Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 167 (2020) 213–223

Procedia Computer Science

www.elsevier.com/locate/procedia

International Conference on Computational Intelligence and Data Science (ICCIDS 2019)

Novel Image Watermarking Approach against Noise and RST Attacks

Sheshang D. Degadwala[a], Mohini Kulkarni[b], Dhairya Vyas[c], Arpana Mahajan[d] *

[a] *Head of Department, Computer Engineering, Sigma Institute of Engineering, Vadodara, India*
[b] *PG Student, Computer Engineering, Sigma Institute of Engineering, Vadodara, India*
[c] *Assistant Professor, E&C Engineering, Sigma Institute of Engineering, Vadodara, India*
[d] *Assistant Professor, Computer Engineering, Sigma Institute of Engineering, Vadodara, India*

Abstract

Digital watermarking is used for copyright protection of intellectual properties and hence it is important to protect and recover data from attacks. Existing systems work on and recover the image from single attacks. This paper aims at proposing a technique for retrieval of cover image and watermarked data from dual attacks like rotation and noise attacks. The proposed system takes as input, Color images and then embeds data using alpha blending method. And also tries to recover from dual attacks using median filtering and pseudo Zernike moment. Proposed approach selects LH band from the 4 sub bands image divided into using DWT and for reducing noise from the image SVD is used. Proposed approach is giving better results in terms of PSNR and MSE as compared to other existing systems using QWT.

Keywords: Digital watermark; Noise attacks; Rotation attack; Scaling; Translate; Pseudo Zernike Moments.

* Corresponding author. Tel.: +91-9898421385.
E-mail address: sheshang13@gmail.com

10.1016/j.procs.2020.03.198

1. Introduction

Copyright protection in digital media is a security threat nowadays as everything is being shared using this medium only. Given to the fact that copyrights being invisible which means invisible to human eyes. Image is embedded inside the host image and it is done by using various techniques. Steganography was one way to protect these copyrights but attackers hacked keys shared by the users and watermarking concept came into the copyright protection. Watermarking uses so many methods so that we can embed data into the image and also can extract the same data from the image. As digital world is growing faster, watermarked image can be attacked geometrically or non-geometrically to gain data or to distort the data hidden inside the image. To avoid and prevent attacks from harming the data image watermark experts tried and succeeded in recovering single attack done on the image but attackers may also apply dual attacks.

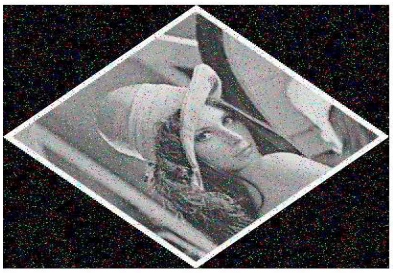

Fig. 1. Dual Attack

As shown in the above image, watermarked image can be rotated and noise can also be added to it. These types of dual attacks harm the cover image as well as the data image which is hidden inside the host image. Hence, proposed system is aiming to retrieve data from single attacks as well as from the dual attacks. Moreover, proposed system also recovers the host image from the attacks.

To achieve the aim proposed system uses methods of transform domain, embedding approach, noise reduction approach, angle detection approach like:

1.1. .DWT

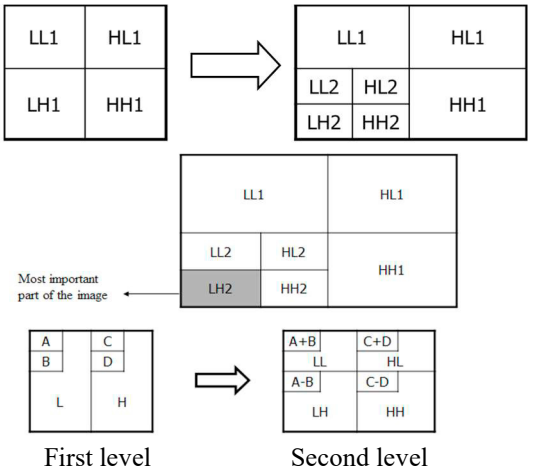

Fig. 2. DWT Application

Discrete Wavelet Transformation is a technique generally utilized in digital signal processing, image compression, watermarking and so on. Discrete Wavelet Transform is a standout amongst the most essential strategies in transforming a spatial domain image into frequency domain image. The wavelet transform breaks down the image into three spatial bearings, for example horizontal, vertical and diagonal. They offer a simultaneous localization in both time & Frequency Domain, Multi resolution analysis, higher compression proportion which is applicable to human discernment. [8]

- DWT fragments an image into an arrangement of band constrained segments.
- DWT isolates an image into four bands of information meant by LL, HL, LH and HH detail parts.
- From which we can select LH band to embed data which is so important because it have the middle frequency of data, and after applying attacks the pixels of pictures will not be damaged as compare to lower frequency bands.

1.2. DCT[14]

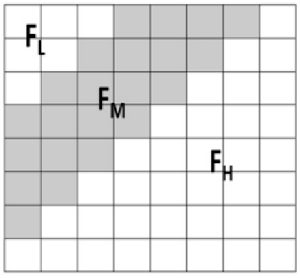

Fig. 3. DCT

Deseret Cosine Transformation speaks to data as far as frequency space as opposed to an amplitude space. Watermarking techniques which depend on DCT are progressively robust contrasted with spatial domain techniques. These algorithms are robust against advanced image preparing activities like low pass filtering. Brightness and contrast adjustment and so forth. In proposed system watermark is embedded into the middles frequency so noticeability of the image will not get influenced. But few higher frequency parts will in general be smothered amid the quantization process. Block wise DCT destroys the immutable property of system.

1.3. SVD[5]

Fig. 4. SVD

SVD is singular value decomposition. Being a simple method this method is used to reduce the noises in the image. Though SVD cannot efficiently remove whole noise from the image but certainly denoises some parts of the image.

1.4. Pseudo Zernike Moment[5]

Pseudo Zernike moments are used to choose and/or acquire angle of the image to embed data into or to extract data from the host image. Pseudo Zernike moments are invariant to rotation, scaling, shift and affine transforms but this method cannot recover image from noise attacks. Proposed system uses this technique to select asymmetric angles of the image to embed data so that cropping on symmetric angles cannot harm secret data.

1.5. Alpha Blending Method[5]

Alpha blending method is utilized to approximate illumination calculations through transparent or translucent objects. Alpha blending is utilized to embed the watermark in the host image. In this procedure the disintegrated segments of the host image and the watermark are duplicated by a scaling factor and are included. Formula of alpha blending in watermarked image is given by,

$$\mathbf{W = C + (ALPHA * DATA)} \quad (1)$$

Where,

W= Watermarked Image

C= Cover Image

Alpha= Value between 0-1

Data = Secret Data

1.6. Median Filtering

123	125	126	130	140
122	124	126	127	135
118	120	150	125	134
119	115	119	123	133
111	116	110	120	130

Fig. 5. Median Filtering

Median filtering is a noise removal technique mostly used for non-geometric attacks like noise attacks. Advantage of using median filtering is that it preserves sharp edges better than any other method. But it may also remove image details like thin lines and corners at time of noise reduction. [13]

For example in figure 5 we can see pixel matrix of an image in which 124,126,127,120,150,125,115,119,123 are neighborhood values. After sorting these values in ascending order we will get 124 as median value. So the middle value 150 will be replaced by median value 124 rather than any other unrepresentative value.

2. Proposed System

Table 1: Comparison between existing system and proposed system

Parameters	Existing[1]	Proposed
Transform	QWT-DCT	DWT-DCT-SVD
Rotation Attack	Only on symmetric angles	Symmetric and Non symmetric angles
Scale Attack	Yes	Yes
Noise Attacks	Yes	Yes
Dual Attacks	No	Yes
Attack Recovery	Arnold Map	Pseudo Zernike Moment
PSNR	40-50 dB	More than 50 dB
Cover Image	Grey	Grey, Colour
Embedding Approach	Colour Model	Alpha Blending

Proposed system uses DWT-DCT-SVD as transformation methods which is better than existing system which uses QWT because dual approach of DWT and DCT makes host image more robust against digital processing and embedding data into middle frequency makes it harder to remove data image by attacks whereas QWT is less efficient when it comes to color images because host image needed to convert in to YIQ space.

Proposed system uses Pseudo Zernike Moment to help recover data image from rotation and scaling in to different ratio images where existing system uses Arnold map which limits the scope of recovering image which are in N X N formats only.

2.1. Embedding Approach

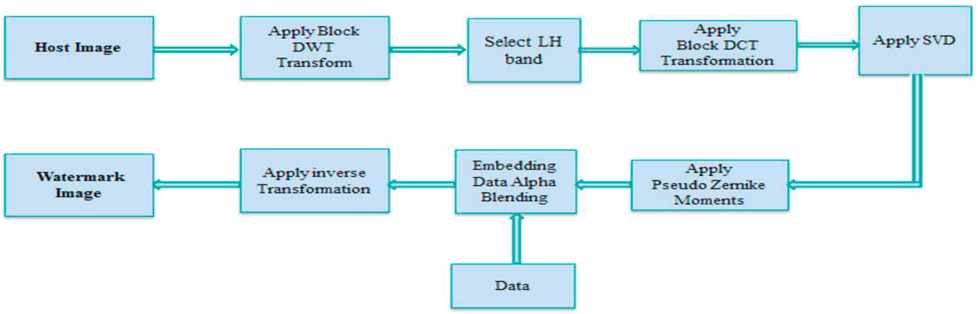

Fig. 6. Proposed System Embedding process

In embedding process of proposed system as first step host image is selected. In second step Block DWT transformation is applied and this will partition host image into 4 bands. From which LH bit is selected. So that user can embed large data as compared to other bits and it maintains higher resolution of image. On LH bit block DCT

transformation is applied so that middle frequency can be selected of the host image which will prevent image from losing its higher resolutions. As step 5 SVD is applied to reduce noise if there is any after all the procedure. After denoising image asymmetric angle for data embedding is chosen using pseudo Zernike moments. Then in step 7 data is embedded using alpha blending method where in our system we are using alpha value 0.32. After this step inverse transformation is applied to gain the original image and this is how we will get original image with watermark.

2.2. Extraction Approach

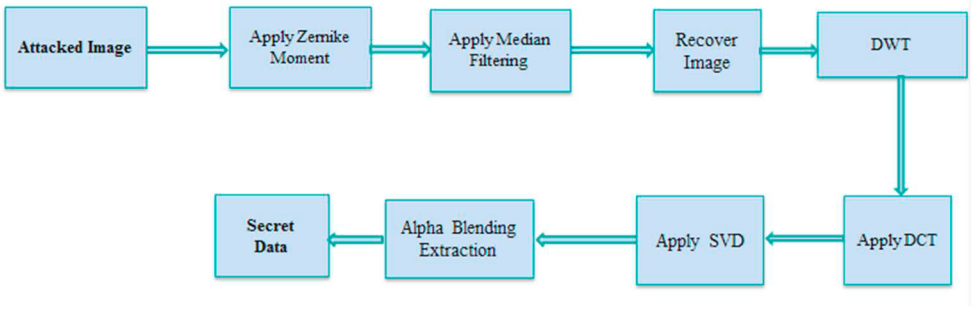

Fig. 7. Proposed system extraction process

In extraction process of proposed system firstly attacked image is received. Then pseudo Zernike Moment is applied on attacked image after that median filtering is applied to remove any noise existing in image. And this is how cover image is recovered. After that DWT is applied to select LH bit of the image. Then DCT is applied to select middle frequency of LH bit where data is hidden. On this SVD is applied to reduce noise if there is any. Further, Alpha blending method is used to extract secret data from cover image and secret data is acquired.

3. Results Analysis

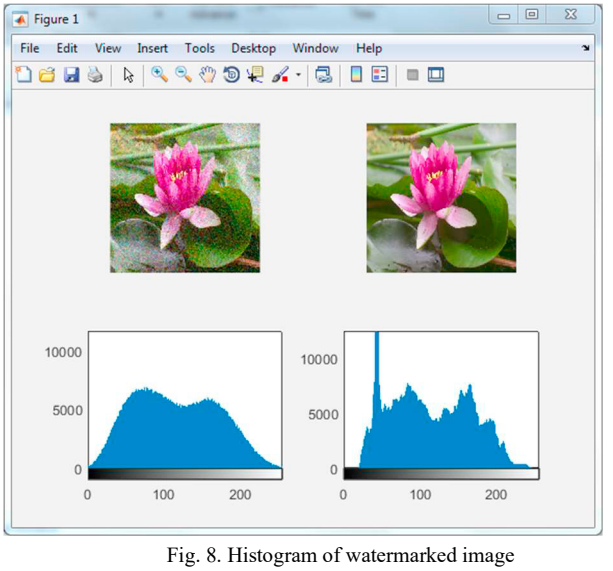

Fig. 8. Histogram of watermarked image

Figure 8 shows difference in original and watermarked image's pixel values before and after embedding data and attack. Here, Gaussian attack is applied to host image having data image embedded into it and there is visible difference in intensity of image after embedding data into host image.

Table 2. PSNR of cover image after embedding

NO.	IMAGE	DATA	EXISTING System[1]	PROPOSED System
1		A	48.84	54.6
2		C	49.23	56.49
3		D	48.86	47.7
4		B	49.04	49.52
5		M	49.38	52.93
	Average PSNR		49.07 Db	52.24 Db

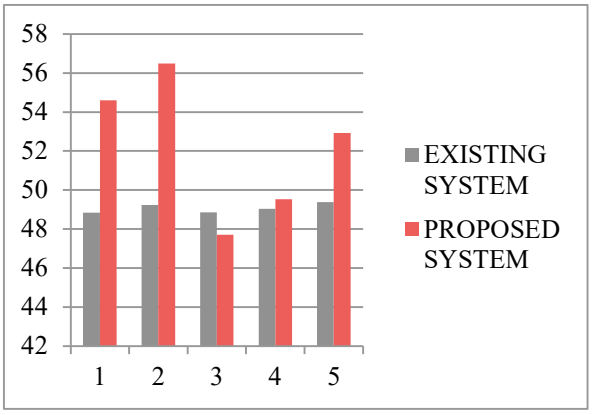

Fig. 9. Graph of cover image PSNR after embedding

Here, Table 2 shows PSNR difference of existing system and proposed system after embedding data image into host image. As per table 2 proposed system's PSNR is higher because in embedding process alpha blending method is used and existing system uses Arnold map. Proposed system gives PSNR around 52 Db where existing system gives PSNR around 49 Db. And figure 9 shows graphical representation of the given difference.

Table 3. PSNR of data image after rotation attack

NO.	IMAGE	DATA	EXISTING System[1]	PROPOSED System	EXISTING System[1]	PROPOSED System
1		A			59.82	64.9
2		C			67.35	70.27
3		D			57.71	54.16
4		B			61.75	57.00
5		M			55.46	63.60
	Average PSNR				60.41 Db	61.98 Db

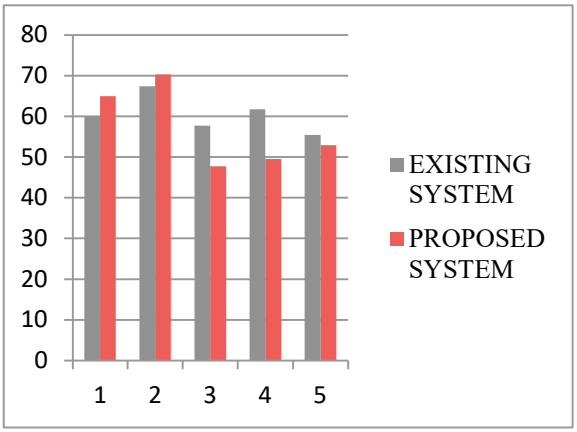

Fig. 10. PSNR of data image after rotation attack Graph

In table 3 results are shown of extracted data after rotation attack. Proposed system uses SVD to reduce noise in attacked image, Median filtering to preserve sharp edges of image, and Pseudo Zernike Moment to recover from rotation attack. Hence, proposed system gives higher PSNR than existing systems and there is visible difference of extracted data in proposed system and existing system. Figure 10 shows graphical representation of table 2.

Table 4. PSNR of data image after Noise attack

NO.	IMAGE	DATA	EXISTING System[1]	PROPOSED System	EXISTING System[1]	PROPOSED System
1		A			53.2	65.16
2		C			53.43	69.63
3		D			54.01	54.21
4		B			52.65	56.97
5		M			53.52	63.92
	Average PSNR				53.36 Db	61.97 Db

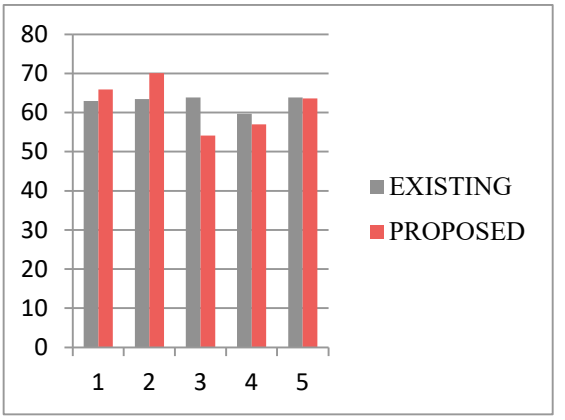

Fig. 11. PSNR of data image after Noise attack Graph

In table 4 results are shown of extracted data after noise attack. Proposed system gives higher PSNR than existing systems and there is visible difference of extracted data in proposed system and existing system. Figure 11 shows graphical representation of table 2.

Table 5. PSNR of data image after Rotation + Noise attack

NO.	IMAGE	DATA	EXISTING System[1]	PROPOSED System
1		A	Not recovered	66.22
2		C	Not recovered	70.63
3		D	Not recovered	54.23
4		B	Not recovered	57.29
5		M	Not recovered	63.72
	Average PSNR			62.41 Db

Table 6. PSNR of data image after Rotation + Translation attack

NO.	IMAGE	DATA	Attacked Image	Recovered Data	EMBEDDING	EXTRACTION
1		A			54.60	65.44
2		C			56.49	69.63
3		D			49.7	54.22
4		B			49.52	57.22
5		M			52.93	63.57
	Average PSNR				52.64 Db	62.01 Db

Table 5 shows PSNR after Rotation + noise attack on host image as image is rotated first and then noises like Salt and pepper, Gaussian, speckle, and poison is added to host image to try and distort data. Existing system only recover images from single attacks and cannot retrieve image from dual attacks. Proposed system recovers host image from dual attacks and gives data image as result. PSNR ratio of proposed approach is 62.41 dB.

Table 6 shows PSNR after Rotation + Translation attacks on image as first rotation is applied on image first and then image will be translated. Though existing systems do not recover images from dual attacks proposed system's PSNR is around 62.01 dB.

Table 7. Different Alpha blending

NO.	COVER IMAGE	DATA IMAGE	ALPHA VALUE	EXCTRACTED DATA	EMBEDDING	EXTRACTION
1			0.10		57.32 ↑	56.30 ↓
2			0.15		54.25 ↓	51.15 ↓
3			0.20		54.13 ↓	54.25 ↓
4			0.25		55.39 ↓	59.97 ↓
5			0.30		56.48 ↑	67.91 ↓
6			0.32		56.06	71.03
7			0.40		54.72 ↓	64.04 ↓

Table 8. Different sized data hiding

COVER IMAGE	DATA IMAGE	COVER IMAGE SIZE	DATA SIZE	EXCTRACTED DATA	EMBEDDING	EXTRACTION
			128 x 128		55.43 ↓	56.41 ↓
		1024 x 1024	64 x 64		56.49	71.03
			32 x 32	ERROR	NA	NA
			128 x 128		48.58 ↓	55.13 ↓
		512 x 512	64 x 64		48.49 ↓	54.01 ↓
			32 x 32		48.89 ↓	56.50 ↓

Table 7 shows different results after embedding different alpha values into the image. We can see best results at 0.32 alpha values. From minimum alpha value embedding PSNR is higher but at time of Extraction PSNR ratio goes down. As we increase alpha value best results are only at 0.32. Even after this value PSNR of embedding and extraction is lower.

In table 8 result analysis is shown of different sized cover image and data images. We can get best results at 1024*1024 cover images and 64*64 data image. Because we are using 2D-DWT hence it will divide the image into 4 parts twice like, 1024/4=256 and 256/4=64. Other sizes may exceed matrices after dividing into 4 parts. Another possible size combination is 512*512 cover image and 32*32 data image. But this combination does not give better results compared to 1024*1024.

Table 9. Different Gaussian noise value

NO.	DATA IMAGE	COVER IMAGE	ALPHA VALUE	EXCTRACTED DATA	EMBEDDING	EXTRACTION
1			0.01		54.60	79.96
2			0.05		51.21	78.23
3			0.10		51.21	77.28
4			0.50		51.21	77.26
5			0.60	ERROR	51.21	ERROR

Table 10. Different salt and pepper noise value

NO.	DATA IMAGE	COVER IMAGE	ALPHA VALUE	EXCTRACTED DATA	EMBEDDING	EXTRACTION
1			0.01		51.21	78.23
2			0.05		51.21	76.47
3			0.10		51.21	75.22
4			0.50		51.21	78.23
5			0.60	ERROR	51.21	ERROR

Table 9, 10 shows different intensity of Gaussian noise and salt and pepper noise respectively. We can see that from minimum value of noise to maximum up to 0.50 values proposed system recovers cover image as well as data image with accurate PSNR values. After 0.50 intensity of noise, system cannot recover data and cover image as at maximum intensity it changes all the pixel values of image and makes it impossible to recover data.

4. Conclusion

Proposed system concludes that the dual approach of "Block DWT-SVD-DCT" as well as "Pseudo Zernike Moment" and "median filtering" for Recovery of Attacks and "alpha blending" method for embedding data increases system privacy and robustness for recovered image. The proposed system will provide efficient Privacy Preserving Communication in the Traditional Systems using alpha blending method and Pseudo Zernike Moment. So implementation of proposed system will prevent dual attacks on images and recover original cover image as well as data image. Proposed system aimed and gained PSNR more than 50 dB where as in existing systems PSNR is up to 40 dB. In future proposed system may give higher PSNR and Lower MSE ratio and as per the results of proposed system there is drop of PSNR value in the image having blue color as major color so, may recover data efficiently from images having blue color as major color.

5. References

[1] S. cheng Han, J. feng Yang, R. Wang, and G. min Jia, "A robust color image watermarking algorithm against rotation attacks," *Optoelectron. Lett.*, vol. 14, no. 1, pp. 61–66, 2018.

[2] S. D. Degadwala and S. Gaur, "A study of privacy preserving system based on progressive VCS and RST attacks," *Proc. - Int. Conf. Glob. Trends Signal Process. Inf. Comput. Commun. ICGTSPICC 2016*, pp. 138–142, 2017.

[3] S. D. Degadwala and S. Gaur, "4-share VCS based image watermarking for dual RST attacks," *Lect. Notes Comput. Vis. Biomech.*, vol. 28, pp. 902–912, 2018.

[4] S. Kumar and A. Dutta, "A study on robustness of block entropy based digital image watermarking techniques with respect to various attacks," *2016 IEEE Int. Conf. Recent Trends Electron. Inf. Commun. Technol. RTEICT 2016 - Proc.*, pp. 1802–1806, 2017.

[5] S. D. Degadwala and S. Gaur, "An efficient privacy preserving system using VCS, block DWT-SVD and modified zernike moment on RST attacks," *2017 Int. Conf. Algorithms, Methodol. Model. Appl. Emerg. Technol. ICAMMAET 2017*, vol. 2017-January, pp. 1–4, 2017.

[6] Z. Zhang, L. Wu, S. Xiao, and S. Gao, "Adaptive reversible image watermarking algorithm based on IWT and level set," *EURASIP J. Adv. Signal Process.*, vol. 2017, no. 1, 2017.

[7] R. Ahmed, M. M. Riaz, and A. Ghafoor, "Attack resistant watermarking technique based on fast curvelet transform and Robust Principal Component Analysis," *Multimed. Tools Appl.*, vol. 77, no. 8, pp. 9443–9453, 2018.

[8] E. Najafi, "A robust embedding and blind extraction of image watermarking based on discrete wavelet transform," *Math. Sci.*, vol. 11, no. 4, pp. 307–318, 2017.

[9] P. Jain and U. Ghanekar, "Robust watermarking technique for textured images," *Procedia Comput. Sci.*, vol. 125, no. 2009, pp. 179–186, 2018.

[10] M. Haribabu, C. H. Bindu, and K. V. Swamy, "A Secure & Invisible Image Watermarking Scheme Based on Wavelet Transform in HSI Color Space," *Procedia Comput. Sci.*, vol. 93, no. September, pp. 462–468,

2016.

[11] N. N. Hurrah, N. A. Loan, S. A. Parah, and J. A. Sheikh, "A transform domain based robust color image watermarking scheme for single and dual attacks," *2017 4th Int. Conf. Image Inf. Process. ICIIP 2017*, vol. 2018-January, pp. 21–25, 2018.

[12] D. Image, P. Instructor, M. S. Submitted, A. Goswami, and C. Engineering, "INTRODUCTION TO DIGITAL WATERMARKS AND CLASSIFICATION OF ATTACKS ESE558 DIGITAL IMAGE PROCESSING Instructor: Dr. Murali Subbarao," no. 105209898, pp. 1–13.

[13] Z. Teng, X. F. Qiu, and J. W. Liu, "A New Robust Color Image Watermarking Based on DWT and DRT," *Appl. Mech. Mater.*, vol. 278–280, pp. 1366–1373, 2013.

[14] O. Abodena, M. Agoyi, and E. Celebi, "Hybrid technique for robust image watermarking using discrete time fourier transform," *2017 25th Signal Process. Commun. Appl. Conf. SIU 2017*, pp. 1–4, 2017.

[15] L. Tian, "A zero-watermarking method to protect intellectual property under strong geometric attacks," *Proc. - 2017 2nd Int. Conf. Multimed. Image Process. ICMIP 2017*, vol. 2017-January, no. 1, pp. 172–176, 2017.

[16] C. Preet and R. K. Aggarwal, "Multiple image watermarking using LWT, DCT and arnold transformation," *Proc. - Int. Conf. Trends Electron. Informatics, ICEI 2017*, vol. 2018-January, pp. 158–162, 2018.

[17] M. Boreiry and M. R. Keyvanpour, "Classification of watermarking methods based on watermarking approaches," *7th Conf. Artif. Intell. Robot. IRANOPEN 2017*, pp. 73–76, 2017.

[18] W. H. S. Wang, "A Robust Watermarking Algorithm Based on Histogram," *IWISA), 2009 Int. Work.*, no. Iwisa, pp. 453–456, 2009.

[19] S. Agarwal, Priyanka, and U. Pal, "Different Types of Attack in Image Watermarking including 2D, 3D Images," *Int. J. Sci. Eng. Res.*, vol. 6, no. 1, pp. 841–845, 2015.

[20] R. Murali, S. Saravanakumar, B. S. Parthasarathi, and G. Subramaniam, "A Review of Smart Grid Technology Transmission and Distribution," *Int. J. Innov. Res. Electr. Electron. Instrum. Control Eng.*, vol. 3, no. 1, pp. 86–89, 2015.

[21] A. Aggarwal and M. Singla, "Image Watermarking Techniques in Spatial Domain : A Review," vol. 2, no. 5, pp. 1357–1363, 2011.

[22] V. Licks and R. Jordan, "Geometric attacks on image watermarking systems," *IEEE Multimed.*, vol. 12, no. 3, pp. 68–78, 2005.

[23] M. Patel, Swati, and A. Chauhan, "The study of various attacks on Digital watermarking technique," *Int. J. Adv. Res. Comput. Eng. Technol.*, vol. 3, no. 5, pp. 1567–1570, 2014.

[24] M. Thapa, S. K. Sood, and A. . M. Sharma, "Digital Image Watermarking Technique Based on Different Attacks," *IJACSA Int. J. Adv. Comput. Sci. Appl.*, vol. 2, no. 4, pp. 14–19, 2011.

[25] P. R. Reddy, M. V. N. K. Prasad, and D. S. Rao, "Robust Digital Watermarking of Color Images under Noise attacks," *Int. J. Recent Trends Eng.*, vol. 1, no. 1, pp. 334–338, 2009.