Indian Journal of Science and Technology, *Vol 11(32), DOI: 10.17485/ijst/2018/v11i32/126951,* August 2018
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

IS-BRW: Image Security using Blind Reverse Watermarking with Various Attacks

K. J. Kavitha[1*] and B. Priestly Shan[2]

[1]Jain Institute of Technology, Davangere and Department of CSE Sathyabama University, Chennai - 600119, Tamil Nadu India; kavithakj219@gmail.com
[2]Eranad Knowledge City-Technical Campus, Manjeri – 676122, Kerala, India; priestlyshan@gmail.com

Abstract

Objective: In the advanced digital world, images are widely transmitted in many applications including health care. Robust blind watermarking is implemented for digital image content security and confidentiality. **Statistical Analysis:** The existing mechanism requires new benchmarking performance metric along with its response to the various attacks on digitally watermarked images. The proposed evaluation framework for image security using blind watermarking namely IS-BRW takes cover image along with secret image of varying resolution by applying different level of Fast Fourier Transformation (FFT) as well frequency, time, and wavelet transformation. The method adopts varying data embedding size of the watermark image. **Findings:** The efficiency of the IS-BW is estimated by measuring Peak-to-Signal-to-Noise (PSNR), Correlation Coefficient (CCR) and Bit Error Ratio (BER). A comparative analysis is done for various attacks which include JPEG compression, Median filter, Wiener filter, Gaussian filter, Image cropping, Image rotation and Image resize. The metric parameters evaluated before and after various attacks do not changes and it remains same which shows the efficiency of the proposed algorithm with other existing systems. **Applications:** The proposed system is more suitable in the healthcare system where it involves the transmission of scanned medical images over the internet which strictly prohibits the modifications.

Keywords: Digital Watermarking For Images, Image Security, Wavelet Transformation, Watermarking Attacks

1. Introduction

The distribution of multimedia content such as audio, video, image etc., through different communication channel from the various applications is possible seamlessly with advance communication and network system. Regulations have been made to safeguard the intellectual property rights on these multimedia contents[1]. The research in digital watermarking too aims for providing protection to the image or videos[2]. Rigorous research is required to evolve new performance metric for the benchmarking algorithms along with its effectiveness under varied attacks[3]. The watermark shall be inserted into the images in such a way that it should not be noticeable, whereas the copyright owner can easily find its presence by the use of private key[4]. Many recent contributions in the field of digital watermarking algorithm for images have been mentioned in the work[5–18]. Quite obviously these methods shall be resistive enough against attack performed on watermark images. Few well known attacks include: Geometric attack, Inversion attack, D-Synchronization attack and Estimation attack etc. Recently many literatures have been found towards algorithms for image watermarking to counterfeit the effect of watermark attacks[19–25]. The typical classification of image watermark includes Perceptual and non-Perceptual watermarking technique. Based on the processing mechanism it can be divided into spatial and transform domain[26]. The patterns can be directly identified if the watermark technique is of non-blind. The watermark image is general-

*Author for correspondence

lyhidden into the lowestweighted bit of the cover/original image if the approach followed is of type spatial or non-blind approach[27--31]. In past; these methods were improvised to exhibit better performance against the effect of filtering and compression[32–34]. Irrespective of simple implementation and low computational complexity, the spatial based watermarking having bit capacity and less robust to image compression. These kinds of watermark can be easily removed by cropping[35]. For the optimization of embedding capacity, transform methods are evolved. This method is optimized for robustness to sustain the effect of many attacks including noise, Gaussian filter and compression etc.

The existing research on watermarking uses self-designed assessment mechanism on the consideration of various attacks on the images[36]. Further to meet the goal of optimal watermarking methods various transformation methods have been used such as Curve let Transformation (CT)[37], Arnoldtransformation[38], Discrete Wavelet Transform (DWT)[39], along with Discreet Cosine and Fast Fourier Transformations (DCT, FFT)[40,41].

The current trend in watermarking adopts a joint and hybrid method of spatial-temporal as space and frequency domain. The work done in this direction includes some of the significant work such as space-time coding for water making colour image[42], space-time block coding by Irene[43]. The limitations found these approaches that watermarked image non-sustainable to the signal processing attacks[44]. To encounter this problem, gray image watermarking was adopted which sustain some of the attacks of compression with balance compression ratio[45]. The adoptable watermarking method need to be robust against most of the attacks, shall attain optimal visual perception after reconstruction and should be non-blind in nature. This paper introduces a novel evaluation framework namely IS-BRW with the objective of achieving optimal embedding capacity with constant visual perception against most of the attacks.

The recent trend of digital watermarking algorithms from[5–18] is discussed in this section and come to the conclusion that the major trade-off between imperceptibility and robustness is the key for image watermarking research.

In the conventional method[5], a watermarking method is proposed to sustain it from three kinds of attacks, which includes i) Random-Bending (RB-attack), ii) Cropping attack and 3) Other general attacks. Gaussian filter is used for pre-processing while embedding. They have exploited a unique secret key for grey level selection by histogram. The robustness is achieved by combined effect of indexing and modifying the high frequency component. Though this is an appropriate attempt towards Image Watermarking Technique (IWT), but lacks benchmarking performance metric to validate the method. In contrast to the conventional method of histogram-shifting for the purpose of separating marked and un-marked pixel and achieving optimal image quality along with higher embedding capacity, a reversible watermarking was proposed which includes an error predictive method[6].

Image transmission is widely used in the field of advanced medical science field. The work proposed by. uses a system of medical image consistency,validation by wavelet transformation watermarking (WTW) and this work is based on integer wavelet transformation in order to avoidwrong diagnoses[7]. In this work, it is been said that the efficiency of watermarking depends on the efficiency of decomposition.

Many other approaches used Discrete Cosine Transformation (DCT), Krawtchouk Transformation (FrkT) and Quantum Cosine Transformation (QCT) with blocking operations in order to achieve effective embedding in the process of watermarking[11–13].

In the proposed a blind imagewatermarking technique based on Hessenberg decomposition and is evaluated for various attacks[14].

A visual attention oriented watermarking technique in Wavelet transform domain and its performance is evaluated under both blind and non-blind system. This system provides 25-40% of improvement against JPEG 2000 and filtering attacks[15].

A Firefly algorithm along with Discrete Wavelet Transform (DWT) along with QR- codes to enhance the computation capability andestimated Structural Similarity Index Measure (SSIM) and Bit Error Rate (BER) and found the trade-off between image quality and strength[16] and a similar objective was proposed by a system using Curve Let Transform domain [CT][17]. One of the very effective method using fractal encoding and DCT was proposed which uses a double encryption to improve over conventional DCT method and found sustainable to various attacks to maintain its optimality between strength and PSNR[18].

2. IS-BRW: System Model

The proposed IS-BRW algorithm is used to perform blind reverse watermarking for gray image. The original cover image (DIcover) is digitized and resized to get gray scale Input Cover image (IC). The watermark logo (Is) at varying logo resolution (Rl) is converted to binarywith threshold value '1'. The 1st and 2nd order of FFT is set between a range of 0 and 1 before applying transform domain. Then the input Cover Image ICis applied with Discrete Fractional Fourier transformation (DFFT) with an angle obtain as a power (P) by concatenating 1st and 2nd value of the range to get the transform coefficient (S). The Figure 1 shows the outcome of the above three processes.

The transformed coefficient (S) is applied with Wavelet packet transform to decompose in order to get wavelet tree (T). The four-wavelet coefficients are obtained as: Approximation (A), horizontal (H), vertical (V), and diagonal (D) and are computed for the wavelet tree (T). These processed coefficients are copied to the processor memory block (t) and later reconstruction process will be performed to get final wavelet packet coefficient (X).

Then DFFT is performed on X which results in angle -P and we get the reference image (I_R). This reference image is separated in to real (I_{RR}) and imaginary ((I_{RI}) part. Then the real part of the image is defined into n×n block and the secret watermark image (Is) is bipolarized and in each block information is hidden and finally added with the imaginary part I_{RI} to get watermarked Image (I_{EL}). The Figure 2 shows the images of X, I_R, $I_{wmi.}$

Further watermarked frequency (F-I_{EL}) of X is obtained by FFFT. Wavelet packet decomposition for X is done to get an individual coefficient [A, H, V, D] to obtain final wavelet coefficient as inverse wavelet tree (T').

Further IFFFT is applied on transformed coefficient S to get inverse fraction of original cover image (I_{CI}) and for this image, PSNR is computed which will be considered as threshold shown in Figure 3. If the same PSNR is maintained against different attacks then this technique is called robust and optimal for both visual perception and security.

The watermarked image is applied with various noise type of no attack, No Attack, JPEG compression, Median Filter, Wiener Filter, Gaussian Filter, Image Cropping,

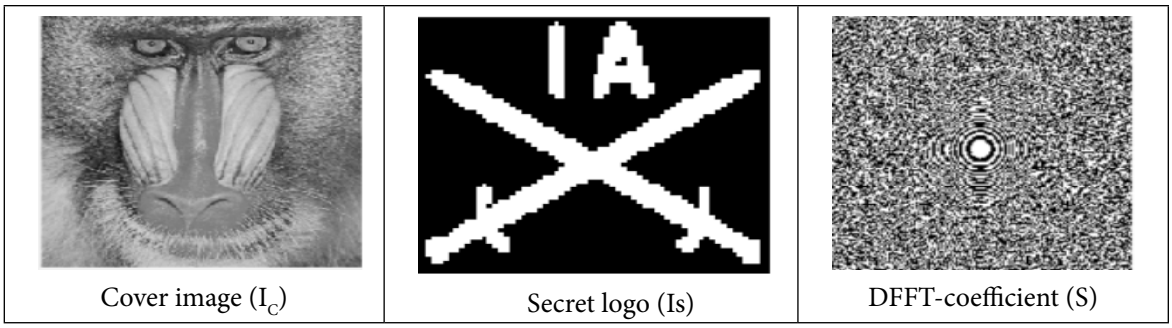

Figure 1. Cover image (I_C), watermark logo (Is) and DFFT-coefficient (S).

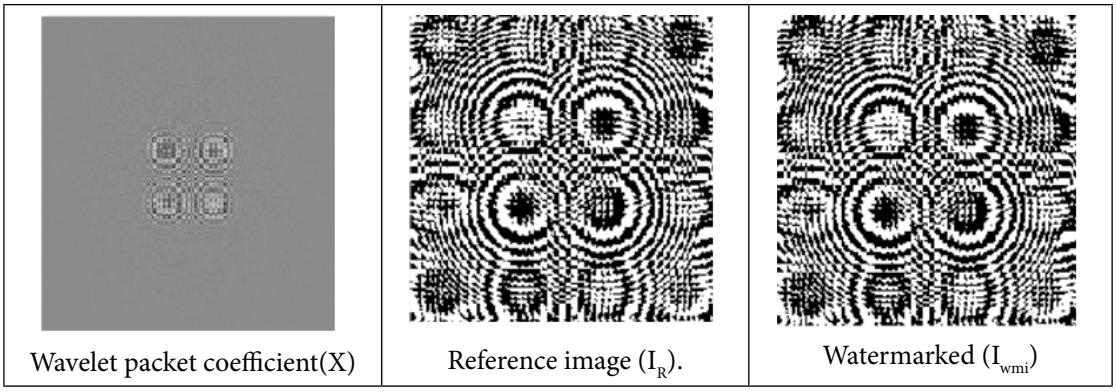

Figure 2. Wavelet packet coefficient(X), Reference image (I_R), Watermarked (I_{wmi}).

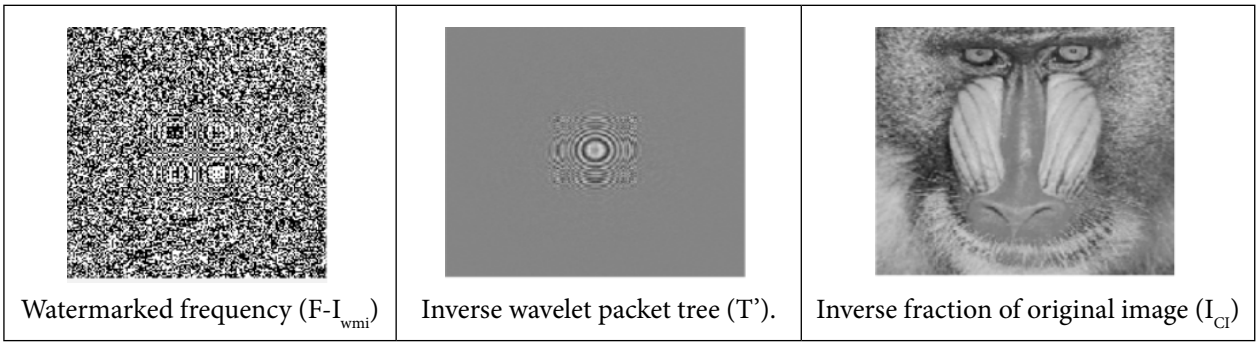

Figure 3. Visual perception of Watermarked frequency (F-I$_{wmi}$), Inverse wavelet packet tree (T'), Inverse fraction of original cover image (I$_{CI}$).

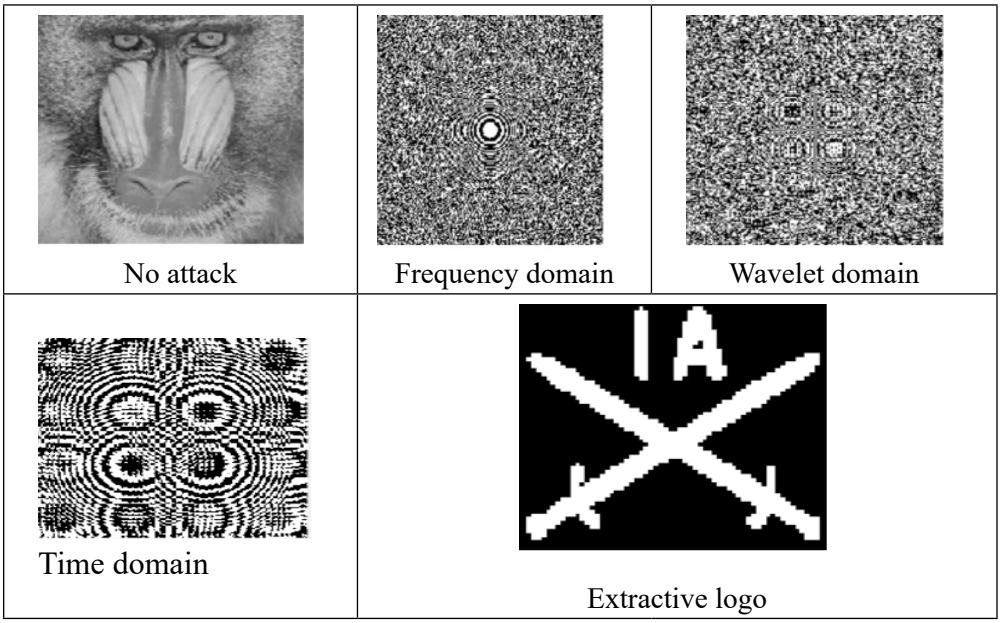

Figure 4. No attack, Frequency domain, Wavelet domain, Time domain, extractive logo.

Image Rotation, Image resize with respective variables of noise parameter. At the extraction side frequency, wavelet and time domain processes is applied and finally embedded watermark image isextracted. The value of PSNR, correlated coefficient and BER is computed for respective attacks and the performance graph for each attack is shown in section 5. (Figure 4) displays the inverse process.

3. IS-BRW: Algorithm

This section explains abstractive form of pseudo language to describe the entire IS-BRW system model in algorithmic format. The operation carried out by the proposed system at both frequency and time domain for the obtained image is as shown. The algorithm initially takes the input as the cover image which has to be protected using a confidential image. For better scalability, the system offers different dimensionality of the confidential image i.e., 16x16, 32x32, 64x64, and 128x128. The confidential image is then binarized followed by embedding process for image security. For this purpose, the first and second order of Fast Fourier Transform is considered followed by extraction of transform domain of the image. The outcome image is than subjected to the wavelet transformation that is further followed by extraction of time domain of information. The proposed system also retains flexibility to offer intensity of embedding considering different scales of it. This process is resumed with finally embedding the confidential image. Similar process of

extraction of frequency domain, wavelet transform, and time domain is continued in order to finally secure the cover image. The significant steps of the proposed algorithm are as follows:

IS-BW: Overall algorithm for watermarking process

$I_C \leftarrow f(DI_{cover})$

$Is \leftarrow f(Is, R_1)$

If Is ≠binary

Is(binary)

End

$S \leftarrow f_{DFFT}(I_{C,} P)$

$T \leftarrow f_{WPD}(S)$

$[A, H, V, D] \leftarrow f_{WPC}(T)$

$T \leftarrow f_{PMB}([A, H, V, D])$

$X \leftarrow r_{econstruction}(t)$

$I_R \leftarrow f_{DFFT}(X_{,-}P)$

$[I_{RR,} I_{RI}] \leftarrow f(I_R)$

$Block \leftarrow f(I_{RR,}n,n)$

$I_{EL} \leftarrow (Block \Theta Is)+I_{RI}$

$F\text{-}I_{EL} \leftarrow f_{DFFT}(X)$

$T' \leftarrow [A, H, V,P] \leftarrow f_{WTD}(X)$

The proposed algorithm considers the presence of different types of noise along with related attributes. Theproposed algorithm offers resistance from security threats and also ensures good quality from noise related parameters.

4. Evaluation of the Proposed Algorithm against Various Attacks and its Performance

The usual evaluation performance parameter of watermarking algorithm are[46–53]:

- Imperceptibility
- Capacity
- Safety
- Strength
- Compression
- JPEG Compression
- Median filter
- Wiener filter
- Gaussian filter
- Image cropping
- Image rotation
- Image resize

5. Results and Discussion

This section discusses the results proposed algorithm. The analysis of the algorithm is done on various parameters like Normalized Correlation Coefficient (CC), Bit Error Rate (BER) and PSNR for varying alpha and is evaluated for eight different attacks. The JPEG compression performance is shown in Figure 5-10 the possible impact on change of any parameters on the security.

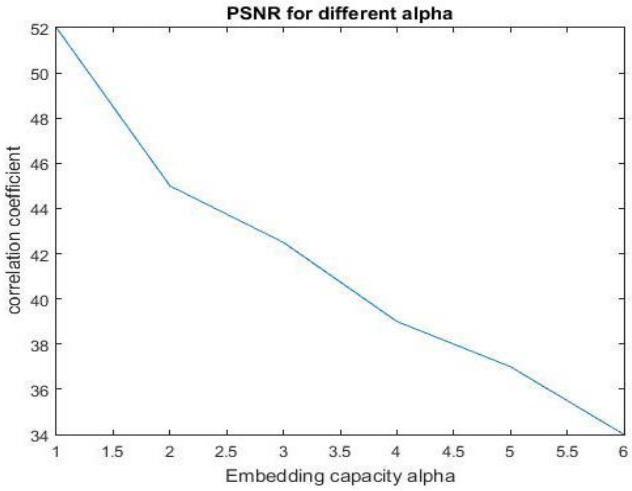

Figure 5. Correlation Coefficient for varying α value.

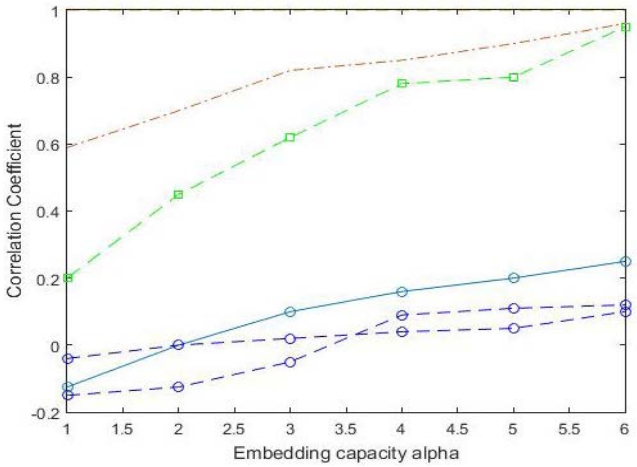

Figure 6. Correlation Coefficient for varying embedded intensity α.

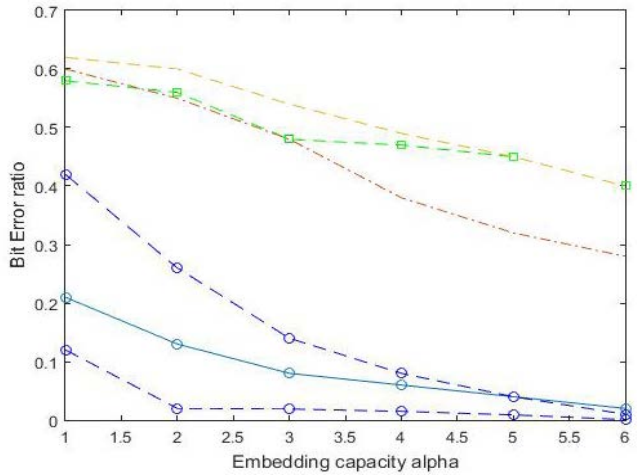

Figure 7. BER for varying embedded intensity α.

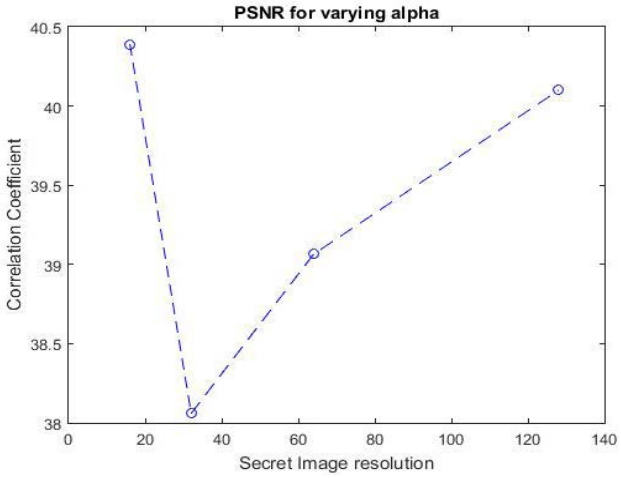

Figure 8. Correlation Coefficient for varying logo resolution.

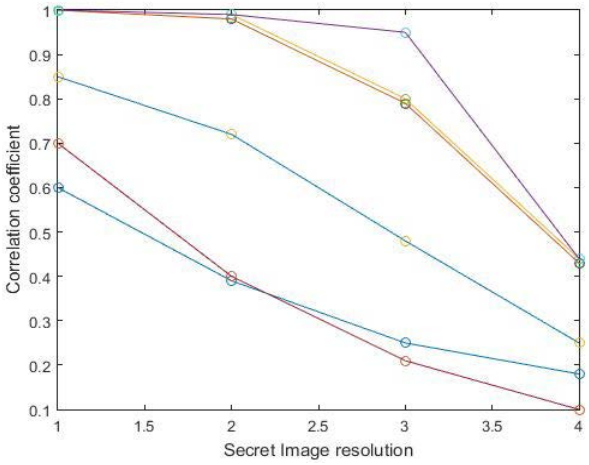

Figure 9. Correlation Coefficient for varying logo resolution.

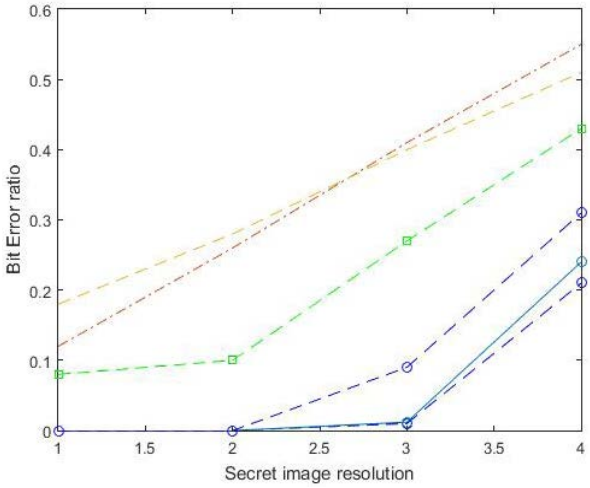

Figure 10. BER for varying logo resolution.

Figure 5-10 Analysis of Correlation Coefficient for JPEG compression for varying α.

The similar results are obtained for BER. This outcome is further confirmed by assigning some finite value of alpha as seen in next part of result analysis. Figure 11-22 shows analysis of various attacks like JPEG form of compression, Median filter; Weiner filter and Gaussian filter for metric parameters PSNR, Correlation Coefficient (CC) and Bit Error Rate (BER). PSNR values increases in accordance with the increased value of alpha (Figure11) whereas correlation coefficient decreases in correspond to the decreased value alpha as (Figure12). Similarly, BER is found to be high for less value of alpha (Figure13). The similar results are shown for median, wiener and Gaussian filters in the Figure 14-22.

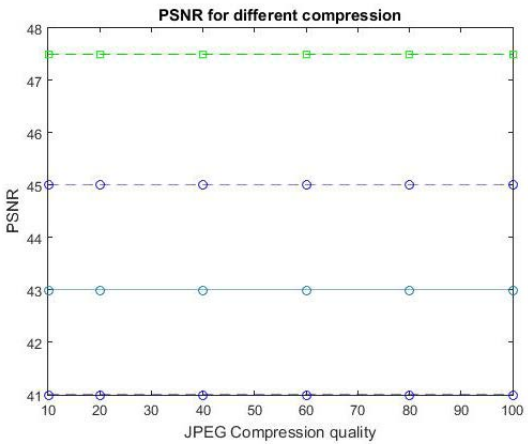

Figure 11. PSNR for JPEG compression at α = 1.5, 2, 2.5 and 3

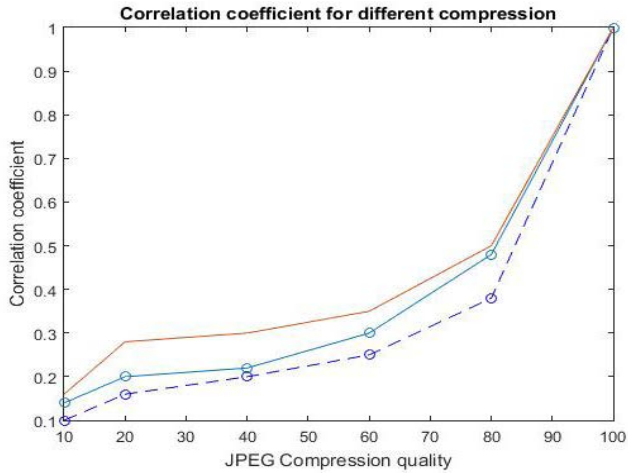

Figure 12. Correlation coefficient for JPEG compression at α = 1.5, 2, 2.5 and 3.

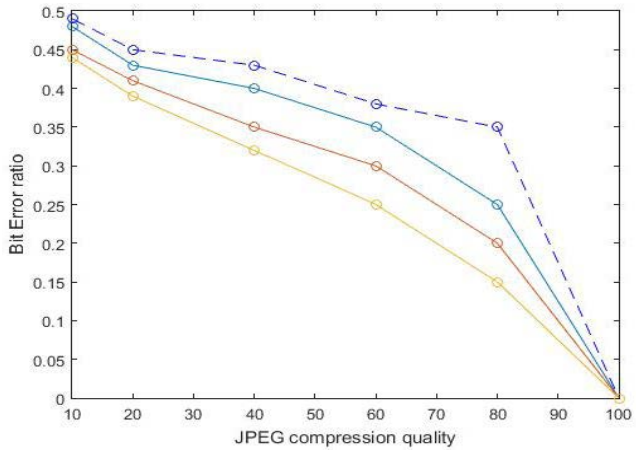

Figure 13. BER for JPEG compression at α = 1.5, 2, 2.5 and 3.

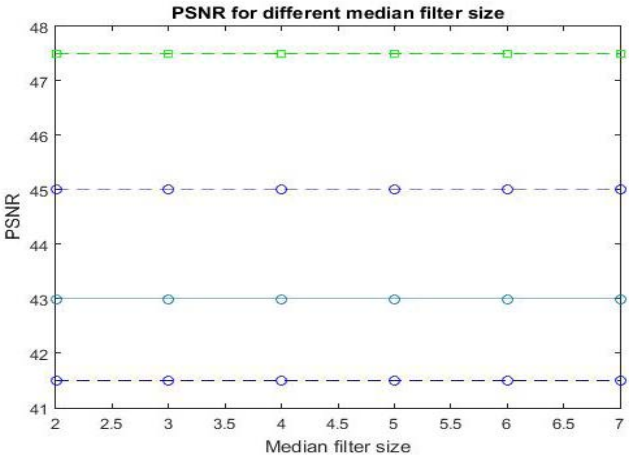

Figure 14. PSNR for Median filter at α = 1.5, 2, 2.5 and 3.

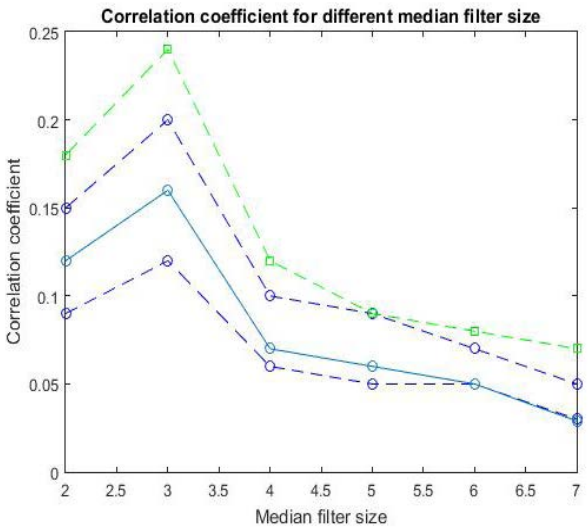

Figure 15. Correlation coefficient for Median filter at α = 1.5, 2, 2.5 and

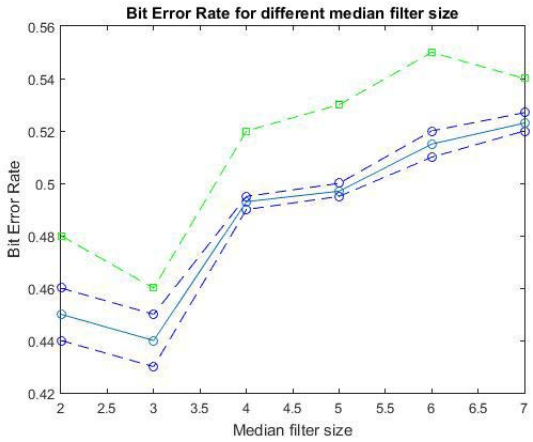

Figure 16. BER for Median filter at α = 1.5, 2, 2.5 and 3.

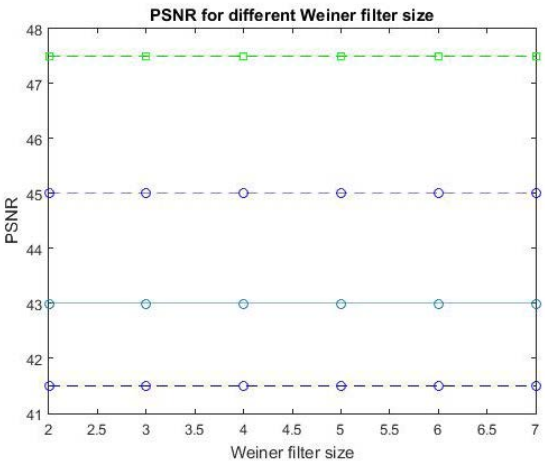

Figure 17. PSNR for Wiener filter at α = 1.5, 2, 2.5 and 3.

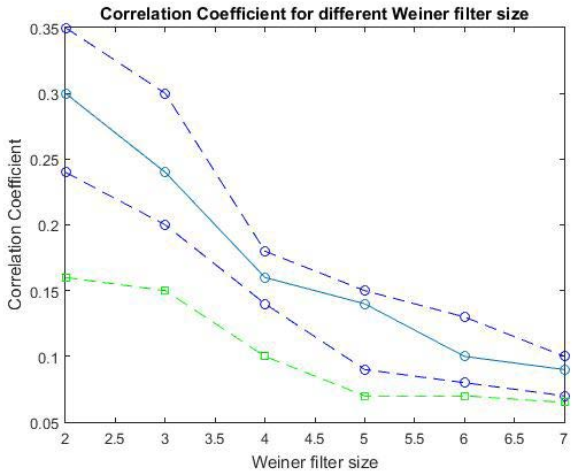

Figure 18. Correlation coefficient for Wiener filter at α = 1.5, 2, 2.5 and 3.

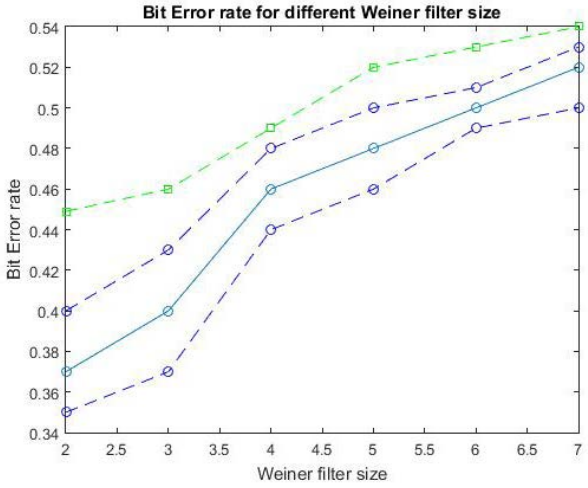

Figure 19. BER for Wiener filter at α = 1.5, 2, 2.5 and 3.

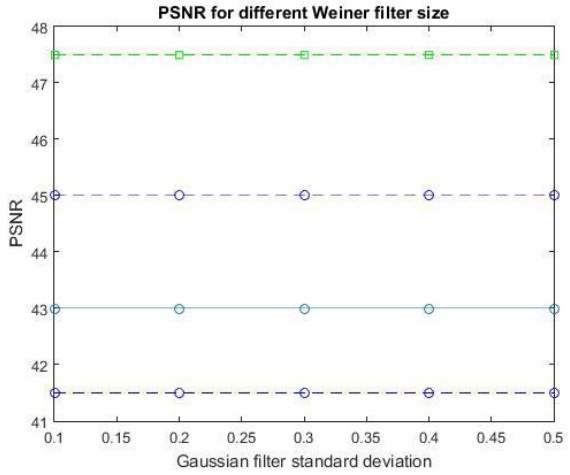

Figure 20. PSNR for Gaussian filter at α = 1.5, 2, 2.5 and 3.

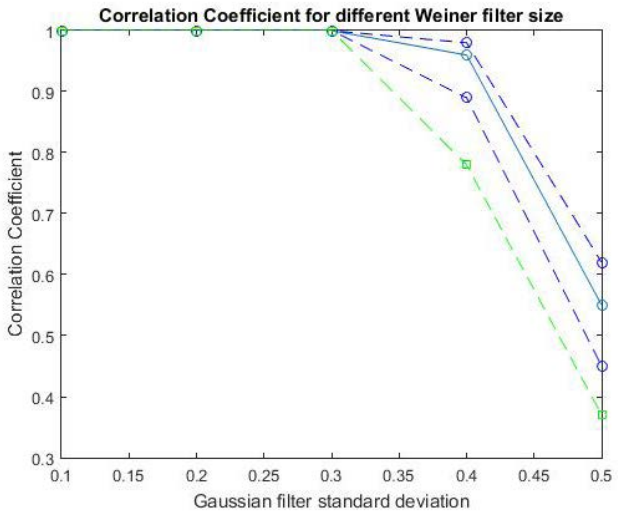

Figure 21. Correlation coefficient for Gaussian filter at α = 1.5, 2, 2.5 and 3.

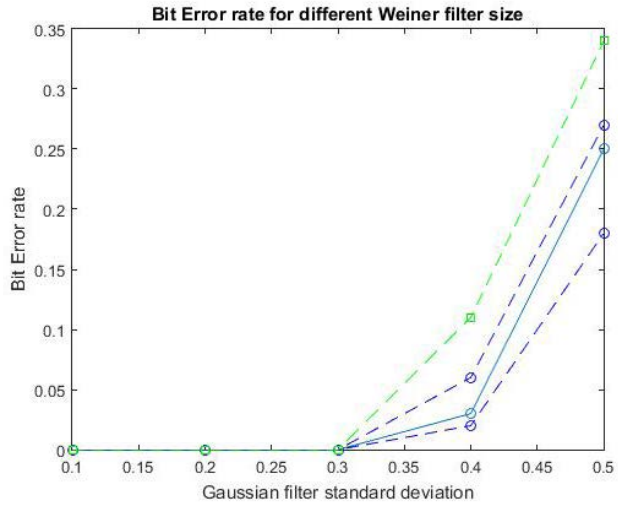

Figure 22. BER for Gaussian filter at α = 1.5, 2, 2.5 and 3.

Figure11-22 Evaluation of the proposed algorithm against various attacks with quality metrics PSNR, CC and BER.

A slightly different performance is observed for Median filter forCC and BER as compared to JPEG. In this case, CC is observed to be minimized while BER is observed to be maximized with increasing size of median filter unlikely that of JPEG compression quality. Theeffect of Weiner filter is nearly same when observed using median filter. Figure 23-31 shows the impact of Geometric attacks; image cropping (Figure 23-25), image rotation (Figure 26-28), image resize (Figure 29-31), and usage of Gaussian filter over same performance parameters. It can

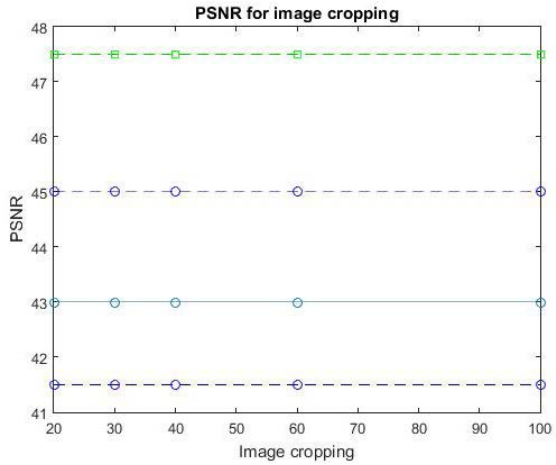

Figure 23. PSNR for Image cropping at α = 1.5, 2, 2.5 and 3.

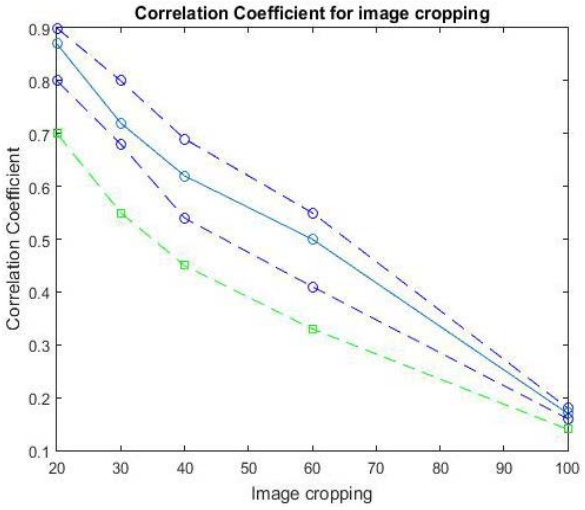

Figure 24. Correlation Coefficient for Image cropping at α = 1.5, 2, 2.5 and 3.

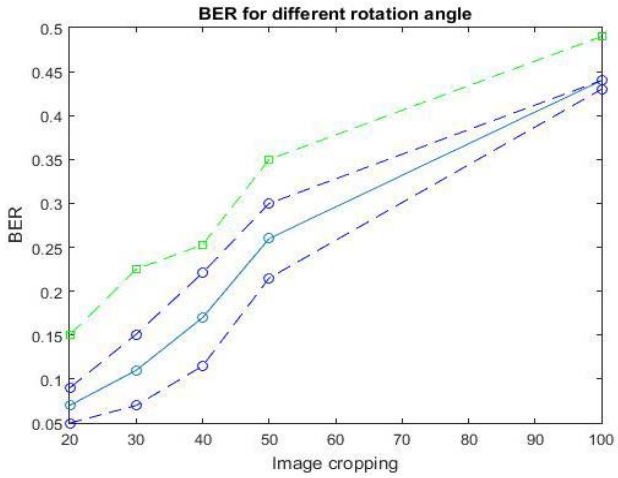

Figure 25. BER for Image cropping at α = 1.5, 2, 2.5 and 3.

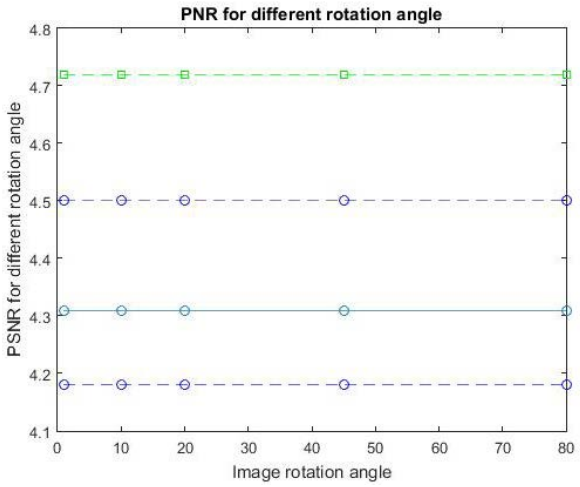

Figure 26. PSNR for Image rotation at α = 1.5, 2, 2.5 and 3.

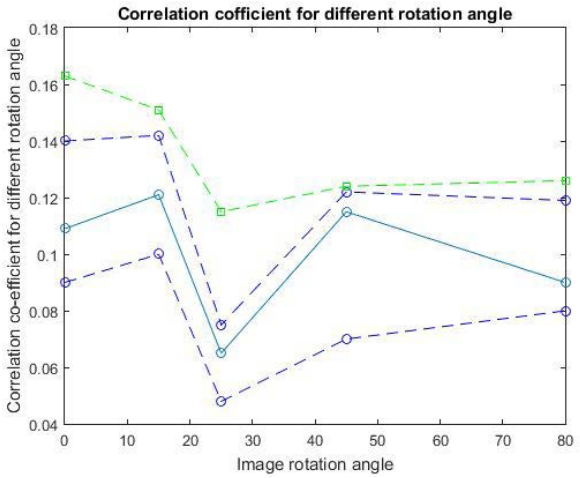

Figure 27. Correlation Coefficient for Image rotation at α = 1.5, 2, 2.5 and 3

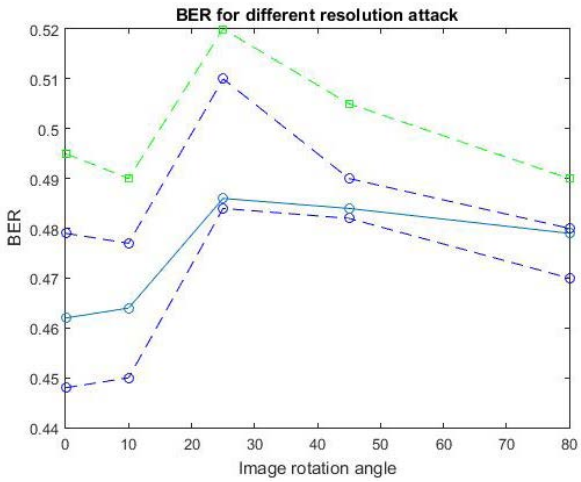

Figure 28. BER for Image rotation at α = 1.5, 2, 2.5 and 3.

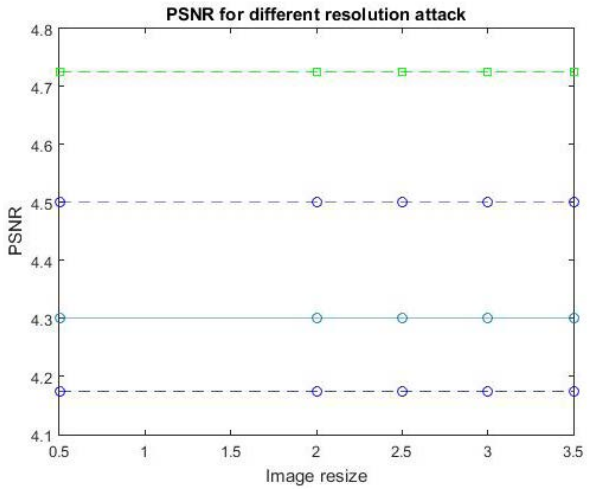

Figure 29. PSNR for Image resize at α = 1.5, 2, 2.5 and 3.

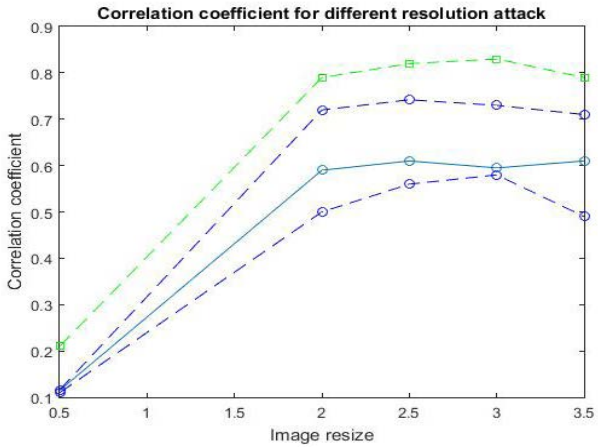

Figure 30. Correlation coefficient for Image resize at α = 1.5, 2, 2.5 and 3.

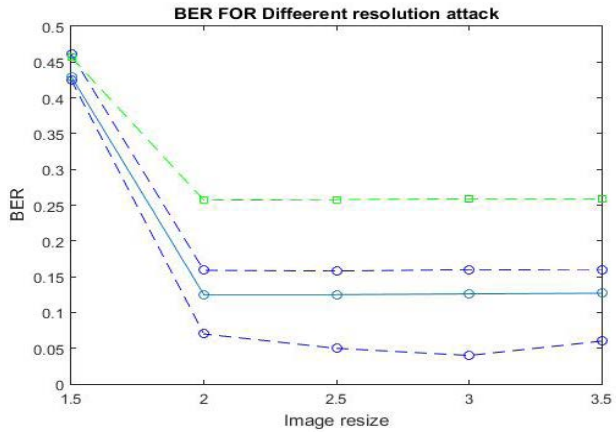

Figure 31. BER for Image resize at α = 1.5, 2, 2.5 and 3.

Figure 23-31. Analysis of PSNR, CC and BER for Geometric attacks with varying α.

be seen that correlation coefficient and bit error rate are quite unique while PSNR has absolutely no change.

6. Conclusion

The watermarking techniques are very useful in the applications of confidential video conferencing, and many such other applications. The proposed algorithm is a simple methodology of securing image using a cost effective technique. With a discrete value of CC and BER, the algorithm shows that there is a unique attack pattern which can be successfully identified and captured. At the same time, the proposed algorithm doesn't use any form of encryption technique which makes it further simple algorithm by itself. Our future work will be further optimizing the present approach.

7. References

1. Podilchuk CI. Digital watermarking: algorithms and applications. IEEE Signal Processing Magazine. 2001 July;18(4):33–46. https://doi.org/10.1109/79.939835
2. Kundur D. Enabling security technologies for digital rights management. Proceedings of the IEEE. 2004Jun; 92(6):879–882. https://doi.org/10.1109/JPROC.2004.827336
3. MACQ B. Benchmarking of image watermarking algorithms for digital rights management. Proceedings of the IEEE. 2004 Jun; 92(6):971–84. https://doi.org/10.1109/JPROC.2004.827361
4. Lang J. Blind digital watermarking method in the fractional Fourier transform domain. Optics and Lasers in Engineering. 2014; 53:112–21. https://doi.org/10.1016/j.optlaseng.2013.08.021
5. Zong T. Robust histogram shape-based method for image watermarking. IEEE Transactions on Circuits and Systems for Video Technology. 2015 May; 25(5):717–29. https://doi.org/10.1109/TCSVT.2014.2363743
6. Siddiqa A. High capacity reversible image watermarking using error expansion and context-dependent embedding. Electronics Letters. 2015 Jun; 51(13):985–7. https://doi.org/10.1049/el.2015.0247
7. Eswaraiah R. Robust medical image watermarking technique for accurate detection of tampers inside region of interest and recovering original region of interest. IET Image Processing. 2015 Aug; 9(8):615–25. https://doi.org/10.1049/iet-ipr.2014.0986
8. Muhammad N. Digital image watermarking using partial pivoting lower and upper triangular decomposition into the wavelet domain. IET Image Processing. 2015 Sep; 9(9):795–803. https://doi.org/10.1049/iet-ipr.2014.0395

9. Andalibi M. Digital image watermarking via adaptive logo texturization. IEEE Transactions on Image Processing. 2015; 24(12):5060–73. https://doi.org/10.1109/TIP.2015.2476961 PMid:26353371
10. Makbol NM. Block-based discrete wavelet transform-singular value decomposition image watermarking scheme using human visual system characteristics. IET Image Processing. 2016 Jan; 10(1):34–52. https://doi.org/10.1049/iet-ipr.2014.0965
11. Zong, T. Rank-based image watermarking method with high embedding capacity and robustness. IEEE Access. 2016; 4:1689–99. https://doi.org/10.1109/ACCESS.2016.2556723
12. Wang S. Quantum cosine transform based watermarking scheme for quantum images. Chinese Journal of Electronics. 2015 Apr; 24(2):321–5. https://doi.org/10.1049/cje.2015.04.016
13. Liu X. Fractional krawtchouk transform with an application to image watermarking. IEEE Transactions on Signal Processing. 2017 Apr; 65(7):1894–908. https://doi.org/10.1109/TSP.2017.2652383
14. Su Q. Novel blind colour image watermarking technique using Hessen berg decomposition. IET Image Processing. 2016 Nov; 10(11):817–29. https://doi.org/10.1049/iet-ipr.2016.0048
15. Bhowmik D. Visual attention-based image watermarking. IEEE Access .2016; 4:8002–18. https://doi.org/10.1109/ACCESS.2016.2627241
16. Guo Y. Optimised blind image watermarking method based on firefly algorithm in DWT-QR transform domain. IET Image Processing. 2017 Jun; 11(6):406–15. https://doi.org/10.1049/iet-ipr.2016.0515
17. KimWH. Blind curvelet watermarking method for high-quality images. Electronics Letters. 2017 Sep; 53(19):1302–4. https://doi.org/10.1049/el.2017.0955
18. Liu S. Digital image watermarking method based on DCT and fractal encoding. IET Image Processing. 2017 Oct; 11(10):815–21. https://doi.org/10.1049/iet-ipr.2016.0862
19. Licks V. Geometric attacks on image watermarking systems. IEEE Multimedia. 2005Jul-Sep; 12(3):68–78. https://doi.org/10.1109/MMUL.2005.46
20. Wang S. A novel DIBR 3D image watermarking algorithm resist to geometrical attacks. Chinese Journal of Electronics. 2017; 26(6):1184–93. https://doi.org/10.1049/cje.2017.09.025
21. Vellaisamy S. Inversion attack resilient zero-watermarking scheme for medical image authentication. IET Image Processing. 2014 Dec; 8(12):718–27. https://doi.org/10.1049/iet-ipr.2013.0558
22. Wang X. A new digital image watermarking algorithm resilient to desynchronization attacks. IEEE Transactions on Information Forensics and Security. 2007 Dec; 2(4):655–63. https://doi.org/10.1109/TIFS.2007.908233
23. Lin CH. Histogram-oriented watermarking algorithm: Colour image watermarking scheme robust against geometric attacks and signal processing. IEEE Proceedings- Vision, Image and Signal Processing. 2006 Aug; 153(4):483–92.
24. Chun-Shien L. Media hash-dependent image watermarking resilient against both geometric attacks and estimation attacks based on false positive-oriented detection. IEEE Transactions on Multimedia.2006 Aug, 8(4), pp. 668-685. https://doi.org/10.1109/TMM.2006.876300
25. Agung IW.Method for combating random geometric attack on image watermarking. Electronics Letters. 2001 Mar; 37(7):420–1. https://doi.org/10.1049/el:20010277
26. Lang J. Blind digital watermarking method in the fractional Fourier transform domain. Optics and Lasers in Engineering. 2014; 53:112–21. https://doi.org/10.1016/j.optlaseng.2013.08.021
27. Qingtang S. Robust color image watermarking technique in the spatial domain. Soft Computing. 2018; 22(1):91–106. https://doi.org/10.1007/s00500-017-2489-7
28. Srivastava M. Digital watermarking using spatial domain and triple DES. 3rd International Conference on Computing for Sustainable Global Development; New Delhi. 2016. p. 3031–35.
29. Maity S. Robust and blind spatial watermarking in digital image. ICVGIP Proceedings of the 3rd Indian Conference on Computer Vision, Graphics and Image Processing; 2002.
30. Sarkar T. Digital watermarking techniques in spatial and frequency domain. ArXiv: 1406.2146; 2014.
31. Sebé F. Spatial-domain image watermarking robust against compression, filtering, cropping, and scaling. International Workshop on Information Security; 2000. p. 44–53. https://doi.org/10.1007/3-540-44456-4_4
32. Goos G. Information security. ISW: International Workshop on Information Security. Berlin, Heidelberg: Springer; 2000. https://doi.org/10.1007/3-540-44456-4
33. Nana Z. Watermarking algorithm of spatial domain image based on SVD. International Conference on Audio, Language and Image Processing (ICALIP); 2016. p. 361–5. https://doi.org/10.1109/ICALIP.2016.7846588
34. Alirezanejad M. Improving the performance of spatial domain image watermarking with high boost filter. Indian Journal of Science and Technology. 2014; 7(12):2133.
35. NikolaidisaI N, Pitasb I. Robust image watermarking in the spatial domain. Journal Signal Processing. 1998; 66(3):385–403. https://doi.org/10.1016/S0165-1684(98)00017-6
36. GoliMS. Introducing a new method robust against crop attack in digital image watermarking using two-step Sudoku. 3rd International Conference on Pattern

Recognition and Image Analysis (IPRIA); 2017. p. 237–42. https://doi.org/10.1109/PRIA.2017.7983054
37. Sujatha CN. Analysis of robust watermarking techniques: A retrospective. International Conference on Communication and Signal Processing (ICCSP); 2016. p. 0336–41. https://doi.org/10.1109/ICCSP.2016.7754151
38. Wang T. A novel scrambling digital image watermark algorithm based on double transform domains. Mathematical Problems in Engineering; 2015. p. 1–13. https://doi.org/10.1155/2015/281681
39. Zhang C. Digital image watermarking algorithm with double encryption by arnold transform and logistic. 4th International Conference on Networked Computing and Advanced Information Management; 2008. p. 329–34. https://doi.org/10.1109/NCM.2008.121
40. Malonia M. Digital Image watermarking using Discrete Wavelet Transform and Arithmetic Progression technique. 2016 IEEE Students' Conference on Electrical, Electronics and Computer Science (SCEECS); 2016. p. 1–6.
41. Chen WY. Digital watermarking using DCT transformation. Department of Electronic Engineering National ChinYi Institute of Technology; 2000.
42. Pun CM. A Novel DFT-based digital watermarking system for images. 8th international Conference on Signal Processing; 2006. p. 1–9.
43. Ashourian M. Using space-time coding for watermarking color images. International Conference Image Analysis and Recognition; 2006. p. 580–6. https://doi.org/10.1007/11867586_54
44. KarybaliI G. Improved embedding of multiplicative watermarks via space-time block coding. 13th European Signal Processing Conference; 2005. p. 1–4.
45. Stankovic S. Watermarking in the space/spatial-frequency domain using two-dimensional Radon-Wigner distribution. IEEE Transactions on Image Processing. 2001 Apr; 10(4):650–8. https://doi.org/10.1109/83.913599 PMid:18249654
46. Nguyen BP. Perceptual watermarking robust to JPEG compression attack. 5th International Symposium on Communications, Control and Signal Processing; 2012. p. 1–4. https://doi.org/10.1109/ISCCSP.2012.6217798
47. Lee JC. Analysis of attacks on common watermarking techniques. IEEE, Electrical and Computer Engineering; 2017. p. 1–7.
48. Song C. A spatial and frequency domain analysis of the effect of removal attacks on digital image watermarks. 11th of Post Graduate Network Symposium; 2010 Jun. p. 119–24.
49. Hiroshi I. A local Wiener attack for additive watermarks. IEEE 13th International Symposium on Consumer Electronics; 2009. p. 507–10. https://doi.org/10.1109/ISCE.2009.5156830
50. Samˇcovic A, et al. Attacks on digital wavelet image watermarks. Journal of Electrical Engineering. 2008; 59(3):131–8.
51. Lee JS. Self-recognized image protection technique that resists large-scale cropping. IEEE Multimedia. 2014 Jan-Mar; 21(1):60–73. https://doi.org/10.1109/MMUL.2014.14
52. Nini B. Security analysis of a three-dimensional rotation-based image encryption. IET Image Processing. 2015 Aug; 9(8):680–9. https://doi.org/10.1049/iet-ipr.2014.0702
53. Taherinia AH. A new watermarking attack based on content-aware image resizing. International Multimedia, Signal Processing and Communication Technologies. 2009; 177–80. https://doi.org/10.1109/MSPCT.2009.5164204