ISSN: 2393-8528

IJICSE
Open Access

Contents lists available at www.ijicse.in

International Journal of Innovative Computer Science & Engineering

Volume 4 Issue 3; May-June-2017; Page No. 57-64

AN WELL-ORGANIZED VITAL PICTURE WATERMARKING BASED ON AC FORECAST METHOD USING DCT SYSTEM

M. Kavitha

Assistant Professor, Department of M.Sc. Software systems

KG College of Arts & Science, Coimbatore-35.

kavithalakshmi.m@gmail.com

Received 02 April 2017; Accepted 04 May 2017

ABSTRACT

The extension of knowledge has made several simple ways to direct the novel content. This has brought the apprehension for defense of the content which is easily available in open network. Digital watermarking is the most appropriate solution for the distinct problem. Digital watermarking is the art of inserting the symbol into multimedia object to have proof of ownership at any time it is required. The proposed algorithm is useful in authorized sharing and ownership confirmation. The algorithm uses the idea of AC forecast using DCT to embed the watermark in the image. The algorithm has tremendous vigor against all the attacks and outperforms the like work with commendable performance in terms of Normalized Correlation (NC), Peak Signal to Noise Ratio (PSNR) and Tamper Assessment Function (TAF).

Keywords: Blind rescue, Digital Rights organization, Error Correction, Invisibility, vigor

I. INTRODOCTION

A multi-agent system (MAS) is a computerized The usage of internet has increased enormously over the earlier period decade. The multimedia content is transferred frequently in excess of the network. The development of the knowledge has cut down distribution of the digital images, videos or any other legal certificate. But at the same instance, the hazard of unauthorized access and allocation of such multimedia content is raised. The trouble of unlawful entrance can be solved by adding digital autograph with the certificate. By introducing the digital signature, the authorized user can only capable to contact the certificate. Though, the certified user may not have the ownership of the same. Thus, for this reason, a watermark of the authorized dispenser is added to the image. Watermarking may be of any type such as visible/invisible, blind/non-blind, fragile/robust/semi-fragile etc. The watermark may be any text, picture or symbol of the dispenser which acts as the ownership information of the valid or authorized dispenser. The watermark is entrenched such that it should not deform the swarm image and should also be unseen to the viewer. The watermark is extracted from the swarm image in order to recognize the authorized dispenser. If the extracted watermark correlates the novel watermark within some acceptable acceptance limit then the picture is genuine otherwise it is not. The image has to endure some possible attacks once it has been transmitted over the noisy waterway. The numerous ordinary attacks are JPEG density, salt-pepper/gaussian noise and filtering. The watermarking algorithm must be designed to have considerable vigor against all forms of attacks. One application for watermarking algorithm is in armed where message takes place over highly noisy channel i.e. link may be temporary, low bandwidth radio set up etc. Sometimes, it may not be feasible to exact the watermark it its novel form. The error correcting codes are inserted in order to reduce the Bit Error Rate (BER). Another application of digital watermarking scheme is in Digital Rights Management (DRM) systems. It addresses the problem interconnected to content recognition, ownership, storage and sharing rights of digital content [4-6]. DRM systems also handle issues interconnected to Intellectual Property Rights (IPR) organization. The main purpose of this investigate is to plan vigorous picture watermarking algorithm for ownership and sharing rights. The proposed system is based on

Corresponding author: M. Kavitha |

alteration of DCT coefficients and AC forecast of little AC coefficients [7].

The depiction is prepared as follows: Section 2 describes the literature cram of the existing watermarking algorithm. Section 3 explains the steps for the projected algorithm. Section 4 converse the results which are compared with associated earlier algorithms and Section 5 concludes the investigate effort.

Semi-fragile watermarking techniques aim at detecting malicious manipulations on an image, while allowing acceptable manipulations such as lossy compression. Although both of these manipulations are considered to be pixel value changes, semi-fragile watermarks should be sensitive to malicious manipulations but robust to the degradation introduced by lossy compression and other defined acceptable manipulations. In this paper, after studying the characteristics of both natural images and malicious manipulations, we propose two new semi-fragile authentication techniques robust against lossy compression, using random bias and nonuniform quantization, to improve the performance of the methods proposed by Lin and Chang.

2. Literature Review

The prose obtainable contains a variety of watermarking algorithms which are vigorous to a variety of blare attacks and JPEG density. The vigor of the algorithm is determined of how exactly it is capable to recover the watermark when the watermarked picture is attacked by blare or JPEG density. Factors like Normalized correlation (NC) and Tamper Assessment Function (TAF), discussed in Section 4, are used to create the vigor algorithm. The occurrence area watermarking algorithms are based on orthogonal transforms similar to Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) or Singular Value Transform (SVD). Chinmayee et al. [8] utilized the connection between the two DCT coefficients of the adjacent 8x8 blocks at the similar location. The DCT coefficient is customized to bring the variation from the contiguous chunk coefficient in the specified array. Patra et al. [9] projected a Chinese Remainder Theorem (CRT) based digital watermarking method in DCT area which has the vigor to various attacks. This method is useful for official document defense and verification of multimedia information. The projected technique works improved than the SVD based watermarking method in expressions of TAF and Peak Signal to Noise Ratio (PSNR). The above algorithms engage modifying the DC or low occurrence coefficients of the novel picture. Such procedure modifies the force substance of the picture and this could effect in the alter in the perceptibility to the client. To survive with such a crisis, a novel algorithm was projected by Liu **al. [10]**

To implant the watermark in the high rate at coefficient after applying the Quadratic DCT transforms. It leads to a little change in the energy content of the image which suggests less degradation in the perceptibility to the viewer. Local typical instant is used by Wu and Ren which is used to adapt the selected AC coefficients to embed the watermark. A pseudo slack sum of time and a top secret key is used to choose the AC coefficient whose rate is to be modified. SVD is applied to bind the image blocks and then DCT is applied on universal blocks comprised of the first singular values (SV) of each image chunk. The watermark bits are embedded into the high rate crew of SVD-DCT block by impressive a fussy relationship between a few pseudo-randomly chosen pairs of the DCT coefficients. Joshi et al. [13] here the presented dual area watermarking system for image copy true application. The projected method is used to add the watermark in both spatial domain and frequency domain. It has advantages of low complexity as well as acceptable robustness against some standard attacks. The author further developed for video watermarking algorithm which is suited to H.264 video standard [14]. It uses the idea of Integer Discrete Cosine Transform (Int-DCT) to have better speed with little complexity. The algorithm is implemented on VIRTEX-4 FPGA to verify the real time performance.

3. Proposed watermarking algorithm

The proposed scheme involves embedding the watermark payload into the DC coefficients of each block and modification of AC(1, 1) coefficient using AC prediction technique.

3.1 watermark embedding

The following steps explain the functioning of algorithm for embedding the watermark bits in the original image.

- Watermark placed into information content of novel Image to create Watermarked Image
- Image Content Spatial Domain (Least Significant Bit)
- FFT - Enormity and Stage
- Wavelet Transforms
- DCT Coefficients
- Setup-Watermark Embedding

Criteria for a good watermark:

Although watermarks fit in to special categories, some of the general characteristics that watermarks should possess are the following [6]:

1. The watermark should be strongly bound to the image and any changes to the watermark should be evident in the image.
2. Watermark should also be capable to withstand changes made to the image. Such changes contain modifications and enhancements of images such as size modifications, cropping, and lossy compression, to surname a little.
3. The watermark must not dent the visual demand of the image by its presence (especially for invisible watermarks).
4. Watermark must be permanent and must be able to endure linear or non-linear operations on the image [2].

The following are criteria for a observable watermark: [7]

1. The watermark must be evident on all kinds of images.
2. The size of the watermark is vital. The more insidious the watermark the improved so that the watermarked area cannot be modified without tampering with the image itself.
3. The watermark must be fairly easy to embed in the image.

The Watermarking Process:

The watermarking procedure comprises of the following stages [9]:

1. Embedding stage
2. Extraction phase
3. Distribution stage
4. Decision stage

Embedding stage:

The image to be watermarked is preprocessed to key it for embedding. This involves converting the image to the desired change. This includes the discrete cosine transform (DCT), the discrete Fourier transform (DFT) and the wavelet domains. The watermark to be embedded might be a binary image, a bitstream or a pseudo-random amount that adheres to, say, a Gaussian distribution. The watermark is after that appended to the desired coefficients (low frequency or intermediate frequency) of the transform, as recommended by Human Visual System (HVS) research. The watermarked image is the output of this procedure and is obtained by performing an inverse transform on the altered transform coefficients [9].

Distribution stage: The watermarked image obtained over is then distributed through digital channels (on an Internet site). In this procedure, this may have undergone one of several mappings, such as compression, image manipulations that downsize the image, enhancements such as rotation, to name a little. Any of the above may put the watermarking system to test, as well observe in the ensuing part. In addition, hateful attacks also are possible in this stage to battle with the watermark.

Extraction stage: In this stage, an effort is made to recover the watermark or signature from the distributed watermarked image. This stage may need a private key or a shared public key, in permutation with the original image, or just the watermarked image [9].

Decision stage: In this stage, the extracted watermark is compared with the original watermark to check for any discrepancies that might have place in at some point of distribution. A common way of doing this is by computing the Hamming distance [9].

$$HD = \frac{(W^{mod} . W)}{||W^{mod}||.||W||}$$

Where both the numerator and denominator are dot products.

HD obtained above is compared to a threshold, T, to determine how close W^{mod} is to W.

1. Split the original image I(i, j) into 8 $_X$ 8 pixels blocks I_Bq(x, y), where, I_Bq(x, y) represents the qth block and q is in the range $1 \leq q \leq$ k. The size of original image is M $_X$ N pixels. The number of pixel blocks is given by Eq.(1).

No of 8 $_X$ 8 blocks (k) = M * N/ 8*8 (1).

2. Compute the DCT transform of each block. The transformed 8 $_X$ 8 block of image is given by I_BTq(u, v).

I_BTq(u, v) = DCT (I_BTq(x, y)) (2).

Where, $1 \leq q \leq$ k., $1 \leq$ x, y$\leq$ 8 and I_BTq(u, v) represents the DCT transform of qth block I_BTq(x, y).

3. The binary watermark image is changed into an array of single row. The m X n watermark image consists of m * n bits. Repeat every watermark bit four times at each pose. Suppose the watermark

bits W(n) are 11001101. The first bit of the sequence is'1'. Now, repeat this bit four times '1111'. The second bit is '0'. Reproduce this bit again four times '0000'. In this way, the resulting watermark sequence W_R(q) becomes '1111111100000000111111110000111'. Thus a single watermark image is embedded four times in the original image. In case, if one of the blocks is attacked after that it is probable to recover the embedded bit from the other blocks. This increases the robustness of the algorithm, where, W_R represents the repetitive watermark series.

4. Embed the repetitive series of watermark bits into the DC coefficients according to the following rule.

If W_R(q) = 1,

$$I\_BT'_q(u,v) = \{\alpha * F_0\{ (I_{BTq}(u,v)/ \alpha) \text{ if } u,v=0$$
$$I\_BTq(u,v) \quad \text{if } u,v \neq 0 \quad (3)$$

Else,

$$I\_BT'_q(u,v)= \{\alpha * F_1\{ (I_{BTq}(u,v)/ \alpha) \text{ if } u,v=0$$
$$I\_BTq(u,v) \quad \text{if } u,v \neq 0 \quad (4)$$

Where, F0(x) indicates converting the value of x to most approximate odd number and F1(x) indicates converting the value of x to most approximate even number. α is the parameter of quantization. This parameter plays a vital role in increasing the robustness of the algorithm. The value of α is selected in the range 15 < α < 35.

5. Predict the AC(1, 1) coefficient using AC prediction technique used employed in [7].

$$AC(1,1)= \lambda*(DC1+DC9-DC3-DC7) \quad (5)$$

The value of λ is modified in our proposed algorithm. The value of λ is chosen to be 0.35.

6. Apply the inverse DCT to each modified block I_BTq(u, v) to obtain the watermarked image I_W(i, j), where, I_BTq(u, v) represents the qth block after AC(1, 1) modification.

The above mentioned procedure is shown in Fig.1.

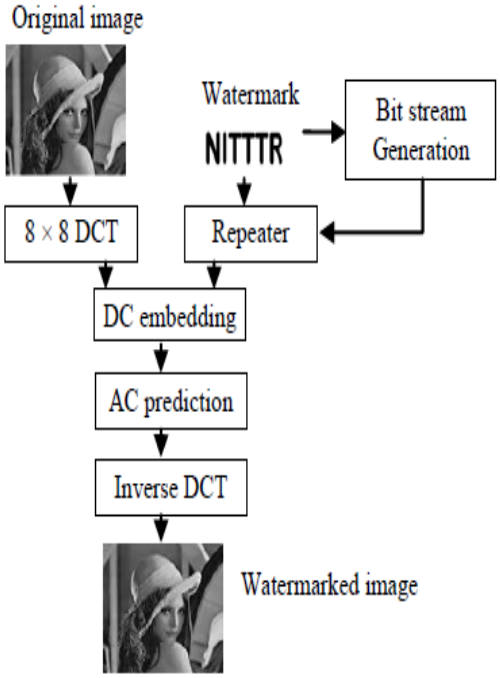


Fig.1: procedure for water marking embeding

3.2 watermark salvage

The following steps describe the procedure for retrieving the watermark from the watermarked image:

1. The watermarked image I_W(i, j) is divided into k non- overlapping blocks of size 8 x 8. Each block is denoted by I_WBq(x, y) .

2. Perform DCT transform of each 8 □ 8 block. Each DCT transformed block is denoted by I_WBq(u, v)

$$I\_WBT_q(u,v) = DCT(I\_WB_q(x,y)) \quad (6)$$

3. Retrieve the continual watermark bits sequence from the DC coefficients of every block as given by equivalent weight.(7) and Eq.(8).
where, F(x) could be a spherical operate. during this approach, calculate the whole bit sequence W_R'.

4. Calculate the AC(1,1) in each block consistent with equivalent weight.(5). it's denoted by AC'(1, 1). Now, compare I_WBTq(1, 1) with AC'(1, 1). If the distinction of those 2 values happens to be larger than a pre-determined threshold η, then the block is attacked otherwise not. the worth of threshold η is given by equivalent weight.(9).

5. To extract the first watermark bits sequence W' from the continual sequence W_R', choose one bit from W_R' and replica to W' and drop next 3 bits. during this approach, do a similar procedure for the complete bits sequence out there in W_R'.

6. Convert the extracted original watermark series

W' into watermark image. The Fig.2 shows the procedure of retrieving the watermark.

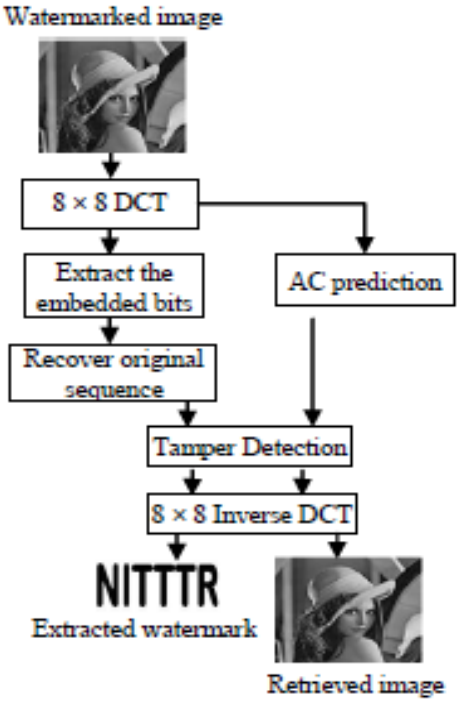


Fig.2: procedure for extracting the watermark

3.3 Watermark Properties

Watermark should appear random, noise-like sequence
Appear Undetectable
Good Correlation Properties

- High correlation with signals similar to watermark
- Low correlation with other watermarks or random noise

Common sequences

- Normal distribution
- m-sequences

3.3 Watermarking Techniques

Watermarking techniques will generally be classified supported their inherent characteristics: visible and invisible.]

Visible watermarks: a clear alteration of the digital image by appending a "stamp" on the image is termed a clear watermark. this method directly maps thereto of the pre-digital era wherever a watermark was imprinted on the document of option to impose legitimacy.

Invisible watermarks: against this, AN invisible watermark, because the name suggests that this can be invisible for the foremost half and is employed with a unique motive. Whereas the patency of visible watermarking makes characteristic legitimate and illegitimate versions straightforward, its conspicuousness makes it less appropriate for all applications. Invisible watermarking revolves around such appropriate factors that embody recognizing authentic recipients, characteristic verity supply and non-repudiation.

Another way of classifying watermarking technique could be a issue of its usage : sturdy, fragile, or semi-fragile, and spacial or spectral watermarks.

Robust watermarks: Watermarks is accustomed hold data of possession. Such watermarks ought to stay steadfast to the initial image to try and do what they advertise. The perfection of the watermark could be a live of its hardiness. These watermarks should be ready to stand up to traditional manipulations to the image like reduction of image size, lossy compression of image, dynamical the distinction of the pictures, etc.

Fragile watermarks: this area unit complementary to sturdy watermarks and area unit, as a rule, additional change-sensitive than sturdy watermarks. They lose their heart once they area unit subject even to the tiniest changes. Their use lies in having the ability to pin-point the precise region that has been modified within the original watermarked image. The strategies of fragile watermarking vary from checksums and pseudo-random sequences within the LSB venue to hash functions to smell any changes to the watermark.
Semi-fragile watermarks: These watermarks area unit a middle ground between fragile watermarks and fragile watermarks. They engulf the simplest of each worlds and area unit additional resilient than fragile ones in terms of their hardiness. They are higher than sturdy watermarks in terms of locating the regions that are changed by AN inadvertent recipient.

Spatial watermarks: Watermarks that area unit applied to the "spatial domain of the image" area unit aforementioned to be spacial watermarks [5].
Spectral watermarks: These area unit watermarks that area unit applied to the "transform coefficients of the image". [2]

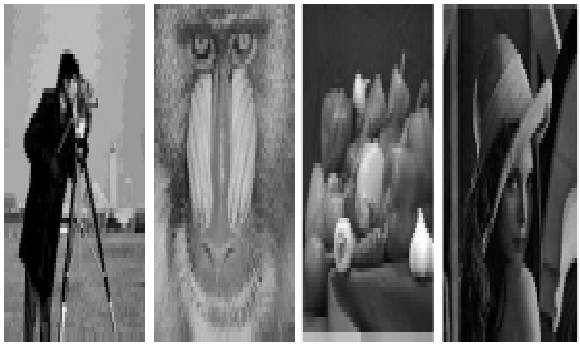
The rest of the paper is organized as follow. the bottom rules for an honest watermark are arranged down within the next section. when describing the varied stages of the watermarking method, i will be able to additionally think again 3 algorithms for watermarking, and at last analyze the algorithms.

4. Results and discussions

The original image is taken to be 512 x 512 in size and also the watermark could be a binary image of size thirty two x thirty two. For testing this formula, pictures of Lena, Baboon, camera operator and pepper are used. Fig.3 shows the watermark pictures and Fig.4 shows the host pictures.

(a) (b)

Fig.3: (a) & (b) watermark payload



(a)Camera man (b) Bapoon (c) Peppers (d) Lena

Fig.4. Host images

The PSNR, MSE and SF values are calculated and are shown in Table.1 so as to verify the projected watermarking formula. The worth of PSNR is coming back to be over 40dB in each case which suggests the validity of the projected formula. the worth of SF is coming back nearly one in each case that shows that watermark is with success retrieved in every case while not distortion.

The value of the parameter of division α is taken within the vary twenty < α < thirty. This parameter affects the PSNR values. This parameter conjointly plays a significant role in increasing the strength of the formula. Increasing the worth of α decrease the PSNR however will increase the SF once the image is attacked or JPEG compressed. Optimizing this price in step with our want is a crucial task. the worth of λ utilized in AC prediction is another issue poignant the PSNR values of the formula. When examining the impact of various values of λ on the PSNR values, it's ascertained that for λ = zero.35, most PSNR is calculated. The worth of threshold η varies with the necessity of each application. If each minor attack is to be detected, then the worth of η is taken within the vary five < η< ten and if major attacked space is to be highlighted, then eleven < η < thirty.

The live of distortion occurred to host image done because of watermarking method is given by MSE and Peak Signal to Noise magnitude relation (PSNR). MSE is outlined by equivalent. (10) And PSNR is outlined by equivalent. (11) For associate 8-bit grey scale image.

$$MSE = \frac{1}{M*N}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}\left(f'(x,y)-f(x,y)\right)^2 \qquad (10)$$

$$PSNR\,(dB) = 20\log_{10}\frac{255}{MSE} \qquad (11)$$

Where, M x N is that the size of the host image. F(x, y) is that the original host image and f′(x, y) is that the watermarked image. Another parameter that shows however with success watermark is retrieved from the watermarked image is Normalized Correlation (NC). This parameter is given by Eq. (12).

$$NC = \frac{\sum_{i=0}^{N-1} w*w'}{\sum_{i=0}^{N-1} w^2} \qquad (12)$$

Where, w is that the original watermark and w′ is that the retrieved watermark. N is that the size of the watermark. For 2 identical pictures, the worth of SF and Tar Heel State is sort of one. However, the worth of SF will be tolerated up to zero.80. Another parameter accustomed take a look at the lustiness of the rule is Tamper Assessment perform (TAF) that is given by

$$TAF(\%) = \frac{1}{M*N}\left[\sum_{i=0}^{N-1} w \oplus w'\right]*100 \qquad (13)$$

Where, Φ is XOR operation between w(i) and w′(i) bits. for 2 identical pictures, the worth of TAF ought to be zero. The smaller the values of TAF, the additional similar area unit the photographs. For testing the hardiness of the planned formula, following attacks area unit considered: JPEG compression, Median Filtering (3 x 3), Gaussian noise (mean = zero, variance = zero.001) and salt and pepper noise (density = zero.01). Table.2 and Table.3 offer the comparative analysis of the experimental values of TAF and SF with the prevailing algorithms.

The experimental results of the planned formula show an impressive hardiness against JPEG compression as compared to [8]-[12]. The planned formula conjointly shows improved hardiness against median filtering and Gaussian

noise attacks. But, there's slight degradation in hardiness against salt & pepper noise attack. However, the Old North State and TAF area unit in acceptable vary.

5. Conclusion

Proposed formula relies on the conception of repetition the sequence of watermark bits to boost the lustiness. it's additionally accustomed discover the change of state with AC prediction technique. The performance of the formula is simulated on MATLAB platform. The obtained values of Table.1, Table.2 and Table.3 make sure the flexibility of formula against numerous channel attacks. The formula is additionally compared with previous work and shows the commendable accomplishment in performance.

Table 1: PSNR, MSE and SF for 512 x 512 original and watermarked images.

Watermark image	512x512 host image	MISE	PSNR (db)	Normalized Correlation
NITTTR	Lena	5.0758	41.0758	1
MNIT	Lena	5.0963	41.0587	1
NITTTR	Cameraman	6.0643	40.3030	1
MNIT	Cameraman	5.9732	40.3688	1
NITTTR	Bapoon	6.5348	40.0046	0.9927
MNIT	Bapoon	6.5467	40.0097	0.9992
NITTTR	Peppers	4.2035	41.8946	1
MNIT	Peppers	4.1611	41.9387	1

Table.2: Comparative Analysis of NC under different Attacks for different algorithms

Algorithm	JPEG compression (50%)	Median Filterting (3x3)	Gaussion noise (mean=0, variance= 0.001)	Salt and Pepper noise (density=0.01)
Propsed algorithm	0.9949	0.9834	0.8978	0.7752
Chinmayee et al.[8]	0.8847	0.9118	0.8816	0.8112

Table.3: Comparative Analysis of TAF under different attacks for different algorithms

Algorithm	JPEG compression	Median Filterting (3x3)	Gaussion noise (mean=0, variance= 0.001)	Salt and Pepper noise (density=0.01)
Propsed algorithm	0.3926	1.4648	9.7656	22.8561
Chinmaye e et al.[8]	17.21	8.8710	11.391	18.19
J. C Patra et al.[8]	10	Not available	16.53	Not available

References

1. *Rita Choudhary; Girish Parmar, "*A robust image watermarking technique using 2-level discrete wavelet transform (DWT)", 2016 2nd International Conference on Communication Control and Intelligent Systems (CCIS) Year: 2016, Pages: 120 – 124.
2. *Zhi Zhang; Chengyou Wang; Xiao Zhou,,"*Image watermarking scheme based on Arnold transform and DWT-DCT-SVD" 2016 IEEE 13th International Conference on Signal Processing (ICSP), Year: 2016, Pages: 805 – 810.
3. Milad Barazandeh; Maryam Amirmazlaghani, "A new statistical detector for additive image watermarking based on dual-tree complex wavelet transform" 2016 2nd International Conference of Signal Processing and Intelligent Systems (ICSPIS), Year: 2016, Pages: 1 – 5.
4. R. Naskar and R. S. Chakraborty, "Performance of reversible digital image watermarking under error-prone data communication: a simulation-based study", IET Image Processing, Vol. 6, No. 6, pp. 728-737, 2012.

5. Md. Moniruzzaman; Md. Foisal Hossain, Watermarking approach of embedding patient facial information into RONI of Brain CT scan image, 2015 18th International Conference on Computer and Information Technology (ICCIT), Year: 2015, Pages: 248 – 253.
6. Hicham Tribak; Youssef Zaz, "Remote identification of solar panels using QR code recognition and image watermarking" 2015 3rd International Renewable and Sustainable Energy Conference (IRSEC), Year: 2015, Pages: 1 – 6.
7. Purnima K. Sharma; Paresh Chandra Sau; Dinesh Sharma, "Digital image watermarking: An approach by different transforms using level indicator", 2015 Communication, Control and Intelligent Systems (CCIS) Year: 2015, Pages: 259 – 263.
8. Chinmayee Das, Swetalina Panigrahi, Vijay K. Sharma and Kamalakanta Mahapatra, "A novel blind robust image watermarking in DCT domain using inter-block coefficient correlation", International Journal of Electronics and Communications, Vol. 68, No. 3, pp. 244-253, 2014.
9. Wei Liu, Shuiyuan Yu and Xuan Wang, "A Robust Digital Image Watermarking Algorithm Based On Quadratic DCT Transform", Proceedings of 3rd International Conference on System Science, Engineering Design and Manufacturing Informatization, Vol. 1, pp. 133-137, 2012.
10. M. Joshi, R. M. Patrikar and V. Mishra, "Design of low complexity video watermarking algorithm based on Integer DCT", International Conference on Signal Processing and Communications, pp. 1-5, 2012.
11. Amit Joshi, Vivekanand Mishra and R. M. Patrikar, "Real Time Implementation of Digital Watermarking Algorithm for Image and Video Application", Watermarking, Vol. 2, pp. 65-91, 2012.

Web references

1. http://www.ece.purdue.edu/~ace/water2/digwmk.html
2. http://www.acm.org/~hlb/publications/dig_wtr/dig_watr.html
3. http://www.cs.unt.edu/~smohanty/research/confpapers/2002/mohantyicme2000.pdf