

Ministry of Higher Education and Scientific Research

University of Babylon : College of Science for Girls

Computer Department : fourth stage



Image Watermarking as authentication technique

*A research submitted to the Department of Computer
Science at the College of Science for Girls at the University
of Babylon as part of the requirements for obtaining a
bachelor's degree
.in computer science*

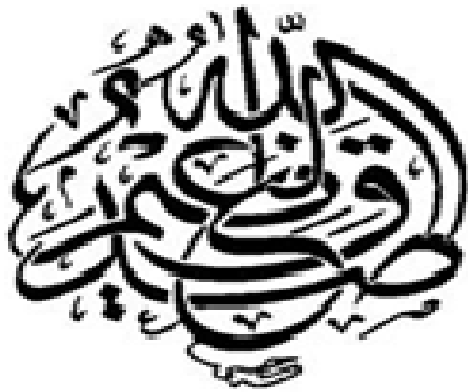
By :- shamam Falih Hassan

Supervised by :- zanab falah

2024-2023



فبدأ بأوامرهم قبل وهاء أخيه ثم استخرجها من وهاء أخيه
كذلك كدنا ليوسف ما كان ليأخذ أخاه في دين
الملك إلا أن يشاء الله نرفع درجات من نشاء وفوق كل
ذي علم علیم



إقرار المشرف

اشهد ان هذا المشروع

(*Image Watermarking as authentication technique*) قد جرى تحت
اشرافي في قسم علوم الحاسوب في كلية العلوم للبنات/جامعة بابل كجزء من متطلبات نيل
شهادة البكالوريوس في علوم الحاسوب من قبل الطالبة المرحلة الرابعة (شمم فالح حسن)

توقيع المشرف

اسم المشرف:

المرتبة العلمية:

التاريخ | | 2024

CONTENTS

<i>Acknowledgments</i>	<i>I</i>
<i>Abstract</i>	<i>II</i>
<i>Contents</i>	<i>III</i>
<i>Table of figures</i>	<i>IV</i>

Chapter one: Overview

<i>1.1 Introduction</i>	<i>2</i>
<i>1.2 Related Works</i>	<i>3</i>
<i>1.3 Aims of watermarking</i>	<i>4</i>
<i>1.4 Work Layout</i>	<i>4</i>

Chapter Two: theoretical part

<i>2.1 Introduction</i>	<i>6</i>
<i>2.2 important properties of digital watermarking</i>	<i>6</i>
<i>2.3 the types of digital watermarking</i>	<i>7</i>
<i>2.4 techniques for watermarking</i>	<i>8</i>
<i>2.4.1 DCT techniques</i>	<i>9</i>
<i>2.4.2 DWT techniques</i>	<i>10</i>
<i>2.5 digital watermarking Applications</i>	<i>11</i>

Chapter Three :Proposed Method

<i>3.1 Introduction</i>	<i>14</i>
<i>3.2 Proposed Method</i>	<i>14</i>
<i>3.2.1 DCT Application image</i>	<i>15</i>
<i>3.2.2 Hiding Method</i>	<i>15</i>

3.2.3 Evaluation of Hiding operation.....	16
3.2.4 Retrieval of image.....	16
3.2.5 Attacks processes	16
3.3 RESULTS.....	16

Chapter Four: Conclusions and future works

4.1 Conclusions.....	20
4.2 Future Works.....	20
References.....	21

Table of Figures

<i>Figure no.</i>	<i>Figure Address</i>	<i>Figure pag.</i>
	<i>CHAPTER THREE</i>	
3.1	Watermarking of image with alpha=0.3.	17
3.2	Watermarking of image with Gaussian attack.	18

الاهـداء

الى من جرع الكأس فارغ ليسقيني قطرة حب

الى من كلت انامله ليقدم لنا لحظة سعادة

الى من حصد الاشوك عن دربي ليمهد لي طريق العلم الى القلب الكبير

والدي العزيز.....

الى من ارضعتني الحب والحنان

الى رمز الحب وبلسم الشفاء

الى القلب الناصع بالبياض

الى من كان دعائها سر نجاحي وحنانها بلسم جراحي اغلى الحبايب ملاكي

والتفاني بسمة الحياة وسر الوجود بكى اكبر وعليك في الحياة معنى الحب

اعتمد يا شمعة متقدة تنير ظلمة حياتي بوجودك اكتسب قوه ومحبه لا

حدود لها

حبيبتى الغالية والدتي الحبيبه.....

الى الروح التي سكنت روحي

زوجي الغالي.....

الى القلوب الطاهرة الرقيقه والنفوس البريئة

الى رياحين حياتي

اخوتي.....

شكر وتقدير

الحمد لله رب العالمين خالق السماوات والأرضين والسلاة والسلام على خير خلق الله محمد رسول الله وعلى اله الطيبين الطاهرين ونحمد الله ونشكره

لتوفيقنا في انجاز هذا المشروع.

وأقدم بجزيل الشكر لأولئك المخلصين الذين لو بألوجهدنا في مساعدتنا

في مجال البحث العلمي ، وخص بالذكر الاستاذة الفاضلة زينب فلاح

ساحبة الفضل الكبير في توجيهنا ومساعدتنا في تجميع المادة البحثية

فجزاها الله خير الجزاء .

وكذلك أتقدم بالشكر الجزيل الى رئاسة قسم الحاسبات وأقدم شكري الى

كل من ساندني ولو بكلمة طيبة.

ومن الله التوفيق

Abstract:

In today's digital era, ensuring the authenticity and integrity of digital images has become a crucial aspect of various applications, such as copyright protection and forensic analysis. Among the numerous techniques available, watermarking has emerged as a popular method for embedding imperceptible information into images to authenticate their origin and deter unauthorized tampering.

This paper explores the application of watermarking images as an authentication method, with a focus on utilizing the Discrete Cosine Transform (DCT) shared with hiding method. The DCT is a widely adopted technique in image processing, known for its ability to convert image data into a frequency domain representation. By leverage the properties of DCT, watermarking can be achieved by embedding unique identification data within the image without significantly altering its visual quality.

The proposed approach involves several key steps. First, the original image is divided into non-overlapping blocks, and the DCT is applied to each block independently. The resulting DCT coefficients are then modified to embed the watermark information, while ensuring minimal perceptual distortion.

To evaluate the effectiveness of the proposed method, experiments are conducted on various image datasets, considering factors such as watermark invisibility and robustness against common attacks. The results demonstrate that watermarking using DCT-based techniques offers a promising solution for image authentication, providing a balance between imperceptibility and robustness.

Chapter one

Overview

1.1 Introduction:

Watermarking is the practice of imperceptibly altering a piece of data in order to embed information about the data. According to the definition there are two important characteristics of watermarking. First, information embedding should not cause perceptible changes to the host medium. Second, the message should be related to the host medium. In this sense, the [watermarking techniques](#) form a subset of information hiding techniques, which also include cases where the hidden information is not related to the host medium. This chapter reviews the main application domains of watermarking [1].

Watermarks have played an important role in the government, adding identifiers to stamps, money, and documents to avoid counterfeiting or fabrication. In the digital world, watermarks have also helped in licenses and ownership of media such as photos, audios, and videos. For common folks like us, watermarks also help identify information to come across each reader. For instance, if you have an article that is not finished yet but you want your friends or teachers to read it to gather insights, then you can label it with a watermark stating the word “Draft.”[2]

The watermark also evolved as technology improved. From paper, watermarks can now be found to various creations such as audio, images, documents and digital files. These days, watermarks are not just shadowing anymore at the back of the text printed on paper. It could be a hidden code, encryption, an obvious mark, a unique print or even a digital insert. Let’s look into the different types:

1. Physical Watermarks

Physical or traditional watermarks are those marks that we’ve all known and loved for years. It has evolved from wet paper markings to printing. These visible marks are printed or applied in light shades and can vary on conveyed light.

2. Audio Watermarks

Unlike documents, audios cannot be soaked in water and be printed with labels. Audios are marked with signals and codes, that becomes its identifier to show the author's ownership.

3. Digital Watermarks

A mark, a stamp or an identifier, a digital watermark is an embed on a signal that identifies the owner or the author. It can be placed on audio, video or image.[2].

Digital watermarking technology is being adopted to ensure and facilitate data authentication, security and copyright protection of digital media. It is considered as the most important technology in today's world, to prevent illegal copying of data. Digital watermarking can be applied to audio, video, text or images.[3]

1.2 Related work

Hewe Majeed Zangana , This researcher used the technique of least significant bit (LSB) in watermarking. The results show us that the system is working well and the security of the image is really good[4]

Abdullah Bamatraf, Rosziati Ibrahim and Mohd. Najib Mohd. Salleh This researcher In this reserch, introduce a new digital watermarking algorithm using least significant bit (LSB). LSB is used because of its little effect on the image. This new algorithm is using LSB by inversing the binary values of the watermark text and shifting the watermark according to the odd or even number of pixel coordinates of image before embedding the watermark. [5]

Rajni Verma1 and Archana Tiwari assumed new digital watermarking algorithm using least significant bit (LSB). LSB is used because of its little

effect on the image. This new algorithm is using the third and the fourth least significant bits (LSB) technique and shifting the watermark of pixel coordinates of image before embedding the watermark. The proposed algorithm is flexible depending on the length of the watermark text[6]

1.3 Aim of watermarking

Watermarking is play an important role in scientific research and commercial application, this work provide a method for Watermarking.

One of the most popular interests for Watermarking is authentication and protect of copyrights where many techniques are employed for this purpose, the popular one is least significant bit. The improvement of authentication for watermarking can based on Discrete Cosine Transform that proposed here.

1.4 Work Layout

Chapter Two:

In this chapter, some of the most important applications of digital watermarking are presented , explain some key properties that are desirable in a watermarking system, and give an overview of the most common models of watermarking and explain some of steganography methods, Image definition additional to Performance Evaluation Metric (PSNR , DCT Algorithm).

Chapter Three:

A digital watermark is used to hide information within a signal that cannot be easily by the third party. One of its applications is the image. Digital watermark includes two main operations, watermark embedding and watermark extraction, which will be explained in this chapter as well as watermark attacks operations.

Chapter Four:

This chapter includes the conclusions and what can be done in the future.

Chapter Two

Theoretical Part

2.1 Introduction

A digital watermark is an identification code, permanently embedded into digital data, carrying information on copyright protection and data authentication

The term digital watermarking was first appeared in 1993, when Tirkel presented two watermarking techniques to hide the watermark data in the images [7]. A digital watermark is a digital signal or pattern inserted into a digital image. Since this signal or pattern is present in each unaltered copy of the original image, the digital watermark may also serve as a digital signature for the copies. A given watermark may be unique to each copy (e.g. to identify the intended recipient), or be common to multiple copies (e.g. to identify the document source). In either case, the watermarking of the document involves the transformation of the original into another form. Digital watermarking can also be contrasted with public-key encryption, which also transforms original files into another form. It is a common practice nowadays to encrypt digital documents so that they become unviewable without the decryption key. Unlike encryption, however, digital watermarking leaves the original image or file basically intact and recognizable. In addition, digital watermarks, as signatures, may not be validated without special software.

2.2 Important Properties of Digital watermarking

Ideal properties of a digital watermark have been stated as follows:[7,8,9]

- **Robustness:** The watermark should be reliably detectable after alterations to the marked documents [10]. Robustness means that it must be difficult (ideally impossible) to defeat a watermark without degrading the marked document

severely—so severely that the document is no longer useful or has no (commercial) value.

- **Imperceptibility or a low degree of obtrusiveness:** To preserve the quality of the marked document, the watermark should not noticeably distort the original document. Ideally, the original and marked documents should be perceptually identical.

- **Security:** Unauthorized parties should not be able to read or alter the watermark. Ideally, the watermark should not even be detectable by unauthorized parties.

- **Multiple watermarks:** It may also be desirable to embed multiple watermarks in a document. For example, an image might be marked with a unique watermark each time it is downloaded.

2.3 The Types of Digital Watermarking

The two types of digital watermarks are distinguished by their visibility to the casual viewer.

- Visible watermarks is done to mark the paper manufacturer or paper type. One might view digitally watermarked documents and images as digitally "stamped".

- Invisible watermarks, on the other hand, are potentially useful as a means of identifying the source, author, creator, owner, and distributor or authorized consumer of a document or image. For this purpose, the objective is to permanently and unalterably mark the image so that the credit or assignment is beyond dispute.

Visible and invisible watermarks both serve to deter theft but they do so in very different ways. Visible watermarks are especially useful for conveying an

immediate claim of ownership. The main advantage of visible watermarks, in principle at least, is that they virtually eliminate the commercial value of the document to a would-be thief without lessening the document's utility for legitimate, authorized purposes. A familiar example of a visible watermark is in the video domain where CNN and other television networks place their translucent logo at the bottom right of the screen image. Invisible watermarks, on the other hand, are more of an aid in catching the thief than discouraging the theft in the first place.

2.4 Techniques for Watermarking

Several different methods enable watermarking in the spatial domain [13]. The simplest (too simple for many applications) is to just flip the lowest-order bit of chosen pixels in a grey scale or color image. This will work well only if the image is subjected to any human or noisy modification. A more robust watermark can be embedded in an image in the same way that a watermark is added to paper. Such techniques may superimpose a watermark symbol over an area of the picture and then add some fixed intensity value for the watermark to the varied pixel values of the image. One disadvantage of spatial domain watermarks is that picture cropping (a common operation of image editors) can be used to eliminate the watermark.

2.4.1 DCT Technique:

Image fusion using the Discrete Cosine Transform (DCT) is a well-established technique in computer vision and image processing. It involves combining multiple images by utilizing the frequency domain representation provided by the DCT, resulting in a composite image that contains enhanced information[14]. The DCT is a widely used transform for converting images from the spatial domain to the frequency domain, enabling effective analysis and manipulation of image data .The problem

statement loss of spatial details is a significant concern in image fusion based on DCT. The use of DCT-based fusion methods often leads to a reduction in fine spatial information since the focus of the transform is on frequency representation rather than preserving precise spatial details. As a result, the quality and accuracy of the fused image can be adversely affected. Another issue pertains to the inadequate representation of relevant features. DCT may not sufficiently capture and represent all the essential features necessary for fusion, such as edges or textures. This limitation can result in suboptimal fusion outcomes and an insufficient preservation of accurate features in the fused image[15]. Image fusion has diverse applications in remote sensing, medical imaging, surveillance, and multimedia, aiming to improve the quality, clarity, and interpretability of the resulting composite image[16]. By integrating complementary information from input images, image fusion enables a more comprehensive representation of the scene or object of interest[17].

The fusion process relies on the DCT and involves several essential steps.

First, the input images undergo preprocessing to eliminate noise, correct distortions, and enhance overall quality. Then, the DCT transformation is applied to each input image, converting them to the frequency domain. This transformation represents the images as a collection of DCT coefficients, highlighting the various frequency components present. To achieve fusion, a fusion rule is applied to the DCT coefficients of the input images, determining how they are combined to generate fused coefficients. Different fusion strategies can be employed, such as weighted averaging, maximum coefficient selection, or other algorithms tailored to specific requirements.

Finally, the fused coefficients are inverse transformed using the inverse DCT, resulting in the final fused image in the spatial domain[18].

2.4.2 DWT Technique

With the increasing use of multimedia technologies, image compression requires higher performance. To address needs and requirements of multimedia and internet applications, many efficient image compression techniques, with considerably different features, have been developed [19]. Traditionally, image compression adopts discrete cosine transform (DCT) in most situations which possess the characteristics of simpleness and practicality. DCT has been applied successfully in the standard of JPEG, MPEGZ, etc. However, the compression method that adopts DCT has several shortcomings that become increasing apparent. One of these shortcomings is obvious blocking artifact and bad subjective quality when the images are restored by this method at the high compression ratios [20]. In recent years, many studies have been made on wavelets. An excellent overview of what wavelets have brought to the fields as diverse as biomedical applications, wireless communications, computer graphics or turbulence. Image compression is one of the most visible applications of wavelets. The rapid increase in the range and use of electronic imaging justifies attention for systematic design of an image compression system and for providing the image quality needed in different applications [21]. In recent times, much of the research activities in image coding have been focused on the DWT, which has become a standard tool in image compression applications because of their data reduction capability. In a wavelet compression system, the entire image is transformed and compressed as a single data object rather than block by block as in a DCT-based compression system [22]. It allows a uniform distribution of compression error across the entire image. DWT offers adaptive spatial-frequency resolution (better spatial resolution at high frequencies and better frequency resolution at low frequencies) that is well suited to the properties of an HVS. It Signal & Image Processing : An International Journal(SIPIJ) Vol.1, No.2, December 2010 23

can provide better image quality than DCT, especially on a higher compression ratio [23]

2.5 Digital Watermarking Applications

1- Copyright protection: Digital watermarking can be used to identify and protect copyright ownership. Digital content can be embedded with watermarks depicting metadata identifying the copyright owners.

- Copy protection: Digital content can be watermarked to indicate that the digital content cannot be illegally replicated. Devices capable of replication can then detect such watermarks and prevent unauthorized replication of the content.

-Digital right management: Digital right management (DRM) can be defined as —the description, identification, trading, protecting, monitoring, and tracking of all forms of usages over tangible and intangible assets. It concerns the management of digital rights and the enforcement of rights digitally.

2- Tamper proofing: Digital watermarks which are fragile in nature, can be used for tamper proofing. Digital content can be embedded with fragile watermarks that get destroyed whenever any sort of modification is made to the content. Such watermarks can be used to authenticate the content.

3- Broadcast monitoring: Over the last few years, the number of television and radio channels delivering content has notably expanded. And the amount of content flowing through these media vehicles continues to grow exponentially. In this highly fragmented and fast changing market, knowing the real broadcast

reality has become critical for content owners, copyright holders, distributors and broadcasters.

4- Fingerprinting: Fingerprints are the characteristics of an object that tend to distinguish it from other small objects. As in the applications of copyright protection, the watermark for finger printing is used to trace authorized users who violate the license agreement and distribute the copyrighted material illegally. Thus, the information embedded in the content is usually about the customer such as customer's identification number.

5- Access control: Different payment entitles the users to have different privilege (play/copy control) on the object. It is desirable in some systems to have a copy and usage control mechanism to prevent illegal copy of the content or limit the number of times of copying. A robust watermark can be used for such purpose.

6-Medical application: Names of the patients can be printed on the X-ray reports and MRI scans using techniques of visible watermarking. The medical reports play a very important role in the treatment offered to the patient. If there is a mix up in the reports of two patients this could lead to a disaster[11].

7- Image and content authentication: In an image authentication application the intent is to detect modifications to the data. The characteristics of the image, such as its edges, are embedded and compared with the current images for differences. A solution to this problem could be borrowed from cryptography, where digital signature has been studied as a message authentication method. One example of digital signature technology being used for image authentication is the trustworthy digital camera[12].

Also, application can be included *Communication enhancement, Content protection for audio and video content* where modern digital format employed for sale or rental of commercial audio and video content to consumers-such as

DVD, BluRay Disc, and iTunes-incorporate content protection technologies that control access to and use of the content and limit its unauthorized copying and redistribution, and *Content filtering*.

Chapter Three

Proposed Method

3.1 Introduction

In the digital image, protecting creative works has become more important than ever. Whether you're a photographer, graphic designer, or artist, watermarking of images is a crucial step in safeguarding intellectual property. Watermarks not only serve as a means of identification, but they also act as a deterrent against unauthorized use and theft.

To achieve authenticity of image, in this work, the watermarking of images is employed using Discrete Cosine Transform (DCT) with hiding method. Where DCT is a widely used technique in image processing that allows us to transform an image from the spatial domain to the frequency domain. By applying DCT to an image, its frequency components can be manipulated and a watermark can be embedded in a way that is difficult to remove without degrading the image quality.

3.2 Proposed Method:

Watermarking of images is applied using DCT technique shared with hiding method. Rearranging cover and watermark images is used to hide data for watermark image into cover image. The DCT has a main role that is applied firstly on images. The steps of the proposed system consist of :

- 1- DCT application on images.
- 2- Hiding method.
- 3- Evaluation of Hiding Operation.
- 4- Retrieval of Image
- 5- Attacks processes.

3.2.1 DCT Application on images:

Step 1: Convert the Image to Grayscale

To simplify the watermarking process, it is common to convert the image to grayscale. This reduces the complexity of the algorithm and ensures that the watermark is applied uniformly across the image.

Step 2: Apply DCT on cover and watermark images:

For each block in the image, 4D_DCT is applied to obtain the frequency coefficients. This is done by taking the 4D_DCT of the block matrix. The resulting coefficients represent the frequency components of the block.

3.2.2 Hiding method:

Step 1: Embed the Watermark

Embedding process includes two operations:

- 1- The columns of watermark image rearrange in reverse before embed.
- 2- Odd columns of cover image is only used to embed rather than sequential order.
- 3- Ratio of each value (alpha) from watermark image that obtained from 1 is add to values of specified positions from cover image that obtained from 2.

Step 2: Inverse DCT

Once the watermark is embedded, the modified DCT coefficients back to the spatial domain. This is done by applying the inverse DCT.

3.2.3 Evaluation of Hiding Operation:

Peak Signal to Noise Ratio (PSNR) is used as a performance measure for evaluation the effect of watermarking operation. Also, the normalized correlation (NC) is used to evaluate the system.

3.2.4 Retrieval of Image:

The watermark image is retrieved using inverse steps of embedding that can listed as follows:

- 1- 4D _DCT application on watermarked image.
- 2- 4D_DCT application on cover image.
- 3- Get values of the odd column of DCT watermarked that have values of watermark
- 4- Reverse the column of the watermark image to obtain the valid order.
- 5- Subtract the ratio from values of watermarked image that obtained from 4 from cover image that obtained from 3.
- 6- Inverse DCT apply on the result

3.2.5 Attacks Processes:

The performance of the proposed method tests against many attacks. In general, different attacks are applied to the watermarked image such as salt& pepper noise, median, cropping, and Gaussian attacks

3.3 RESULTS:

The results of the proposed system for different ratios are shown in the figure 3.1 and 3.2. The size of cover image is 225*255 and watermark image is 80*60.

The results are shown that the method is effective in watermarking and extracting processes. In addition, the proposed method give efficient results with median and salt and pepper attacks while the result is good with Gaussian attack.

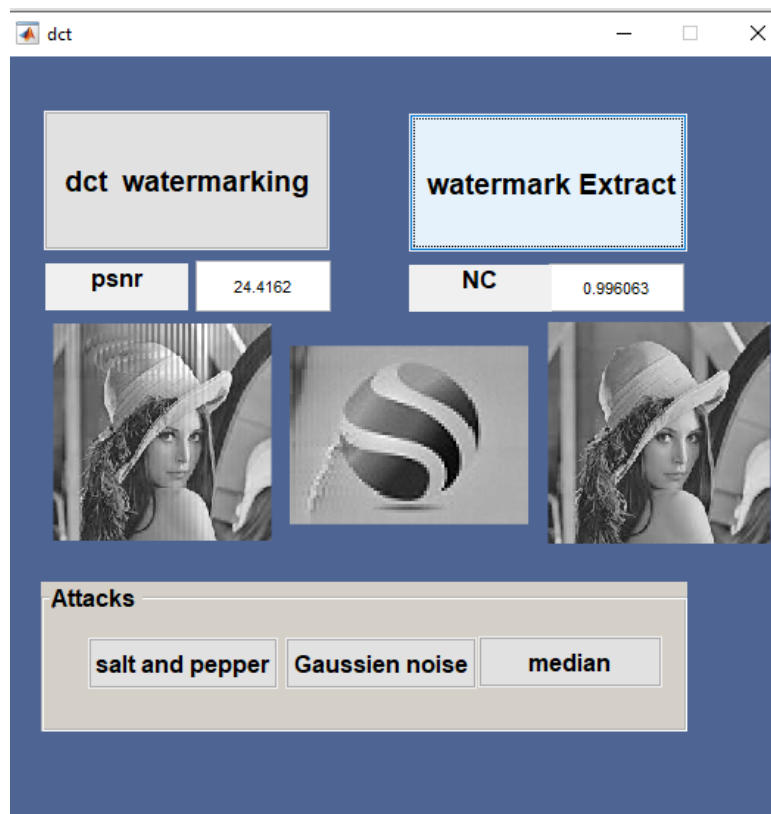


Fig. 3.1: Watermarking of image with $\alpha=0.3$.

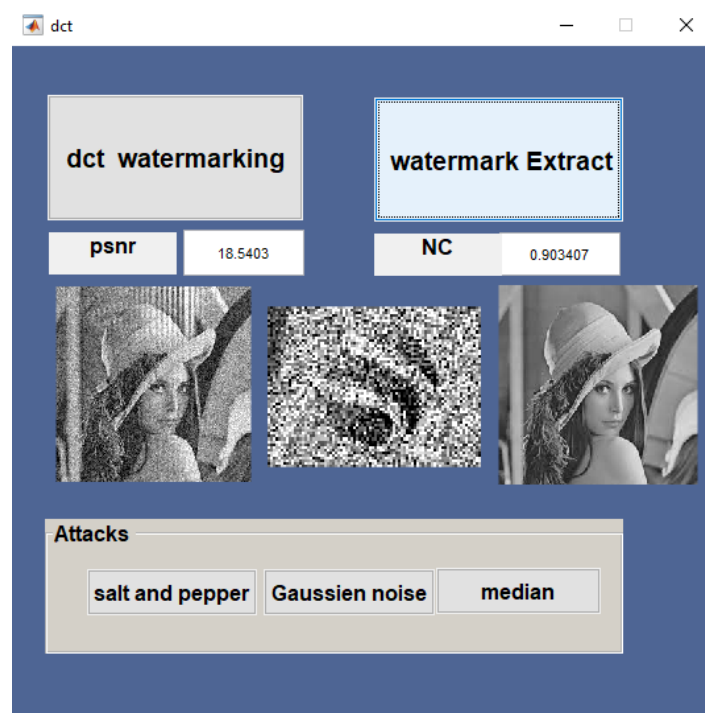


Fig. 3.2: Watermarking of image with Gaussian attack.

Table 3.1: The Proposed System Performance with different Inputs.

<i>Without attack</i>	<i>Ratio value</i>	<i>Performance(NC)</i>	<i>Performance(PSNR)</i>
	<i>0.2</i>	<i>0.999858</i>	<i>27.6107</i>
	<i>0.4</i>	<i>0.987784</i>	<i>22.3353</i>

The performance of system is shown in table 3.1 where it is used different values of alpha for hiding and the system can obtain efficient results as PSNR and NC measure.

Chapter Four

Conclusions and future works

4.1 Conclusions:

Watermarking of images using DCT is a powerful technique for protecting. By applying DCT to an image and embedding a watermark in the frequency domain, you can ensure the integrity and ownership of your images. DCT-based watermarking offers robustness, imperceptibility, security, and efficiency, making it an ideal choice for professionals in various creative fields.

However, the obtained results show the robustness of used system and its efficiency.

4.2 Future Works:

Some capabilities can be applied as improvements or studies on system such as:

- 1- Another Frequency domain method other than DCT.
- 2- Combined another technique with DCT for watermarking operation for robustness.

References

- 1- The Essential Guide to Image Processing (Second Edition) 2009, Pages 597-648 Author panel Anastasios Tefas , Nikos Nikolaidis , Ioannis Pitas Aristotle University of Thessaloniki Available online 27 July 2009. Chapter 22 - Image Watermarking: Techniques and Applications 7
- 2- Different Types of Watermarks 20 / 12 / 2019 Andere Beiträge
- 3- International Journal of Computer Applications Technology and Research Volume 5–Issue 3, 147150, 2016, ISSN:2319–8656 www.ijcat.com 147 Digital Watermarking Applications and Techniques: A Brief Review Aaqib Rashid MCA (Kashmir University) M.Phil Computer Science (Dr. C.V Raman University)
- 4-Watermarking System using LSB\IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661,p-ISSN: 2278-8727 , Volume 19, Issue 3, Ver. II (May.-June. 2017), PP 75-79,www.iosrjournals.org\ Hewe Majeed Zangana , Department of Computer Science / College of Computer Science and IT / Nawroz University / Kurdistan Region of Iraq
- 5-JOURNAL OF COMPUTING, VOLUME 3, ISSUE 4, APRIL 2011, ISSN 2151-9617
[HTTPS://SITES.GOOGLE.COM/SITE/JOURNALOFCOMPUTING/](https://sites.google.com/site/journalofcomputing/)
[WWW.JOURNALOFCOMPUTING.ORG](http://www.journalofcomputing.org) A New Digital Watermarking Algorithm Using Combination of Least Significant Bit (LSB) and Inverse Bit\ Abdullah Bamatraf, Rosziati Ibrahim and Mohd. Najib Mohd. Salleh
- 6-Advance in Electronic and Electric Engineering. ISSN 2231-1297, Volume 4, Number 5 (2014), pp. 499-506 © Research India Publications <http://www.ripublication.com/aeee.htm>\ Copyright Protection for Watermark Image Using LSB Algorithm in Colored Image\ Rajni Verma1 and Archana Tiwari Department of Electronics & Telecommunication, CSIT, Durg,

Chhattisgarh, Bhiilai-India CSVTU (durg) ME Scholar (CSIT-Durg) E&I, (CSITDurg)

7- I. Cox, J. Kilian, F. Leighton, and T. Shamoon, "Secure Spread Spectrum Watermarking for Multimedia," IEEE Transactions on Image Processing, vol. 6, no. 12, pp. 1673-1687, Dec. 1997.

8- M. Swanson, B. Zhu, and A. Tewfik, "Transparent Robust Image Watermarking," Proc. IEEE Int. Conf. on Image Processing, Sept. 1996, vol. III, pp. 211-214.

9- 3. I. Pitas, "A Method for Signature Casting on Digital Images," Proc. IEEE Int. Conf. on Image Processing, Sept. 1996, vol. III, pp. 215-218 Chapter Two Theoretical Part

10- C.S. Lu, Multimedia Security: Steganography and Digital Watermarking for Protection of Intellectual

11- G. Coatrieux, L. Lecornu, Members, IEEE, Ch. Roux, Fellow, IEEE, B. Sankur, Member, IEEE "A Review of digital image watermarking in health care".

12-Edin Muharemagic and Borko Furht —A Survey of watermarking techniques and applications 2001.

13-Avani Bhatia, Mrs. Raj Kumari U.I.E.T, Panjab University: "Digital Watermarking Techniques" .

14- R.G. Schyndel, A. Tirkel, and C.F Osborne, —A Digital Watermark, Proceedings of IEEE International Paper ID: 02013645 312 International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064 Volume 2 Issue 12, December 2013 www.ijsr.net conference on Image Processing, ICIP-1994, pp. 86- 90, 1994

15- V. P. S. Naidu, "Novel Image Fusion Techniques using DCT," Int. J. Comput. Sci. Bus. Informatics, vol. 5, no. 1, pp. 1–18, 2013, [Online]. Available: <http://ijcsbi.org/ijcsbi/index.php/ijcsbi/article/view/119>.

- 17- D. Mishra and B. Palkar, "Image Fusion Techniques: A Review," *Int. J. Comput. Appl.*, vol. 130, no. 9, pp. 7–13, 2015, doi: 10.5120/ijca2015907084
- 16- C. Li and A. Zhu, "Application of image fusion in diagnosis and treatment of liver cancer," *Appl. Sci.*, vol. 10, no. 3, 2020, doi: 10.3390/app10031171.
- 17- Z. Al-Mokhtar, F. Ibraheem, and H. Al-Layla, "A Review of Digital Image Fusion and its Application," *Al-Rafidain Eng. J.*, vol. 26, no. 2, pp. 309–322, 2021, doi: 10.33899/rengj.2021.127928.1055.
- 18- A. O. Salau, S. Jain, and J. N. Eneh, "A review of various image fusion types and transforms," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 24, no. 3, pp. 1515–1522, 2021, doi: 10.11591/ijeecs.v24.i3.pp1515-1522
- 19- Pattanaik, S.K.; Mahapatra, K.K.; "A Lossless Image Compression Technique using Simple Arithmetic Operations and its FPGA Implementation"; *IEEE Chapter Two Theoretical Part International Conference on Industrial Technology, ICIT 2006*. Page(s): 2211 – 2216.
- 20- Zhu Mengyu; Yang Yuliang; Zhao Baojun; "An efficient FPGA design for lifting wavelet", 3rd International Conference on Computational Electromagnetics and Its Applications, 2004. *Proceedings. ICCEA*. Page(s): 508 – 511.
- 21- Grgic, S.; Grgic, M.; Zovko-Cihlar, B.; "Performance analysis of image compression using wavelets *Industrial Electronics*", *IEEE Transactions on* Volume: 48 , Issue: 3. Publication Year: 2001 , Page(s): 682 – 695. *Signal & Image Processing : An International Journal(SIPIJ)* Vol.1, No.2, December 2010
- 22- Grgic, S.; Grgic, M.; Zovko-Cihlar, B.; zem, Aksahya & Ayese, "Optimal decomposition for wavelet image compression", *Image and Signal Processing and Analysis*", *First International Workshop 2000, IWISPA*. Page(s): 203 – 208.
- 23- Nguyen, C., Redinbo, G.R.; "Fault tolerance design in JPEG 2000 image compression system *Dependable and Secure Computing*", *IEEE Transactions on* Volume:2, Issue: 1 Publication Year: 2005 , Page(s): 57 – 75.