

Arabic text images watermarking: a survey of current techniques

Yasmeen Sayaheen

Jordan University for Science and Technology

Irbid, Jordan

yosayaheen@cit.just.edu.jo

Sawsan Al-odibat

Jordan University for Science and Technology

Irbid, Jordan

Smalodibat15@cit.just.edu.jo

Abstract

Digital media has many challenges today such as the violation of copy and paste, illegal use, and weak copyrights protection. Digital watermarking comes to solve these problems by making authority information hidden in digital media. This survey presents a discussion of watermarking for text image especially Arabic text images. This survey talks about Arabic text digital watermarking techniques: Discrete Wavelets Transform (DWT), Discrete Cosine Transform (DCT), Singular Value Decomposition (SVD), Spatial domain watermarking and Frequency domain watermarking.

Keywords—*watermarking; Arabic text; style; authority security; watermarking technique*

I. INTRODUCTION

Digital multimedia technologies are rapidly upward, and throw this growing it bringing significant attraction to the security discipline [4]. There are three security mechanisms used widely in literature; these mechanisms are cryptography, steganography and watermarking. The last two mechanisms are a little bit hard to apply since they are interrelated and interconnected with other concepts and can mix with different disciplines [7].

Watermarking is the process of adding an authority signature inside variety of media such as audio, video, image and text. Watermarking first inserts a watermark object in the embedding phase, next the

detection of this object occurs in the extraction phase. Figure 1 shows watermarking phases across variety of media [17].

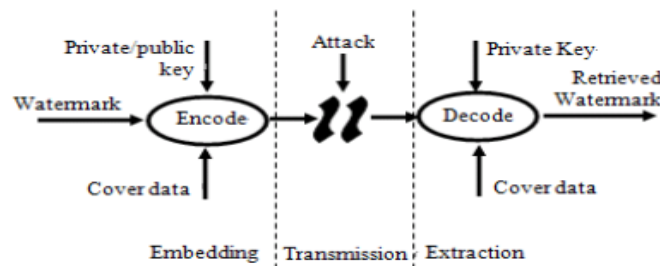


Figure 1: Watermarking phases

Several watermarking categories are realized in regard of digital media watermarking including image watermarking, video watermarking, audio watermarking, text watermarking, and graphic watermarking [2].

Multimedia copyright protection by watermarking techniques is widely deployed to protect copyrights of specific media and to identify any illegal copy or use. Watermarking category including image watermarking inserts data “bits” into images’ pixels to protect authors' copyrights and intellectual properties. Video watermarking and audio watermarking add the identify signal to audio and video frames, whereas, text watermarking adds data inside character shape contained in the image to prove authority [4].

Generally, watermarking goes through two phases, insertion (encoding) and extraction (decoding), that comprise of three main components [17]:

- The watermark (data object)
- The embedding algorithm that inserts the watermark into the object
- The decoder that verifies, detects, and extracts the watermark.

In this research, we provide an explanation of different types and methods used in watermarking. This research focuses on the review of watermarking in digital images containing Arabic texts by examining detailed surveys on watermarking media tools. This section will provide a review analysis of several researches in literature containing current used watermarking and cluster them into sub categories according to methods and domains. Thus, this section will review some proposed methods by prior studies for watermarking in text image.

II. ARABIC TEXT IMAGE WATERMARKING

Securing digital content becomes a challenge task specially those published and transmitted over internet. Storing and transferring digital media are major challenges in data security and protection. Securing text on the internet becomes the dominant requirements over our communications, so it needs to be securely stored and transferred [3]. The main use of image watermarking is to protect intellectual property, copyright, original copy, purchasing identity, digital signature, and author information from illegal use [17].

Text image watermarking approaches have presented a set of adopted techniques, including character coding, line shift, and word shift. Text image watermark uses grayscale image for digital watermarking by utilizing most significant bits in the original image pixels such as LSB. Grayscale image and binary image are used as watermarking media to embed it with watermarked data [1].

Previous work on digital text watermarking has been categorized into different approaches: image-based approach, syntactic approach, and semantic approach. Several digital text watermarking techniques have been proposed in the past, including acronym based, synonym based, noun-verb based, word-sentence based, presupposition-based, and text watermarking using text image. Some examples of text watermarking using image-based approach have been proposed to embed data into text images by inserting it between words spaces and lines.

Digital watermarking methods dedicated to text images are very limited, compared to many previous proposed methods in digital watermarking for texts, images, audios, and videos. The main reason that the binary representation of images texts has rich white spaces and any change of the grey areas can be observed by human vision [13]. The type of text image watermarking is concerned with embedding data into images to protect authors' copyrights. Image watermarking can be extended to video watermarking that requires strong compression techniques; this technique can be valuable to manage applications containing videos. The hot issues of the music property on the internet can be resolved by the audio watermarking that applies great standards [2].

Arabic texts are extensively used, so they need to appropriate methods to preserve privacy and enforce security. Most text watermarking methods are easy to implemented with the highest rate of robustness and capacity. Certainly, in Arabic digital text appearance such as Holly Quran, the demonstration is so important in today digital texts. Additionally, the Unicode methods presenting watermarking with high imperceptibility are still only limited to digital texts [5].

Arabic text difficulties regarding recognition and segmentation features are:

- The variety of shapes of Arabic characters, depending on the character position within a word. An Arabic character can appear stand alone, at the beginning of the word, in the middle, or at the end of the word.
- The way of writing is completely different from one writer to other according to various conditions, using different Arabic characters.
- Many characters have unique shapes, while others have very similar shapes making them difficult to recognize whether they represented in external objects or non-character.
- The contextual information effects on the handwritten Arabic characters, depending on the classification of characters and their position in a word or sentence.

The requirements of watermarking techniques are different based on the data types and the used application of watermarking. Mainly, they should include “robustness”, “security”, “Imperceptibility” and

“capacity”. The robustness requirement denotes to have the ability of avoiding all kinds of modification and distortion that can effect hatefully such activity of data files or discard its quality. Additionally, it applies the watermark to discover any data theft. The security feature can be got by applying “cryptographic” key to keep data hidden from illegal discovery. However, the capacity is much hard to be attained since it tries to Unicode enough amount of information as bits in a reasonable amount of time using hiding techniques. Imperceptibility requirement should not destroy the original text after watermarking it under hidden cover text, meaning that the original text can be retrieved in a short amount of time and with small changes [5].

III. ARABIC TEXT IMAGES WATERMARKING

Digital media protection from unauthorized access or use has become much required necessity with the rapid increasing of technologies and applications on the internet. For this purpose, Arabic text watermarking can be used to strengthen the security of Arabic text files that consist of different Unicode of shapes and types of letters. From literature, there are different approaches of Arabic text watermarking have been discussed and compared in terms of robustness, Imperceptibility, capacity, and their advantages and disadvantages [5].

Variety criteria are measured when classifying watermarking techniques such as robustness, which assurances that watermark can care the popular operations of image processing. According to ability to watermark to resist attack, digital watermarking types are Fragile watermarking and Semi-fragile watermarking [11]. However, the strength of watermarking technique can be further classified into other groups such as “fragile, semi-fragile, and robust” [2].

In this manner, we investigate some popular watermarking types of Arabic text images including Kashida-based watermarking, spatial domain watermarking, frequency domain watermarking and many others. We will discuss and evaluate each individual type or technique during the following sections in order to state our conclusion.

A. *Kashida-based watermarking*

Kashida is an extending character that can be utilized in all characters that can be extended to be appropriate to insert bits inside words.

The authors of [18] have purposed a method to review and evaluate the existing watermarking applications to identify their properties according to Arabic text documents and other Semitic languages. The paper has evaluated different approaches of embedding digital watermark, but it mainly explored Kashida-based watermarking, that cover digital texts such as copyright protection, content authenticity, and tamper detection. Moreover, it investigated the impact of using two watermarking parameters: the number of embedded bits in each group and the group size or word group. The proposed method examined different applications of cover text to address the effects of these two parameters on watermarking capacity and imperceptibility properties. The findings of the paper have clarified that Arabic texts are likely to be

considered the optimal to accomplish an adequate level of imperceptibility and to achieve the required capacity of the application by counting these two variant parameters in Arabic text watermarking [18].

In the work of [3], a proposed technique of Kashida watermarking was introduced. Kashida omits zero bits and place a bit for ones, where the watermarking key is predefined. The invisible technique of this work utilized Kashida to fully embed the entire key by inserting Kashidas before a specified list of characters in the text. The proposed method has developed two variations of characters' properties based on their frequency recurrence. The main advantage of using frequency recurrence in this method was the dynamic enabling of the target application robustness and imperceptibility. The main goal of the proposed method was to improve the perceptual similarity and robustness in order to protect the documents authenticity. The new method proposed in this work purposed to enhance authentication, verification, and document copyright protection. At the same time, it intended to reduce security attacks vulnerabilities of Arabic text watermarking.

The proposed method in [12] has utilized all characters that can be extended to be appropriate for bits illustration of words. Kashida based method uses the extension of Arabic letters with dots to hide 1 bit and uses Arabic letters without dots to hide 0 bit, added before or after the letter without affecting the original content. The method included traditional cryptography to choose the secret key in order to insert bits of Arabic e-texts using “Kashida” character. The results of this paper proved that the proposed method when it compared with other previous methods. Additionally, the proposed method can be applied for authentication to protect other watermarking methods in order to notice any adjustment alter the file.

B. Digital watermarking techniques

Recently, there are many presented digital watermarking techniques; these techniques are based on Discrete Fourier Transforms (DFT), Discrete Wavelets transform (DWT), and, Discrete Cosine Transform (DCT). DCT and DWT are mostly used by the domain transformation watermarking techniques [20]. Digital watermarking techniques are commonly applied in the transform domain larger than spatial domain.

DWT technique works by dividing the image into four areas based on coefficient value of non-overlapping area as shown in figure 2.

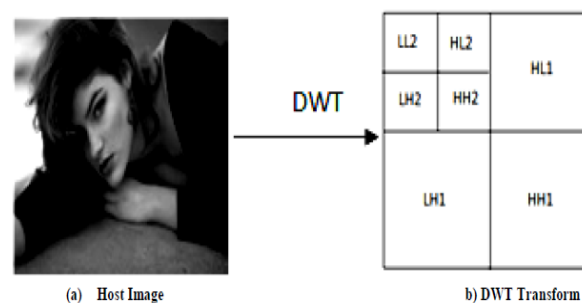


Figure 2: DWT technique

In contrast, DCT divides the image into three pieces: low, middle and height frequency as show in figure 3.

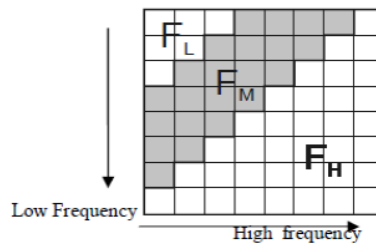


Figure 3: DCT technique

Another discrete transform called singular Value Decomposition (SVD) is a powerful numeric analysis technique that is mostly used in several watermarking techniques. The use of SVD is frequent in many useful statistical and signal processing as one of mathematical techniques that analyse complex matrices using linear algebra. Moreover, it can be seen as a data reduction method due to the transformations of different correlations between variables inside a matrix [20].

The proposed watermarking algorithm in [20] was designed to utilize Singular Value Decomposition (SVD) in digital watermarking techniques. It consists of two procedures; the first is for embedding and the second for extraction. In general, the robustness of digital watermarking techniques is highly obtained in images watermarking especially in copyright protection [20].

According to the domain of watermark insertion, digital watermarking types are “Spatial domain” watermarking techniques and “Transform frequency domain” technologies [11].

C. Spatial domain watermarking techniques

There were many proposed algorithms of image watermarking to protect copyright. The spatial domain watermarking directly embed a watermark into the digital images by modifying pixels. However, recently, the main focus of researches is on spectrum domain watermarking, transforming the digital image to spectrum domain by modifying the spectrum of coefficients in order to embed a watermark [4].

Spatial watermarking applies the algorithm on color bands by separating them visibly which is hard to be detected regularly. After the colors separated, the mark appears immediately. The main use of spatial watermarking is in commercial journals, in order to embed digital images with a specific marking data [10]. Spatial domain watermarking alters images' pixels by changing their bits' order, but it this technique is not reliable for lossy compression and filtering. Frequency domain techniques use invisible image watermarking; these techniques have frequency factor which might neglected by compression [2].

The three invisible text-watermarking techniques proposed in [18] have presented newest watermarking encoding methods to involve them in Arabic text. There were some considered fixed values in the paper: using 48 bits watermark key, inserting the watermark at least once, testing large size documents, dividing based on a set of words, considering the number of words to indicate the size, and embedding texts

according to circular or spatial methods [18]. Typically, high “imperceptibility” indicates of low “capacity”, but according to the results of this paper, the number of words in each group (the number of embedded bits) has produced high “capacity” as well as high “imperceptibility”. Certain level of embedded bits of all methods investigated in the paper made them proper to be used in a wide range of copyright and other applications [18].

In terms of spatial domain, a new way for medical images watermarking has been proposed in the study. This type of watermarking has been employed for medical images to swap between pixel values of image's gray level watermark. The new proposed image watermarking can hide data based on the image size, while the difference between watermarked and the original image is trivial and cannot be noticed. Moreover, this method can transfer information content by combining different watermarked documents and images. The advantage of this way is the inability to access watermarked documents and their decryption key, so it is difficult to modify the original image content. The watermarking technique used for patients' images efficiently utilizes memory, cost, and time required for data transmission. Therefore, by encryption of watermarked information, this way protects the privacy of patients. At present, the focus is moving to work on visible watermarks to enhance image watermarking and covering.

D. Frequency domain watermarking techniques

Watermarking techniques provided in the frequency domain also called Spread spectrum are more beneficial considering invisible embedded watermark [2]. The basic principle in frequency domain is the modification of DCT coefficient value to embed watermarking. [8]. Frequency domain (transform domain) applies on frequencies values such as Fast Fourier (FFT) that modifies the chosen frequencies by altering their original values. When the watermarking is hidden and destroyed into the host, then it can be called fragile watermarking [10]. Spread spectrum communication technique is commonly used by most frequency domain algorithms. They use larger bandwidth for total power signal transmission [15].

In the work of [19], in each level of decomposition in frequency domain, the image is divided into four segments; Horizontal Level (HL), Vertical Level (VL), Diagonal (HH), and Approximation (LL). The input signal of DWT decomposition should be multiplied by 2^n . Where n is the number of current level. Watermark is embedded into these four regions, providing sufficient information, less computational time, and increase robustness. DCT transforms the signals from spatial domain to frequency domain, according to its high robustness compared to spatial domain techniques. However, we need to 2D version of DCT to analyze 2D dimensional of signals [19].

E. Visible and invisible watermarks

Watermarking process can be done visibly or invisibly. According to the visibility, digital watermarking types are visible watermark and invisible watermark [11]. The main difference between visible and invisible watermark refers to the ability of user to perceptually notice the embedded watermark.

The method of [12], as a type of visible watermarking, hides a secure data of Arabic digital text in web applications. This work has explored several planned text watermarking techniques that cannot be

generalized to Arabic language but they are good only for English. The main goal was the special cases of Arabic language including distinctive characteristics and features of Arabic e-text watermarking. These characteristics have been taken in consideration in using “Kashida” Character comprehensive to enhance Arabic e-text watermarking methods.

F. Blind and non-blind watermark

According to watermark detection and extraction Digital watermarking types are Blind watermarking techniques that require the original image to extract watermark and Non-blind watermarking technique that does not require the original image [11].

According to the data required to extract, digital watermarking can be partitioned into two kind of watermarking: private watermarking and blind watermarking. Private or informed watermarking requires the original un-watermarked cover to extract watermarking. While blind or public watermarking does not require the original un-watermarked cover to extract watermarking [10]. The best examples of the digital watermark applications (visible watermark) are enhancing copyright protection and indicating the ownership of original copies. While the detecting misappropriated images is an application of invisible digital watermark. Lastly, invisible-fragile watermarking can be used to trust worth the origin of images captured by digital cameras by embedding capturing time [17].

One of blind text watermarking methods has been presented in [9] using the common characteristics of Persian language letters. The type of blind text watermarking used in this method exploits the majority of Farsi words containing sloping letters by changing their slope to hide information into text (as shown in figure). This method can be applied on Arabic and Urdu texts due to the noticed similarities over them. Compared with line shifting and word shifting, this method has been proved by experiments showing the highest capacity and imperceptibility obtained. Moreover, the ability to apply in several applications also can be obtained by using this method to authenticate users, protect copyright etc.

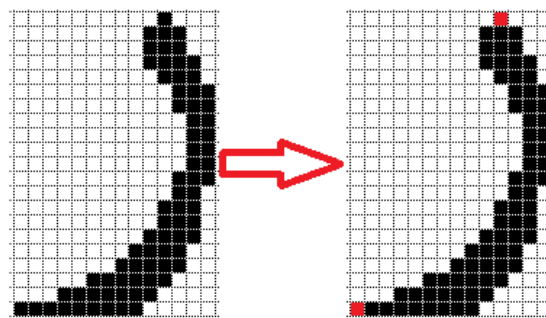


Figure 4: data hiding in the sloping of letters

IV. ANALYSIS AND DISCUSSION

The most effective solution to achieve artificial intelligence and protect information is the use of digital image watermarking. The methods of watermark have large problems if they destroy the original

watermarked file even they are simple to implement. Digital image watermarking is also robust against several types of attacks according to the strong resistant and the quality of digital watermarking [20].

The vulnerabilities in literature of Kashida approaches including security attacks have been considered the highest rates of encoding and embedding of watermarking applications. The results also showed that this method was fast, simple, and can be manually implemented since it does not need to big working out it increases the difficult of hacking tasks. Moreover, it can secretly hide digital texts data application with more security, increasing the protection and demonstrating of copyrights, ownership and knowledgeable properties. Whenever the attacker wants to remove the inserted “Kashida” from the file after watermarking it, it will be much solider to return the generated random values of secret key of the original “Kashidas” to repaire the text. Accordingly, the attacker will not be able to fraud of ownership to change the normal ownership watermark [12].

On the other hand, Spatial domain is simple, no need to frequency transform, and has low computing complexity to change the intensity of the gray image pixels. Spatial domain cannot be easily attacked by image processing and noise, so it makes a tradeoff between robustness and invisibility. Popular spatial domain techniques such as Least Significant Bit (LSB) and Texture Block Coding (TBC) have a significant drawback which is the limitless of its robustness. Frequency domain has complicated and sophisticated approaches [15]. Spatial domain applications can be done easily with minimal computational power requirements. Spatial domain methods work on direct modification of pixel values by modifying colors and brightness values based on simple, efficient, and computational modifications [6]. The approaches operating in spatial domain directly work on the image pixels, while other approaches operating in frequency domain perform transformations on the image. The watermarking algorithms operating in frequency domain overcome the robustness problems existed in the watermarking algorithms that represent low resistance, and limited robustness against attacks. On the other hand, the algorithms of spatial domain are more suitable for real-time applications, requiring less computation and complexity [14]. In spatial domain, the most used approach is to replace the least significant bits of the original image with watermarks bits. However, this approach cannot hide large number of bits in an image, and thus it can alter the quality of an image caused by the lack of pixel dependency in most efficient watermarking techniques. Frequency domain techniques have dealt this issue, depending on the Human Visual System (HVS) characteristics that can be captured better by frequency domain. The signal is divided into two sets; high frequency and low frequency in the case of one-dimensional signal. High frequency set remains unchanged, but low frequency set so therefore divided into other subsets until the desired level [16].

In DWT, the watermark embedded is not robust against JPEG attacks if it embedded into high frequency region. While if it embedded into low frequency regions, it will destroy the entire image [8]. Frequency domain should be applied to lower frequencies or in the most important frequencies that carry useful information in order to avoid frequency loss during scaling or compression. Signal transmission can be recovered even though after losing several bands. Spread spectrum communications are used in digital spread spectrum watermarking schemes to embed watermarks in the whole host image [15]. The most used

techniques in transform domain is DCT, while DWT is also a popular spatial based technique. DCT can be applied in international standards of compression techniques such as MPEG and JPEG. DCT should balance between the precision and the speed of operation of feature vector extraction [21]. The multiple advantages of SVD make it the mostly used by digital watermarking techniques. For instance, the non-fixed size of SVD transmission memory can be represented in a square or a rectangular which decrease the size of required memory and increase the accuracy. SVD has the algebraic properties that minimize the affection of the singular values of digital images in general image watermarking [20].

Lastly, we add last point regarding our comparison between spatial and frequency domain. Frequency domain gains more attention due its high robustness and common usability in image compression. In frequency domain, the image is partitioned into 8x8 blocks, and they are selected based on Gaussian network classifier decision. After that, the frequency coefficient values are altered by DCT [15].

V. CONCLUSION AND FUTURE WORK

Some approaches involve text watermarking algorithms that rely on the language so their applicability is limited. Thus, some documents with different types and sizes have sensitive nature of text image in a way cannot be transformed due to a robust protection. However, the best approach should be flexible to the structure of text content such as the spelling, grammar rules, and acronyms of sentence structure that include letters, spaces, shapes, and white spaces. Therefore, good approaches exploit these text images components to insert and embed data into objects without affecting the size and quality of the text image. In conclusion, watermarking techniques presented by this research are not absolute; they suffer from some issues need to resolve. In future, we intend to develop one of the investigated watermarking techniques in order to enhance their performance in the regard of data protection from illegal use. For example, we can optimize Arabic letters contained in text images to insert watermark that can protect the authority of the producers or owners.

Acknowledgment

We specially thank Dr. Mohammad Isaleh for his assistance and comments that greatly improved this work, and we are thankful to our parents for their support.

References

- [1] Abraham, J. and Paul, V. (2001). Watermarking grayscale images using text for copyright protection. International journal of computer applications, pp.9-12.
- [2] Agrawal, K. and Singh, R. (2015). A Survey: Digital Watermarking with its Applications Using Different Methods. International Journal of Digital Contents and Applications Vol.2, No.1, pp.17-24.
- [3] Alginahi, Y. and Kabir, M. and Tayan, O. (2014). An Enhanced Kashida-Based Watermarking Approach for Increased Protection in Arabic Text-Documents Based on Frequency Recurrence of Characters. International Journal of Computer and Electrical Engineering Volum 6, Number 5.

- [4] Al-Haj, A. M. (2010). Advanced techniques in multimedia watermarking: image, video and audio applications. Princess Sumaya University for Technology, Jordan. Information science preference, New York.
- [5] Alotaibi, R. Elrefaei, L. (2015). Arabic Text Watermarking : A Review. International Journal of Artificial Intelligence and Applications (IJAIA) Vol. 6, No. 4, July 2015 DOI: 10.5121/ijaia.2015.6401 1.
- [6] Asatryan, D. and Asatryan, N. (2009). Combined spatial and frequency domain watermarking. In Proceedings of the 7th International Conference on Computer Science and Information Technologies (pp. 323-326).
- [7] Cheddad, J. Codell, K. Curran, and P. Mc Kevitt. (2010). "Digital Image Steganography: Survey and Analysis of current Methods". Signal Processing, Volume 90, Issue 3, Pages 727-752.
- [8] Chen, H.C., Chang, Y.W. and Hwang, R.C. (2012). A watermarking technique based on the frequency domain. Journal of multimedia, 7(1), pp.82-89.
- [9] Davarzani, R. and Yaghmaie, K. (2009). Farsi Text Watermarking Based on Character Coding. International Conference on Signal Processing Systems. 2009 IEEE. DOI 10.1109/ICSPS.2009.28.
- [10] El-Gayyar, M. (2006). Watermarking Techniques, Spatial Domain, Digital Rights Seminar. University of Bronn Germany: Media Informatics.
- [11] Gunjal, B.L. and Manthalkar, R.R. (2010). An overview of transform domain robust digital image watermarking algorithms. Journal of Emerging Trends in Computing and Information Sciences, 2(1), pp.37-42.
- [12] Gutub, A. Al-Haidari, F. Al-Kahsah, K. and Hamodi, J. (2008). e-Text Watermarking: Utilizing 'Kashida' Extensions in Arabic Language Electronic Writing.
- [13] Huang, D. and Yan, H. (2001). Interword distance changes represented by sine waves for watermarking text images. Circuits and Systems for Video Technology, IEEE Transactions on, 11(12), pp.1237-1245.
- [14] Laouamer, L. and Tayan, O. (2015). A Semi-Blind Robust DCT Watermarking Approach for Sensitive Text Images. Arabian Journal for Science and Engineering, 40(4), pp.1097-1109.
- [15] Liu., (2005). A survey of digital watermarking technologies. Department of Electrical and Computer Engineering, State University of New York at Stony Brook, NY, pp.11794-2350.
- [16] Leena, G.D. and Dhayanithy, S.S. (2013). Robust image watermarking in frequency domain. International Journal of Innovation and Applied Studies ISSN, pp.2028-9324.
- [17] Mohanty, S. P. (1999). Watermarking of Digital Images. Master thesis, Department of Electrical Engineering.

- [18] Muhammed, K. Alginahi, O. Tayan, N. and Yasser, M. (2013). Evaluation of Watermarking Approaches for Arabic Text Documents. International Journal of Computer Science and Information Security 11.3 (Mar 2013): 49-54.
- [19] Rahman, M.,(2013). A DWT, DCT and SVD based watermarking technique to protect the image piracy. arXiv preprint arXiv:1307.3294.
- [20] Thapa, M., Sood, S. K., and Sharma, M. (2011). Digital Image Watermarking Technique Based on Different Attacks. (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 2, No. 4, 2011.
- [21] Wu, F., Huang, M. and Li, J. (2015). Robust Watermarking for Text Images Based on Arnold Scrambling and DWT-DCT.