Integrated Normalized Content System for Efficient Watermarking

G. Rosline Nesakumari
Associate Professor
Godavari Institute of Engineering & Technology
Rajahmundry,A.P,India

S. Rajendran
Head of the Department IT
SRM University
Kattankulathur,Chennai

V. Vijayakumar, PhD.
Dean Computer Sciences,
Godavari Institute of Engineering & Technology
Rajahmundry,A.P,India

ABSTRACT
In contemporary years, different watermarking schemes are proposed for image authentication and copyright protection. In images, any tiny change to the content is not acceptable; the embedding distortion has to be compensated for perfectly. In this paper a powerful Image watermarking method using DWT based on integrated normalized content based chaotic (DWT- INCC) system is proposed, to obtain better digital content authentication, originality, higher embedding capacity, quality of the information and better robustness. The objective of the proposed integrated scheme is to examine how content image normalization and discrete wavelet domain based chaotic system procedure are used to enhance robustness of a digital image watermark especially for statistical attacks. The proposed integrated scheme consists of four stages. In the stage two image normalization is performed, to achieve the scaling and rotational invariance. In stage two DWT is applied on the normalized image. In stage three a block based content authentication scheme is adopted on the normalized image of stage one for image authentication and tamper localization. In stage four chaotic models is adopted on the stage three to achieve excellent robustness against any statistical attacks and to increase the security of the digital watermarking system. The experimental result shows that the proposed DWT-INCC method is more robust and effective even in the presence of various attacks when compared with many existing methods.

Keywords: Discrete Wavelet Transformation, Normalization, Content authentication and Chaotic System.

1. INTRODUCTION
The rapid magnification of information technology has improved the ease of admittance to digital data. It also leads to the complexity of proscribed copying, copy protection, tampering and transmission of digital data. Digital watermarking emerged as a instrument for protecting the multimedia data from copyright infringement. Image watermarking is a progression of embedding hidden information called watermark into original host image signals [1, 2, 3, 4, 5]. That's why many researchers started working to build efficient watermarking systems using various methods [11, 12, 13]. Ideal properties of digital watermarks are stated in the literature [6, 7, 8, 9]. These properties include perceptual invisibility to stop difficulty of the original image, statistical invisibility, fairly simple extraction, and robustness to filtering, additive noise, compression and other forms of image manipulation as well as the ability to establish the owner of the original image.
Transform domain watermarking methods employ well-known transformation techniques such as Discrete Cosine Transform (DCT), Fourier Transform (FT), or Discrete Wavelet Transform (DWT). Spatial domain methods are simpler and have bulky capacity compared to transform domain methods, while transform domain methods are more robust and vigorous compared to spatial domain methods. The frequently used watermarking techniques in the spatial domain are based on the concept of mixing systems [14, 15, 16]. Such approaches are uncomplicated and computationally proficient, because they modify the color, brightness or intensity values of a digital image pixel. Therefore the application is done very easily and requires minimal computational power. In terms of watermark security, the spatial domain is in most horrible place to insert a watermark. Usually, the frequency domain offers good capacity, high excellence and better robustness to attacks. The key factors for the protected communication are high security, high embedding capacity and good imperceptibility to the exposed eye.
The rest of this paper is organized as follows. Section 2 and 3, introduces the concept of DWT and block based content authentication schemes. Section 4 describes the proposed DWT-INCC watermark embedding and extraction scheme. In Section 5, the experimental results and comparisons with the existing methods are discussed. The conclusions are stated in Section 6.

2. DISCRETE WAVELET TRANSFORMATION
Among the transform domain watermarking techniques, Discrete Wavelet Transform (DWT) based on watermarking techniques are gaining more attractiveness. Wavelet based watermarking techniques have multi-resolution hierarchical characteristics. In addition, its capability to decompose an image into bands that differ in both spatial frequency and orientation (vertical, horizontal and diagonal) has made it of huge significance when modeling the anisotropic properties of a Human Visual System (HVS). This mimics the human visual perception and allows the self-governing processing of the resulting mechanism [10]. The high frequency subbands of the wavelet transform include the edges and textures of the image and the human eye is not generally very sensitive identity them to changes in such bands. Also, watermark detection may be achieved at lower image resolutions, which saves computational load. DWT has number of advantages over other transforms such as progressive and low bit-rate transmission, quality scalability and region-of-interest (ROI) coding demand more efficient and versatile image coding that can be exploited for both, image compression and watermarking applications. DWT is very suitable to identify the areas in the host image where a watermark is embedded successfully. Wavelets are also being used in more than a few

emerging image and video compression standards such as JPEG2000 and MPEG 4. That is the reason the present integrated approach considers the wavelet transform domain for watermarking applications.

3. BLOCK BASED CONTENT AUTHENTICATION SCHEME

Walton's [17] Authentication scheme is one of the first techniques used for image tampering detection based on inserting check-sums into the least significant bits (LSB) of the image data. The scheme computes an array of checksum as the authentication information out of the seven most significant bits (MSBs) of each pixel of the original image. The check-sum value is obtained by summing the numbers determined by the 7 most significant bits (MSB) of selected pixels. Then the check-sum bits are embedded in the LSB. The checking process is similar to the embedding process. It consists in comparing, for each block, the check-sum determined by the MSB of the tested image with the original check-sum value recovered from the LSB. The main advantage of this method is that it does not produce visible changes in the image and provides a very high probability of tamper detection. After a careful study we found the following disadvantages of Walton's method. However, there are several problems found in Walton's scheme:

i) An attack can swap the pixels in a seal path that will not affect the checksum of the image.

ii) The scheme cannot indicate the tampered location of the tampered image.

iii) The scheme cannot distinguish between an innocent adjustment and a malice replacement.

Chang et al. [27] proposed an authentication method based on fragile watermarking. At first the image is divided into 3×3 overlapping blocks. The center pixel of each block is embedded with the cryptographic hash of the features of the corresponding block. The feature of a block consists of the eight neighboring pixels, the index of the block, the height and width of the image and the user's secret key. A cryptographic hash of the feature of the block is calculated using MD5. Let X be the center pixel in which the data is embedded. The 8-neighbors of the center pixel are P1, P2… P8 as shown in Figure 1.

P_3	P_2	P_1
P_4	X	P_8
P_5	P_6	P_7

Fig 1: Embedded pixel X and its eight neighbors

The cryptographic hash of the block is given by,

$$(B_i) = \left(P_1||P_2||\ldots.||P_8||i||ID||K_u\right) \qquad (1)$$

Where ‖·‖ denotes concatenation, B_i is the i^{th} block of the image, 'i' is the block number, ID is the image identity and K_u is the user secret key. The hash of each block is obtained, and is embedded into r least significant bits (LSBs) of the pixel X, where $2 \leq r \leq 4$. The value of r is determined by the block variance (σ),

$$\sigma = \sum_{i=1}^{8}(P_i - P_{i+1\ mod\ 8})^{2} \qquad (2)$$

$$r = \begin{cases} 2, & 0 \leq \sigma < 8 \\ 3, & 8 \leq \sigma < 16 \\ 4, & 16 \leq \sigma < 255 \end{cases} \qquad (3)$$

The present paper found that this scheme is also not suitable for the purpose of image authentication because it suffers with the following disadvantages.

i) The content authentication of 9 pixels is placed in the form of one bit in the center pixel of a 3×3 block. This results a very poor content authentication.

ii) This method is using block variance which is a complex operation when compared to block average.

iii)It is complex in nature due to the use of MD5 for finding checksum.

iv)The block features calculated do not depend on the watermarked pixel.

v) The computation of the block variance (σ) does not depend on the watermarked pixel; hence it is the same for both the tampered watermarked pixel and the non-tampered watermarked pixel.

To address the above the proposed system introduced a new model of block based content authentication system.

4. PROPOSED DWT-INCC SYSTEM

In this section, detail mechanism of DWT-INCC scheme is explained. The two main phases of watermarking system are embedding of the watermark and its extraction or detection of watermark process. In the proposed DWT-INCC approach image normalization is employed to acquire the scaling invariance for the circular region. It transforms the image into its standard form by translating the origin of the image to its centroid. With the scaling normalization, the aligned circular regions are transformed to its compact size. The selected circular regions are scaling invariant. Then a simple and powerful block based content authentication scheme is employed to achieve both content authentication and digital watermark insertion. The block diagram of the proposed scheme is represented in the Figure 2 and the detailed process is explained below.

4.1 Watermark embedding process

STAGE ONE - Image Normalization with Wavelet transform

Image normalization is generally used in pattern recognition and image registration [18]. It also helps researchers to achieve scaling invariance in watermarking domain [19]. Geometric moments are used for normalizing the image geometrically before watermark embedding at the encoder and before extracting the watermark at the decoder. Image normalization, orientation assignment, rotation, scaling, and translation invariant regions are used for watermark embedding and extraction, to avoid the quality degradation caused by interpolation in image normalization. The image normalization is just used for calculating the transform parameters. So that the watermark embedding and detection is performed in the original coordinate system.

Transforming the images into its standard form requires defining the normalization parameters that are computed from the geometric moment of the image. Moment normalization is much a useful technique as the moments of an image is used to describe its contents with respect to the axes. Moments are used to characterize the images and to express the properties that have analogy in statistics.

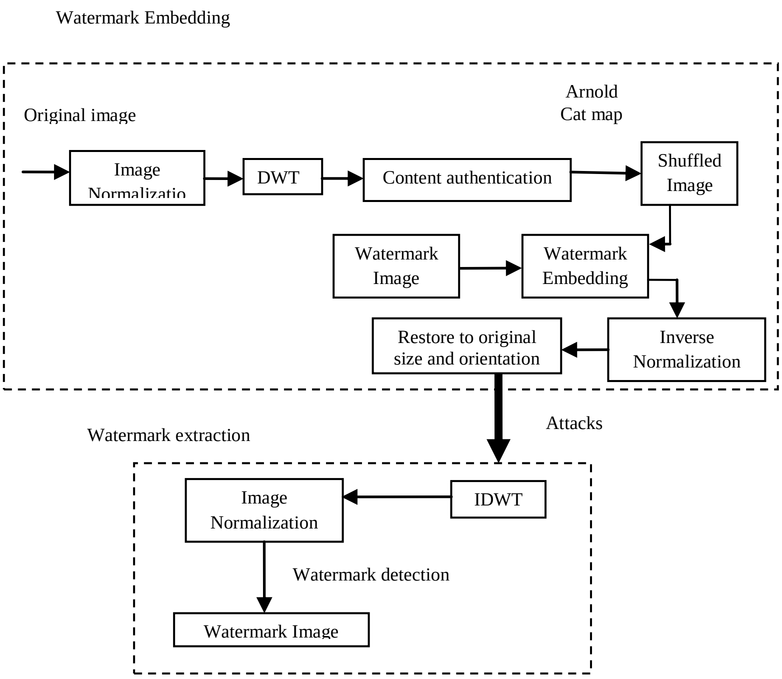


Fig 2: Block diagram of proposed DWT-INCC approach

Moment normalization is done mainly to resist geometrical attacks [20, 21]. The normalization process of the proposed integrated method consists of two steps. In step one scaling normalization and step two rotation normalization are performed.

STAGE TWO: DWT on the Normalized Image

In the stage two DWT is applied on the normalized image of the stage one. In the proposed DWT-INCC approach, DWT identifies the areas in the content normalized image where a watermark is embedded effectively to achieve further authentication and security. Based on the above analysis, rotation and scaling invariant regions are located in the image for watermark embedding.

STAGE THREE: Content authentication

To overcome the drawbacks of Chang et al. [27] scheme and Walton's scheme [17], described in the section 3, the present paper proposed a block based content authentication scheme which embeds the checksum computed on the block B_i into the 2×2 sub block that has the maximum average compared to other sub blocks of the block. By this any change in the watermarked block results in a wrong checksum. The present paper is not considered the variance of the block for finding the r value. This is because the variance changes if the pixels in the block change. The proposed Block based content authentication method is shown in Figure 3. The shaded region is the watermarked pixels. our bits of watermark is embedded into four pixels.

The checksum computation of the proposed DWT-INCC method is based on Walton's method [17]. The DWT-INCC modifies the Walton's scheme by dividing the original image into 4×4 blocks. Then a hierarchical relation is established in the DWT-INCC by dividing into 2×2 blocks, which is not there in Walton's method. The watermark embedding process of the proposed DWT-INCC scheme consists of five steps, which are given below.

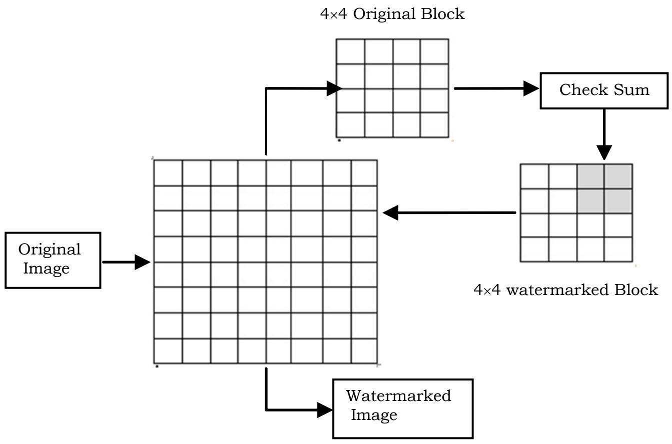


Fig 3: Block Diagram of proposed content authentication scheme

Step 1: DWT subbands of the normalized images I of M×N pixels is divided into M/4 × N/4 non- overlapping blocks of size 4×4 pixels.
Step2: Each 4×4 block is watermarked with 4 bits of the binary logo by Difference Expansion of 4 pixel pairs selected based on a key.
Step 3: The check sum C(S) of DWT-INCC for each block is calculated by the following algorithm

Algorithm: Checksum Computation
(1) For each block B:
(i) Denote the pixels in the block as $(P_1, P_2, \ldots\ldots, P_{16})$
(ii) Generate a pseudorandom sequence of 16 integers $n_1, n_2, n_3 \ldots n_{16}$ in a range of [0, N] controlled by a secret key.
(iii) The check-sum value CS is calculated as

$$CS = \sum_{i=1}^{16} n_i \cdot f(P_i) \bmod N \quad (4)$$

Where N is an odd number and should be chosen in such a way that CS should be of 8 bits. Where $f(P_i)$ is the grey-level of the pixel P_i (determined by the 6 MSB); this binary sequence of the checksum (7th bits) forms the *content watermark.*

Step 4: Divide each 4×4 block into four 2×2 non-overlapping sub blocks. Let the sub blocks of a block B_i be B_i^1, B_i^2, B_i^3 and B_i^4.

Step 5: The average intensity of each sub block is computed. Let the average intensities be A_i^1, A_i^2, A_i^3 and A_i^4.

Step 6: The sub block with the maximum average intensity is considered for embedding. If two or more sub blocks show the maximum average intensity then the first block from the top left is chosen.

Step 7: The sub block B_i^j selected for embedding consists of four pixels, P_1, P_2, P_3 and P_4 into 7th bit of these pixels the content watermark is embedded.

STAGE FOUR: Chaotic system

The proposed DWT-INCC systems considered chaotic system [28] because they have important characteristics such as highly sensitive to initial conditions and system parameters, pseudo random property and non-periodicity. These characteristics of chaotic signals make chaos system an excellent and robust against any statistical attacks. To achieve high security, the content normalized image of stage two is shuffled using Arnold cat map, for better authentication and protection. This integrated system is impossible to predict over a long time.

4.2 Watermark extracting process

In the proposed DWT-INCC scheme, watermark extraction is blind, that is, the original host image is not required for watermark extraction. Watermark is extracted from the watermarked image by applying the Normalization procedures which is possibly distorted or attacked. As a result, a normalized watermarked image is obtained. DWT operations are carried out on normalized image. DWT subbands of the normalized images W is divided into 4×4 non-overlapping blocks. Divide each block into 2×2 non-overlapping sub blocks. Let the sub blocks of a block be BW_i be BW_i^1, BW_i^2, BW_i^3 and BW_i^4. The average intensity of each sub block is computed. Let the average intensities be Aw_i^1, Aw_i^2, Aw_i^3 and Aw_i^4. The sub block with the maximum average intensity contains the content watermark. From the sub block Aw_i^j the 7th bit four pixels, Pw_1, Pw_2, Pw_3 and Pw_4 is extracted. The extracted bits form the content watermark. Using the chaotic system, extract bits of binary logo and recover the original pixels from the watermarked pixels. The checksum can be recomputed on the image block using Equation (1) and compared with content watermark. The equality of the both indicates that the block is not modified maliciously.

5. EXPERIMENTAL RESULTS AND ANALYSIS

Eight 256×256 sized cover images Lena, Barbara, Cameraman, Peppers, Bear, Lake, Aeroplane, and Joker are considered in the proposed DWT-INCC approach, as shown in Figure 4. A binary image "Logo MGR" of size 64×64 is used as the watermark image as shown in Figure 5. The normalized image is shown in Figure 6. In the proposed DWT-INCC approach, a = 2, b = 3 and c = 4 are chosen as three independent parameters of Arnold cat map. The initial watermark position (i,j) is chosen as (4, 6). The watermark pixel is embedded to the kth bit of pixel P(x,y) of the 2-level normalized wavelet image.

Fig 4: Cover images (a) Lena (b) Barbara (c) Cameraman (d) Peppers (e) Bear (f) Lake (g) Aeroplane (h) Joker

Fig 5: Watermark image "Logo MGR"

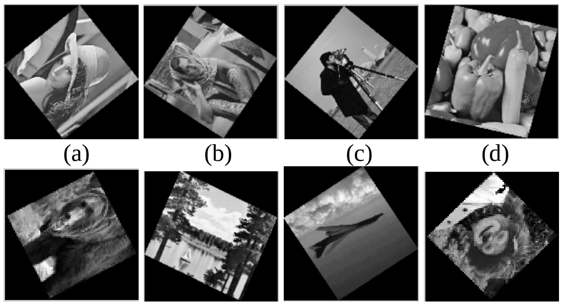


Fig 6: Normalized images (a) Lena (b) Barbara (c) Cameraman (d) Peppers (e) Bear (f) Lake (g) Aeroplane (h) Joker

The k value is determined by the subinterval of z_n generated by logistic map (4). The initial value of logistic map $z_0 = 0.5$ and μ is taken as 4 for the experiments. By this the watermark bits are embedded into 4th, 5th, or 6th bits of the pixel P(x,y) in wavelet image randomly. Let the embedded watermark pixel be denoted as P'(x,y). If w(i, j) is the same as the kth bit of P(x,y), then P'(x,y) = P(x,y), i.e., the pixel value is kept unchanged; otherwise, the kth bit of P(x,y) is substituted by w(i,j). The procedure is repeated until all watermark pixels are embedded.

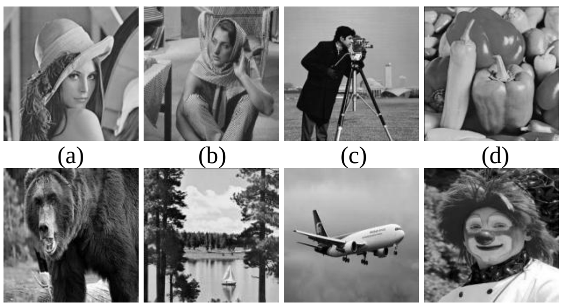


Fig 7: Watermarked images (a) Lena (b) Barbara (c) Cameraman (d) Peppers (e) Bear (f) Lake (g) Aeroplane (h) Joker

The upshots expose that there are no discernibly visual degradations on the watermarked image of proposed DWT-INCC approach presented in Figure 7. The proposed DWT-INCC approach solemnized that there is no visual degradations on the reverenced watermarked images. For further analysis of the current schemes two more metrics, universal Image Quality Index (IQI) and Structural Similarity Index Metric (SSIM) which are based on HVS are used. For all the different original test images, the watermark is successfully extracted with unit NCC. Table 1 indicates that NCC coefficient is nearly one for all extracted watermarks, which indicate the quality of the watermarked image is not degraded by the proposed DWT-INCC approach. The PSNR values of Table 1 clearly indicate the high robustness of the proposed DWT-INCC approaches. These two values are lying near to 1 that suggests watermark is highly invisible since that difference between watermarked and cover image is small as shown in Table 1. IQI and SSIM values of the proposed DWT-INCC approach is nearer to 1, this indicating the cover images and watermarked images are identical as shown in Table 1.

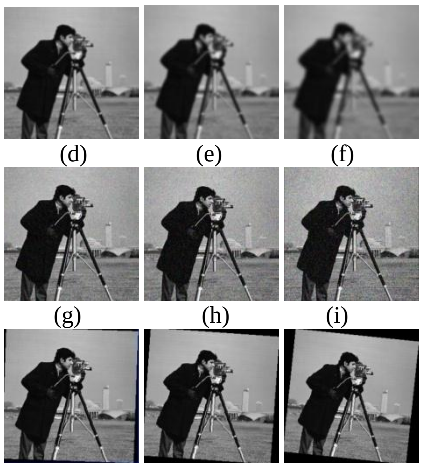
Table 1. Values of various parameters for proposed DWT-INCC approach

Original images	Proposed DWT-INCC approach			
	PSNR(dB)	IQI	SSIM	NCC
Lena	44.34	0.93	0.95	0.99
Barbara	42.69	0.99	0.97	0.98
Cameraman	42.45	0.99	0.99	1
Pepper	42.78	0.99	0.98	0.98
Bear	41.38	0.91	0.96	0.99
Lake	44.48	0.9 8	0.97	0.98
Aeroplane	42.35	0.95	0.98	0.99
Joker	42.34	0.92	0.97	0.98
Boy	42.98	0.94	0.97	0.99
Eye	43.59	0.95	0.9 8	0.99
Food	42.49	0.98	0.91	0.98
House	43.29	0.92	0.92	0.98

5.1 Proposed DWT-INCC approach with attacks

To provide evidence of the competence of proposed DWT-INCC approach, it is tested with Cropping (5%,10%,15%), Gaussian Bluring (1px,2px,3px), Noising (10%,15%,20%), Rotation (2^0,4^0,6^0) attacks. Figure 8(a)-(i) expose the watermark recognition upshots of the different attack of the Cameraman image. From the upshots, it is evident that the proposed DWT-INCC approach is proficient to perfectly detect the watermark in the watermarked images. Extracted watermark images of proposed DWT-INCC approach is given in the Figure 9.

(a) (b) (c)



(d) (e) (f)
(g) (h) (i)
(j) (k) (l)

Fig 8: Attacked watermarked images of proposed DWT-INCC approach (a) Cropping 5% (b) Cropping 10% (c) Cropping 15% (d) Gaussian Blur 1px (e) Gaussian Blur 2px (f) Gaussian Blur 3px (g) Noise 10% (h) Noise 15% (i) Noise 20% (j) Rotate 2^0 (k) Rotate 4^0 (l) Rotate 6^0

The proposed DWT-INCC approach detects perfectly the watermark from the watermarked images and it is well built robustness to the geometric and non-geometric attacks. The experimental results show that the proposed algorithm performs well against rotation, cropping, and other attacks such as Gaussian noise pollution and Gaussian Blur. Table 2 shows PSNR and NCC values respectively with various attacks on the considered images. Table 2 clearly indicates the high robustness and image quality of the DWT-INCC approach even in the presence of various attacks.

Table 2. PSNR and NCC values with various attacks of the proposed DWT-INCC approach

Type of Attack	Lena		Barbara		Cameraman		Pepper	
	PSNR	NCC	PSNR	NCC	PSNR	NCC	PSNR	NCC
Cropping 5%	40.38	0.94	40.54	0.98	39.49	0.97	40.46	0.97
Cropping 10%	39.45	0.93	39.27	0.93	38.28	0.95	38.22	0.94
Cropping 15%	37.09	0.90	38.36	0.86	36.16	0.88	37.34	0.90
Gaussian Blur 1px	39.12	0.97	40.37	0.97	39.47	0.97	38.28	0.95
Gaussian Blur 2px	38.86	0.94	38.40	0.95	38.41	0.94	37.27	0.91
Gaussian Blur 3px	36.19	0.89	37.13	0.84	36.24	0.90	36.33	0.89
Noise 10%	41.36	0.98	40.44	0.99	40.76	0.95	39.64	0.95
Noise 15%	39.48	0.93	38.67	0.93	39.40	0.94	38.29	0.93
Noise 20%	38.91	0.91	37.20	0.88	37.28	0.89	36.45	0.90
Rotate 2^0	40.20	0.93	39.67	0.96	39.60	0.95	40.37	0.96
Rotate 4^0	39.31	0.92	37.48	0.92	38.98	0.94	38.88	0.90
Rotate 6^0	38.19	0.87	36.79	0.89	36.51	0.91	37.19	0.89

Fig 9: Extracted watermark images of proposed DWT-INCC approach (a) Cropping 5% (b) Cropping 10% (c) Cropping 15% (d) Gaussian Blur 1px (e) Gaussian Blur 2px (f) Gaussian Blur 3px (g) Noise 10% (h) Noise 15% (i) Noise 20% (j) Rotate 2^0 (k) Rotate 4^0 (l) Rotate 6^0

5.2 Comparison of the proposed DWT-INCC approach with various other methods

The proposed DWT-INCC approach is compared with Latha Parameswaran et.al method [24], Say Wei Foo et. al method [25], Ping Dong et.al method [22] and Chun-Shien Lu [26] results are furnished in the Table 3. The proposed method shows better PSNR compared to other normalized based watermarking schemes [22] [24] [25] [26]. Compared with many watermarking schemes, the proposed method is resistant against many image processing attacks. For Cropping, Rotation and Noise affects the proposed DWT-INCC method is more robust than other four methods. Figure 10 clearly indicates that the proposed method shows very high PSNR value when compared with the other existing methods.

Table 3. Comparison of the proposed DWT-INCC approach with various other methods

Test Images	Latha Parameswaran et. al method	Say Wei Foo et. al method	Ping Dong et. al method	Chun-Shien Lu method	Proposed DWT-INCC approach
	PSNR(dB)				
Lena	3.38	43.30	29.29	43.94	44.34
Barbara	3.28	42.67	29.37	43.28	42.69
Cameraman	3.17	42.76	29.18	42.98	42.45
Pepper	3.58	43.01	28.38	40.47	42.78
Bear	3.83	43.12	29.24	43.1	41.38
Lake	3.82	44.16	28.87	43.76	44.48
Aeroplane	3.37	41.12	29.45	43.99	42.35
Joker	3.69	42.09	28.65	42.87	42.34

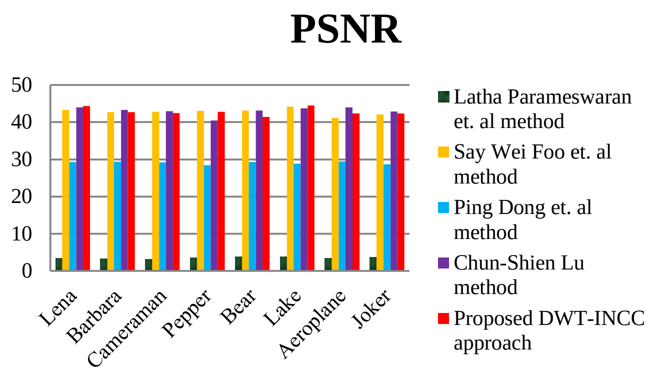


Fig 10: Comparison graph of the proposed DWT-INCC approaches with various other methods

6. CONCLUSION

The proposed DWT-INCC approach overcomes the degradation problem by embedding the watermarks in visually insensitive locations. The proposed DWT-INCC method highlights security, invisibility and quality, by preserving the original image, while maintaining robustness against common signal processing operations and attacks. The proposed DWT-INCC watermarking scheme achieve high perceptual quality of the watermarked image for human eyes, it possesses high performance of robustness to various malicious manipulations including median filtering, low pass filtering, image rescaling, image cropping, JPEG, and JPEG 2000 compression. Even the proposed DWT-INCC scheme is implemented to provide that the value of NCC of the extracted watermark is as high as 0.9 while the watermarked image is attacked by the JPEG compression with a quality factor as low as 40%. The high PSNR value of the proposed DWT-INCC indicates that it is robust to various attacks. The high NCC value of the proposed DWT-INCC with or without attacks indicates that an embedded watermark is still recoverable. Thus the proposed DWT-INCC achieves high security, authenticity, robustness, good quality, with large data capacity, high data redundancy, and high sensitivity to secret keys even in the presence of various attacks. The proposed DWT-INCC offers a sufficient level of security for a whole range of applications in computer science. Future work will be focused on more robust signature extraction method and possible ways to recover the illegally modified image without the original image. Experimental consequences shown resiliency of the proposed system against attack like image Cropping, Rotation, Adding noise, Blurring and Motion blurring and image Rotation.

7. ACKNOWLEDGMENTS

The authors would like to express their gratitude to Sri K.V.V. Satyanarayana Raju, Founder & Chairman, and Sri K. Sasi Kiran Varma, Managing Director, Chaitanya group of Institutions for providing necessary Infrastructure. Authors would like to thank the anonymous reviewers for their valuable comments.

8. REFERENCES

[1] S.W. Foo, H.S. Muh, and N.M. Mei "Image watermarking using time frequency compression expansion" IEEE International Symposium on Circuits and Systems, 2004, pp. 201-204.

[2] S.W. Foo, X. Feng, and M. Li "A blind imagewatermarking scheme using peak point extraction",

IEEE International Symposium on Circuits and Systems, 2005, pp. 4409-4412.

[3] M. Acevedo, “Image watermarking: properties, techniques and evaluation. ultimedia security: Steganography and Digital Watermarking Techniques for Protection of Intellectual Property, Idea Group Publishing. Pennsylvania, 2005.

[4] S.W. Foo, Y.T. Hee, and H.D. Yan, “An adaptive image watermarking system”, IEEE Tencon 2005, pp. 509-513.

[5] N. Cvejic and T. Seppänen, “Audio watermarking: requirement, algorithms, and benchmarking”. Digital watermarking for digital media, Information Science Publishing, Pennsylvania, 2005.

[6] A. Michael, M. Schmucker and D.Wolthusen, “Techniques and applications and Digital Watermarking and content protection”, Brithich library Cataloguing in publication data, Artech House computer security series, ISBN 1-58053-111-3. 685 Canton Street, Norwood, MA 02062.

[7] Z. Xiong, K. Ramchandran, M. T. Orchard and Y Zhang, “A comparative study of DCT- and wavelet-based image coding”, IEEE Trans. on Circuits and Systems for Video Technology, Vol.9 No.5, August, 1999

[8] K. Matsui and K. Tanaka. “Video-Steganography: How to secretly embed a signature in a picture” in IMA Intellectual Property Project Proceedings, January 1994, pp. 187-206.

[9] S. Pereira and T. Pun, “Robust Template Matching for Affine Resistant Image Watermarks”, IEEE Transactions on Image Processing, Vol. 9 No. 6, 2000, pp. 1123-1129.

[10] D. Zheng, Y. Liu, J. Zhao, and A. E. Saddik, “A survey of RST invariant image watermarking algorithm,” ACM Comput. Surv., vol. 39, no. 2, pp. 1–91, Jun. 2007, Article 5.

[11] S.Maruthuperumal, Dr.V.Vijayakumar & B.Vijayakumar (2012),” Sorted Pixel Value Difference on Fuzzy Watermarking Scheme “, Global Journal of Computer Science and Technology,Volume 12 Issue 4 Version 1.0 Fabruary.

[12] S.Maruthuperumal, B.Vijayakumar, Dr.V.Vijayakumar , ” Significant Wavelet Hierarchical Approach Using Even Odd Method for Watermarking, International Journal of Scientific & Engineering Research Volume 3, Issue 4, April-2012.

[13] S.MaruthuPerumal, Dr.V.Vijayakumar, L.Sumalatha, “Image Watermarking Based on Simplified Significant Wavelet Tree Quantization”, (IJCSIS) International Journal of Computer Science and Information Security Vol. 10, No. 2, 2012.

[14] Yeung. M.M., et al. (1997), “Digital Watermarking for High-Quality Imaging”, Proc. IEEE First Workshop on Multimedia Signal Processing, June Princeton, New Jersey, pp- 357-362

[15] Yamanaka. O, Yamaguchi. T, Maeda. J, Suzuki. Y (2008), “Image compression using wavelet transform and vector quantization with variable block size”, IEEE Conference on Soft Computing in Industrial Applications (SMCia),, Page(s): 359 – 364.

[16] Xie. L and Arce. G. R (1998), “Joint wavelet compression and authentication watermarking,” in Proc. IEEE Int. Conf. Image Processing, vol. 2, Oct., pp. 427–431.

[17] Walton, S., (1995), “Information authentication for a slippery new age”, Dr. Dobbs J. 20 (4), 18–26.

[18] X. Dai and S. Khorram, “A feature-based image registration algorithm using improved chain-code representation combined with invariant moments,” IEEE Trans. Geosci. emote Sens., vol. 37, no. 5, pp.2351–2362, May 1999.

[19] M. Alghoniemy and A. H. Tewfik, “Geometric invariance in image watermarking,”IEEE Trans. Image Process., vol. 13, no. 2, pp. 145– 153,Feb. 2004.

[20] M. Alghoniemy and A. H. Tewfik, “Image Watermarking by moment Invariants” Proceedings of IEEE international conference on Image Processing, Vancouver, 2000.

[21] P. Bas, J. M. Chassery and B. Macq, “Geometrically Invariant Watermarking using Feature Points”, IEEE Trans. on Image Processing, Vol. 9, 2002.

[22] Ping Dong and Galatsanos, N.P., "Affine transformation resistant watermarking based on image normalization", Image Processing. 2002. Proceedings. 2002 International Conference on, vol. 3, 24-28 June 2002

[23] Rothe, I.; Susse, H.; Voss, K., "The method of normalization to determine invariants", in IEEE Trans.on Pattern Analysis andMachine Intelligence, vol. 18, no. 4, April 1996, pp. 366 – 376

[24] Latha Parameswaran, and K. Anbumani (2006),” A Robust Image Watermarking Scheme using Image Moment Normalization “ , World Academy of Science and Technology 19,PP.112-116.

[25] Say Wei Foo, Qi Dong (2010),” A Normalization-based Robust Image Watermarking Scheme Using SVD and DCT”, International Journal of Information and Communication Engineering 6:4 pp.207-210.

[26] Chun-Shien Lu (2004), “Towards Robust Image Watermarking Combining Content-Dependent Key, Moment Normalization, and Side-Informed Embedding”, Technical Report ,Istitute of Information science,Taiwan.

[27] C.C.Chang, Y.S. Hu, T.C. Lu, “A Watermarking based image ownership and tampering authentication scheme, Pattern Recognition Lett.27(5) (2006) 439-446.

[28] Xianyong Wu , Zhi-Hong Gua (2007) , “A novel digital watermark algorithm based on chaotic maps,” Physics Letters A .