Development of Efficient Watermarking Techniques for Document Images

THESIS SUBMITTED
FOR THE AWARD OF DEGREE OF

DOCTOR OF PHILOSOPHY

BY

BALKAR SINGH
REGISTRATION NO. 951503002

UNDER THE GUIDANCE OF

DR. MAHESH KUMAR SHARMA
PROFESSOR



COMPUTER SCIENCE AND ENGINEERING DEPARTMENT
THAPAR INSTITUTE OF ENGINEERING AND TECHNOLOGY
PATIALA, PUNJAB, INDIA-147004
FEBRUARY 2022

Certificate

I hereby declare that the work being presented in this thesis titled as **Development of Efficient Watermarking Techniques for Document Images**, in fulfillment of the requirements for the award of degree of **DOCTOR OF PHILOSOPHY** submitted in Department of Computer Science and Engineering, Thapar University, Patiala, is an authentic record of my own work carried out under the supervision of Dr. Mahesh Kumar Sharma, Professor, School of Mathematics and refers other researcher works which are duly listed in the reference section.

The matter presented in this thesis has not been submitted for the award of any other degree of this or any other university.

(**Balkar Singh**)

Registration No. 951503002

This is to certify that the above statement made by the candidate is correct and true to the best of my knowledge and belief.

(**Dr. Mahesh Kumar Sharma**)

Professor

School of Mathematics

Thapar Institute of Engineering and Technology, Patiala

Supervisor

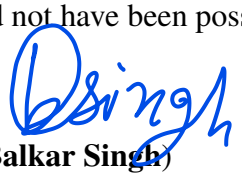
Acknowledgements

Undertaking this Ph.D. has been a truly life-changing experience for me and I would not have been able to complete it without the help and guidance of many people.

I would like to express my sincere gratitude to my supervisor, **Dr. Mahesh Kumar Sharma**, Professor, School of Mathematics, for his consistent support, encouragement and vast knowledge. I am highly indebted to him for invaluable time and efforts he invested in me throughout this research journey. His guidance and patience helped me conducting the research effectively.

I am thankful to my Ph.D. committee which includes **Dr. Maninder Singh**, Professor and Head, **Dr. Jhilik Bhattacharya**, Associate Professor, **Dr. Shreelekha Pandey**, Assistant Professor, Computer Science and Engineering Department and **Dr. Kulbir Singh**, Professor, Electronics and Communication Engineering Department, for keeping track of my progress and giving helpful suggestions to improve my work. I appreciate the assistance and cooperation of the entire faculty and staff of the Computer Science and Engineering Department.

I would like thank my loving mother, **Smt. Sunehari Devi**, for believing in me and encouraging me to achieve my goals. Finally, I'd like to express gratitude to my sister, brothers, sisters-in-laws, my wife **Reena**, and my son **Krishan Kasana** for always being there for me and encouraging me to keep going. Last but not least, I would like to thank God for providing me the courage, the wisdom, the ability and the opportunity to pursue and complete this research. Without His blessings, this success would not have been possible.



(**Balkar Singh**)

Abstract

Watermarking is used in copyright protection and authentication of multimedia data such as text, image, audio , video and document images. Among these media, document images exhibit peculiar characteristics such as binary nature, block/line/word patterning, and clear separation between foreground and background areas. As a result, watermarking techniques are required to address these characteristics of document images.

In this thesis, four watermarking techniques for document images are proposed. The first technique is based on zero watermarking approach. In this technique, Lifting Wavelet Transform is applied on the cover document image to generate its subbands. These subbands are further divided into non-overlapping blocks of same size. A zero watermark is generated by using the features of these blocks. This watermark is combined with the key watermark to create a meaningful watermark. This meaningful watermark is stored with a trusted authority. On the receiver side, a watermark is generated using the received image and compared with the meaningful watermark to check the authenticity of the image.

The second watermarking technique is based on hashing and Zero Width Characters. Hash value of the input image is generated by applying Message Digest 5 on it. A lookup table is used to translate this hash value into Zero Width Characters. Watermark is also translated into Zero Width Characters before embedding in the cover image. The Zero Width Characters are embedded at the end of every sentence. At the receiver side, watermark and hash values are generated from Zero Width Characters extracted from the watermarked image. Watermark value is used for the protection purpose while hash value is used to authenticate the watermarked image.

Third technique is developed on the basis of Markov Matrix and Entropy to detect tamper in

the text images. Entropy of every sentence of document image is calculated and Markov Matrix is generated by using the occurrences of characters of the cover image. Entropy and character patterns values are converted into Zero Width Characters by using a lookup table. Zero Width Character of entropy of each sentence is embedded at the end of every sentence after terminator. Patterns of the Zero Width Characters are embedded in the end of the text of the cover image. On receiver side, Zero Width Characters are extracted from the watermarked image and converted to numerical form using the same lookup table. Entropy of every sentence and character patterns are recalculated and compared with extracted values for tamper detection.

The fourth technique is based on Discrete Curvelet Transform and Discrete Cosine Transform to provide the protection of document images. Discrete Curvelet Transform generates the six layers of the document image. Sixth layer is selected for the embedding process. Discrete Cosine Transform is applied on the 8×8 blocks of the sixth layer and the required number of discrete cosine coefficients are selected in zig zag pattern to embed the watermark bits. Watermark bits are extracted at the receiver side by using the steps used in embedding in the reverse order. In extraction process, watermarked image as well as cover image are required. Imperceptibility and robustness parameters are evaluated to measure resistivity of the watermarked image against image processing attacks.

Experimental results demonstrate the efficiency of the proposed techniques. Comparisons with existing document image watermarking techniques show the effectiveness of the proposed techniques.

Abbreviations

AES	Advanced Encrypted Standard
BER	Bit Error Rate
CA	Certifying Authority
CNN	Convolution Neural Network
DAS	Document Analyzer and Signature
DCT	Discrete Cosine Transform
DCuT	Discrete Curvelet Transform
DES	Data Encryption Standard
DR	Distortion Robustness
DRDM	Distance-Reciprocal Distortion Measure
DSA	Digital Signature Algorithm
ECL	Effective Characters List
ER	Effectiveness Ratio
HF	High Frequency
HVS	Human Visual System
IB	Interlaced Block
IR	Integrity Rate
IWT	Integer Wavelet Transform
LF	Low Frequency
LP	Loosing Probability

LSB	Least Significant Bit
LZW	Lempel Ziv Welch
M	Markov Matrix
MF	Middle Frequency
MOFL	Most Frequently
MP	Matching Pair
MSE	Mean Square Error
NAE	Normalized Absolute Error
NHD	Normalized Hamming Distance
NIB	Non-Interlaced Block
NQM	Noise Quality Measure
PDF	Portable Document Format
POS	Part of Speech
PSNR	Peak Signal to Noise Ratio
QR	Quick Response
RSA	Rivest-Shamir-Adleman
RSE	Render Sequence Coding
SSIM	Structural Similarity Index Modulation
TMR	Text-Meaning Representations
UQI	Universal Quality Index
VIF	Visual Information Fidelity
VIFC	Visual Information Fidelity Criterion
WAT	Wave Atom Transform
WPSNR	Weighted Peak Signal-to-Noise Ratio
WOR	Word Occurrence Ratio
WSR	Word Selection Ratio

Notations and Symbols

b_i	i^{th} Block
CT_w	Watermarked Text Image
p_i	i^{th} Prediction Filter Coefficient
u_i	Updation Filter Coefficient
fw	Meaningful Watermark
G	High pass filters
H	Low pass filters
X_e	Even indexed Subset
X_o	Odd indexed Subset
(M, N)	Size of the image
P_i	Transition Pattern of i^{th} Character of the Text
R	Wavelet Decomposition Level
μ	Average of the pixel values of an Image
σ	Variance of the pixel values of an Image

Contents

Certificate i

Acknowledgements ii

Abstract ii

Abbreviations v

Notations and Symbols vii

List of Figures xii

List of Tables xiv

List of Publications xvii

1 Introduction 1

1.1 Document Image Watermarking 1

1.2 Main Characteristics of a Watermarking Technique 3

1.3 Types of Watermarking Techniques 4

1.4 Image Authentication 6

1.5 Image Protection 7

1.6 Approaches Used for Document Image Watermarking 8

1.6.1 Structural based Document Watermarking Approaches 8

1.6.2 Linguistic based Document Watermarking Approach 9
1.6.3 Image based Document Watermarking Approach 10
1.7 Methodology of the Proposed Work 11
1.8 Thesis Contribution 14
1.9 Thesis Organization 15

2 Literature Survey **17**
2.1 Classification of Document Watermarking Techniques 17
2.2 Zero Watermarking Techniques 18
2.3 Physical Embedding Techniques 27
2.4 Objectives 44

3 Tamper Detection Technique for Document Images using Zero Watermarking in Wavelet Domain **45**
3.1 Introduction 45
3.2 Preliminary 46
3.2.1 Lifting Scheme 46
3.3 Proposed Watermarking Technique 48
3.3.1 Zero Watermark Generation Algorithm 49
3.3.2 Document Image Authentication Algorithm 50
3.4 Experimental Results and Performance Analysis 51
3.5 Conclusion 59

4 Efficient Watermarking Technique for Protection and Authentication of Text Images **61**
4.1 Introduction 61
4.2 Preliminary 62
4.2.1 Unicode Standard based Table 62
4.2.2 Encoding Table 62
4.3 Proposed Technique 63
4.3.1 Embedding Algorithm 64

4.3.2 Extraction Algorithm 65
4.4 Experimental Results and Performance Analysis 67
4.4.1 Invisibility 69
4.4.2 Distortion Robustness 70
4.4.3 Embedding Capacity 71
4.4.4 Prevention Against Malicious Attacks 73
4.5 Conclusion 79

5 Markov Matrix and Entropy based Tamper Detection Technique for Text Images 81
5.1 Introduction 81
5.2 Preliminary 82
5.2.1 Unicode Standard 82
5.2.2 Character Pattern Generation using Markov Matrix 82
5.3 Proposed Technique 83
5.3.1 Embedding Algorithm 84
5.3.2 Extraction Algorithm 85
5.4 Experimental Results and Performance Analysis 86
5.4.1 Invisibility 86
5.4.2 Distortion Robustness 86
5.4.3 Embedding Capacity 89
5.4.4 Prevention against Malicious Attacks 91
5.5 Conclusion 98

6 Discrete Curvelet Transform and Discrete Cosine Transform based Watermarking for Document Images 99
6.1 Introduction 99
6.2 Preliminary 100
6.2.1 Discrete Curvelet Transform 100
6.2.2 Discrete Cosine Transform 102

6.3 Proposed Technique 103
6.3.1 Embedding Algorithm 106
6.3.2 Extraction Algorithm 107
6.4 Experimental Results and Performance Analysis 108
6.4.1 Imperceptibility 110
6.4.2 Robustness 112
6.5 Conclusion 116

7 Conclusion and Future Scope **117**
7.1 Conclusion 117
7.2 Future Scope 118

List of Figures

1.1 A General Watermarking Framework 2
1.2 Characteristics of Watermarking 4
1.3 Blind Watermarking Process 5
1.4 Semi-Blind Watermarking 5
1.5 Non-Blind Watermarking 6
1.6 Image Authentication Framework 6
1.7 Image Protection Framework 7
1.8 Types of Document Watermarking 8

2.1 Document Watermarking Techniques 17
2.2 Classifications of Zero Watermarking Techniques 18
2.3 Classifications of Physical Embedding Watermarking Techniques 28

3.1 Forward Lifting Scheme 46
3.2 Inverse Lifting Scheme 47
3.3 Lifting Scheme Structure 48
3.4 Flowchart of proposed technique 48
3.5 Key Watermark 51
3.6 Original Document Images of DIQA Dataset 52
3.7 Tampered Document Images Corresponding to Original Images of Figure 3.6 53
3.8 Meaningful Watermark corresponding to the images of Figure 3.6 54

3.9 (a)-(i) Watermark Extracted from Corresponding Tampered Images of Figure 3.7 . . 54
3.10 *SSIM* Comparison of the Different Images at Different Block Size 56
3.11 *BER* Comparison of the Different Images at Different Block Size 56
3.12 Extracted Watermark comparison with the existing techniques from Corresponding Tampered Images of Figure 3.7 58

4.1 Text Watermarking Scheme 63
4.2 Original Document Image 1 67
4.3 Watermarked Document Image 1 67
4.4 Watermark Image 68
4.5 Original Images 69
4.6 Tampered Images corresponding to Original Images 69
4.7 Comparison of DR of the Proposed Technique and Existing Techniques 71
4.8 Embedding Capacity of the Proposed Technique Vs Existing Techniques 73
4.9 Tamper Detection Process 74
4.10 Protection Process used in Proposed Technique 76
4.11 Tampered Document Images Corresponding to Original Images of Figure 3.6 78

5.1 Text Watermarking Scheme 83
5.2 Embedding process Example 86
5.3 Deletion Attack Example 92
5.4 Deletion Attack Example 92
5.5 Insertion Attack Example 94
5.6 Insertion Attack Example 94
5.7 Tamper Attack Example 96
5.8 Tamper Attack Example 96

6.1 Frequency wrapping based DCuT 101
6.2 Sixth layer of original document image 102
6.3 DCT Coefficients matrix and frequency bands 102

6.4 Embedding Process 104
6.5 Zigzag process 105
6.6 Extraction Process 105
6.7 Watermarked Document Image Corrsponding to Original Image 108
6.8 Watermarked Document Images Corresponding to Original Images of Figure 3.6 . . 109
6.9 Extraction of Watermark 112
6.10 Extraction of watermark after attacks on the Watermarked Images 113
6.11 Comparison of Extracted Watermark of Proposed Technique with existing techniques 114

List of Tables

2.1 Types of Attacks and Performance Evaluation of Zero Watermarking Techniques . . 26

2.2 Types of Attacks and Performance Evaluation of Physical Embedding Watermarking Techniques 42

3.1 *SSIM* values between original zero watermark and extracted watermark at various block sizes 55

3.2 Bit Error Rate of Various Image at Different Block Size 55

3.3 Robustness Results of Proposed Technique against some attacks 57

3.4 Robustness results of Proposed Technique against *JPEG* Compression Attacks 58

3.5 Comparison of *BER* of Proposed Technique with the Existing Techniques 58

4.1 Unicode zero width characters 62

4.2 Encoding pattern of *ZWC*s 3-bit classification 62

4.3 Encoding Lookup Table 63

4.4 Embedding Algorithm Example 68

4.5 *DR* comparison with the Existing Techniques 70

4.6 Embedding Capacity(in bits) comparison with the Existing Techniques 72

4.7 Tamper Detection Example 74

4.8 Tamper Detection Example 75

4.9 *IR* comparison of the Proposed Technique with the existing Technique 76

4.10 Distortion Robustness 77

4.11 Compression effect with Quality Parameters 79

5.1 Encoding pattern of *ZWCs* 82
5.2 Comparison of *DR* of the Proposed Technique with *DR* of the Existing Techniques . 87
5.3 Comparison of the Embedding Capacity of the Proposed Technique with the Existing Techniques 89
5.4 Deletion Attack Example 91
5.5 Insertion Attack Example 93
5.6 Tamper Attack Example 95
5.7 Comparison of *IR* with the existing technique 97

6.1 Imperceptibility comparison results using averages *PSNR* (in d**B**) 110
6.2 Imperceptibility of the Proposed Technique 111
6.3 Robustness results of the proposed technique comparison with the existing techniques 115
6.3 Continued.. 115

List of Publications

1. **Balkar Singh** and M. K. Sharma. "Tamper detection technique for document images using zero watermarking in wavelet domain", *Computers and Electrical Engineering*, SCI Indexed, Vol. 89, pp. 106925(1-11), 2021, Impact Factor 3.818.

2. **Balkar Singh** and M. K. Sharma. "Markov Matrix and Entropy based tamper detection technique for text images", *Journal of Engineering Research*, 2021, SCI Indexed, Impact Factor 0.64, DOI: https://doi.org/10.36909/jer.10947.

3. **Balkar Singh** and M. K. Sharma. "Efficient Watermarking Technique for Protection and Authentication of Text Images", *Multimedia Tools and Applications*, SCI Indexed, Vol. 81, pp. 22985-23005, Impact Factor 2.757.

4. **Balkar Singh** and M. K. Sharma. "Tamper Detection Technique for Text Images based on Vowels and Unicode Zero Length Characters", *Journal of Circuits, Systems and Computers*, Under Revision.

CHAPTER 1

Introduction

This Chapter is intended to serve as an overview of the fundamentals of document image watermarking. The basic terminology of watermarking are explained. The objectives and scope of the thesis are then stated. Finally, the thesis outline is provided.

1.1 Document Image Watermarking

The advancements in computations and communications have created an electronic environment which is capable to transfer, duplicate and share digital documents. In the transmission digital documents across the Internet, the issue of maintaining the integrity of digital documents has become a necessity. The main approaches employed in the security of digital documents include cryptography, watermarking, and steganography.

Watermarking is one of the approach, used to secure the digital documents. It uses the embedding process to embed the secret information in digital cover media. The cover media may be in the form of text, image, audio or video [Alattar and Alattar (2004); Alginahi et al. (2013); Hussain et al. (2015); Behera and Gangopadhyay (2021)].

The authenticity and copyright protection of document images have become extremely important when these images are shared online. A general framework of digital watermarking is shown in Figure 1.1.

- **Cover Image**: The image in which the secret data bits are embedded, is called a cover image. This image can be binary, gray scale, color or a document image *etc*.

- **Watermark**: A watermark is a secret data usually a logo, stamp or a signature. The bits of the watermark are embedded in a cover image. Depending upon the embedding, watermarks are classified into two types. The first is the visible watermark, which the user may see. Another is the invisible watermark, which the user is unable to see.

- **Watermarked Image**: A watermarked image is the modified cover image obtained after embedding bits of the watermark into the cover image. This image is transferred via Internet to the other user. During this transmission, attacks may be performed by the unauthorized user. Due to these attack(s), it may be difficult to extract the embedded watermark.

- **Key**: Key is the information which is used in the embedding and the extraction processes. It makes the technique secure. If the receiver has the correct key, then only he/she should be able to able to extract the watermark.

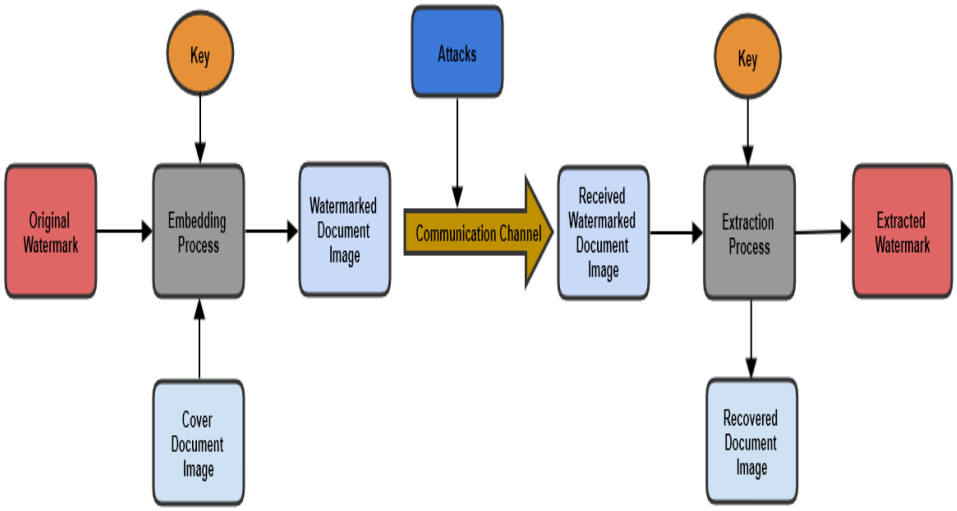


Figure 1.1: A General Watermarking Framework

The embedding process in a watermarking system uses the cover image, a watermark and the key to generate a watermarked image. The watermarked image should have the same visual appearence as the cover image so that it wouldn't create any suspension. Using the extraction procedure and key, the

receiver of the watermarked image can be able to retrieve the watermark [Bailey and Curran (2006); Zhang et al. (2019); Lin et al. (2019)].

Document images can be differentiated from the natural images by considering the following points:-

- **Diversity of Text**: The text in document images are usually with regular fonts, similar color, and horizontal orientation whereas text in natural images are far more diverse, *i. e.*, they may exhibit significant variations in font, color, orientation or even language type, if it present .
- **Background**: The background of document images are almost plain whereas the background of natural images may contain a lot of non-text elements like branch, grass, fence and sign.
- **Interference Factors**: Both the images have different factors like noise, blur and non-uniform illumination.

Due to these differences, watermarking techniques applicable to natural images are not directly applicable to the document images and there is the need to develop watermakring techniques for the document images.

1.2 Main Characteristics of a Watermarking Technique

Watermarking techniques have following fundamental characteristics [Chetan and Nirmala (2015)] and shown in Figure 1.2:

- **Embedding Capacity**: It is the maximum number of watermark bits that can be embedded in a cover image. The cover image is properly utilised in the embedding process if the embedding capacity is high.
- **Imperceptibility**: Imperceptibility means that the Human Visual System *(HVS)* should not be able to detect the embedded watermark in a watermarked image. The watermarked image should visually match the cover image.

- **Robustness**:It refers to the ability of a watermarking technique to withstand any attack such as filtering, rotation, compression, noise addition, cropping parts of the document, changing font type, font size *etc*.

- **Security**: The ability of watermarking technique to prevent an unauthorised user from processing the watermarked image is known as security. The users having the key can only be able to extract the embedded watermark.

To design an efficient watermarking technique, there is a need of trade-off between these requirements as by increasing the embedding capacity, the robustness and imperceptibility decreases and vice versa.

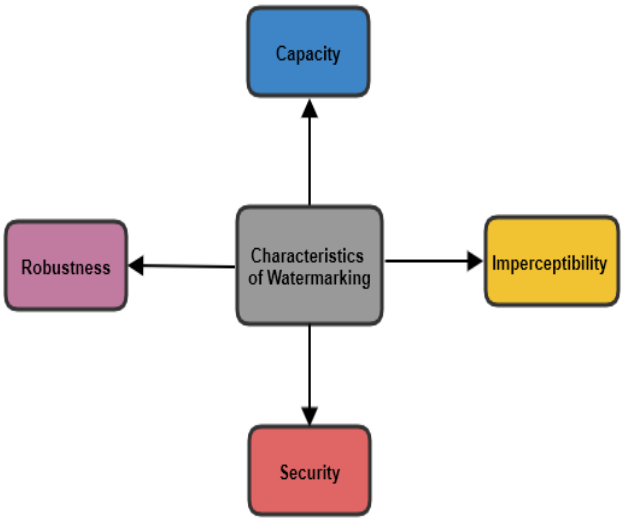


Figure 1.2: Characteristics of Watermarking

1.3 Types of Watermarking Techniques

A digital watermarking technique mainly depands on two basic processes- Embedding and Extraction. Embedding is an information hiding process in which bits of watermark image are embedded in the digital cover document. The embedded bits can be extracted to validate the ownership.

On the basis of the extraction process, watermarking techniques can be divided into following types [Qadir and Ahmad (2005); Jane et al. (2014); Chaubey and Singhadia (2015); Salameh et al. (2018)]:

- **Blind Watermarking**: The blind watermark method does not require the cover image to extract the watermark [Jane et al. (2014)]. It extracts the watermark bits from the watermarked image and generates a watermark for verification, as shown in Figure 1.3.

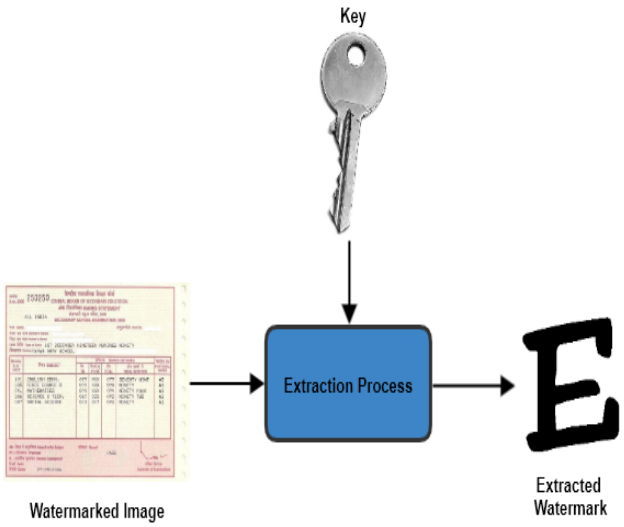


Figure 1.3: Blind Watermarking Process

- **Semi-Blind Watermarking**: In semi-blind watermarking, embedded watermark bits are extracted by using the watermarked image, key and some information of the cover image [Mohammadi (2015)], as shown in 1.4.

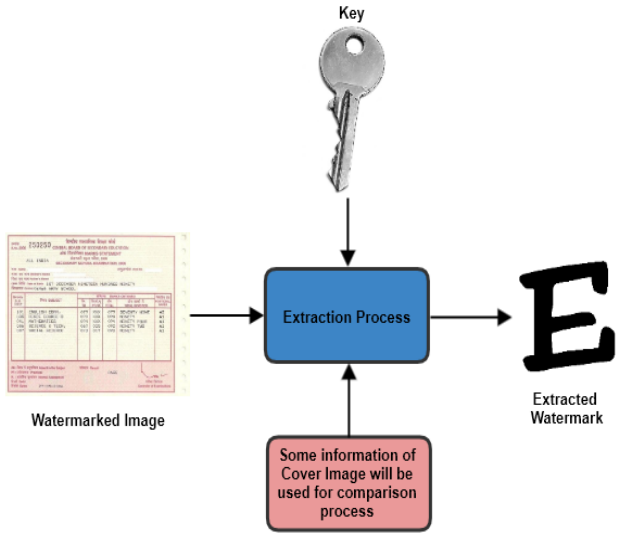


Figure 1.4: Semi-Blind Watermarking

- **Non-Blind Watermarking**: Non-blind watermarking techniques need watermarked image, cover

image as well as key to extract the watermark [Jaseena and John (2011)], as shown in Figure 1.5.

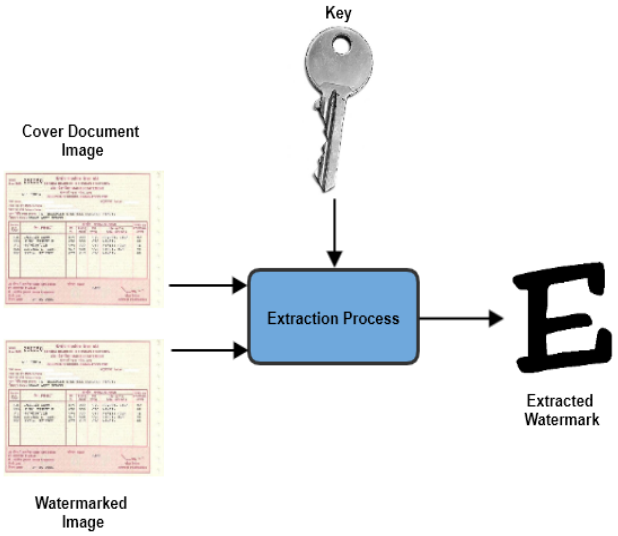


Figure 1.5: Non-Blind Watermarking

1.4 Image Authentication

Image authentication is the ability to determine if the input image is original or has been tampered [Zhao et al. (2010); Lin and Yang (2011); Kim and Yang (2021)]. In the authentication process, we compare the information extracted from the watemarked image with the original authentication information to judge whether the image was tampered with, as shown in Figure 1.6.

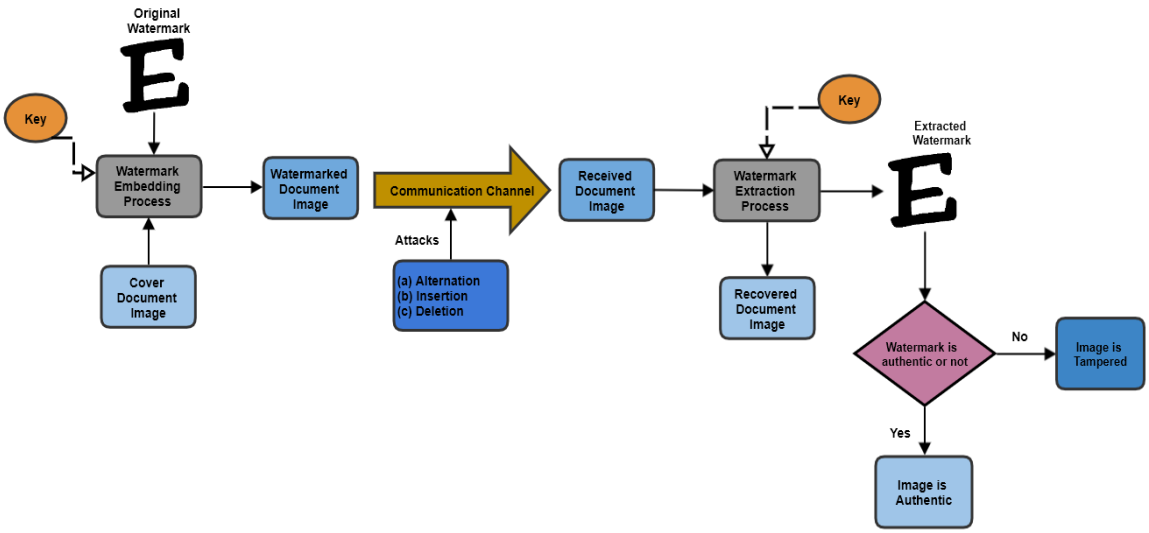


Figure 1.6: Image Authentication Framework

- **Complete authentication**: Complete authentication is the technique that consider the entire part of multimedia contents and do not permit any modification or alteration in it. Digital signature or watermark can be used for complete authentication.

- **Content authentication**: In this type of authentication, important features of the content are protected from the modification. For example, signature and logo can be protected using the content authentication.

1.5 Image Protection

It is the procedure for determining whether or not a person's ownership is legitimate. The watermark bits are embedded in an image to preserve the copyright of the image. These watermarks bits are extracted from the image and used to confirm ownership of a document image, when it is needed, as shown in Figure 1.7. Text, image, audio and video all can be used as watermarks. The embedded watermark bits are extracted in order to prove ownership identity. If someone copies a watermarked document, for example, the reversibility of watermarking techniques can be used to establish ownership of the copied documents.

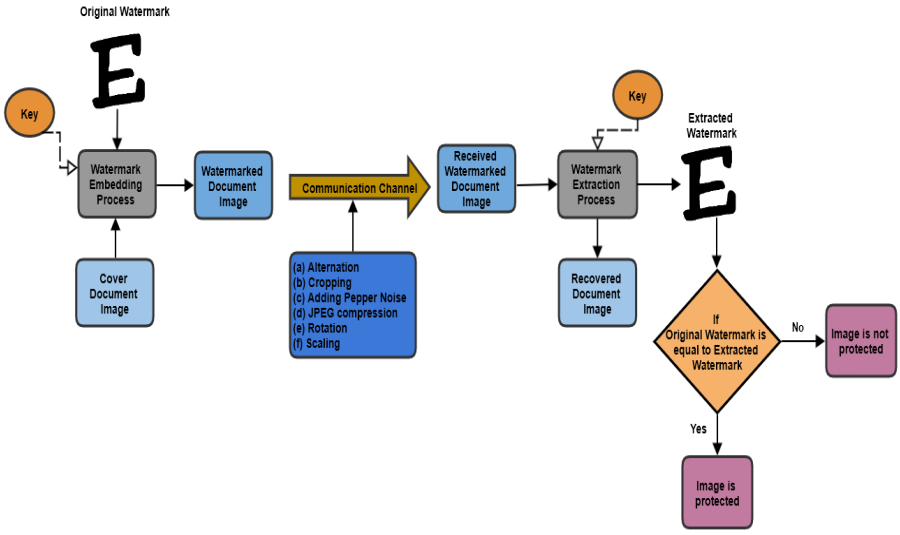


Figure 1.7: Image Protection Framework

1.6 Approaches Used for Document Image Watermarking

As document images are different than the natural images. There was the requirement to develop watermarking techniques for these images. Work related to watermarking of document images began in 1997. This initiative prompted other researchers to pay careful attention to the study of watermarking of the document images. Several watermarking approaches have been proposed for authentication and protection of digital document images [Maxemchuk and Low (1997); Singh et al. (2013)]. These approaches can be categorized in three categories, as shown in Figure 1.8.

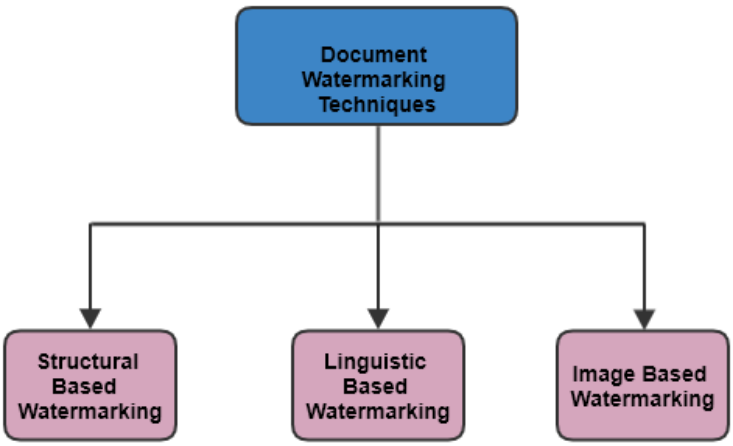


Figure 1.8: Types of Document Watermarking

1.6.1 Structural based Document Watermarking Approaches

In this approach, lines, letters and spaces between the text contents are modified to embed the bits of the watermark. Here, the structure or features of the text are adjusted to embed the bits of the watermark. It includes the general formatting of the cover text resources, in which text content is changed by using its words or sentences to embed the bits of the watermark. Locations of words and letters or the writing style are also modified for embedding the watermark. The general properties of the text are observed, and some physical properties are used to embed the watermark image bits into the text structure [Low et al. (1998); Brassil et al. (1999); Krishnamoorthy and Punidha (2012)]. Analysis of the average distance between the words in each line is also one of the structural based method used in watermarking [Huang and Yan (2001)]. Other methods were also developed, based on word clas-

sifications (Kim and Oh (2004)). In order to embed the watermark bits, other modifications exploit the justified paragraphs and irregular spacing contained in the text of document images. [Alattar and Alattar (2004)].

Approaches for text watermarking for languages other than English have also found their way. The first watermarking method based on Chinese text was developed by Li and Dong (2008). The authors utilized the features of the pictographic characters in Chinese script. These features are used in their technique to create the redundancy that is further used to embed the watermark. Other Chinese document watermarking methods often made use of Chinese character properties as they offered themselves as ideal objects to hide information. A watermarking algorithm was developed by adopting the pronunciation of polyphonic characters and the characteristics between two Chinese character polyphones [Fei and Tang (2011)]. One of the approach employed Chinese sentence entropy, measured on the basis of word frequency. The key sentences for embedding the secret bits are chosen based on entropy [Meng et al. (2010)].

In the case of watermark to be embedded in Arabic text material, the features of the Arabic script characters were used by most existing techniques. The characters are expanded and replaced with similar Unicode characters, or the diacritics are modified to embed watermark bits [Gutub et al. (2010); Alotaibi and Elrefaei (2016)].

The structural based approaches are not immune to formatting-based attacks like copying, pasting and retyping. None of these techniques are immune to print and font change attack.

1.6.2 Linguistic based Document Watermarking Approach

The linguistic based approach is based on natural language processing based methods. The language of text present in document image is analyzed and modified to embed watermark bits [Atallah et al. (2002)]. To embed the watermark bits,the syntactic and semantic essences of the cover image are also analyzed. The bits of watermarks are inserted in such a way that the text's structure and context remain unchanged[Topkara et al. (2005); Chen et al. (2016)]. Some of the watermarking techniques based on linguistic use the combination of semantic and syntactic transformation of the text (Li and Wu (2013)). The substitutions of synonym words are used to preserve the imperceptibility and one

word per sentence increases the embedding capacity [Gort et al. (2020)].

To insert the watermark bits, words of the content are manipulated according to the syntactic approach. The embedding utilises the verbs, nouns, adjectives, pronouns, prepositions, synonyms, and other grammatical characteristics of the text content. These grammatical changes are implemented without altering the content's originality. Also, the word sequence in the contents can be rearranged to add the watermark bits. This can be achieved by altering the structure of the text, such as moving the adverbial phrase, inserting the subject matter or altering the sentence from active to passive. Modifications in the watermarking techniques have introduced several other syntactic-based approaches [Kim (2008); Meral et al. (2007, 2009); Wang et al. (2008); Kim and Goebel (2012)].

In the semantic based approach, the watermark bits are inserted by manipulating the words in the text. This includes methods such as substitution of synonyms, algorithms based on noun-verbs, typo-based algorithms, acronyms and abbreviations, presuppositions-based algorithms based on linguistic approaches, and text-based representational strings. These methods rely on the language and use vocabulary, grammar or structure to embed the watermark bits [Vybornova and Macq (2007); Mir (2011); Lou and Liu (2012); Chen et al. (2016)].

1.6.3 Image based Document Watermarking Approach

In this approach, characteristics of the document image are used to generate the watermark. This watermark is then embedded into the cover image by using an embedding algorithm. Text contents are viewed as a series of text images. The watermarked text is considered to be an image and the text can no longer be copied and pasted, and must be retyped for reproduction. A watermark logo is generally used to identify the validity of the original image. This approach of watermarking is deemed safe against format based attacks.

One solution is to use letter pixels to embed the bits of a watermark . The curvaceous letters are used in these approaches for watermarking by changing the curves of the letters according to the respective bits. The process of embedding the bit includes the curve of the watermarked text, which changes a little in direct relation to the modified bit [Yazdani et al. (2013)].

1.7 Methodology of the Proposed Work

Following is the methodology used in the proposed work:

1. After doing a review of the existing protection and authentication document watermarking techniques, gaps were identified. On the basis of these gaps, objectives of the proposed work are defined.

2. Document images used by existing techniques and *DIQA* dataset images are used for the implementation of the proposed techniques.

3. Lifting Wavelet Transform, Zero Width Characters, Entropy, Markov Matrix, Discrete Curvelet Transform and Discrete Cosine Transforms are used to transform or process the cover images in the proposed techniques.

4. To evaluate the proposed techniques, following parameters are considered.

   i **PSNR:** To compare the visual quality of cover image with watermarked image, Peak Signal-to-Noise Ratio is used. *PSNR* value determines the visual quality of watermarked image. It is a function of Mean Square Error (*MSE*) and is defined as,

$$PSNR = 10 \times log_{10} \frac{(2^b - 1)^2}{MSE} \tag{1.1}$$

   where b is the bit depth of image. and MSE is defined as,

$$MSE = \sum_{i=1}^{M} \sum_{j=1}^{N} \frac{\delta(i,j)^2}{M \times N} \tag{1.2}$$

   where $\delta(i,j)$ is defined as

$$\delta(i,j) = S(i,j) - C(i,j) \tag{1.3}$$

   where $S(i,j)$ is the pixel of watermarked image and $C(i,j)$ is the pixel of cover image, *M*

and *N* is the height and width of image respectively.

ii **BER:** Bit Error Rate is determined by the sum of the correct bits obtained divided by the total number of bits transmitted.

$$BER = \frac{Number\ of\ correct\ bits\ received}{Total\ number\ of\ bits\ transferred} \tag{1.4}$$

iii **DR:** Distortion Robustness is measured using Loosing Probability. Loosing Probability is the probability of how much proportion of the embedded watermark bits has been droped from the watermarked image.

$$P(DR) = [1 - LP] \tag{1.5}$$

Where *LP* is the loosing probability.

$$LP = \frac{NL}{LC} \tag{1.6}$$

Where *NL* is the number of sentences and *LC* is the total length of cover text.

iv **SSIM :** Structural Similarity Index Measure is a metric used to quantify the deterioration of image quality induced by embedding in the image. It is used to evaluate the robustness of a watermarking technique. *SSIM* between the cover watermark and the extracted watermark is also evaluated, as defined by

$$SSIM = \frac{\sum_m \sum_n W(m,n) \times W(m,n)^{'}}{\sum_m \sum_n [W(m,n)]^2} \tag{1.7}$$

v **Correlation:** The correlation between the original watermark and the extracted watermark is often used as a quality parameter. It is given by

$$Correlation = \frac{\sum_m \sum_n (Se(m,n) - \bar{Se}) \times (Se^{'}(m,n) - \bar{Se^{'}})}{\sqrt{\sum_m \sum_n (Se(m,n) - \bar{Se})^2 \times \sum_m \sum_n (Se'(m,n) - \bar{Se'})^2}} \tag{1.8}$$

where $Se(m,n)$ is the original watermark data and $Se^{'}(m,n)$ is the extracted watermark data. $\bar{Se}$ is the mean of original watermark and $\bar{Se}^{'}$ is the mean of extracted watermark.

vi **Imperceptibility:** Imperceptibility is the watermark's ability to stay unnoticed with naked eye, after embedding in the cover image. This is accomplished by a high level of resemblance among the original image and watermarked image. Imperceptibility is inversely proportional to capacity *i.e.* higher imperceptibility decreases the embedding capacity of the technique.

$$Imperceptibility = \frac{No.\ of\ extendable\ characters}{Watermark\ Length} \tag{1.9}$$

vii **Embedding Capacity:** Capacity is given by maximum value of watermark bits or information embedded in the original image for a particular period of time.

$$Capacity = \frac{Total\ number\ of\ watermark\ bits\ embedded}{M \times N} \tag{1.10}$$

where $M \times N$ denotes the cover image size.

viii **UQI:** Universal Quality Index is a metric used to find the distortion between two images using correlation, luminance and contrast.

$$UQI = \frac{4\sigma_{xy}\mu_x\mu_y}{(\sigma_x + \sigma_y)(\mu_x + \mu_y)} \tag{1.11}$$

Where μ_x and μ_y are the averages of the pixel values of original and distorted images images respectively. σ_x and σ_y are the variances and σ_{xy} is the covariance.

5. The proposed techniques are tested and evaluated against various attacks like deletion, insertion, rotation, scaling, *JPEG* compression, salt and noise pepper, croping *etc*.

6. The proposed techniques are also compared with the existing state-of-art document image wa-

termrking technique. These comparisons are analysed in depth.

1.8 Thesis Contribution

In this thesis, four watermarking techniques are proposed for document images. In the first tehnique, zero watermark is generated using wavelet features of the cover document image. A key watermark is also used to generate final visual watermark. Final visual watermark is stored with the Certifying Authority. This watermark is used to compare with the watermark that is generated from the watermarked image. If both the watermarks are same then image is authentic otherwise image is tampered. The quality of the watermarked image will no degrade because watermark is not embedded in the cover document image. *SSIM* and *BER* values are greater than 99 %. The *BER* value of the proposed technique is high as compared to the values of the existing techniques. In the second technique, hash values of the cover document image and watermark bits are converted into Zero Width Characters *(ZWC)*s. Both these values are concatenated and embedded at the end of each sentence of the cover document images. On the receiver side, these values are extracted from the watermarked image. Extracted values of hash and watermark are compared with the original values. Hash values are used to autheticate the watermarked document image and the extracted watermark is used for protection purpose of the document image. The technique is evaluated by using attacks like addition, insertion and tamper. In the third technique, entropy and markov matrix are used for the tamper detection of text images. Entropy is calculated of every sentence and converted into *ZWC*. Thess *ZWC* values are embedded at the end of every sentence after the sentence terminator. A character pattern is generated by using markov matrix and this character pattern is converted into *ZWC*. The *ZWC* of character pattern is embedded at the end of the text. Entropy values and character pattern are generated from the watermarked image on the receiver side. If the entropy values are equal then image is not tampered otherwise it is tampered. Character pattern values are used to find the probable location of the tampered word(s). The technique is tested and found efficient against the attacks like insertion, deletion and tampered of the text. In the fourth technique, Discrete Curvelet Transform(*DCuT*) and Discrete Cosine Transform(*DCT*) are used to protect color cover document image. Firstly *DCuT* is applied on the cover image and then *DCT* is applied on the blocks of size 8×8 of sixth layer to

generate the *DCT* coefficients. *DCT*. Zigzag pattern is used to select the *DCT* coefficients from low to medium except the first *DC* coefficient. The same process is applied on the cover image as well as watermarked image on the receiver side. Watermark is compared to prove the authenticity of image. Imperceptibility of the proposed technique is compared with the existing techniques by using average *PSNR* value. The proposed technique shows good robustness against *JPEG* compression attack.

1.9 Thesis Organization

The thesis is organized as follows: Chapter 1 provides an overview of document image watermarking. It also discusses how watermarking can be used to protect and authenticate the document images. The existing copyright protection and authentication schemes relevant to document image watermarking are thoroughly reviewed in Chapter 2. The gaps in these schemes have been identified as a result of this review. These gaps are then used to formulate objectives. Chapter 3 presents a zero watermarking technique for tamper detection using wavelet transform. Chapter 4 presents a protection and authentication technique using zero width characters. A Markov matrix and entropy-based technique for tamper detection of text images is presented in Chapter 5. Chapter 6 presents a discrete curvelet and discrete cosine transform based watermarking technique. These proposed techniques have been concluded in Chapter 7, along with the possible future scopes.

CHAPTER 2

Literature Survey

Existing watermarking technique for document images are reviewed in this Chapter and various gaps are identified. The proposed work's objectives have been identified based on these gaps, leading to the formulation and solution of the problems addressed in the following Chapters.

2.1 Classification of Document Watermarking Techniques

On the basis of data embedding, document watermarking techiques are divided in two categories: zero emebedding and physical embedding, as shown in Figure 2.1. Various techniques have been proposed in the literature in both of the categories. Both type of techniques have their advantages and drawbacks, as discussed in the following sections.

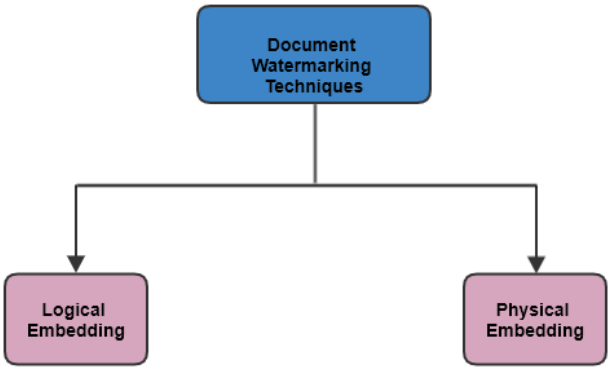


Figure 2.1: Document Watermarking Techniques

Embedding in a document image is the process by which the watermark bits are created and inserted in the original document image to create a watermarked image.

2.2 Zero Watermarking Techniques

Zero watermarking is a fully invisible or imperceptible approach to watermarking. It is equivalent to data hiding in which the viewer is absolutely transparent to concealed data due to this, no embedding is implemented on the cover media. The solution involves digitally embedding the watermark bits into content of text, without embedding the watermark physically inside a digital carrier. This is achieved by producing the watermark data from the features of the carrier image. The watermarked document is kept confidential and the original document is released to the public. The watermark information is generated again from the same features of the cover image and compared with the original watermark bits to validate the authenticity of document being targeted. Authenticity or protection is proved if the comparison is true [Wen et al. (2003); Zhou et al. (2009); Jalil et al. (2010c); Tayan et al. (2014)]. The categories wise of zero based watermarking techniques are shown in Figure 2.2. The following requirements should be fulfilled by a zero watermarking technique:

- The features used to create a zero watermark should fully reflect the cover image.
- These features should satisfy the collision resistance *i.e.* from different cover images, the probability of same extracted watermarks should be very less.

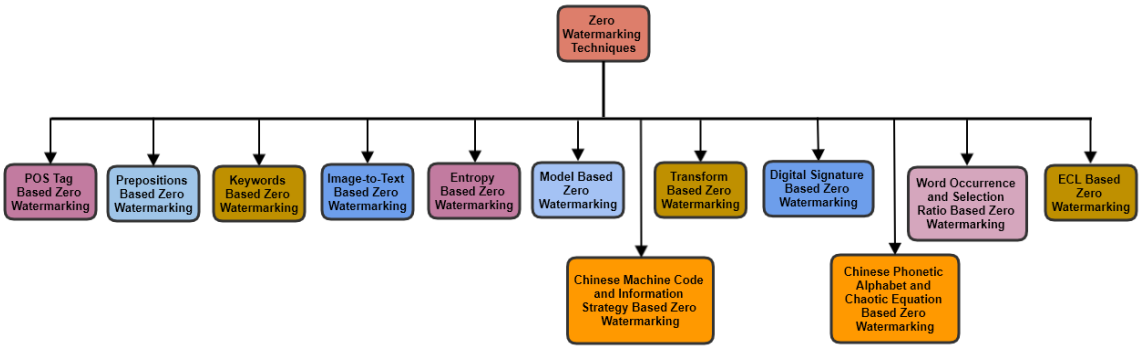


Figure 2.2: Classifications of Zero Watermarking Techniques

In this technique, the structural or attribute properties of the text contents of the image are analyzed

and then used to create a watermark. This watermark is kept secure with Certifying Authority(*CA*) and can be used for future authentication process. This method is robust as well as imperceptible, as there is no watermark information in the cover document image being released to the public. Nevertheless, there are some disadvantages that need to be stressed. Even though it is safe against format-based attacks or attacks based on content, all of the contents can be easily changed or modified by a possible attacker so that the information about the watermark can no longer be found. The text information can be misused if the watermark is hard to recognise. Logical or zero embedding methods relevant to document images have been explored in this section. The study of these approaches in relation to attacks and results is summarized in Table 1.

Part of Sequence Tag Sequence based Zero Watermarking

The patterns of a sentence are represented by Part of Sequence(*POS*) tag sequence. These tag sequence are used in zero watermarking techiques. Many sentences can be built up to reflect the same meaning. The contents and expressions of various texts may be different and also their *POS* tag sequences are expected to be different. Final zero watermarked image is produced by applying transformation to the characteristic of the *POS* sequences.

A zero watermarking technique using *POS* tag sub-sequences is proposed by He et al. (2009). Tag sequences have been extracted using a chaotic method to create a watermark. This approach offers good protection as sequence of selected *POS* tags is not known to the attacker, whereas the chaotic process has uncertain properties. Robustness is also assured against reformatting, transforming document type, interchangeable substitution, and sentence transformation attacks.

Qi and Liu (2013) proposed a zero watermarking technique to authenticate Chinese document images. The frequency of *POS* tags as well as entropy are used as features. Watermark bits are generated by using forward cloud model generator and features generated from the *POS* tags. This technique is very vulnerable to insertion and deletion attacks. A good tamper detection rate is achieved only if insertion and deletion is less than 20%.

Prepositions based Zero Watermarking

The words or phrases in a sentence that connect a noun or pronoun to a verb or an adjective is referred to as preposition. This preposition is used in a various ways in the watermarking techniques.

Maximum occurring prepositions in the text contents are used by Jalil et al. (2010a) to construct a text separator. The maximum occurring Non-Vowel ASCII characters in every partition are listed and the author key is generated by using this list and watermark bits. The generated watermark is then stored with *CA* to make it secure. The insertion and deletion attacks are considered to evaluate the performance of the technique. The insertion and deletion rate is checked at 5%, 10%, 20% and 50% and the watermark accuracy results are analyzed. The precision is found to be lowest at the highest addition and deletion ratios.

A preposition and a double letter were used by Jalil and Mirza (2010) to build the watermark. The data partitions in the document image are evaluated using the frequency of repeated letters. By using the number of letters in the time interval, the watermark is formed. To judge the degree of closeness, original and modified watermark bits are matched. This strategy ensures the protection and is more stable in terms of resistance to any attacks like insertion, deletion and reordering.

A blind watermark technique based on the appearance of prepositions and double letters in the text document was suggested by Jalil and Mirza (2013). This technique provides protection of copyright from addition, deletion and reordering attacks.

Keywords based Zero Watermarking

There are various keywords in the text of a document image. These keywords are used in watermarking process by considering their length and frequency of occurrences.

A zero watermarking technique on the basis of keywords is proposed by Jalil et al. (2010b). To create a watermark key for every sentence, all words with more than four letters are chosen and used. Watermark distortion rate and pattern matching are evaluated for insertion and deletion attacks. At a constant rate, experimental results for low, moderate and high-level tampering attacks are evaluated.

Characteristics of the text are used by Jalil et al. (2010c) to propose another technique for creating the zero watermark. The keyword that appears several times is selected, and the length of the word

that precedes and follows the keyword is used to build the watermark. Watermark distortion rate is evaluated against the insertion and deletion attacks. The tamper detection accuracy of the technique is measured and found to be better than the existing techniques.

Another secure and robust technique is proposed by Jalil et al. (2011) in which the bits of watermark image are logically embedded in the text content of the digital document cover image. Watermark key is created by using text elements, double letters and most commonly used English words. The technique is being tested for insertion and deletion attacks and found to be efficient in comparison of existing techniques.

Image to Text based Zero Watermarking

Image to text based zero watermarking technique extracts the text from a document image. The first letter that most commonly appears is generally used to create a watermark, in these techniques.

An image to text watermarking technique, in which a watermark image is transformed into an alphabetical watermark image [Jalil et al. (2010a)]. After using the propositions of the text as separator, a key is generated by using the first letter that appears Most Frequently (*MOFL*). To construct a *MOFL* list, every group's first double letter occurrence is used. The watermark letters and the list are used to generate the watermark key. This technique is robust against insertion, reordering and deletion attacks. This technique also provides a higher percentage of successfully detected watermarks.

A technique to generate a watermark key by using an image-to-text converter is suggested by Tayan et al. (2013). The watermark image is embedded in the duplicated original file where it is processed and categorized into word sets and based on its features, the watermark key is created. This technique provides protection against forgery and unauthorized exploitation. The blind and fragile watermark extraction procedure is used to secure watermark key.

Entropy based Zero Watermarking

Entropy of the word of the text information is amount of average information which tells the randomness of the word in the contents of the document image.

The words of Chineses text are used by Meng et al. (2010) to produce a watermark. The entropy is

also measured using the word frequency and is further used to select the key phrases. The watermark is generated in accordance with the order of the sentences. Technique is tested against attacks such as adding, deleting and synonym substitutions.

A technique that uses the features of Chinese content sentences is proposed by Liu et al. (2015). Text of the document is partitioned into sentences and semantic code of each word of a sentence is then used to measure its entropy. Word entropy, relevance, weighting function and length are used to generate the watermark. This watermark is then encrypted and stored with *CA*. This technique offers security, robustness as well as protection of document images.

Model based Zero Watermarking

In this watermarking approach, probabilistic features as well as syntactic and semantic features of textual contents of an image are used to generate zero watermark.

Space models based zero watermarking was developed by Meng et al. (2011). The zero watermark is generated from a three dimensional (3-*D*) model on the basis of 2-D coordinates of word level and sentence weights of the sentence-level. 2-D word space layout consists of both the length and frequency of the word and is expanded to a 3-D format. The text watermark is constructed by mapping 3-D model with the sentence. This technique is evaluated against three most frequent attacks; attack of syntactic transformation, synonymous replacement attack and deleting attack. This technique is used to protect the digital document images.

Markov's model is utilized by Al-Wesabi et al. (2012) to propose a watermarking technique in which watermark is generated by using the probabilistic features for document image content authentication. Text information is analyzed with the help of hidden Markov model. This strategy provides protection against insertion and deletion attacks.

Meng et al. (2012) proposed a 3-D space model by using syntactic and semantic features of document image. A watermark is generated by comparing the distances of the sentences of a document image. Syntactic transformation, synonymous substitution, addition, deletion and reordering attacks are performed in the experiment. Deletion and reordering attacks demonstrated the model's vulnerability to the modifications, syntactic transformation and synonymous replacement attacks were well

resisted.

Three order Markov model for English text image is analyzed by Ba-Alwi et al. (2014). In order to generate the watermark bits, the analysis is further utilized to find the relationship that exists between the contents of text image. The contents of English text document are used to extract the probabilities of the interrelationships in the contents. This technique is used for authentication and provides better robustness against attacks like insertion, deletion and reordering as compared to existing techniques.

A zero watermarking technique based on Markov Model for English text document is proposed by Ghilan et al. (2014). The technique is capable to provide content authentication and tamper detection for English text documents. This technique provides more robustness and better performance as compared to other existing techniques, especially for insertion and deletion attacks.

Markov model is used by Al-Wesabi et al. (2020) to propose a zero watermarking technique for Arabic text. This technique is based on the fourth level of word mechanism that provides tamper detection and content authentication. Integration of the zero watermarking with the hidden Markov model enhances the embedding capacity as well as robustness.

Chinese Machine Code and Information Strategy based Zero Watermarking

Chinese machine code and information gain approach are used in text zero watermarking scheme that uses distance to generate the zero watermark. In each paragraph, the distance is computed between the characteristic words and used to select the commutation location to create a distance matrix to generate a zero watermark.

A watermarking technique for text document based on Chinese machine code and information tactics is proposed by Yingjie et al. (2013). This technique has good robustness and protection against attacks like addition and deletion, synonymous substitution, and syntactic transformation. It provides security with the help of copyright holder identifier and date stamp for every generated key.

Transforms based Zero Watermarking

Transforms like *DCT*, Discrete Wavelet Transform (*DWT*) and Discrete Fourier Transform (*DFT*) are used in zero watermarking techniques. A transform converts an image from spatial domain to

transform domain. After transformation, the image is divided into blocks of different coefficients values. These blocks may also be further used for watermarking.

Feng and Huang (2012) proposed a *DCT* based zero watermarking technique for Chinese document images. Cover document image is partitioned into 64 blocks and then *DCT* is applied to every block. Low-frequency to medium-frequency band *DCT* coefficients are chosen to form a one dimensional series. Keys are used to encrypt the sequence, using the logistic mapping to create the zero watermark sequence. The detected watermark and registered watermark are compared in order to measure the similarity parameter for verification.

Digital Signature based Zero Watermarking

A digital signature is a mathematical feature used to confirm that the digital images or documents are authentic or not. The digital signature technique is based on symmetric key and asymmetric key approaches. It guarantees the content authenticity, integrity, and privacy of the digital data. Two most commonly used public key digital signature methods are Rivest-Shamir-Adleman (*RSA*) encryption algorithm and the Digital Signature Algorithm (*DSA*).

Tayan et al. (2014) proposed a hybrid technique on the basis of zero watermarking and digital signatures to secure digital media. Logical embedding is done by embedding the watermark bits in the cover document and watermark image is transformed into a character sequence. Unicode is used to numerate words into binary values. This technique provides better performance in terms of tamper detection, robustness, capacity ratio, imperceptibility, to verify authentication of a document, and language independence as compared to the other existing watermarking techniques. It has its drawback because it needs a large amount of memory to store the created keys with *CA*.

Chinese Phonetic Alphabet and Chaotic Equation based Zero Watermarking

Chinese phonetic alphabets are divided into three categories:initials, finals and syllables. A watermarking technique connecting the syllable parts of the Chinese phonetic alphabet is proposed by Zhu et al. (2016). Every syllable is assigned initial and final values, and frequency is calculated according to its occurences. A sequence is constructed by using the logistic chaotic. Transformation of the se-

quence is used to create the watermark. One dimensional logistic chaotic equation has been evaluated as these chaotic features follow the demands of sequence key to evaluate its robustness against content attacks such as format, deletion and addition. The outcome demonstrates the algorithm's ability to perform anti-adding attacks. It demonstrates good robustness as well as high resistance against tampering attacks. In order to prevent illegal access, the key needs to be registered with *CA* along with the date and licence.

Word Occurrence and Selection Ratio based Zero Watermarking

Words present in the text of a document image play a vital role in determining the ratio of word occurrence and also in determining the size of replacement attack.

A zero watermarking approach on the basis of a word replacement attack for document images was developed by Bashardoost et al. (2017). The replacement attack changes the contents of a document without altering the structure of text content. Word Occurrence Ratio (*WOR*) is used to determine the rate of presence of the word within a document and Word Selection Ratio (*WSR*) has been used to determine the size of replacement attack. This technique depends on the three stages *i.e.* replacement resource selection, new word preparation as well as replacement action. *WOR* of word *z* is computed by using the following equation:

$$WOR(z) = \frac{Number\ of\ occurrence\ of\ z\ in\ document}{Total\ number\ of\ words\ in\ document} \tag{2.1}$$

By measuring *WOR* for every word of the original document, *WSR*, that is equal to the size of replacement attack, is calculated by

$$WSR = \frac{\sum WOR(z)}{Total\ number\ of\ words\ in\ Document} \tag{2.2}$$

The results show that the technique is not capable of detecting document's replacement attack and also less accurate for calculating the size of advance replacement attacks compared with normal attacks.

Effective Characters List based Zero Watermarking

Saba et al. (2020) proposed a zero watermarking technique for document images based on Effective Characters List(*ECL*). The watermark is created by using the concept of the converting selected text in a document. The number of characters to be selected for watermark generation is calculated by Effectiveness Ratio (*ER*). To test the technique's effectivenss deletion, insertion and reordering attacks are used on the digital documents.

The different attacks and metrics used by the authors to measure the efficiency of the existing zero watermarking techniques are summarized in Table 2.1.

Table 2.1: Types of Attacks and Performance Evaluation of Zero Watermarking Techniques

Author	Types of attack					Other Evaluation metric
	Insertion	Deletion	Reordering	Synonym Substitution	Syntatic Transformation	
[He et al., 2009]	No	No	No	Yes	Yes	No
[Jalil *et al.*, 2010]	Yes	Yes	No	No	No	No
[Jalil *et al.*, 2010]	Yes	Yes	No	No	Yes	No
[Jalil *et al.*, 2010]	Yes	Yes	Yes	No	No	No
[Jalil *et al.*, 2010]	Yes	Yes	No	No	No	No
[Jalil and Mirza, 2010]	Yes	Yes	Yes	No	No	No
[Jalil *et al.*, 2011]	Yes	Yes	No	No	No	No
[Al-Wesabi *et al.*, 2012]	Yes	Yes	No	No	No	No
[Meng *et al.*, 2012]	Yes	Yes	Yes	Yes	Yes	No
[Yingjie *et al.*, 2012]	Yes	Yes	Yes	Yes	Yes	No
[Tayan et al., 2013]	No	No	No	No	No	Computation at time to encode and decode watermark

[Yingjie et al., 2013]	Yes	Yes	No	Yes	Yes	No
[Qi *et al.*, 2013]	Yes	Yes	No	Yes	No	No
[Jalil and Mirza, 2013]	Yes	Yes	Yes	No	No	No
[Yingjie *et al.*, 2013]	No	No	No	No	No	Robustness
[Ba-Alwi *et al.*, 2014]	Yes	Yes	Yes	No	No	Robustness
[Feng and Huang, 2012]	Yes	No	No	No	No	Robustness and Capacity
[Ghilan *et al.*, 2010]	Yes	Yes	Yes	No	No	Robustness
[Tayan *et al.*, 2014]	No	No	No	No	No	Computation at time to encode and decode watermark
[Liu *et al.*, 2015]	Yes	Yes	No	Yes	Yes	No
[Zhu *et al.*, 2016]	Yes	Yes	No	No	No	No
[Bashardoost *et al.*, 2017]	Yes	Yes	Yes	No	No	No

2.3 Physical Embedding Techniques

In this approach, the watermark bits are actually embedded into the original digital image. The bits of watermark are in the pattern of a linguistic, image or structural manipulations. Embedded watermark bits can be completely invisible, slightly visible or visible. In visible watermarking, embedded watermark bits are visible to the receiver and therefore prevents copying as well as reusing the image. So it is helpful in promoting the owner of task. This type of embedding is usually done in the form of an image watermark, but text content is not well-known because the text content can be easily manipulated and retyped [Chen et al. (2001); Panah et al. (2016)]. The categories wise of physical based embedding techniques are shown in Figure 2.3.

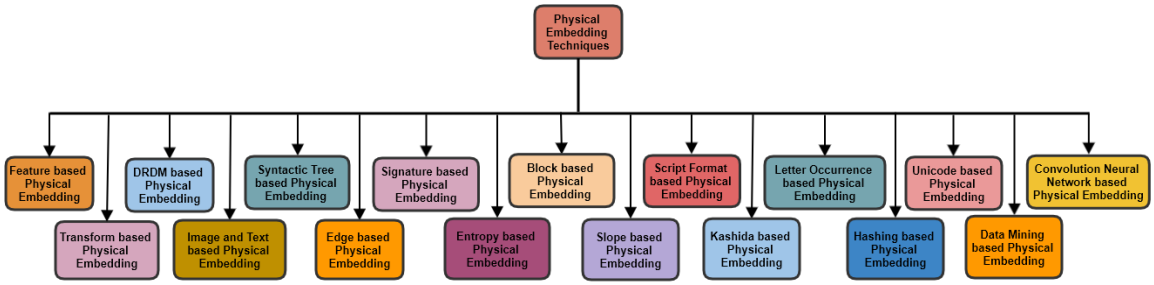


Figure 2.3: Classifications of Physical Embedding Watermarking Techniques

Depending on the embedding process used, the modifications made to the text vary from barely visible to completely invisible. In invisible as well as partially visible physical embedding, only authorized users are aware of the watermark. Thus, in the case of copying and tampering, the watermark bits are not lost or removed as the unauthorized user does not know that there is watermark bits in the text. The invisible watermark can impede the tampering of the text and it is easy to detect any kind of manipulation. The related work on the physical embedding of document image watermarking are summarized in Table 2.2.

Feature based Physical Embedding

As document image contains different elements such as lines, words and characters. The physical embedding can be achieved using the features of these elements. Each element has different features that can be used to embed watermark bits. The watermark bits may be embedded into the digital document image by shifting or altering these elements.

Different shifting in the lines and words of the cover image are used by Brassil et al. (1994) to embed the watermark bits. The watermark is embedded in the line shift approach by dislodging the entire text line vertically. In line shifting, the selected lines are shifted up or down. In word shifting approach, the position of a word inside a text line is moved horizontally to embed the watermark bits. Moving may be either right or left while neighboring words will remain unchanged. In character shifting, features of a character are altered to embed the watermark bits. These alterations are made by extending or shortening the length of the characters by (at least one) pixels.

Brassil et al. (1995) proposed watermarking techniques by embedding a single code word for each recipient. In this work, the authors proposed three techniques *i.e.* Line-shift coding, Word-shift coding and Feature coding. These techniques are quite reliable even if the documents is photocopied.

Feature calibration based technique for embedding and detecting watermarks in the document images is

proposed by Amano and Misaki (1999). Within that technique, two sets of symmetrically arranged partitions are specified in the bounding boxes of the text line and features have been extracted from every partition. The difference between the average feature values of the two sets is encoded as a positive or negative displacement of every bit of the watermark. This technique is used for protection purpose. In order to calculate the efficiency of the technique, the average and standard deviations of the feature displacement are evaluated.

Some of the measureable properties of digital content fonts are used by Bhattacharjya and Ancin (1999) to develop a technique for embedding data in color document images. The embedding process includes two times scanning of original document. The first scan is used to produce the preview of the document image at a lower resolution and the second scan provides maximum resolution that is used to create the copy of document.

A data embedding technique for document images is proposed by Chotikakamthorn (1999). The data embedding is performed by changing the widths of a few successive characters space in selected lines. In the embedding process, characters are grouped into blocks by using the sentence or word spacing as a group boundary. Blocks with character size less than the threshold value are not used for embedding a watermark. The disadvantage of their technique is that width of the character spacing is very limited relative to width of the word spacing.

A technique to embed watermark bits in binary images like scanned text, figures, and signatures was suggested by Wu *et al.* (2000). Two basic approaches are used to embed the watermark bits in binary images by adjusting the pixel value as well as features of a group of pixels. First approach changes the pixel value from white to black or black to white while the second approach alters the features like stroke thickness, curvature as well as relative location. The document cover image is divided into blocks of same size. In embedding process, one bit of watermark image is embedded in each block and pixels to be flipped are the ones with lowest scores. These approaches are used for the authentication purpose.

An authentication technique based on a block pixel rearrangement for binary images is developed by Huang and Yan (2001). Grayscale image conversion into binary image is achieved by using Halftone technique. The first image is divided into 9×9 non-overlapping blocks. Standard deviation is used as a authentication signal and is created by reordering the pixels in the selected blocks. The main drawback of this approach is the deterioration introduced in the binary image encoded.

Wu and Liu (2004) proposed a blind watermarking technique for binary image authentication and annotation. The flipping of pixels is used before the embedding process and a significant amount of data is embedded without any visible artifacts. Watermark bits are embedded by manipulating pixels with high score of flippabil-

ity. The features created by using group of pixels are used to embed the watermark.

A blind watermarking technique for authentication of text document images by combining inter-character and word-spaces was suggested by Yang and Kot (2007). Inter character spaces are incorporated with word spaces in enhancing the hiding capacity. To embed watermark bits, different embedding rules are used. English and Frech text documents are used in the experiment. The main disadvantages of this technique are its high computational complexity as well as susceptibility to noise attack.

Zhu et al. (2006) used Render Sequence Encoding (*RSE*) to propsoe a watermarking technique for authenticating a document image. It encodes the embedded data into the documents by altering the display sequence of words and characters, without altering the appearance or contents of the document image. Encoding is accomplished by means of a special permutation of the sequence of the display. *RSE* embeds the watermark data into the formatted document that includes all text data layout information such as PostScript, Portable Document Format (*PDF*), Printer Control Language and Device Independent Document.

Adaptive Least Significant Bit (*LSB*) replacement technique is used by Roy et al. (2020) to propose a copyright protection watermarking technique. A embedding capacity map is generated by using a saliency map after that adaptive *LSB* replacement is performed to generate a watermarked image. Imperceptibility and robustness are used to validate the technique.

Transform based Physical Embedding

Transforms are also used in physical watermarking embedding. A transform changes the spatial domain of the cover image into transform domain. Coefficients of the transformed image are used to embed bits of a watermark. Tranform based watermarking techniques have better robustness compared to the techniques of spatial domain.

Lu et al. (2002) developed a watermarking technique using *DCT* coefficients of the binary images. The *DC* components are used to embed bits of watermark image. Prior to watermark embedding, a pre-processing approach is used to blur the binary image into gray scale image. A post-processing process is then used after the embedding the watermark to binarizes the image. Their technique provides robustness as well as protection against cropping and noise attacks.

Spread spectrum modulation and Human Visual System are used by Zhu et al. (2012) to develop a watermarking technique for binary document images. Watermark patterns are created using the DCT coefficients and are inserted into the cover document image. Perceptual masks are used to evaluate the places of flipped pix-

els. Robustness of technique is evaluated against four types of attacks such as noising, denoising, geometrical and print scan. The performance of the technique is evaluated by using *PSNR* parameter.

A blind watermarking technique by using *DWT*, *DFT* and Arnold scrambling for document images is proposed by Li and Wu (2013). Before the embedding process, Arnold scrambling transform is applied to the watermark image for security purposes. *DWT* is used to transform the cover image into four subbands LL_1, LH_1, HL_1 and HH_1. Since most of the image energy is compacted in LL_1, it is selected for embedding the watermark bits. *DFT* is then applied on the LL_1 sunband to produce the *DFT* coefficient matrix. *PSNR* and *NC* parameters are used to evaluate the performance of the technique.

A hybrid non-blind watermarking technique using *DWT* and Singular Value Decomposition (*SVD*) is proposed by Jane et al. (2014). Four subbands (*LL, HL, LH,* and *HH*) of cover image are generated using DWT transform, then the *SVD* is applied on the LL sub-band. The diagonal singular value coefficients are modified with the help of the scaling factor to embed the watermark bits. Coefficients of *LL* sub-band are reshaped with the aid of altered singular values and then inverse *DWT* is applied to generate a watermarked image. The efficiency of technique is evaluated using the *PSNR* parameter. The technique is tested against attacks like filtering, scaling, Gaussian, *JPEG* compression, rotation or cropping.

Laouamer and Tayan (2015) proposed a *DCT* based semi-blind watermarking technique for Quran images. The cover image is split into 8×8 blocks and *DCT* is applied to every block. *DCT* and Interpolation is used during embedding process. *PSNR*, *MSE*, Visual Information Fidelity (VIF), *UQI*, *SSIM*, Noise Quality Measure (*NQM*) and Visual Information Fidelity Criterion (*VIFC*) are used to evaluate performance of the technique.

Authenticity and copyright protection of printed images by using Wave Atom Transform (*WAT*) is achieved by Ahmad and Cheng (2018). This is the multipurpose technique that incorporates print scan resistant watermarking and hybrid hashing to support multiple applications for print scan images. One channel of color image is chosen to embed the watermark bits and the generation of image hash. The authors used green channel for both image hash calculation and embedding of the watermark since the green channel is known to be the least noisy channel.

A watermarking technique on the basis of *DCT* and Integer Wavelet Transform (*IWT*) for text images is proposed by Alotaibi and Elrefaei (2018). *IWT* is applied on cover image to create sub-bands and *DCT* is applied on low frequency sub-band. For each block- 9, 16, 25 and 36 coefficients are selected to embed the watermark. The *JPEG* compression, rotation, cropping, median filter, salt and pepper and histogram equalization attacks have been used. This technique is used for the purpose of protection. *MSE*, *PSNR*, *UQI*, *SSIM* and *NCC*

parameters are used to validate the technique.

A watermarking technique based on stable region and object fill-based for grayscale document images was suggested by Loc et al. (2018). The image processing operations are used to transform the document image into intermediate form to find its stable region. Object segmentation is then applied to find the separated objects in stable region. The performance of technique is measured by using imperceptibility, robustness and capacity against attacks like *JPEG* compression, geometric transformation as well as print and scan process.

Dang et al. (2019) proposed a *DWT* based blind watermarking technique to protect document images. Cover image is decomposed into n-level of frequency channels with the help of *DWT*. *QR* code of the watermark is embedded in a sub-bands of final level of *DWT*. Robustness of the technique is tested against attacks like JPEG compression, cropping, scaling as well as salt and pepper noise. *SSIM* and *PSNR* are the parameters used to measure the performance of technique.

Yuwei and Su (2020) proposed a *DCT* based semi blind watermarking technique. Cover document image is divided into blocks of equal size and *DCT* is applied on every block. Singular Value Decomposition (*SVD*) is applied on the selected blocks. Two dimensional *DCT* and *SVD* is also applied on watermark image. The technique shows good robustness, invisibility, low computational cost and high security.

A watermarking technique for digital documents by using encryption and compression is proposed by Singh et al. (2021). Multiple watermarks are embedded by using non sub-sampled contourlet transform, *DWT* and *SVD* transform. *SHA*-256 and Lempel Ziv Welch (*LZW*) are used to encrypt and compress the digital document, respectively. Multiple watermarks can be extracted from distorted cover image.

Distance Reciprocal Distortion Measure based Physical Embedding

Distance Reciprocal Distortion Measure (*DRDM*) measures distortion by applying a weighted matrix with every one of its weights calculated by the reciprocal of a relative distance from the center pixel. The amount of distortion is determined by flipping a particular pixel of a binary document image. Distance among the pixels plays a crucial role in the perception of distortion in document images.

A watermakring technique for binary document images is suggested by Lu et al. (2003). This technique provides security against tampering and authentication. The amount of distortion that occurred due to flipping a specific pixel in binary document images is measured using *DRDM*. This technique is derived from a combination of *DRDM* technique and 2-D shifting technique with an even-odd embedding approach.

A watermarking technique based on human visual perception for binary document images is proposed by

Lu et al. (2004). *PSNR*, *MSE* and *SNR* are the objective distortion measures considered in this technique. This technique relies on the calculation of distortion using a weighted matrix. The weights are calculated on the reciprocal basis of the *DRDM*.

Daraee and Mozaffari (2014) proposed a Fractal coding based watermarking technique. The fractal coding approach encodes a cover image. Particular range segments with prescribed criteria are selected so that bits of watermark image can be inserted uniformly over the entire cover image. The *DRDM* parameter is used for evaluating the technique's efficiency. Transparency as well as robustness of the technique is tested against attacks like as cropping, *JPEG* compression, Print-scan and photocopy, rotation, salt and pepper.

Image and Text based Physical Embedding

Image as well as text can be used in watermarking techniques. Watermarks created by using an image and text are combined to generate another watermark. This watermark is embedded in the document image to make it secure. This approach of watermark generation also enhances the robustness of watermarking technique.

A watermarking technique by using the combination of image and text watermark for document images is proposed by Jaseena and John (2011). The watermark bits are inserted in the content of text image and also text image is further encrypted by using *RSA* algorithm to provide the security. On the receiver side, the encrypted text is decrypted prior to the extraction phase. The extracted watermark bits are compared with original watermark to prove the document image.

A text image watermarking for printed documents is propsoed by Huang et al. (2019). Fourier descriptor is used to flip the trivial pixels with frequency information on the boundary of a character. Multiple bits watermark with respect to a single character is embedded with the help of quadratic quantization function. Quick Response (*QR*) code with high decoding reliability and robust error correction capability are used as a watermark to reduce the effect of bit error as well as enhance the robustness of the technique.

Ahvanooey et al. (2020) developed a intelligent text watermarking technique to protect Latin-based information from malicious attacks on social media. A watermark is inserted in the text which can be extracted to prove the of ownership whenever required. This technique is based on instance based learning mechanism and all text words are labelled that can be used to evaluate their integrity against attacks like forgery, tampering and plagiarism.

Syntactic Tree based Physical Embedding

The syntactic structures of the document image are represented by syntactic trees and generally these trees are not so large in size. These syntactic tree are used for document watermarking.

Atallah et al. (2002) developed a watermarking technique based on natural language for document images. This technique relies on the Text Meaning Representations (*TMR*) of the text sentences that are richer and larger trees that like the syntactic trees. The semantic marking scheme and syntactic are used together to design a system that can detect the tampered text without using any side information.

Meral et al. (2007) proposed a based natural language based watermarking technique for text document images. Original text image is used to generate a syntactic tree in which the syntactic hierarchies and functional dependencies are encoded. In order to embed the bits of watermark, sentences in syntax tree structures are used.

Edge based Physical Embedding

The characteristic of text document images can be identified by using the histogram of the edge directions. These characteristics are used for embedding the watermark bits. Edge directions histogram improves the robustness of the technique. These techniques have good embedding capacities as Edge pixels are in good number in the document images.

A watermarking technique based on edge direction histograms for grayscale text document is proposed by Kim and Oh (2004). The histogram is used to create empty spaces for embedding. Sobel edge director is used to find the edge strengths and directions for a grayscale document image. After that, each edge direction is quantized into 16 levels. The image is partitioned into a set of primitive blocks, using the concept of mother and child blocks. The child blocks are then used to embed the watermark data. English, Korean and Chinese document images have been used in the experiment to evaluate efficiency of the technique.

A high data capacity watermarking technique is proposed by Tirandaz et al. (2009) by using edge pixels of the cover image. In the embedding process, connected components of edge pixels are used to embed the watermark data. For blind data embedding, the total number of vertical and horizontal lines between two consecutive embeddable diagonal edge lines are taken as a parameter. The external boundary of a character is often used to embed data. Inner boundaries are used to enhance the embedding capacity of the technique.

Signature based Physical Embedding

Digital signature also can be used for physical embedding. For the authentication of images, digital signature and watermarking techniques are used. Digital signature is a cryptographic tool that is used to verify the authenticity as well as integrity of a digital images.

Yang et al. (2005) developed a semi-fragile watermarking technique to authenticate the text document images. This technique considers the smoothness and connectivity of the block. The block's content signature is generated and embedded in the block. A pixel's flippability depends on denoise pattern matching. During embedding process a block size of 7×7 is used and a moving window of size 3×3 is used for each block. The Look Up table consisting of the denoise pattern index is used. The documents in English and Chinese language are used as a cover image.

A watermarking technique based on document analyzer and signature generator for digital document is proposed by Qadir and Ahmad (2005). Document Analyzer and Signature (*DAS*) generator works on the user information, the actual text and its features. The number of watermark bits that can be embedded in document image are computed by *DAS*. The main contribution of this technique is that the watermarked image is the visually same as the input image.

Self-embedding watermarking appraoch is used by Singh et al. (2018) to propose a watermarking technique for digital documents. The technique provides detection of seal and signature entities. Recovery information is derived from these entities and embedded throughout the document after encryption. The pixel level is used to authenticate using three integrity check bits is based on location, neighborhood and pixel value.

Entropy based Physical Embedding

Entropy is also used in physical embedding watermakring. An entropy based watermarking technique for digital document images is suggested by (Kurup et al. (2007); Upadhyay and Chhabra (2021)). The smallest fonts that appear most frequently in the document are first identified followed by unique regions at word level where the embedding process causes lease perceptual distortion. Variations of the entropy are used to detect the beginning and end of the character, as well as the suitable positions in the word for embedding the data of the watermark.

Another entropy based watermarking technique for binary document images is proposed by Khan et al. (2011). Entropy is used to select blocks of the cover image with minimal perceptual distortion. This technique

provides good visual quality, reduces response time as well as computational complexity.

Block based Physical Embedding

Prior to the embedding process, document cover image is partitioned into blocks as it is easier to process a block than the entire image. The size of the block is determined as per the embedding approach.

A data hiding technique on the basis of pixel's connectivity for binary images authentication is proposed by Yang and Kot (2007). The flippability of the pixels is assessed before to the embedding process. The flipable pixel does not break the pixels' connections. Fixed Block (FB), Non-Interlaced Block (NIB) and Interlaced Block (IB) definitions are used to partition the image into blocks. In each block, only one bit of watermark image is embedded in each block. The efficacy of the approach is tested using a variety of pictures, including cartoons, French, Chinese, English, Japanese, and handwritten text.

Shivananda et al. (2014) proposed a fragile watermarking technique for document image. Cover document is partitioned into blocks of same size and a pseudo random mapping of each block is generated. The watermark is created using the pseudo random and is embedded in the corresponding block. Authentication information is created with the help of *LSB* value of every pixel in the block. A dual option parity check approach is used to authenticate the watermarked image. This technique is used for both recovery and tamper detection.

Wang et al. (2014) proposed an authentication technique using the principle of block patterns for binary images. The non-symmetrical blocks and dual pair block pattern are designed to improve the visual quality of watermarked images. To reduce the embedding process effects, two types of Matching Pair (*MP*) methods are used : internal *MP* adjustment and external *MP* adjustment. Chinese, English text images, Lena and Baboon images are used in the experiment. The efficiency of this technique is evaluated using *PSNR*, Edge line distortion, and bit rate.

Segmentation based robust watermarking technique for protection of document images was suggested by Chetan and Nirmala (2015). The block encoding approach is used to compress the binary watermark logo image. Empty and non-empty segments are formed based on the presence of information in the original document image. In order to obtain subbands, the two-level integer wavelet transformation is applied to the non-empty segments of the cover document image. To embed the compressed watermark bits in the lower subband blocks, quantization is used. *PSNR* and *NCC* parameters are used to determine the efficiency of the technique.

Rakhmawati et al. (2018) proposed a fragile watermarking technique for document image by using linear block mapping. This technique is used to authenticate the image by detecting the small changes in extracted

watermark. Chaotic map is used to spread the neighboring pixels of the document image to a mostly dispersed location. *PSNR* parameter is used to evaluate the performance of the technique.

Slope based Physical Embedding

Slopes of a letter can be used for physical embedding watermarking for document images. Characteristics of sloping letter of the language are utilized to embed the watermark bits.

A watermark technique for Farsi language based on sloping letters is proposed by Davarzani and Yaghmaie (2009). By changing the value of their slopes, watermark bits are embedded in four common slope letters. The key parts of the sloping letters are located below the baseline and the difference between letters are placed on top of them. Sloping letters generally appear in a distinct and associated form. The slope of the letter are determined as follows:

$$Slope(r) = \frac{L_r}{W_r} \tag{2.3}$$

where L_r and W_r are the vertical length and the horizontal width of a letter respectively.

Script Format based Physical Embedding

A document file has a particular format such as *PDF* or Open Document Format (*ODF*). These formats are smaller than other image file formats and are known to be more secure than other file formats.

A watermarking technique for document authentication using script format is suggested by Gonzalez-Lee et al. (2009). Watermark sequence is explicitly embedded in the document description file to modify the metrics of each character. The embedding process does not increase the size of watermarked image. *NCC* parameter is used for watermark detection.

A script format document authentication technique is developed by González-Lee et al. (2015). Watermark bits are embedded into the document file and the tamper detection capability is determined. If more than 0.25 % of total characters of the document are changed, then technique found to be able to detect alteration in the document.

Al-Haj and Barouqa (2017) proposed a watermarking technique for document images to be used in E-governmence. Second level *DWT* is applied on the cover image and *SVD* then applied on the wavelet subbands. Non-reversible embedding is performed on the diagonal elements of *DWT-SVD* decomposed document im-

age. *PSNR* and imperceptibility parameters are used to evaluate the performance against attacks like *JPEG* compression, salt and noise, Gaussian noise.

A watermarking technique based on Discarded Page Object for *PDF* documents is suggested by Zhang et al. (2017). The contents of *PDF* document are read with the help of translator in binary form. Advanced Encrypted Standard (*AES*) is used for encryption and decryption process. Robustness and invisibility parameters are used to evaluate the performance of the technique.

Chia et al. (2018) proposed a watermark technique for *PDF* document to improve the content accuracy extraction. When a watermark is embedded into the *PDF* document then watermark can affect the order of content, this technique handles this issue. Direct extraction of text from *PDF* and Optical Character Recognition (*OCR*) are used to improve the extraction of content.

A watermarking technique for *PDF* based on file page objects is proposed by Khadam et al. (2019). Huffman coding is used to compress the *PDF* document. Suitable page object is utilized to embed the watermark bits. Content as well as format of document is not affected because the watermark is embedded in *PDF* document page objects. The technique shows good robustness and imperceptibility.

Double watermarking technique for *PDF* document is proposed by Zhao et al. (2020). Data Encryption Standard (*DES*) is applied on watermark image to generate the hexadecimal watermark information and embed this hexadecimal sequence in the end of *PDF* file.

Kashida based Physical Embedding

Kashida, an Arabic character, used for adjacent letters, is used in the developmet of watermarking techniques. There are some rules for using Kashida in a document image that it can not be used at the beginning or end of a preposition and a word. These rules can be used to produce a watermark. Imperceptibility in these types of techniques depend on the average number of kashida per word.

Gutub et al. (2010) proposed a Kashida based watermarking technique in which watermark bits are embedded in Arabic characters. Embedding process does not alter contents of the text and may be placed before and after particular letters. The technique randomises the position of every kashida based on a random value. The random number assigned to each partition is determined by using a pseudo random number generator. The ratio of capacity is more than the existing watermarking techniques. It also provides good capacity, security and robustness.

Alginahi et al. (2013) proposed an improved kashida technique for copyright protection and authentication of Arabic document images. The kashidas are embedded in front of a particular characters. For bit 1, the kashida is set and for bit 0, it is omitted. In order to provide security, some rules are followed in the embedding process. The technique provides better imperceptibility.

A authentication technique based on frequency recurrence properties is proposed by Alginahi et al. (2014). in which kashida is inserted in front of specific characters. For bit 1, the kashida is set and for bit 0, it is omitted. This technique provides good security, capacity as well as robustness. However, several kashida characters may increase suspicion and may reduce the security and imperceptibility. Watermark bits are not embedded within every letters which decreases the embedding capacity of the technique. For short texts, the kashida approach is also not applicable. While the technique supports invisibility and is also vulnerable against attacks like copy and paste, retyping *etc*.

Letter Occurrence based Physical Embedding

Letters that appear in a document image may also be used for physical embedding. A document image consists of a number of words, letters and lines. The occurrence of letters is known to be embedding of watermark bits.

A text watermarking technique using a combination of image-plus-text watermarking is proposed by Jalil and Mirza (2010). Watermark bits are inserted in its embedding process through the use of double letters. First, the watermark image is divided into text and image. Alphabetical watermark is created by converting the image to an alphabet. Depending upon the preposition input and the size of the group, partitions and groups are formed. By using watermark and the second largest double letter occurrences from every group, the key generator produces an author key that is stored with the *CA* and used to authenticate the cover image.

A information hiding technique in vocalized Arabic text is proposed by Bensaad and Yagoubi (2011). Diacritics (vowel signs), which are optional to put, are used for embedding. In the embedding process, when the secret bit is 1 then use diacritics as it is, but if this is 0 then delete diacritics. The number of letters and spaces as well as the number of diacritics of the cover image are considered for embedding.

Kamaruddin et al. (2017) proposed an invisible digital watermarking method for Arabic digital document images. In Arabic, diacritics of the letters have a crucial role to play in their sense. Each paired letter with the diacritic and its Unicode standard is changed into *UTF*-8 form and *XOR* operation is used to generate the watermark key. This technique is also extended to sensitive text because it does not change the nature and text content.

There is no particular shape for Arabic letters and their shapes depend on their location in the word. This characteristics is used by Alotaibi and Elrefaei (2018) to propose two watermarking techniques. These techniques use the pseudo space in Arabic text document. These spaces make the connected letters appear separate. This space is used to embed watermark bits. The very first technique embeds the watermark bits in the text by adding a pseudospace in Arabic text by using dot character. Second technique adds normal space to the pseudo space, which improves the embedding capacity of the first techninque. This technique shows good robustness and imperceptibility against attacks like copy and paste, formatting and tempering, but it is perceptible against retyping attacks.

Hashing based Physical Embedding

A hash function is used to adjust discretionary size data to fixed-size values and returns hash codes, digests, or hashes. A fixed-size table called a hash table is created using these values and is used in the develoment of watermarking technique.

A watermarking technique by using character encoding and attributes for combined text of Chinese and English was suggested by Rui et al. (2013). The Message Digest 5 (*MD*5) hashing approach is used to encrypt the original watermark prior to its embedding. The technique can embed more than one bit in a single character and provides error correction mechanism. This technique is used for the protection of document images.

Unicode based Physical Embedding

Microsoft word supports the characteristics that can be used for physical embedding. Unicode extended character set are used in the development of watermarking techniques which provides a robustness, high imperceptibility and adequate embedding capacity.

Unicode extended characters are used by Al-maweri et al. (2016) to propose a watermarking technique for digital documents. Two lookup tables are designed to divide the available characters into two groups. The first group implies that 0s are embedded and the second group implies that 1s are embedded. This technique demonstrates high imperceptibility and robustness for attacks like conversion, copying, addition as well as deletion. The robustness analysis showed that the technique tolerates almost all of the possible attacks and the watermark is retrieved with high precision. Capacity assessment indicates that technique has a excellent payload capacity of around 2 bits per word. The watermark does not survive retyping and font change attacks, and demonstrates only a certain degree of resistance to attack reordering. This Technique provides protection

to the documents images.

Text watermarking technique by using homoglyph characters substitution for latin symbols was suggested by Rizzo et al. (2016). It conserves the shape and content without transferring the text to an image. It reveals invisibility, preserves the content's properties and is also blind in nature. The technique utilizes alternate Unicode symbols to make sure visual indistinguishability as well as length conservation. The symbols selected are converted into same symbols and analyzed as well as encrypted by Unicode. This technique used a set of data of 1.8 million New York papers to analyse its performance.

Rizzo et al. (2019) proposed a text watermarking technique to protect the intellectual property of document images. The technique is based on homoglyph characters substitution for white-spaces and latin symbols. The technique does not alter content of text and watermark is generated with the help of hash function is visually indistinguishable from the original text content. The technique shows good robustness against attacks like partial copy and paste attack.

Data Mining based Physical Watermarking

A watermarking technique based on data mining for the security of copyright and verification of ownership was suggested by Khadam et al. (2019). Data mining principles are used to select features from document image to embed watermark bits. The techniques provides copyright protection for local and cloud computing paradigm in text documents. In order to test attacks like formatting, addition, and deletion, 20 separate text documents have been used. The technique is capable of achieving a high degree of imperceptibility. *PSNR* between cover and watermarked image is between 64.67% and 71.03%, and *SSIM* between original watermark and extracted watermark is between 99.92% and 99.99%. The technique shows good robustness and also resists attacks like formatting formatting.

Convolution Neural Network based Watermarking

A watermarking technique for handwritten documents based on Fully Convolution Network (*FCN*) was suggested by Cu et al. (2018). Mean value of document content is used to replace the gray level with highest values by using a pre-processed. *FCN* is used to find the watermarking region that is used to hide the watermark bits. Imperceptibility and robustness are parameters used to test the efficiency of technique.

Li et al. (2020) proposed a technique for document images by using Convolution Neural Network (*CNN*). Three views of document images are generated by extracting table frame, text region and shape. These views are

merged and resized to a standard image. Three classic methods are used to evaluate the proposed technique.

The different attacks and metrics used by the authors to measure the efficiency of the existing physical watermarking techniques are summarized in Table 2.2.

Table 2.2: Types of Attacks and Performance Evaluation of Physical Embedding Watermarking Techniques

Technique	Types of Attack					Other Evaluation Metric
	Crop	Deletion	Reordering	Synonym Substitution	Syntatic Transformation	
[Brassil *et al.*, 1994]	No	No	No	No	No	Robustness
[Brassil *et al.*, 1995]	No	No	No	No	No	Robustness
[Amano and Misaki, 1999]	No	No	No	No	No	Robustness
[Chotikakamthorn, 1999]	No	No	No	No	No	Capacity
[Lu *et al.*, 2002]	Yes	No	No	No	No	Robustness
[Atallah *et al.*, 2003]	No	No	No	No	No	No
[Kim and Oh, 2004]	No	No	No	No	No	Robustness
[Yang and Kot, 2004]	No	No	No	No	No	Capacity
[Yang *et al.*, 2005]	No	No	No	No	No	No
[Qadir and Ahmad, 2006]	No	No	No	No	No	No
[Kurup *et al.*, 2007]	No	No	No	No	No	No
[Meral *et al.*, 2007]	No	No	No	No	No	Robustness and Capacity
[Yang and kot ,2007]	No	No	No	No	No	Capacity
[Zhu *et al.*, 2006]	No	No	No	No	No	Robustness and Capacity
[Davarzani and Yaghmaie, 2009]	No	No	No	No	No	Capacity
[Gonzalez-Lee *et al.*, 2009]	No	No	No	No	No	NCC

[Tirandaz *et al.*, 2009]	No	No	No	No	No	Capacity
[Gutub *et al.*, 2010]	No	No	No	No	No	Average Capacity
[Bensaad and Yagoubi, 2011]	No	No	No	No	No	Capacity
[Jaseena and John, 2011]	Yes	Yes	Yes	No	No	No
[Khan *et al.*, 2011]	No	No	No	No	No	Computational Cost
[Zhu *et al.*, 2012]	No	No	No	No	No	Robustness
[Alginahi *et al.*, 2013]	No	No	No	No	No	Average Capacity
[Li and Wu, 2013]	Yes	No	No	No	No	Robustness
[Rui *et al.*, 2013]	No	No	No	No	No	No
[Alginahi *et al.*, 2014]	No	No	No	No	No	Average Capacity
[Chetan and Nirmala, 2014]	No	Yes	Yes	No	No	PSNR
[Daraee and Mozaffari, 2014]	Yes	No	No	No	No	Transparency and Robustness
[Jane *et al.*, 2014]	Yes	No	No	No	No	No
[Wang *et al.*, 2014]	No	No	No	No	No	PSNR and Capacity
[Chetan and Nirmala, 2015]	Yes	No	No	No	No	PSNR
[Gonzalez-Lee *et al.*, 2015]	No	No	No	No	No	Cross-correlation
[Laouamer and Tayan, 2015]	No	No	No	No	No	Robustness
[Rizzo *et al.*, 2016]	No	No	No	No	No	Memory Complexity
[Al-Maweri *et al.*, 2016]	No	Yes	Yes	No	No	Imperceptibility and capacity
[Alotaibi and Elrefaei, 2016]	No	Yes	Yes	No	No	Capacity
[Al-Haj and Barouqa, 2017]	No	No	No	No	No	PSNR and Imperceptibility

[Kamaruddin *et al.*, 2017]	No	No	No	No	No	Memory consumption and time complexity
[Alotaibi and Elrefaei, 2018]	Yes	No	No	No	No	Imperceptibility and Robustness
[Loc *et al.*, 2018]	No	No	No	No	No	Imperceptibility and Robustness
[Loc *et al.*, 2018]	No	No	No	No	No	Imperceptibility, Capacity and Robustness
[Rakhmawati *et al.*, 2018]	No	No	No	No	No	PSNR
[Dang *et al.*, 2019]	Yes	No	No	No	No	SSIM and PSNR
[Khadam *et al.*, 2019]	No	No	No	No	No	Robustness and Imperceptibility
[Rizzo *et al.*, 2019]	No	Yes	No	No	No	Robustness and Capacity
[Yuwei and Su, 2020]	Yes	No	No	No	No	PSNR
[Zhao *et al.*, 2020]	No	No	No	No	No	Robustness
[Singh *et al.*, 2021]	Yes	No	No	No	No	SSIM and PSNR

2.4 Objectives

On the basis of the gaps in the existing techniques of document images, following objectives have been formulated.

1. To analyze existing watermarking techniques for document images.
2. To develop efficient watermarking technique for protection and authentication of Gray scale document images.
3. To develop efficient watermarking technique for protection and authentication of color document image,
4. To compare the proposed techniques with existing watermarking techniques for document images.

CHAPTER 3

Tamper Detection Technique for Document Images using Zero Watermarking in Wavelet Domain

.

3.1 Introduction

In this Chapter, a tamper detection technique for document iages is proposed. Lifting Wavelet Transform is used on the cover document image to generate subbands of the cover image. These subbands are further divided into non-overlapping blocks of same size. A zero watermark is generated by using the features of these blocks. This watermark is combined with the key watermark to create a meaningful watermark. This meaningful watermark is stored with a trusted authority. On the receiver side, a watermark is generated using the received image and compared with the meaningful watermark to check the authenticity of the image. *SSIM*, *BER*, *PSNR* are evaluated to show the effectiveness of the proposed technique.

Contents of the work presented in this Chapter have been published in *Computer and Electrical Engineering*, Vol. 89, pp. 106925(1-11), 2021. (SCI Indexed)

3.2 Preliminary

Lifting Wavelet Transform (*LWT*) used in the proposed technique is discussed in this section. Lifting wavelet transform is used to get the subbands of cover document image. These subbands are further partitioned into non-overlapping blocks of the same size. Features of each block are extracted to create a zero watermark.

3.2.1 Lifting Scheme

Lifting scheme is an approach to design and implement *LWT* on the given input data Sweldens (1998). In this scheme, the convolution operation in *LWT* is performed using wavelet filters Daubechies and Sweldens (1998). This scheme required low computation, since it does not use any complex mathematical operations. It operates on in-memory input data, which means that no additional memory space is required compared to *DWT*. The basic steps of the scheme are shown in Figure 3.1.

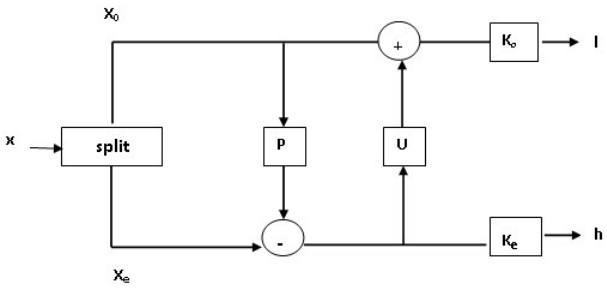


Figure 3.1: Forward Lifting Scheme

Consider *X*[*i*, *j*] as the input data. In forward lifting scheme, following steps, along the rows of the input image, are carried out:

i. Splitting: In this step, the image data is split into two subsets i.e. X_e and X_o subsets having even and odd indexed pixels respectively.

$$X_e[i,j] = X[2i,j] \tag{3.1}$$

$$X_o[i,j] = X[2i+1,j] \tag{3.2}$$

ii. Prediction: This step predicts the odd coefficients from the even coefficients X_e by using the prediction

filter p_i and then replaces the next new odd coefficients, recursively. This operation can be written mathematically as

$$X_o[i,j] = X_o[i-1,j] - p_i \times X_e[i-1,j] \tag{3.3}$$

iii. Update: This step updates the even indexed samples $X_e[i,j]$ from the new odd coefficients $X_o[i,j]$ by using updation filter u_i and then replace the old even coefficients by the new even coefficients, recursively. Mathematically, this operation is expressed as

$$X_e[i,j] = X_e[i-1,j] + u_i \times X_o[i,j] \tag{3.4}$$

iv. Normalization: The outputs of the intermediate lifting steps are normalized by multipling with K_0 and K_e. This step is performed to preserve the energy of the input image.

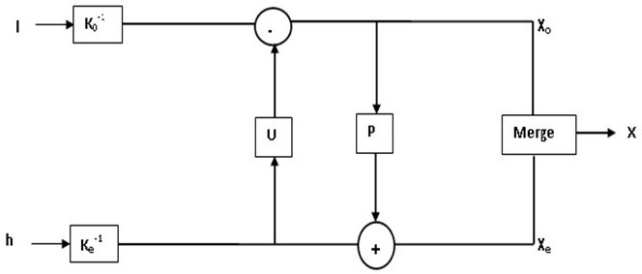


Figure 3.2: Inverse Lifting Scheme

These steps are also performed along the columns of the updated data of the input cover image to get four subbands. In Inverse lifting scheme, we perform the steps used for forward lifting transform in reverse direction, as depicted in Figure 3.2.

One time implementation of *LWT* produces four subbands of the input image. Wavelet decomposition of $R-1$ level is associated with *R* resolution levels from 0 to $R-1$. At each level, lower subband can be further transformed to get next level subbands. For example, LL_{R-1} subband is decomposed to get LL_{R-2}, LH_{R-2}, HL_{R-2}, and HH_{R-2} subbands. This process can be executed until the sufficient number of subbands has been obtained. The general structure of the lifting scheme is illustrated in Figure 3.3.

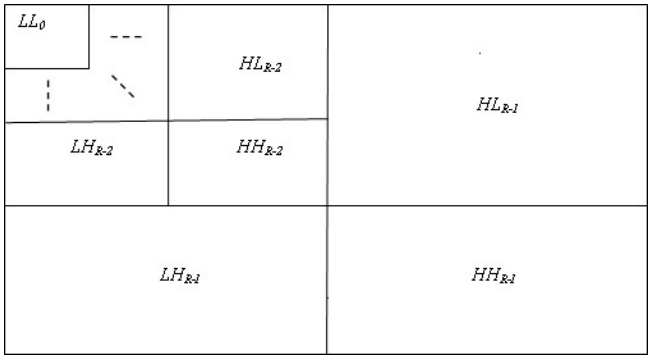


Figure 3.3: Lifting Scheme Structure

3.3 Proposed Watermarking Technique

The proposed technique is made up of two algorithms. The first algorithm is used to create a visual watermark and the second algorithm is used to authenticate and locate a tampered image. The basic idea behind the document watermarking approach is shown in Figure 3.4.

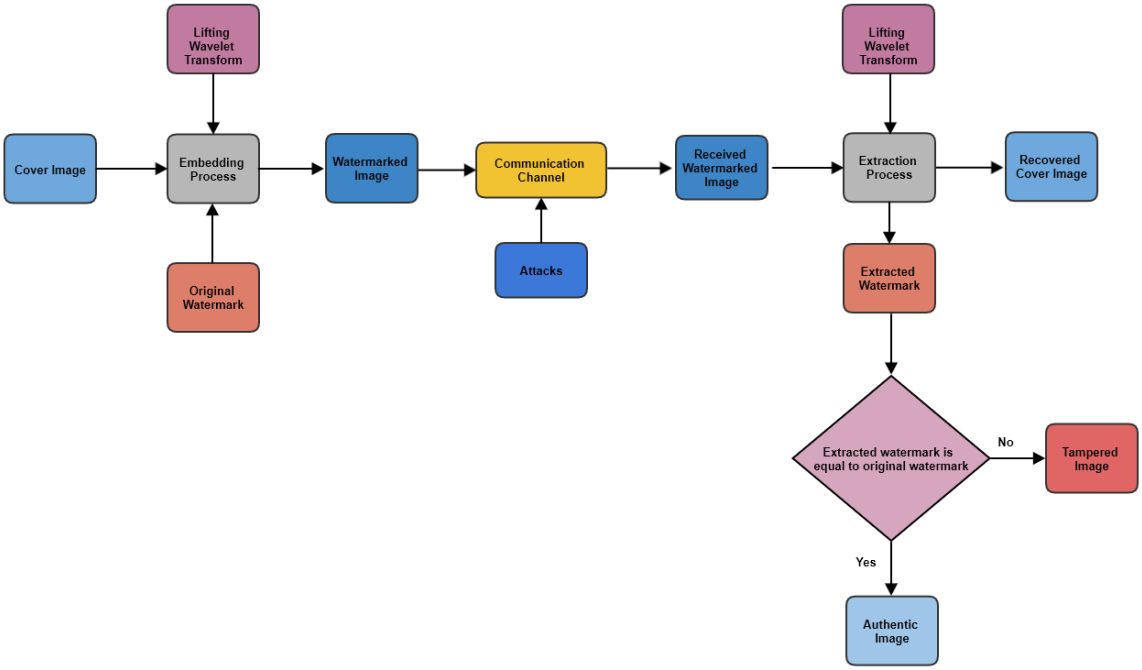


Figure 3.4: Flowchart of proposed technique

The zero watermark generation algorithm is used to generate a meaningful watermark using the features of cover image. Firstly, *LWT* is applied on the cover image to generate its subbands. These subbands are then divided into non-overlapping blocks of equal size. Each block's mean value is calculated and number of

wavelet coefficients larger and smaller than that mean value are counted. These wavelet coefficients are used to generate the watermark bits. The final visual watermark is generated with the help of a key watermark and the generated watermark. The final visual watermark is stored with the trusted authority and can be used to authenticate the received image whenever required.

3.3.1 Zero Watermark Generation Algorithm

Algorithm 1: Zero Watermark Generation Algorithm

Input: Input Image *I*; Key Watermark of size equal to number of blocks of cover image

Output: Meaningful watermark fw

Apply *LWT* on the input image *I* to get its subbands.

These subbands are further partitioned into non-overlapping blocks b_i of equal size.

Repeat the following steps for each of the b_i blocks.

Measure the mean value of each of the block and store into μ_i.

Count the number of wavelet coefficients larger and smaller than μ_i and store it in $cnt1_i$ and $cnt2_i$.

If $cnt1_i \geq cnt2_i$ then

    watermark bit w_i=1

else

    watermark bit w_i=0

Read the key watermark to generate the final visual watermark fw

If w_i==0 and kw_i==0 then

    fw_i=0

else if w_i==1 and kw_i==0 then

    fw_i=0

else if w_i==0 and kw_i==1 then

    fw_i=1

else

    fw_i=1

end if

Final visual watermark is stored with the Trusted Authority.

3.3.2 Document Image Authentication Algorithm

Algorithm 2: Document Image Authentication Algorithm

Input: Document Image I'; Meaningful Watermark received from trusted authority; Key Watermark

Output: Authenticity of Document Image I' as well as its tampered regions.

Apply *LWT* on the input image I' to get its subbands.

These subbands are further partitioned into non-overlapping blocks b'_i of equal size.

Repeat the following steps for each of the block b'_i.

Measure the mean value of each of the block and store into μ'_i.

Count the number of wavelet coefficients larger and smaller than μ'_i and store them in $cnt1'_i$ and $cnt2'_i$.

If $cnt1'_i \geq cnt2'_i$ then

    watermark bit w'_i=1

else

    watermark bit w'_i=0

Read the key watermark to generate the final visual watermark fw'

If w'_i==0 and kw_i==0 then

    fw'_i=0

else if w'_i==1 and kw_i==0 then

    fw'_i=0

else if w'_i==0 and kw_i==1 then

    fw'_i=1

else

    fw'_i=1

end if

Watermarks fw and fw' are compared. If both are identical then the image is authentic otherwise it is a tampered image.

If the image is tampered, identify the blocks where the values of fw and fw' are different. Positions of these blocks indicate the regions being tampered with. These regions give the localization of affected regions.

This algorithm takes as inputs a watermarked image, key watermark and meaningful visual watermark. The watermarked image and key watermark are combined to generate a meaningful watermark. If this watermark

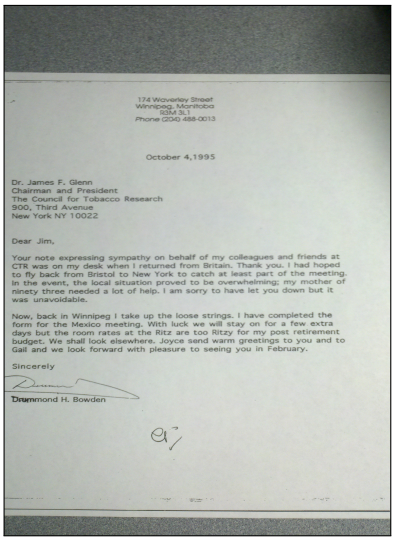
matches the received meaningful watermark, the image is authentic else it has been tampered. If the image has been tampered, mismathcing blocks are used to locate the locations where the values of both the watermarks differ. The locations of these blocks denote the area that have been tampered. These regions provides the localizations of tampered regions.

3.4 Experimental Results and Performance Analysis

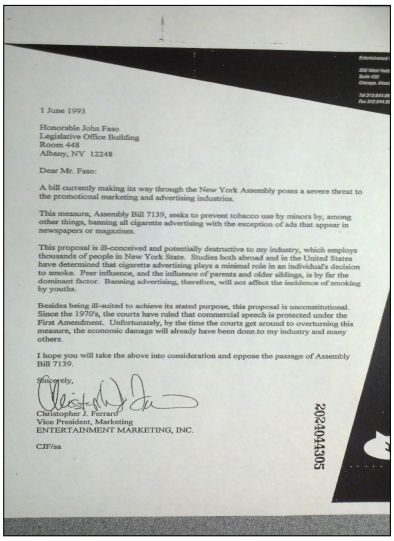
The proposed technique is implemented in R2019a version of *MATLAB* tool. For this implementation, *DIQA* dataset [Kumar et al. (2013)] images have been considered, some of which are shown in Figure 3.6. *LWT* is applied interactively on these images upto 5th level to create subbands. These subbands are divided into blocks to extract the features. These features are combined with the key watermark to generate final zero watermark. These images are being tampered with at various locations. Proposed technique is developed to detect the tamper localtion in text and non-text regions while existing techniques works for the text regions only. Some of the tampered images are shown in Figure 3.7. Key watermark considered in this experiment is shown in Figure 3.5. Meaningful watermark using different images are shown in Figure 3.8 and corresponding reconstructed meaningful watermarks are shown in Figure 3.9. *SSIM* and *BER* parameters are used to evaluate the performance of the technique.



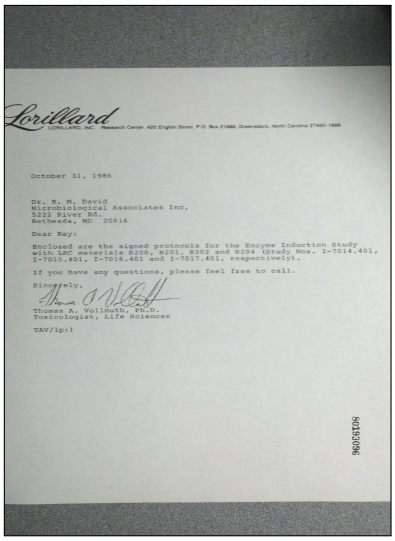
Figure 3.5: Key Watermark



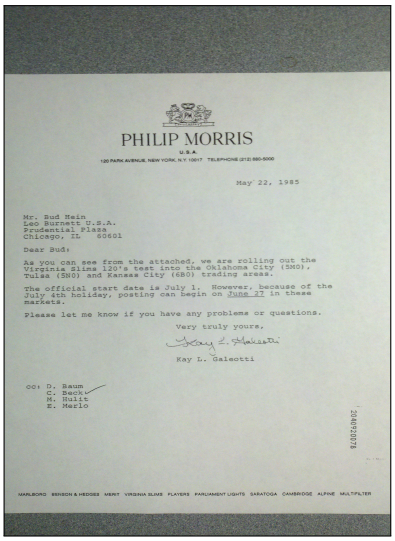
(a) 2012-04-16_17-42-48_976



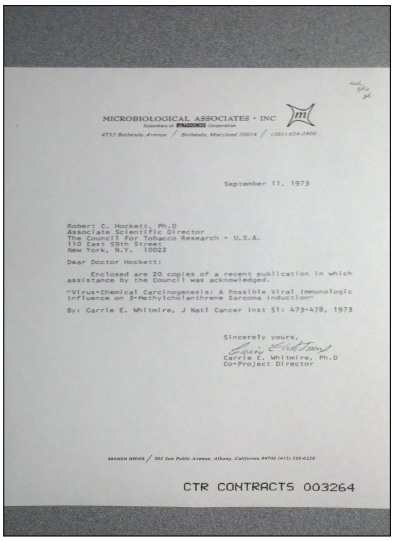
(b) 2012-04-16_17-32-27_295



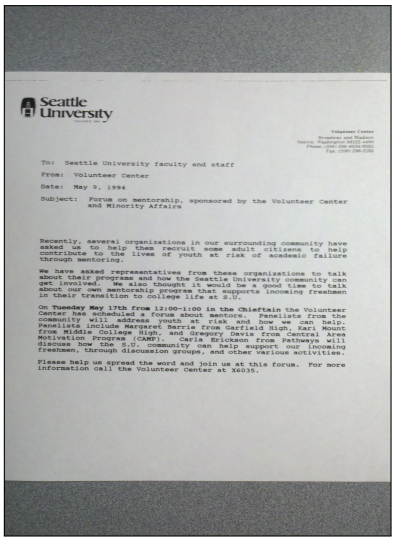
(c) 2012-04-16_17-35-31_279



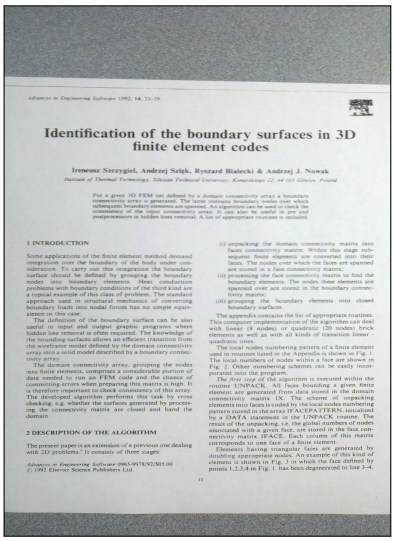
(d) 2012-04-17_17-37-56_610



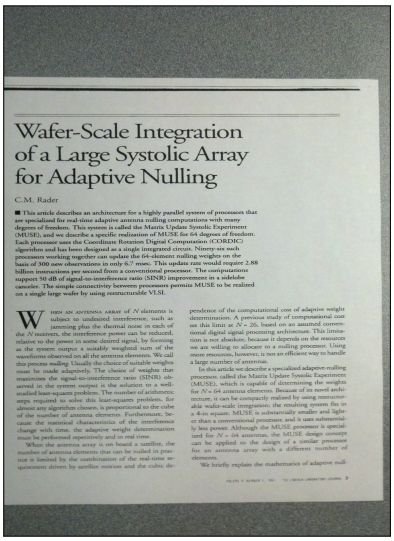
(e) 2012-04-17_17-40-31_436



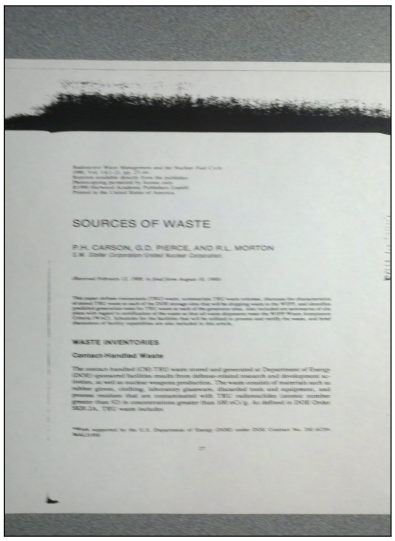
(f) 2012-04-23_12-27-02_949



(g) 2012-04-23_13-54-17_17

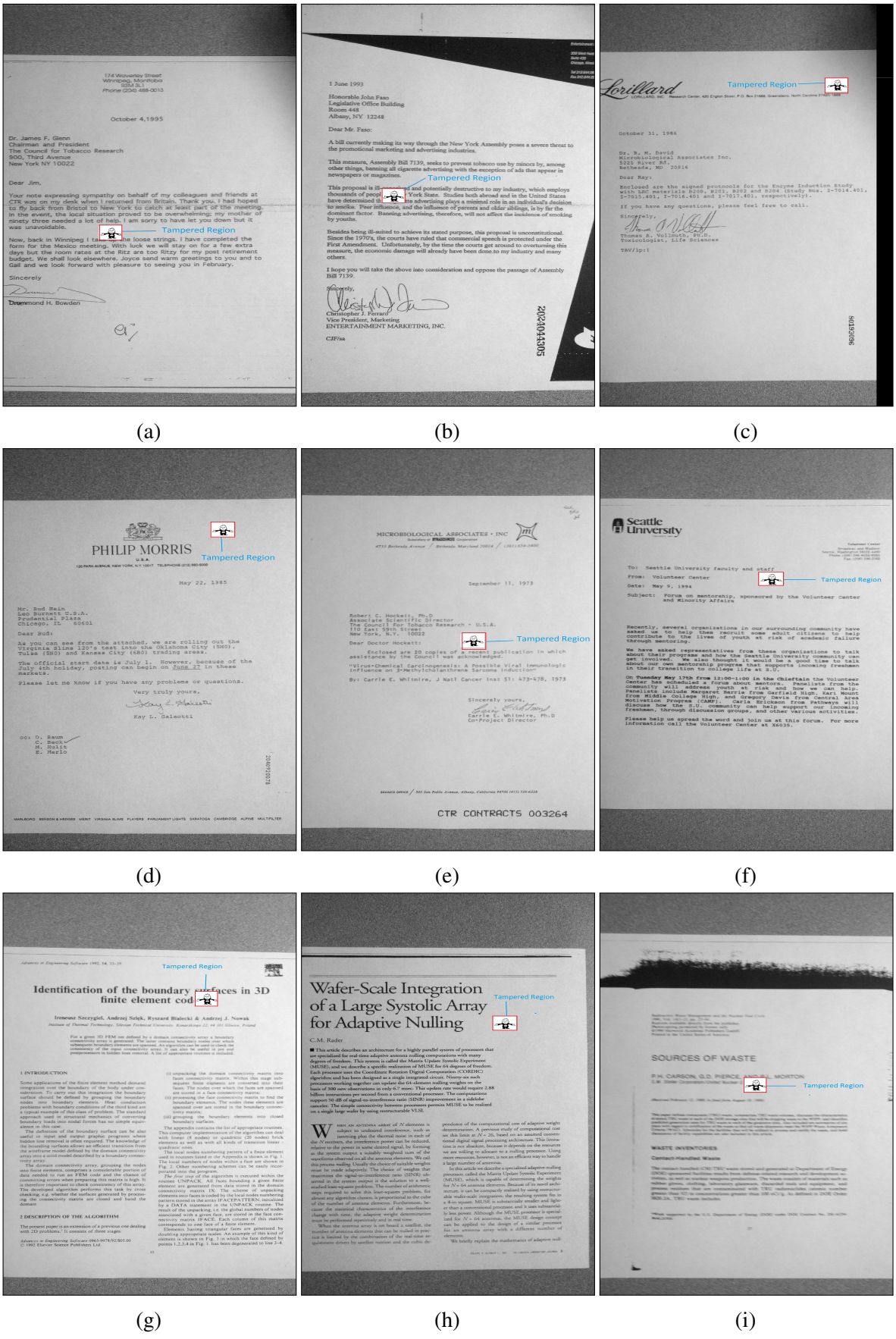


(h) 2012-04-23_13-58-38_54



(i) 2012-04-23_16-14-33_660

Figure 3.6: Original Document Images of DIQA Dataset

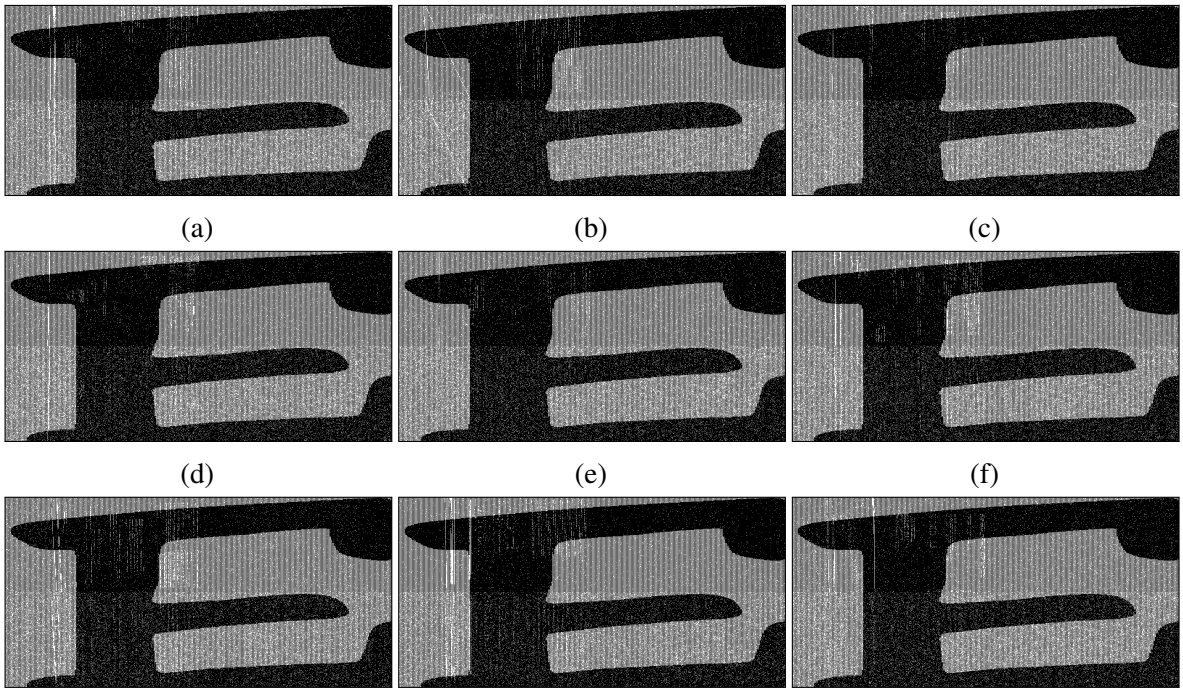


(a) (b) (c)

(d) (e) (f)

(g) (h) (i)

Figure 3.7: Tampered Document Images Corresponding to Original Images of Figure 3.6

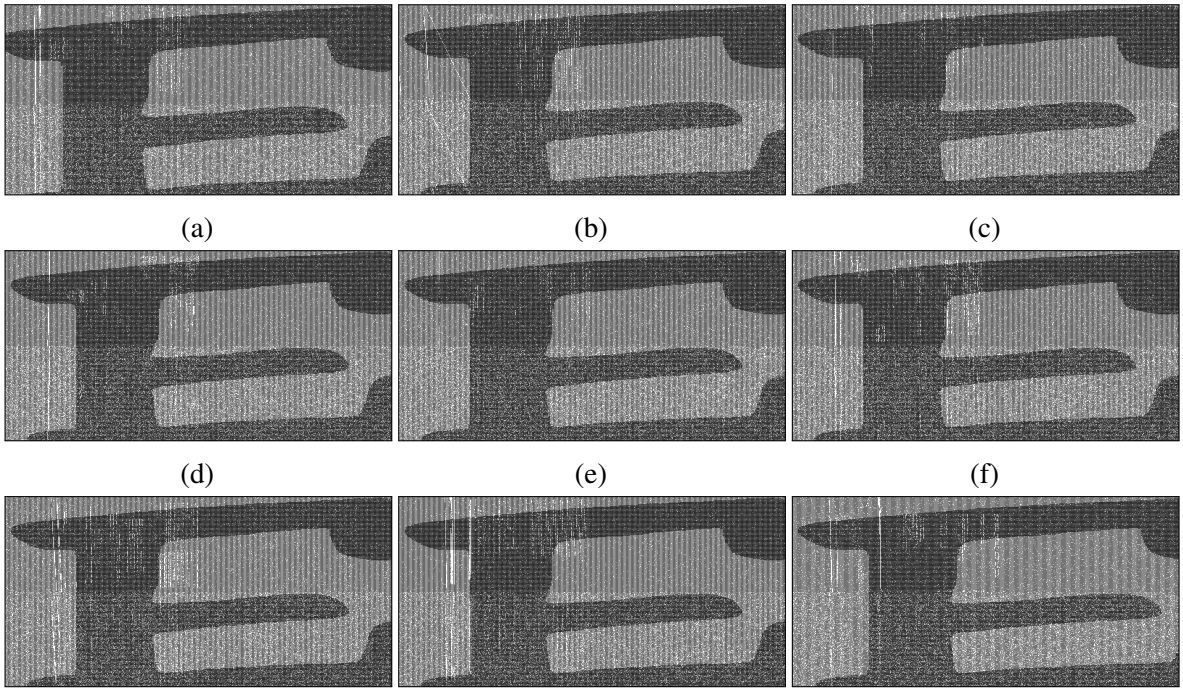


(a) (b) (c)

(d) (e) (f)

(g) (h) (i)

Figure 3.8: Meaningful Watermark corresponding to the images of Figure 3.6



(a) (b) (c)

(d) (e) (f)

(g) (h) (i)

Figure 3.9: (a)-(i) Watermark Extracted from Corresponding Tampered Images of Figure 3.7

SSIM values of the images considered for this experiment are shown in Table 3.1. Block sizes of 4×4, 8

$\times$ 8 and 16 $\times$ 16 have been used to find *SSIM* values between the original image and its tampered version.

Table 3.1: *SSIM* values between original zero watermark and extracted watermark at various block sizes

Image	Block Size	SSIM	Block Size	SSIM	Block Size	SSIM
2012-04-16_17-42-48_976	4 $\times$ 4	0.45	8 $\times$ 8	0.58	16 $\times$ 16	0.71
2012-04-16_17-32-27_295	4 $\times$ 4	0.43	8 $\times$ 8	0.49	16 $\times$ 16	0.68
2012-04-16_17-35-31_279	4 $\times$ 4	0.44	8 $\times$ 8	0.47	16 $\times$ 16	0.62
2012-04-17_17-37-56_610	4 $\times$ 4	0.46	8 $\times$ 8	0.51	16 $\times$ 16	0.63
2012-04-17_17-40-31_436	4 $\times$ 4	0.37	8 $\times$ 8	0.53	16 $\times$ 16	0.70
2012-04-23_12-27-02_949	4 $\times$ 4	0.42	8 $\times$ 8	0.49	16 $\times$ 16	0.64
2012-04-23_13-54-17_17	4 $\times$ 4	0.37	8 $\times$ 8	0.45	16 $\times$ 16	0.69
2012-04-23_13-58-38_54	4 $\times$ 4	0.39	8 $\times$ 8	0.53	16 $\times$ 16	0.70
2012-04-23_16-14-33_660	4 $\times$ 4	0.43	8 $\times$ 8	0.52	16 $\times$ 16	0.72
2012-04-23_16-17-36_15	4 $\times$ 4	0.42	8 $\times$ 8	0.43	16 $\times$ 16	0.64

From Table 3.1, one can include that *SSIM* values between the original watermark and reconstructed watermark are very less. From this it can be inferred that proposed technique is capable to detect the tampered image. *BER* of the received images is calculated by using different block size and shown in Table 3.2.

Table 3.2: Bit Error Rate of Various Image at Different Block Size

Image	Block Size	*BER*	Block Size	*BER*	Block Size	BER
2012-04-16_17-42-48_976	4 $\times$ 4	99.94	8 $\times$ 8	99.16	16 $\times$ 16	98.13
2012-04-16_17-32-27_295	4 $\times$ 4	99.94	8 $\times$ 8	99.19	16 $\times$ 16	98.42
2012-04-16_17-35-31_279	4 $\times$ 4	99.96	8 $\times$ 8	99.15	16 $\times$ 16	98.62
2012-04-17_17-37-56_610	4 $\times$ 4	99.83	8 $\times$ 8	99.21	16 $\times$ 16	98.32
2012-04-17_17-40-31_436	4 $\times$ 4	99.55	8 $\times$ 8	99.11	16 $\times$ 16	98.13
2012-04-23_12-27-02_949	4 $\times$ 4	99.61	8 $\times$ 8	99.18	16 $\times$ 16	98.29
2012-04-23_13-54-17_17	4 $\times$ 4	99.69	8 $\times$ 8	99.14	16 $\times$ 16	98.41
2012-04-23_13-58-38_54	4 $\times$ 4	99.70	8 $\times$ 8	99.08	16 $\times$ 16	98.17
2012-04-23_16-14-33_660	4 $\times$ 4	99.71	8 $\times$ 8	99.13	16 $\times$ 16	98.27
2012-04-23_16-17-36_15	4 $\times$ 4	99.62	8 $\times$ 8	99.19	16 $\times$ 16	98.17

From Table 3.2, it can be inferred that more than 98 percent of the watermark bits are lost when the image is tampered with. The proposed technique is therefore capable of detecting that the image is being tampered with.

Localization of the tampered region is calculated by using tampered block locations as if a block is tampered then its features are changed. These changes are used to detect the block tampering. If the extracted bit does not match the corresponding original watermark bit this implies that the block is tampered with. The index of the tampered block helps to localize the tampered regions.

The impact of the block size on *SSIM* and *BER* was analyzed and shown in Figure 3.10 and 3.11. From these figures, it can be concluded that for block size of 4×4, *BER* is higher than other block sizes. While the *SSIM* values are higher for block sizes of 16×16. The reason for this is that in a small block size, tampering affects the large number of wavelet coefficients in the adjacent regions of the tamper compared to a large block size.

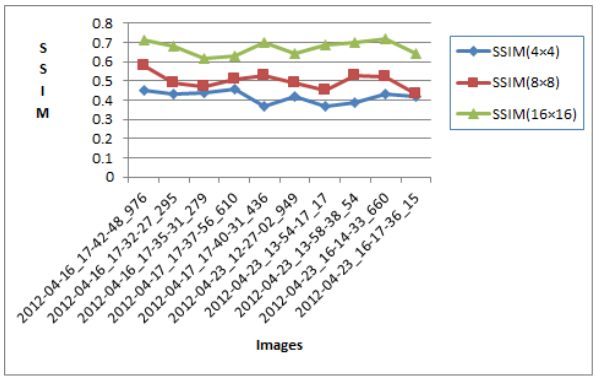


Figure 3.10: *SSIM* Comparison of the Different Images at Different Block Size

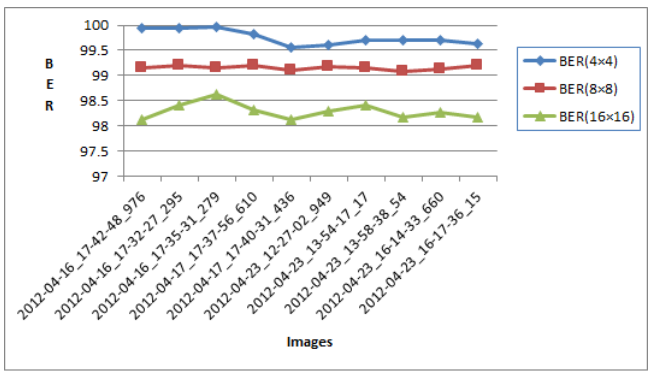


Figure 3.11: *BER* Comparison of the Different Images at Different Block Size

Robustness of the proposed technique is shown in Table 3.3. Robustness is tested by using the *PSNR* value. *PSNR* value is calculated against some attacks with respect to the different images.

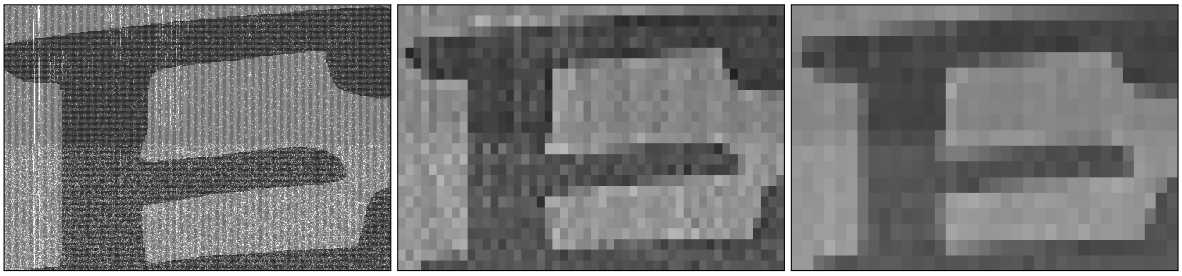
Table 3.3: Robustness Results of Proposed Technique against some attacks

Image	Types of Attacks	*PSNR*	Types of Attacks	*PSNR*
2012-04-16_17-42-48_976	Median Filter	36.88	Rotation (45°)	20.33
	Salt & Pepper Noise 0.001	41.74	Cropping	59.45
2012-04-16_17-32-27_295	Median Filter	37.88	Rotation (45°)	21.55
	Salt & Pepper Noise 0.001	42.21	Cropping	58.79
2012-04-16_17-35-31_279	Median Filter	36.18	Rotation (45°)	23.25
	Salt & Pepper Noise 0.001	43.73	Cropping	56.89
2012-04-17_17-37-56_610	Median Filter	39.28	Rotation (45°)	24.51
	Salt & Pepper Noise 0.001	44.39	Cropping	55.17
2012-04-17_17-40-31_436	Median Filter	40.23	Rotation (45°)	25.53
	Salt & Pepper Noise 0.001	46.21	Cropping	54.77
2012-04-23_12-27-02_949	Median Filter	41.42	Rotation (45°)	26.35
	Salt & Pepper Noise 0.001	47.29	Cropping	55.11
2012-04-23_13-54-17_17	Median Filter	42.44	Rotation (45°)	28.08
	Salt & Pepper Noise 0.001	48.46	Cropping	56.23
2012-04-23_13-58-38_54	Median Filter	43.12	Rotation (45°)	27.17
	Salt & Pepper Noise 0.001	47.16	Cropping	57.35
2012-04-23_16-14-33_660	Median Filter	42.29	Rotation (45°)	28.59
	Salt & Pepper Noise 0.001	48.53	Cropping	58.87
2012-04-23_16-17-36_15	Median Filter	42.55	Rotation (45°)	27.34
	Salt & Pepper Noise 0.001	46.16	Cropping	57.29

Robustness is also tested by using the *PSNR* value against *JPEG* compression attacks. *PSNR* value is calculated against *JPEG* compression attacks with respect to the different images shown in Table 3.4. Value of *PSNR* is increasing as the quality parameters is increasing as shown in Table 3.4. *PSNR* value is lowest when quality parameter is 10 and highest when quality parameter is 30.

Table 3.4: Robustness results of Proposed Technique against *JPEG* Compression Attacks

Image	Quality Parameters (Q)	PSNR
2012-04-16_17-42-48_976	10/20/25/30	42.44/46.83/47.87/49.41
2012-04-16_17-32-27_295	10/20/25/30	41.23/44.69/45.91/47.49
2012-04-16_17-35-31_279	10/20/25/30	43.66/45.83/46.77/48.72
2012-04-17_17-37-56_610	10/20/25/30	42.61/44.91/46.53/47.19
2012-04-17_17-40-31_436	10/20/25/30	41.13/43.95/44.89/45.61
2012-04-23_12-27-02_949	10/20/25/30	43.17/46.69/48.21/49.05
2012-04-23_13-54-17_17	10/20/25/30	42.29/45.56/47.48/48.89
2012-04-23_13-58-38_54	10/20/25/30	41.79/44.07/46.96/47.59
2012-04-23_16-14-33_660	10/20/25/30	42.43/45.79/47.15/48.89
2012-04-23_16-17-36_15	10/20/25/30	42.71/44.39/46.29/47.19



(a) Proposed Technique (b) Chetan and Nirmala (2015) (c) Jalil et al. (2010b)

Figure 3.12: Extracted Watermark comparison with the existing techniques from Corresponding Tampered Images of Figure 3.7

Extracted watermark comparison of proposed technique with the existing techniques shown in 3.12. The quality of the extracted watermark of proposed technique is good as compared to the quality of extracted watermark of the existing techniques. Proposed technique is compared with the existing techniques applicable to document images. This comparison is shown in Table 3.5.

Table 3.5: Comparison of *BER* of Proposed Technique with the Existing Techniques

Image	Proposed Technique	Jalil et al. (2010b)	Chetan and Nirmala (2015)
2012-04-16_17-42-48_976	99.94	49.94	72.29
2012-04-16_17-32-27_295	99.94	68.28	74.15
2012-04-16_17-35-31_279	99.96	49.52	75.38

2012-04-17_17-37-56_610	99.83	46.32	75.98
2012-04-17_17-40-31_436	99.55	45.27	75.09
2012-04-23_12-27-02_949	99.61	39.28	71.69
2012-04-23_13-54-17_17	99.69	49.29	76.29
2012-04-23_13-58-38_54	99.70	39.46	74.29
2012-04-23_16-14-33_660	99.71	49.37	68.29
2012-04-23_16-17-36_15	99.57	45.23	69.29

Table 3.5 shows that the proposed technique performs better than that of Jalil et al. (2010b) and Chetan and Nirmala (2015) for each of the images considered. The data given in this table for the existing techniques is produced by implementing these techniques in *MATLAB* tool as the proposed technique is also implemented in the same tool. Jalil et al. (2010b) technique works on the text present in the document image and if the unauthorized user tampers with the regions where text is not present, the output of the technique degrades. Chetan and Nirmala (2015) technique classifies image blocks and embeds data into complex blocks using the concept of threshold. If unauthorized users tamper with smooth regions, the performance of the technique will be degraded. There is no such problem with the proposed technique as a result of which the performance of the proposed technique is higher than the existing techniques.

3.5 Conclusion

A tamper detection technique for document images has been proposed in this work. The features of the transformed document image are used to create the zero watermark. This watermark is stored by a trusted authority. The image is tampered to validate the proposed technique and original watermark is compared to the watermark produced using tampered image to prove the authenticity of the cover image. Using this technique, the tampered regions of the cover image can be easily located. Block size has also been observed to influence the tamper detection of the document image. The efficiency of the proposed technique can be improved by integrating the spatial and transform domain features of the cover image. Maximum value of *BER* is 99.96 in case of 4×4 block size and *SSIM* value is 0.72 in case of 16×16 block size. Maximum value of *PSNR* between

cover and watermarked image has a maximum value of 58.87 dB indicating strong robustness of the technique.

CHAPTER 4

Efficient Watermarking Technique for Protection and Authentication of Text Images

.

4.1 Introduction

A watermarking technique for the protection and authentication of document images is proposed in this Chapter. Hash value is generated by applying *MD*5 on the cover document image. A lookup table is used to translate this hash value into Zero Width Character. Watermark is also translated into Zero Width Character before embedding in the cover image. The Zero Width Characters are embedded at the end of every sentence. At the receiver side, watermark and hash values are generated from Zero Width Character from the watermarked image. Watermark value is used for the protection purpose while hash value is used to authenticate the watermarked image. *DR*, *EC* and other tampering attacks are performed to show the effectiveness of the proposed technique.

Contents of the work presented in this Chapter have been published in *Multimedia Tools and Applications*, Vol. 81, pp. 22985-23005, 2022. (SCI Indexed)

4.2 Preliminary

This section presents a brief description of the Unicode standard and encoding pattern.

4.2.1 Unicode Standard based Table

The Unicode is a standard defined for the representation, encoding and handling of digital texts. Unicode have special *ZWC* which are used to handle particular entities like zero Width Joiner combines two supportable characters together in specific language [Ahvanooey et al. (2020)]. There are four *ZWC*s used for embedding the encoding value in cover text, as shown in the Table 4.1.

Table 4.1: Unicode zero width characters

ZWC	Hexadecimal Code	Symbol Used
Left to Right Mark	U + 200E	No symbol/width
Zero Width Non-Joiner	U + 200C	No symbol/width
POP Directional	U + 202C	No symbol/width
Left to Right Override	U + 202D	No symbol/width

4.2.2 Encoding Table

There are two types of encoding tables are used for encoding and pattern purpose.

Encoding Pattern

Table 4.2 contains the encoding pattern of *ZWCs* 3-bit classification. This pattern is used to generate a watermark in the invisible form and image quality is not degraded after embedding the watermark (Ahvanooey et al. (2020)).

Table 4.2: Encoding pattern of *ZWC*s 3-bit classification

3-Bit Classification	Two ZW Hex Codes	3-Bit Classification	Two ZW Hex Codes
000	”200E” + ”200E”	100	”202C” + ”202C”
001	”200C” + ”200E”	101	”202C” + ”200E”
010	”200E” + ”200C”	110	”200E” + ”202C”
011	”200C” + ”200C”	111	”200C” + ”202C”

Encoding Lookup Table

Table 4.3 contains a specific value in the form of 6-bits for upper and lower alphabets as well as for specific symbol like '.' and '!' (Ahvanooey et al. (2020)).

Table 4.3: Encoding Lookup Table

”11” + UpperA[4-Bit]						”01” + LowerA[4-Bit]					
UpperA[Binary, Binary]	*	00	01	10	11	LowerA[Binary, Binary]	*	00	01	10	11
Shows special character	00	A	B	C	D	Shows special character	00	a	b	c	d
For Example:	01	E	F	G	H	For Example:	01	e	f	g	h
UpperA[11,00]=’M’	10	I	J	K	L	LowerA[10,10]=’k’	10	i	j	k	l
6-bit=”111100”	11	M	N	O	P	6-bit=”011010”	11	m	n	o	p
”00” + UpperB[4-Bit]						”10” + LowerB[4-Bit]					
UpperB[Binary, Binary]	*	00	01	10	11	LowerA[Binary, Binary]	*	00	01	10	11
Shows special character	00	Q	R	S	T	Shows special character	00	q	r	s	t
For Example:	01	U	V	W	X	For Example:	01	u	v	w	x
UpperB[11,00]=’2’	10	Y	Z	0	1	LowerB[00,11]=’t’	10	y	z	6	7
6-bit=”001100”	11	2	3	4	5	6-bit=”100011”	11	8	9	” ”	!

4.3 Proposed Technique

In this section, embedding and detection algorithms of the proposed technique are discussed. Main goal of the document watermarking is to protect the contents by embedding a watermark, which consists of a signature or copyright information. The basic idea behind the document image watermarking scheme is shown in Figure 4.1.

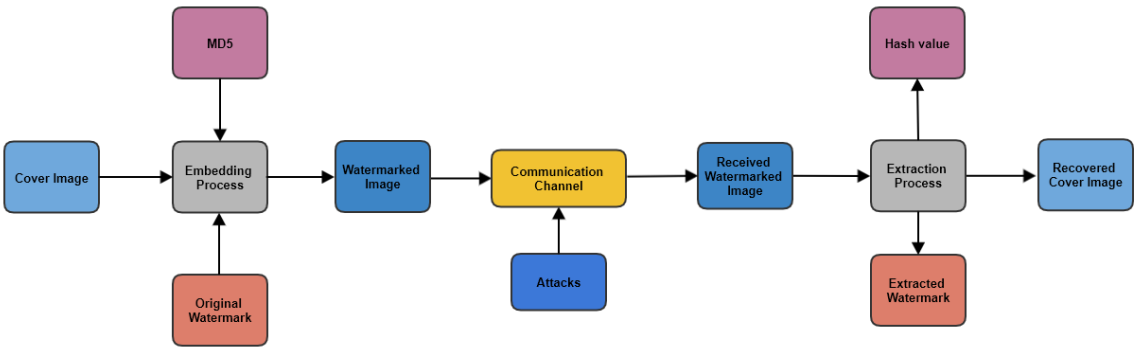


Figure 4.1: Text Watermarking Scheme

As shown in Figure 4.1, in the embedding algorithm a cover image is used for process. First an external watermark is converted into 6-bits string using Table 4.3. These bits are replaced by group of two *ZWC* according to Table 4.2. *MD*5 [Rivest, 1992] hashing technique is then applied on the cover document image to generate a 128 bits hexadecimal value. These hexadecimal values are further converted into 6-bits pattern according to Table 4.3. After that these bits are replaced by a group of two *ZWC* according to Table 4.2. The *ZWC* of watermark and hash value of cover document image is embedded at the end of sentence. After the completion of this process, we have a new image that is called a watermarked image. This image is transmitted through a communication channel. During this process an attacker can alter the content of watermarked image. In the extraction algorithm on the receiver side, the process is reversed. The watermark is extracted to ensure that the image is protected, while the hash value of the contents of the document image is generated to prove the authenticity of the image.

4.3.1 Embedding Algorithm

The proposed technique's embedding method is explained in Embedding Algorithm. The embedding method uses the Hashing technique and an external watermark to authenticate the cover document image on the sender's side. Hashing algorithm is used to the cover document to get a 128-bit hexadecimal value, which is then converted into 6-bits using Table 4.3. Table 4.2 is used to generate the *ZWC* of these bits. A watermark, provided by the user, is converted into bit string using Table 4.3 for encoding its letters. *ZWC*s of the watermark string are generated according to Table 4.2. *ZWCs* of hash value and watermark are embedded at the end of each sentence of the cover document image.

Algorithm 3: Embedding Algorithm

Input: A Cover Text Image *CT*, Watermark W

Output: A watermarked text image *CTw*.

Read a cover text *CT*.

Apply *MD5* hashing technique on *CT* to generate a 128 bits hexadecimal value and save into *HBS*.

Convert *HBS* into a 6-bits string according to a specific patterns shown in Table 4.3.

WH_1 = " " /* WH_1 is an empty string */

while (Length (HBS)>=3)

do

    Three_bit=*HBS*.Substring(0,3) /* Extract 3 characters of the input text */

    HBS = *HBS*.Substring(3:end) /* Update HBS

    Convert Three_bit string by a group of two *ZWCs* using Table 4.2 and save into Temp

    WH_1 = WH_1 + Temp

end while

Read a watermark image (W) and convert it into a 6-bits string using patterns defined in Table 4.3.

WH_2 =" " /* WH_2 is an empty string */

while (Length (*W*)>=3)

do

    Three_bit=*W*.Substring(0,3) /* Extract 3 characters of the watermark */

    W = *W*.Substring(3:end) /* Update watermark

    Convert Three_bit string by a group of two *ZWCs* using Table 4.2 and save into Temp.

    WH_2 = WH_2 + Temp

end while

Concatenation of WH_1 and WH_2 are embedded into end of each sentence of the cover text. This concatenated contents are stored into *CTw*

Return *CTw*

4.3.2 Extraction Algorithm

Extraction algorithm is used at the receiver side to authenticate the received watermarked document image. 128-bits hash value is generated by using *MD*5 hashing technique of each sentence of the image. The embedded

ZWC of hash value and watermark are extracted from the watermarked image by using the reverse steps as used in the embedding process.

Algorithm 4: Extraction Algorithm

Input: Watermarked Image $CT_w^{'}$

Output: A *MD5* value, and a result (R) which provides the proof of protection, authentication and integrity rate for $CT_w^{'}$

1 Read a received text image $CT_w^{'}$.

2 Apply *MD5* hashing technique on $CT_w^{'}$ to generate a 128 bits hexadecimal value and store into $HBS^{'}$.

3 $WH_1^{'}$ =" " /* WH_1 is an empty string */

4 **while** (Length ($HBS^{'}$)>=3)

5 **do**

6 Three_bit=$HBS^{'}$.Substring(0,3) /* Extract 3 characters of the input text */

7 $HBS^{'}$= $HBS^{'}$.Substring(3:end) /* Update $HBS^{'}$

8 Convert Three_bit string by a group of two *ZWCs* using Table 4.2 and save into Temp.

9 $WH_1^{'}$ = $WH_1^{'}$ + Temp

10 Convert $WH_1^{'}$ to a HBS_1 6-bit according to patterns as shown in Table 4.3.

11 **end while**

12 Generate the watermark $W^{'}$ using $WH_1^{'}$

13 $WH_2^{'}$ = " " /* WH_2 is an empty string */

14 **while** (Length ($W^{'}$)>=3)

15 **do**

16 Three_bit=$W^{'}$.Substring(0,3) /* Extract 3 characters of the watermark W */

17 $W^{'}$ = $W^{'}$.Substring(3:end) /* Update $W^{'}$

18 Convert Three_bit string by a group of two *ZWCs* using Table 4.2 and save into Temp.

19 $WH_2^{'}$ = $WH_2^{'}$ + Temp

20 Convert $WH_2^{'}$ to a HBS_2 6-bit according to a specific pattern as shown in Table 4.3.

21 **end while**

22 HBS_1 value is used for the authentication while HBS_2 value is used for the protection purpose.

These *ZWC* are converted into original values using reverse steps used in Algorithm 3, *i.e. ZWC* of hash value are converted into hash value and *ZWC* of embedded watermark are converted into letter using Tables

4.2 and 4.3. These values of hash and extracted watermark are compared with the original values. Watermark value is used for the protection purpose while hash value is used to check the image is authentic or not.

4.4 Experimental Results and Performance Analysis

Proposed technique has been implemented in R2019a version of MATLAB tool. Proposed technique is developed to protect and tamper derection of document images. The quality of watermarked images is not degraded due to non-visual effect of *ZWC*s. Document images used by the existing state-of-art techniques, as well as *DIQA* document images are used as the cover images. Watermark considered in this experiment is shown in Figure 4.4. One of the cover document image whose data is given as an example is shown in Figure 4.2 and its watermarked image is shown in Figure 4.3. Other cover images and their tampered versions are shown in Figures 4.5 and 4.6 respectively.

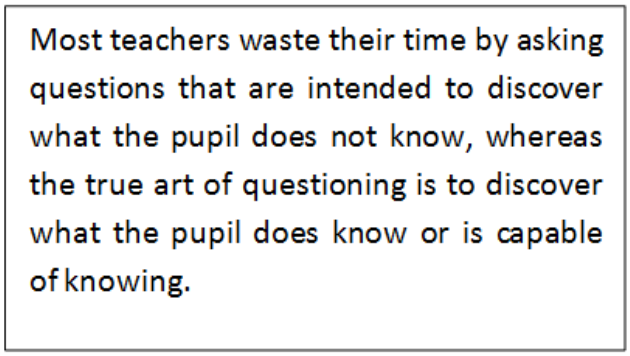


Figure 4.2: Original Document Image 1

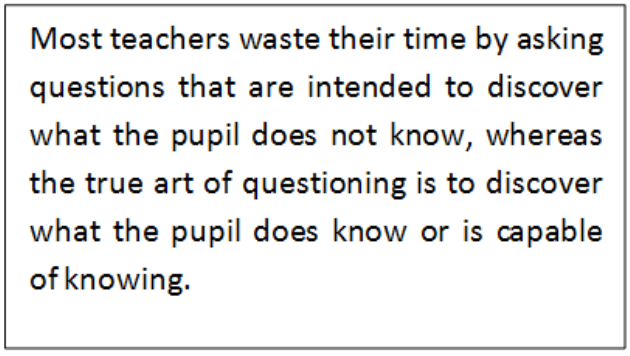


Figure 4.3: Watermarked Document Image 1

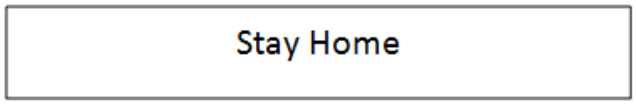


Figure 4.4: Watermark Image

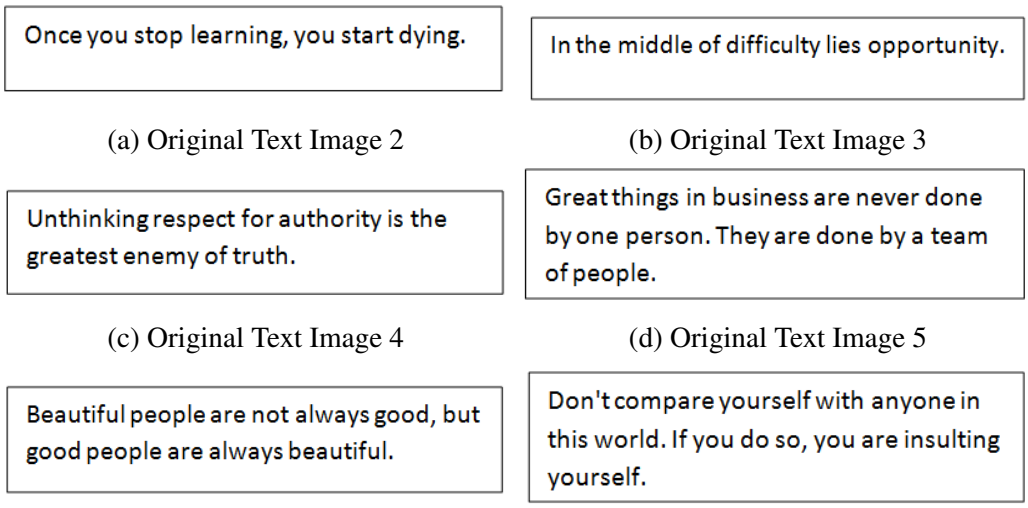
Table 4.4: Embedding Algorithm Example

Watermark Bits 00001010001101000010100010111011011101111001110001010 0
ZWC of watermark ’200E’+’200E’+’200E’+’200C’+’202C’+’202C’+’200C’+’200C’+’200E’ +’200C’+’200E’+’200E’+’202C’+’200E’+’200E’+’200E’+’202C’+’200E’ +’200E’+’202C’+’200E’+’202C’+’200C’+’202C’+’200C’+’200C’+’200E’ +’202C’+’200C’+’200C’+’202C’+’202C’+’200E’+’200C’+’202C’+’202C’
MD5 bits 01010100101110101100110110101100111101000101010001010100101000 11 00001100001100101011001100010000010001001101010011001011010001 01 00100011010011110011011011010011011011000010110101000011111011 00
ZWC of MD5 value ’200E’+’200C’+’202C’+’200E’+’200C’+’200E’+’200C’+’200C’+’202C’+’200E’ +’200C’+’200C’+’200C’+’200E’+’202C’+’200E’+’202C’+’200E’+’200C’+’200C’ +’200C’+’200E’+’200C’+’202C’+’200E’+’200C’+’200C’+’200E’+’200E’+’200C’ +’202C’+’202C’+’200E’+’200C’+’202C’+’200E’+ ’200C’+’200E’+’200E’+’200C’ +’200C’+’200E’+’202C’+’202C’+’200C’+’200E’+’202C’+’202C’+ ’200C’+’200E’ +’202C’+’202C’+’202C’+’200E’+’200C’+’200C’+’200C’+’200E’+’202C’+’202C’ + ’200E’+’200C’+’200E’+’200E’+’200E’+’200C’+’200C’+’200E’+’200C’+’200E’ +’202C’+’200E’+ ’200E’+’200C’+’200C’+’200C’+’200C’+’200E’+’200C’+’200C’ +’200E’+’200C’+’200C’+’200E’+ ’200E’+’200C’+’200E’+’200C’+’200C’+’200E’ +’202C’+’200E’+’200C’+’200E’+’200C’+’202C+ ’200C’+’200E’+’202C’+’200E’ +’202C’+’200E’+’202C’+’200E’+’200C’+’200E’+’202C’+’200E’+ ’202C’+’200E’ +’202C’+’202C’+’200C’+’200E’+’200C’+’200C’+’200E’+’200C’+’202C’+’202C’ + ’200C’+’200E’+’200C’+’202C’+’202C’+’200E’+’202C’+’202C’

Table 4.4 describes embedding process in which ”Stay Home” is used as a watermark and calculating the hash value of the cover original document image 1. *ZWC* of watermark and hash value are generated as the discussed in the algorithm steps. *ZWCs* values is embedded at the end of text. Due to zero space characteristics of *ZWC*, end user only able to view the original text not the embedded bits. This can be observed from the watermarked image, shown in Figure 4.3.

4.4.1 Invisibility

As shown in Table 4.4, the technique does not degrade the contents of the document image as we are embedding the watermark and *MD5* hash value by using *ZWCs*. End users is only able to view the text and Human Vision Systems (*HVS*) is not able to detect the affect of embedded bits.

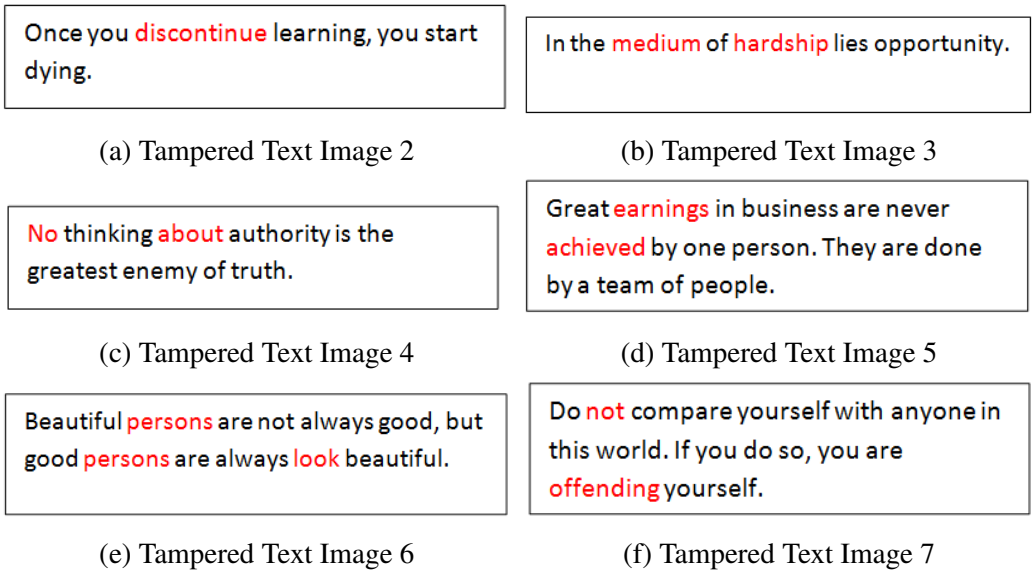


(a) Original Text Image 2 (b) Original Text Image 3

(c) Original Text Image 4 (d) Original Text Image 5

(e) Original Text Image 6 (f) Original Text Image 7

Figure 4.5: Original Images



(a) Tampered Text Image 2 (b) Tampered Text Image 3

(c) Tampered Text Image 4 (d) Tampered Text Image 5

(e) Tampered Text Image 6 (f) Tampered Text Image 7

Figure 4.6: Tampered Images corresponding to Original Images

4.4.2 Distortion Robustness

DR is calculated with the help of Loosing Probability (*LP*) (Ahvanooey et al. 2020). The *LP* value is calculated by the number of sentences and the total length of the string. *LP* is equal to the number of sentences divided by total length of the cover text *i.e.* $LP=\frac{NS}{LT}$, where *NS* is number of sentences of the *CT* and *LT* is length of *CT*. If *CT* = [Most teachers waste their time by asking questions that are intended to discover what a pupil does not know, whereas the true art of questioning is to discover what the pupil does know or is capable of knowing.] then the value of *LP* is then calculated by $LP=\frac{1}{210}$ = 0.004. The probability of the *DR* is determined by P(*DR*) = [1-0.004] = 0.996 = 99.6 %.

Table 4.5: *DR* comparison with the Existing Techniques

Watermark (W)	Image	Proposed Technique	Ahvanooey et al. (2020)	Naqvi et al. (2018)	Rizzo et al. (2017)	Alotaibi and Elrefaei (2018)	Patiburn et al. (2017)	Por et al. (2012)
Albert	Original Document Image 2	97.5	97.5	90	72.5	83.3	85	83.3
Einstein	Original Document Image 3	97.7	97.7	84.4	57.7	83.3	85.6	83.3
Albert Einstein	Original Document Image 4	98.4	98.4	82.8	78.1	88.8	85.9	88.8
Steven Paul Jobs	Original Document Image 5	97.7	97.7	86.5	74.1	94.1	80.5	94.1
Ali ibn Abi Tali	Original Document Image 6	98.6	98.6	81.3	72	90.9	85.3	90.9
William Henry Gates III	Original Document Image 7	97.8	97.8	80.2	67	93	83.5	93.3

If a malicious user tries to modify the portion of the CT_w except the end of each sentence, then *ZWC*s

values of watermark and hash value will remain in the CT'_w and can be retrieved by extraction procedure. A malicious user is not able to view the *ZWC*s value due to its zero width characteristics. Proposed technique applies the same rule used by existing technique [Ahvanooey et al., 2020] that is reason *DR* of the proposed technique is equal to the existing technique, as shown in Table 4.5.

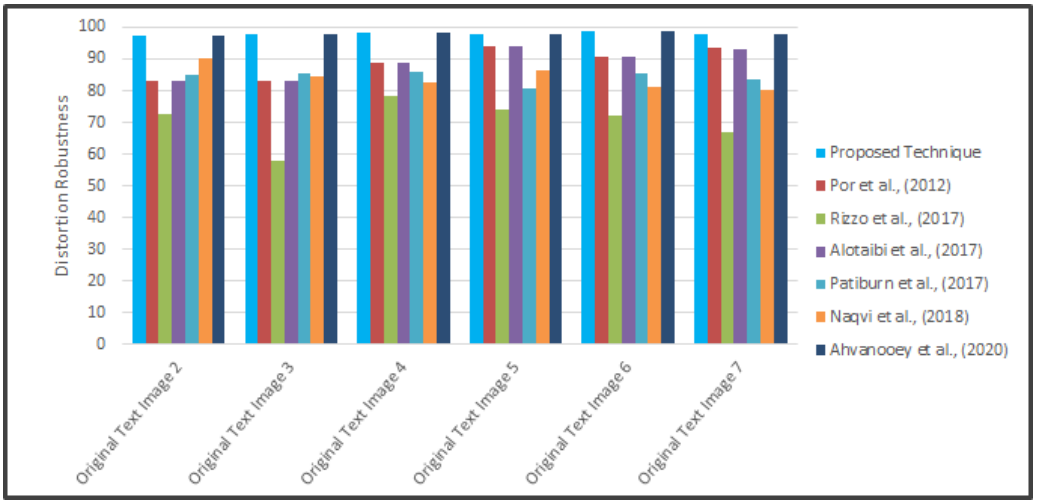


Figure 4.7: Comparison of DR of the Proposed Technique and Existing Techniques

DR comparisons between the proposed technique and existing techniques are shown in Figure 4.7. One can infer from this comparison that *DR* of proposed technique is high as compared to existing techniques.

4.4.3 Embedding Capacity

To embed data into the text, the embedding process converts every character of the watermark and hash value of the cover document image to *ZWC*. The proposed technique shows more capacity as compared to the existing techniques as shown in Table 4.6. At the end of each sentence, the proposed technique embeds both the watermark bits and the hash value of the cover document image, whereas existing techniques just embed the watermark bits. Table 4.6 contains the comparison of embedded capacity of proposed technique as well as of other existing techniques. The existing techniques only embed the bits of watermark while proposed technique embeds *ZWCs* of watermark as well as of hash values. This is the reason that embedding capacity of proposed technique is more as compared to existing techniques. The embedding capacity comparisons of proposed technique and existing techniques are shown in the Figure 4.8 with the help of graph. The graph is plotted against different types of cover dcument images. The embedding capacity of proposed technique is larger for every document image as compared to capacity of the existing techniques. In the proposed technique, *ZWC* of

hash value of cover image and watermark is used in the embedding process, whereas the existing techniques just used the watermark.

Table 4.6: Embedding Capacity(in bits) comparison with the Existing Techniques

Text Watermark (W)	Image	Proposed Technique (Watermarks bits and *MD*5 bits)	Ahvanooey et al. (2020)	Naqvi et al. (2018)	Rizzo et al. (2017)	Alotaibi and Elrefaei (2018)	Patiburn et al. (2017)	Por et al. (2012)
Albert	Original Document Image 2	134	6	4	2.8	3	6	1.7
Einstein	Original Document Image 3	136	8	7	3.8	3	6	1.7
Albert Einstein	Original Document Image 4	143	15	11	4	4.5	9	2.25
Steven Paul Jobs	Original Document Image 5	144	32	12	7.2	8.5	11	4.25
Ali ibn Abi Talib	Original Document Image 6	145	17	14	5.3	5.5	15	2.75
William Henry Gates III	Original Document Image 7	151	46	18	7.5	7.5	15	3.73

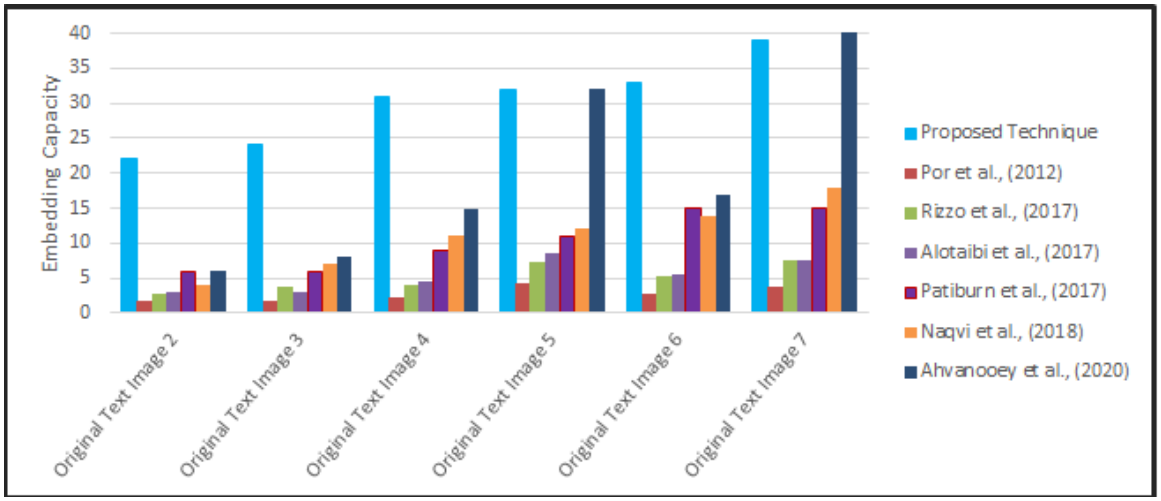


Figure 4.8: Embedding Capacity of the Proposed Technique Vs Existing Techniques

4.4.4 Prevention Against Malicious Attacks

The technique is capable to protect CT_w from a variety of threats while it is being transmitted across a communication channel. Malicious users will be unable to locate the *ZWC*.

Tampering Attack

Tampering Attack Type 1. The hashing value can be used to detect if a malicious user altered the content of watermarked text.”Most” is changed to ”Cost,” and ”waste” is changed to ”caste,” as seen in Table 4.7. Table 4.7 demonstrates that the hash value in both cases is different, indicating that the text has been tampered with. Tamper detection example is shown in the Table 4.7. Hash value of the cover text is different from hash value of tampered text. The altered words are shown in red color in this table. Due to alteration in cover text, value of hash of cover text is not same. Different value of hash means that watermarked text has been tampered during the communicated channel. Figure 4.9 explains the tamper detection process in which extracted hash value is compared with the original hash value. If both the values are same then image is authentic otherwise image is tampered.

Table 4.7: Tamper Detection Example

Most teachers waste their time by asking questions that are intended to discover what the pupil does not know, whereas the true art of questioning is to discover what the pupil does know or is capable of knowing.
Hash Value f17375bef022272ab3d1bc3539381e58
Cost teachers caste their time by asking questions that are intended to discover what the pupil does not know, whereas the true art of questioning is to discover what the pupil does know or is capable of knowing.
Hash Value a30c4ae2f5b1e9b47340a710f22011c9

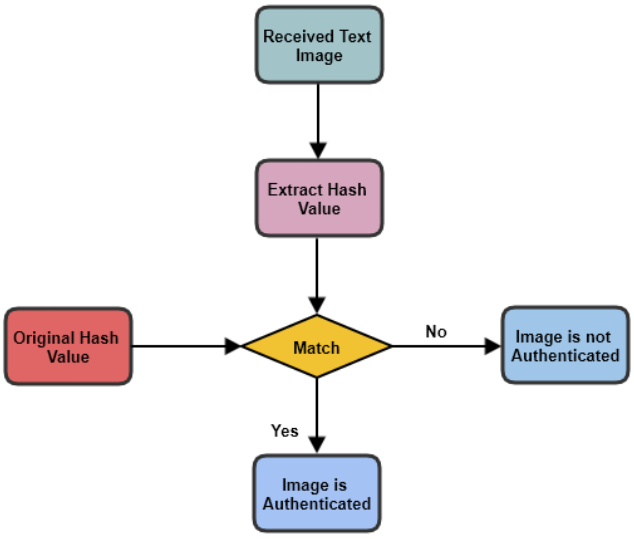
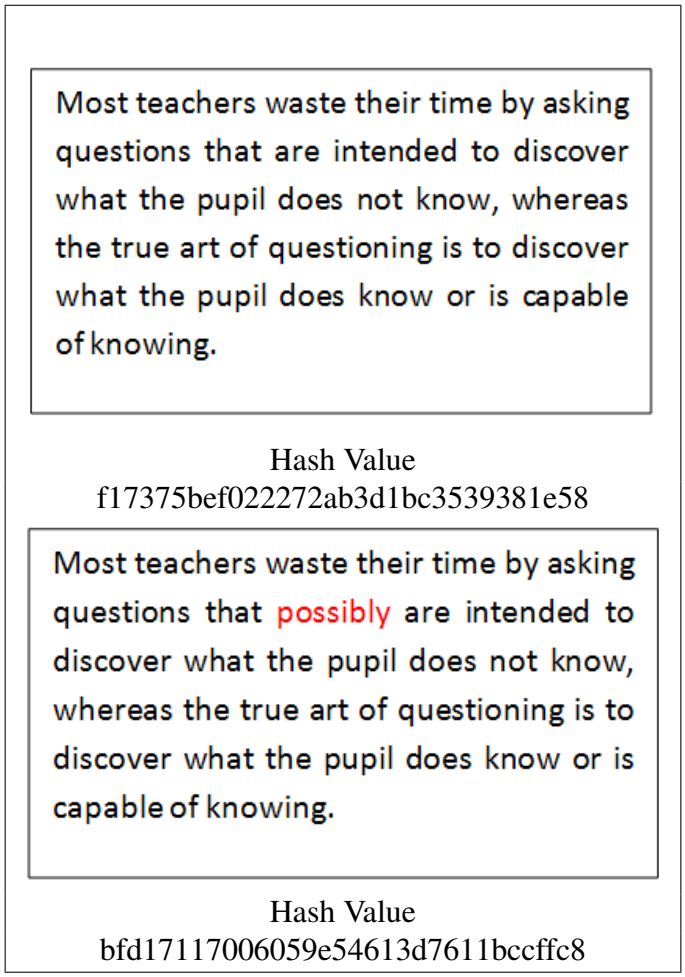


Figure 4.9: Tamper Detection Process

Tampering Attack Type 2. If a malicious user add a extra word in the text then types of attack also detected by the proposed technique with the help of hash value as shown in Table 4.8. It is cleared that hash values are different for both the cases. Hash value changes due to addition of 'possibly' word in the text. A malicious user may have inserted a word into the image, as illustrated in Table 4.8, during the tampering process.The hash value of the tampered text differs from the cover text due to the addition of this extra word. This differnnce helps in detection the tamperness of the image.

Table 4.8: Tamper Detection Example



Integrity Rate (*IR*): If a malicious user alters or adds any extra word in the text, the technique is able to catch this type of attack, it is known the *IR* of the technique. The proposed technique is able to detect every types of activities like alteration or addition of any word in the text. Hash value is used to calculate the *IR* of the technique. From Tables 4.7 and 4.8, it is cleared that proposed technique works for both types of attack and its *IR* is 100%. Table 4.9 describes the comparison of *IR* between the proposed technique with the existing

techniques. *IR* of the proposed technique is 100% in every case and Hash value is used to calculate the *IR*. The words has been changed or inserted during the attack by a malicious user is shown in red color in tampered images, shown in Figure 4.6.

Table 4.9: *IR* comparison of the Proposed Technique with the existing Technique

Original Image	Tampered Image	Ahvanooey et al. (2020)	Proposed Technique
Original Document Image 2	Tampered Document Image 2	86%	100%
Original Document Image 3	Tampered Document Image 3	71%	100%
Original Document Image 4	Tampered Document Image 4	82%	100%
Original Document Image 5	Tampered Document Image 5	84%	100%
Original Document Image 6	Tampered Document Image 6	62%	100%
Original Document Image 7	Tampered Document Image 7	74%	100%

Copyright Protection

If a malicious user duplicates the CT_w and claims as its owner. Then, *W* can be extracted to provide the ownership for the CT_w. The embedded watermark is used as a protection purpose in the technique.

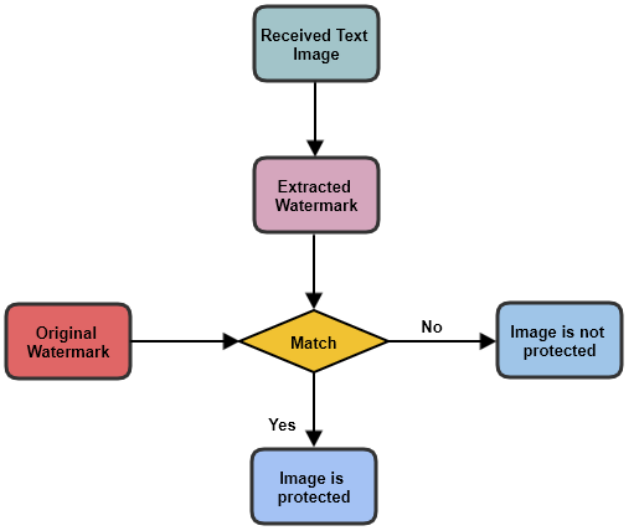


Figure 4.10: Protection Process used in Proposed Technique

The proposed technique provides the protection against forgery or plagiarism attack with the help of watermark. Watermark is extracted from the received image and compared with the original watermark. If both

watermarks are the same, the image is protected; otherwise, it isn't. This procedure is shown in Figure 4.10.

Distortion Robustness for DIQA Dataset Images

To check the *DR* of the proposed technique, images used are shown in Figure 3.6 and their corresponding tampered images are shown in Figure 4.11.

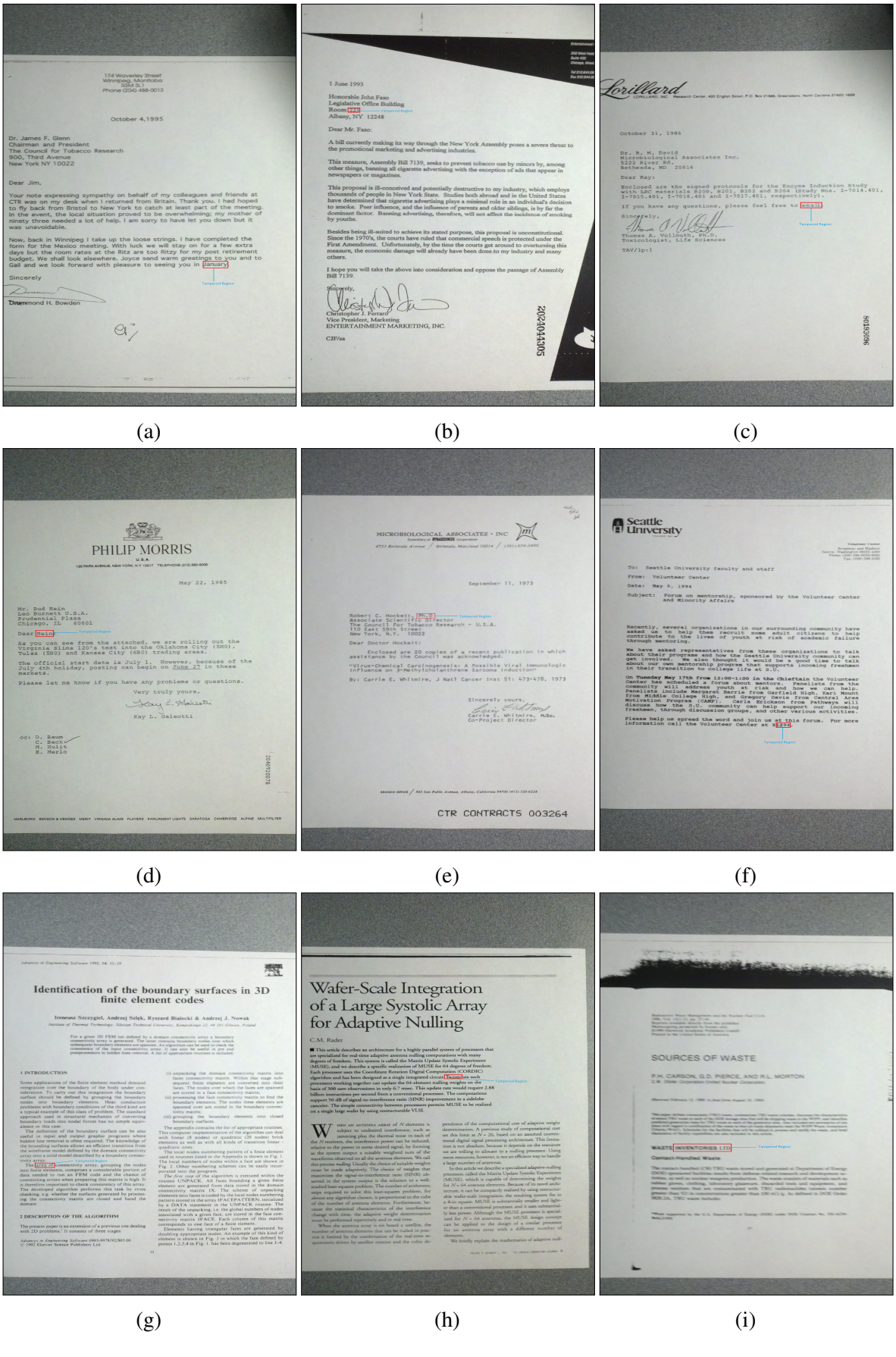
Table 4.10: Distortion Robustness

Image	Text Watermark (W)	Distortion Robustness (DR)
2012-04-16_17-42-48_976	Albert	98.9
2012-04-16_17-32-27_295	Einstein	99.3
2012-04-16_17-35-31_279	Albert Einstein	99.0
2012-04-17_17-37-56_610	Steven Paul Jobs	99.0
2012-04-17_17-40-31_436	Ali ibn Abi Talib	99.5
2012-04-23_12-27-02_949	William Henry Gates III	99.3
2012-04-23_13-54-17_17	Stay Home	99.2
2012-04-23_13-58-38_54	Be Safe	99.3
2012-04-23_16-14-33_660	Stay Home Be Safe	98.5

Table 4.10 described the *DR* value that are calculated with respect to the document images by using different text watermark image. *DR* is calculated by using the Loosing Probability as described by Ahvanooey et al. (2020).

Compression Effect

The proposed technique is also tested against the compression effect using different quality parameters as shown in Table 4.11. *SSIM* parameter is used to check the effect of compression on the extracted watermark. When lossless compression is applied, there is no loss in the visual quality of the recovered image and *SSIM* between extracted and original watermark is 1. NA stands for Not Applicable as compression paramters is not used in case of lossless compression. When compression is applied with the help of different values of quality parameters, then there is some loss and in that state value of *SSIM* will not be equal to 1, as shown in Table 4.11.



(a) (b) (c)

(d) (e) (f)

(g) (h) (i)

Figure 4.11: Tampered Document Images Corresponding to Original Images of Figure 3.6

Table 4.11: Compression effect with Quality Parameters

Image	Compression	Compression Parameters (Q)	*SSIM*
2012-04-16_17-42-48_976	Lossless	NA	1.00
	Lossy	90/80/70/60/50	0.99/0.97/0.96/0.95/0.94
2012-04-16_17-32-27_295	Lossless	NA	1.00
	Lossy	90/80/70/60/50	0.98/0.96/0.94/0.93/0.92
2012-04-16_17-35-31_279	Lossless	NA	1.00
	Lossy	90/80/70/60/50	0.98/0.96/0.95/0.93/0.92
2012-04-17_17-37-56_610	Lossless	NA	1.00
	Lossy	90/80/70/60/50	0.97/0.95/0.94/0.93/0.91
2012-04-17_17-40-31_436	Lossless	NA	1.00
	Lossy	90/80/70/60/50	0.98/0.96/0.94/0.93/0.91
2012-04-23_12-27-02_949	Lossless	NA	1.00
	Lossy	90/80/70/60/50	0.99/0.97/0.96/0.94/0.92
2012-04-23_13-54-17_17	Lossless	NA	1.00
	Lossy	90/80/70/60/50	0.98/0.97/0.95/0.94/0.91
2012-04-23_13-58-38_54	Lossless	NA	1.00
	Lossy	90/80/70/60/50	0.97/0.96/0.95/0.93/0.92
2012-04-23_16-14-33_660	Lossless	NA	1.00
	Lossy	90/80/70/60/50	0.99/0.97/0.95/0.94/0.92

4.5 Conclusion

A document watermarking technique for the protection and authentication of document images is proposed in this Chapter. A watermark and hash value of cover image are embedded as Unicode *ZWC* at the end of each sentence of the cover text. By using *ZWC*, both of these values are embedded in the invisible form and visual quality of document images is not degraded. Embedding capacity and *IR* are better than the existing techniques. Distortion robustness values are comparable to those provided by the existing techniques. *IR* of the proposed technique is 100 %. Maximum value of *SSIM* is 0.99 against *JPEG* compression attack. Maximum value of *DR* is 99.5 of the proposed technique.

CHAPTER 5

Markov Matrix and Entropy based Tamper Detection Technique for Text Images

5.1 Introduction

In this Chapter, Markov Matrix and Entropy based technique is proposed for tamper detection of text images. Entropy of every sentence of document image is calculated and Markov Matrix is used to generate a character pattern using the occurrences of character of the cover image. Entropy and character patterns values are converted into Zero Width Character with the help of lookup table. Zero Width Character of entropy of each sentence is embedded at the end of every sentence after terminator. Zero Width Character of the character patterns are embedded in the end of the text of the cover image. On receiver side, Zero Width Character are extracted and converted to numerical form using the same lookup table. Entropy of every sentence and character patterns are recalculated and compared with extracted values for tamper detection. *DR*, *EC* and other attacks are shown in the experimental results to show the proposed technique.

Contents of the work presented in this Chapter have been published in *Journal of Engineering Research*, 2021. (SCI Indexed)

Entropy of a sentence is amount of average information. It is defined as

$$H(X) = -\sum_{k} p_k \log_2(p_k) \tag{5.1}$$

where K is the number of gray levels and p_k is the probability associated with gray level k.

5.2 Preliminary

This section presents a brief description of the Unicode standard as well as encoding pattern and markov matrix.

5.2.1 Unicode Standard

The Unicode is a standard defined that is used to represent, encode and handle a digital text. Unicode have specific *ZWC* which are used to handle specific entities like zero width joiner combines two supportable characters together in particular language [Ahvanooey et al. (2020)]. There are four *ZWCs* used to embed the encoding value in cover text, as shown in Table 4.1. Table 5.1 contains the encoding pattern of *ZWCs*. This pattern helps to generate a *ZWCs* of a value in the invisible form and image visual quality is not degrading after a embedding process.

Table 5.1: Encoding pattern of *ZWCs*

Value	Two ZW Hex Codes	Value	Two ZW Hex Codes
0	200E + 200E	5	200C + 202C
1	200E + 202C	6	200C + 200D
2	200E + 202D	7	202C + 202C
3	200E + 200C	8	202C + 200C
4	200C + 200E	9	202C + 202D
		’.’	200C + 200C

5.2.2 Character Pattern Generation using Markov Matrix

Characters are the smallest elements in a text’s structure. In proposed technique, occurrence of the characters are used to create a Markov matrix. This matrix is used to create a character pattern. For matrix generation, all

of the characters in the text are converted to small cases and a list of all of the document's characters is created. This list is used to generate a Markov Matrix, *M*, as shown below:

$$M = \left\{ \left| \begin{array}{ccccc} * & c_1 & c_2 & .. & c_n \\ c_1 & t_{11} & t_{12} & .. & t_{1n} \\ c_2 & t_{21} & t_{22} & .. & t_{2n} \\ .. & .. & .. & .. & .. \\ c_n & t_{n1} & t_{n2} & .. & t_{nn} \end{array} \right| \left[\begin{array}{c} P \\ P_1 \\ P_2 \\ . \\ P_n \end{array} \right] \right\} \tag{5.2}$$

Where, c_i refers to an element of list, t_{ij} is the number of immediate appearance of c_j after c_i in the document, * denotes the transition point, and P_i shows the transition pattern of each element of the list. The sum of each row in the given matrix is 1 and none of the list elements are negative.

5.3 Proposed Technique

In this section, embedding, and extraction algorithms of the proposed technique are discussed. Main goal of the text watermarking scheme is to tamper detection in the text image by embedding a *ZWcs* of entropy after every sentence. The basic idea behind the text watermarking scheme is shown in Figure 5.1.

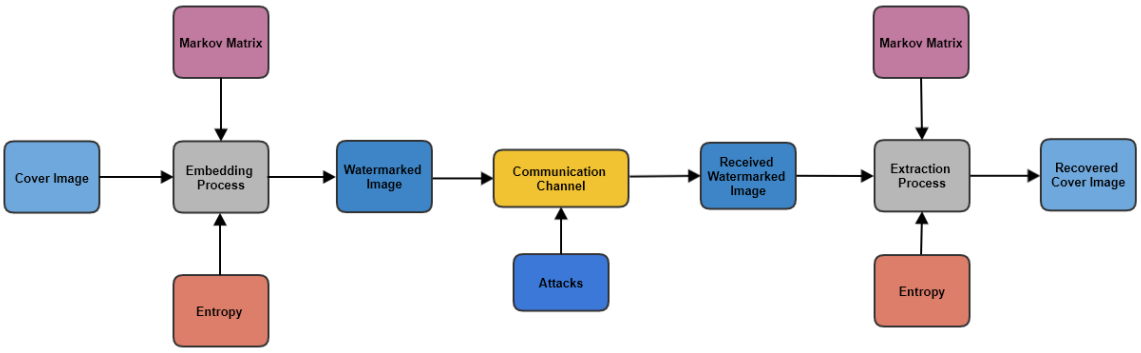


Figure 5.1: Text Watermarking Scheme

5.3.1 Embedding Algorithm

Algorithm 5: Embedding Algorithm

Input: Cover Text Image *CT*

Output: Watermarked Text Image CT_w

1 Calculate the entropy E_i of every sentence of the cover text using (5.1), where i =1,2,....

2 A terminator is selected at end of every sentence that changes language to language like '.' is used in English language while '|' in Hindi as well as in Punjabi language.

3 Convert E_i to *ZWCs* by using the mapping given in Table 5.1.

4 Convert each character of the cover text into lower case and count the total occurrence of each character. Generate a Markov Matrix M, as shown in (5.2). Embed the pattern of the cover text in the end of the cover text by converting into ZWCs given in Table 5.1.

5 Embed *ZWCs* values of the entropies at end of sentence and ZWCs of the character pattern in the end of the cover text.

A text image is utilized as a cover image in the embedding process. Entropy of each sentence of the cover image is calculated using equation 5.1. A terminator is used to pick the end of a sentence that varies from language to language; such as '.' in English. Table 5.1 is used to construct the *ZWC* of each sentence's entropy value. Following that, each character in the cover text is converted to lower case and total occurrence of each is counted. Equation 5.2 is used to create a Markov Matrix to generate a pattern and converted into *ZWC*. *ZWC* of entropy value is embedded at the end of every sentence and *ZWC* of character pattern is embedded at the end of cover text to generate a watermarked image.

5.3.2 Extraction Algorithm

Algorithm 6: Extraction Algorithm

Input: Watermarked Text Image CT_w

Output: Watermarked text image CT_w is tampered or not.

1 Read the watermarked text image CT_w.

2 Calculate the entropy E_i of every sentence of the watermarked text using (5.1), where i =1,2,....

3 Generate the character pattern of each character k by using Markov Matrix M, as shown in (5.2) and store into $P_k^{'}$.

4 Extract *ZWCs* of entropy of every sentence of the watermarked text image and *ZWCs* of each character pattern.

5 Convert *ZWCs* of the entropies of the i^{th} sentence to a number $E_i^{'}$ and character pattern of each character P_k by using Table 5.1.

6 Compare E_i and $E_i^{'}$ for each i where i =1,2,.....

7 if E_i==$E_i^{'}$

8 then i^{th} sentence of the received watermarked text is not tampered,

9 otherwise it is tampered and use the character patterns P_k and $P_k^{'}$ to find the tampered words.

A watermarked image is used as an input image in the extraction process. Equation 5.1 is used to determine the entropy of each sentence of watermarked image. Equation 5.2 is used to construct the pattern for each character. *ZWC* of entropy value is generated and converted into a number using Table 5.1. A character pattern from *ZWC* of each character is also generated using Table 5.1. To determine whether or not an image has been tampered, entropy value of watermarked image is compared to the entropy value extracted from the watermarked image. If both the entropy values are equal, then image is not tampered else image is tampered. The character pattern generated from the watermarked image is compared to the extracted pattern to locate the tampered words. If the image is not tampered, the value of both patterns will be the same. However, if the watermarked text image has been tampered with, the character pattern of the tampered word will not match with the extracted pattern for that word.

5.4 Experimental Results and Performance Analysis

Proposed technique has been implemented in R2019a version of *MATLAB* tool. Text images, having the contents used by the existing state-of-art techniques, are used as the cover images. Proposed technique is developed to protect the text images using entropy and markov matrix. *ZWC* is used in the embedding process to maintain the quality of watermarked image. This technique is applicable to the images of different langauges. Only the sentene terminator of the specific language needs to be used in the embedding and extraction algorithms of the technique. Different watermarks are also considered in this experimental analysis.

5.4.1 Invisibility

The proposed technique does not degrade the quality of cover text due to embedding of *ZWCs*. *ZWCs* of entropy is embedded at the end of every sentence according to the entropy of that sentence as shown in Figure 5.2. Human Vision Systems is not able to detect the effect of embedding process.

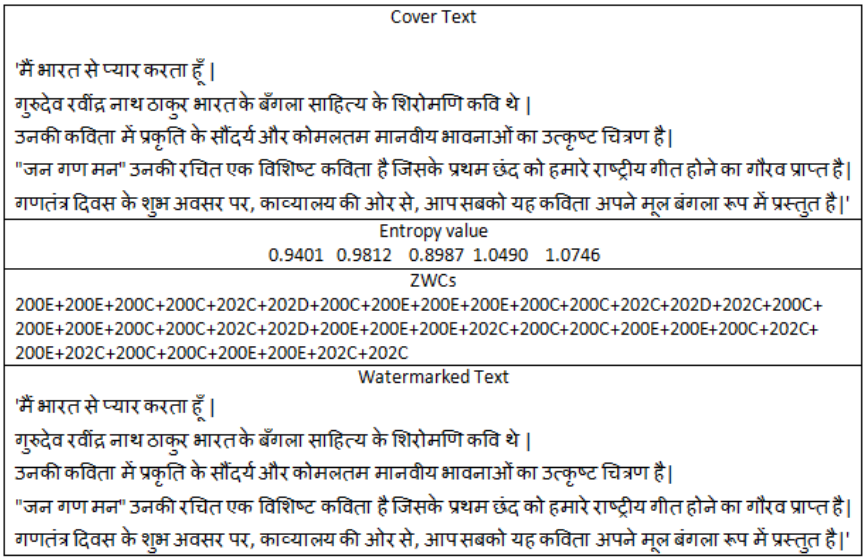


Figure 5.2: Embedding process Example

5.4.2 Distortion Robustness

DR is computed with the help of Loosing Probability (*LP*) (Ahvanooey et al. (2020)). *LP* is calculated by using the sentences and total length of string. *LP* is equal to the number of sentences divided by total length of string i.e $LP=\frac{NS}{LT}$, where *NS* is number of sentences through the *CT* and *LT* is length of *CT*. If *CT* = [Once you stop

learning, you start dying.] then value of *LP* is determined by *LP*=$\frac{1}{40}$ = 0.025. The probability of the *DR* is determined by P(*DR*) = [1-0.025] = 0.97.5 = 97.5 %.

Table 5.2: Comparison of *DR* of the Proposed Technique with *DR* of the Existing Techniques

Water-mark (W)	*CT*	Length of *CT*	Proposed Tech-nique	Ahvanooey et al. (2020)	Alotaibi and El-refaei (2018)	Naqvi et al. (2018)	Patiburn et al. (2017)	Por et al. (2012)	Rizzo et al. (2017)
Albert	Once you stop learning, you start dying.	40	97.5	97.5	83.3	90	85	83.3	72.5
Einstein	In the mid-dle of diffi-culty lies op-portunity.	45	97.7	97.7	83.3	84.4	85.6	83.3	57.5
Albert Ein-stein	Unthinking respect for authority is the greatest enemy of truth.	64	98.4	98.4	88.8	82.8	85.9	88.8	78.1

Steven Paul Jobs	Great things in business are never done by one person. They are done by a team of people.	89	97.7	97.7	94.1	86.5	80.5	94.1	74.1
Ali ibn Abi Talib	Beautiful people are not always good, but good people are always beautiful.	75	98.6	98.6	90.9	81.3	85.3	90.9	72
William Henry Gates III	Don't compare yourself with anyone in this world. If you do so, you are insulting yourself.	91	97.8	97.8	93	80.2	83.5	93.3	67

Table 5.2 describes the *DR* comparison with the existing technique. *DR* is calculated by using total number of sentences and total length of string. The proposed technique and existing technique [Ahvanooey et al. (2020)] follow the same rule to determine the *DR*. This is reason *DR* of the proposed technique as well as existing technique [Ahvanooey et al. (2020)] is same.

5.4.3 Embedding Capacity

The entropy value of each sentence is converted into *ZWCs* before the embedding process. The comparison with existing technique is shown in Table 5.3.

Table 5.3: Comparison of the Embedding Capacity of the Proposed Technique with the Existing Techniques

Water-mark (W)	Cover Text(*CT*)	Length of *CT*	Proposed Tech-nique	Ahvanooey et al. (2020)	Alotaibi and El-refaei (2018)	Naqvi et al. (2018)	Patiburn et al. (2017)	Por et al. (2012)	Rizzo et al. (2017)
Albert	Once you stop learning, you start dying.	40	6	6	3	4	6	1.7	2.8
Einstein	In the mid-dle of diffi-culty lies op-portunity.	45	6	8	3	7	6	1.7	3.8
Albert Ein-stein	Unthinking respect for authority is the greatest enemy of truth.	64	6	15	4.5	11	9	2.25	4

Steven Paul Jobs	Great things in business are never done by one person. They are done by a team of people.	89	12	32	8.5	12	11	4.25	7.2
Ali ibn Abi Talib	Beautiful people are not always good, but good people are always beautiful.	75	6	17	5.5	14	15	2.75	5.3
William Henry Gates III	Don't compare yourself with anyone in this world. If you do so, you are insulting yourself.	91	12	46	7.5	18	15	3.73	7.5

The comparison between the proposed technique and existing technique is shown in the Table 5.3. As shown in Table 5.3, different external watermark is used by existing techniques for every string. But the proposed technique embeds *ZWCs* of entropy value after every sentence. Embedding capacity of the proposed technique depends upon number of sentences in a text.

5.4.4 Prevention against Malicious Attacks

Deletion Attack

If a malicious user deletes the content of the watermarked text then it can be detected with the help of entropy value. It is cleared from Table 5.4 that value of entropy in both cases have changed which shows that received text has been tampered.

Table 5.4: Deletion Attack Example

Cover Text Once you stop learning, you start dying. In the middle of difficulty lies opportunity. Unthinking respect for authority is the greatest enemy of truth. Great things in business are never done by one person. They are done by a team of people.
Entropy value (Entropy of first sentence =4.0276, Entropy of second sentence=4.1313, Entropy of third sentence=4.0470, Entropy of fourth sentence= 3.8913, Entropy of fifth sentence= 3.6144)
Tampered Text Once stop learning, you start dying. In middle of difficulty lies opportunity. Unthinking respect for authority is greatest enemy of truth. Great things in business never done by one person. They done by a team of people.
Entropy Value (Entropy of first sentence =4.0487, Entropy of second sentence=4.1008, Entropy of third sentence=4.0932, Entropy of fourth sentence= 3.9086, Entropy of fifth sentence= 3.5988)

As shown in Table 5.4, red color words of cover text has been deleted by a malicious user attack and these words are missing in the tampered text. The value of entropy and character patterns are changed due to deletion of these words.

Figure 5.3 shows the deletion attack on Hindi cover text. Entropy of every sentence of cover text is calculated as shown in the Figure 5.3. Entropy of every sentence is embedded behind every sentence individually during the embedding process.

Cover Text
मैं भारत से प्यार करता हूँ।
गुरुदेव रवींद्र नाथ ठाकुर भारत के बँगला साहित्य के शिरोमणि कवि थे।
उनकी कविता में प्रकृति के सौंदर्य और कोमलतम मानवीय भावनाओं का उत्कृष्ट चित्रण है।
"जन गण मन" उनकी रचित एक विशिष्ट कविता है जिसके प्रथम छंद को हमारे राष्ट्रीय गीत होने का गौरव प्राप्त है।
गणतंत्र दिवस के शुभ अवसर पर, काव्यालय की ओर से, आप सबको यह कविता अपने मूल बंगला रूप में प्रस्तुत है।
Entropy value
(Entropy of first sentence=0.9401, Entropy of second sentence=0.9812, Entropy of third sentence=0.8987, Entropy of fourth sentence=1.0490, Entropy of fifth sentence=1.0746)
Tampered Text
मैं भारत से प्यार हूँ।
गुरुदेव रवींद्र नाथ भारत के बँगला साहित्य के शिरोमणि कवि थे।
उनकी कविता में प्रकृति के सौंदर्य और कोमलतम भावनाओं का उत्कृष्ट चित्रण है।
"जन गण मन" उनकी रचित एक कविता है जिसके प्रथम छंद को हमारे राष्ट्रीय गीत होने का गौरव प्राप्त है।
गणतंत्र दिवस के शुभ अवसर पर, काव्यालय ओर से, आप सबको यह कविता अपने मूल बंगला रूप में प्रस्तुत है।
Entropy value
(Entropy of first sentence=0.9738, Entropy of second sentence=1.0063, Entropy of third sentence=0.9217, Entropy of fourth sentence=1.0820, Entropy of fifth sentence=1.0751)

Figure 5.3: Deletion Attack Example

Figure 5.3 describe the tamper detection that is occurred due to deletion attack. The words shown with underline are deleted from the cover text during deletion attack. The different values of entropy of every sentence show that text has been tampered.

In the Figure 5.4, the cover text and its corresponding tampered text of Punjabi language are shown. The words with underline in cover text are deleted from the tampered text.

Cover Text
ਨਾਨਕ ਅੰਮ੍ਰਿਤੁ ਏਕੁ ਹੈ ਦੂਜਾ ਅੰਮ੍ਰਿਤੁ ਨਾਹਿ।
ਅੰਮ੍ਰਿਤੁ ਏਕੋ ਸਬਦੁ ਹੈ ਨਾਨਕ ਗੁਰਮੁਖਿ ਪਾਇਆ।
ਅੰਮ੍ਰਿਤ ਸਬਦੁ ਅੰਮ੍ਰਿਤ ਹੁਰਿ ਬਾਣੀ।
ਅੰਮ੍ਰਿਤ ਨਾਮੁ ਸਦ ਮੀਠਾ ਲਾਗਾ ਗੁਰ ਸਬਦੀ ਸਾਦੁ ਆਇਆ।
ਅੰਮ੍ਰਿਤੁ ਨੀਰੁ ਗਿਆਨਿ ਮਨੁ ਮਜਨੁ ਅਠਸਠਿ ਤੀਰਥ ਸੰਗਿ ਗਹੇ।
Entropy value
(Entropy of first sentence=0.8060, Entropy of second sentence=1.1149, Entropy of third sentence=1.1745, Entropy of fourth sentence=1.1279, Entropy of fifth sentence=1.0412)
Tampered Text
ਨਾਨਕ ਅੰਮ੍ਰਿਤੁ ਏਕੁ ਦੂਜਾ ਅੰਮ੍ਰਿਤੁ ਨਾਹਿ।
ਅੰਮ੍ਰਿਤੁ ਸਬਦੁ ਹੈ ਨਾਨਕ ਗੁਰਮੁਖਿ ਪਾਇਆ।
ਅੰਮ੍ਰਿਤ ਸਬਦੁ ਅੰਮ੍ਰਿਤ ਬਾਣੀ।
ਅੰਮ੍ਰਿਤ ਨਾਮੁ ਸਦ ਲਾਗਾ ਗੁਰ ਸਬਦੀ ਸਾਦੁ ਆਇਆ।
ਅੰਮ੍ਰਿਤੁ ਨੀਰੁ ਗਿਆਨਿ ਮਜਨੁ ਅਠਸਠਿ ਤੀਰਥ ਸੰਗਿ ਗਹੇ।
Entropy value
(Entropy of first sentence=0.7852, Entropy of second sentence=1.1692, Entropy of third sentence=1.1991, Entropy of fourth sentence=1.1642, Entropy of fifth sentence=1.0354)

Figure 5.4: Deletion Attack Example

Entropy values and Character Patterns each character of cover and tampered text are different. These differences show that both the text is different. On this basis, one can say that the proposed technique is able to detect the deletion attack.

Insertion Attack

A malicious user can insert extra word in the cover text during transmission time is known as a insertion attack. Due to change in the entropy value, the proposed technique is able to detect insertion type of tampering.

Table 5.5: Insertion Attack Example

Cover Text Once you stop learning, you start dying. In the middle of difficulty lies opportunity. Unthinking respect for authority is the greatest enemy of truth. Great things in business are never done by one person. They are done by a team of people.
Entropy value (Entropy of first sentence =4.0276, Entropy of second sentence=4.1313, Entropy of third sentence=4.0470, Entropy of fourth sentence= 3.8913, Entropy of fifth sentence= 3.6144)
Tampered Text Once you stop the learning, you start dying. In the middle of difficulty lies a opportunity. Unthinking respect for authority is the greatest enemy of a truth. Great things in business are never done by one from person. They are not done by a team of people.
Entropy Value (Entropy of first sentence =4.0522, Entropy of second sentence=4.1650, Entropy of third sentence=4.0393, Entropy of fourth sentence= 3.9825, Entropy of fifth sentence= 3.6240)

Table 5.5 shows the result of insertion attack by a malicious user. Red words are inserted in the cover text during the attack. Values of entropy is changed due to insertion of words as shown in Table 5.5. Only one alphabet insertion effects entropy as shown in Table 5.5.

Figure 5.5 describe the example of insertion attack on Hindi language. Some words are shown with underline inserted within the original cover text. These words are inserted by an malicious user.

Cover Text
मैं भारत से प्यार करता हूँ |
गुरुदेव रवींद्र नाथ ठाकुर भारत के बँगला साहित्य के शिरोमणि कवि थे |
उनकी कविता में प्रकृति के सौंदर्य और कोमलतम मानवीय भावनाओं का उत्कृष्ट चित्रण है|
"जन गण मन" उनकी रचित एक विशिष्ट कविता है जिसके प्रथम छंद को हमारे राष्ट्रीय गीत होने का गौरव प्राप्त है|
गणतंत्र दिवस के शुभ अवसर पर, काव्यालय की ओर से, आप सबको यह कविता अपने मूल बंगला रूप में प्रस्तुत है|
Entropy value
(Entropy of first sentence=0.9401, Entropy of second sentence=0.9812, Entropy of third sentence= 0.8987, Entropy of fourth sentence=1.0490, Entropy of fifth sentence=1.0746)
Tampered Text
मैं भारत से प्यार मैं करता हूँ |
गुरुदेव रवींद्र नाथ ठाकुर भारत उनकी के बँगला साहित्य के शिरोमणि कवि थे |
उनकी कविता में प्रकृति के सौंदर्य प्यार और कोमलतम मानवीय भावनाओं का उत्कृष्ट चित्रण है|
"जन गण मन" उनकी रचित एक विशिष्ट कविता है जिसके प्रथम छंद को हमारे राष्ट्रीय गीत होने का गौरव प्राप्त चित्रण है|
गणतंत्र दिवस के शुभ अवसर पर, काव्यालय की ओर से, कविता आप सबको यह कविता अपने मूल बंगला रूप में प्रस्तुत है|
Entropy value
(Entropy of first sentence=0.9308, Entropy of second sentence=0.9680, Entropy of third sentence=0.8854, Entropy of fourth sentence=1.0257, Entropy of fifth sentence=1.0553)

Figure 5.5: Insertion Attack Example

As shown in Figure 5.5, entropy of cover text is different as compared to tampered text. Change in the entropy is occurred due to insertion some words in the original text. A change in entropy means that cover text has been tampered.

Figure 5.6 shows the Punjabi language cover text and its tampered text. The entropy of both texts are different as shown in Figure. The words with underline are inserted during the insertion attack.

Cover Text
ਨਾਨਕ ਅੰਮ੍ਰਿਤੁ ਏਕੁ ਹੈ ਦੂਜਾ ਅੰਮ੍ਰਿਤੁ ਨਾਹਿ |
ਅੰਮ੍ਰਿਤੁ ਏਕੋ ਸਬਦੁ ਹੈ ਨਾਨਕ ਗੁਰਮੁਖਿ ਪਾਇਆ |
ਅੰਮ੍ਰਿਤ ਸਬਦੁ ਅੰਮ੍ਰਿਤ ਹਰਿ ਬਾਣੀ |
ਅੰਮ੍ਰਿਤ ਨਾਮੁ ਸਦ ਮੀਠਾ ਲਾਗਾ ਗੁਰ ਸਬਦੀ ਸਾਦੁ ਆਇਆ |
ਅੰਮ੍ਰਿਤੁ ਨੀਰੁ ਗਿਆਨਿ ਮਨ ਮਜਨੁ ਅਠਸਠਿ ਤੀਰਥ ਸੰਗਿ ਗਹੇ |
Entropy value
(Entropy of first sentence=0.8060, Entropy of second sentence=1.1149, Entropy of third sentence=1.1745, Entropy of fourth sentence=1.1279, Entropy of fifth sentence=1.0412)
Tampered Text
ਨਾਨਕ ਅੰਮ੍ਰਿਤੁ ਏਕੁ ਹੈ ਦੂਜਾ ਅੰਮ੍ਰਿਤੁ ਹੈ ਨਾਹਿ |
ਅੰਮ੍ਰਿਤੁ ਏਕੋ ਸਬਦੁ ਹੈ ਨਾਨਕ ਏਕੁ ਗੁਰਮੁਖਿ ਪਾਇਆ |
ਅੰਮ੍ਰਿਤ ਸਬਦੁ ਏਕੋ ਅੰਮ੍ਰਿਤ ਹਰਿ ਬਾਣੀ |
ਅੰਮ੍ਰਿਤ ਨਾਮੁ ਸਦ ਮੀਠਾ ਲਾਗਾ ਗੁਰ ਸਬਦੀ ਸਾਦੁ ਆਇਆ ਬਾਣੀ |
ਅੰਮ੍ਰਿਤੁ ਨੀਰੁ ਨਾਮੁ ਗਿਆਨਿ ਮਨ ਮਜਨੁ ਅਠਸਠਿ ਤੀਰਥ ਸੰਗਿ ਗਹੇ |
Entropy value
(Entropy of first sentence=0.8226, Entropy of second sentence=1.0991, Entropy of third sentence=1.1885, Entropy of fourth sentence=1.1207, Entropy of fifth sentence=1.0203)

Figure 5.6: Insertion Attack Example

As shown in Figure 5.6, entropy value is changed due to insertion attack. Different entropy means that the

cover text has been tampered.

Tampered Attack

In this type of attack, a word is altered from a malicious user. Due to alteration of a word, entropy value always effects as shown in Table 5.6.

Table 5.6: Tamper Attack Example

Cover Text Once you stop learning, you start dying. In the middle of difficulty lies opportunity. Unthinking respect for authority is the greatest enemy of truth. Great things in business are never done by one person. They are done by a team of people.
Entropy value (Entropy of first sentence =4.0276, Entropy of second sentence=4.1313, Entropy of third sentence=4.0470, Entropy of fourth sentence= 3.8913, Entropy of fifth sentence= 3.6144)
Tampered Text Once you stops learning, you start dying. In the middless of difficulty lies opportunity. Unthinking respects for authority is the greatest enemy of truth. Great things in business are never do by one person. They are done by an team of people.
Entropy Value (Entropy of first sentence =4.0036, Entropy of second sentence=4.1525, Entropy of third sentence=4.0500, Entropy of fourth sentence= 3.9251, Entropy of fifth sentence= 3.6416)

The words with red color are altered due to tampered attack by a malicious user as shown in Table 5.6. The entropy of every sentence is changed due to alter a word. So, the proposed technique is able to detect these types of tampering with help of entropy value.

Cover and tampered text are shown in the Figure 5.7 of Hindi language. Entropy value of both the text is calculated as shown in the Figure. As shown in the Figure 5.7, entropy value of both the text is different. The entropy value is different of both the text due to some words are tampered due to tampered attack. The words with underline as shown in Figure 5.7 are tampered of the cover text. At the base of entropy value, the proposed technique can detect the tampered text.

Cover Text
मैं भारत से प्यार करता हूँ |
गुरुदेव रवींद्र नाथ ठाकुर भारत के बँगला साहित्य के शिरोमणि कवि थे |
उनकी कविता में प्रकृति के सौंदर्य और कोमलतम मानवीय भावनाओं का उत्कृष्ट चित्रण है|
"जन गण मन" उनकी रचित एक विशिष्ट कविता है जिसके प्रथम छंद को हमारे राष्ट्रीय गीत होने का गौरव प्राप्त है|
गणतंत्र दिवस के शुभ अवसर पर, काव्यालय की ओर से, आप सबको यह कविता अपने मूल बंगला रूप में प्रस्तुत है|
Entropy value
(Entropy of first sentence=0.9401, Entropy of second sentence=0.9812, Entropy of third sentence=0.8987, Entropy of fourth sentence=1.0490, Entropy of fifth sentence=1.0746)
Tampered Text
मैं भारत से प्यार कर हूँ |
गुरुदेव रवींद्र नाथ ठाकुर भारत के बँगला साहित्य के शिरो कवि थे |
उनकी कविता में प्रकृति के सौंदर्य और कोमल मानवीय भावनाओं का उत्कृष्ट चित्रण है|
"जन गण मन" उनकी रचित एक विशिष्ट कविता है जिसके प्रथम छंद को हम राष्ट्रीय गीत होने का गौरव प्राप्त है|
गणतंत्र दिवस के शुभ अवसर पर, काव्यालय की ओर से, आप सब यह कविता अपने मूल बंगला रूप में प्रस्तुत है|
Entropy value
(Entropy of first sentence=0.9790, Entropy of second sentence=1.0093, Entropy of third sentence=0.9132, Entropy of fourth sentence=1.0681, Entropy of fifth sentence=1.0879)

Figure 5.7: Tamper Attack Example

Figure 5.8 describes the cover and tampered text of Punjabi language. The words with underline are altered word of cover text. These words are altered due to tamper attack.

Cover Text
ਨਾਨਕ ਅੰਮ੍ਰਿਤੁ ਏਕੁ ਹੈ ਦੂਜਾ ਅੰਮ੍ਰਿਤੁ ਨਾਹਿ |
ਅੰਮ੍ਰਿਤੁ ਏਕੋ ਸਬਦੁ ਹੈ ਨਾਨਕ ਗੁਰਮੁਖਿ ਪਾਇਆ |
ਅੰਮ੍ਰਿਤ ਸਬਦੁ ਅੰਮ੍ਰਿਤ ਹਰਿ ਬਾਣੀ |
ਅੰਮ੍ਰਿਤ ਨਾਮੁ ਸਦ ਮੀਠਾ ਲਾਗਾ ਗੁਰ ਸਬਦੀ ਸਾਦੁ ਆਇਆ |
ਅੰਮ੍ਰਿਤੁ ਨੀਰੁ ਗਿਆਨਿ ਮਨ ਮਜਨੁ ਅਠਸਠਿ ਤੀਰਥ ਸੰਗਿ ਗਹੇ |
Entropy value
(Entropy of first sentence=0.8060, Entropy of second sentence=1.1149, Entropy of third sentence=1.1745, Entropy of fourth sentence=1.1279, Entropy of fifth sentence=1.0412)
Tampered Text
ਨਾਨਕ ਅੰਮ੍ਰਿਤੁ ਏ ਹੈ ਦੂਜਾ ਅੰਮ੍ਰਿਤੁ ਨਾਹਿ |
ਅੰਮ੍ਰਿਤੁ ਏਕੋ ਸਬ ਹੈ ਨਾਨਕ ਗੁਰਮੁਖਿ ਪਾਇਆ |
ਅੰਮ੍ਰਿਤ ਸਬਦੁ ਅੰਮ੍ਰਿਤ ਹਰਿ ਬਾ |
ਅੰਮ੍ਰਿਤ ਨਾਮੁ ਸਦ ਮੀਠਾ ਲਾਗਾ ਗੁਰ ਸਬਦੀ ਸਾ ਆਇਆ |
ਅੰਮ੍ਰਿਤੁ ਨੀ ਗਿਆਨਿ ਮਨ ਮਜਨੁ ਅਠਸਠਿ ਤੀਰਥ ਸੰਗਿ ਗਹੇ |
Entropy value
(Entropy of first sentence=0.8306, Entropy of second sentence=1.1505, Entropy of third sentence=1.2235, Entropy of fourth sentence=1.1586, Entropy of fifth sentence=1.0693)

Figure 5.8: Tamper Attack Example

It is clear from the Figure 5.8, entropy value of every sentence of tampered image is changed due to tamper attack. Entropy value of every sentence of tampered image is different as compared to entropy value of every sentence of cover image. Different entropy value means that cover text has been tampered as shown in Figure 5.8.

Integrity Rate

A malicious user can alter or add any extra word in the text during the transmission process. Integrity rate *IR* of a technique is ability to detect a malicious user's activity. The proposed technique can detect different types of activities like alter or add any word in the text. It is cleared from deletion, insertion and tampered attacks example that proposed technique works for different types of attack and its *IR* is 100%.

IR of the proposed technique is compared with [Ahvanooey et al. (2020)]. The results of this comparison are shown in Table 5.7.

Table 5.7: Comparison of *IR* with the existing technique

Original *CT*	Compromised *CT*	Ahvanooey et al. (2020)	Proposed Technique
Once you stop learning, you start dying.	Once you discontinue learning, you start dying.	86 %	100 %
In the middle of difficulty lies opportunity.	In the medium of hardship lies opportunity.	71 %	100 %
Unthinking respect for authority is the greatest enemy of truth.	No thinking about authority is the greatest enemy of truth.	82 %	100 %
Great things in business are never done by one person. They are done by a team of people.	Great earnings in business are never achieved by one person. They are done by a team of people.	84 %	100 %
Beautiful people are not always good, but good people are always beautiful.	Beautiful persons are not always good, but good persons are always look beautiful.	62 %	100 %
Don't compare yourself with anyone in this world. If you do so, you are insulting yourself.	Do not compare yourself with anyone in this world. If you do so, you are offending yourself.	74 %	100 %

Table 5.7 describes the comparison of *IR* between the proposed technique with the existing technique. The idea behind the *IR* to verify the integrity and originality of the watermarked text. If an unauthorized user manipulates CT_w and the technique can detect this manipulation process is known as *IR* of the technique. The proposed technique can detect tampered occurred due to different types of attacks. This is the reason that *IR* of the proposed technique is 100% in every case.

5.5 Conclusion

The technique is evaluated on the document images of English, Hindi and Punjabi langauges. The quality of watermarked image is not degraded as embedding of *ZWCs* are not visible to the user. The proposed technique can detect the tamper occurred due to attack like insertion, deletion and tampering attack. The *IR* of the technique is 100% and provides good embedding capacity as well as good tamper detection capability against different attacks.

CHAPTER 6

Discrete Curvelet Transform and Discrete Cosine Transform based Watermarking Technique for Document Images

6.1 Introduction

In this Chapter, Discrete Curvelet Transform and Discrete Cosine Transform based watermarking technique is proposed to protect the document images. Discrete Curvelet Transform generates the six layer of the document image. Sixth layer is selected for the embedding process and discard other layers. Discrete Cosine Transform is applied on the 8×8 blocks of the sixth layer. Select the Discrete Cosine Transform coefficients from low to medium except the first Discrete Cosine Transform coefficient. Zigzag function is used to select the *DC* coefficients to embed the watermark bits. Watermark image is extracted at the receiver side. In this process, we need watermarked image as well as cover image because this is a non-blind technique. Apply the Discrete Cosine Transform on both the images. Extract the watermark image by comparing the Discrete Cosine Transform coefficients of watermarked image and the cover image. *PSNR*, *SSIM*, *MSE*, *NC*, *UQI* and *JPEG* attacks are evaluated to measure resistivity of the watermarked image against image processing attacks.

6.2 Preliminary

This section presents a brief description of the *DCuT* and *DCT*.

6.2.1 Discrete Curvelet Transform

DCuT, which is a multiresolution transform, was proposed by Candès and Donoho (2004). It imparts a sparser representation of images as compared to other transforms. To represent an image, Fractional Fourier Transform (*FrFT*) and *DWT* need a higher number of frequency coefficients and wavelet basis functions, respectively. *DCuT* represents edges and curves information of the image. For an image $I(x, y)$, *DCuT* generates coefficients using:

$$C^D(sc, ot, tr) = \sum_{0 \leq x,y \leq h} f(x, y)^{\theta^D_{sc,ot,tr}(x,y)} \tag{6.1}$$

Here, $\theta^D_{sc,ot,tr}(x, y)$ represents digital curvelet waveform of a cartesian array of form $f(x, y)$ where $0 \leq x, y \leq h$. $h \times h$ represents image size. *sc*, *ot* and *tr* refer to scale, orientation and translation parameters, respectively. According to Candès and Donoho (2004), there are two variations of *DCuT*: Unequi-spaced Fast Fourier Transform(*FFT*) and *WRAP*. Image watermarking and compression applications mostly use *WRAP* due to it's simpler implementation and low computation time as compared to Unequi-spaced *FFT*. *WRAP* based *DCuT* is graphically represented in Figure 6.1.

WRAP is implemented as follows:

(i) Obtain Fourier samples $\hat{f}[i_1, i_2]$ by applying 2D *FFT* on image.

(ii) For every scale *sc* and angle *ot*

  (a) Perform: $\hat{f}[i_1, i_2] \times \hat{u}_{j,l}[i_1, i_2]$

  (b) Wrap this result around origin

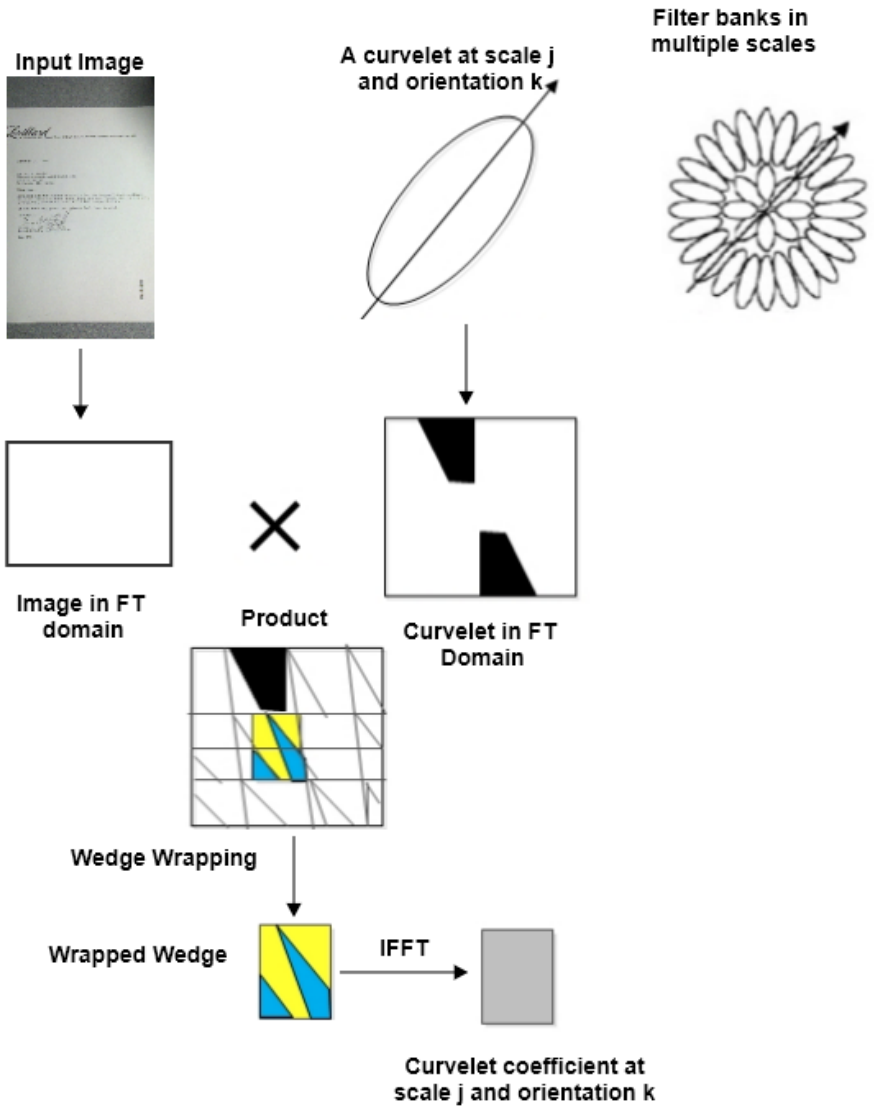
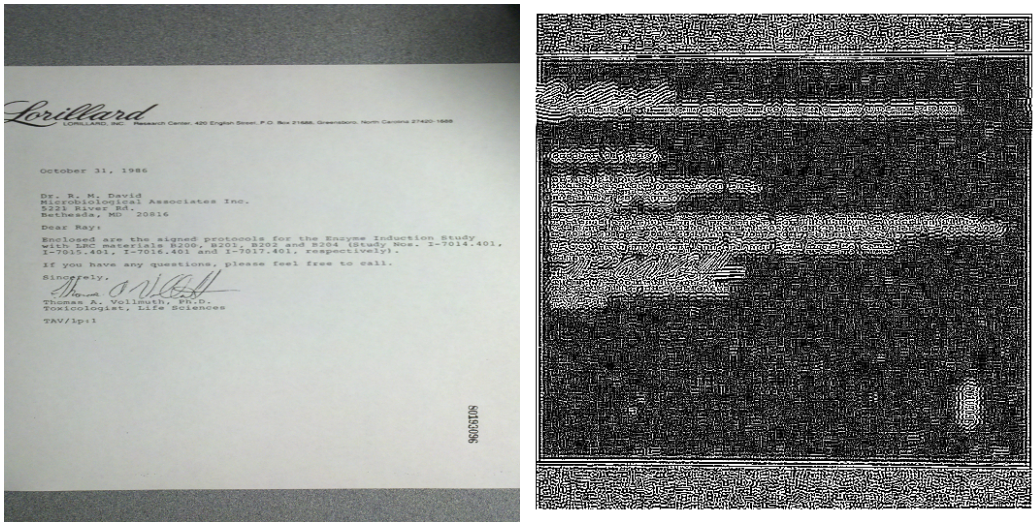


Figure 6.1: Frequency wrapping based DCuT

The obtained curvelet coefficients $C(sc, ot, tr)$, where sc, ot and tr represent scale, direction and translation parameters, respectively, are divided into three frequency sub-bands: Low Frequency *(LF)*, Middle Frequency *(MF)* and High Frequency *(HF)*. The coefficient count in every sub-band depends on the image size. For example, an image of size 512×512 is decomposed using *DCuT-WRAP* into different cells, represented as C(1,1), C(1,2), C(1,3), C(1,4), C(1,5), C(1,6), with 6 scale parameters and 16 orientation parameters. The innermost cell C(1,1) consists *LF* coefficients, middle cells C(1,2) to C(1,5) contain *MF* coefficients and the outermost C(1,6) contains *HF* coefficients and is equal to the image size. *LF* and *MF* coefficients provide better robustness to the scheme as compared to *HF*. The watermark is retrieved successfully to prove the copyright, even when the image is attacked by different image processing attacks. Sixth layer for document image

constructed using *DCuT* is shown in Figure 6.2.



(a) Original Image (b) Sixth Layer of Original Image

Figure 6.2: Sixth layer of original document image

6.2.2 Discrete Cosine Transform

DCT is a mathematical transform which converts the function from time domain into the frequency domain. It generates many coefficients: single Direct Current (*DC*) and a set of Alternting Current (*AC*). Figure 6.3 shows 8×8 blocks of the *DCT* matrix. Low frequency coefficients located in the upper left corner of *DCT* matrix. The coefficients in the lower right corner are high frequency coefficients [Lin et al. (2010)].

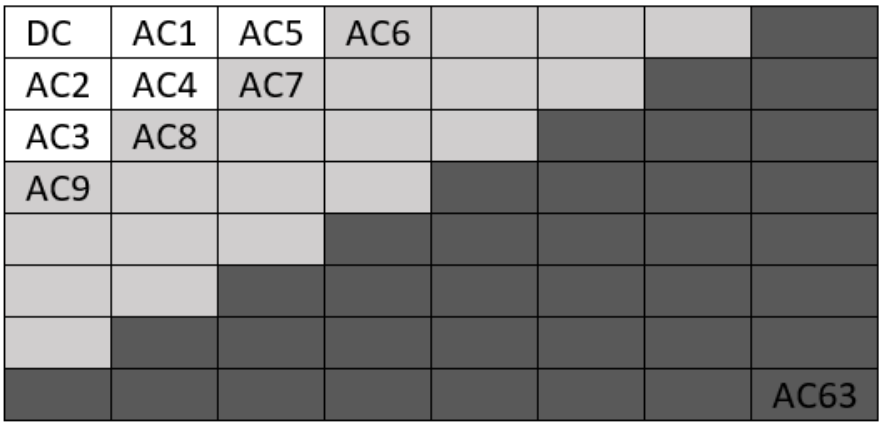


Figure 6.3: DCT Coefficients matrix and frequency bands

Any image I with size $M\times N$ in spatial doamin is transformed into *DCT* domain by using the following

equations:

$$I^{'}(u,v) = a(u) \times a(v) \sum_{x=1}^{M-1} \sum_{y=1}^{N-1} I(x,y) \cos\left[\frac{(2x+1)u\pi}{2M}\right] \cos\left[\frac{(2y+1)v\pi}{2N}\right] \tag{6.2}$$

Where, a(u) = $\sqrt{\frac{1}{M}}$ for u = 0; a(u) = $\sqrt{\frac{2}{M}}$ for u = 1,2,3...M-1;
a(v) = $\sqrt{\frac{1}{N}}$ for v = 0; a(v) = $\sqrt{\frac{2}{N}}$ for v = 1,2,3...N-1.

$$I(x,y) = \sum_{u=1}^{M-1} \sum_{v=1}^{N-1} a(u) \times a(v) \times I^{'}(u,v) \cos\left[\frac{(2x+1)u\pi}{2M}\right] \cos\left[\frac{(2y+1)v\pi}{2N}\right] \tag{6.3}$$

$I^{'}$(0,0) is the *DC* coefficient, which contains the most energy of the image. The high frequency coefficients represents the edge and detailed information of the image. The details are increased by moving to the bottom right of the *DCT* block[Alotaibi and Elrefaei (2019)].

6.3 Proposed Technique

In this section, embedding and extraction algorithms of the proposed approach are discussed. Main goal of the proposed technique to protect the digital document images against different attacks by embedding a watermark using *DCuT* and *DCT*. In the embedding process, *DCuT* generates six layer after applying on the cover image. Select the sixth layer for the embedding process and discard other layers. Low frequency coefficients are modified in the robust watermarking methods, while in imperceptible watermarking method the high frequency coefficients are changed. *DCT* is mostly used in digital watermarking because it is compatible with *JPEG* compression and its output is real matrix.

In the embedding process, a color document image is used as a cover image. First *DCuT* is applied on the cover image to generate six layer of the image. Real part of the sixth layer is selected for the further process and discard others layer as shown in Figure 6.4. The number of *AC* coefficients for embedding process in each *DCT* block are: 9, 16, 25 and 36. The first 9 bits of the watermark image are embedded in the first 9 *AC* coefficients in ziz zag pattern. The next 9 bits of the watermark image are embedded in the first 9 *AC* coefficients of the second block and so on. The proposed *DCuT-DCT* -16, proposed *DCuT-DCT* -25 and proposed *DCuT-DCT* -36 use the same procedure with changing the number of the *AC* coefficients of *DCT* blocks.

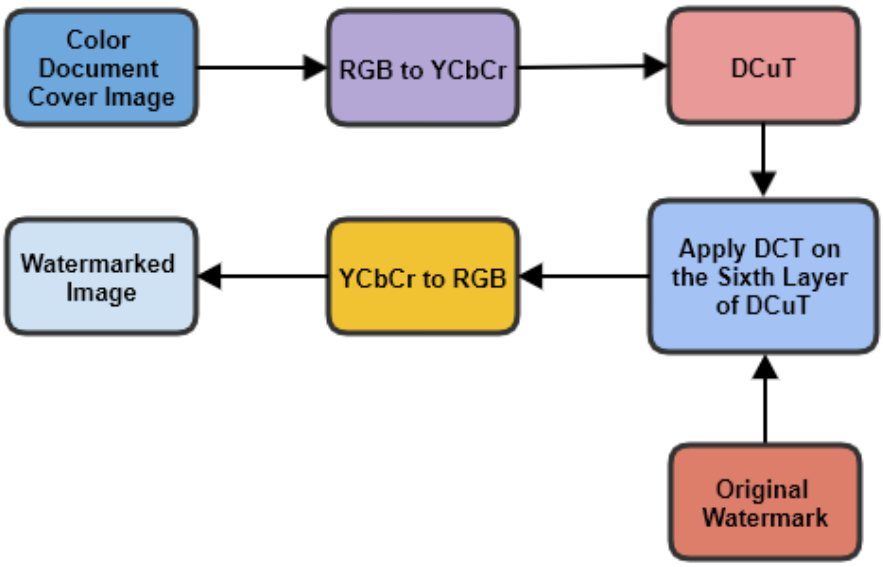


Figure 6.4: Embedding Process

RGB image is converted into *YCbCr* image before the embedding process by using the following formula. *RGB* to *YCbCr* is used to decrease the complexity. *Y* component is selected for the embedding process because it contains the most of the image information as compared to other components.

$$Y = 0.299R + 0.587G + 0.114B \tag{6.4}$$

$$Cb = 128 - 0.168736R - 0.331264G + 0.5B \tag{6.5}$$

$$Cr = 128 + 0.5R - 0.418688G - 0.081312B \tag{6.6}$$

The reverse process is applied on the *YCbCr* image to convert it into *RGB* image before the reconstruction process by using the following formula.

$$R = Y + 1.402(Cr - 128) \tag{6.7}$$

$$G = Y - 0.34414(Cb - 128) - 0.71414(Cr - 128) \tag{6.8}$$

$$B = Y + 1.772(Cb - 128) \tag{6.9}$$

Zigzag process is used to select the *DCT* coefficients for the embedding process as shown in Figure 6.5.

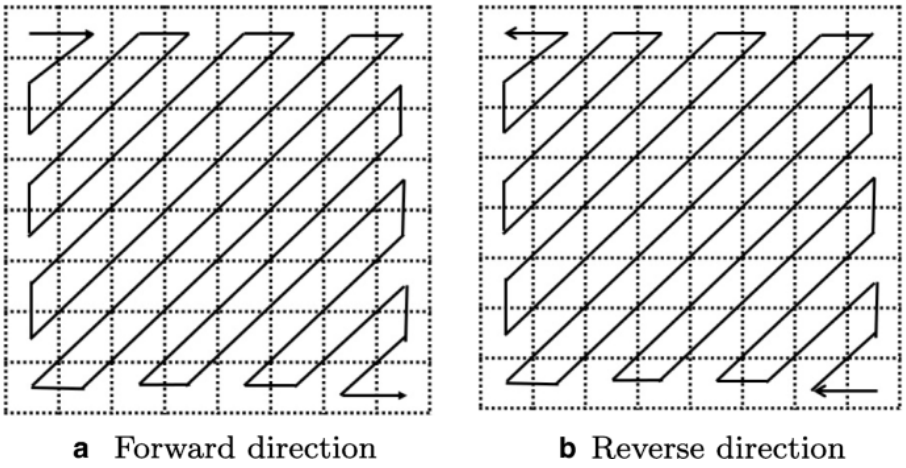


Figure 6.5: Zigzag process

In the extraction process, both the watermarked image as well as cover image are required. Apply the same processes on both the image to extract the watermark as shown in Figure 6.6. Cover and watermarked images are converted from *RGB* into *YCbCr* color space. Y component is selected in the embedding process. *DCuT* is applied on the selected component to generate the six layers. *DCT* is applied on the sixth layer. Watermark is extracted and used to compare with the orginal watermark for protection process.

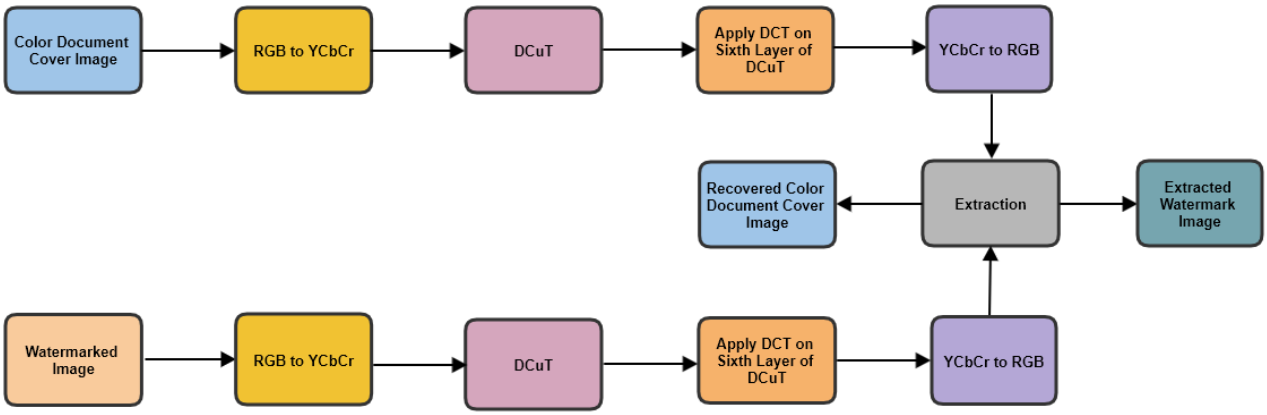


Figure 6.6: Extraction Process

Embedding algorithm explains the method of embedding used in proposed technique. First, *DCuT* is applied on the cover image. *DCuT* generates six layers of the cover image. Sixth layer contains the most energy of the image so six layer is selected for the embedding process and discard others layer. Now apply 8×8 block *DCT* on the sixth layer to generate the *DCT* coefficients. Select the *DCT* coefficients from low to medium except the first *DC* coefficient. Zigzag function is used to select the *DC* coefficients to embed the watermark bits.

6.3.1 Embedding Algorithm

Algorithm 7: Embedding Algorithm

Input: A cover document image , Watermark W

Output: A watermarked document image.

1 Read a cover document image.

2 Convert *RGB* into *YCbCr*.

3 Apply *DCuT* on *Y* component of *YCbCr* image to generate six layers.

4 Apply 8×8 block *DCT* on real part of sixth layer and discard other layers. Select the *DCT* coefficients from low to medium except the first *DC* coefficient.

5 $DC_b.AC_{b,1}.AC_{b,2}...AC_{b,N}....AC_{b,63}$ = *DCT*(Real part of Sixth Layer, $Sixth_{Real}$) for b =1:B

6 Where *N* is the number of the chosen coefficients per block and *B* is the number 8×8 *DCT* blocks which is calculated as:

$$B = \frac{m \times n}{64} \tag{6.10}$$

7 Resize the watermark image *W* is of size r $\times$ r.

8 Convert the watermark image *W* into a vector *V* of size $1 \times r^2$.

9 Embed the *V* which represents the watermark image in the chosen *DCT* coefficients from $AC_{b,1}$ to $AC_{b,N}$ in each block using the following equations:

10 $AC'_{b,i}$ = $AC_{b,i}$ + (α $\times$V(i +(b-1) $\times$ N)) for i = 1:N, b = 1:B, where $AC_{b,i}$ is indicating to *DCT* coefficient α indicates the scaling factor and *V* indicates the vector representing the watermark image.

11 Perform zigzag function to select the *DCT* coefficients to embed the watermark bits.

12 To reconstruct the *DCT* coefficients apply Inverse zigzag function. Now, apply Inverse *DCT* to each block in the real part of sixth layer.

13 $Sixth'_{Layer}$ = *IDCT* ($DC_b.AC_{b,1}.AC_{b,2}...AC_{b,N}....AC_{b,63}$)

14 Apply Inverse *DCuT* on the $Sixth'_{Layer}$ to get watermarked image.

15 **Return** Watermarked Image

6.3.2 Extraction Algorithm

Algorithm 8: Extraction Algorithm

Input: Document cover Image, Watermarked image

Output: Cover document image, Extracted Watermark

1 Read a watermarked image and Cover image.

2 Convert both the images from *RGB* into *YCbCr* image.

3 Apply *DCuT* on *Y* component of *YCbCr* image to generate six layers.

4 Apply 8×8 block *DCT* on real part of sixth layer and discard other layers. Select the *DCT* coefficients from low to medium except the first DC coefficient.

5 $DC_b.AC_{b,1}.AC_{b,2}...AC_{b,N}....AC_{b,63}$ = *DCT*(Real part of Sixth Layer, $Sixth_{Real}$) for b =1:B

6 Where N is the number of the chosen coefficients per block and B is the number 8×8 *DCT* blocks which is calculated as:

$$B = \frac{m \times n}{64} \tag{6.11}$$

7 Apply *DCuT* on watermarked document image to generate six layer.

8 Apply 8×8 block *DCT* on real part of sixth layer and discard other layers. Select the *DCT* coefficients from low to medium except the first DC coefficient.

9 $DC'_b.AC'_{b,1}.AC'_{b,2}...AC'_{b,N}....AC'_{b,63}$ = *DCT*($Sixth_{Real}$) for b =1:B, where N is the number of the chosen coefficients per block

10 Extract the vetor V which represents the watermark image by comparing the *DCT* coefficients $AC_{b,1}$ to $AC_{b,N}$ of cover document image and *DCT* coefficients $AC'_{b,1}$ to $AC'_{b,N}$ of watermarked image using the following equation:

11 V(i +(b-1) $\times$ N) =($AC'_{b,i}$ - $AC_{b,i}$)/α for i = 1:N, b = 1:B

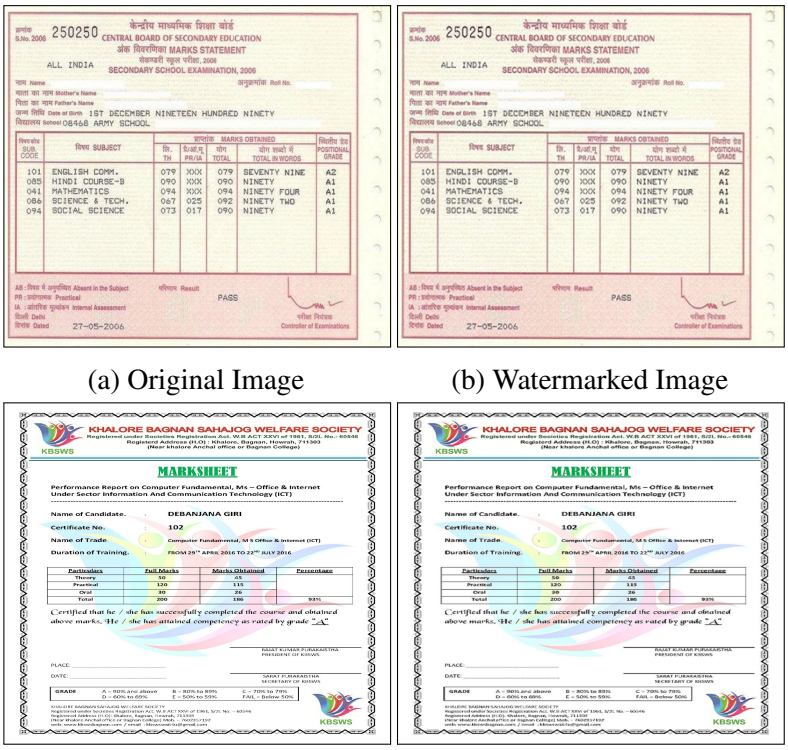
12 The resulting vector V is with size of $1 \times r^2$, r^2 is calculated as: r^2 = B $\times$ N

13 Convert the vector V into watermark image W of size r $\times$ r.

Extraction algorithm is used to extract the watermark image at the receiver side. During this process, we need watermarked image as well as cover image because this is a non-blind technique. Apply the *DCuT* and *DCT* on both the images. Extract the watermark image by comparing the *DCT* coefficients of watermarked image and *DCT* coefficients of cover image.

6.4 Experimental Results and Performance Analysis

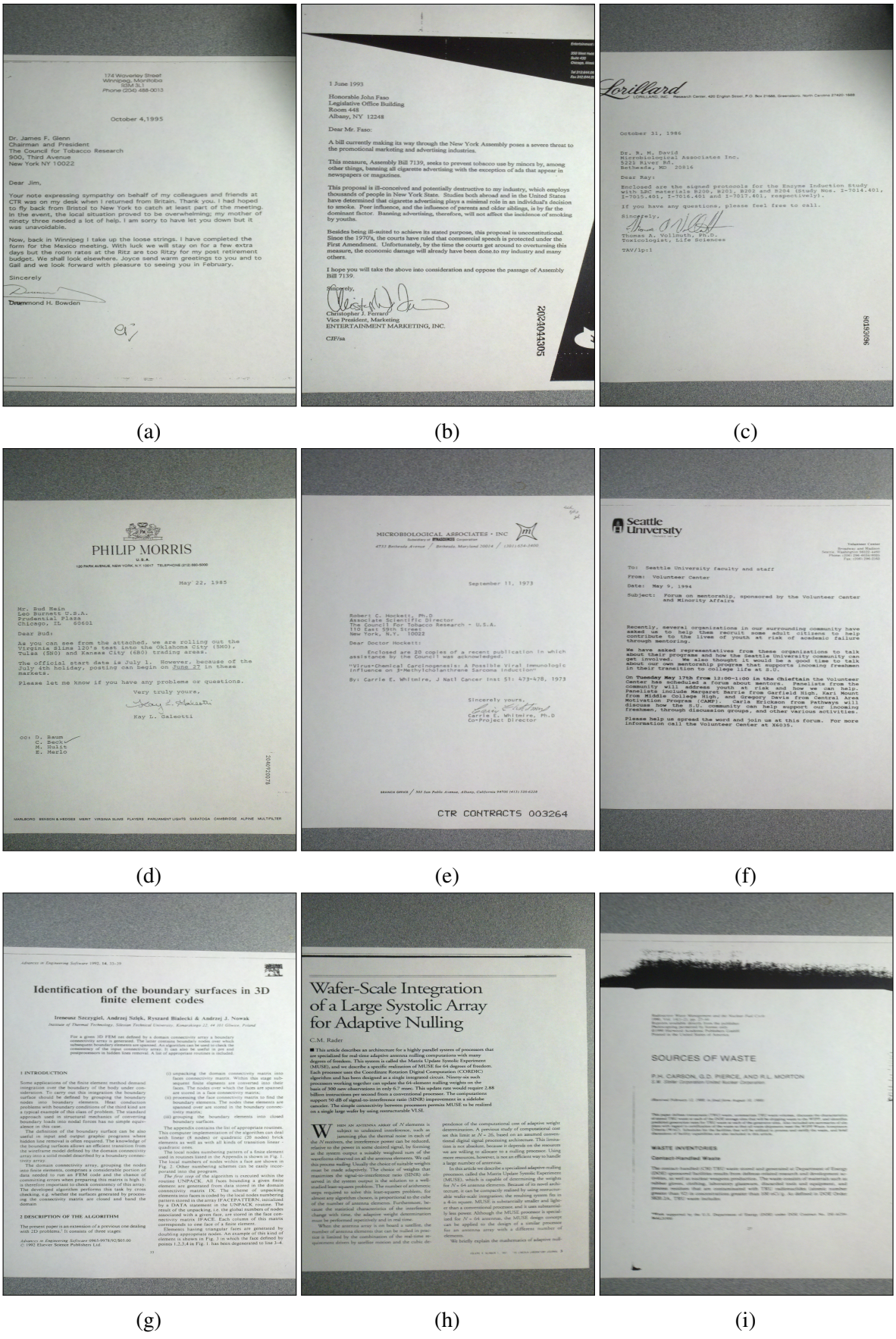
The proposed technique is implemented in R2019a version of *MATLAB* tool. For this implementation, *DIQA* dataset [Kumar et al. (2013)] images have been considered. Proposed technique is developed to protect the document images using *DCuT* and *DCT*. *PSNR, SSIM, NC and UQI* are used to evaluate the performance of the technique. Figure 3.6 contains the original document images with size 512×512 that are used in the implementation process. Figure 6.7 contains the watermarked image corresponding to the original color document image. Figure 6.8 contains the watermarked images corresponding to the original document images shown in Figure 3.6.



(a) Original Image (b) Watermarked Image

(c) Original Image (d) Watermarked Image

Figure 6.7: Watermarked Document Image Corrsponding to Original Image



(a) (b) (c)

(d) (e) (f)

(g) (h) (i)

Figure 6.8: Watermarked Document Images Corresponding to Original Images of Figure 3.6

6.4.1 Imperceptibility

The imperceptibility results of the proposed *DCuT-DCT* using different numbers of bits is shown in Figure 6.2. The numbers of hidden bits effects the transparency, but the distortion is very less. Cover document images and corresponding watermarked document images are shown in Figure 3.6 and Figure 6.8 respectively when number of coefficients is equal to 9. It is shown that there is no visual difference between cover and watermarked images. Table 6.1 shows the imperceptibility results of the proposed *DCuT-DCT* approach with other approaches: *IWT-DCT*[Alotaibi and Elrefaei (2019)], *IWT-SVD*[Makbol and Khoo (2014)], *IWT-SVD*[Gokhale and Joshi (2012)], *DCT-DWT*[Jiansheng et al. (2009)], *DWT-DCT*[Akter et al. (2014)], *DCT-SVD*[Mukherjee and Pal (2012)], *IWT-DCT*[Agrwal et al. (2016)].

Table 6.1: Imperceptibility comparison results using averages *PSNR* (in d**B**)

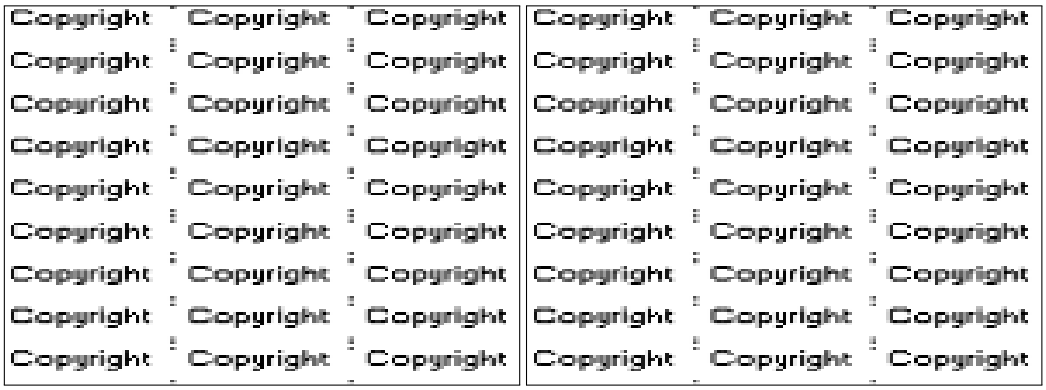
Technique	No. of bits embedded	*PSNR*
Proposed Technique	9	60.65
	16	60.21
	25	59.77
	36	59.22
Alotaibi and Elrefaei (2019)	9	58.17
	16	57.99
	25	57.89
	36	57.45
Jiansheng et al. (2009)	NA	50.28
Mukherjee and Pal (2012)	NA	41.44
Gokhale and Joshi (2012)	NA	43.67
Akter et al. (2014)	NA	36.52
Makbol and Khoo (2014)	NA	50.11
Agrwal et al. (2016)	NA	45.09

Table 6.2: Imperceptibility of the Proposed Technique

Image	No. of bits per *DCT* Block	Metrics				
		PSNR	SSIM	MSE	NC	UQI
Original Image 1	4	61.15	0.99	0.05	0.99	0.99
	9	60.23	0.99	0.07	0.99	0.99
	16	60.12	0.99	0.07	0.99	0.99
	25	59.45	0.99	0.09	0.99	0.99
	36	59.17	0.99	0.1	0.99	0.99
Original Image 2	4	60.21	0.99	0.06	0.99	0.99
	9	60.15	0.99	0.08	0.99	0.99
	16	60.11	0.99	0.08	0.99	0.99
	25	59.45	0.99	0.09	0.99	0.99
	36	59.31	0.99	0.11	0.99	0.99
Original Image 3	4	61.88	0.99	0.05	0.99	0.99
	9	61.33	0.99	0.08	0.99	0.99
	16	60.34	0.99	0.08	0.99	0.99
	25	60.21	0.99	0.09	0.99	0.99
	36	59.21	0.99	0.09	0.99	0.99
Original Image 4	4	60.89	0.99	0.07	0.99	0.99
	9	60.31	0.99	0.08	0.99	0.99
	16	59.23	0.99	0.08	0.99	0.99
	25	59.22	0.99	0.09	0.99	0.99
	36	58.67	0.99	0.11	0.99	0.99
Original Image 5	4	60.91	0.99	0.06	0.99	0.99
	9	60.72	0.99	0.08	0.99	0.99
	16	59.93	0.99	0.08	0.99	0.99
	25	59.54	0.99	0.11	0.99	0.99
	36	58.97	0.99	0.11	0.99	0.99
Original Image 6	4	61.67	0.99	0.05	0.99	0.99
	9	60.19	0.99	0.07	0.99	0.99
	16	60.13	0.99	0.07	0.99	0.99
	25	59.96	0.99	0.08	0.99	0.99
	36	59.71	0.99	0.09	0.99	0.99
Original Image 7	4	62.11	0.99	0.06	0.99	0.99
	9	61.05	0.99	0.08	0.99	0.99
	16	60.59	0.99	0.08	0.99	0.99
	25	60.55	0.99	0.09	0.99	0.99
	36	59.09	0.99	0.1	0.99	0.99
Original Image 8	4	61.96	0.99	0.06	0.99	0.99
	9	60.11	0.99	0.07	0.99	0.99
	16	59.98	0.99	0.07	0.99	0.99
	25	58.79	0.99	0.08	0.99	0.99
	36	58.71	0.99	0.1	0.99	0.99
Original Image 9	4	62.17	0.99	0.05	0.99	0.99
	9	61.78	0.99	0.07	0.99	0.99
	16	61.53	0.99	0.07	0.99	0.99
	25	60.79	0.99	0.08	0.99	0.99
	36	59.67	0.99	0.09	0.99	0.99

6.4.2 Robustness

Robustness is an important parameter to evaluate a watermarking technique. The robustness of the proposed technique is evaluated using images as shown in Figure 3.6. Original watermark image and extracted watermark image was compared with the help of *PSNR* parameter. Different attacks like scaling, filtering, rotation, histogram equalization, *JPEG* compression and noise are used in robustness test. The value of robustness is increased with increasing the coefficients value. *DCuT-DCT-36* provides the highest robustness against most attacks. The average of nine images are used to compare proposed technique with the existing techniques.



(a) Original Watermark (b) Extracted Watermark without attack

Figure 6.9: Extraction of Watermark

Figure 6.9 contains the original watermark and extracted watermark. The extracted watermark image is same as the original watermark when there is no attack on the watermarked image. Figure 6.10 shows the extraction of watermark against different attacks like cropping, *JPEG* compression, scaling, rotation, median filter and salt & noise pepper. Due to an attack, the extracted watermark is distorted in different places as shown in Figure 6.10. *PSNR* value between cover image and watermwrked image is calculated against some attacks such as *JPEG* compression with different quality parameters, rotation, salt & pepper noise. These *PSNR* values are shown in Table 6.3. Robustness of the proposed technique is compared with the existing techniques by using *PSNR* value. Robustness of proposed technique is better as compared to the existing techniques as shown in Table 6.3.

Extracted watermark of proposed technique is compared with the existing technique is shown in Figure 6.11. The quality of extracted watermark of proposed technique is good as compared to existing technique.



(a) Histogram Equalization (b) Median Filter (c) Salt & noise 0.001

(d) Scaling (e) Rotation (15°) (f) Rotation (45°)

(g) Cropping-I (h) Cropping-II (i) Salt & Noise 0.005

Figure 6.10: Extraction of watermark after attacks on the Watermarked Images



(a) Proposed Technique (b) Alotaibi and Elrefaei (2019) (c) Agrwal et al. (2016)



(d) Akter et al. (2014) (e) Makbol and Khoo (2014) (f) Gokhale and Joshi (2012)



(g) Jiansheng et al. (2009) (h) Mukherjee and Pal (2012)

Figure 6.11: Comparison of Extracted Watermark of Proposed Technique with existing techniques

Table 6.3: Robustness results of the proposed technique comparison with the existing techniques

Attacks	Proposed DCuT-DCT-9	Proposed DCuT-DCT-16	Proposed DCuT-DCT-25	Proposed DCuT-DCT-36	IWT-DCT-9 [Alotaibi and Elrefaei (2019)]	IWT-DCT-16 [Alotaibi and Elrefaei (2019)]	IWT-DCT-25 [Alotaibi and Elrefaei (2019)]	IWT-DCT-36 [Alotaibi and Elrefaei (2019)]
JPEG compression Q=10	43.89	42.08	41.93	41.16	40.32	40.91	41.48	41.07
JPEG compression Q=20	46.71	45.83	45.15	45.05	44.46	44.78	44.87	44.47
JPEG compression Q=25	47.39	46.12	45.29	45.14	43.77	44.6	44.9	44.83
JPEG compression Q=30	48.42	47.83	46.13	45.08	40.32	40.91	41.48	41.07
Rotation (15°)	20.52	19.49	19.79	18.94	14.51	15.98	17.36	18.66
Salt & pepper noise	43.17	42.89	41.69	40.27	40.18	40.21	40.53	39.58

Table 6.3: Continued..

Attacks	DWT-DFT[Li and Wu (2013)]	DCT[Laouamer and Tayan (2015)]	SVD[Li and Wu (2013)]	DWT-DCT[Wu et al. (2015)]
JPEG compression Q=10	17.71	NA	NA	17.71
JPEG compression Q=20	19.95	NA	NA	19.95
JPEG compression Q=25	21.6	NA	NA	21.6
JPEG compression Q=30	23.07	NA	NA	23.07
Rotation (15°)	5.239	NA	NA	5.239
Salt & pepper noise	NA	37.82	37.59	NA

6.5 Conclusion

This Chapter proposes a novel watermarking technique for protection of document images based on *DCuT* and *DCT* is proposed. The technique shows good imperceptibility that is measured with the help of metrics like *PSNR*, *MSE*, *SSIM*, *NC* and *UQI*. Maximum value of *PSNR* is 48.42 against *JPEG* compression in case of proposed *DCuT-DCT-9* to show the good robustness. *SSIM*, *NC* and *UQI* value is 0.99 to prove the good imperceptibility. The proposed technique shows good robustness against *JPEG* compression as compared to the existing techniques.

CHAPTER 7

Conclusion and Future Scope

7.1 Conclusion

There are seven Chapters in this thesis. Chapter 1 introduces the problems tackled in the thesis and also discusses the fundamentals related to the watermarking domain. In Chapter 2, detailed literature survey related to document image watermarking is carried out. In Chapter 3, a zero watermarking technique is proposed in which the watermark is generated by using features of the transformed image and stored by a Certifying Authority. Original watermark and watermark generated from the tampered image are compared to check the authenticity of the image is authentic. *BER* of the tampered image provided by the technique is better as compared to the *BER* of the existing techniques. Maximum value of *BER* is 99.96 in case of 4×4 block size and maximum *SSIM* value is 0.72 in case of 16×16 block size. Maximum value of *PSNR* between cover and watermarked image is 58.87 d*B* which indicates strong robustness of the technique.

In Chapter 4, *ZWC*s of Unicode standard are utilized to propose a watermarking technique. In this technique, the watermark and hash value of cover image are embedded after converting into *ZWC* values at the end of each sentence of the cover image text. By using *ZWC*s, both of these values are embedded in the invisible form, due to which the visual quality of the watermarked images is not degraded. Embedding capacity and *IR* of the proposed technique are better than the existing techniques. *IR* of the proposed technique is 100 %. Maximum value of *SSIM* is 0.99 against *JPEG* compression attack. Maximum value of *DR* of the proposed technique is 99.5.

In Chapter 5, Entropy and Markov Matrix are used to propose a tamper detection technique for the text images. The quality of watermarked image is not degraded as the embedding of *ZWC*s of entropy value is invisible. The proposed technique can detect the tamper occurred due to various attacks like insertion, deletion and tampering. The *IR* of the technique is 100 % and the technique has tamper detection capability against different image processing attacks.

A watermarking technique based on *DCuT* and *DCT* is proposed in Chapter 6 which can be used to provide the protection to the document images. This technique shows good imperceptibility that is measured with the help of metrics like *PSNR*, *MSE*, *SSIM*, *NC* and *UQI*. The proposed technique shows good robustness against *JPEG* compression in comparison to the robustness of the existing techniques. Maximum value of *PSNR* is 48.42. *SSIM*, *NC* and *UQI* values are 0.99 which indicate that the technique has good imperceptibility. The proposed technique shows more robustness against *JPEG* compression as compared to the existing techniques.

7.2 Future Scope

This work has focused on the development of watermarking techniques. Four different techniques have been proposed to remove the gaps in the existing techniques. However, there is still a scope of improvement in the implementation of these tehniques. This section discusses a few possible improvements that can further improve the watermarking techniques applicable to document images.

- Wavelet based zero watermarking technique can be extended by generating zero watermark by combining the spatial and transformed features of the cover document image.
- Proposed technique(s) can be extended to develop the hybrid watermarking technique by using seperate embedding approaches for textual regions as well as for the non-textual regions of the document.
- Advanced transforms like Slantlet, Ridgelet *etc*. can be used to extend the Curvelet based watermarking technique.

References

Agrwal, S. L., Yadav, A., Kumar, U., and Gupta, S. K. (2016). Improved invisible watermarking technique using iwt-dct. In *2016 5th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO)*, pages 283–285. IEEE.

Ahmad, F. and Cheng, L.-M. (2018). Authenticity and copyright verification of printed images. *Signal Processing*, 148:322–335.

Ahvanooey, M. T., Li, Q., Zhu, X., Alazab, M., and Zhang, J. (2020). Anitw: A novel intelligent text watermarking technique for forensic identification of spurious information on social media. *Computers & Security*, 90:101702.

Akter, A., Ullah, M. A., et al. (2014). Digital image watermarking based on dwt-dct: Evaluate for a new embedding algorithm. In *2014 International Conference on Informatics, Electronics & Vision (ICIEV)*, pages 1–6. IEEE.

Al-Haj, A. and Barouqa, H. (2017). Copyright protection of e-government document images using digital watermarking. In *2017 3rd International Conference on Information Management (ICIM)*, pages 441–446. IEEE.

Al-maweri, N. S., Adnan, W. W., Ramli, A., Samsudin, K., and Rahman, S. (2016). Robust digital text watermarking algorithm based on unicode extended characters. *Indian Journal of Science and Technology*, 9(48):1–14.

Al-Wesabi, F. N., Alshakaf, A. Z., and Vasantrao, K. U. (2012). A zero text watermarking algorithm based on the probabilistic weights for content authentication of text documents. In *IJCA Proceedings on National Conference on Recent Trends in Computing (NCRTC)*, volume 7, pages 26–31. Citeseer.

Al-Wesabi, F. N., Mahmood, K., and Nemri, N. (2020). A zero watermarking approach for content authentication and tampering detection of arabic text based on fourth level order and word mechanism of markov model. *Journal of Information Security and Applications*, 52:102473.

Alattar, A. M. and Alattar, O. M. (2004). Watermarking electronic text documents containing justified paragraphs and irregular line spacing. In *Security, Steganography, and Watermarking of Multimedia Contents VI*, volume 5306, pages 685–695. International Society for Optics and Photonics.

Alginahi, Y. M., Kabir, M. N., and Tayan, O. (2013). An enhanced kashida-based watermarking approach for arabic text-documents. In *2013 International Conference on Electronics, Computer and Computation (ICECCO)*, pages 301–304. IEEE.

Alginahi, Y. M., Kabir, M. N., 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*, 6(5):381.

Alotaibi, R. A. and Elrefaei, L. A. (2016). Utilizing word space with pointed and un-pointed letters for arabic text watermarking. In *2016 UKSim-AMSS 18th International Conference on Computer Modelling and Simulation (UKSim)*, pages 111–116. IEEE.

Alotaibi, R. A. and Elrefaei, L. A. (2018). Improved capacity arabic text watermarking methods based on open word space. *Journal of King Saud University-Computer and Information Sciences*, 30(2):236–248.

Alotaibi, R. A. and Elrefaei, L. A. (2019). Text-image watermarking based on integer wavelet transform (iwt) and discrete cosine transform (dct). *Applied Computing and Informatics*, 15(2):191–202.

Amano, T. and Misaki, D. (1999). A feature calibration method for watermarking of document images. In *Proceedings of the Fifth International Conference on Document Analysis and Recognition. ICDAR'99 (Cat. No. PR00318)*, pages 91–94. IEEE.

Atallah, M. J., Raskin, V., Hempelmann, C. F., Karahan, M., Sion, R., Topkara, U., and Triezenberg, K. E. (2002). Natural language watermarking and tamperproofing. In *International workshop on information hiding*, pages 196–212. Springer.

Ba-Alwi, F. M., Ghilan, M. M., and Al-Wesabi, F. N. (2014). Content authentication of english text via internet using zero watermarking technique and markov model. *International Journal of Applied Information Systems (IJAIS)*, 7(1):25–36.

Bailey, K. and Curran, K. (2006). An evaluation of image based steganography methods. *Multimedia Tools and Applications*, 30(1):55–88.

Bashardoost, M., Rahim, M. S. M., Saba, T., and Rehman, A. (2017). Replacement attack: a new zero text watermarking attack. *3D Research*, 8(1):8.

Behera, P. K. and Gangopadhyay, S. (2021). An improved hybrid genetic algorithm to construct balanced boolean function with optimal cryptographic properties. *Evolutionary Intelligence*, pages 1–15.

Bensaad, M. L. and Yagoubi, M. B. (2011). High capacity diacritics-based method for information hiding in arabic text. In *2011 International Conference on Innovations in Information Technology*, pages 433–436. IEEE.

Bhattacharjya, A. K. and Ancin, H. (1999). Data embedding in text for a copier system. In *Proceedings 1999 International Conference on Image Processing (Cat. 99CH36348)*, volume 2, pages 245–249. IEEE.

Brassil, J., Low, S., Maxemchuk, N., and O'Gorman, L. (1995). Hiding information in document images. In *Proc. Conf. Information Sciences and Systems (CISS-95)*, pages 482–489.

Brassil, J. T., Low, S., and Maxemchuk, N. F. (1999). Copyright protection for the electronic distribution of text documents. *Proceedings of the IEEE*, 87(7):1181–1196.

Brassil, J. T., Low, S., Maxemchuk, N. F., and O'Gorman, L. (1994). Marking text features of document images to deter illicit dissemination. In *Proceedings of the 12th IAPR International Conference on Pattern Recognition, Vol. 3-Conference C: Signal Processing (Cat. No. 94CH3440-5)*, volume 2, pages 315–319. IEEE.

Candès, E. J. and Donoho, D. L. (2004). New tight frames of curvelets and optimal representations of objects with piecewise c2 singularities. *Communications on Pure and Applied Mathematics: A Journal Issued by the Courant Institute of Mathematical Sciences*, 57(2):219–266.

Chaubey, P. and Singhadia, A. (2015). An art to protect originality of digital data: Digital watermarking. *Int. J. Sci. Res. Eng. Trends*, 1(6):112–115.

Chen, J., Yang, F., Ma, H., and Lu, Q. (2016). Text watermarking algorithm based on semantic role labeling. In *2016 Third International Conference on Digital Information Processing, Data Mining, and Wireless Communications (DIPDMWC)*, pages 117–120. IEEE.

Chen, M., Wong, E. K., Memon, N. D., and Adams, S. F. (2001). Recent developments in document image watermarking and data hiding. In *Multimedia Systems and Applications IV*, volume 4518, pages 166–176. International Society for Optics and Photonics.

Chetan, K. and Nirmala, S. (2015). An efficient and secure robust watermarking scheme for document images using integer wavelets and block coding of binary watermarks. *Journal of Information Security and Applications*, 24:13–24.

Chia, W. C., Teh, P. L., and Gill, C. M. H. D. (2018). Text extraction and categorization from watermark scientific document in bulk. In *2018 3rd International Conference on Computational Intelligence and Applications (ICCIA)*, pages 47–51. IEEE.

Chotikakamthorn, N. (1999). Document image data hiding technique using character spacing width sequence coding. In *Proceedings 1999 International Conference on Image Processing (Cat. 99CH36348)*, volume 2, pages 250–254. IEEE.

Cu, V. L., Burie, J.-C., and Ogier, J.-M. (2018). Watermarking for security issue of handwritten documents with fully convolutional networks. In *2018 16th International Conference on Frontiers in Handwriting Recognition (ICFHR)*, pages 303–308. IEEE.

Dang, Q. B., Louisa, K., Coustaty, M., Luqman, M. M., and Ogier, J.-M. (2019). A blind document image watermarking approach based on discrete wavelet transform and qr code embedding. In *2019 International Conference on Document Analysis and Recognition Workshops (ICDARW)*, volume 8, pages 1–6. IEEE.

Daraee, F. and Mozaffari, S. (2014). Watermarking in binary document images using fractal codes. *Pattern Recognition Letters*, 35:120–129.

Daubechies, I. and Sweldens, W. (1998). Factoring wavelet transforms into lifting steps. *Journal of Fourier analysis and applications*, 4(3):247–269.

Davarzani, R. and Yaghmaie, K. (2009). Farsi text watermarking based on character coding. In *2009 International Conference on Signal Processing Systems*, pages 152–156. IEEE.

Fei, W. and Tang, X. (2011). A chinese text watermark algorithm based on polyphone. In *Proceedings of 2011 Cross Strait Quad-Regional Radio Science and Wireless Technology Conference*, volume 2, pages 1215–1218. IEEE.

Feng, G. and Huang, X. (2012). An improved dct based zero-watermarking algorithm for text image. In *Anti-counterfeiting, Security, and Identification*, pages 1–4. IEEE.

Ghilan, M. M., Ba-Alwi, F. M., and Al-Wesabi, F. N. (2014). Combined markov model and zero watermarking techniques to enhance content authentication of english text documents. *International Journal of Computational Linguistics Research*, 5(1):26–42.

Gokhale, U. and Joshi, Y. (2012). A semi fragile watermarking algorithm based on svd-iwt for image authentication. *International Journal of Advanced Research in Computer and Communication Engineering*, 1(4):217–222.

González-Lee, M., Nakano-Miyatake, M., Pérez-Meana, H., and Sanchez-Perez, G. (2015). Script format document authentication scheme based on watermarking techniques. *Journal of applied research and technology*, 13(3):435–442.

Gonzalez-Lee, M., Santiago-Avila, C., Nakano-Miyatake, M., and Perez-Meana, H. (2009). Watermarking based document authentication in script format. In *2009 52nd IEEE International Midwest Symposium on Circuits and Systems*, pages 837–841. IEEE.

Gort, M. L. P., Olliaro, M., Cortesi, A., and Uribe, C. F. (2020). Semantic-driven watermarking of relational textual databases. *Expert Systems with Applications*, page 114013.

Gutub, A. A.-A., Al-Haidari, F., Al-Kahsah, K. M., and Hamodi, J. (2010). e-text watermarking: utilizing'kashida'extensions in arabic language electronic writing. *Journal of Emerging Technologies in Web Intelligence*, 2(1):48–55.

He, L., Zhang, L., Ma, G., Fang, D., and Gui, X. (2009). A part-of-speeach tag sequence text zero-watermarking. In *Proceedings. The 2009 International Symposium on Computer Science and Computational Technology (ISCSCI 2009)*, page 187. Citeseer.

Huang, D. and Yan, H. (2001). Interword distance changes represented by sine waves for watermarking text images. *IEEE Transactions on Circuits and Systems for Video Technology*, 11(12):1237–1245.

Huang, K., Tian, X., Yu, H., Yu, M., and Yin, A. (2019). A high capacity watermarking technique for the printed document. *Electronics*, 8(12):1403.

Hussain, A. J., Al-Jumeily, D., Radi, N., and Lisboa, P. (2015). Hybrid neural network predictive-wavelet image compression system. *Neurocomputing*, 151:975–984.

Jalil, Z., Aziz, H., Shahid, S. B., Arif, M., and Mirza, A. M. (2010a). A zero text watermarking algorithm based on non-vowel ascii characters. In *2010 International Conference on Educational and Information Technology*, volume 2, pages V2–503. IEEE.

Jalil, Z., Jaffar, M. A., and Mirza, A. M. (2011). A novel text watermarking algorithm using image watermark. *International Journal of Innovative Computing, Information and Control*, 7(3).

Jalil, Z. and Mirza, A. M. (2010). Text watermarking using combined image-plus-text watermark. In *2010 Second International Workshop on Education Technology and Computer Science*, volume 1, pages 11–14. IEEE.

Jalil, Z. and Mirza, A. M. (2013). A robust zero-watermarking algorithm for copyright protection of text documents. *Journal of the Chinese Institute of Engineers*, 36(2):180–189.

Jalil, Z., Mirza, A. M., and Jabeen, H. (2010b). Word length based zero-watermarking algorithm for tamper detection in text documents. In *2010 2nd International Conference on Computer Engineering and Technology*, volume 6, pages V6–378. IEEE.

Jalil, Z., Mirza, A. M., and Sabir, M. (2010c). Content based zero-watermarking algorithm for authentication of text documents. *arXiv preprint arXiv:1003.1796*.

Jane, O., Elbaşi, E., et al. (2014). Hybrid non-blind watermarking based on dwt and svd. *Journal of applied research and technology*, 12(4):750–761.

Jaseena, K. and John, A. (2011). Text watermarking using combined image and text for authentication and protection. *International Journal of Computer Applications*, 20(4):8–13.

Jiansheng, M., Sukang, L., and Xiaomei, T. (2009). A digital watermarking algorithm based on dct and dwt. In *Proceedings. The 2009 International Symposium on Web Information Systems and Applications (WISA 2009)*, page 104. Citeseer.

Kamaruddin, N. S., Kamsin, A., and Hakak, S. (2017). Associated diacritical watermarking approach to protect sensitive arabic digital texts. In *AIP Conference Proceedings*, volume 1891, page 020074. AIP Publishing LLC.

Khadam, U., Iqbal, M. M., Azam, M. A., Khalid, S., Rho, S., and Chilamkurti, N. (2019). Digital watermarking technique for text document protection using data mining analysis. *IEEE Access*, 7:64955–64965.

Khan, A., Khanam, M., Bashir, S., Khiyal, M. S. H., Iqbal, A., and Khan, F. H. (2011). Entropy based data hiding in binary document images. *International Journal of Computer and Electrical Engineering*, 3(4):503.

Kim, C. and Yang, C.-N. (2021). Self-embedding fragile watermarking scheme to detect image tampering using ambtc and opap approaches. *Applied Sciences*, 11(3):1146.

Kim, M.-Y. (2008). Text watermarking by syntactic analysis. In *Proc. of WSEAS International Conferences on Computers*, pages 904–909.

Kim, M.-Y. and Goebel, R. (2012). Adaptive-capacity and robust natural language watermarking for agglutinative languages. *Security and Communication Networks*, 5(3):301–310.

Kim, Y.-W. and Oh, I.-S. (2004). Watermarking text document images using edge direction histograms. *Pattern Recognition Letters*, 25(11):1243–1251.

Krishnamoorthy, R. and Punidha, R. (2012). An orthogonal polynomials transform-based variable block size adaptive vector quantisation for colour image coding. *IET image processing*, 6(6):635–646.

Kumar, J., Ye, P., and Doermann, D. (2013). A dataset for quality assessment of camera captured document images. In *International Workshop on Camera-Based Document Analysis and Recognition*, pages 113–125. Springer.

Kurup, S., Sridhar, G., and Sridhar, V. (2007). Entropy based data hiding for document images. *International Journal of Computer and Information Engineering*, 1(11):3582–3585.

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):1097–1109.

Li, J., Mei, Z., and Zhang, T. (2020). A method for document image enhancement to improve template-based classification. In *Proceedings of the 2020 4th High Performance Computing and Cluster Technologies Conference & 2020 3rd International Conference on Big Data and Artificial Intelligence*, pages 87–91.

Li, J. and Wu, F. (2013). Robust watermarking for text images based on arnold scrambling and dwt-dft. In *Proceedings 2013 International Conference on Mechatronic Sciences, Electric Engineering and Computer (MEC)*, pages 1182–1186. IEEE.

Li, Q.-C. and Dong, Z.-H. (2008). Novel text watermarking algorithm based on chinese characters structure. In *2008 International Symposium on Computer Science and Computational Technology*, volume 2, pages 348–351. IEEE.

Lin, J.-Y., Chen, Y., Chang, C.-C., and Hu, Y.-C. (2019). Dual-image-based reversible data hiding scheme with integrity verification using exploiting modification direction. *Multimedia Tools and Applications*, 78(18):25855–25872.

Lin, S. D., Shie, S.-C., and Guo, J. Y. (2010). Improving the robustness of dct-based image watermarking against jpeg compression. *Computer Standards & Interfaces*, 32(1-2):54–60.

Lin, S. D. and Yang, Z.-L. (2011). Hierarchical fragile watermarking scheme for image authentication. *Intelligent Automation & Soft Computing*, 17(2):245–255.

Liu, Y., Zhu, Y., and Xin, G. (2015). A zero-watermarking algorithm based on merging features of sentences for chinese text. *Journal of the Chinese Institute of Engineers*, 38(3):391–398.

Loc, C. V., Burie, J.-C., and Ogier, J.-M. (2018). Stable regions and object fill-based approach for document images watermarking. In *2018 13th IAPR International Workshop on Document Analysis Systems (DAS)*, pages 181–186. IEEE.

Lou, M. and Liu, J. (2012). Watermarking text document based on structure and semantic of chinese characters. In *Proc. 7th Int. Conf. Syst. Eng.*, pages 866–869.

Low, S. H., Maxemchuk, N. F., and Lapone, A. M. (1998). Document identification for copyright protection using centroid detection. *IEEE Transactions on Communications*, 46(3):372–383.

Lu, H., Kot, A. C., and Cheng, J. (2003). Secure data hiding in binary document images for authentication. In *Proceedings of the 2003 International Symposium on Circuits and Systems, 2003. ISCAS'03.*, volume 3, pages III–III. IEEE.

Lu, H., Kot, A. C., and Shi, Y. Q. (2004). Distance-reciprocal distortion measure for binary document images. *IEEE Signal Processing Letters*, 11(2):228–231.

Lu, H., Shi, X., Shi, Y. Q., Kot, A. C., and Chen, L. (2002). Watermark embedding in dc components of dct for binary images. In *2002 IEEE Workshop on Multimedia Signal Processing.*, pages 300–303. IEEE.

Makbol, N. M. and Khoo, B. E. (2014). A new robust and secure digital image watermarking scheme based on the integer wavelet transform and singular value decomposition. *Digital Signal Processing*, 33:134–147.

Maxemchuk, N. F. and Low, S. H. (1997). Marking text documents. In *ICIP (3)*, page 13. Citeseer.

Meng, Y., Gao, L., Liu, M., and Bai, L. (2012). Chinese text zero-watermark based on three-dimensional space model. *JCP*, 7(8):2063–2070.

Meng, Y., Gao, L., Wang, X., and Guo, T. (2011). Chinese text zero-watermark based on space model. In *2011 3rd International Workshop on Intelligent Systems and Applications*, pages 1–5. IEEE.

Meng, Y., Guo, T., Guo, Z., and Gao, L. (2010). Chinese text zero-watermark based on sentence's entropy. In *2010 International Conference on Multimedia Technology*, pages 1–4. IEEE.

Meral, H. M., Sankur, B., Özsoy, A. S., Güngör, T., and Sevinç, E. (2009). Natural language watermarking via morphosyntactic alterations. *Computer Speech & Language*, 23(1):107–125.

Meral, H. M., Sevinc, E., Ünkar, E., Sankur, B., Özsoy, A. S., and Güngör, T. (2007). Syntactic tools for text watermarking. In *Security, Steganography, and Watermarking of Multimedia Contents IX*, volume 6505, page 65050X. International Society for Optics and Photonics.

Mir, N. (2011). Zero watermarking for text on www using semantic approach. In *International Conference on Software Engineering and Computer Systems*, pages 306–316. Springer.

Mohammadi, S. (2015). A semi-blind watermarking algorithm for color images using chaotic maps. In *2015 2nd International Conference on Knowledge-Based Engineering and Innovation (KBEI)*, pages 106–110. IEEE.

Mukherjee, S. and Pal, A. K. (2012). A dct-svd based robust watermarking scheme for grayscale image. In *Proceedings of the international conference on advances in computing, communications and informatics*, pages 573–578.

Naqvi, N., Abbasi, A. T., Hussain, R., Khan, M. A., and Ahmad, B. (2018). Multilayer partially homomorphic encryption text steganography (mlphe-ts): a zero steganography approach. *Wireless Personal Communications*, 103(2):1563–1585.

Panah, A. S., Van Schyndel, R., Sellis, T., and Bertino, E. (2016). On the properties of non-media digital watermarking: a review of state of the art techniques. *IEEE Access*, 4:2670–2704.

Patiburn, S. A., Iranmanesh, V., and Teh, P. L. (2017). Text steganography using daily emotions monitoring. *International Journal of Education and Management Engineering*, 7(3):1.

Por, L. Y., Wong, K., and Chee, K. O. (2012). Unispach: A text-based data hiding method using unicode space characters. *Journal of Systems and Software*, 85(5):1075–1082.

Qadir, M. A. and Ahmad, I. (2005). Digital text watermarking: Secure content delivery and data hiding in digital documents. In *Proceedings 39th Annual 2005 International Carnahan Conference on Security Technology*, pages 101–104. IEEE.

Qi, X. and Liu, Y. (2013). Cloud model based zero-watermarking algorithm for authentication of text document. In *2013 Ninth International Conference on Computational Intelligence and Security*, pages 712–715. IEEE.

Rakhmawati, L., Rochmawati, N., Ismayati, E., et al. (2018). Fragile watermarking technique using a linear block mapping for document image authentication with recovery capability. In *2018 International Seminar on Research of Information Technology and Intelligent Systems (ISRITI)*, pages 518–521. IEEE.

Rizzo, S. G., Bertini, F., and Montesi, D. (2016). Content-preserving text watermarking through unicode homoglyph substitution. In *Proceedings of the 20th International Database Engineering & Applications Symposium*, pages 97–104.

Rizzo, S. G., Bertini, F., and Montesi, D. (2019). Fine-grain watermarking for intellectual property protection. *EURASIP Journal on Information Security*, 2019(1):1–20.

Rizzo, S. G., Bertini, F., Montesi, D., and Stomeo, C. (2017). Text watermarking in social media. In *Proceedings of the 2017 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining 2017*, pages 208–211.

Roy, S. S., Basu, A., and Chattopadhyay, A. (2020). On the implementation of a copyright protection scheme using digital image watermarking. *Multimedia Tools and Applications*, pages 1–14.

Rui, X., XiaoJun, C., and Jinqiao, S. (2013). A multiple watermarking algorithm for texts mixed chinese and english. *Procedia Computer Science*, 17:844–851.

Saba, T., Bashardoost, M., Kolivand, H., Rahim, M. S. M., Rehman, A., and Khan, M. A. (2020). Enhancing fragility of zero-based text watermarking utilizing effective characters list. *Multimedia Tools and Applications*, 79(1):341–354.

Salameh, H. B., Almajali, S., Ayyash, M., and Elgala, H. (2018). Securing delay-sensitive cognitive radio iot communications under reactive jamming attacks: Spectrum assignment perspective. In *2018 Fifth International Conference on Software Defined Systems (SDS)*, pages 20–24. IEEE.

Shivananda, N. et al. (2014). A new fragile watermarking approach for tamper detection and recovery of document images. In *2014 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, pages 1494–1498. IEEE.

Singh, A. K., Dave, M., and Mohan, A. (2013). A hybrid algorithm for image watermarking against signal processing attacks. In *International Workshop on Multi-disciplinary Trends in Artificial Intelligence*, pages 235–246. Springer.

Singh, A. K., Thakur, S., Jolfaei, A., Srivastava, G., Elhoseny, M., and Mohan, A. (2021). Joint encryption and compression-based watermarking technique for security of digital documents. *ACM Transactions on Internet Technology (TOIT)*, 21(1):1–20.

Singh, P., Raman, B., and Roy, P. P. (2018). Detection of seal and signature entities with hierarchical recovery based on watermark self embedding in tampered digital documents. *Displays*, 54:47–59.

Sweldens, W. (1998). The lifting scheme: A construction of second generation wavelets. *SIAM journal on mathematical analysis*, 29(2):511–546.

Tayan, O., Alginahi, Y. M., and Kabir, M. N. (2013). An adaptive zero-watermarking approach for text documents protection. In *International Conference on Advances in Computer and Information Technology*.

Tayan, O., Kabir, M. N., and Alginahi, Y. M. (2014). A hybrid digital-signature and zero-watermarking approach for authentication and protection of sensitive electronic documents. *The Scientific World Journal*, 2014.

Tirandaz, H., Davarzani, R., Monemizadeh, M., and Haddadnia, J. (2009). Invisible and high capacity data hiding in binary text images based on use of edge pixels. In *2009 International Conference on Signal Processing Systems*, pages 130–134. IEEE.

Topkara, M., Taskiran, C. M., and Delp III, E. J. (2005). Natural language watermarking. In *Security, Steganography, and Watermarking of Multimedia Contents VII*, volume 5681, pages 441–452. International Society for Optics and Photonics.

Upadhyay, P. and Chhabra, J. K. (2021). Multilevel thresholding based image segmentation using new multistage hybrid optimization algorithm. *Journal of Ambient Intelligence and Humanized Computing*, 12(1):1081–1098.

Vybornova, O. and Macq, B. (2007). A method of text watermarking using presuppositions. In *Security, Steganography, and Watermarking of Multimedia Contents IX*, volume 6505, page 65051R. International Society for Optics and Photonics.

Wang, C.-C., Chang, Y.-F., Chang, C.-C., Jan, J.-K., and Lin, C.-C. (2014). A high capacity data hiding scheme for binary images based on block patterns. *Journal of Systems and Software*, 93:152–162.

Wang, H., Sun, X., Liu, Y., and Liu, Y. (2008). Natural language watermarking using chinese syntactic transformations. *Information Technology Journal*, 7(6):904–910.

Wen, Q., Sun, T.-F., and Wang, S.-X. (2003). Concept and application of zero-watermark. *Acta Electronica Sinica*, 31(2):214–216.

Wu, F., Huang, M., and Li, J. (2015). Robust watermarking for text images based on arnold scrambling and dwt-dct. In *2015 International Conference on Mechatronics, Electronic, Industrial and Control Engineering (MEIC 2015), Shenyang, China*, pages 568–572. Citeseer.

Wu, M. and Liu, B. (2004). Data hiding in binary image for authentication and annotation. *IEEE transactions on multimedia*, 6(4):528–538.

Yang, H. and Kot, A. C. (2007). Pattern-based data hiding for binary image authentication by connectivity-preserving. *IEEE Transactions on Multimedia*, 9(3):475–486.

Yang, H., Kot, A. C., and Liu, J. (2005). Semi-fragile watermarking for text document images authentication. In *2005 IEEE international symposium on circuits and systems*, pages 4002–4005. IEEE.

Yazdani, H., Doostari, M., and Yazdani, V. (2013). A new method to persian text watermarking using curvaceous letters. *Journal of Basic and Applied Scientific Research*, 3(4).

Yingjie, M., Xianlong, W., Wenjun, L., and Wei, C. (2013). Text zero-watermark based on chinese edit distance. In *2013 International Conference on Computational and Information Sciences*, pages 686–689. IEEE.

Yuwei, Y. and Su, Y. (2020). A two-dimensional code security authentication method based on digital watermarking. In *Proceedings of the 2nd International Conference on Industrial Control Network And System Engineering Research*, pages 94–99.

Zhang, J., Li, Y., Niu, S., Cao, Z., and Wang, X. (2019). Improved fully convolutional network for digital image region forgery detection. *CMC-Computers Materials & Continua*, 60(1):287–303.

Zhang, S., Wu, Y., Li, Q., and Li, G. (2017). Pdf document watermarking algorithm based on discarded page object. In *2017 13th International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery (ICNC-FSKD)*, pages 3107–3111. IEEE.

Zhao, W., Guan, H., Huang, Y., and Zhang, S. (2020). Research on double watermarking algorithm based on pdf document structure. In *2020 International Conference on Culture-oriented Science & Technology (ICCST)*, pages 298–303. IEEE.

Zhao, X., Ho, A. T., and Shi, Y. Q. (2010). Image forensics using generalised benford's law for improving image authentication detection rates in semi-fragile watermarking. *International Journal of Digital Crime and Forensics (IJDCF)*, 2(2):1–20.

Zhou, X., Wang, S., Zhao, W., and Peng, R. (2009). A semi-fragile watermarking scheme for content authentication of chinese text documents. In *2009 2nd IEEE International Conference on Computer Science and Information Technology*, pages 439–443. IEEE.

Zhu, B., Wu, J., and Kankanhalli, M. S. (2006). Render sequence encoding for document protection. *IEEE transactions on multimedia*, 9(1):16–24.

Zhu, P., Xiang, G., Song, W., Li, A., Zhang, Y., and Tao, R. (2016). A text zero-watermarking algorithm based on chinese phonetic alphabets. *Wuhan University Journal of Natural Sciences*, 21(4):277–282.

Zhu, X., Wen, L., and Chen, Y. (2012). Novel binary document image watermarking exploiting the features of double domains. *International Journal of Computer and Electrical Engineering*, 4(1):87–92.