Ibn Al-Haitham Journal for Pure and Applied Sciences
Journal homepage: jih.uobaghdad.edu.iq

Secured Mechanism Towards Integrity of Digital Images Using DWT, DCT, LSB and Watermarking Integrations

Mohammed Hassan Abd
Department of Computer Sciences, College of Education Pure and Applied Science Ibn Al-Haitham, University Baghdad, Iraq.
mohammed.h@uobaghdad.edu.iq

Osamah Waleed Allawi
AL Kalam High Secondary School, Baghdad, Basmayah Iraq.
osamahwaleed@Gmail.com

Article history: Received 24 October 2022, Accepted 6 March 2023, Published in April 2023.

doi.org/10.30526/36.2.3088

Abstract

"Watermarking" is one method in which digital information is buried in a carrier signal; the hidden information should be related to the carrier signal. There are many different types of digital watermarking, including traditional watermarking that uses visible media (such as snaps, images, or video), and a signal may be carrying many watermarks. Any signal that can tolerate noise, such as audio, video, or picture data, can have a digital watermark implanted in it. A digital watermark must be able to withstand changes that can be made to the carrier signal in order to protect copyright information in media files. The goal of digital watermarking is to ensure the integrity of data, whereas steganography focuses on making information undetectable to humans. Watermarking doesn't alter the original digital image, unlike public-key encryption, but rather creates a new one with embedded secured aspects for integrity. There are no residual effects of encryption on decrypted documents. This work focuses on strong digital image watermarking algorithms for copyright protection purposes. Watermarks of various sorts and uses were discussed, as well as a review of current watermarking techniques and assaults. The project shows how to watermark an image in the frequency domain using DCT and DWT, as well as in the spatial domain using the LSB approach. When it comes to noise and compression, frequency-domain approaches are far more resilient than LSB. All of these scenarios necessitate the use of the original picture to remove the watermark. Out of the three, the DWT approach has provided the best results. We can improve the resilience of our watermark while having little to no extra influence on image quality by embedding watermarks in these places.

Keywords: Image Security, Image Watermarking, Watermarking Based Securing in Digital Images.

1. Introduction

There has been a dramatic reduction in the cost and time required to generate and disseminate digital snaps and images due to image processing technology and the internet. Data privacy and security are at risk as a result of the rapid advancement of network technologies [1]. Because of the current and future dangers to digital information, content authentication, copyright protection, and protection against duplication are needed. Digital image watermarking is the process of adding a digital watermark to an image in order to protect it from tampering, prove ownership of intellectual property, and make multimedia documents more secure. Digital stuff, including images, music, and video, can conceal information. A physical transmission media may readily be used to unlawfully obtain and distribute digital content, as well as process, store, and transmit it. When watermark data is integrated into a multimedia product, it can be recovered from the watermarked product or identified by the watermarked product itself. There are several ways to protect the image from tampering: authentication, content verification, and image integration. Transforming watermarked data into another file format is not a simple way to get rid of the watermark. As a result, following an assault, the watermark might provide insight into the change. The ability to distinguish between digital watermarking and other methods, such as encryption, is crucial [2]. Digital image watermarking techniques can also withstand digital-to-analog conversion, compression, file format changes, re-encryption, and decryption. It's an alternative (or supplementary) to cryptography because of these tasks. When you use the material, you can't erase the information because it's incorporated into the content.

An embedded, communication channel and a detector are the three essential components of a watermarking system. It is possible for the detector to extract watermark information since it is not tucked away in the file header or encrypted like other security measures. Before the watermarked signal [3] is transferred via a communication channel, a watermark is inserted into the host signal to allow the watermark to be recognized at the detector. There are optional components that may or may not be necessary depending on the application. The dotted lines represent these components. First, a watermark Wo is formed by the watermark generator, which may use a secret watermark generation key Kg to generate this watermark. A logo or a pseudo-random signal can be used as the watermark Wo.

In order to strengthen the watermark's resistance against probable signal processing procedures or its imperceptibility, the watermark Wo might be pre-coded instead of being embedded directly into the host signal. An information encoder may need the original signal to do this task; a watermark may be encoded using the spread spectrum method [4].

2. Materials and Methods

A 1-D binary string containing just the values 0 and 1 is generated from the offline handwritten signature of the owner for the purpose of authentication. In order to watermark the image, these two values must be entered.

2.1 Watermark Embedding

The following are the stages involved in inserting a watermark:

•The first step is to divide the color picture into three channels.

•Synchronized registration information may be saved by utilizing SIFT to calculate feature points in the red channel and saving them.

•Use bi-orthogonal wavelet transforms to perform a two-level DWT on the carrier image's blue and green components.
•Create a pseudorandom sequence equal to the watermark's length using a private key.
•This mask is used to choose wavelet coefficients from the LH sub-bands of the decomposed image's blue and green channels. Pseudorandom sequences generated with a private key are used in this method.
•Add a watermark to the host picture by embedding it in the blue component.
A wide variety of methods exist for concealing information in digital material , hidden data might be stored in unallocated memory space or in unused portions of files. Unused header file sections may contain little amounts of data. If a partition isn't accessible under normal circumstances, there are a few tools that can grant you complete access to that disc.

The technique based on substitution uses secret data to replace unnecessary elements of the picture. The stenographic holder structure and the RGB (Red-Green-Blue) systems are crucial to comprehending this idea .The RGB color system uses the relative intensities of red, green, and blue to represent each color.

An octet, or 8-bit sequence, determines the intensity of each of the three colors, which can range from 0 to 255 for each component. Using the three components of the RGB system, we get a 24-bit scheme that offers 16,777,216 distinct colors.
The 24-bit method is supported by the majority of today's image processing and display software, although an 8-bit technique can be used to reduce the picture size. However, a palette that defines the colors to be utilized in the image is employed in conjunction with 24-bit color pixels in this system. An 8-bit value is assigned to each pixel and used to represent the chosen color in the palette. In order to maintain an 8-bit color palette, this approach caps the number of colors utilized in the image at 256. GIF (Graphics Interchange Format) is a lossless image compression format that uses an 8-bit pattern.
Discrete Cosine Transform (DCT):
The 8x8 block values are coded by means of the discrete cosine transform.
This part is an image of an 8x8 area of a black-white frame.

The normal way is to determine the brightness of each of the 64 pixels and to scale them to some limits, say from 0 to 255, so «0» means «black» and «255» means «white». We can also represent the values in form of an 8x8 bar diagram. Normally the values are processed line by line. This requires 64 byte of storage.

But, you can define all the 64 values by only 5 integers if you apply the following formula called discrete cosine transform (DCT)

$$F(u,v) = \frac{C_u}{2}\frac{C_v}{2}\sum_{y=0}^{7}\sum_{x=0}^{7} f(x,y)\cos\left[\frac{(2x+1)u\pi}{16}\right]\cos\left[\frac{(2y+1)v\pi}{16}\right]$$

with:

$$C_u = \begin{cases} \frac{1}{\sqrt{2}} & \text{if u} = 0, \\ 1 & \text{if u} > 0 \end{cases}; C_v = \begin{cases} \frac{1}{\sqrt{2}} & \text{if v} = 0, \\ 1 & \text{if v} > 0 \end{cases}$$

Where f(x,y) is the brightness of the pixel at position [x,y]. The result is F an 8x8 array:

The decoder can reconstruct the pixel values by the following formula called inverse discrete cosine transform (IDCT):

$$f(x,y) = \sum_{u=0}^{7}\sum_{v=0}^{7} F(u,v)\,\frac{C_u}{2}\,\frac{C_v}{2}\cos\left[\frac{(2x+1)u\pi}{16}\right]\cos\left[\frac{(2y+1)v\pi}{16}\right]$$

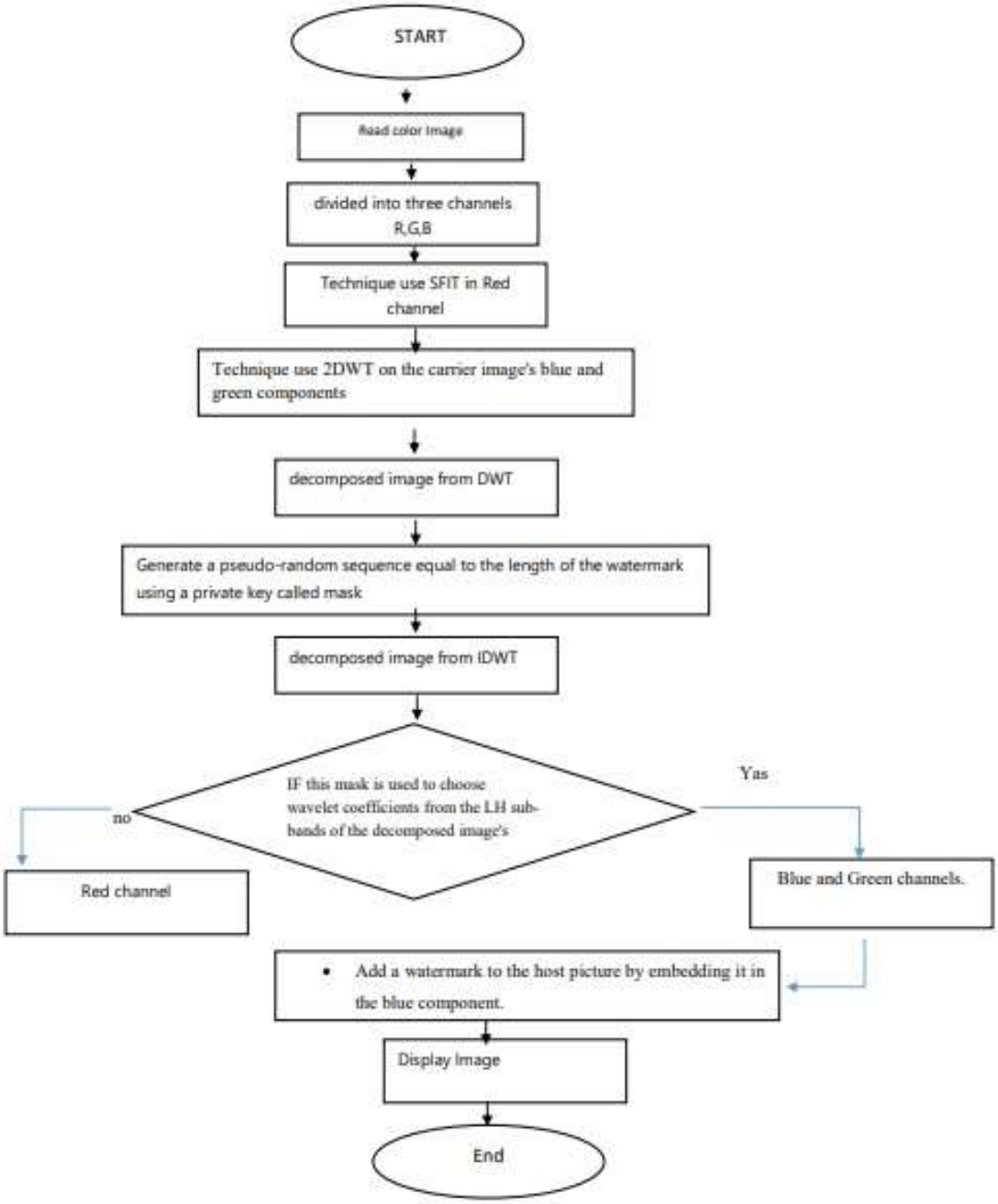


Figure 1. The figure shows the algorithm for adding a watermark to the image and hiding the information using DWT

2.2 Substituting only the most essential elements

The most popular steganography approach in multimedia steganography is the substitution of the least significant bits (LSB substitution). The "minimum important bit" (or "MIB") refers to the octet's least significant eight bits. The most critical bit has an arithmetic value of 12810,

whereas the least critical bit has an arithmetic value of 0. (110). All octets in a multimedia file are affected by a change in the minimum number of bits. However, because of our limited ability to detect subtle alterations in hue, the previously mentioned theory is considerably more successful. Using stenographic techniques, it is possible to replace the least important bits in selected octets with the most significant ones by breaking the secret messages encoded in the bits.

By inserting bytes through secret messages in an easy way, like a series of adjacent bytes at the beginning of the file, it's very likely that this section will have statistics that differ from those of the rest of the image, attracting attention and compromising the privacy of any secret messages that may be contained within it. As a result, the random selection of the destination octet is one of the aspects that make steganography message detection exceedingly difficult. Using the supplied approach, the integration followed the example of concealing one image over another. People can use steganography's high-tech techniques to hide and safeguard their communications. An extra layer of security on top of cryptography protects the data even further. As stenographic technology is exceedingly difficult to detect, it is extremely easy to employ. There have been several debates in recent years about the potential misuse of steganography, particularly by terrorists.

Steganography has been the topic of a number of debates in recent years about its misuse, particularly in the context of terrorist activity. The use of steganography to distribute unlawful material via multimedia files on the Internet is becoming a rising issue for various legal agencies. Steganography's sister discipline, steganalysis, is substantially more recent. Today, we have a variety of stage techniques at our disposal that allow us to identify and prevent such crimes.

As steganography has several advantages in legal contexts, such as digital watermarking to establish copyright ownership or more secure means of keeping critical and secret information, the technology will continue to be developed and its application possibilities will expand in future years. MATLAB offers a wide range of options for visualizing data in the form of vectors and matrices, as well as for notating and printing these representations. Animation, data visualization, image processing, and other high-level operations are available in a single package. In today's world, the internet has become an essential element of everyday life, and digital media has grown exponentially as a result. The emergence of large-capacity digital recording devices has increased the possibility of piracy. Watermarking's fast rise in popularity is most likely the result of heightened awareness about the importance of copyright protection for digital work. It is possible to watermark audio, picture, and video files. Embedding and recovering information from other digital data is a sort of information concealing, and digital watermarking is one example of this type of information hiding. Other methods of concealing information include covert communication (steganography) and the incorporation of additional data into multimedia files. If the encoded information can be read even after A/D and D/A conversion, the latter use is particularly fascinating. A digital watermark must be imperceptible to the human eye, such that the watermarked data and the original data are indistinguishable to the eye. This means that the watermarked data cannot be damaged or even destroyed during processing without causing the processed data to be rendered ineffective. Permission-based access means that only those with the proper credentials may access the embedded data. Watermarking can be used in a variety of ways, including:

Instead of exploiting a specific section of the broadcast signal, watermarking is included in the program itself. When it comes to owner identification, watermarks may be better than text because they may be rendered invisible and impossible to remove from the work they are attached to. As long as watermark detectors are provided to customers, they can identify watermarked works even if textual copyright notices have been removed from them. The watermark records one or more transactions in the history of the copy of a work in which it is contained. Each copy of the work would have a unique watermark applied by the piece's creator. In the event that the work is misused, the owner will be held accountable.

Content Authentication: Watermarking provides localized authentication and checks for lossy compression of the file. Using watermarks is a great way to ensure that the content cannot be reproduced without permission. The detection of a never-copy watermark at the input of a recording device might be made to prevent recording if the device was equipped with a watermark detector. We classify applications like copy control under the umbrella term "device control." Printed and disseminated graphics, such as magazine adverts, tickets, etc., are encoded with a unique identification. Using a digital camera to capture the image again, the watermark is read by PC software, and the identification is used to route a web browser to an associated web page.

This technique, known as picture watermarking, is used to hide information inside an image by making small changes to its pixels. Watermarking is highly secure, however, there are still a number of potential attack vectors that might be exploited:

Enhancement: sharpness, contrast, and color correction. Gaussian, uniform, and speckle noise are examples of additive and multiplicative noise, respectively. The low pass, high pass, and band pass are all examples of linear filtering. Morphological and nonlinear filtering are examples of nonlinear filtering.

Measuring perceptibility and robustness is more challenging. The **Table** shows a system proposed by Petit colas and others for evaluating perceptibility.

Table 1 shows a preliminary set of reliability and robustness measures provided by Petit colas; they are presented below.

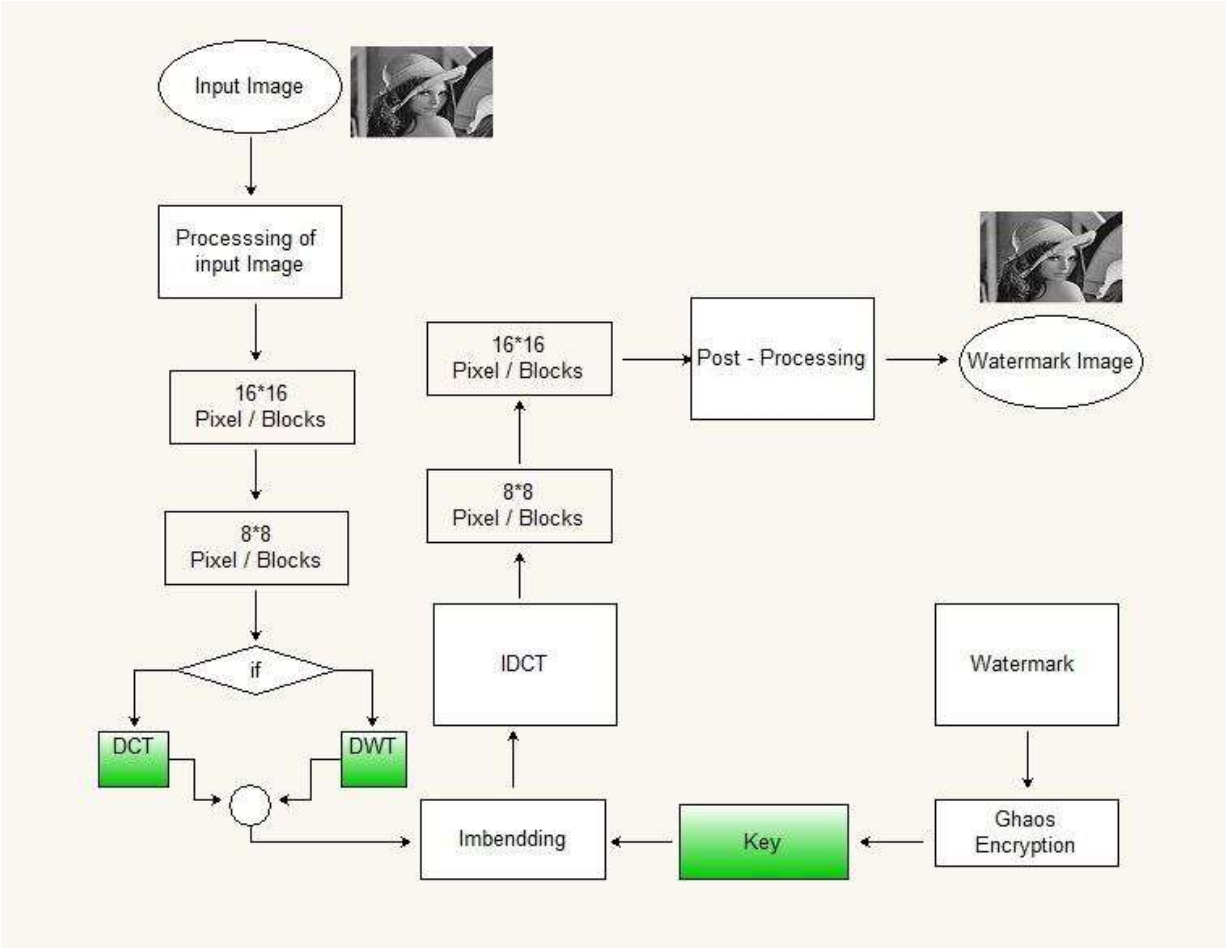


Figure 2. The figure shows the use of the water footprint to hide information using the DCT and DWT compression algorithms

Table 1. Robustness Analytics.

	Low Level	**Level Zero**	**Moderate**
Standard JPEG Compression Quality	100 – 75	100 – 90	100 – 50
Color Reduction (GIF)	256	256	16
Cropping	100 - 75%	100 - 90%	100 - 50%
Gamma Correction	0.7-1.2		0.5-1.5
Scaling	$\frac{1}{2} - \frac{3}{2}$		$\frac{1}{3} - 2$
Rotation	+/- 0 - 2 deg.		+/- 0 - 5 deg. 90 deg.
Horizontal Flip	Yes		Yes
Uniform Noise	1-5%		1-15%
Contrast	+/- 0 - 10%		+/- 0 – 25%
Brightness	+/- 0 – 10%		+/- 0 – 25%
Median Filter			3 x 3

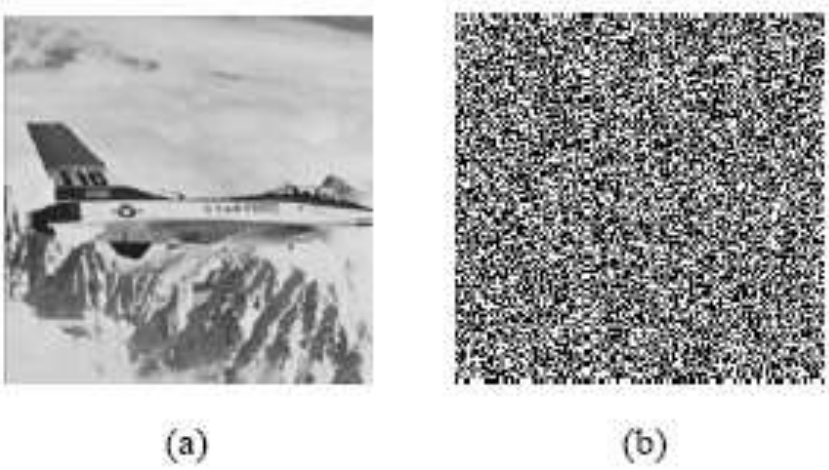


Figure 3. Filtering Based Approach

Figure 4. Detection of Forger with Geometric Attacks

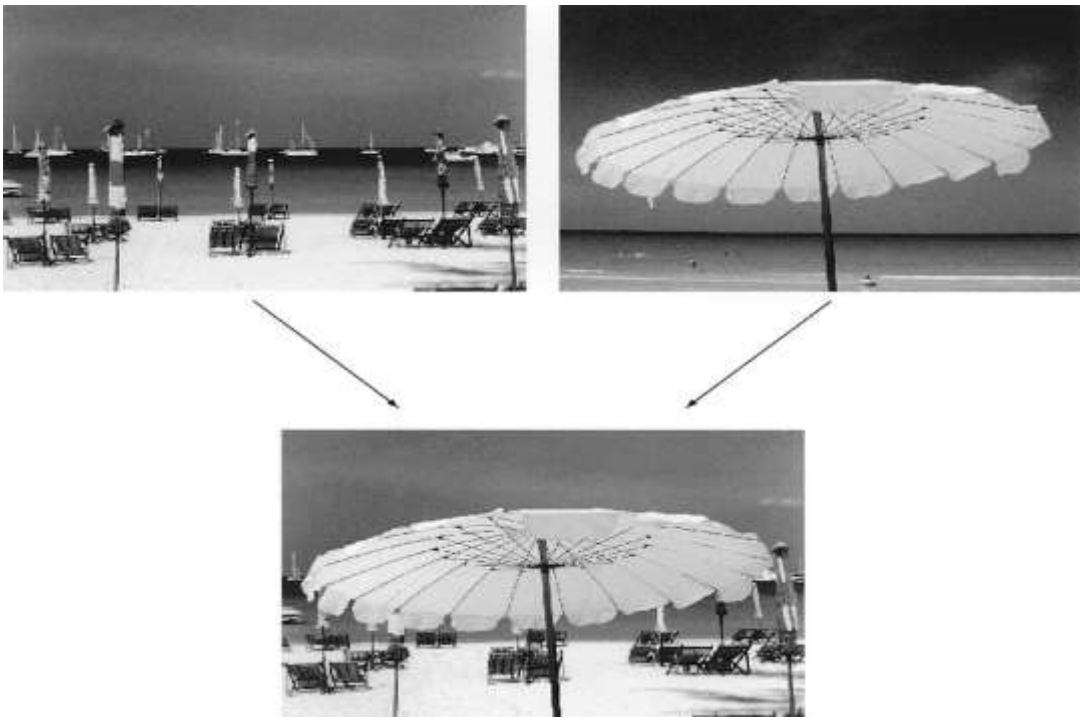


Figure 5. Image Composition

Figure 6. Image Security Analytics

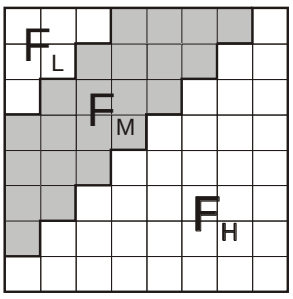


Figure 7. Analytics Patterns

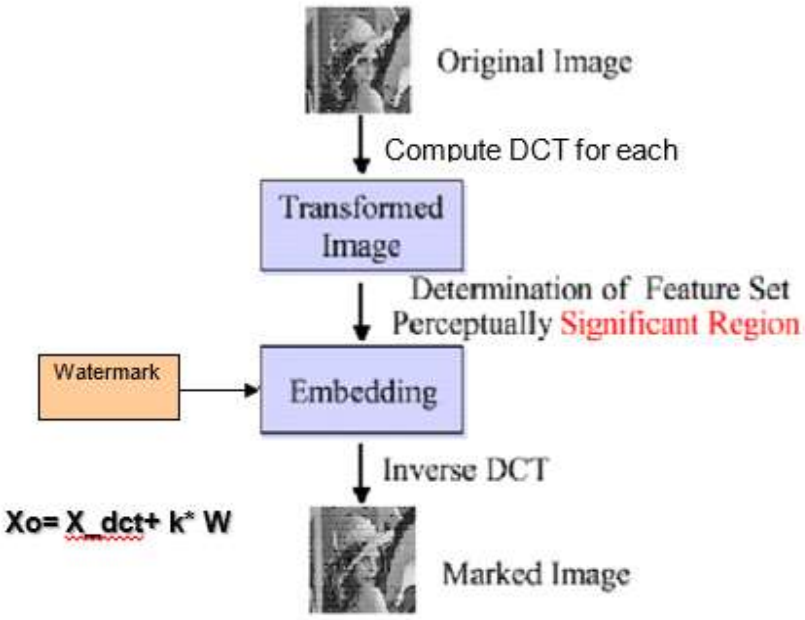


Figure 8. DCT Integration with Watermark

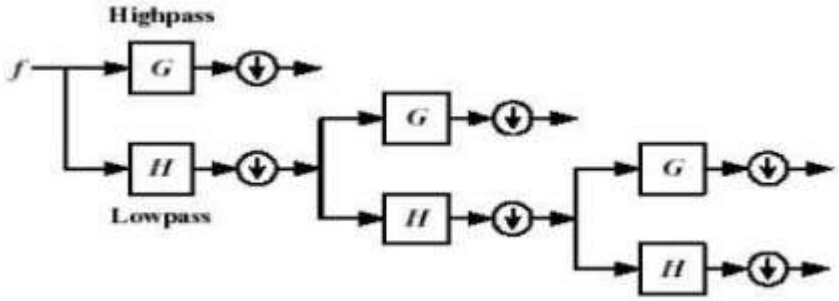
DWT: Discrete Wavelet Transform is a technique to transform image pixels into wavelets, which are then used for wavelet-based compression and coding.

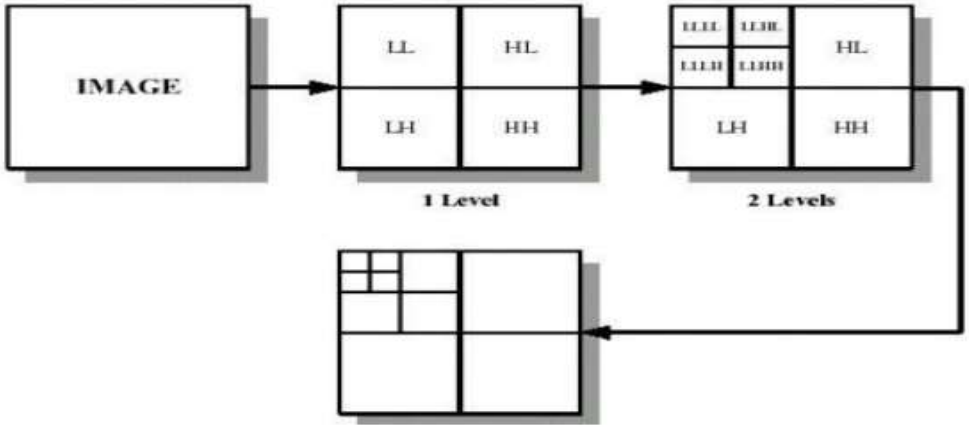
Discrete wavelet transforms (DWT), which transforms a discrete time signal to a discrete wavelet representation. ω it converts an input series x0, x1, ..xm, into one high-pass wavelet coefficient series and one low-pass wavelet coefficient series (of length n/2 each) given by:

$$H_i = \sum_{m=0}^{k-1} x_{2i-m} \cdot s_m(z) \qquad (1)$$

$$L_i = \sum_{m=0}^{k-1} x_{2i-m} \cdot t_m(z) \qquad (2)$$

Figure 9. 2 scale 2 dimensional DWT





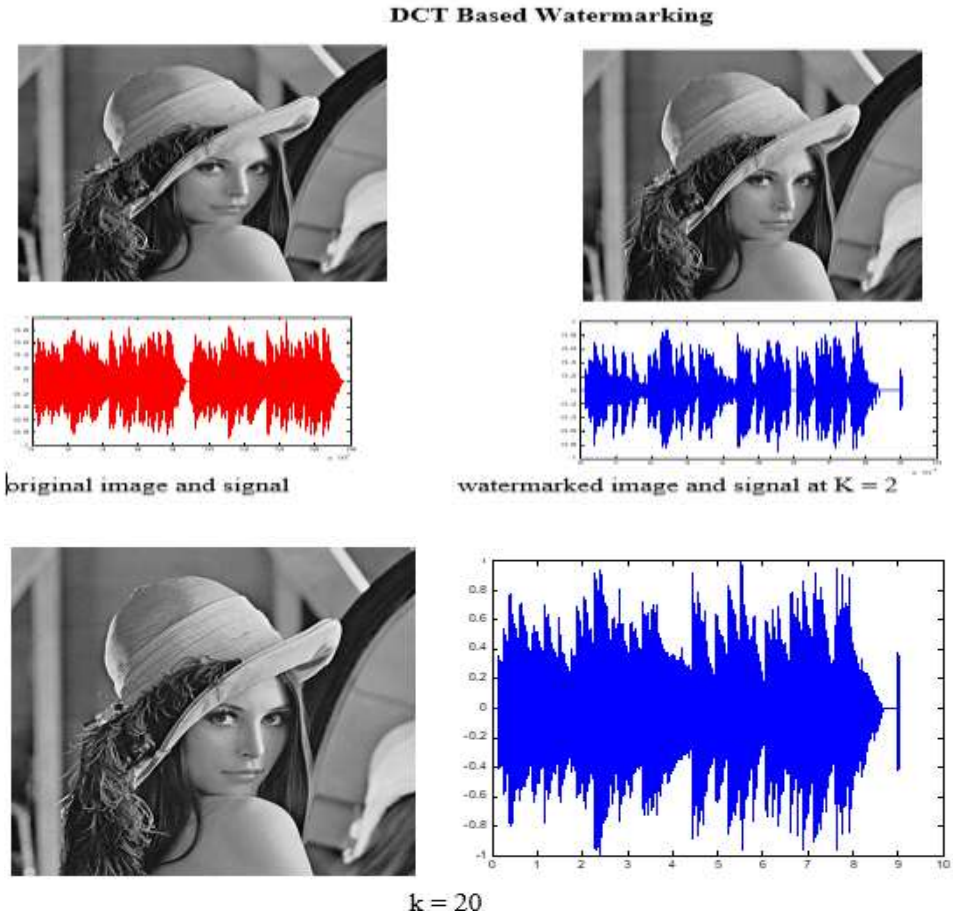


Figure 10. Secured Approach with Waveforms

2.3 Least Significant Bit Modification (LSB Modification):

Embed the watermark into the cover object's least important bits. That's the simplest way to go about embedding it. Using the entire cover as a transmission channel, a smaller item may be inserted numerous times because of the enormous channel capacity. Although many of them have been destroyed, a single watermark that is still intact is still considered a success.

The gray scale image's bit-planes are shown on the left, with the MSB at the top. Bit-plane pixels have binary values of 0s and 1, which are represented by the dark and bright boxes, respectively. It is substituted with concealed data in the center, which becomes the LSB plane of the stage-cover image's image LSB-plane. The LSB plane discrepancies between the cover and stage pictures are shown in the bottom-right map. There are circles that indicate the flipped bits; with an average of 50 percent modified, it's visually identical to the cover with stego imaging.
LSB substitution, despite its simplicity, has a slew of downsides that must be considered. The watermark may be able to withstand cropping and other changes, but any noise or lossy compression is likely to destroy it. In order to completely remove the watermark, all that is needed is to change the LSB bits of each pixel to one. Once the technique is found, the encoded watermark may be simply changed by an intermediary party.

2.4 Techniques in the Frequency Domain

SIFT It is a technique for detecting salient, stable feature points in an image. Due to their universality and ease of use, the spatial approaches described above may be applied to any image (whether they survive this processing, however, is a different matter entirely). Spatial approaches may have the drawback of preventing the further processing needed to boost the watermark's resilience from being utilized. Adaptive watermarking methods are even more challenging to implement in the case of spatial data. If the features of the cover picture could be similarly leveraged, the watermark's resilience and quality may be increased. Watermarking information should be hidden in areas with a lot of noise and edges rather than smoother areas of a picture. Both the HVS and lossy compression algorithms benefit from this because the degradation in the smoother portions of a picture is more obvious. Due to all of these factors, working in some form of frequency domain becomes quite appealing. The Discrete-Cosine-Transform, or DCT, is an image processing classic that is still widely used today. With the DCT, images may be divided into many frequency bands, making it easier to incorporate watermarking information into the image's intermediate frequency bands. As a result, the intermediate frequency bands are selected such that they avoid the most visually significant elements of the image (low frequencies) while not overexposing themselves to elimination through compression and noise assaults (high frequencies).For example, comparing middle-band DCT coefficients can be used to encode only one bit into a whole block of DCTs. In order to begin, we need to establish the 8x8 DCT block's middle-band frequencies (FM).

The lower frequency components of the block are designated as FL, while the higher frequency components are designated as FH. Embedding in FM avoids large changes in the cover picture while providing further resilience to lossy compression approaches.

2.5 Problem

The security and integrity of digital images and multimedia content are quite important and are the main focus of this work. Many frequent signal and geometric processes impact the image's perceptually inconsequential portions (or spectrum), which is why the watermark shouldn't be put

there. An image watermark applied in the high-frequency range may be readily removed with little harm to the picture using any low-pass filtering procedure.

Watermarking in the most perceptually important parts of the spectrum while maintaining integrity is a challenge. As long as the change is minimal, any spectral coefficient can be adjusted. On the other hand, Noise has a tendency to amplify even the tiniest adjustments.

Watermarks can be considered as a signal delivered across the frequency domain of the picture or sound at hand in order to address this problem. These inadvertent errors are treated as noise by the submerged signal and must be protected against. Watermarks can be hidden in data, but the same logic can be used to transmit any kind of message via media data [5].

First, we drew inspiration from spread spectrum communication. Broadcasting a narrowband signal over a much greater bandwidth, the signal energy existing in any particular frequency is completely unnoticeable in spread spectrum communications, Similarly, the watermark's energy is dispersed across a large number of frequency bins, making it very impossible to detect. There are numerous weak signals that may be concentrated in a single output with a high signal-to-noise ratio because of the watermark verification process' knowledge of the watermark's position and content. It is, nevertheless, necessary to introduce noise of large amplitude to every frequency bin in order to remove a watermark [6].

Unintentional or intended attacks can be greatly reduced by using a watermark that covers the whole image. To begin with, it's hard to see where the watermark is. It's also important to set frequency zones in a way that assures substantial deterioration of original data if the watermark is breached.

A well-placed watermark in the frequency domain of a picture or sound recording will be nearly hard to detect. Unless the watermark energy is infinitesimally small, this will always be the case. There are ways to amplify specific frequencies by using the human auditory and visual systems' understanding of masking events. To put it another way, perceptual masking may be used to describe any circumstance where information in certain parts of an image or a sound is obliterated by more prominent information elsewhere in the picture. For low-bit-rate data encoding in digital waveform coding, frequency domain (and, in certain situations, time/pixel domain) masking is used extensively. High-energy, low-frequency spectrum areas of an auditory or visual picture have been shown to have more resolution than lower frequencies [7]. The majority of the information in images and sounds may be found in the low-frequency ranges, as can be seen by doing a spectrum analysis of the data.

2.6 Image Watermarking System Needs and Tradeoffs

Security: Depending on the intended use, a watermarking system's security requirements may change somewhat. Security in watermarking means that the watermark should be difficult to remove or modify without causing harm to the host signal. Watermarking security may be defined as the capacity to ensure the secrecy and integrity of watermark information and to resist harmful assaults since all watermarking systems attempt to safeguard watermark information without losing generality [8].

The watermark's perceptual transparency is what we mean by its "imperceptibility" Ideally, there should be no discernible change between the watermarked signal and the original signal. Embedment into an undetectable section of a host signal is an easy approach to decrease distortion during the watermarking process. As a result, a hacker may easily modify the watermark data without being detected.

It is important to note that watermarking capacity refers to the quantity of information that can be encoded into a host signal. Imperceptibility and robustness, as well as the capacity needed, are often at odds with each other [9]. Higher capacity is frequently achieved at the price of either strength or imperceptibility.

2.7 Low Pass Filtering

A difference map is created by applying a low-pass filter to the watermarked picture.

As a general rule, any alterations that alter the shape of the image (such as flipping, rotating, or cropping) should be recognizable. The figure depicts a cropping assault from the right side and the bottom of the image [10].

2.8 Geometric attacks

The tampering can be clearly visible in the difference map where two noisy stripes surround the picture. To distinguish cropping attacks from global manipulations like scaling, low-pass filtering, or histogram equalization that would result in a completely noisier difference map when used in conjunction, the suggested method is capable of doing just that [11].

Changing the scene's backdrop or adding or removing objects as a result of forgery attempts is equivalent to replacement. As a result, the forgery attacks discussed above may be reduced to a single replacement assault. To counter a replacement attack, the following experiment replaces the watermarked picture component with a different, unwater marked portion of the identical image [12]. In terms of watermarks and watermarking processes, there are a number of subcategories. Depending on the type of document to be watermarked, watermarking techniques may be split into four groups: It may be used for a variety of purposes, including tagging images and audio, as well as for video watermarking [13].

3. Results

Wavelet-Based Watermarking: Wavelet embedding is another alternative watermark embedding domain. Images may be divided into approximation (LL), detail (HL), and approximation images (LL) using the DWT, a Discrete Wavelet Transform. Afterward, it is possible to do numerous "scale" wavelet decompositions, such as seen in the image below. When compared to the FFT or DCT, one of the wavelet transform's numerous advantages is that it is thought to better simulate the HVS. Using higher energy watermarks in locations where the HVS is known to be less sensitive, such as high-resolution detail bands LH, HL, and HH, is possible. We can improve the resilience of our watermark while having little to no extra influence on image quality by embedding watermarks in these places.

4. Discussion

It is important to note that feature points are components of information that are intrinsically related to the content. Large picture distortions have a high possibility of matching these local invariant characteristics. As a result, following an assault, the relative location of a feature point like this remains constant, making it useful for synchronization purposes [14].

However, David Lowe's SIFT method has shown to be quite effective in the extraction of features. Local features based on SIFT will remain unchanged even if the image is zoomed, rotated, brightened, or affine transformed. SIFT operator retrieves features and their attributes such as the location (x,y), scale S, and orientation è based on the local picture characteristics. By identifying

stable points in the scale space, the SIFT is possible to extract features using staged filtering that selects candidates for features by looking for peaks. The Difference of the Gaussian (DoG) function is used to determine the scale spacing D(x,y,) in order to extract potential feature locations [15].

Pictures are smoothed with a variable-scale Gaussian kernel to produce scale-space images, which are then subtracted from each other. The Gaussian function's variance (also known as its scale) serves as the parameter. It is possible to locate local maximum and minimum values by examining the eight scales immediately adjacent to them, as well as the nine scales above and below. Extreme (x,y) and scale 'S' (invariant to scale and orientation change) establish the SIFT features' position (x,y) and scale [15].

Biometric characteristics such as a handwritten signature can be included in color images using the watermarking approach provided here. The separation of red, blue, and green colors into their respective channels occurs in a color picture. In order to identify watermarks, feature points are extracted from the red channel using SIFT and recorded as synchronous registration information. For aesthetic reasons, we choose to place our watermark in blue instead of other colors. Stable features are achieved by purposely separating the channels for feature point extraction and watermark insertion. Geometric distortion may be estimated from feature points in the original picture without needing the original. As a result, the algorithm is semi-blind in nature. Before embedding, an offline user's handwritten signature is preprocessed and transformed into a binary bit string. A total of four processes are involved in the proposed watermarking method: preparation, embedding, geometric attack estimate, and detection .

5. Conclusion

This work focuses on strong digital image watermarking algorithms for copyright protection purposes. Watermarks of various sorts and uses were discussed, as well as a review of current watermarking techniques and assaults. The project shows how to watermark an image in the frequency domain using DCT and DWT, as well as in the spatial domain using the LSB approach. When it comes to noise and compression, frequency domain approaches are far more resilient than LSB. All of these scenarios necessitate the use of the original picture to remove the watermark. Out of the three, the DWT approach has provided the best results. Algorithms in the future are projected to be able to extract watermarks from images that have been damaged by various geometric and signal processing methods, such as cropping, rotation, scaling, and translation, without the need for the original picture. It's possible to utilize feature points as a reference for both embedding and detecting the watermark in watermarking. The feature points are identified via feature point detectors, and these detectors should extract the feature points that are resistant to different distortions (compression, filtering, geometric distortions, etc.). Both detectors performed quite well when it came to JPEG and JPEG 2000 filtering and compression. SIFT descriptors were computed for each feature point that was retrieved using the SIFT detector. The correlation coefficient between the SIFT descriptors was used to determine the correspondences between the points. As soon as one image's correspondence to another is established, it is possible to estimate the parameters of the geometric transformation that took place and compute an inverse geometrical transformation that may be applied to it. This method has the advantage of not requiring the original or watermarked image to be present.

References

1. Arrasyid, A. A.;Soeleman, M. A.; Sari, C. A.; Rachmawanto, E. H. November. Image watermarking using triple transform (DCT-DWT-SVD) to improve copyright protection performance. *In International Seminar on Research of Information Technology and Intelligent Systems (ISRITI)* **2018** , 522-526. IEEE.

2. Zhang, L.; Wei, D. Dual DCT-DWT-SVD digital watermarking algorithm based on particle swarm optimization. *Multimedia Tools and Applications*, **2019,***78(19*), 28003-28023.

3. Begum, M.; Ferdush, J.; Uddin, M. S. A Hybrid robust watermarking system based on discrete cosine transform, discrete wavelet transform, and singular value decomposition. *Journal of King Saud University-Computer and Information Sciences*. **2021**.

4. Hamidi, M.; El Haziti, M.; Cherifi, H.; El Hassouni, M. A Hybrid Robust Image Watermarking Method Based on DWT-DCT and SIFT for Copyright Protection,*Journal of Imaging*, **2021,***7(10),* 218.

5. Singh, P. K. Robust and imperceptible image watermarking technique based on SVD, DCT, BEMD and PSO in wavelet domain. Multimedia Tools and Applications, **2021,**1-26.

6. Chacko, A.; Chacko, S. Deep learning-based robust medical image watermarking exploiting DCT and Harris hawks optimization. *International Journal of Intelligent Systems*. **2021**.

7. Garg, P.; Kishore, R. R. An efficient and secured blind image watermarking using ABC optimization in DWT and DCT domain. *Multimedia Tools and Applications*, **2021,** 1-18.

8. Dhaked, D. K. Combined DCT-DWT Color Image Digital Watermarking Technique. In Emerging Trends in Data Driven Computing and Communications, *Springer*, Singapore.**2021** ,169-177.

9. Ernawan, F.; Ariatmanto, D.; Firdaus, A. An Improved Image Watermarking by Modifying Selected DWT-DCT Coefficients. IEEE Access, **2021,** *9*, 45474-45485.

10. Varghese, J.; Razak, T. A.; Hussain, O. B.; Subash, S. A Hybrid Digital Image Watermarking Scheme Incorporating DWT, DFT, DCT and SVD Transformations. *Journal of Engineering Research*, **2021**.

11. Zainol, Z.; Teh, J. S.; Alawida, M. An FPP-resistant SVD-based image watermarking scheme based on chaotic control. *Alexandria Engineering Journal*. **2021.**

12. Lydia, E. L.; Raj, J. S.; Pandi Selvam, R.; Elhoseny, M.; Shankar, K. Application of discrete transforms with selective coefficients for blind image watermarking. Transactions on Emerging Telecommunications Technologies, **2021,***32(2)*, e3771.

13. Sisaudia, V.; Vishwakarma, V. P. Copyright protection using KELM-PSO based multi-spectral image watermarking in DCT domain with local texture information based selection. *Multimedia Tools and Applications*, **2021,** *80(6),* 8667-8688.

14. Amine, K.; Fares, K.; Redouane, K. M.; Salah, E. Medical Image Watermarking for Telemedicine Application Security. *Journal of Circuits, Systems and Computers*, **2021,** 2250097.

15. Khare, P.; Srivastava, V. K. A Novel Dual Image Watermarking Technique Using Homomorphic Transform and DWT. *Journal of Intelligent Systems,* **2021,***30(1),* 297-311.