Indonesian Journal of Electrical Engineering and Computer Science
Vol. 15, No. 2, August 2019, pp. 750~757
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v15.i2.pp750-757

Performance analysis of DCT and successive division based digital image watermarking scheme

Prajwalasimha S N, Chethan Suputhra S, Mohan C S
Department of Electronics and Communication, ATME College of Engineering, India

Article Info

Article history:

Received Oct 13, 2018
Revised Feb 4, 2019
Accepted Mar 19, 2019

Keywords:

Frequency domain
Imperceptibility
Robustness
Vulnerable
Watermarking

ABSTRACT

In this article, a combined Discrete Cosine Transformation (DCT) and Successive Division based image watermarking scheme is proposed. In many spatial domain approaches, the watermark information is embedded into Least Significant Bits (LSBs) of host image. These LSBs are more vulnerable to noise and other unwanted information contents in the channel, in few cases these are subjected for modifications also. Many frequency domain approaches withstands LSB interference problem but utilizes more execution time. The proposed technique is a frequency domain approach which can withstand LSB attack and utilizes very less execution time than other existing approaches. Performance analysis is done based on robustness, imperceptibility, data embedding capacity and time of execution. The experimental results are better compared to other existing techniques.

Corresponding Author:

Prajwalasimha S N,
Department of Electronics and Communication Engineering,
ATME College of Engineering,
Mysuru, Karnataka, India.
Email: prajwalasimha.sn1@gmail.com

1. INTRODUCTION

The swift maturation of multimedia technology has created an easy way of digital communication between source and destination. Security concerns are the major parameters of communication, which comprises data integrity authentication and copyright protection [1-3]. Images being pictorial depiction of information, are the major class of multimedia. In digital image watermarking process, the authentication is provided by watermark to host image and the watermark is protected by the host, since it is embedded inside the host.

Digital image watermarking process is classified as: spatial and frequency domain approaches based on the methods used to develop the algorithm [4]. In spatial domain approach, the host image is not subjected for any class of transformations and watermark is directly embedded into it. This approach is more prone to security attacks [5] and utilizes less execution time. In frequency domain approach, the host image is subjected for transformations and watermark is then embedded into it. This approach is robust and imperceptibility to security attacks and utilizes more execution time [6]. Further, these are classified as robust, fragile and semi fragile techniques based on applications and blind, semi-blind and non blind approaches based on information required for extraction and detection processes [7, 8]. Imperceptibility is another important aspect of robust watermarking techniques, which describes the quality of retrieved watermark when watermarked image is subjected for various intentional or unintentional threats. An efficient watermarking scheme should resist such security attacks and provide better imprecebility [9, 10].

Digital image watermarking algorithms are characterized based on robustness, imperceptibility, data embedding capacity and time of execution. These parameters are correlated to each other. Less the data embedding capacity, better will be the robustness and imperceptibility, and vice-versa. Similarly, better the robustness and imperceptibility, more will be the time of execution and vice-versa.

Visual texturization method has been adopted by Mehran A *et al.* [11] to embed gray scale logo image into host. The texture similarity is matched between host and watermark in order to provide high degree of invisibility. Affine parameter compensation method has been adopted to increase the robustness against noise interference. The method embeds watermark with $1/16^{th}$ size of host, indicating less data capacity. The algorithm utilizes huge time for execution, even with the modern high speed processors. A hybrid two stage watermark embedding process has been proposed by Chih-Chin Lai *et al.* [12]. They adopted both Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD) techniques for embedding process. The host image is first subjected for DWT and watermark is then embedded into the singular value co-efficients of the host image's DWT subbands. The algorithm gives better imperceptibility, robustness and data capacity by embedding watermark with $1/4^{th}$ size of the host. The algorithm utilizes more time of execution due to two stage embedding process. A wavelet based watermarking scheme has been developed by Chuntao Wang *et al.* [13] Hidden Markov Model (HMM) based spherical codes are constructed and then embedded into the subbands of host. Better imperceptibility is observed. The algorithm utilizes huge execution time and provides comparatively less robustness against noise interference. A robust multiscale gradient direction quantization and DWT based watermarking scheme has been proposed by Eshan N *et al.* [14]. In this method, the invisibility of watermark is enhanced by embedding watermark into gradient vectors of subbands of transformed host at multiple wavelet scales in different angles. The algorithm provides better robustness against noise attacks and more data capacity by embedding watermark with $1/4^{th}$ the size of host. Robustness against geometrical attacks is unnoticed in the algorithm.

A combined Integer Wavelet Transform (IWT) and Singular Value Decomposition (SVD) based watermarking scheme has been developed by Nasrin M *et al.* [15]. The host image is first subjected for IWT and then decomposed into subbands. The watermark element is then embedded into these subbands. The algorithm embeds watermark with $1/4^{th}$ the size of host indicating more capacity and provides better robustness against differential and geometrical attacks. The time of execution is unnoticed and comparatively less imperceptibility is observed. Bin Wang *et al.* [16] designed an image watermarking algorithm using chaotic maps and DNA coding techniques. The watermark is first subjected for encryption process using chaotic logistic map and then embedded into host using DNA coding principle. The algorithm is more vulnerable to Least Significant Bit (LSB) attacks, since the watermark data is embedded into LSBs of host image. The algorithm utilizes more time for execution due to two stage authentication process. Musrrat Ali *et al.* [17] designed a hybrid technique which combines SVD and Artifical Bee Colony (ABC) in order to embed watermark into host. The host image is first subjected for transformation using invariant wavelet transform. The low frequency subbands are then decomposed. These are then optimized using ABC techniques and then subjected for embedding process with the watermark. Better invisibility is observed, but the algorithm support watermark with $1/16^{th}$ the size of host indicating comparatively less data capacity. Hong-Ying Yang *et al.* [18] adopted Undecimated Discrete Wavelet transformation (UDWT) and Fuzzy Support Vector Machine (FSVM) model to embed watermark into host image. The algorithm is developed to provide better imperceptibility to geometrical attacks, but supports less data capacity by embedding watermark with $1/16^{th}$ size of the host image. The algorithm utilizes more execution time. To increase imperceptibility and robustness against security attacks, Tanya Koohpayeh Araght *et al.* [19] proposed two level singular decomposition and DWT based algorithm. Even though the algorithm supports watermark with $1/8^{th}$ size of host, it utilizes more execution time for watermarking process.

A new frequency domain watermarking scheme has been developed by Prajwalasimha S N *et al.* [20]. Logarithmic transformation has been adopted to embed watermark into host image. The watermark of size $1/4^{th}$ the size of host is first subjected for logarithmic transformation and embedded into the host. Better imperceptibility and data embedding capacity is observed. The algorithm utilizes very less execution time, but robustness against noise interference is unnoticed.

Based on the above considerations a robust watermarking scheme is developed in frequency domain, which utilizes very less execution time and gives better results compared to other existing techniques. The paper is organized as follows: Section 2 describes methodology. Performance analysis is described in Section 3 and Section 4 concludes the approach.

2. RESEARCH METHODLOGY

The proposed algorithm entails two stages: Watermark embedding and Extraction processes. In the watermark embedding process, the watermark image is first subjected for concatenation to get a bulk watermark and then pixel intensities are reduced using successive division method. The host image is then subjected for DCT. The processed watermark is then embedded into the transformed host. The embedded host is then subjected for IDCT. In the de-watermarking process, the watermarked image is first subjected for DCT and then watermark is separated from the host. The separated watermark is then subjected for

successive multiplication to enhance the pixel intensities. Finally, filtering and block wise truncation are done to get individual watermarks from bulk image. Figure 1 shows the flow diagram of proposed watermarking scheme.

2.1. Watermark Embedding Process

Step1: Host image of size M X N is subjects for two dimensional Discrete Cosine transformation (DCT).

$$\beta_{pq} = \lambda_p \lambda_q \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} \delta_{mn} \cos\frac{\pi(2m+1)p}{2M} \cos\frac{\pi(2n+1)q}{2N} \quad (1)$$

Where,
$0 \le p \le M-1$
$0 \le q \le N-1$

$$\lambda_p = \begin{cases} \frac{1}{\sqrt{M}}, & p = 0 \\ \sqrt{\frac{2}{M}}, & 1 \le p \le M-1 \end{cases}$$

$$\lambda_q = \begin{cases} \frac{1}{\sqrt{N}}, & q = 0 \\ \sqrt{\frac{2}{N}}, & 1 \le q \le N-1 \end{cases}$$

Step2: Watermark of size $\frac{M}{4}$ X $\frac{N}{4}$ is subjected for concatenation to get a bulk watermark image of size n X n, same as that of the host.

$$\mathrm{r}' = \begin{bmatrix} \mathrm{r} & \mathrm{r} & \mathrm{r} & \mathrm{r} \\ \mathrm{r} & \mathrm{r} & \mathrm{r} & \mathrm{r} \\ \mathrm{r} & \mathrm{r} & \mathrm{r} & \mathrm{r} \\ \mathrm{r} & \mathrm{r} & \mathrm{r} & \mathrm{r} \end{bmatrix} \quad (2)$$

Step3: The bulk watermark image subjected for successive division process with a factor of 2/3 the maximum pixel intensity in the watermark.

$$\mathrm{r}'' = \left\{ \frac{\mathrm{r}'}{\left(\frac{2}{3}\right) Maximum\ pixel\ intensity} \right\} \quad (3)$$

Step4: The DCT host image and the compressed watermark are subjected for embedding process corresponding to each pixel.

$$\psi'(\mathrm{p},\mathrm{q}) = \beta(\mathrm{p},\mathrm{q}) + \mathrm{r}''(\mathrm{p},\mathrm{q})\ 1 < p, q < n \quad (4)$$

Where,
$\psi'(\mathrm{p},\mathrm{q})$ is the watermarked image
$\beta(\mathrm{p},\mathrm{q})$ is the host image
$\mathrm{r}''(\mathrm{p},\mathrm{q})$ is the compressed watermark
Step5: The embedded watermarked image is then subjected for Inverse Discrete Cosine Transformation (IDCT) corresponding to each pixel.

$$\delta_{mn} = \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} \alpha_p \alpha_q \psi'_{pq} \cos\frac{\pi(2m+1)p}{2M} \cos\frac{\pi(2n+1)q}{2N} \quad (5)$$

Where,
$0 \le p \le M-1$
$0 \le q \le N-1$

$$\wp_p = \begin{cases} \frac{1}{\sqrt{M}}, & p = 0 \\ \sqrt{\frac{2}{M}}, & 1 \le p \le M-1 \end{cases}$$

$$\wp_q = \begin{cases} \frac{1}{\sqrt{N}}, & q = 0 \\ \sqrt{\frac{2}{N}}, & 1 \le q \le N-1 \end{cases}$$

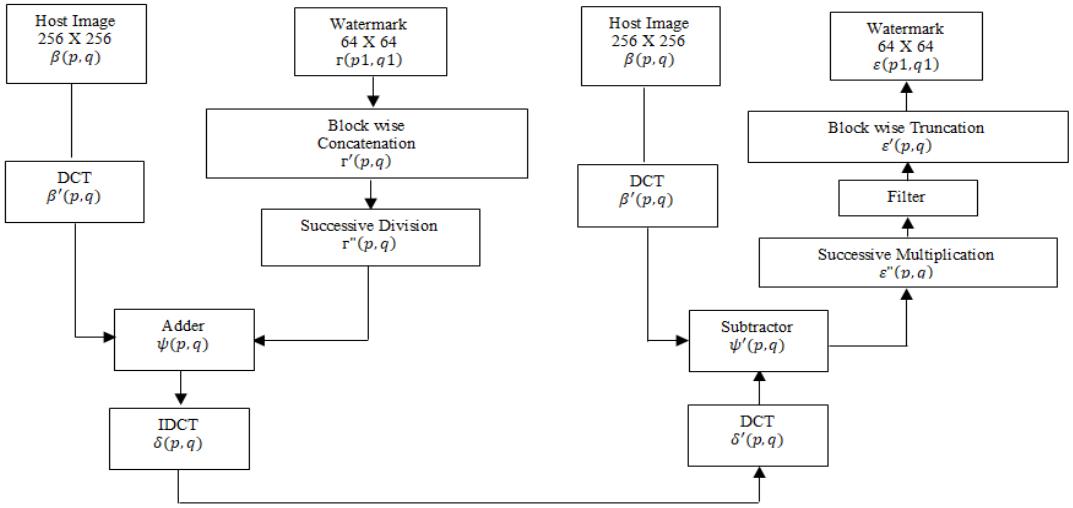


Figure 1. Flow diagram of proposed watermark embedding and De-watermarking

2.2. De-watermarking Process

Step1: Host image of size M X N is subjects for two dimensional Discrete Cosine transformation (DCT).

Step2: The obtained watermarked image is also subjected for two dimensional Discrete Cosine transformation (DCT).

Step3: The DCT watermarked image and DCT host image are subjected for de-watermarking process corresponding to each pixel.

$$\varepsilon''(p,q) = \psi'(p,q) - \beta(p,q) \; 1 < p, q < n \tag{6}$$

Where,

$\psi'(p,q)$ is the watermarked image

$\beta(p,q)$ is the host image

$\varepsilon''(p,q)$ is the compressed watermark

Step4: The compressed watermark is then intensified to get bulk watermark image using successive multiplication process.

$$\varepsilon' = \left\{\varepsilon'' * \left(\frac{2}{3}\right) Maximum\ pixel\ intensity\right\} \tag{7}$$

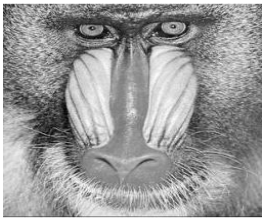
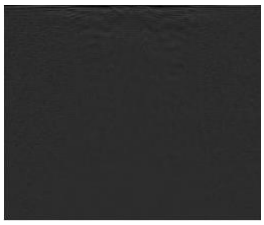
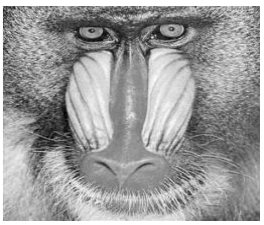
Step5: The bulk watermark is subjected for filtering process to remove noise contents.

Step6: Each pixel in the retrieved multiple watermarks is compared with each other and the median value of that will be the final pixel values of the final watermark image.

Step7: The filtered image is then subjected for block wise truncation to get multiple watermarks of 1/4th size of host.

Revelation of images under each stage of algorithm as shown in Table 1.

Table 1. Revelation of Images Under Each Stage of Algorithm

 Host Image	 Watermark image	 DCT of host
 Concatenated Watermark	 Concatenated Watermark after	 Watermarked

3. PERFORMANCE ANALYSIS

The proposed algorithm is implemented using Matlab software. Data set of ten standard test images are considered from Computer Vision Group (CVG), Dept. of Computer Science and Artificial Intelligence, University of Granada, Spain. The analysis involves peak signal to noise ratio (PSNR), mean square error (MSE), Correlation (NC), and watermark to document ratio (WDR) between host image and watermarked images. In all the above tests, the proposed system has given much better results compared to existing algorithms as tabulated below. Comparison of PSNR, MSE, WDR and correlation between host and watermarked images as shown in Table 2.

Table 2. Comparison of PSNR, MSE, WDR and Correlation between Host and Watermarked Images

Images	PSNR (dB)	MSE	WDR (dB)	Correlation(NC)
Lena	**49.29** (DWT)[20] **29.589** (DCT) [20] **37.27 (**HFT) [20] **41.28** (IMD-WC-T) [20]	**1** (DWT)[20] **26** (DCT) [20] **12 (**HFT) [20] **5** (IMD-WC-T) [20]	**-67.6553**	**1** (DWT)[20] **0.984** (DCT) [20] **0.994 (**HFT) [20] **0.999** (IMD-WC-T) [20]
Cameraman	**40.6926** (Genetic Algorithm) [10] **49.4069**	**0.7454**		**0.9999**
Pirate	**40.2608** (Genetic Algorithm) [10] **47.8271**	**1.0724**	**-66.0754**	**1**
Peppers	**52.3612** (Genetic Algorithm) [10] **49.9313**	**0.6606**	**-68.1796**	**1**
Donna	**48.3389**	**0.9532**	**-66.5872**	**0.9999**
Carnev	**50.1339**	**0.6305**	**-68.3822**	**0.9999**
Elaine	**58.8307**	**0.0851**	**-77.0790**	**0.9999**
Galaxia	**47.1476**	**1.2541**	**-65.3959**	**0.9999**
Montage	**51.6464**	**0.4451**	**-69.8948**	**0.9997**
Tulips	**48.6226**	**0.8929**	**-66.8710**	**1**
	48.1192	**1.0027**	**-66.3676**	**1**

3.1. Noise Interference

The Watermark to Document Ratio (WDR) decides the amount of recovery of watermark after the entire process. The watermarked image is subjected for median filtering process in order to remove noise in it, after intensification in de-watermarking process. Comparison is made between original and retrieved watermark images. Less the WDR (dB) value, more will be the information content in the retrieved data compared to original one. Pepper and Salt, Gaussian, Speckle and Poisson noise are considered for analysis under different density levels. Comparison of WDR between the retrieved and original watermarks under noise as shown in Table 3.

Table 3. Comparison of WDR between the Retrieved and Original Watermarks Under Noise

Noise density in watermarked image	WDR(dB) Salt & Pepper	Gaussian	Speckle	Poisson
0.1	-39.5548	-39.4931	-39.5257	
0.2	-39.5377	-39.5256	-39.4725	
0.3	-39.4690	-39.5960	-39.5665	
0.4	-39.4441	-39.6477	-39.5688	-40.0262
0.5	-39.4532	-39.6879	-39.5721	
0.6	-39.4226	-39.8175	-39.5601	
0.7	-39.3892	-39.7908	-39.5240	

3.2. Cropping Attack

Watermarked image is subjected for cropping processes in four levels. About 99.43% and 98.94% of similarities are observed between original and retrieved watermarks under 25% and 50% of cropping the watermarked images. This indicates, even though 50% of information in the watermarked image is removed or corrupted, it is possible to retrieve around 99% of watermark information from the host. Performance analysis of retrieved watermark and watermarked image under cropping attack conditions as shown in Table 4. Comparison of PSNR between the retrieved and original watermarks under cropping as shown in Table 5.

Table 4. Performance Analysis of Retrieved Watermark and Watermarked Image Under Cropping Attack Conditions

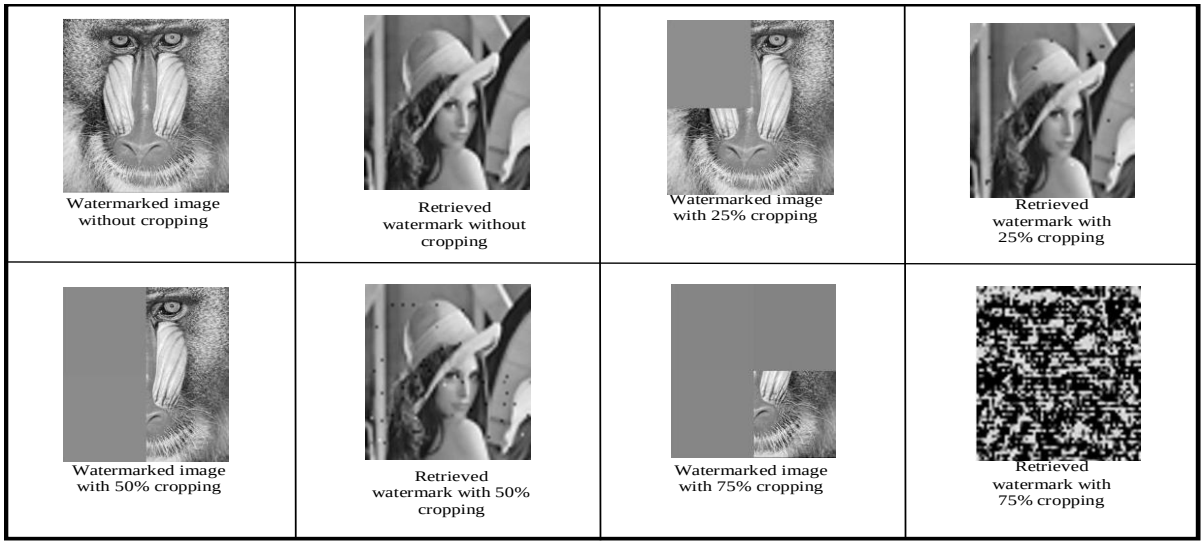


Table 5. Comparison of PSNR between the Retrieved and Original Watermarks Under Cropping

Cropping the watermarked image (%)	Correlation (NC)
0	0.9999
25	0.9943
50	0.9894
75	0.0611

3.3. LSB Neutralization & Modification Effect

Noise or unwanted contents in the channel always accumulates to least significant bit (LSB) of an image. All the LSBs of watermarked image are subjected for neutralization and modification processes and then the retrieved watermark is compared with original watermark in terms similarity index. About 93.42% and 76.59% of similarities are observed between original and retrieved watermarks under LSB neutralization and modification processes, indicating more than 75% of watermark information can be retrieved from the host, even though all the LSBs of watermarked image are neutralized or modified. Performance analysis of original and retrieved watermark image under lsb attack neutralization attack conditions as shown in Table 6. Comparison of correlation between the retrieved and original watermarks under LSB attack as shown in Table 7.

Table 6. Performance Analysis of Original and Retrieved Watermark Image under LSB Attack Neutralization Attack Conditions

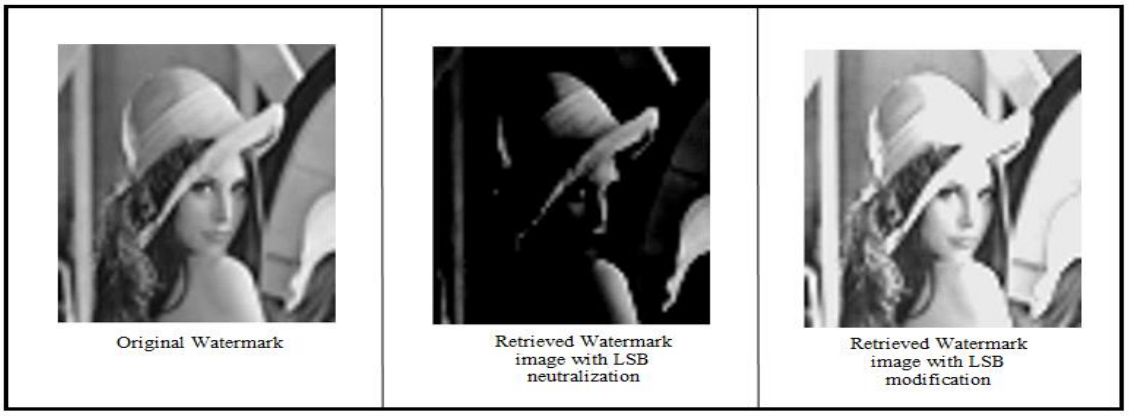


Table 7. Comparison of Correlation between the Retrieved and Original Watermarks Under LSB Attack

Degree of rotation	Correlation (NC)
LSB neutralization	0.7659
LSB modification	0.9342

3.4. Time of Execution

Time of execution is measured separately for embedding and de-watermarking processes. Intel i3 processor @ 1.7 GHz, 4GB DDR RAM and Windows 8 OS. Comparison of execution time in seconds as shown in Table 8.

Table 8. Comparison of Execution Time in Seconds

	G&E[12]	L&T[12]	DWT&SVD[12]	SHT[21]	Proposed scheme
Watermark embedding	2.989	5.701	2.107	0.11	0.087
Watermark extraction	2.301	3.964	1.086	0.47	0.376

4. CONCLUSION

The proposed technique is a frequency domain approach which embeds watermark image into host using DCT and successive division methods. The algorithm utilizes about 25 times less execution time than other existing frequency domain approaches. The algorithm results with much better PSNR, MSE, WDR and NC values compared to most popular techniques. More than 75% of watermark information can be retrieved from the host, under LSB neutralization attack, which is the major drawback of many time domain approaches. The algorithm provides data capacity by embedding watermark with $1/16^{th}$ size of the host image, which is common with the other algorithms. From all the above considerations, the proposed algorithm is a better alternative to many time and frequency domain approaches. Further, DWT can be considered instead of DCT to get still better results and more data embedding capacity than other watermarking schemes.

REFERENCES

[1] Zigang Chen, *et al.*, "A Novel Digital Watermarking Based on General Non-Negative Matrix Factorization,'' *IEEE Transactions on Multimedia*, Vol. 20, No.8, pp. 1973-1986, 2018.
[2] Prajanto Wahyu Adi, *et al.*"Robust Watermarking through Dual Band IWT and Chinese Remainder Theorem," *Bulletin of Electrical Engineering and Informatics (BEEI)*, Vol. 7, No.4, pp. 561-569, 2018.
[3] Ferda Ernawan, *et al*., "A Blind Multiple Watermarks based on Human Visual Characteristics," *International Journal of Electrical and Computer Engineering(IJECE)*, Vol. 8, No.4, pp. 2578-2587, 2018.
[4] Prajwalasimha S N *et al*.," Digital Image Watermarking Based on Sine Transformation with Constant Co-Efficient," *Proceedings of the International Conference on Inventive Research in Computing Applications*, pp. 21-24, 2018.
[5] S. Behnia, *et al.,* "Watermarking based on discrete wavelet transform and q -deformed chaotic map," *Chaos, Solitons and Fractals*, Vol. 104, pp. 6-17, 2017.

[6] Xianyong Wu, *et al.*, "A Chaos Based Robust Spatial Domain Watermarking Algorithm," *Lecture Notes in Computer Science, Springer*, Vol. 4492,pp. 113–119, 2007.
[7] Prajwalasimha S N, *et al.*, "Digital Image Watermarking using Tenth Root of Exponential Function," *Proceedings of IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology*, pp. 634-637, 2018.
[8] Prajwalasimha S.N., *et al.*, (2019) Digital Image Watermarking Using Sine Transform Technique. In: Pandian D., Fernando X., Baig Z., Shi F. (eds) *Proceedings of the International Conference on ISMAC in Computational Vision and Bio-Engineering 2018 (ISMAC-CVB)*. ISMAC 2018. *Lecture Notes in Computational Vision and Biomechanics*, vol 30. Springer, Cham.
[9] Ashok Kumar *et al*.,"A Hybrid Digital Watermarking Approach Using Wavelets and LSB," *International Journal of Electrical and Computer Engineering (IJECE)*, Vol. 7, No.5, pp. 2483-2495, 2017.
[10] Prajwalasimha S N and Pavithra A C, "Digital Image Watermarking based on Successive Division," *Proceedings of IEEE International Conference on Communication and Electronics Systems*, pp. 31-35, 2018.
[11] Mehran Andalibi and Damon M. Chandler, "Digital Image Watermarking via Adaptive Logo Texturization,'' *IEEE Transactions on Image Processing*, Vol.24, No.12, pp. 5060-5073, 2015.
[12] Chih-Chin Lai and Cheng-Chih Tsai, "Digital Image Watermarking Using Discrete Wavelet Transform and Singular Value Decomposition,'' *IEEE Transactions on Instrumentation and Measurement*, Vol.59, No.11, pp. 3060-3063, 2010.
[13] Chuntao Wang, *et al*., "An Informed Watermarking Scheme Using Hidden Markov Model in the Wavelet Domain,'' *IEEE Transactions on Information Forensics and Security*, Vol.7, No.3, pp. 853-86, 2012.
[14] Ehsan Nezhadarya, Z.Jane Wang and RababKreidieh Ward, "Robust Image Watermarking Based on Multiscale Gradient Direction Quantization,'' *IEEE Transactions on Information Forensics and Security*, Vol.6, No.4, pp. 1200-1213, 2017.
[15] Nasrin M. Makbol and Bee Ee Khoo, "A new Robust and Secure Digital Image Watermarking Scheme based on Integer Wavelet Transform and Singular Value Decomposition,'' *Journal of Digital Signal Processing*, Elsevier, Vol. 33, pp. 134-147, 2014.
[16] Musrrat Ali, *et al.*, "An image watermarking scheme in wavelet domain with optimized compensation of singular value decomposition via artificial bee colony," *Journal of Information Sciences*, Vol. 301, No. 20, pp. 44-60, 2015
[17] Bin Wang, *et al.*, "Image Watermarking using Chaotic Map and DNA Coding," *International Journal for Light and Electron Optics, Elsevier*, Vol. 126, Issue 24, pp. 4846-4851, 2015.
[18] Hong-ying Yang, *et al.*, "A Robust Digital Watermarking Algorithm in Undecimated Wavelet Transform Domain," *Journal of Computers and Electrical Engineering*, Vol. 39, pp. 893-906, 2013.
[19] Tanya Koohpayeh Araghi, *et al.*, "A Secure Blind Discrete Wavelet Transform based Watermarking Scheme Using Two-level Singular Value Decomposition," *Journal of Expert Systems With Applications, Elsevier*, vol. 6, pp. 23733-23746, 2018
[20] Prajwalasimha S.N., *et. al.*. (2019) Logarithmic Transform based Digital Watermarking Scheme. In: Pandian D., Fernando X., Baig Z., Shi F. (eds) *Proceedings of the International Conference on ISMAC in Computational Vision and Bio-Engineering 2018 (ISMAC-CVB)*. ISMAC 2018. *Lecture Notes in Computational Vision and Biomechanics*, vol 30. Springer, Cham.
[21] Prajwalasimha S N, *et al*., "Digital Image Watermarking based on Cosine Hyperbolic Transformation," *Proceedings of 3rd IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT)*, pp. 1245-1250, 2019.