

Lossless Watermarking for Image Ratification: An Implementation based on 12^{th} Root of Exponential Function



Prajwalasimha S N, Aishwarya V Kumar, Arpitha C R, Swathi S, Spoorthi B

Abstract: In this article, an exponential transformation based digital image watermarking scheme has been described. The method is employed with 12^{th} root of exponential function for embedding watermark into the cover image. Due to bulk data capacity of the image, many watermarking techniques uses more time for data insertion and separation processes. Algorithm is designed in such a way to embed a watermark of $1/16^{\text{th}}$ size of host. The retrieved watermark is examined under various security analysis. Many standard test images are subjected for watermarking process under proposed scheme resulted with better scale and utilizes less computational time compared to other techniques.

Keywords: Watermarking, Exponential, Computational time, Bulk data and Security analysis.

I. INTRODUCTION

The simplicity of digital media modification and dispersion compels satisfied armor ahead of encryption. In decrypted form information is veiled in the form of watermarks. By embedding purveyor's information, their property is endangered and copyright protection is fortified [1]. To advance robustness and security, multiple image watermarking is applied for the copyright of purveyor's. Numerous fictions were certainly about Discrete Wavelet Transform (DWT) watermarking methods for data fortification. These DWT based watermarking schemes are establish to be scarcer robust beside image processing attacks and the shift variance of Wavelet Packet Transform (WPT) causes erroneous extraction. With the extensive increase of broadcast means, digital data are spread all over the world and becomes vulnerable to unofficial admittance. Consequently, a logical possessions deliberates more concentration on digital data to safe guard them. Digital

watermarking is a one of the expectant techniques to make certain the copyright of digital data [2].

In digital watermarking, the watermark is a recognition cryptogram that takes information of the copyright owner. Watermarking is a significant technique in the region of information security [3-12]. It is one of the important techniques which are used for preservation the genesis of the image by defensive it against piracy [13-18].

Multiple watermarking closely combines the compensation of single watermarking to produce classy watermarking techniques for high security and robustness. The multiple images watermarking technique based on hybrid Steerable Pyramid with Discrete Wavelet Transform (SPDWT) is proposed and it is compared with Integer Wavelet Transform (IWT). In this implant, input image is transformed by steerable pyramid results in various sub-bands and DWT is applied to these sub-bands. Then watermarks are embedded in particular sub-bands and inverse is done to obtain the watermarked image. For watermark extraction, Pearson Independent Component Analysis (PICA) is applied as it attains the new attribute, not entails the renovation procedure in watermark extraction. The invariance properties of the steerable pyramid transform may be broken to retaliation geometrical attacks. Robustness is also procured by the multiresolution feature ensuing from the request of the steerable pyramid transform [19]. This makes probable to pelt watermarks with more power in an image and also to insert information redundancies from one band to another

Seok Lee et. al. [20] anticipated a new digital image watermarking method based on variation prediction mapping and Discrete Wavelet Transformation (DWT). The algorithm results with very less data entrenching capacity of $1/768^{\text{th}}$ size of host. Fan D et al. [21] proposed a combined digital image watermarking algorithm in Contourlet domain using adaptive quantization. The algorithm supports less data entrenching capacity by inserting watermark image of size $1/256^{\text{th}}$ size of host. The algorithm results with improved similarity between original and retrieved watermark images.

In pooled entropy and histogram based digital image watermarking outline, the host image is separated into blocks. These blocks are called on the basis of entropy. The algorithm results with less data embedding capacity with $45/65536^{\text{th}}$ size of host [22]. In the scheme developed by Tanya et. al. [23], DWT and two level SVD entrenches the watermark into host.

Revised Manuscript Received on November 30, 2019.

* Correspondence Author

Prajwalasimha S N*, Department of Electronics & Communication Engineering, ATME Research Centre, Mysuru, India.

Email: prajwalasimha.sn1@gmail.com

Aishwarya V Kumar, Department of Electronics & Communication Engineering, ATME College of Engineering, Mysuru, India.

Arpitha C R, Department of Electronics & Communication Engineering, ATME College of Engineering, Mysuru, India.

Swathi S, Department of Electronics & Communication Engineering, ATME College of Engineering, Mysuru, India.

Spoorthi B, Department of Electronics & Communication Engineering, ATME College of Engineering, Mysuru, India.

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an open access article under the CC-BY-NC-ND license <http://creativecommons.org/licenses/by-nc-nd/4.0/>

The algorithm implants watermark of 1/32th size of host signifying less data embedding capacity and results with enhanced similarity between original and retrieved watermark images. Zhuhong Shao et. al. [24] described a combined watermarking method using Orthogonal Fourier transformation and chaotic maps.

The algorithm results with bulk data capacity by entrenching watermark of 1/16th size of host. Improved similarity is perceived between original and retrieved watermark images. But time of execution is unnoticed in the scheme.

Based on the above facets, a stalwart watermarking scheme is developed in frequency domain, which utilizes very less execution time and gives improved similarity between original and retrieved watermark images compared to other existing schemes. The paper is organized as follows: Section 2 describes methodology. Performance analysis is described in Section 3 and Section 4 concludes the approach.

II. PROPOSED METHOD

In the anticipated scheme, watermarking image is imperiled to exponential transformation and concatenated together to get a bulk watermark. After secrete key verification process, the bulk watermark is embedded into host. In the de-watermarking process, watermark is parted from host with the help of secrete key and subjected for filtering process. The processed watermark is then subjected for intensification using anti-exponential operator. The bulk watermark is de-concatenated to get separate watermark images. The individual watermark images are combined together to get resultant watermark image. Fig. 1 shows the flow diagram of proposed technique.

A. Watermark Entrenching Process

Step1: In watermark embedding process, a gray scale image of size 256X256 is reserved as cover image.

Step2: Secrete key verification process.

Step3: After obtaining the preferred secrete key combination, the watermark image (64X64) is imperiled for twelveth root of exponential function.

$$WM|(\alpha, \beta) = \sqrt[12]{[WM(\alpha, \beta)]} \quad 1 < \alpha, \beta < 64 \quad (1)$$

Where,

$WM(\alpha, \beta)$ is the input watermark

$WM|(\alpha, \beta)$ is the transformed watermark

Step4: A concatenated watermark of size 256X256 is composed.

$$WM||(\alpha, \beta) = \begin{bmatrix} W|(\alpha', \beta') & W|(\alpha', \beta') & . & . \\ W|(\alpha', \beta') & . & . & . \\ . & . & . & . \\ . & . & . & W|(\alpha', \beta') \end{bmatrix} \quad (2)$$

Where,

$W|(\alpha', \beta')$ is the transformed watermark of size 64X64

$WM||(\alpha', \beta')$ is the concatenated watermark of size 256X256

Step5: The cover image and corresponding bulk watermark are exposed to arithmetic addition to get the final watermark.

$$WM'(\alpha, \beta) = HI(\alpha, \beta) + WM||(\alpha, \beta) \quad (3)$$

$$1 < \alpha, \beta < 256$$

Where,

$WM'(\alpha, \beta)$ is the Watermarked image.

$HI(\alpha, \beta)$ is the host image of size.

$WM||(\alpha, \beta)$ is the transformed watermark.

B. De-Watermarking Process

The number of rounds for decryption stage (d) is taken from the pixel values in the four extreme corners of the cipher image.

Step1: The obtained watermarked image is imperiled to median filtering process to de-noise the image.

Step2: The de-noised image is imperiled to arithmetic subtraction with the same cover to get the watermark in the exponential level.

$$WM'|(\alpha, \beta) = WM'(\alpha, \beta) - HI(\alpha, \beta) \quad (4)$$

$$1 < \alpha, \beta < 256$$

Where,

$WM'(\alpha, \beta)$ is the Watermarked image.

$HI(\alpha, \beta)$ is the host image.

$WM'|(\alpha, \beta)$ is the transformed

watermark.

Step3: The obtained watermark of size 256X256 is de-concatenated.

$$WM||(\alpha, \beta) = \begin{bmatrix} W|(\alpha', \beta') & W|(\alpha', \beta') & . & . \\ W|(\alpha', \beta') & . & . & . \\ . & . & . & . \\ . & . & . & W|(\alpha', \beta') \end{bmatrix} \quad (5)$$

Where,

$W|(\alpha, \beta)$ is the transformed watermark of size 64X64

$WM||(\alpha, \beta)$ is the concatenated watermark of size 256X256

Step4: After obtaining the desired secrete key combination, the obtained watermark of size 64X64 in the transformed phase is subjected for twelveth power of exponential function.

$$WM'|(\alpha, \beta) = [WM||(\alpha, \beta)]^{12} \quad 1 < \alpha, \beta < 64 \quad (6)$$

Where,

$WM||(\alpha, \beta)$ is the transformed watermark

$WM'|(\alpha, \beta)$ is the resultant watermark

III. EXPERIMENTAL RESULTS

The proposed algorithm is implemented using Matlab2013a software along with Intel i3 processor @ 1.7 GHz, 4GB DDR RAM and Windows 8 OS. The performance analysis involves Watermark to Document Ratio (WDR), Peak Signal to Noise Ratio (PSNR), Average Correlation (NC), Mean Square Error (MSE) and Time of Execution.



Standard test images are considered from Computer Vision Group (CVG), Dept. of Computer Science and Artificial Intelligence, University of Granada, Spain.

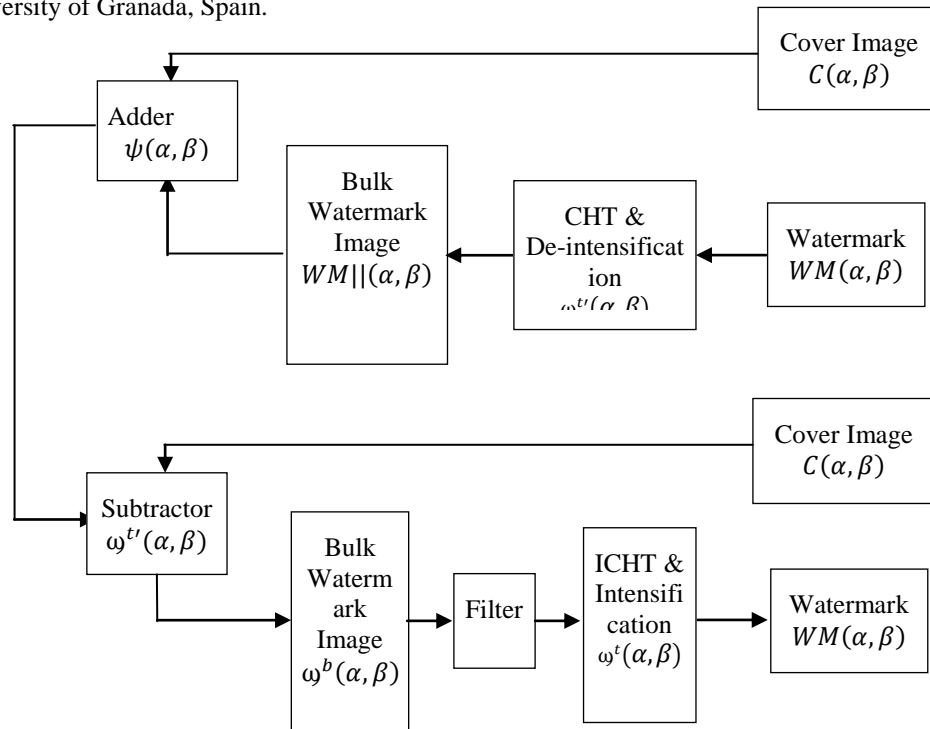
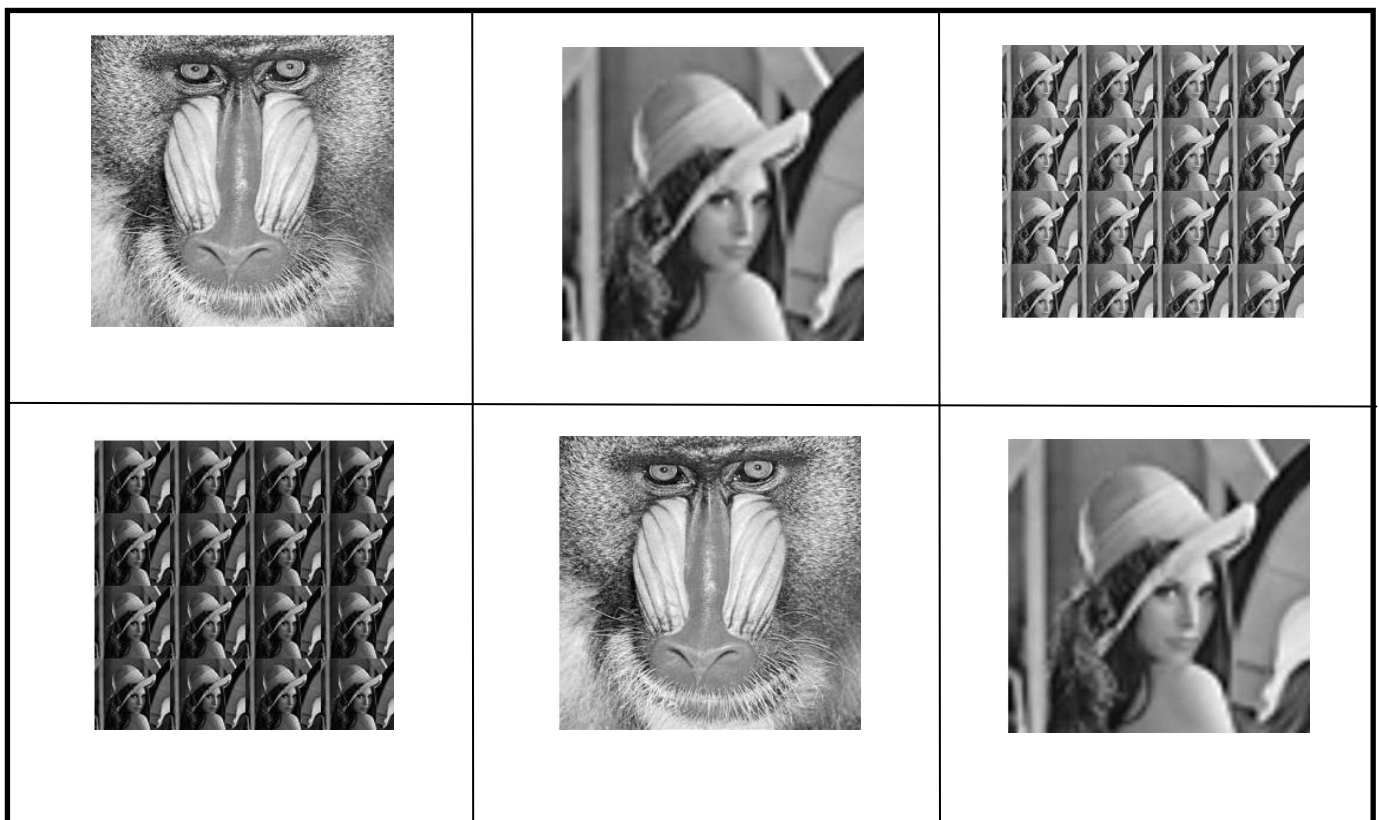


Fig.1 Flow diagram of proposed Watermark embedding and

Table 1 Revelation of images in watermarking process



embedded images

Images	PSNR (dB)	MSE
Lena	49.29 (DWT)[7]	1 (DWT)[7]
	29.589 (DCT) [7]	26 (DCT) [7]
	37.27 (HFT) [10]	12 (HFT) [10]
	41.28 (IMD-WC-T) [10]	5 (IMD-WC-T) [10]
	40.6926 (Genetic Algorithm) [3]	2.1031
	44.9022	
Barche	44.6983	2.2042
Peppers	44.7661	2.1701
Baboon	44.6355	2.2363
Donna	44.9798	2.0658
Carnev	47.5055	1.1549
Elaine	44.6078	2.2506
Galaxia	44.9459	2.0820
Plane	44.5315	2.2905
Pallon	44.7449	2.1807

Table II: Comparison of WDR and Correlation between cover and embedded images

Images	WDR (dB)	Average Correlation
Lena	-62.6341	1 (DWT)[7]
		0.984 (DCT) [7]
		0.994 (HFT) [10]
		0.999 (IMD-WC-T) [10]
		0.9996
Barche	-62.4302	0.9995
Peppers	-62.4979	0.9995
Baboon	-62.3674	0.9991
Donna	-62.7117	0.9992
Carnev	-65.2374	0.9992
Elaine	-62.3397	0.9991
Galaxia	-62.6778	0.9975
Plane	-62.2634	0.9976
Pallon	-62.4768	0.9994

Table III Comparison of execution time in seconds

Different Techniques	Watermark embedding	Watermark extraction
G&E[11]	2.989	2.301
L&T[11]	5.701	3.964
DWT&SVD[11]	2.107	1.086
ALT-MARK [11]	4.8	0.9
Proposed scheme	0.21	0.53

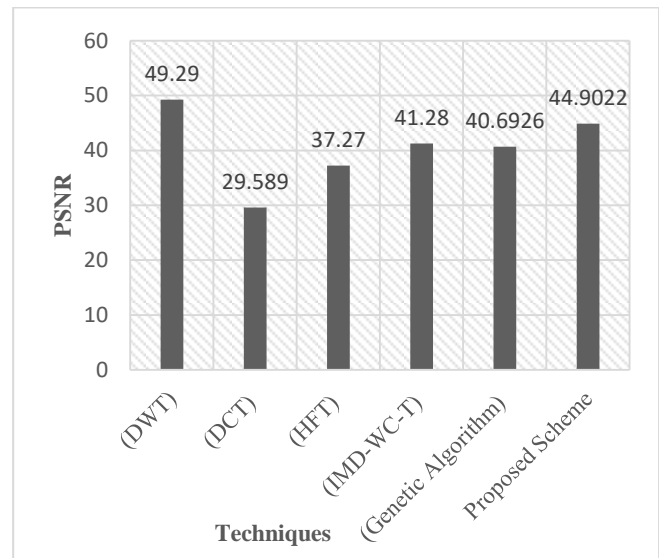


Fig.2 Comparison of PSNR

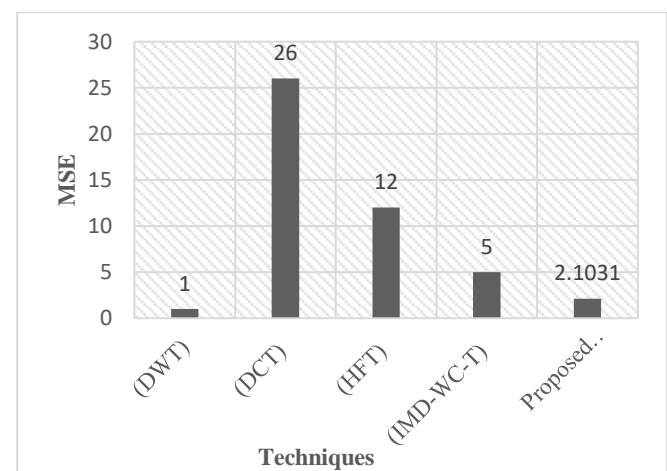


Fig.3 Comparison of MSE

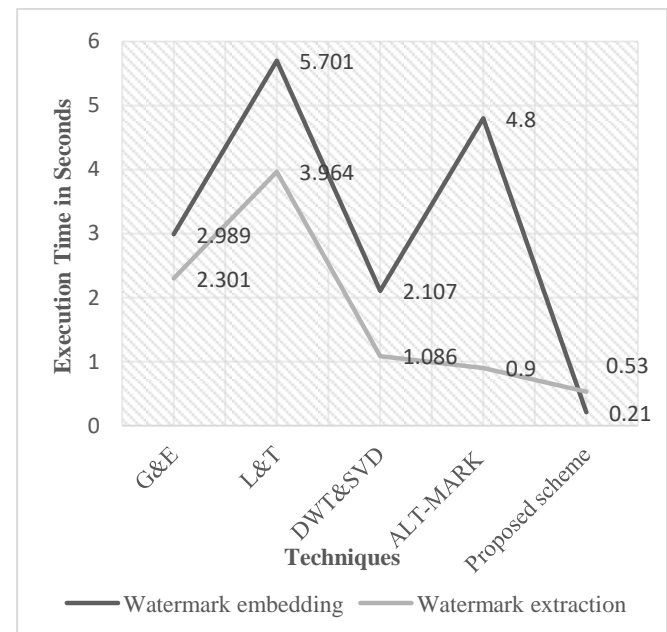


Fig.4 Comparison of execution time in seconds

Inference-1:

The average Mean Square Error (MSE) value is 2.1, slightly more than DWT technique and very much less than other popular watermarking approaches. The average Peak Signal to Noise Ratio (PSNR) value is 44.9 dB, which is very much close to DWT technique and very much high compare to other popular techniques.

Inference-2:

The average correlation co-efficient value is 0.999, indicating 99.9% similarity between original and retrieved watermark images. The value is very close to DWT technique and very much high compare to other hybrid techniques.

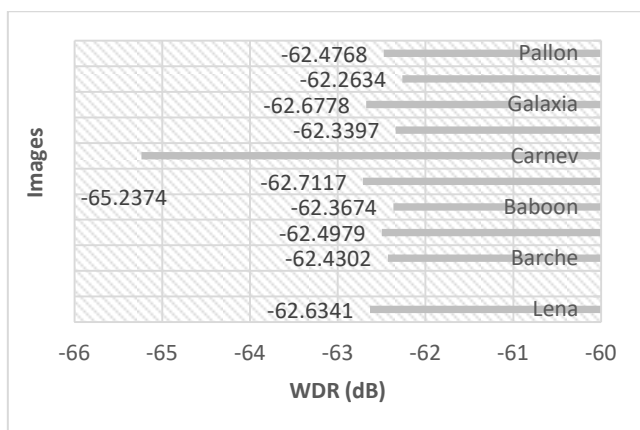


Fig.5 Comparison of WDR (dB)

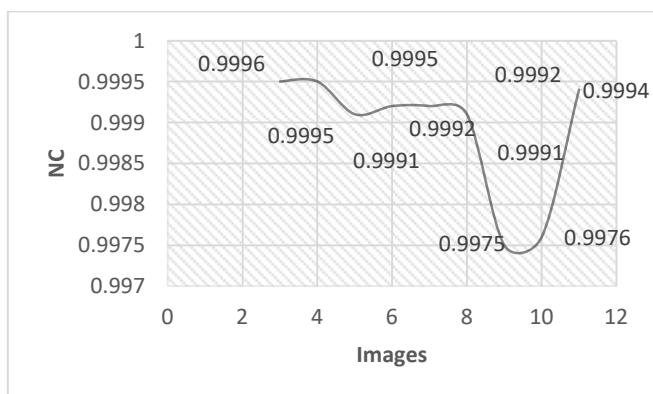


Fig.6 Comparison of Correlation between original and retrieved watermark images

IV. CONCLUSION

The suggested scheme entrenches watermark into host using 12th root of exponential function. Data implanting ability of the algorithm is about 1/16th size of the host. Better robustness is achieved under security analysis. Computational time of the proposed scheme is about 15 times less than other existing approaches. With this, the proposed scheme is a fast frequency domain method which supports bulk data embedding capacity. Further, Discrete Sine Transformation, Discrete Cosine Transformation and Discrete Wavelet Transformation can be adopted to enhance robustness and imperceptibility.

REFERENCES

1. Zigang Chen, Lixiang Li, Haipeng Peng, Yuhong Liu and Yixian Yang, "A Novel Digital Watermarking Based on General Non-Negative Matrix Factorization," IEEE Transactions on Multimedia, Vol.20, No.8, pp. 1973-1986, 2018
2. 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
3. Prajwalasimha S N et. al., "Performance analysis of DCT and successive division based digital image watermarking scheme," Indonesian Journal of Electrical Engineering and Computer Science, Vol. 15, No. 2, pp. 750-757, 2019
4. Prajwalasimha S N and Basavaraj L, "Performance Analysis of Transformation and Bogdonov Chaotic Substitution based Image Cryptosystem," International Journal of Electrical and Computer Engineering, Vol. 10, No. 1, 2020, pp. 188-194
5. Anupama Shetter et. al., "Image de-noising algorithm based on filtering and histogram equalization," Proceedings of the International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud), I-SMAC 2018, pp. 325-338
6. Prajwalasimha S N and Basavaraj L, "Design and Implementation of Transformation and non-Chaotic Substitution based Image Cryptosystem," International Journal of Engineering and Advanced Technology, Vol. 8, Issue 6, pp.1079-1083, 2019
7. Prajwalasimha S.N., Sowmyashree A.N., Suraksha B., Shashikumar H.P. (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 (ISMAL-CVB). ISMAC 2018. Lecture Notes in Computational Vision and Biomechanics, vol 30. Springer, Cham
8. 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
9. 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
10. Prajwalasimha S.N., Sonashree S., Ashoka C.J., Ashwini P. (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 (ISMAL-CVB). ISMAC 2018. Lecture Notes in Computational Vision and Biomechanics, Vol 30. Springer, Cham
11. Prajwalasimha S N et. al., "Performance Analysis of Combined Discrete Fourier Transformation (DFT) and Successive Division based Image Watermarking Scheme," International Journal of Recent Technology and Engineering, Vol. 8, Issue 3, 2019, pp. 34-39
12. Prajwalasimha S N et. al., "Digital Image Watermarking based on Sine Hyperbolic Transformation," Proceedings of 3rd IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT), pp. 1245-1250, 2019
13. Prajwalasimha S N et. al., "Design and Implementation of Image Watermarking Scheme based on Exponential Function," International Journal of Innovative Technology and Exploring Engineering, Vol. 8, Issue 12, 2019, pp.5789-5792
14. Prajwalasimha S.N. (2019) Pseudo-Hadamard Transformation-Based Image Encryption Scheme. In: Krishna A., Srikantaiah K., Naveena C. (eds) Integrated Intelligent Computing, Communication and Security. Studies in Computational Intelligence, vol 771. Springer, Singapore
15. Prajwalasimha S N and Bhagyashree S R, "Image Encryption using Discrete Radon Transformation and Non chaotic Substitution," Proc. of IEEE International Conference on Electrical, Computer and Communication Technologies, pp. 842-846, 2017
16. Prajwalasimha S N and Usha Surendra, "Multimedia Data Encryption based on Discrete Dyadic Transformation," Proc. of IEEE International conference on Signal processing and Communication, pp. 492-496, 2017
17. Prajwalasimha S N et. al., "Design and analysis of pseudo hadamard transformation and non-chaotic substitution based image encryption scheme," Indonesian Journal of Electrical Engineering and Computer Science, Vol. 15, No. 3, 2019, pp. 1297-1304
18. Prajwalasimha S N et. al., "On the Sanctuary of a Combined Confusion and Diffusion based scheme for Image Encryption," International Journal of Engineering and Advanced Technology, Vol. 9, Issue 1, pp.3258-3263, 2019

19. Azz El Arab El Hossaini and Mohamed El Aroussi, "A New Robust Blind Watermarking Scheme based on Steerable pyramid and DCT," *Journal of Computers*, Vol. 9, pp. 2315-2327, 2014.
20. Yong-Seok Lee, et al., "Digital blind watermarking based on depth variation prediction map and DWT for DIBR free-viewpoint image," *Signal Processing: Image Communication*, Vol. 70, pp. 104–113, 2019
21. Di Fan, et al., "A blind watermarking algorithm based on adaptive quantization in Contourlet domain," *Multimedia Tools and Applications*, pp. 1-15, 2019
22. Sunesh Malik, et al., "Histogram and entropy based digital image watermarking scheme," *Information Technology*, Vol. 11, No. 22, pp. 373-379, 2019
23. Tanya Koohpayeh Araghi, et al., "A Secure Blind Discrete Wavelet Transform based Watermarking Scheme Using Two-level Singular Value Decomposition," *ESWA*, Elsevier, vol. 6, pp. 23733-23746, 2018
24. Zhuhong Shao et al., "Robust Watermarking using Orthogonal Fourier-Mellin Moments and Chaotic Map for Double Images," *International journal of Signal Processing*, Vol. 120, pp. 522-531, 2016