ISSN: 0067-2904
GIF: 0.851

Embedding a Digitized Watermark Upon Colored Image Using Wavelet Transform with Comparative Technique

Matheel Emaduldeen Abdulminuim*
Department of Computer Science, University of Technology, Baghdad, Iraq

Abstract

A special methodology for adding a watermark for colored (RGB) image is formed and adding the wavelet transform as a tool during this paper. The watermark is added into two components. The primary one is by taking the key that contain associate eight range from (0...7) every range in it determines the actual bit position in specific component of canopy image. If that bit is analogous to the bit in watermark, (0) are hold on within the Least Significant Bit (LSB) of the watermarked image; otherwise (1) are hold on. The other is that it will add multiple secret keys victimization shift and rotate operations. The watermark is embedded redundantly over all extracted blocks in image to extend image protection. This embedding is completed within the frequency domain using wavelet transform. This improved algorithm incorporates wavelet transform to supply high security for two reasons, the embedded bit won't be hold on in LSB directly and this approach can use multiple secret keys.

Keywords: Watermark, Wavelet transform, Least significant bit.

طمر علامة مائية رقمية في صوره ملونه باستخدام التحويل الموجي مع تقنية المقارنة

مثيل عمادالدين عبدالمنعم*
قسم علوم الحاسوب ، الجامعة التكنولوجية ، بغداد، العراق

الخلاصة

تم صياغة طريقة خاصة لاضافة علامة مائية للصور (الحمراء،الخضراء، الزرقاء)RGB واضافة التحويل الموجي كاداة خلال عرض البحث. العلامة المائية اضيفت بجزئين. الجزء الاول هو باخذ المفتاح الذي يحوي مجموعة متجمعة من الارقام بين (0–7) كل حد فيها يحدد موقع البت الفعلي في الجزء الخاص للصوره. اذا كان هذا البت متقابل مع البت في العلامة المائية سوف يوضع (0) مع الت الاقل اهتماما LSB للصوره المعشقة بالعلامة المائية، خلافا لذلك يوضع (1). كذلك سوف يضاف مفاتيح سرية متعددة من خلال عملية التحريك والتدوير. العلامة المائية سوف تضاف حالا على كل المجاميع في الصورة لتوسعة الحماية للصوره. هذا الطمر يتم اكتماله مع المجال الترددي باستخدام النقل الموجي. هذه الخوارزمية المحسنة دمجت التحويل الموجي لتوفير حماية عالية لسببين. البت المطمورة سوف لن يتم ايجادها مباشرة في ال LSB وهذا الاسلوب ممكن ان يستخدم مفاتيح سرية عديده.

1. Introduction

Because of internet developing, the requirement of assurance of knowledge credibleness is exaggerated (image, video or the other type).

Watermark is one of the used techniques to attain that purpose. Watermark is admittedly the same as steganography as a result of it contains hidden info in it. However it differs in purpose as a result of watermark is employed to relinquish credibleness to causation knowledge however stego area unit accustomed send hidden info [1, 2].

*Email: matheel_74@yahoo.com

Although, it not recognizable by human senses, easily, watermarking will be discovered by computer code detectors, and it might stay unchanged through multiple actions like writing, encryption, compression, and broadcast while not influencing on the standard of the content [3,4].

This technology depends on terribly fact the actual fact that our eyes has very restricted ability to watch minor changes within the color values of a picture and even though they're noticeable they're subconsciously corrected in order that no distinction would be noticed by the observer [5,6].

Steganography techniques hide the existence of a digital message by cryptography it into another media, so creating the planned method terribly arduous. The importance of steganography was recently planned by governments with notice to the safety of net [7, 8].

Beside, digital watermark focuses to safeguard the rights of intellectual possession and also the agreement of the digital media. The same as steganography ways, there are a unit some ways to cover info via the watermark in digital media.

The aim of the hidden info is pertains to the digital medium itself and has info concerning the integrity of the content, its owner and conjointly its vendee. Digital watermarking techniques prepare fast and low cost grouping of digital info over the web further as a completely unique ways of confirmation the appropriate protection of copyright man of affairs within the rational property distribution action [9, 10].

The format of this work is as follows. The sections below describes the connected work, the standard LSB, transformation, the planned algorithm and also the results of this algorithmic program, finally the conclusions was mentioned [11- 13].

2. Related Work

Technology is evolving at a staggering pace; it's having vital influence on our work, social life and overall quality of life. The net and digital signal area unit far more wide accustomed transmit info because of this speedy evolution of technology, and as a result the utilization of digital watermarking is increased for a large field of applications such as: the protection of copyright, origin chase, broadcast management, cowl communication, security, and legitimacy identification is a lot of outstanding than ever in recent history [14]. In (2010), Calagna brand new technique for embedding message in (6-7-8)th bits of constituent rate of a picture is improved [15, 16].

The advantage offered by this system is that the message will be preserved though the interloper changes the LSB of all pixels within the image within which message has been enclosed [17, 18]. In (2012), Wang propose a new algorithm of watermark on the space field for digital images to include and opened the invisible watermark also using the secret key. Depending on the secret key, the watermark determines in a haphazard method vertically or horizontally over the initial image [19, 20]. Transforms aim it vary the illustration of an indication or a perform by use of a computing. It's potential additionally to decompose a fancy downside into easier ones for getting easier solutions.

Transforms play vital role in several signal process applications like filtering, pattern recognition, restoration, spectrum estimation, signal improvement, localization and compression. The performance of every application depends on many factors, and hence, every application might have a distinct remodel technique for a higher answer [21].

3. Transformation Techniques

Transforms aim to change the representation of a signal or a function by use of a mathematical operation. It is possible also to decompose a complex problem into simpler ones for obtaining simpler solutions. Transforms play important role in different signal processing applications like filtering, pattern recognition, restoration, spectrum estimation, signal enhancement, localization and compression. The performance of each application depends on several factors, and hence, each application may need a different transform technique for a better solution [21].

3.1 Wavelet Transform (WT)

One of the foremost vital and powerful tool of signal illustration is that the WT. Now days, it's been utilized in completely different image and signal process applications. It's necessary to use time-frequency atoms with different totally completely different time supports so as to investigate signals of terribly different sizes. The WT decomposes signals over “dilated” and “translated” functions known as wavelets, that transform a continual perform into a high plenteous perform [21].

Transform domain watermarking is analogous to spatial domain watermarking; during this case, the coefficients of transforms like Discrete Cosine Transform (DCT), Discrete Fourier Transform

(DFT), or Discrete Wavelet Transform (DWT) are a unit changed [22]. In general, most of image energy is condensed at the low frequency constant set of the Low Low (LL) bands, and thus as well as watermarks in these sets of constant that will degrade the image gravity. However, embedding the watermark within the LL bands effectively will increase hardiness [10]. One incontrovertible fact that makes our study novel is that we have a tendency to increase the hardiness of the watermarked image beneath sure attacks while not degrading the image, by embedding a binary watermark on the LL band. This conjointly explains why the LL sub band is chosen for watermark embedding [22]. The primary plan of WT is to require associate degree "absolute function" f(x) as a linear unification of a basis functions [23]. The "mother wavelet" area unit gets these basis functions that are known as dilation and also the translation factors, as shown in equations (1).

$$\Psi_{S,L}(T) = \frac{1}{\sqrt{S}} \Psi\left(\frac{T-L}{S}\right) \qquad (1)$$

Where: $\Psi_{S,L}$ (T): represent the "translated" and "scaled" function of the mother function. S: The "scale coefficient", T: The "shift coefficient". $\sqrt{S}$: The "energy normalization" that keeps the energy of small wavelet equal to that of the mother wavelet [23]. The variations between completely different "mother wavelet" functions like "Haar" wavelet are a part of however these scaling signals and also the wavelets area unit determined. The final waveform shape determines the choice of wavelet; also, the decomposed waveforms are always sinusoid for "Fourier transform. We need to select the orthogonal wavelets to perform the transforms to have a solitary reconstructed signal from WT [23].

3.2 Discrete Wavelet Transform (DWT)

The DWT may be a "linear transformation" that operates on a knowledge vector whose length is associate number power of 2, remodeling it into a special vector of a similar length numerically. It's a tool that separates information into totally different frequency parts, so studies every part with resolution matched to its scale. The transform will be implementation on a pair of separate transforms. First, the image is filtering on the coordinate axis and decimated by 2. It's followed by filtering the image on the coordinate axis then decimated by 2 [24]. DWT algorithmic program for 2-dimensional decomposition is analogous. The DWT is performed first on all image rows so for all columns [24]. Figure-1 represents the sort of coefficients resulted.

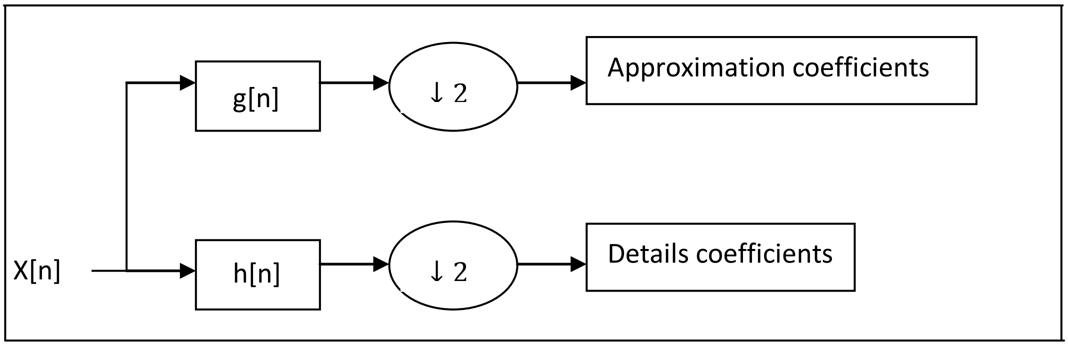

Figure 1- Block diagram of filter analysis [30].

In the discipline of Digital Signal Process (DSP), the filtering of a sequence of variety is achieved by convolving the sequence with another set of numbers known as the "filter coefficients", taps, weights, or impulse response. This makes intuitive sense if you're thinking that of a moving average with coefficients being the weights [24]. Figure-2 describe this idea.

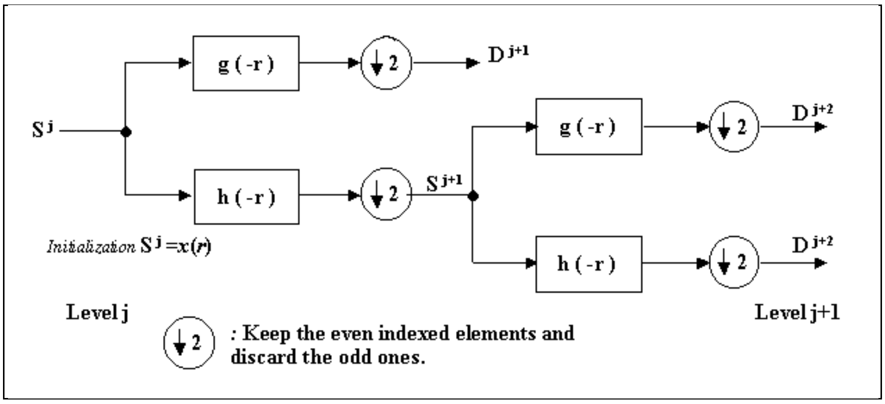
g(-r)
↓2
D^{j+1}
S^j
h(-r)
↓2
S^{j+1}
g(-r)
↓2
D^{j+2}
h(-r)
↓2
D^{j+2}
Initialization $S^j = x(r)$
Level j
Level j+1
↓2 : Keep the even indexed elements and discard the odd ones.

Figure 2- A multiple level of filter bank [30].

Therefore, the Haar wavelet is a set of rescaled functions which form together a wavelet family. Wavelet analysis is similar to “Fourier analysis” therein it separates a final perform over an interval to be employed in terms of an “orthonormal function” basis [23]. Thus, the four pictures terminated from every decomposition level are LL, LH, HL, and HH. Solely the LL image is employed to administer a next level of decomposition, these details are represented in Figure (3) [24].

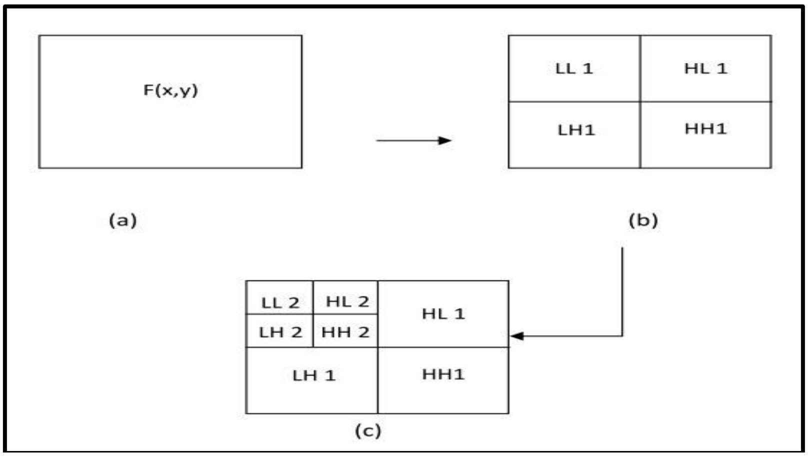

Figure 3-Two-dimensional WT [30].

4. The Proposed System

Embedding a watermark in image using wavelet transform and comparison technique depends on comparison between specific bits in pixels of the extracted blocks in cover image and bits of the watermark. If they're equal (0), it'll be hold on in watermarked image, otherwise (1) it'll be hold on in watermarked image. The positions of those bits square measure determined by key, wherever the key contains eight digit from (0...7). For instance assume the key's (01234567) once one shift and rotate operation, the key become (70123456). Therefore the Embedded Stream (ES) is (011110111010).

To highlight the concept we’ll take constituent three as a sample of pixels P3=R= (10101000), G=(10111000), and B=(10001111). It's noted that the LSB of Red channel in constituent three become (1)as a result of watermark bit metal is totally different from (bit with underline (0)) that is decided by key (6) that find the position of bit in this channel of constituent. While, LSB of Green channel in pixel3 still the same (0), as a result of watermark bit (ES) is capable last bit in Green channel of pixel 3. Thus P3 R=(10101001), K=6, and ES=1, G=(10111000), K=7 and ES=1 finally B=(10001111), K=7 and ES=1. The subsequent steps make a case for the projected rule for embedding the appropriate bit in LSB of every pixel’s channel. The following algorithm represents the schema.

```
Input: - Original image, Watermark.
Output: Watermarked Image.
Begin
Step1: Divide image into many blocks (8x8) constituent for everyone.
Step2: check every block in image to work out the blocks that doesn't loss info.
Step3: choose key that consist from (0 to 7) for instance (10235476).
Step4: Use the extracted block in step (2) to introduce watermark.
Step5: Compare every constituent within the extracted block with one variety key to work out the situation of bit in constituent. If those bits almost like the one in watermark image, (0) are hold on within the LSB in this constituent. Otherwise (1) are hold on instead.
Step6: once complete the key of step (3) another key may be created. This will be done by shift and rotate the primary key by one.
Step7: Repeat steps from (3-6) till complete all extracted blocks.
End
```

Figure-4 and Figure-5 describe the general embedding and extracting models.

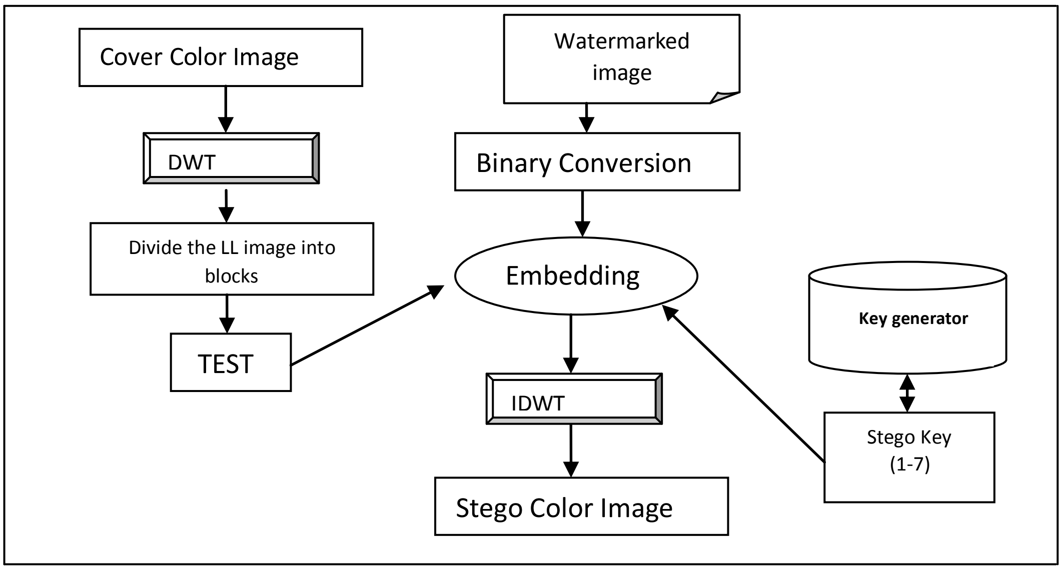

Figure 4- Embedding Module

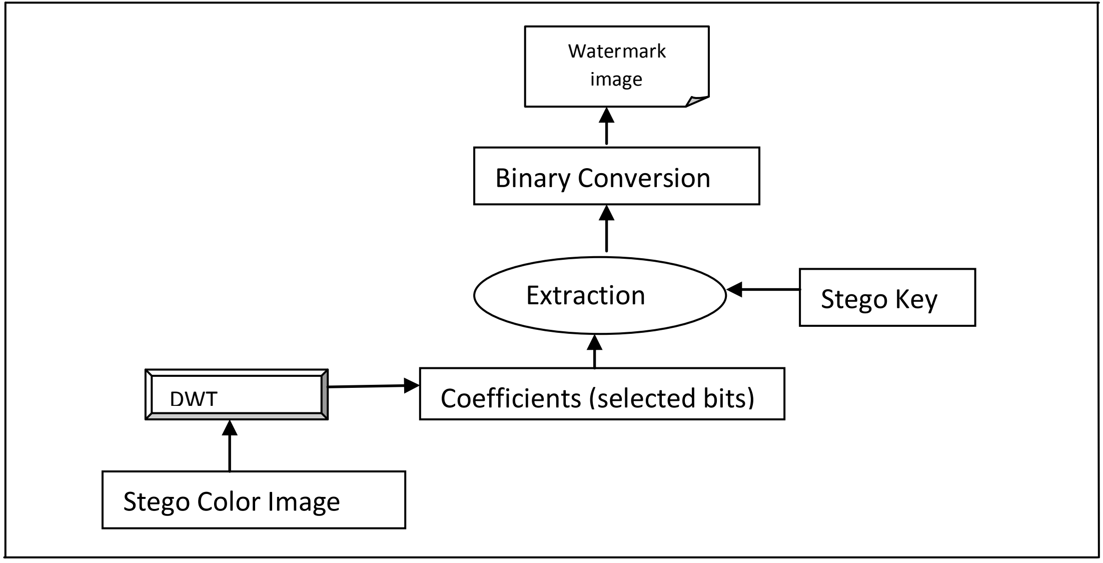

Figure 5- Extraction Module

4. Results and Discussions

In this work 50 color images were used with different types depends on variations of color, smoothness and with different variance. The values resulted from the Peak Signal to Noise Ratio (PSNR) within the image and video compression is around from 30 to 50 dB, wherever invariably the upper is best. The Table-1 shows that the results of watermark during this rule provides a better quality of watermarked image (PSNR is high) and store watermark in non-direct manner that provides high security, it forestall attacker from even sight there's watermark store in it. In the table one can show that the third picture has a high PSNR when one show to other pictures this is because the third picture was smoother than the others and has a suitable contrast over the other ones. During this paper, payload capability depends on the extracted block within the cover image. If the extracted blocks are high, the capability is high. This approach provides an ideal result which supplies high similarity between watermarked image and original one because the MSE that occur for the results was accepted. Multiple secret is used through ever-changing key using shift and rotate operation which supplies high level of security.

The proposed system solve the matter of the normal LSB technique, by preventing attacker from watermark extraction by accumulating LSB in pixels of watermarked image (because of the embedding in LSB is done based on the comparison between embedded bit and bit in pixels of cover image that is determined by key), as well as, prevent the watermark destroying, watermark is continual on all extracted block of watermarked image. Mean square Error (MSE) is low and PSNR is high as a result of using only 1 bit in LSB. Using the WT was a suitable choose to add more robust algorithm that add more secure and more speed depending on frequency domain embedding watermark.

Table 1- The PSNR and MSE values after embed watermark into image.

Image no.	Image size(KB)	Size of embedded Data(Bytes)	MSE	PSNR
Image1	230400	35008	0.0135	66.569
Image2	773	2080	0.0009	77.007
Image3	396	149	0.0003	86.322

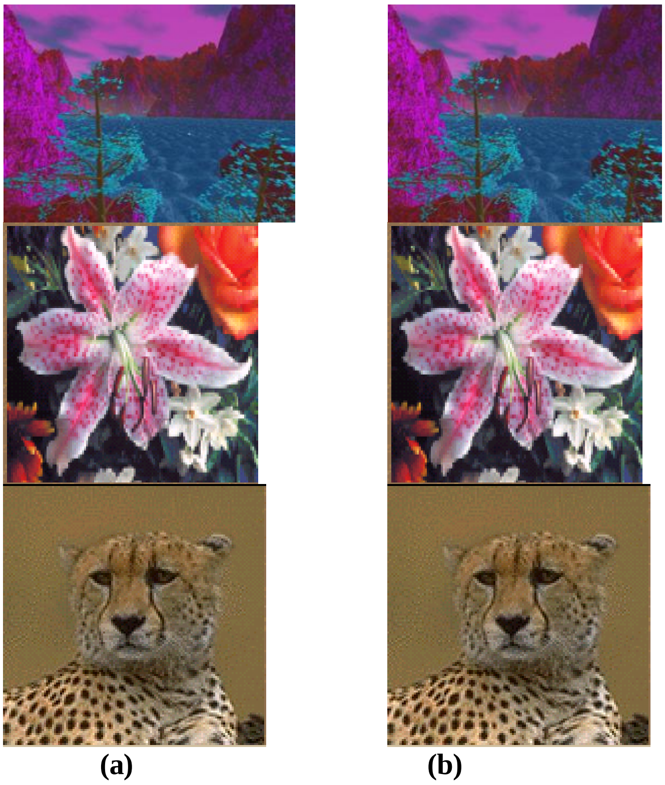

Figure 6- The resulted images after adding a watermarked image that explain there is no visual difference between these images, (a): The original images, (b): The resulted images after adding a watermark.

References

1. Mohanty, S., Ranganathan, N., and Namballa, R. **2003**.VLSI implementation of invisible digital watermarking algorithms towards the development of a secure JPEG encoder. Proceedings of the IEEE Workshop on Signal Processing System; 6, pp:183-188.
2. Cruz-Ramos, C., Reyes-Reyes, R., Nakano-Miyatake, M., and Perez-Meana, H. **2010**. A blind video watermarking scheme robust to frame attacks combined with MPEG2 compression. *Journal of Applied Research and Technology*; 8, pp: 323-369.
3. Akar F, Yalman Y, and Varol H. **2012**. Data hiding in digital images using a partial optimization technique based on classical LSB method. *Turkish Journal of Electrical Engineering & Computer Sciences*; 21, pp: 2037-2047.
4. Zhang Q, Li Y, and Wei X. **2012**.An improved robust and adaptive watermarking algorithm based on DCT. *Journal of Applied Research and Technology*; 10, pp: 405-415.
5. Victor OnomzaWaziri, AuduIsah, and Abraham Ochoche.**2012**. Steganography and Its Applications in Information Dessimilation on the Web Using Images as Security Embeddment: A Wavelet Approach. *International Journal of Computer and Information Technology*, 1(2).
6. Shubhendu S. Shukla, Vijay Jaiswal, Sumeet Gupta and Anurag Singh.**2013**. Steganography Technique of Sending Random Passwords on Receiver's Mobile, *IOSR Journal of Computer ngineering*, 15(3), pp:17-25.
7. Aparna S. Kulkarni, and S. S. Lokhande.**2014**.Digital Watermarking Using DWT and DCT, *International Journal of Scientific & Engineering Research*, 5.
8. Elbasi E, and Eskicioglu A. **2006**.A DWT-based robust semi-blind image watermarking algorithm using two bands. Proceedings of the SPIE 18th Annual Symposium on Electronic Image Security, Steganography, and Watermarking of Multimedia Contents VIII (6072), pp: 1-11.
9. Elbas E. **2010**. Robust multimedia watermarking: hidden Markov model approach for video sequences. *Turkish Journal of Electrical Engineering & Computer Sciences*; 18, pp: 159-170.
10. Singh S, Rawat P, and Agrawal S. **2012**. A robust watermarking approach using DCT-DWT. *International Journal of Emerging Technology and Advanced Engineering*; 2, pp: 300-305.
11. Fridrich J, Du R, and Long M. **2000**.Steganalysis of LSB encoding in color images. IEEE International Conference on Multimedia and Expo; 3, pp:1279-1282.
12. Yavuz E, and Telatar Z. **2007**. *Improved SVD-DWT based digital image watermarking against watermark ambiguity*.Proceedings of the 2007 ACM Symposium on Applied Computing; 5, pp:1051-1055.
13. Chandra D. **2002**.Digital image watermarking using singular value decomposition, Proceedings of the 45th Midwest Symposium on Circuits and Systems; 3, pp: 264-267.
14. Liu R, and Tan T. **2002**.An SVD-based watermarking scheme for protecting rightful ownership. IEEE Transactions on Multimedia; 4, pp: 121-128.
15. Calagna M, Guo H, Mancini L, and Jajodia S. **2006**.A robust watermarking system based on SVD compression. Proceedings of ACM Symposium on Applied Computing; 15, pp: 1341-1347.
16. Bao P, and Ma X. **2005**.Image adaptive watermarking using wavelet domain singular value decomposition. IEEE Transactions on Circuits and Systems for Video Technology; 15, pp: 96-102.
17. Ghazy R, El-Fishawy N, Hadhoud M, Dessouky M, and El-Samie F. **2007**.An efficient block-by-block SVD based image watermarking scheme. *Ubiquitous Computing and Communication Journal*; 2, pp:1-9.
18. Niu S, Niu X, and Yang Y. **2004**.Digital watermarking algorithm based on LU decomposition. *Journal of Electronics & Information Technology*; 26, pp: 1620-1625.
19. Wang S, Zhao W, and Wang Z. **2008**.A gray scale watermarking algorithm based on LU factorization. International Symposiums on Information Processing, 45, pp: 598-602.
20. Elbasi E. **2006**.A survey on digital image & video watermarking. First Portion of Second Examination Report Graduate Center. The City University of New York.
21. Pigazo A, Liserre M, Mastromauro R, Moreno V, and Aquila A. **2009**.Wavelet based islanding detection algorithm for single-phase PV distributed generation systems. *IEEE Transactions on Industrial Electronics*, 56, pp: 4445-4455.
22. Jameelah H. S. **2012**. Discrete Cosine Transform using in Hiding Image Technique, *Al-Mustansiriyah J. Sci.*, 23(7).

23. Kim C., and Aggarwal R. **2000**.Wavelet transforms in power systems, Part 2: Examples of application to actual power system transients, *IEEE Power Eng. J.*, 15, pp: 193-202.

24. Daubechies I. **1992**. *Ten Lectures on Wavelet*. Second Edition, Philadelphia, SIAM.