel. IEEE-International Conference on Advances in Engineering, Science and Management (ICAESM). 302-308.
- [59] J. J. K. ' O Ruanaidh, W. J. Dowling, and F. M. Boland. 1996. Phase Watermarking of Digital Images. In Proc. Int. Conf. Image Processing (ICIP). 3: 239-242.
- [60] W. Yingli. 2013. Digital Image Watermarking Based on Texture Block and Edge Detection in the Discrete Wavelet Domain. International Conference on Sensor Network Security Technology and Privacy Communication System, SNS and PCS.
- [61] B, Yong. 2013. Image Watermark Detection in the Wavelet Domain using Bessel K densities. IET Image Processing. 7(4): 281-289.
- [62] B, Yong. 2013. Locally Optimal Detection of Image Watermarks in the Wavelet Domain Using Bessel K Form Distribution. IEEE Transactions on Image Processing. 22(6): 2372-2384.
- [63] Y, Shu-Guo. 2005. A Fractal Watermarking Scheme For Images in the DCT Domain. Proceedings of SPIE-The International Society for Optical Engineering. (6041). ICMIT 2005: Information Systems and Signal Processing.
- [64] Z, Peijia. 2013. Walsh-Hadamard transform in the Homomorphic Encrypted Domain and Its Application in Image Watermarking. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). 7692 LNCS. 240-254.
- [65] M. Ramkumar and A. Akansu. 1999. On the Choice of Transforms for Data Hiding In Compressed Video. In Proc. IEEE Int. Conf. Acoustics, Speech, and Signal Processing. (ICASSP) Phoenix, AZ.

#### 216 Reza Aghababaeyan & Seyed Fariborz Seyed Asrari / Jurnal Teknologi (Sciences & Engineering) 78:1 (2016) 209–216

- [66] J. J. K. O Ruanaidh and T. Pun. 1997. Rotation, scale and Translation Invariant Digital Image Watermarking. In Proc. IEEE Int. Conf. Image Processing 1997 (ICIP 97). Santa Barbara, CA. 1: 536-539.
- [67] Signal Processing. 1998. Rotation, Scale, and Translation Invariant Spread Spectrum Digital Image Watermarking. Special Issue on Watermarking. 66(3): 303-318.
- [68] W, Wang. 2009. Robust Image Watermarking Scheme Based on Phase Features in DFT Domain and Generalized Radon Transformations. Proceedings of the 2009 2nd International Congress on Image and Signal Processing, CISP'09.
- [69] M. Barni, F. Bartolini, V. Cappellini, A. Piva, and F. Rigacci. 1998. A M. A. P. Identification Criterion for DCT-based Watermarking. In Proc. Europ. Signal Processing Conf. (EUSIPCO '98). Rhodes, Greece.
- [70] 1995. Secure Spread Spectrum Watermarking for Images, Audio, and Video. NEC Res. Inst, Princeton, NJ, Tech. Rep.
- [71] J. J. K. O Ruanaidh and T. Pun. 1997. Rotation, Scale And Translation Invariant Digital Image Watermarking. In Proc. IEEE Int. Conf. Image Processing 1997 (ICIP 97), Santa Barbara, CA. 1: 536-539.
- [72] Santorini, Greece. 1997. Digital Watermarking for Video. In Proc. of DSP'97, July 1997.
- [73] F. Deguillaume, G. Csurka, J. O Ruanaidh, and T. Pun. 1999. Robust 3D DFT Video Watermarking. In IS&T/SPIE's 11th Annu. Symp. Electronic Imaging '99: Security and

Watermarking of Multimedia Contents. San Jose, CA, Jan. 3657.

- [74] J. K. Su and B. Girod. 2007. On the imperceptibility and Robustness of Digital Fingerprints, Submitted for Publication. Power spectrum Condition for L2-Efficient Watermarking, Submitted For Publication.
- [75] B. Chen and G. W. Wornell. 1998. Digital Watermarking And Information Embedding Using Dither Modulation. In Proc. IEEE Workshop Multimedia Signal Processing, Los Angeles, CA.
- [76] R. Aghababaeyan, T. Siddiqui, N. AhmadKhan. 2011. Forecasting the Tehran Stock Market by Artificial Neural Network. International Journal of Advanced Computer Science and Applications (IJACSA), Special Issue on Artificial Intelligence. 1(3).
- [77] R. Aghababaeyan, S., bin Abdullah. M. Zamani. 2013. New Approach of Non-Blind Watermarking Algorithm, PPI UTM TESIC 2013 Technology, Education, and Science International. Nov 1, 2013.
- [78] Abdolvahab Ehsanirad. 2010. Plant Classification Based on Leaf Recognition. International Journal of Computer Science and Information Security. 8(4): 78-81.
- [79] Mohd Shafry Mohd Rahim, Abdolvahab Ehsani Rad, Amjad Rehman, and Ayman Altameem. 2014. Extreme Facial Expressions Classification Based on Reality Parameters. 3D Research. 5(3): 1-8.