

Enhanced Watermarking Technique to Implement Invisible Watermark through GLCM & PCA Algorithm

Hemant Goutam¹ Ram Lal Yadav²

¹M.TechScholar, KITE, Jaipur, ²Associate Professor, KITE, Jaipur

Email -hemantgoutam007@gmail.com,ram.bitspilani@gmail.com

Abstract- The spatial domain method and frequency domain method are the two broader categorizations of several watermarking techniques proposed over the time. The lower order bits of cover image are improved for embedding a watermark through the spatial domain technique. Minimizing the complexity and including minimum computational values are the major benefits achieved through this technique. However, in the presence of particular security attacks, the robustness of this technique is very high. Further, the techniques that use some invertible transformations such as Discrete Cosine Transform (DCT) are known as the frequency domain transform techniques. The image is hosted by applying Discrete Fourier transforms (DFT) and Discrete Wavelet Transform (DWT) techniques. The coefficient value of these transforms is modified as per the watermark for embedding the watermark within the image easily. Further, on the original image, the inverse transform is applied. The complexity of these techniques is very high. Also, the computational power required here is high. The security attacks are provided with more reverts through these methods. GLCM (Gray Level Co Occurrence Matrix) technique is better approach compare with other approach. In this paper, GLCM (Gray Level Co Occurrence Matrix) and PCA (Principal Component Analysis) algorithms are used to improve the work capability of the neural networks by using watermarking techniques. PCA selects the extracted images and GLCM is used to choose the features extracted from the original image. The output of the PCA algorithm is defined by using scaling factor which is further used in the implementation. In this work, the proposed algorithm performs well in terms of PSNR (Peak Signal to Noise Ratio), MSE (Mean Squared Error), and Correlation Coefficient values. The proposed methods values are better from the previous work.

Keywords- Invisible Watermarking, Blind Watermarking, PCA, GLCM, PSNR, MSE

I. INTRODUCTION

The image processing is defined as process of producing input images at a particular place. It consists of metric and topological [1] edges in order to analyze and for cracking the edges for the creation of structures between the pixels of images. The intensity of the captured is varied from small neighboring pixel boundary. This pixel boundary is very important term used in this image processing. The image is viewed by using sinkhole and the processing of the images is completely based on the knowledge and execution. The decisions are made by using human cognition method according to the provided information. The percentage of the degradation is calculated by analyzing the quality of images.

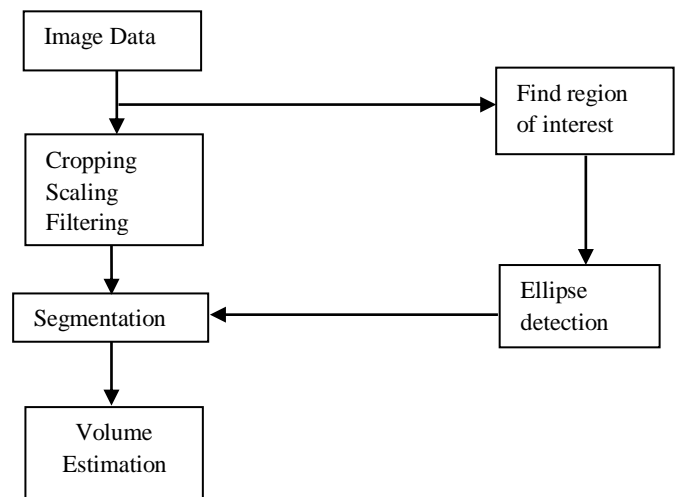


Figure 1.1: Image processing flow

The image quality depends upon two respective factors:

- Subjective used in television technology

- Objective quantitative methods measuring image quality are more interesting for our purposes

The objectives of image processing can be divided into five groups:

1. Hallucination (monitor the objects that are not visible.)
2. Image restoration and sharpening (for creating better image.)
3. Image repossession (search for the image of interest.)
4. Measurement of pattern (measures a range of objects in an image.)
5. Image acknowledgment (differentiate the objects in an image)

Digital Image Watermarking

Digital watermarking embeds the data called watermark into a multimedia objects so that the watermarked can be identified in order to make an assertion regarding objects. It is of two types visible or invisible. For e.g. the logo of television channel is clearly visible at the corner of the television picture, is visible watermark whereas the invisible watermark is hidden inside the objects which can only be detected and identified by the authorized user. These types of watermarks are suitable for making authentication [8] and detection of unauthorized copies. It holds the embedded images with the information and then these watermarked images are transmitted and extracted by the receiver. There are two different kinds of detection types in watermarking. In first type the detector does not require original cover of the image to detect the watermark and it is called blind watermarking. In the second type, the detector requires the original cover of the image to identify the watermark and is called non-blind watermark.

The model of digital image watermarking is divided into two parts; the first one is the watermark embedding process and is shown in the figure 1.2.

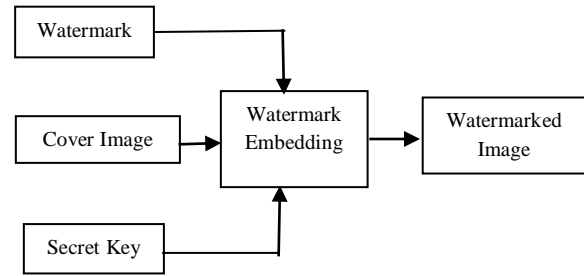


Figure 1.2 Watermark Embedding

In Figure 1.3, shows represents sender, the Watermark is embedded into the Cover Image with the Secret Key that ensures the security [9] of watermarking process. The output is the Watermarked Image.

The embedding watermark in the LSB provides best image quality whereas the embedding watermark in the MSB The process of watermarking is divided into two parts:

- a) Embedding of watermark into host image
 - b) Extraction of watermark from image
- a) **Watermarking Embedding:**The process of image watermarking is performed at the source end. The watermark is embedding the host image by using any of the watermarking algorithms. The complete process is described in the figure 1.3.

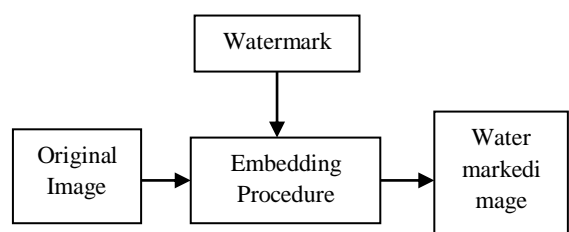


Fig 1.3 Embedding process of image watermarking

- b) **Watermarking Extraction:**In this process, the watermark is extracted from the watermarked image by reversing the embedding [16] algorithm. The complete process is shown by the figure 1.4.

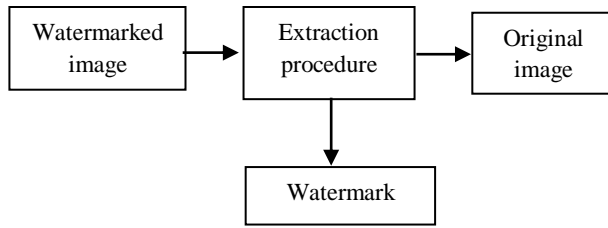


Fig.1.4. watermarking extraction

Watermarking requires some desirable properties based on the application of the embedded watermark images. Some of them are illustrated as follow:

- i. **Effectiveness:** It is most significant property of the watermarking technique that it should be effective and able to detect effectively. If effective watermarking does not takes place then the basic objective of watermarking is not fulfilled.
- ii. **Host signal Quality:** This is also important property. As, it is well known that the watermark is embedded in host signals like images, video, audio, so, the watermarking will takes place in such a manner that the host signals are changed up to minimum values and should not be noticed by the visible watermark.
- iii. **Watermark Size:** Watermarking is used for the owner verification and for the security confirmation of the embedded watermark and it always takes place during data transmission. So, it is very important to minimize the size of the watermark because it will increase the size of the transmitted data which will be visible to all.
- iv. **Robustness:** there are so many reasons by which the watermarking is degraded and altered at the time of transmission. Hence, the watermark should be robust and withstand

II. LITERATURE REVIEW

ArezouSoltaniPanah et.al (2018) reviewed [22] a latest development in the applications which are non-media and have emerged very largely from past so

many years. The receiver is able to detect watermark so the invisibility can be redefined and accepted in all the conditions so that can be generalized more easily. The main purpose of this paper to motivate the research in this field and solves that the research problems occurring during data mining process. By using this model the data was not restricted to multimedia or any other persistent behavior. The complex format of the data affects the format of data mining and discovery of knowledge based methods. So, the digital watermarking methods are performed in such a manner that it will not interfere in data mining process. This improves the security issues which are one of the most common issues. The basic requirements for data mining are low complexity, scalability, able to distribute cooperative apparatus. Therefore, the researchers conclude that the proposed technique of watermarking is suitable for Iot and resolves the problem of ownership of network of collaborated with cloud computing.

Wen Zhang et.al (2018) summarizes [23] the research program for the implementation of watermarking technology and finding such technology which is hard to copy, easy to detect, less expensive and less polluted. The authors explained three stages that generates the watermarks, print, scans, extracts and identifies watermarks, which was divided during the process of watermarking. The digital watermarking methodology which is implemented on the digital images makes the research fragile and prevents to develop any kind of relationship between watermarking algorithm and printing process parameters. Therefore, the researchers concluded that the relationship of invisibility and robustness to resist printing- scanning attacks could be balanced. The process of printing and scanning involves color space transformation.

David-Octavio Muñoz-Ramirez et.al (2018) presented [24] a robust watermarking framework for the representation of color watermark. Discrete Cosine Transform (DCT) and Quantization Index Modulation (QIM) are the methods used to perform color image as a watermark. The color watermark is encoded in such a manner that the data used to represent the color

is reduced. Moreover, the coded watermark converts into mid frequency coefficients of DCT are used to make sure about the robustness of the watermark. The efficiency of most common attacks like JPEG compression, impulsive and Gaussian noises, scaling etc has been compared with the proposed technique in terms of Peak-Signal-to Noise Ration (PSNR). Therefore, the results conclude that the proposed system achieves high imperceptibility with average values of PSNR and SSIM of 40 db and 0.994 respectively. The robustness is also very high as compared to the JPEG compression, impulsive and Gaussian noise, even the watermark could be recovered up to certain limit.

AnirbanPatra et.al (2018) proposed [25] a new technique for invisible watermarking of images by using alpha blending. The purpose of alpha blending is to display a bitmap and alpha bitmap is consisting of transparent and semi transparent pixels. The researchers have worked on color image and gray scale image, in which gray scale is works as watermark image which is placed at a secret place of the main scale image by using different values of alpha in alpha blending. This process is performed on the each plane of the image. Therefore, the resulting image having the information about color image and gray scale image but the original images are invisible. Hence, the researcher concluded that this technique can be used as image stenography after its post processing work.

Irshad Ahmad Ansari et.al (2018)proposed [26] image watermarking algorithm in the paper with the title “Block-based SVD image watermarking in spatial and transform domains”. This proposed technique is used to protect the digital images from unauthorized users. For the identification of the actual owner of host image, robust image watermarking technique is used. The researcher finds that the robust watermarking scheme is faulty and the faults are being studied in this paper. The scheme is full of positive errors and so it is not right choice to figure out the ownership of watermarked image. Hence, the proposed approach improves the robustness and imperceptibility based on SVD approach.

Unfortunately, this approach becomes useless and meaningless due to the presence of false posit improves the robustness and imperceptibly by using block based SVD approach but this improvement become meaningless because of the security flaw (false positive error) that remain untouched in their scheme.

Aoshuang Dong et.al (2017)proposed [28] water marking embedding technique which transforms the domain of two-dimensional image and achieves 3D model protection of copyright. This process of embedding analyzes the principal components, normalization and the choice of the projection. A digital water marking method was proposed based on the three dimensional model projections of images. The experiments were conducted which shows that the proposed algorithm was robust to three dimensional model. Hence, the researcher concluded that the invisibility of the watermark is quiet good in three dimension model of water marking and capable of anti-rotation, anti translation and anti-noise attack.

III. PROPOSED WORK

Problem Definition

For making sure that the multimedia information is not accessed or modified by unauthorized users, several digital techniques have been proposed as per the growth of internet applications. However, the most commonly used technique is the watermarking technique. The spatial domain method and frequency domain method are the two broader categorizations of several watermarking techniques proposed over the time. The lower order bits of cover image are improved for embedding a watermark through the spatial domain technique. Minimizing the complexity and including minimum computational values are the major benefits achieved through this technique. However, in the presence of particular security attacks, the robustness of this technique is very high. Further, the techniques that use some invertible transformations such as Discrete Cosine Transform (DCT) are known as the frequency domain transform techniques. The image is hosted by applying Discrete

Fourier transforms (DFT) and Discrete Wavelet Transform (DWT) techniques. The coefficient value of these transforms is modified as per the watermark for embedding the watermark within the image easily. Further, on the original image, the inverse transform is applied. The complexity of these techniques is very high. Also, the computational power required here is high. The security attacks are provided with more reverts through these methods. GLCM (Gray Level Co Occurrence Matrix) technique is another approach that is applied within this method.

Objectives of Research

Following are the major objectives to be achieved in this research:

1. Analyze the properties of existing watermarking algorithm.
2. Propose improvement in the watermarking technique to generate a blind watermark.
3. Proposed technique will be based on the GLCM algorithm to analyze features of the original image.
4. Implement proposed technique and compare it with existing technique.

Research Methodology

For providing security to the image data, an efficient technique known as watermarking is applied. Blind and semi-blind watermarking techniques are the two broader classifications of various watermarking techniques proposed over the time. The OS-ELM (Online Sequential Extreme Learning Machine) approach that is basically a machine learning approach is utilized to introduce semi-blind watermarked image in the base paper. For the extraction of features from the original and watermark images, the four levels DWT technique is applied. In order to introduce the semi-blind watermarks, the training image that is analyzed using DWT algorithm is given as input such that the final training sets can be created. The textual features of images are

analyzed using DWT algorithm. The proposed technique replaces DWT with GLCM algorithm that is less complex and creates blind watermarks easily by providing simple mechanism was creating the training sets.

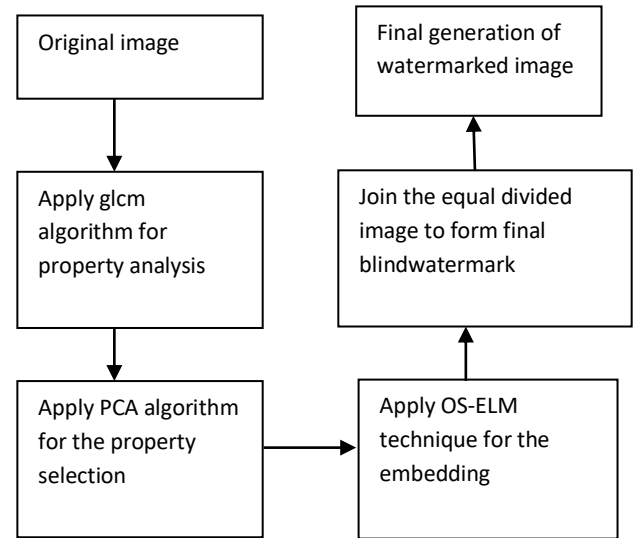


Fig 3.1: Proposed Flowchart of embedding

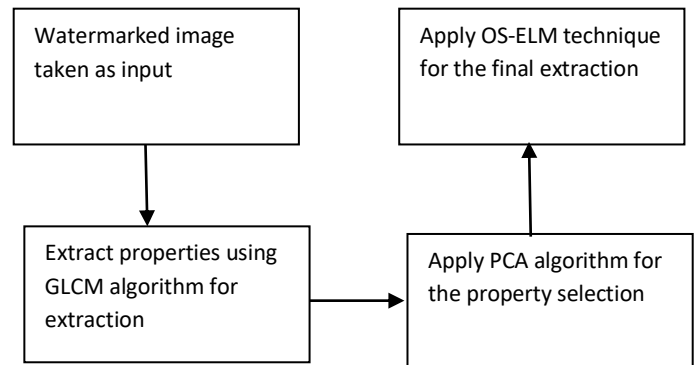


Fig 3.2: Proposed Flowchart for extraction

Following are the steps followed within the proposed algorithm:

1. Input image: - Several sensitive and non-sensitive images are taken as input in the initial phase. For increasing the security of data, it is possible to hide the sensitive image within the non-sensitive image. The keys that encrypt the watermarking images are created using the non-sensitive image.

2. Textural Feature Analysis: - The GLCM algorithm is applied in the secondary phase for extracting the textural features of the sensitive image. The various textural features such as correlation, homogeneity and so on can be extracted by applying GLCM algorithm.

GLCM Algorithm

The GLCM algorithm is performed through following steps:

1. An input is given as an image and this image is stored as pixels. The matrix is considered to count the total number of pixels of an image.
2. Another matrix for instance matrix P is used to save the counted pixels.
3. The similarity amongst pixels those are stored within the input matrix is checked by applying the histogram technique.
4. The following formula is applied to calculate the contrast of matrix:

$$g = \exp\left[\frac{\text{mean}(I) - \text{minimum}(I)}{\text{maximum}(I) - \text{mean}(I)}\right]$$

5. From matrix g, the normalization matrix is generated as:

$$g = \begin{cases} 0.8 & \text{if } g < 0.8 \\ 1.2 & \text{if } g > 1.2 \\ \text{otherwise} & \end{cases}$$

3. Implement Particle Swarm Optimization Algorithm:- From the extracted pixels, features are chosen by the PCA algorithm. The image is taken as input by the PCA algorithm and amongst various pixels, similarities and differences are analyzed. The dimensions of input data are minimized by PCA algorithm through the calculation of similarity amongst pixels. The throughput distance is used to analyze the similarity amongst various pixels. The statistics techniques and mathematical formulas are used to compare the pixels against each other. Within the recognition and image compression fields, PCA is

applied generally. The data is transformed from high to low dimensions by applying the Principal Component Analysis (PCA) technique. The Eigen vector formula is used to calculate the low dimensions.

The PCA mechanism follows certain steps which are:

1. The mean value of matrix known as A is calculated.
2. From the matrix values, the mean value is subtracted and a new matrix B is generated.
3. Eigen formula is applied to calculate the covariance from matrix which is given as $C=AAT$.
4. Eigen formula is applied to calculate the Eigen value of C.
5. The following equation is applied to generate the Covariance matrix from input values:

$$V_N S - \bar{S} = b_1 u_1 + b_2 u_2 + b_3 u_3 + \dots + b_N u_N$$

6. Within the low dimensions, the highest Eigen values are stored:

$$\hat{S} - \bar{S} = \sum_{l=0}^1 b_l u_l; 1 < N$$

IV. RESULTS & DISCUSSION

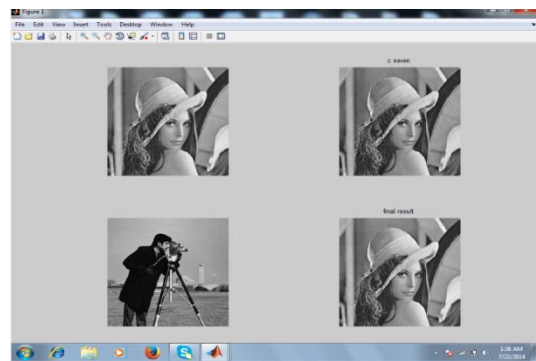


Fig. 4.1 Generation of Watermarked Image

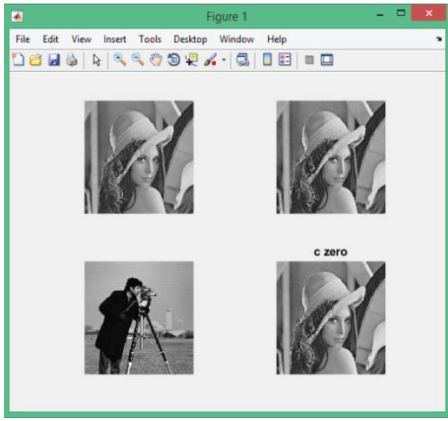


Fig 4.2 Watermark generation with proposed algorithm

In figure 4.2, the GLCM and PCA algorithms are implemented in order to select the scaling factor dynamically and by this factor the watermarked image is generated.

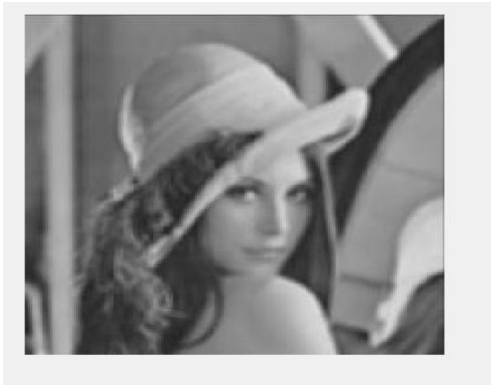


Fig 4.3 Watermark extraction

In figure 4.3, the inverse operation is implemented in order to extract the watermark image from original image. The watermark is shown in the above figure.



Fig 4.4 Watermarked Image

In figure 4.4, the inverse operation is implemented to extract the watermark image from the original image.

Table 4.1 shows the results of the proposed and existing techniques. These results are compared on the basis of the PSNR, MSE, BER and coefficient correlation values.

Table 4.1

Result comparison of different images on different parameters

	Parameter values	Existing Work Values	Proposed Work Values
Watermarked image	PSNR	13.3917	18.0129
	MSE	3001.26	2874.83
	Correlation Coefficient	0.01	0.01
	Entropy	7.9990	7.9989
Contrast Attack	PSNR	20.0542	26.0537
	MSE	647.22	547.30
	Correlation	0.96	0.01

	Coefficient		
	BER	4.2319	4.2200
Sharpened Attack	PSNR	23.6209	29.4842
	MSE	284.70	243.80
	Correlation Coefficient	0.97	0.98
	BER	7.003	6.9047
Salt & pepper Attack	PSNR	22.4476	27.484
	MSE	373.00	293.80
	Correlation Coefficient	0.96	0.91
	BER	7.9012	7.9036
Decrypted image	PSNR	13.3848	18.0130
	MSE	3006.02	3274.75
	Correlation Coefficient	0.01	0.00
	BER	7.6833	3.4237
Elapsed time		0.011795 sec	0.011994 sec

V. CONCLUSION & FUTURE WORK

Conclusion

This research shows that the digital watermarking is categorized into two categories that are public and private. The secret key is used for identification purpose which should always be present with the user so that digital watermarked images can be retrieved. In order to ensure robustness more secured watermarking techniques are proposed. The licensed based identification technique is implemented in the embedded information. A serial number is used to store the information like customer record. The receiver having legal copyright can easily retrieves the public watermark information. In public watermark includes copyright or licensing information which is used to recognize the patent or copyright of the public watermark information. The relevant information is identified by using watermarking technique. The demands of attaining

capacity in the watermarking are very large in the public watermark and the receiver will get more information about copyright with the help of this public watermark. This decreases the requirement of robustness. It involves three basic steps that are embedding, transmissions as well as extraction. In this work, the efficiency of watermarking technique is concluded that, it has capacity to hide all the sensitive information stored in the form of images. GLCM and PCA algorithms are used to improve the work capability of the neural networks by using watermarking techniques. PCA selects the extracted images and GLCM is used to choose the features extracted from the original image. The output of the PCA algorithm is defined by using scaling factor which is further used in the implementation. It has been concluded by performing simulations that the proposed algorithm performs well in terms of PSNR, MSE and Correlation Coefficient values.

Future Work

There are certain future aspects of the proposed algorithm:-

1. This proposed algorithm can be compared with other existing watermarking algorithms on the various parametric values.
2. This algorithm can be improved by using more secure channel algorithms.

VI. REFERENCES

- [1] R. C. Gonzalez & R. E. Woods, "Digital Image Processing", 3rd Edition, Prentice Hall of India, 2009.
- [2] Madhuri A. Joshi, "Digital Image Processing - An Algorithmic Approach", Prentice Hall of India, 2010.
- [3] Aisha Ajmal & Ibrahim M. Hussain, "Vehicle Detection Using Morphological Image Processing Technique", IEEE, 2010.
- [4] Y. Yang, Wei, L. Nishikawa, "Micro calcification Classification Assisted by Content Based Image Retrieval for Breast Cancer Diagnosis", IEEE International Conference on Image Processing, Vol. 5, pp. 1-4, 2007.
- [5] Shailendra Kumar Dewangan, "Human Authentication Using Biometric Recognition", International Journal of Computer Science & Engineering Technology (IJCSET), ISSN: 2229-3345, Vol. 6, No. 4, pp. 240-245, April 2015.
- [6] A. Rattani, N. Poh, and A. Ross, "Analysis of user-specific score characteristics for spoof biometric attacks," in Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit. Workshops (CVPRW), Jun. 2012, pp. 124-129.
- [7] N. Cvejic, "Algorithms for Audio Watermarking and Steganography "Department of Electrical and Information Engineering, University of Oulu, 2004
- [8] A. G. Charles Fung, Walter Godoy Junior, "A Review Study on Image Digital Watermarking," presented at the The Tenth International Conference on Networks, St. Maarten, The Netherlands Antilles, 2011.
- [9] S. Jun and M. S. Alam, "Fragility and Robustness of BinaryPhase-Only-Filter-Based Fragile/Semifragile Digital Image Watermarking," Instrumentation and Measurement, IEEE Transactions on, vol. 57, pp. 595-606, 2008.
- [10] C. De Vleeschouwer, J. F. Delaigle, and B. Macq, "Invisibility and application functionalities in perceptual watermarking an overview," Proceedings of the IEEE, vol. 90, pp. 64-77, 2002.
- [11] A. M. Zeki, A. A. Manaf, C. F. M. Foozy, and S. S. Mahmood, "A Watermarking Authentication System for Medical Images," presented at the World Congress on Engineering and Technology (CET 2011), Shanghai, China, 2011.
- [12] R. F. Olanrewaju, O. O. Khalifa, A.-H. Hashim, A. M. Zeki, and A. A. Aburas "Forgery Detection in Medical Images Using Complex Valued Neural Network (CVNN)," Australian Journal of Basic and Applied Sciences, 2011.
- [13] A. Bamatraf, R. Ibrahim, and M. N. B. M. Salleh " Digital watermarking algorithm using LSB," in Computer Applications and Industrial Electronics (ICCAIE), 2010 International Conference on, 2010, pp. 155-159.
- [14] A. M. Zeki, A. A. Manaf, and M. Zamani, "Bit-Plane Model: Theory and Implementation," in Engineering Conference (EnCon) 2010.
- [15] A. M. Zeki and A. Abdul Manaf "A novel digital watermarking technique based on ISB (Intermediate Significant Bit)," World Academy of Science, Engineering and Technology, vol. 50, pp. 989-996, 2009.
- [16] A. M. Zeki, A. A. Manaf, and S. a. S. Mahmood, "Analysis of ISB watermarking model: block based methods vs embedding repetition methods," presented at the Proceedings of the 9th International Conference on Advances in Mobile Computing and Multimedia, Ho Chi Minh City, Vietnam, 2011.
- [17] Z. Jiang Yong, L. Dong Hong, L. Jiang Zeng, and J. Miao, "A DCT-BASED Digital Watermarking Algorithm for Image," in Industrial Control and Electronics Engineering (ICICEE), 2012 International Conference on, 2012, pp. 1217-1220.
- [18] X. Jun and W. Ying, "Toward a Better Understanding of DCT Coefficients in Watermarking," in Computational Intelligence and Industrial Application, 2008. PACIIA '08. Pacific-Asia Workshop on, 2008, pp. 206-209.
- [19] R. Dubolia, R. Singh, S. S. Bhadoria, and R. Gupta, "Digital Image Watermarking by Using Discrete Wavelet Transform and Discrete Cosine Transform and Comparison Based on PSNR," in Communication Systems and Network Technologies (CSNT), 2011 International Conference on, 2011, pp. 593-596.

- [20] O. O. Khalifa, Y. binti Yusof, A. H. Abdalla, and R. F. Olanrewaju, "State-of-the-art digital watermarking attacks," in *Computer and Communication Engineering (ICCCE)*, 2012 International Conference on, 2012, pp. 744-750.
- [21] V. Licks and R. Jordan, "Geometric attacks on image watermarking systems," *MultiMedia*, IEEE, vol. 12, pp. 68-78, 2005.
- [22] ArezouSoltaniPanah , Ron van Schyndel (Senior Member, IEEE), TimosSellis, and Elisa Bertino, "On the Properties of Non-media Digital Watermarking: A Review of State of the Art Techniques," 2018, IEEE
- [23] Wen Zhang, Jie Men, Conglong Ma, "Research progress of applying digital watermarking technology for printing," 2018, IEEE
- [24] David-Octavio Muñoz-Ramirez , Volodymyr Ponomaryo , Rogelio Reyes-Reyes , Volodymyr Kyrychenko , Oleksandr Pechenin, Alexander Totsky , "A Robust Watermarking Scheme to JPEG Compression for Embedding a Color Watermark into Digital Images," 2018, IEEE
- [25] AnirbanPatra, Arijit Saha, Ajoy Kumar Chakraborty, Kallol Bhattacharya, "A New Approach to Invisible Water Marking of Color Images using Alpha Blending," 2018, IEEE
- [26] Irshad Ahmad Ansari, Chang WookAhn and Millie Pant, "On the Security of "Block-based SVD image watermarking in spatial and transform domains", 2018, IEEE
- [27] Alexander S. Komarov, "Adaptive Probability Thresholding in Automated Ice and Open Water Detection From RADARSAT-2 Images," 2018, IEEE
- [28] Aoshuang Dong, Rui Zeng, "Research and Implementation Based on Three-dimensional Model Watermarking Algorithm," 2017, IEEE
- [29] Enjian Bai, Yiyu Yang and Xueqin Jiang, "Image Digital Watermarking Based on a Novel Clock-controlled Generator," 2017, IEEE
- [30] Oleg Evsutin, Roman Meshcheryakov, Viktor Genrikh, Denis Nekrasov and Nikolai Yugov, "An Improved Algorithm of Digital Watermarking Based on Wavelet Transform Using Learning Automata," 2017, IEEE
- [31] Ritu Gill and Rishi Soni, "Digital Image Watermarking using 2-DCT and 2- DWT in Gray Images," 2017, IEEE
- [32] Mohammad Shahab Goli and Alireza Naghsh, "Introducing a New Method Robust Against Crop Attack In Digital Image Watermarking Using Two-Step Sudoku," 2017, IEEE
- [33] Thien Huynh-The, Sungyoung Lee, "Color Image Watermarking Using Selective MSB-LSB Embedding And 2D Otsu Thresholding," 2017, IEEE
- [34] Shan Liu ,Keming Yue ,Hua Yang ,Lu Liu ,XiaorongDuan ,Ting Gu, "Digital Watermarking Technology and Its Application in Information Security," 2017, IEEE
- [35] Etti Mathur and Manish Mathuria, "Unbreakable Digital Watermarking using combination of LSB and DCT," 2017, IEEE