

Digital Watermarking for Images Security using Discrete Slantlet Transform

Myasar Mundher¹, Dzulkifli Muhamad¹, Amjad Rehman^{2,*}, Tanzila Saba³ and Firdous Kausar⁴

¹ Faculty of Computing, Universiti Teknologi Malaysia, Malaysia

² MIS Department, CBA Salman bin Abdul Aziz University, Alkharj, KSA

³ College of Computer and Information Sciences, Prince Sultan University, Riyadh, KSA

⁴ College of Computer and Information Sciences, Imam University, Riyadh, KSA

Received: 19 Oct. 2013, Revised: 17 Jan. 2014, Accepted: 18 Jan. 2014

Published online: 1 Nov. 2014

Abstract: This paper presents digital images watermarking approach to sustain the ownership and true authentication. To secure intellectual belongings of images, audio and videos, watermark W is converted into a sequence of bits and in order to encrypt the watermark, sequence of size R is selected randomly. Additionally, a pseudo random number is generated to calculate pixels for selection key generation. Finally, 2-level discrete slantlet transform (DST) on the host image is applied to divide it into Red, Green and Blue channels. The results thus produced from proposed methodology exhibit robustness against the existing state of the art. Further, proposed approach effectively extract watermark in the absence of the original images.

Keywords: Discrete Slantlet Transform (DST), Watermarking, RGB, Images security and authentication

1 Introduction

Digital watermark is a symbol of own ship in natural and non-natural (document) images to verify the identity of its owners and data authentication. The digital data might be images, audios or videos and the embedded information could be an image or textual data to verify the owner such as the name of the author, signature, enterprise logo etc [18,19]. Watermark could be detected and extracted from watermarked images to identify the original owner. Embedding the watermark into host image is used by owners to claim that the multimedia data which belongs to them as the watermark is not easy to be removed from images [24,25]. Watermarking algorithms could be classified based on the domain used for embedded watermarks. Studies have shown that there are two popular techniques for this purpose: spatial and transform watermarking. Spatial domain watermarking techniques are useful for higher data embedding applications and transform domain watermarking techniques are suitable in applications where robustness is of prime concern. The techniques reported in state of the art are, Discrete Wavelet Transform [3,4,5]; Discrete Hadamard Transform [6]; Contourlet Transform [7] and Singular

Value Decomposition [8] are some of the useful transformations for image processing applications.

2 Background

With the wide use of internet, there are endless means of copying, tampering and distribution of digital data by experts. Multimedia data is less protected and copyright violations have frequently observed as everybody could download images from different sources and modify them without authorization [20]. Watermarking techniques are used as a solution to this problem by embedding information either text or images in the cover image. Imperceptibility, robustness and security are the important issues that need to be concerned within the watermarking [21,22,23]. Imperceptible watermark means that the watermark is indistinguishable in the digital images as human eyes cannot differentiate. Few researchers employed discrete wavelet transform (DWT) and achieved high capacity, good imperceptibility and low bit error rate. Human visual system (HVS) is employed for improving the transparency of data hiding. A watermark must be hidden in the host image without any kind of

* Corresponding author e-mail: rkamjad@gmail.com

degradation to prove the quality of watermarking process [1]. Robustness means the ability to recover the watermark after several attacks on watermarked image. Simple examples of these attacks are Gaussian noise, cropping, rotation, scaling and JPEG 2000 (compression) and set removal attack [2]. A robust watermarked image will resist a designated class of transformations. The watermarking scheme should be able to preserve watermark, withstanding against the possible attacks and evaluating the quality of the watermark without noticeably altering or degrading the image. The ability to resist unauthorized removal, embedding, or extraction is called security [13]. For intentional attack, it is possible to detect, modify or remove the watermark from natural or non-natural images and to use it for personal benefits. Hence, it is necessary to prevent unauthorized users to access watermark. There are related basic issues which are quite challenging to attain both the desirable robustness and imperceptibility requirements. Some of the techniques used to embed the watermark may be degraded due to several attacks on watermarked images. The purpose of this presented technique is to achieve high imperceptibility, robustness and quality of watermarked image which could resist various attacks. Researchers are focusing on human visual system (HVS) for the purpose of improving the watermarking systems and fulfilling the basic requirements of watermarking [9]. By concerning HVS, a maximum hiding level can be obtained with the method of embedding the watermark by keeping the visible image distortions to a minimum degree. On the other hand, the robust watermark is a watermark that is able to resist severe attacks such as thinning, scaling an image etc for copyright protection. Robust watermark cannot be easily destroyed after several image manipulations have been performed on the watermarked image. Authors in [8] mentioned that the main purpose of using fragile watermark is data authentication and robust watermarks are mainly used for official document security. This research proposed a colour image watermarking technique using SWT so that the basic issues can be improved. The proposed algorithm is applied to find the best quadrant to hiding information in the cover image. The selected quadrant is the best quadrant to embed the watermark because this quadrant contains less detail. According to HVS [6], the human eyes are less sensitive to the distortion in that quadrant. The watermark became more imperceptible due to the distortion made is undistinguished by naked eyes. As a result, this can avoid the modifying and removing watermark by intentionally attack. Moreover, DST has been proposed due to the robustness. Four frequency sub-bands are produced after DST process and the lower frequency sub-band (LL) are selected to embed watermark as lower frequency sub-band (LL) are highly robust [17]. The further paper is organised into four sections. Section 3 presents the proposed methodology for watermarking approach.

3 Proposed Methodology

According to human vision system, human eyes are not so sensitive for regions containing sharp textures & edges. The main purpose of pre-processing stage is to find best RGB channel and quadrant of RGB host image to introduce watermark. The selected quadrant of host image contains highest number of edges among all quadrants. The distortion in this quadrant is difficult to detect by attackers. Thus, it is important to detect the best quadrant for embedding process [15]. The watermark is recovered from watermarked image in extraction stage. In this stage, secret key is required to combine the watermark pieces in the proper sequences. Finally, four well-known attacks namely, Gaussian, Salt and Pepper, Speckle and Poisson noises are implemented to the watermarked image to evaluate its robustness. The general stage of digital watermarking is shown in Figure 1.

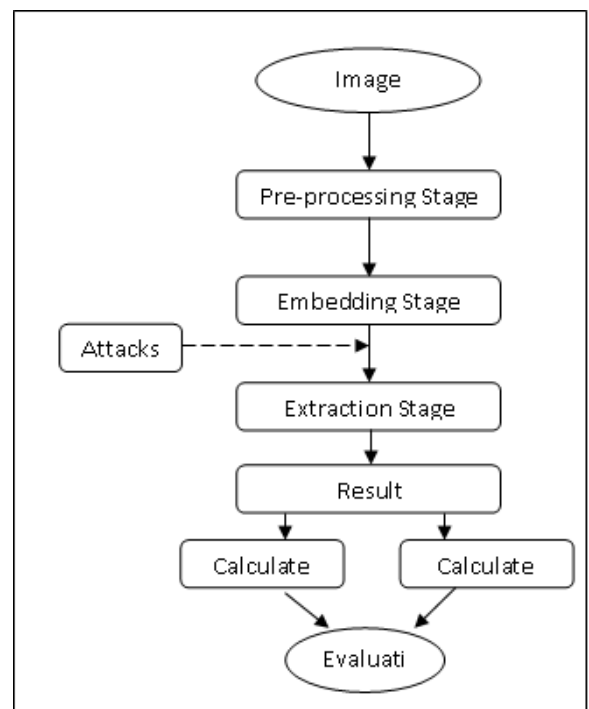


Fig. 1: General stage of digital watermarking

3.1 Pre-processing Stage

Input of pre-processing stage is a RGB colour image which is the cover image and the output is a secret key contains best quadrant of host image [7]. This stage includes the steps like image partitioning. Figure 2 illustrates the pre-processing stage of this watermarking technique.

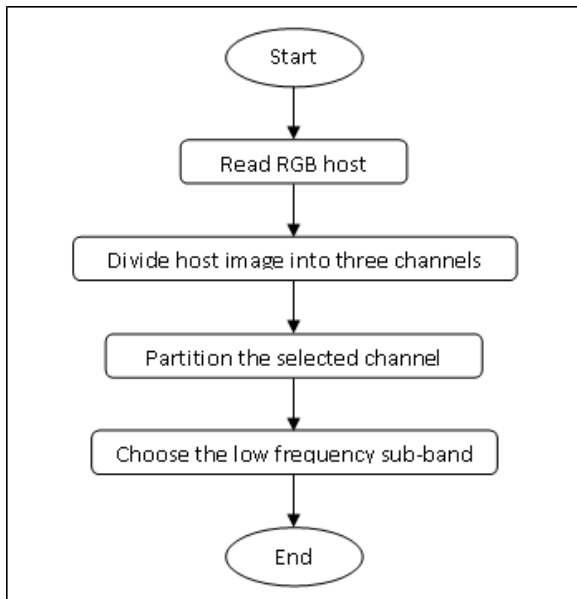


Fig. 2: Pre-processing Stage

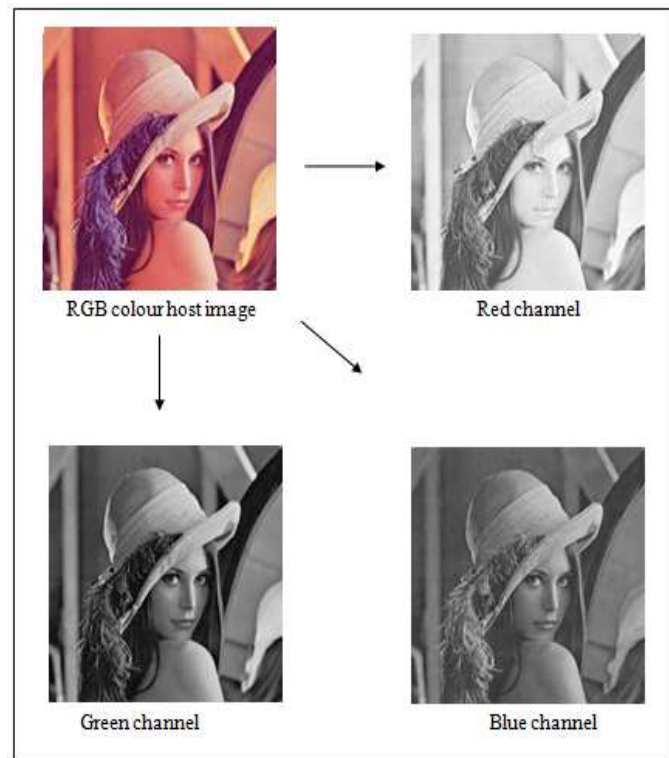


Fig. 3: RGB cover image three channels

3.2 Partitioning RGB Colour Image

First step is dividing the RGB cover image into three channels which are Red, Green and Blue components as shown in Figure 3. Initial embedding is implemented to determine the best channel. The following step is partitioning the selected channel into four quadrants before applying canny edge detection. Figure 4 shows RGB colour image before and after partitioning process [16].

3.3 Embedding Stage

Figure 5 shows the embedding stage of this watermarking technique and the following sub-section describes the details of embedding stage.

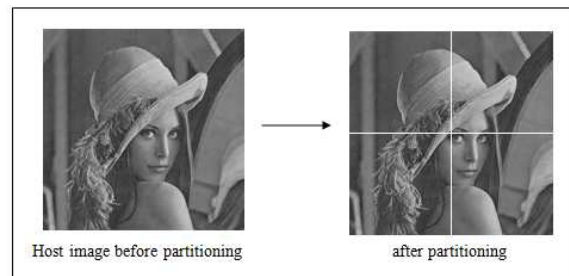


Fig. 4: Partitioning of the selected channel

3.3.1 Applying DST

The output from the pre-processing stage, the selected best quadrant is used as input in embedding stage. In this watermarking technique, a gray scale image as watermark image is being hidden in host image. The next step is applying single level 2-Dimensional DST on the selected quadrant to find the best frequency sub-band for embedding. In this step, DST is applied on R channel to cover image into special domain that have four frequencies LL, LH, HL and HH. Latter 2-level DST is applied on each sub-band to get 16 sub-bands. Similarly this procedure is applied on the second channel G and third channel B to get 16 sub-bands for each channel,

latter each channel is evaluated to choose the best sub-bands to introduce the watermark. The Peak Signal to Noise Ratio (PSNR) is employed to evaluate the watermark prior to embed and it is also evaluated after extracting by Normalize Cross-Correlation (NCC).

3.3.2 Embedding Watermark Pieces

The purpose of partitioning watermark into four pieces before embedding in cover image is to embed the watermark in more invisible manner. The pixel of each watermark quadrant is transformed to bit stream into a

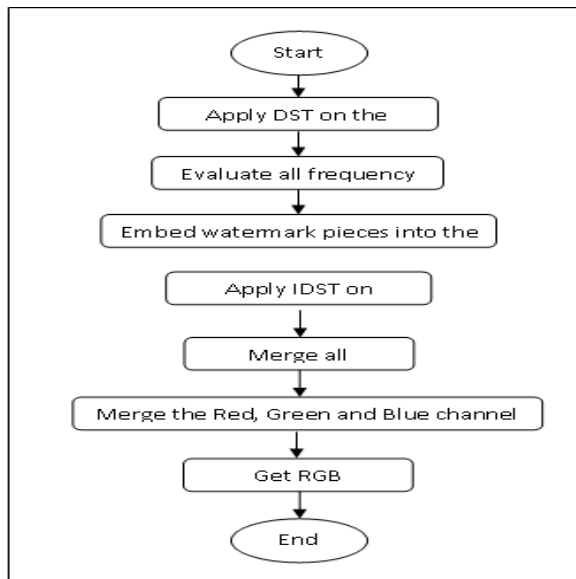


Fig. 5: Research layout

sequence Y_1 to Y_n , where n is the length of the bit stream. Therefore, replacing -1s if the bit value of watermark image is equals to 0s and remains 1s if the bit value is equals to 1. This step changes the watermark in spatial domain to the frequency domain. The embedding is performed by modifying the coefficients of the DST in order to obtain a watermarked image. In order to obtain robust watermarked image, watermark pieces are respectively embedded into the low frequency sub-band (LL) by using equation (i).

$$W'_i = W_i + \alpha Y_i \quad (1)$$

Where:

W'_i = The Watermarked image.

W_i = The Coefficients of partitioned original image.

Y_i = The Watermark image bit (-1s or 1s).

α = The Alpha, the strength of the watermark.

The actual locations of watermark pieces are being embedded are recorded as secret key 2. This secret key is required for extracting process so that the watermark pieces can be extract successfully and arrange them in proper sequence.

3.3.3 Applying IDST

After embedding has been done, assemble all the frequency sub-bands by applying IDST to inverse the frequency based quadrant to regain spatial domain quadrant. This step is to reconstruct all sub-bands in the selected quadrant using inverse steps of DST [19]. A quadrant of watermarked image will be the output after

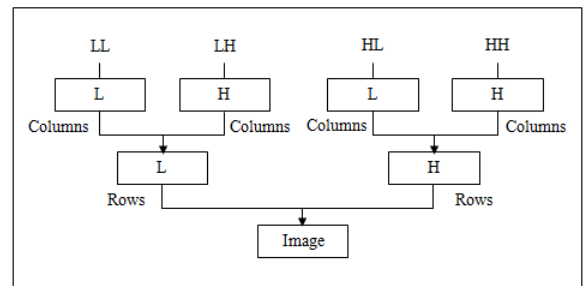


Fig. 6: Image reconstruction using IDST

IDST process. Figure 6 shows the IDST image reconstruction.

The quadrant of watermarked image is then combined with the other three quadrants to generate a watermarked image as new B channel. Figure 7 illustrates the merging of all quadrants.

The last step is merging the new B channel with the other channels into a watermarked image as Figure 8.

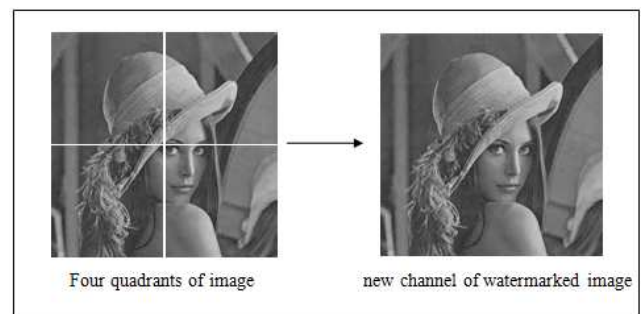


Fig. 7: Merging of all quadrants

3.4 Attacks Mechanism

Before the extraction stage, there may be some possible attacks to the watermarked image by intentional or unintentional attackers such as Gaussian noise, Cropping, Rotation, Scaling, JPEG 2000 (compression) and set removal attack [4]. Figure 9 illustrates there may be some attacks before extraction stage. The robustness of watermarked image is evaluated by calculating the NCC value before and after attacks are been applied to watermarked image [5].

3.5 Extraction Stage

Extraction stage is the last stage in watermarking technique. Figure 10 shows steps in extraction stage. The



Fig. 8: Watermarked image

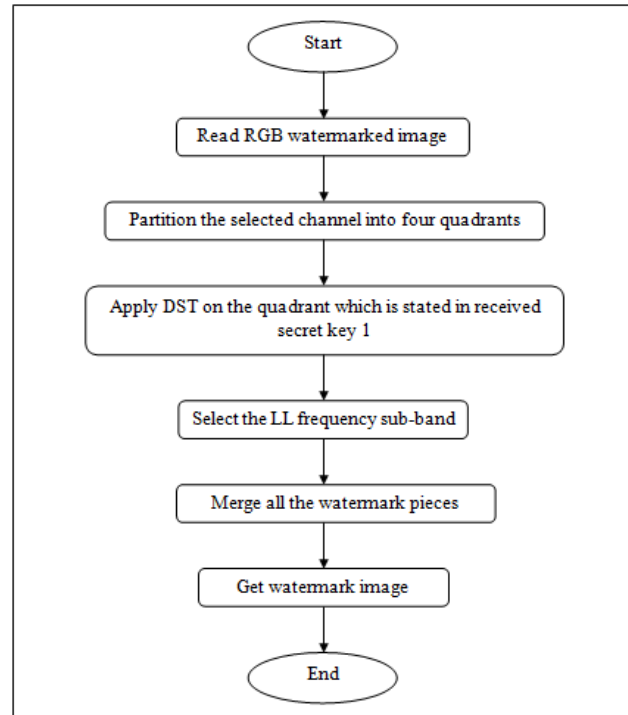


Fig. 10: Extraction stage

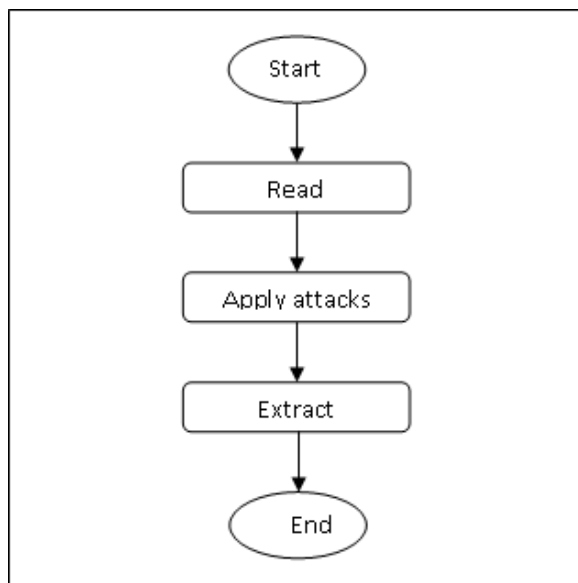


Fig. 9: Attacks stage

algorithm of watermark extraction as following:

- 1.Split watermarked image into Red, Green and Blue components.
- 2.Partition the selected channel of watermarked image into four quadrants.

- 3.Apply DST algorithm on the quadrant which is stated in the received secret key 1.
- 4.Select the LL frequency sub-bands for extraction.
- 5.Extract watermark pieces from the selected sub-band based on actual locations of watermark pieces as formula below:

$$Y_i = (W'_i - W_i) / \alpha$$

Where:

Y_i = Extracted watermark.

W'_i = Coefficients of watermarked image.

W_i = Coefficients of partitioned original image.

α = Alpha, the strength of the watermark image.

- 6.Covert back the watermark image in frequency domain to spatial domain and finally get the bit stream of watermark image.
- 7.Combine all watermark pieces in correct sequence based on the secret key.
- 8.Apply IDST on the selected quadrant to convert from frequency domain to spatial domain image.
- 9.Merge all quadrants.
- 10.Merge all channels to get the host image.

3.6 Robustness Measurement

To evaluate the correlation between original and extracted watermark images, we used the following relation.

$$NCC = \frac{\sum_i W_{ij} \sum_j W'_{ij}}{\sum_i \sum_j (W_{ij})^2} \quad (2)$$

Where W_{ij} and W'_{ij} represent position for actual & extracted images such that .

4 Implementation

Actually, image size used in the experiments is images where the watermarks size is pixels as exhibited in Figure 11. Consequently, the original image and watermarked image is quite similar such that we are unable to differentiate them with open eyes. Watermark should be embedded in host image without degradation and the watermark is able to extract from watermarked image as Figure 12.



Fig. 11: Lena original image and watermarked image



Fig. 12: Embedded watermark image

4.1 Imperceptibility Testing

In fact, PSNR is concerned with class of watermarked image [9]. The output of imperceptibility testing is a value in decibel scale. The PSNR is calculated as below:

$$PSNR = 10 \times \log_{10} \left(\frac{MAX^2}{MSE} \right) \quad (3)$$

The equation computes the maximum possible value using 8 bits plane.

$$MAX = 2^8 - 1 = 255 \quad (4)$$

MSE is the mean squared error for gray scale images I and K which is defined as:

$$MSE = \frac{1}{m \times n} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [(I_{ij}, K_{ij})]^2 \quad (5)$$

Where, $m \times n$ = Size of original host image and watermarked image

I_{ij} = Pixel value of original host image

K_{ij} = Pixel value of watermarked image

Larger PSNR value will indicate that high watermarked image quality. Normally, it must exceed 30db such that it will prove the good quality of watermarking technique which is pointed out in [3]. The Blue is the most suitable channel in the process as the PSNR value of watermarked image is the highest compared to the result of embedding the watermark into the other channels.

5 Results and Analysis

This paper has presented initial results of the proposed watermarking technique. Four well-known attacks namely, Salt and Pepper and Poisson noises are performed onto the watermarked image to determine its robustness. Several embedding and extraction were performed using standard cover images which Lena are exhibited in Figure 13, 14, 15. The watermark image under experiment is a gray scale image namely UTM logo. PSNR and NCC are two benchmark criteria to evaluate the proposed technique. Accordingly, PSNR and NCC values before, after attacks are computed for the watermarked image [11].



Fig. 13: Lena image

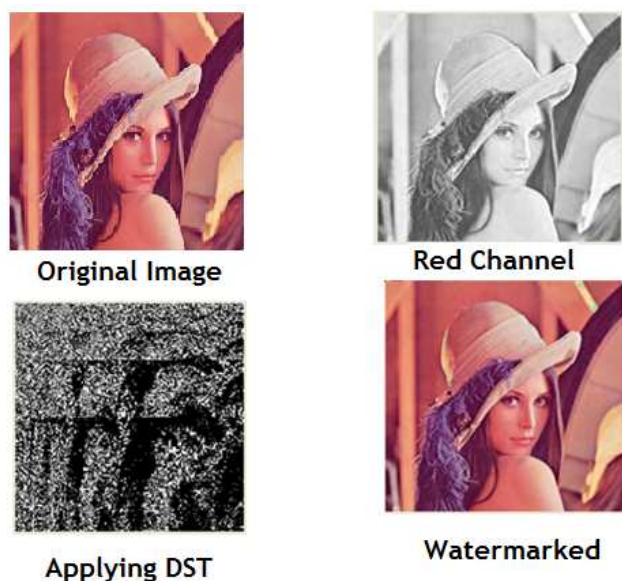


Fig. 14: Comparison




Channel	Selected part	Watermarked Image	PSNR(db)
Red	LL2		45.32
Green	LL4		53.35
Blue	LL4		58.97

Fig. 15: Sample results of PSNR

6 Conclusion

This paper has presented watermark approach embedded in the cover image using discrete slantlet transform. The image is converted into three channels Red, Green and Blue. Finally, 2-level Discrete Slantlet Transform (DST) for each one is applied by choosing the best channel for embedding. The achieved results thus exhibit that is the best channel is Blue. Finally, Discrete Slantlet Transform is a new technique being employed to ensure the imperceptibility and robustness of watermarked images. The authors are grateful to the anonymous referee for a careful checking of the details and for helpful comments that improved this paper.

References

- [1] Tsai, M. J., Yu, K.Y. and Chen, Y.Z.(2000) Joint wavelet and spatial transformation for digital watermarking, *IEEE Trans. on Consumer Electronics*, **46**, 241-245 (2000).
- [2] Wu, C. W. One the design of content-based multimedia authentication systems, *IEEE Trans. on Multimedia*, **4**, 385-393 (2002).
- [3] Dharwadkar, N. V. and Amberker, B.B. watermarking scheme for color images using wavelet transform based texture properties and secret sharing, *international journal of information and communication engineering*, (2010).
- [4] I. J. Cox, M.I. miller and J. a. Bloom, J. Fridrich, T. Kalker, *digital watermarking and steganography*, second edition, morgan kaufmann publishers, (2008).
- [5] RR.Chandramouli, G.Benjamin, and R.Collin A multiple description framework for oblivious watermarking, in *Proceedings of Security, Watermarking and Multimedia*, **4314**, 585-593 (2001).
- [6] P.Premaratne, A novel watermark embedding and detection scheme for images in DFT domain, *Proceedings of IEE 7th International Conference on Image Processing & Applications*, **2**, 780- 783 (1999).
- [7] D.Kundur and D.Hatzinakos, Digital watermarking using multiresolution wavelet decomposition, *Proceedings of IEEE International conference on Acoustics, Speech and Signal Processing*, Seattle, Washington, **5**, 2969-2972 (1998).
- [8] T.S.Ho.Anthony, J.Shen, S.H.Tan, and A.C.Kot, Digital image-in-image watermarking for copyright protection of satellite images using the fast hadamard transform, *IEEE International Geoscience and Remote Sensing Symposium*, **6**, 3311-3313 (2002).
- [9] M.Jayalakshmi, S.N.Merchant, and U.B.Desai, Digital watermarking in contourlet domain, *18th International conference on Pattern Recognition*, **3**, 861-864 (2006).
- [10] B.C.Mohan and S.S.Kumar, A robust image watermarking scheme using singular value decomposition, *Journal of Multimedia*, **3**, 7-15 (2008).
- [11] Ibrahim Nasir, Ying Weng, and Jianmin Jiang, "novel multiple spatial watermarking technique in color images," *fifth international conference on information technology: new generations*, 777-782 (2008).
- [12] Friedman. G. l., The trustworthy digital camera: restoring credibility to the photographic image. *IEEE Transactions on consumer electronics*, **39**, 905-910 (1993).
- [13] Cheng-qun, Li Li, An-Qiang Lv and Li Qu, Color Image Watermarking Algorithm Based on DWT-SVD, *International conference on Automation and Logistics*, August 18-21, (2007).
- [14] Yusnita Yusof and Othman O. Khalifa, Digital Watermarking For Digital Images Using Wavelet Transform, *Proceedings of the 2007 IEEE International Conference on Telecommunications and Malaysia International Conference on Communications*, Penang, Malaysia, (2007).
- [15] Navas K A, Ajay Mathews Cheriyan, Lekshmi. M, Archana Tampy.S, Sasikumar M, *DWT-DCT-SVD Based Watermarking 3rd International Conference on Communication Systems Software and Middleware and Workshops*, (2008).
- [16] Kuo-cheng Liu and Chun-Hsien Chou, Robustness comparison of color image watermarking schemes in

- uniform and non-uniform color spaces, IJCSNS International Journal of Computer Science and Network Security, **7**, (2007).
- [17] Gonzalez, R. C. and Woods, R. E. Digital Image Processing. Prentice Hall. (2008).
- [18] Saba, T. and Altameem, A. "Analysis of Vision based Systems to Detect Real Time Goal Events in Soccer Videos", Applied Artificial Intelligence, **27**, 656-67 (2013).
- [19] Rehman, A. and Saba, T. (2012). Evaluation of Artificial Intelligent Techniques to Secure Information in Enterprises. Artificial Intelligence Review, DOI:[10.1007/s10462-012-9372-9](https://doi.org/10.1007/s10462-012-9372-9).
- [20] Saba, T. and Rehman, A., Effects of Artificially Intelligent Tools on Pattern Recognition, International Journal of Machine Learning and Cybernetics, **4**, 155-162 (2012).
- [21] Saba, T. and Rehman, A., Machine Learning and Script Recognition, Lambert Academic Publisher, ISBN-10: 3659111708, pp: 114-130 (2012).
- [22] Rehman, A. and Saba, T. Neural Network for Document Image Preprocessing Artificial Intelligence Review, DOI: [10.1007/s10462-012-9337-z](https://doi.org/10.1007/s10462-012-9337-z), (2012b).
- [23] Rehman, A. and Saba, T., Features extraction for soccer video semantic analysis: current achievements and remaining issues. Artificial Intelligence Review, DOI: [10.1007/s10462-012-9319-1](https://doi.org/10.1007/s10462-012-9319-1), (2012).
- [24] M.S.M. Rahim, T.Saba, F. Nayer, A.Z. Syed, 3D Texture Features Mining for MRI Brain Tumor Identification, 3D Res, **5**, DOI: [10.1007/s13319-013-0003-2](https://doi.org/10.1007/s13319-013-0003-2), (2014).
- [25] K.Neamah, D.Mohamad, T. Saba and A. Rehman, Discriminative Features Mining for Offline Handwritten Signature Verification, 3D Research, **5**, DOI:[10.1007/s13319-013-0002-3](https://doi.org/10.1007/s13319-013-0002-3) (2014).



Myasar Mundher has done his graduation in computer science from University of Kufa in 2010 and currently is master student in information security in Faculty of Computing Universiti Teknologi Malaysia, Johor Malaysia. His research

interests include pattern recognition and features mining.



Dzulkifli Mohammad is a senior professor in the Faculty of Computing Universiti Teknologi Malaysia (UTM) Johor Malaysia. His keen research interest are intelligent features mining, Pattern Recognition and Security. He has supervised several Master

and PhD students in the field of Computer Science and Information Security. He is author of more than 300 publications that are published in world class conferences and journals of international repute.



Amjad Rehman earned PhD in Image Processing and Pattern Recognition from Universiti Teknologi Malaysia, Malaysia in 2010. During his PhD, he proposed novel techniques for pattern recognition based on novel features mining strategies. He is author of dozens of papers published in international journals and conferences of high repute. His keen research includes information security, data mining and documents analysis, recognition. Currently, three PhD students are conducting research under his supervision.



Tanzila Saba earned PhD in Document Information Security and Information Management from Faculty of Computing Universiti Teknologi Malaysia (UTM), Malaysia in 2012. Her research interests include Intelligent Data Mining, Forensic Documents Analysis and Information Security. She won 2012 best student award in the faculty. Currently, she is serving as Assistant Prof. in College of Computer and Information Sciences Prince Sultan University Riyadh KSA. Her more than twenty research papers are ISI/SCIE indexed. Due to her excellent research achievement, she is included in Marquis Whos Who (S & T) 2012.



Firdous Kausar is currently working as an Assistant Professor in the Department of Information Sciences, College of Computer and Information Sciences, Imam University, Riyadh, Saudi Arabia. She received her Ph.D. in Information Security from National University of Sciences and Technology, Pakistan in 2009. Dr. Kausar has served as a reviewer of several international conferences and journals. She is editorial board member of Future Technology Research Association Publishing. In addition, she served as a Guest Editor for Special Issue on: Advances in Communication Networks for Pervasive and Ubiquitous Applications, Journal of Supercomputing, Springer, 2011. Her research interests are in Cryptography, Cryptanalysis, Information Security Management, Ubiquitous Computing, Network Security, Digital Forensics, Sensor Networks, Mobile and Ad hoc Networks.