International Journal of Computer Trends and Technology
ISSN: 2231-2803 / https://doi.org/10.14445/22312803/IJCTT-V67I1P104

Volume 67 Issue 1, 16-25, January 2019
© 2019 Seventh Sense Research Group®

Review Article

Study of Digital Watermarking Algorithms for Digital Rights Management and their Attacks

Kavitha Soppari [1], N.Subhash Chandra [2]

[1]*Research Scholar, JNTUH, Hyderabad, INDIA*
[2]*Professor, Dept. of Computer Science and Engineering, CVR College of Engineering, Hyderabad, INDIA*

***Abstract* - *Sharing multimedia data (image, audio, video, graphics, animation, text, etc.) using different apps has become very common in this internet era's social media and digital media. This has raised a major problem for multimedia content developers. Proving Ownership rights on multimedia data has made researchers develop different techniques. Digital watermarking has given solutions to many problems like data authentication, ownership identification, content protection, Tamper proofing, copyright protection, etc. This paper discusses most of the techniques used in digital watermarking and attacks on those techniques.*

Keywords - *Digital Rights Management, Image Watermarking, Applications, PSNR, SSIM*

I. INTRODUCTION

Social media has become a platform for sharing multimedia data, images, audio, video, graphics, animation, text, etc. There is no guarantee that the sent data is not misused in various ways. Researchers have developed various techniques to secure such data and also protect ownership rights on such data. Digital watermarking gives a solution to such problems. Digital Watermarking is a process of embedding the ownership credentials in the multimedia data used to prove ownership rights. Here the credential image, i.e., the Watermark image(WI), is embedded into the source image called Cover Image (CI) as shown in Fig.1 and generates Watermarked Image (WM); later (WI) is extracted from (WM) as shown in Fig.2 for verification and proving Ownership Credentials. Hence, Digital rights management is aimed at protecting intellectual property rights.

Digital watermarking can be implemented in two domains, the first is spatial domain and the second is transformation domain. The watermark embedding process is directly implemented in spatial domain watermarking on pixels. In the transformation domain, the embedding process is performed on the frequency transform of the image. Here the original image is first transformed to a predetermined transformation, and then embedding of watermarking is performed on transformed coefficients.

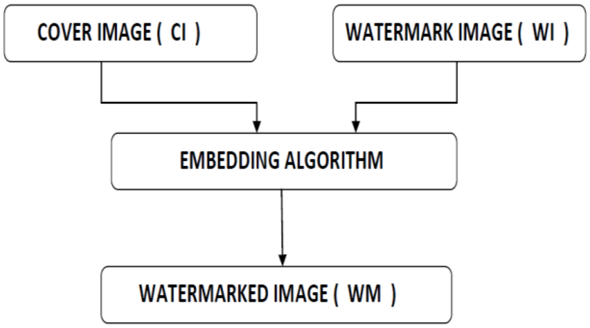


Fig. 1 Watermark Embedding

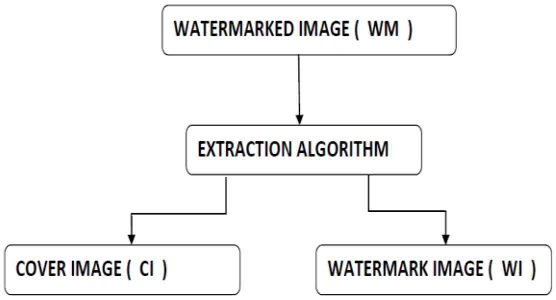


Fig. 2 Watermark Extraction

II.PROPERTIES OF DIGITAL WATERMARK

Watermark, which is embedded as an identity of the owner into the cover image, should satisfy the following properties.

A) Watermark should be imperceptible

The perceptual difference between the original image and the watermarked image should be negligible, i.e., the original image properties should be retained.

B) Watermark should be statistically invisible

The watermark that is embedded should be detected based on statistical analysis. Otherwise, it is prone to deletion.

C) Watermark should be Robust

The embedded watermark should not be noticed, but it should retain the original quality of the image in which the watermark is embedded. The watermark that is embedded should be compatible with the cover image. The watermark should sustain against image processing operations like filtering, compression, etc.,

D) Verification Procedure should be simple

The watermark's embedding process or extraction process should be simple concerning the time complexity.

E) Watermark should be trustworthy

The embedded watermark should not produce false positives. It should guarantee that it should not produce counterfeit watermarks that result in false positives. It should provide a piece of trustworthy evidence to protect ownership rights.

F) Watermarking should be secure

The watermark should sustain despite various attacks.

G) Watermark should be invertible

The process of watermark embedding and Watermark Extraction should be invertible, i.e., the embedded watermark should be the same as the extracted watermark.

G) Watermark should be transparent

If some attack or misuse is done to watermarked content, the owner should have a procedure to prove and find out what has been done. For supposing, if compression is done on the content consequent to which the watermark has been modified should be proved.

III WATERMARKING TECHNIQUES

Digital watermarking is a method of embedding some secret information in the original multimedia content to protect ownership rights. Multimedia content can be images, audio, video, graphics, animation, text, etc.

Watermarking algorithms can be categorized as reversible and irreversible, as shown in figure 3. Reversible watermarking is also called invertible watermarking or lossless watermarking. The ownership rights are embedded into the cover image to produce watermarked image during the embedding phase. Then, during the extraction phase, the cover image and the watermarked image are needed to prove the ownership credentials. Irreversible watermarking algorithms do not need the cover image to prove the ownership credentials during the extraction phase. Both reversible and irreversible watermarking are further categorized based on how much they sustain in cases of attacks as fragile, semi-fragile, and robust.

Fragile watermarking algorithms[1] do not sustain the attacks like RST (rotation, scaling, transformation) or other attacks like geometric attacks. Suppose any part of Watermarked Image(WM) is altered. In that case, we will not be able to extract the watermark from watermarked image(WM) even if we have a cover image(CI), which means that the ownership credentials cannot be proven.

Semi-fragile watermarking[2-3] algorithms show some degree of sustainability in the case of attacks like RST (rotation, scaling, transformation) or other attacks like geometric attacks and JPEG compression. If part of Watermarked Image(WM) is altered, we would be able to extract the watermark from watermarked image(WM) to prove ownership credentials which makes the image deemed authentic.

Robust watermarking[4-5] algorithms will sustain all kinds of attacks, which means that we will be able to prove ownership credentials despite various attacks on the watermarked image(WM).

Based on domains used for embedding and Extraction, watermarking algorithms can be categorized as spatial domain watermarking techniques and transformation domain watermarking techniques.

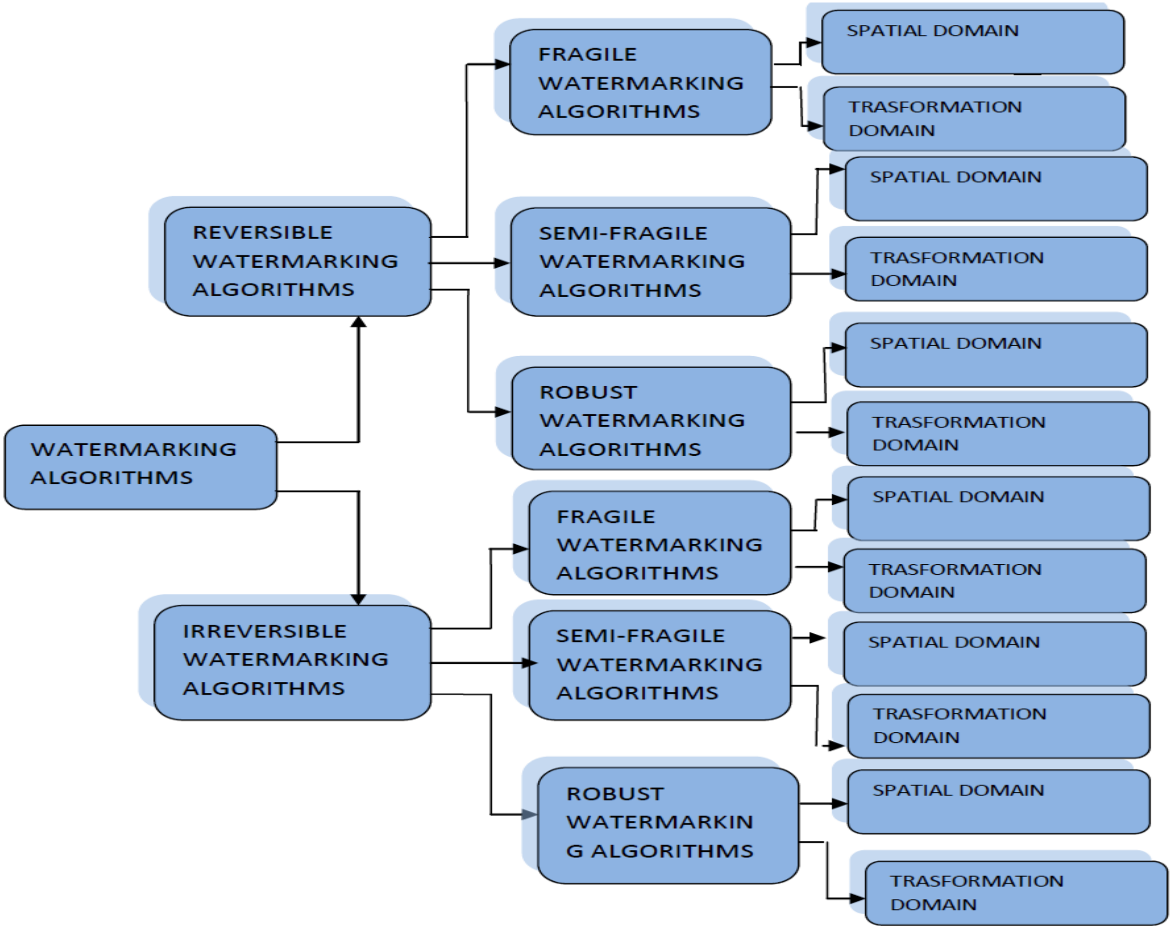

WATERMARKING ALGORITHMS
REVERSIBLE WATERMARKING ALGORITHMS
IRREVERSIBLE WATERMARKING ALGORITHMS
FRAGILE WATERMARKING ALGORITHMS
SEMI-FRAGILE WATERMARKING ALGORITHMS
ROBUST WATERMARKING ALGORITHMS
FRAGILE WATERMARKING ALGORITHMS
SEMI-FRAGILE WATERMARKING ALGORITHMS
ROBUST WATERMARKIN G ALGORITHMS
SPATIAL DOMAIN
TRASFORMATION DOMAIN
SPATIAL DOMAIN
TRASFORMATION DOMAIN
SPATIAL DOMAIN
TRASFORMATION DOMAIN
SPATIAL DOMAIN
TRASFORMATION DOMAIN
SPATIAL DOMAIN
TRASFORMATION DOMAIN
SPATIAL DOMAIN
TRASFORMATION DOMAIN

Fig. 3 Watermarking algorithms categorization

A) Spatial Domain Watermarking Techniques

The spatial domain directly works on pixels. It mostly uses LSB of the pixels and uses different techniques to embed the watermark in LSBs. Image(CI) selects the Least Significant Bits(LSB) for each pixel in the cover. It sets them to zero by shifting bits right side and embedding the watermarked Image(WI) pixels to those LSB to generate Watermarked Image(WM). In Spatial Domain, Watermarking embeds the watermark by modifying some selected pixels' intensity and color value.

[6] LSB modification method. Here the watermark image is divided as a string of L-ary symbols of watermark w_i and is embedded into the payload of the cover image by quantizing and generating the watermarked image S_w. The PSNR ratio of tested images is shown in Table 2. The disadvantage of this method is embedding capacity is very less. The output of this method is shown in figure 4. The PSNR versus BPP of the algorithm on different test images is shown in the graph in figure 9 (a).

Table 1. PSNR values of some test images using LSB modification

Cover Image	PSNR(dB) of watermarked image	Cover Image	PSNR(dB) of watermarked image
Lena	50.9683	Sunflower	51.0063
Panda	51.1151	Scenery	51.1383
penguin	53.9585	food	51.1705

[7-8] LSB modification in the green channel of bit plane. The spatial domain watermarking can be implemented on color images. The cover image(CI) is decomposed into red, green, and blue components. The embedding process is applied to green color as the change in green color will not change the cover image that the normal human eye could not recognize. The PSNR ratio of tested images is shown in Table 2. The advantage of spatial domain watermarking is that the technique used is simple, has very low computational complexity, and is less time-consuming. But the disadvantage of these methods is they are prone to various attacks like signal processing attacks and noise

attacks and are less robust. The output of this method is shown in figure 5.

Table 2. PSNR values of some test images using LSB modification in the green channel of the bit plane

Cover Image	PSNR(dB) of watermarked image	Cover Image	PSNR(dB) of watermarked image
Lena	51.1302	Sunflowe r	51.1415
Panda	51.1358	Scenery	51.1553
penguin	50.1844	food	51.0970

B) Transform Domain Watermarking Techniques

Here the digital image is transformed into the frequency domain using various transformations like DCT, DFT, and DWT, where the image is transformed to the frequency domain. Then the watermark is embedded in transformed coefficients.

[9-12] Discrete Fourier Transforms-based watermarking provides semi fragility in watermarking. In this method, the cover image(CI) is decomposed in frequency bands using DFT using the following equation.

$$F(k ,l) = \sum_{i=0}^{N-1}\sum_{j=0}^{N-1} f(i,j)e^{-i2\Pi\left(\frac{ki}{N}+\frac{lj}{N}\right)}$$

Then the low-frequency bands are selected for embedding the watermark image (WI) to produce a watermarked image (WA). For Extraction of watermark image (WI) from watermarked image (WM), inverse Fourier transformation is applied using the following equation.:

$$f(a,b) = \frac{1}{N^2}\sum_{i=0}^{N-1}\sum_{j=0}^{N-1} F(k,l)e^{-i2\Pi\left(\frac{ki}{N}+\frac{lj}{N}\right)}$$

Table 3: PSNR values of some test images using DFT transformation

Cover Image	PSNR(dB) of watermarked image	Cover Image	PSNR(dB) of watermarked image
Lena	9.0019	Sunflowe r	8.6268
Panda	11.6189	Scenery	8.6098
penguin	7.0757	food	9.5264

The disadvantage of the above method is that the watermarked image quality is degraded. The peak signal-noise ratio is very low on the embedded image from Table 3. The output is shown in figure 6. The PSNR versus BPP of the algorithm on different test images is shown in the graph in figure 9(b).

[13-16] Discrete Cosine Transformation based watermarking embeds watermark in DCT based transformation domain. Here embedding algorithm is divided into two-phase phases. In the first phase, the cover image (CI) is divided into blocks of 8 x 8 pixels per block. In the second phase, the watermark is embedded in the coefficients of DCT, which is generated using the following equation F(u,v). The output is shown in figure 7. The PSNR versus BPP of the algorithm on different test images is shown in the graph in figure 9(c).

$$F(u,v) = \frac{4c(u)c(v)}{n^2}\sum_{i=0}^{N-1}\sum_{j=0}^{N-1} f(j,k)\, cos\left[\frac{(2j+1)u\Pi}{2n}\right] cos\left[\frac{(2k+1)v\Pi}{2n}\right]$$

Using the following equation f(i,j), extraction inverse cosine transformation coefficients are used.

$$f(j,k) = \sum_{i=0}^{N-1}\sum_{j=0}^{N-1} c(u)c(v)F(u,v) cos\left[\frac{(2j+1)u\Pi}{2n}\right] cos\left[\frac{(2k+1)v\Pi}{2n}\right]$$

Table 4: PSNR values of some test images using DCT transformation

Cover Image	PSNR(dB) of watermarked image	Cover Image	PSNR(dB) of watermarked image
Lena	41.416	Sunflower	41.3041
Panda	41.4 353	Scenery	41.407
Penguin	43.8052	food	41.6728

[17-21] proposed a Discrete wavelet transformation based watermarking embeds the watermark by transforming the cover image (CI) is divided into sub-bands LL1, LH1, HL1, and HH1 using Haar wavelet transformation called 1-level DWT which are wavelet coefficients than LL1 is further divided into sub-bands LL2, LH2, HL2, HH2 called 2-level DWT. This division is repeated until the details of the sub-band become close to zero. Watermark is embedded in these wavelet coefficients. The output is shown in figure 8. The PSNR versus BPP of the algorithm on different test images is shown in the graph in figure 9(d).

Table 5: PSNR values of some test images using DWT transformation

Cover Image	**PSNR(dB) of watermarked image**	**Cover Image**	**PSNR(dB) of watermarked image**
Lena	81.5041	Sunflower	81.3992
Panda	81.8	Scenery	81.7451
Penguin	82.0944	food	81.6973

[11] Methaq divided the image into blocks of equal size and applied 2-D DFT for each block separately, and embedded the watermark in the coefficients of the DFT in the blue channel of the host Image. Then inverse DFT is applied to generate a watermarked image.

IV. ATTACKS ON WATERMARKING ALGORITHMS

Attacks can be categorized into linear and Non-Linear Attacks. In a Linear attack, all the Pixels are modifiers by the attacker, and in a Non-Linear attack, only a few selected pixels are modified by the attacker. Attacks like Rotation, Scaling come under linear attacks, and attacks like Pixel Distortion, Noise Addition come under Non-Linear attacks. Different kinds of attacks on Watermarked Images are

A) Collusion attacks

Here the attacker will use statistical measures to analyze the presence of the watermark location and try to remove it or recreate the cover image by copying different objects in it.

B) Noise attacks

Here salt and pepper noise and Gaussian noise are embedded using different mean and variance values to distort the image. These types of attacks are called non-destructive attacks.

C) Removal attacks

De-Noising and watermark prediction are removal attacks.

D) Forgery attack

Here the attacker will embed a valid watermark in a different cover image or another watermarked image to forge the image to confuse the original watermark and the forged watermark. Here image hash is generated with zero-mean random smooth patterns generated using secret keys.

D) Geometric Distortion attacks

Rotation scaling and translation attacks, also called RST attacks and Cropping attacks, in which the attacker performs either rotation or scaling or translation or cropping to make detection impossible.

E) Cryptographic attacks

In these attacks, the attacker removes are destroyed the embedded watermark. Nowadays, watermarking algorithms are known to most researchers, so predicting algorithms used for watermarking using the brute-force method and removing has become very easy.

F) Protocol attack

In this type of attack, a genuine watermark is used to authenticate another unwanted image.

G) JPEG Compression Attack

Here attacker compresses the image using JPEG compression, which leads to a loss of watermark. It is also called lossy compression. Saving our file as a JPEG file itself compresses the image automatically. [29] Wang Gang and Rao Ni-ni have broken the algorithms using JPEG compression.

Analysis of the above attacks on the described algorithms is given in Table 6.

V APPLICATIONS OF WATERMARKING ALGORITHMS

A) Medical Imaging

[23] In medical images, when it is digitized, there is a need for proper authentication of the image, including the details of the diagnosis center and physician details of patients. There is a need to preserve certain ROI (Region of Interest) [4] in medical images.

B) Authentication or Integrity checking or tamper-proofing or Content protection or content identification and management

Watermarking is used for image authentication, i.e., to detect whether any of the attacks modify any part of the image. Content is solely the property of the content developers, but content can be easily copied and transmitted over the network in this digital world. This makes content developers from misusing their content by copying or reproducing, or selling it online without the owners' knowledge. Watermarking provides solutions to all these problems.

C) Law Enforcement and Forensics or piracy deterrence

[24] Watermarking plays a major role in proving against modification in crime scenes photographs which will be used later in the court of law. Forensic watermarking is used to gather evidence for criminal proceedings and enforce contractual usage agreements between a content owner and the people or

companies with which it shares its content. It provides positive, irrefutable evidence of misuse of leaked content assets. Watermarking can also complement digital rights management (DRM) in many situations by balancing content owner copyrights with consumer fair use allowances.

D) Artistic Efforts and Locating Content Online

Many artists now a day's share their art online to raise funds for their art projects. The nightmare for this artist is a copyright infringement and protection of their property.[25] Protection and management of intellectual property for artworks of an artist against copyright infringement can be done using watermarking.[26]

E) Copyright Protection or Ownership Identification or document protection

[27] The owner's details are embedded in the image or document so that it can be protected from unauthorized copying.

F) Information retrieval Systems or locating content online

Watermarked data can be used as content identification and a keyword to identify the content, which can be secured against the access of unrelated data. Especially hiding adult content from children

G) Broadcast Monitoring and Audience Measurement

[28] Broadcast monitoring is needed for TV by embedding a unique watermark identifier used to monitor television broadcasts automatically and registering which assets have been pre-encoded; a mechanism for IPR protection can be provided. Apart from protecting our content during the broadcast, there is a need to keep track of how people access our content so advertisers and broadcasters can tailor their offerings better and maximize impact.

H)Transaction tracking or Fingerprinting

[26] The owner must be able to track the distributions of the work to find the person responsible for the illegal replication and redistribution.

VI MEASURING METRICS USED FOR WATERMARKING

The performance of the watermarking algorithms is analyzed using the following metrics.

*A) Mean Square Error (MS***E)**

Mean Squared Error (MSE) is a measure that tests if two pictures are similar. It is performed using the equation.

$$\text{MSE}= \left(\frac{1}{n}\right)\sum_{i=1}^{n} (x_i - x'_i)^2$$

B) Pick Signal to Noise Ratio (PSNR)

It considers the signal strength for calculating the error. The signal, in this case, is the original data, and the noise is the error introduced by embedding a watermark or modifying the image. It is calculated as

$$\text{PSNR} = 10\log_{10}\left(\frac{255^2}{MSE}\right)$$

C) Normalized Cross-Correlation (NCC)

$$\text{NCC} = \frac{\sum_{i=1}^{M1}\sum_{J=1}^{M2} W(i,j) \,.\, W'(i,j)}{\sqrt{\sum_{i=1}^{M1}\sum_{J=1}^{M2}[W(i,j)\,]^2}\sqrt{\sum_{i=1}^{M1}\sum_{J=1}^{M2}\,[W'(i,j)]^2}}$$

D) Structural Similarity By Index (SSIM)

SSIM is used for measuring the similarity between two images[29]. The SSIM index is a full reference metric; in other words, the measurement or prediction of image quality is based on an initial uncompressed or distortion-free image as a reference. SSIM is designed to improve traditional methods such as peak signal-to-noise ratio (PSNR) and mean squared error (MSE). SSIM is calculated between two images x,y as

$$\text{SSIM(x,y)} = \left(\frac{(2\mu_x\mu_y+C_1)(2\sigma_{xy}+C_2)}{(\mu_x{}^2+\mu_y{}^2+C_1)(\sigma_x{}^2+\sigma_y{}^2+C_2)}\right)$$

Where μ_x is an average of x, μ_y is average of y, $\sigma_x{}^2$ is variance **x,** $\sigma_y{}^2$ is variance y, σ_{xy} is covariance x and y, $C_1 = (K_1, L)^2$, $C_2 = (K_2, L)^2$, two variables to stabilize the division with a weak denominator. L is the dynamic range of pixel values (typically $2^{number\ of\ bits\ per\ pixel} - 1$)

$K_1 = 0.01\ K_2 = 0.03$ by default.

VII RESULTS

We have implemented the attacks discussed in section 4 on the watermarked images generated from the methods discussed in section 3, and the analysis is done and compiled in table 6.

Table 6. Analysis of Watermarking algorithms against various attacks

Algorithm	Domain used	Protection against Collusion attacks	Protection against Noise attacks	Protection against Removal attacks	Protection against Forgery attack	Protection against Geometric Distortion attacks	Protection against Cryptographic attacks	Protection against Protocol attack	Protection against JPEG Compression Attack
LSB modification	Spatial	No	No	No	No	No	No	No	No
LSB modification in the green channel of bit plane	Spatial	No	No	No	No	No	No	No	No
DFT	Transfor mation	No	No	No	No	No	No	No	No
DCT	Transfor mation	Yes	Yes	No	Yes	Yes	No	No	Yes
DWT	Transfor mation	Yes	Yes	No	Yes	Yes	No	No	Yes

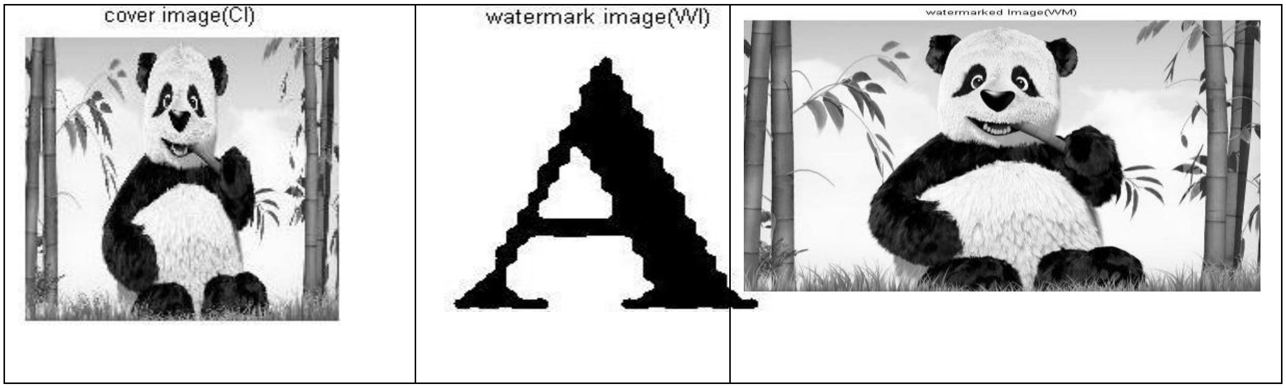


Fig. 4 Watermarking based On the LSB modification method

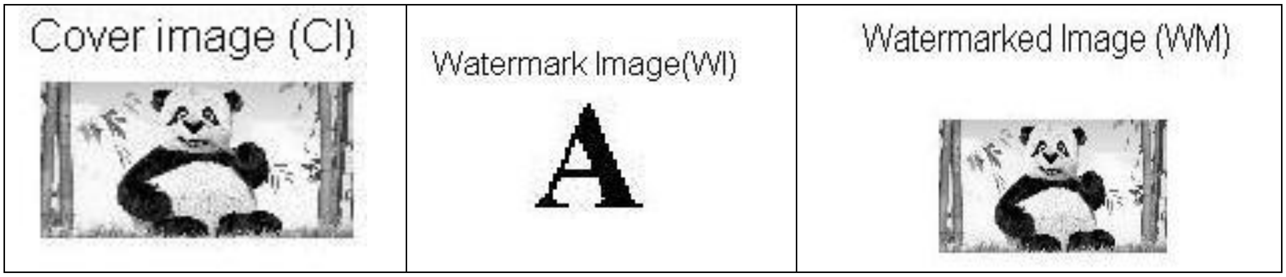


Fig. 5 Watermarking based LSB modification in the green channel of bit plane

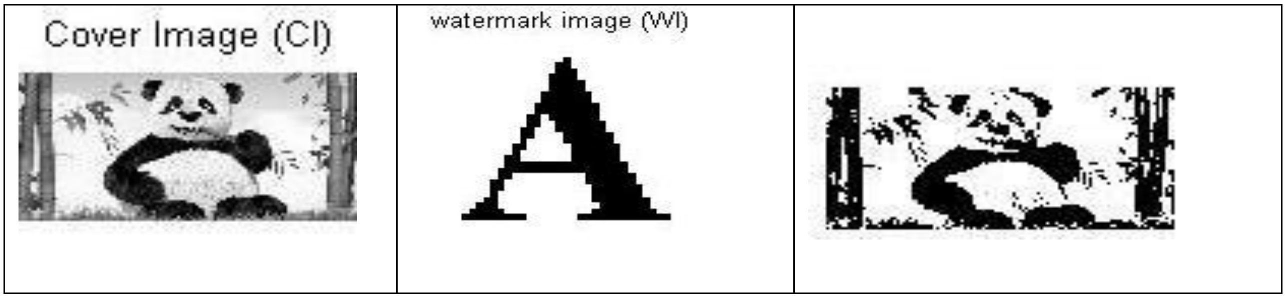


Fig. 6 Watermarking based on DFT

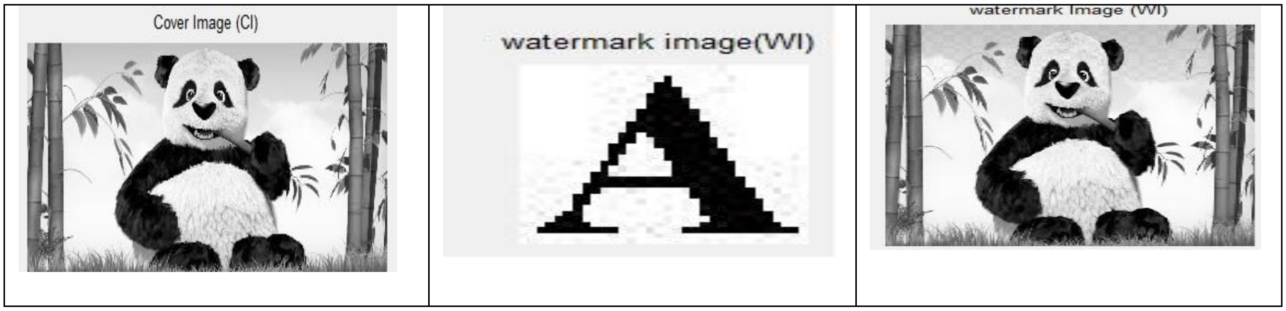


Fig.7 Watermarking based on DCT

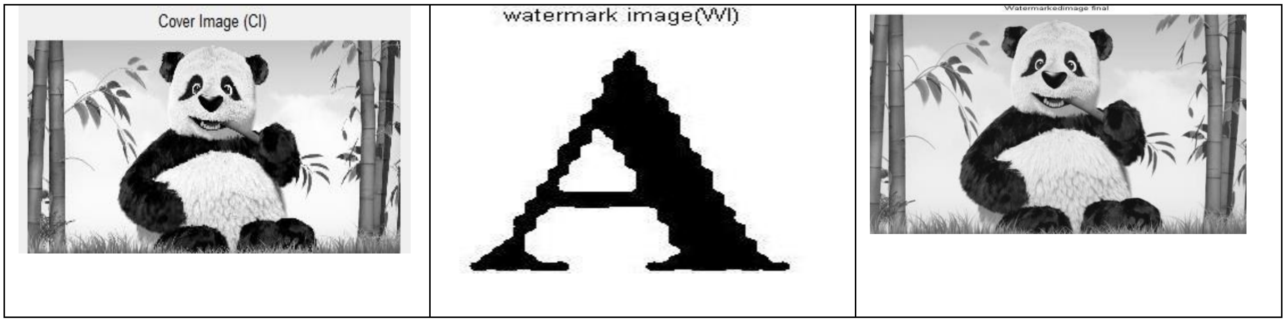
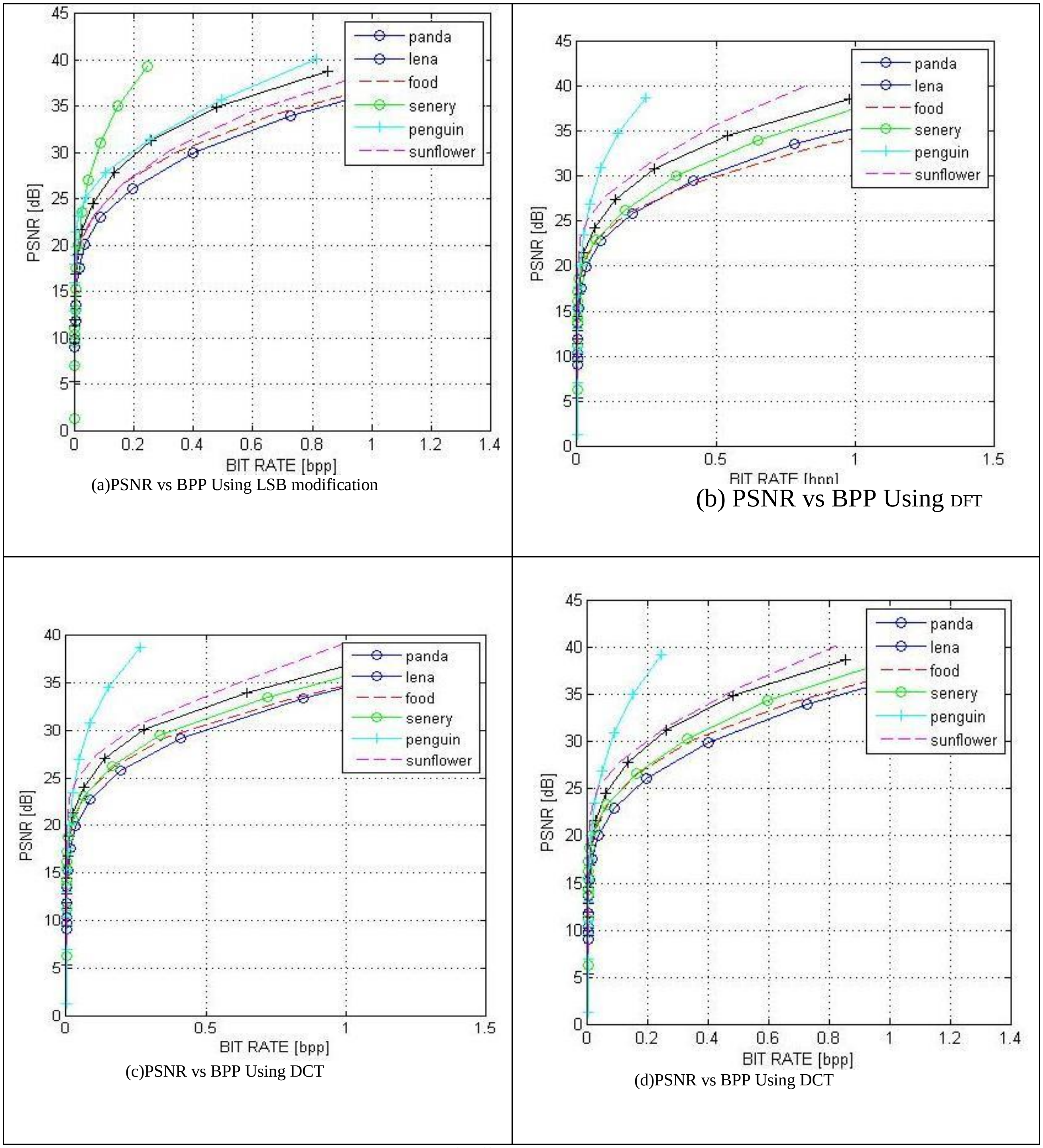


Fig. 8 Watermarking based on DWT



(a)PSNR vs BPP Using LSB modification

(b) PSNR vs BPP Using DFT

(c)PSNR vs BPP Using DCT

(d)PSNR vs BPP Using DCT

Fig. 9 PSNR v/s BPP of Different algorithms on the test image

VIII. CONCLUSION

In this paper, we described different Watermarking algorithms used for various applications like medical imaging, ownership rights protection, fingerprinting, content protection, etc.; a comparative study of various algorithms against various attacks is described. All the algorithms are not completely resilient to various attacks; with the grown inventions of various watermarking techniques, researchers also developed algorithm-breaking methods. Hence there is a need for better techniques of watermarking which are resilient to different attacks.

REFERENCES

[1] Rinaldi Munir, "A Chaos-based Fragile Watermarking Method in Spatial Domain for Image Authentication," 2015 International Seminar on Intelligent Technology and Its Applications, 2015 IEEE.

[2] Zhu Xi'an, "A Semi-Fragile Digital Watermarking Algorithm in Wavelet Transform Domain Based on Arnold Transform," ICSP2008 Proceedings.

[3] Dekun Zou, Yun Q. Shi, Zhicheng Ni, Wei Su, "A Semi-Fragile Lossless Digital Watermarking Scheme Based on Integer Wavelet transform," IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, VOL. 16, NO. 10, OCTOBER 2006.

[4] A.Giakoumaki, S. Pavlopoulos, D. Koutsouris, "Multiple Digital Watermarking Applied to Medical Imaging," Proceedings of the 2005 IEEE Engineering in Medicine and Biology 27th Annual Conference Shanghai, China, September 1-4, 2005.

[5] N.Nikolaidis!, I. Pitas" Robust image watermarking in the spatial domain," Signal Processing 66 (1998) 385Ð403, Elsevier.

[6] Mehmet Utku Celik, Ahmet Murat Tekalp, "Lossless Generalized-LSB Data Embedding," IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 14, NO. 2, FEBRUARY 2005.

[7] Abdulmawla M A e.tal., "A new colour image watermarking technique using spatial Domain," IEEE 2015.

[8] Cik Ku Haroswati Che Ku Yahaya, Harnani Hassan, Mohd Izwan Bin Md Kahmi, "Investigation on Perceptual and Robustness of LSB Digital Watermarking Scheme on Halal Logo Authentication," 2012 International Conference on System Engineering and Technology September 11-12, 2012, Bandung, Indonesia, IEEE 2012

[9] Mahalingam Ramkumar, Ali **N.** Akansu and A Aydan Alatan, **"A** Robust Data Hiding Scheme For Images Using DFT," 1999 IEEE.

[10] M. Ramkumar, A.N. Akansu, A.A. Alatan, "A Robust data hiding scheme for images using DFT," IEEE Proceedings 1999 International Conference on Image Processing.

[11] Methaq T. Gaata, "An Efficient Image Watermarking Approach based on Fourier Transform," International Journal of Computer Applications (0975 – 8887) Volume 136 – No.9, February 2016

[12] Manuel Cedillo-Hernandez, Francisco J. Garcia-Ugalde, Mariko Nakano-Miyatake, Hector M. Perez-Meana, "DFT-Based Watermarking Method for Medical Images," 2012 Ninth Electronics, Robotics, and Automotive Mechanics Conference, IEEE 2012.

[13] Adrian G. Borg Ioannis Pitas, " Image Watermarking Using DCT Domain Constraints," 1996 IEEE.

[14] Yuan-Liang Tang and Chih-Peng Wang, "A Robust Watermarking Algorithm Based on Salient Image Features," 2008 IEEE.

[15] Liwei Chen, Mingfu Li, "An Effective Blind Watermark Algorithm Based on DCT," IEEE Proceedings of the 7th World Congress on Intelligent Control and Automation June 25 - 27, 2008, Chongqing, China.

[16] Jagdish Prasad Maheshwari, Mahendra Kumar, Garima Mathur, R P Yadav, Rajesh Kumar Kakerda, "Robust Digital Image Watermarking using DCT based Pyramid Transform via image Compression," IEEE ICCSP 2015

[17] Bang Guannan Wang Shuwn Nian Guijun, "A Blind Watermarking Algorithm Based on DWT for Color Image," 2004 IEEE.

[18] Gengming Zhu, Nong Sang, DeshegXiang, Shaobo Zhang, " Watermark Algorithm Research and Simulation Based on Different Frequency Coefficients," 2008 IEEE.

[19] FU Yu, WU Xiaoping, Chen Zemao, Ye Qing, "A Wavelet Digital Watermarking Algorithm Based on Chaotic Mapping," 2008 IEEE

[20] Jayprakash Upadhyay Dr. Bharat Mishra Dr. Prabhat Patel, "A Modified Approach Of Video WatermarkingUsing DWT-BP Based LSB Algorithm," IEEE,2017

[21] Rita Choudhary, Girish Parmar, "A Robust image Watermarking Technique using 2-level Discrete Wavelet Transform (DWT)", IEEE 2nd International Conference on Communication, Control and Intelligent Systems (CCIS).2016.

[22] Johnson C. Lee, "Analysis of Attacks on Common Watermarking Techniques," IEEE

[23] Wang Gang, Rao Ni-ni, "A Fragile Watermarking Scheme for Medical Image," 2005 IEEE.

[24] Anthony T.S. Ho, "Semi-fragile Watermarking and Authentication for Law Enforcement Applications," 2007 IEEE.

[25] W.K. ElSaid, "Watermarking Digital Artworks," International Journal of Computer Applications (0975 – 8887) Volume 125 – No.12, September 2015

[26] Ashraf M.A. Ahmad, Ismail Khalil Ibrahim, Textbook on "Multimedia Transcoding in Mobile and Wireless Networks," Published by Information science Reference, Hershey, New York, 2009 by IGI Global

[27] Jobin Abraham, Varghese Paul, " An imperceptible spatial domain color image watermarking scheme," Journal of King Saud University – Computer and Information Sciences (2017)

[28] L.De Strycker, P.Termont, J.Vandewege, J.Haitsma, A.Kalker, M.Maes and G.Depovere," Implementation of a real-time digital watermarking process for broadcast monitoring on a TriMediaVLlW processor," IEE Proceedings,2000

[29] Zhou Wang et al., " Image Quality Assessment: From Error Visibility to Structural Similarity," IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 13, NO. 4, APRIL 2004