Available online at
www.mdl.mazedan.com

MCET

www.mazedan.com

©2021 Mazedan International Research Academy

www.mazedan.com/mcet

COPYRIGHT PROTECTION IN INSECURE COMMUNICATION CHANNELS USING A ROBUST DIGITAL PICTURE WATERMARK

MAZEDAN COMPUTER ENGINEERING TRANSACTIONS
e-ISSN: 2583-0414
Article id: MCET0201004
Vol.-2, Issue-1
Received: 09 Mar 2021
Revised: 25 May 2021
Accepted: 8 Jun 2021

LAKSHMAN JI*, SHIV KUMAR, VARSHA NAMDEO

Citation: Lakshman, J., Kumar, S. & Namdeo, V. (2021). Copyright protection in insecure communication channels using a robust digital picture watermark. *Mazedan Computer Engineering Transactions*, 2(1), 21-29.

Abstract

With the transition from analogue to digital technology, worries about the security and authenticity of digital material and data have grown. Owners of any type of digital material seek out and experiment with innovative copyright multimedia content protection solutions. In recent years, multimedia protection has become a challenge, and researchers are still looking for and testing new and more effective methods to solve the problem. This thesis project aims to improve the visibility and intensity of invisible watermarking in a typical aeroplane using multilayer Discrete Wavelet Transform (DWT) and embed two marks in the image for verification and copyright purposes. When unprotected digital material flows across an unsecured channel Based on five active locations and the usage of two marks, a new watermarking method has been suggested. Marketing pictures will be included in the assault test set, in addition to the extraction procedure. The test technique was used to evaluate the value of SNR, PNSR, MAE, and RMSE in both viewing and post-attack pictures, as well as the invisibility of watermarking before and after the assault. Our lab results demonstrate that our pictures are both SNR and PNSR valuable, with excellent durability and quality.

Keys words- Invisible watermarking, copyright protection, and digital picture watermarking are all terms used to describe the discrete Wavelet Transform

1. INTRODUCTION

In our contemporary lives, our reliance on information and communication technology (ICT) is gradually increasing, and this rising demand for ICT can have a beneficial or bad impact on our lives in a variety of ways. As a result, moving digital media over secure networks like the Internet or private networks like Local Area Networks (LAN), Personal Area Networks (PAN), and Wide Area Networks (WAN) is difficult. To strengthen copyright protection and copyright enforcement, proving ownership of digital multimedia transfers necessitates the use of a strong watermarking system (Gitanjali Verma, 2015). Various academics have developed and presented a number of solutions. Watermarking, on the other hand, is the most well-known and widely used method. Watermarking is the method of embedding information directly into multimedia content using a key that specifies the placement of the watermark. Researchers have created a variety of hospitality programmes and ways to solve this issue (Tao & Eskiciolu, 2015). The major aspects are as follows: Transparency, strength, and high power are all qualities that may be found in a person. The parallelism between the original data and the marked data is what is meant by "transparent display." The original data quality will not be compromised if a mark or mark is introduced to fulfil this criterion (Tao & Eskiciolu, 2015). Consistency refers to the degree to which a mark's correctness can be assessed after it has gone through specific mark processing operations. The length of time it takes to mark anything is determined on the system used. While picture rigidity against channel transmission is necessary in the publishing control application, it is not in the reproduction prevention programme (K. Magai, 2005). The quantity of data that can be saved in actual data is defined as power. The application for strength determines the strength required. For instance, one object's symbol.In most cases, this is enough to inhibit reproduction. For some applications, such as fingerprints, the volume must be around 60-70 bits. It has been demonstrated in several research that techniques of representing space are frequently more successful than other approaches. As a result, this idea will only look at common space techniques. Modifying the proper conversion coefficients results in the creation of a watermark in the common space (R. Sugihara et al, 2001). After that, the labelled picture is given the opposite transition. As more markings are placed, the frequency of the entire image in pixel space will rise. It lasts longer than the markings used in the pixel space after using the opposite version. The most often utilised spaces are DFT, DCT, DWT, and CWT. For the Discrete Wavelet Transform, there exist quicker algorithms (DWT). DWT also has a power compression function that is favourable. DWT has been utilised to address various image processing difficulties as a result of these two properties. In a nutshell, the wavelet transformation divides a picture into numerous

Department of Computer Science and Engineering, Sarvepalli Radhakrishanan University, Bhopal, Madhya Pradesh 462026 India
Corresponding author email- lkshmanji@gmail.com

components that are separated by specific waves (Satik and Sujatha, 2012).

Digital Watermarking

Digital multimedia technology has advanced considerably in recent decades as a result of the widespread usage of this technology on the Internet. The fast advancement and efficiency of multimedia technology has resulted in significant changes, as well as several obstacles for users in gaining access to their material. Copyright protection, standard multimedia security, and multimedia content verification are all threats to using multimedia technology. Copyright protection, on the other hand, is one of the most serious threats to multimedia material (Barni, M., 2001). Operators employ digital watermarking as one of their tactics for protecting their data and avoiding copyright problems. The technique of watermarking encrypts a secret code or signal to protect it from copyright infringement and authentication (Langelaar and Gerhard C., 2000). The code is inserted in such a way that it does not degrade the content's quality while still keeping it secure. Copyright or authentication codes are placed in the data to create digital watermarks. Until the material is sent to a certain detector to obtain the code, this code is invisible to digital content (Zhang, W. et al., 2004).

Requirements for watermarking still pictures

Depending on the nature and security of digital material, a variety of watermark techniques or applications exist. Depending on where it was created, each watermarking method or application has its unique set of criteria. Although the entire process of watermarking and programming cannot be investigated, variety must be considered. During the watermarking process, there are a variety of conditions that must be satisfied (Pu, Y., et al., 2004). The following are some of them:

a. Robustness: The watermarking technique should be resistant to a variety of assaults, such as the mark inside the cover picture not being readily erased. Alternatively, the cost of distortion of the covered pictures should be used to compensate for the loss of the mark.

b. Inadequate watermarking When the conversion is performed to the cover picture, a portion of the marker or logo is removed, which improves the watermarking algorithm's strength.

c. Transparency To incorporate a mark that does not impact the display of cover pictures, a watermarking algorithm procedure is necessary.

d. Power: Power is the quantity of data that a picture may carry to be included; the more power accessible, the more powerful the algorithm; nevertheless, this should not result in a loss of quality or resilience of these algorithms.

Water Marketing Strategy Classification

The technique of embedding data or an image (known as a sign or symbol) into a digital item such as a multimedia file is known as watermarking. The same watermarking method employed in the embedding phase can be modified to remove or acquire this symbol or logo over time. This emblem or logo, known as a cover photo or original images, is created using a host image. A watermarking procedure is just a method of embedding a mark or brand into a cover picture to protect the image's copyright.

One of the most essential criteria for strong watermark systems is that the mark or mark cannot be readily located or removed by attackers, and that the mark or mark inside the cover picture is less vulnerable to external attacks. Watermarking techniques are classified based on the various methods used to process the standardised or modified form of the embedded process, such as the active domain, the type of tag or logo used, and the cover image used; they can also be classified based on human perception and any applications used (THN Le, et al., 2010). Furthermore, imperceptible watermarking, also known as invisible watermarking, is a type of watermarking that is not apparent to the naked eye includes a variety of watermark techniques that cannot be seen physically, such as a marker or logo. The logo or logo cannot be erased without the use of specific software, such as watermarking utilising DCT and DWT methods. Invisible watermarking can either be strong or weak. The phrase "robust watermarking" refers to the fact that the embedded tag or logo causes a pixel bit shift that cannot be detected. Furthermore, only suitable translation equipment should be used throughout the extraction procedure (Petit Colas, F, 1999). While visual watermarking techniques cover a wide range of ways in which a mark or symbol is visible to the human eye, this method is now frequently utilised in media channels, such as logos (Swanson, M.D, 1998). According to recent study, invisible watermarking will be utilised as a backup to visible watermarking when utilising both visible and invisible watermarks (Amit Kumar, 2015). Other watermarking techniques can also be customized according to performance domain:

a. Local background methods, in which watermark techniques are utilised to embed a brand or logo on a cover picture by altering pixel properties inside the image itself, such as pixel fragments or pixel weight (THN Le et al., 2010). Many approaches have been employed in this area, including Least Significant Bits (LSB) techniques and SSM switching techniques. This is one of the most effective ways for concealing the mark; nevertheless, it might have a negative impact on normal image perception.

b. The most frequent domain approach is to apply a mark or logo to the cover image's spectral coefficients. The most commonly utilised algorithms in these categories have been the Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), and Singular Value Decomposition (SVD). Furthermore, several novel approaches based on merging these two or more methods, such as DCT and DWT or DWT and SVD, have been developed (T.H.N. Le, 2010). Because they employ the spectrum coefficients of the pixel bit change picture cover, linking local domain approaches with common domain strategies is frequently used these days.

This makes finding any embedded symbol or brand with the naked eye challenging, necessitating the employment of specialised equipment to locate or remove the mark or logo (Linlin Tang and Yu Tian, 2015).

Furthermore, according to certain research (THN Le et al., 2010), watermarking is classified as follows:

a. Blind watermarking: The detecting procedure in this sort of watermark technology does not require real data to extract a marker or mark. It has a large input field, but it requires advanced watermark technology and is time and money intensive.

b. Blurred watermarking: This sort of watermarking technique necessitates the capture of both an original picture and a logo or logo to complete the procedure.

c. Invisible watermarking: This form of watermark technique necessitates the capture of an actual picture, sign, or symbol in order to complete the detection process.

2. THE PROBLEM OF MARKETING STRATEGIES AND UNSAFE COMMUNICATION

When the owner wishes to transfer the item over an insecure communication channel (Mohammed ALSULTAN., Et al. 2017), watermarking technology is commonly employed in digital objects (I.J. Cox et al., 2001). To comprehend the nature of this transmission, we must first comprehend its carrier technique and its connection to the technical notion of watermark. The conventional data to which the message goes is depicted in Figure-1.

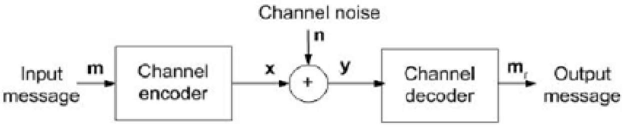

Figure 1 The conventional data

When going over an insecure communication channel, the message (m) appears as shown in the diagram above. We get a signal after the channel encoder (x). Because the message (m) may contain a set of audios (n) or attachments, the signal (x) transforms to a signal (y) (e.g. (X) signal and sound (n)). A receiver or decoder on the opposite side of the communication channel tries to determine the signal (y) and receive the first message (m). Each watermarking process may be represented as a signal communication system, with the message being sent from the embedding to the receiver/desktop [Cox J.; Miller, ML, 1999].

This issue degrades the watermark's quality, which might result in the watermark's full loss and, as a result, the loss of intellectual property rights. As you travel via hazardous intermedia, there are a variety of assaults that might disrupt your communication, and these threats are always changing. It's critical to improve the watermark algorithms so that they save more data than a watermark that operates on an unprotected channel. More information and debate regarding the idea's detractors will be found in the next section.

Classification of Attacks: Images sent through insecure intermedia can be subjected to a variety of assaults. The following are the different types of attacks: (Voloshynovskiy, S. et al., 2001)

a. Cruel Attack: By fooling the specifics of a certain algorithm, this attack generally tries to erase or make a watermark from the covered photos incorrect. Re-scanning, reproducing, and recreating watermarks are some examples.

b. Harmless attacks: Any attack that does not target the host's fundamental information or the watermark details while the attacker tries to influence the watermark through other image structures is deemed harmless. Pressure assaults, as well as common signal processing procedures like A/D modification, D/A conversion, quantization duplication, and re-sampling, are examples.

c. Removing an assault: This is the same as removing a violent attack. The attacker here is attempting to entirely erase the watermarking without misleading the intricacies of any specific technique. Noise reduction, quantization, co-attack, and power reset are some examples.

d. Geometric Assault: This form of attack tries to reverse the watermark removal process, making it impossible to remove the watermark once it has been put. A dynamic backdrop, local shifts, and affine conversions are all examples.

e. Cryptographic Attack: This sort of attack tries to undermine the security mechanisms in watermarking algorithms so that harmful information can be embedded or watermarking can be removed. A thorough search for information is one example.

f. Assault Protocol: This attack tries to capture the whole idea of watermarking techniques. An inescapable assault, in which the attacker tries to seize control of the watermark picture itself, is one example.

3. PREVIOUS RELATED ACTIVITIES

Previous research is split into three sections: investigative investigations, algorithm integration studies, and multi-level DWT studies, all of which are addressed in the sub-sections below.

Investigation Studies

According to Signature (2015), the development of Internet technologies has made copyright protection and verification a challenge. Digital watermarking has long been used to safeguard digital information from copyright problems. The author evaluated the benefits and downsides of different watermarking techniques on web material, as well as HTML and XML approaches.

Watermarking approaches that are both new and resilient should be devised and deployed. The rules for this will be syntactic and semantic. With a robust cryptographic technique and the usage of SALT, these approaches will secure the watermark. In addition, the watermark will be rendered undetectable. The CA's duty is to determine the authorised author of any digital material since the original author is registered with the CA, and the CA will determine the content creator in the case of illegal access or assault. This technique, however, may be utilised in any web language, including HTML, XML, and other comparable services.

Image watermarking has grown increasingly popular in recent years, according to Panchal and Srivastava (2015), due to the increased usage of the Internet and multimedia over the Web. Adding features to an image capture in the form of a logo or text is also known as picture watermarking. Copyright protection, content verification, data integrity, and picture identification are the primary goals of image watermarking. Watermarking, on the other hand, isn't only about copyright protection; it's also about confirming and identifying the owner.

Watermarking, according to the authors, requires durability, strength, great visibility, and security to function successfully. Watermarking techniques based on local domains are simple, can handle a high number of bits, and are relatively easy to implement. Watermarking techniques created using a frequency converter, on the other hand, are resistant to assaults but can't be incorporated in a significant number of bits due to the poor-quality level. As a result, the authors recommend that these approaches be used in high-power local domain strategies.

Integrated studies of algorithms

According to Jane and Elbaş (2013), the field's literature highlights embedding methods, which are extensively utilised to safeguard and protect copyright. Because of the separation of frequency components, the Discrete Wavelet Transform is frequently utilised in various watermarking approaches. In addition, the watermarking business uses Singular Value (SVD) and Lower and Upper (LU) rot. As a result, the authors have suggested a new combination of DWT and SVD based on the LU decay of the watermark method, which needs the detection of the watermark using the cover function. The findings demonstrate that this algorithm is both powerful and dependable when it comes to attacks. Furthermore, the method protects against assault by incorporating a binary watermark. on a very low bandwidth.

According to Malakooti et al (2013), searching for digital pictures from a large number of sources using image content rather than metadata is more challenging. Furthermore, the search results for many techniques are excellent; nonetheless, many pictures other than the target image are present. The authors present a novel image identification technique based on the Wavelet Transform and Singular Value Decomposition (SVD) that can recover a large number of pictures, including the target image. DWT is used in this fashion to transmit pictures from a local domain to a common domain that is split into four sub-bands. On the third step, three layers of 2D DWT were utilised to concentrate the picture components. To extract it, SVD is utilised. values that are unique.

A robust digital video watching technique based on DWT and SVD with a central filtering function was proposed by Kaur and Jindal (2014). As a result, the initial picture is passed through a central filter function to smooth it out, and then the first level of DWT is applied. In addition, the high frequency spectrum is employed for embedding.

DWT Courses with Multiple Levels

To tackle the copyright issue, Sharma and Jain (2014) proposed that copyright protection by watermarking should be evaluated for durability and invisibility over time. The fundamental aims of any DWT watermarking process are stability and invisibility, and these goals must be met in order to maintain the security of digital media. The authors suggest a hybrid transform method that comprises altering the cover picture and transforming it to individual values instead of DWT sub-bands. As a result, the watermark becomes susceptible to many sorts of assaults. Furthermore, according to the findings of this study, the hybrid modification procedure can increase visibility and durability in order to prevent assaults. For academics, data security has long been a key worry.

At the second level of DWT decay, Tao and Eskiolu (2015) added the notion of embedding a binary pattern in the form of a binary picture on the LL and HH bands. They compared watermark embedding at the first and second decay stages using all four bands. Because a watermark is embedded on low frequencies, the suggested technique is effective in resisting repeated assaults. Watermarking digital material at high frequencies protects it from other attack techniques. The authors' tests demonstrate that first-degree decay has a significant benefit since the watermark embedding area is increased and the watermark extensions are textural and have higher viewing quality.

Ammar Jameel Hussein et al. (2015) devised a unique approach based on the location of a strong binary cover picture and a 4-level DWT algorithm. They used two distinct DWT standards to create two watermark logs and advocated these algorithms for authenticity and copyright protection. They used 5-level DWT on the cover image to find the binary value of the low frequency (LL5), as well as to test the dynamic binary value of the selected area for the purpose of embedding in five different locations in the capture image using the same algorithm in the proposed watermarking algorithm. The results of the tests demonstrate that this algorithm system is undetectable and resistant to various image attacks. PSNR and SNR calculations are used to evaluate the quality of watermark images.

4. ALGORITHM AND TESTING SUGGESTIONS

In this part, we'll go through the suggested watermarking method, which uses two tagging pictures as watermarking and is based on the five places on the cover image. The first watermark should be placed in two places (LL2 and LL4), whereas the second watermark should be placed in three places (LL1, LL3, and LL5).

translates the unity value of the watermark to the original image Although there are many alternative methods for doing watermarking, this approach may assure the watermark's robustness against assault when compared to other methods.

The most essential criteria for copyright protection, according to Gunjal and Mali (2014), are strong, strong, and high embedding capabilities, as well as digital picture watermarking approaches. The authors used a non-blind method of presenting digital images to achieve these aims. DWT, DWT Fast Walse-Hadamard, and DWT Fast Walse-Hadamard were used by the authors to assess the effectiveness of this method. Domains of Transform and Singular Value Decomposition The authors argue that, as compared to the DWT domain, the DWT-FWHT-SVD domain may meet the goal of improved comprehending comprehension after using this technique. As a consequence, the findings of the DWT-FWHT-SVD domain show that these approaches can outperform other DWT and DWT-SVD strategies in a range of assaults.

Processing Process

Gives us a watermarked image LW (i, j) 512 × 512 in size) as our computerized images using the following mathematical calculations (512 × 512 in size) as a result for watermarking processor, this will be the first image with watermark, and LW2 (i, j) (512 × 512 in size) will be the second image with watermark. As a result, summary

in them gives us a watermarked image LW (i, j) 512 × 512 in size) as our computerized images using the following mathematical calculations:

We suppose we obtain the LW1 I j) image as the first watermark image and W2 I j) as the second watermark picture.

$$LW1\ (i, j) = IM\ (i, j) + W1\ (i, j) \qquad (1)$$

$$LW2\ (i, j) = IM\ (i, j) + W2\ (i, j) \qquad (2)$$

$$LW\ (i, j) = (LW1\ (i, j) + LW2\ (i, j)) / 2 \qquad (3)$$

Extract Process

Assuming we have an IM I j) (512 × 512 in size) picture as our cover image and a watermarking image LW I j), we can generate the first watermark image LW1 and the second watermark image LW2 using the following arithmetic statistics:

$$LW1 = IM\ (i, j) – LW\ (i, j) \qquad (4)$$

$$LW2 = IM\ (i, j) – LW\ (i, j) \qquad (5)$$

Figure 2 depicts the total performance of the suggested methods, which includes the embedding, extraction, application of attack sets, and testing processes.

Laboratory Testing

Our laboratory is built with MATLAB code, and our suggested methods in Figure 13 are implemented with a single piece of system code to assure quality and efficiency. We used a range of 512 × 512 standard image scanner pictures to test our suggested algorithms, including Lena, Muhammad Ali, Girl face, Zelda, Sailing boat, Lighthouse, Cameraman, Gold hill, Barbara, and others. In addition, as a watermark logo, we employed a range of 512 × 512 picture sizes. After the embedding procedure, Table 1 displays the five test pictures and the liquid images. Table 2 indicates which log was utilised.

Table 1 Test Images Along with Watermarked Image after Embedded Process

Image Name	Cover Image	Watermarked
Lena		
Girl face		
Muhammad Ali		
Zelda		
Sailing boat		

Table 2 Watermark Logo Used in Our Lab

Logo Number	Logo Images
1	**LA**
2	**BC**

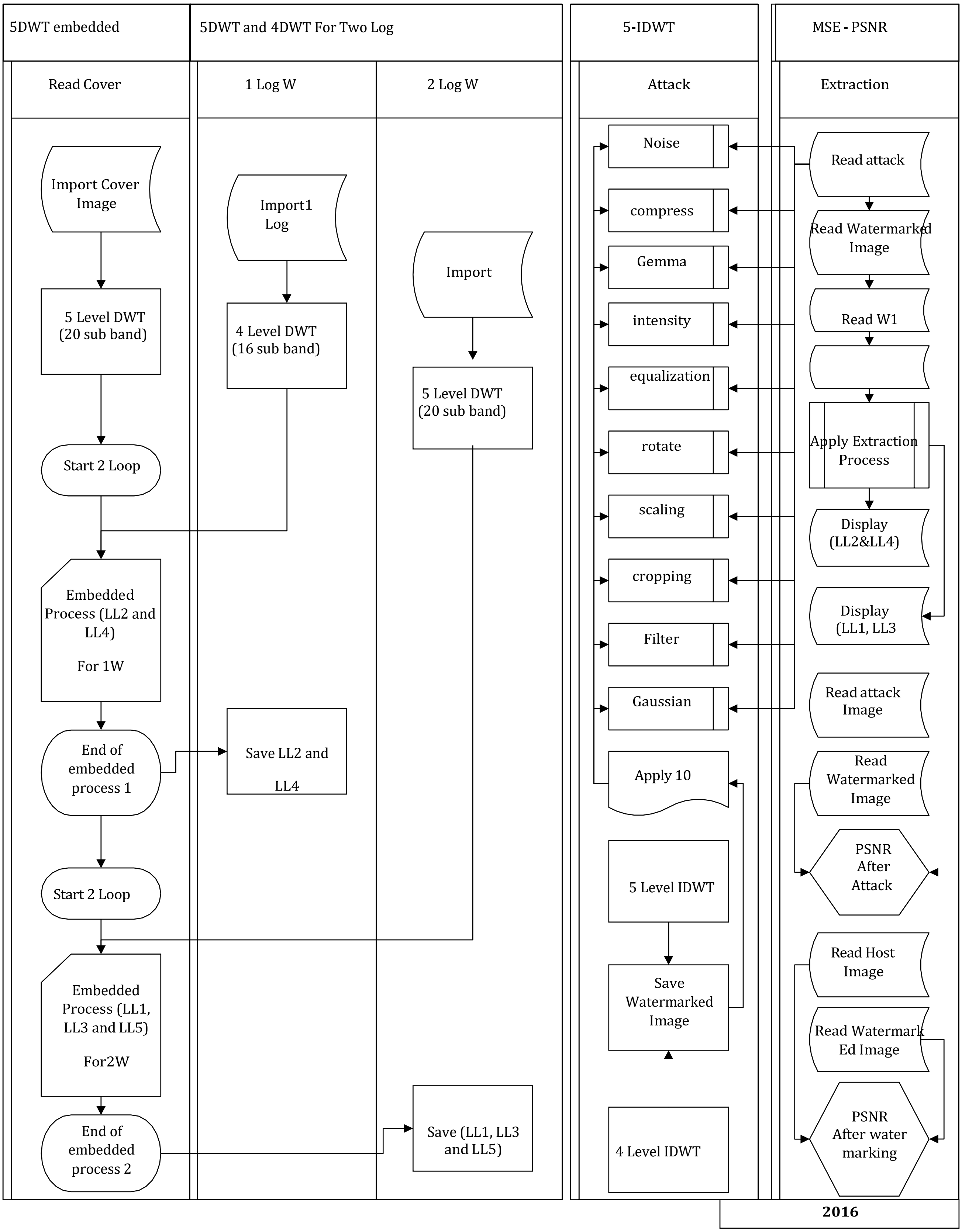

Figure 2 Overall proposed algorithm

Attack Test

Using the MATLAB environment, we conducted several sorts of assaults to a picture with a watermark to evaluate the resilience of our lab technique. Repetitive assaults, circular attacks, equality attacks, uneven adjustment attacks, Gaussia attacks, clashes, noise attacks, low pass attacks, and gamma attacks are all examples of these types of attacks. Table 3 shows the attack parameters used in our lab and the watermark image after the assault for Lana's image, while Table 4 shows the attack parameters used in our lab and the watermark image after the attack for the Girl's face picture.

Table 3 Watermark Image after Attacks (Lana)

No.	Name	Parameters	Result Image
1.	Watermarked Image	2 Logo	
2.	Gaussian noise	Mean=0Vari ance=0.001	
3.	Low Pass Filtering	Window Size=3×3	
4.	Cropping	On bothsides	
5.	Scaling	512×256	
6.	Rotation	20°	
7.	Equalization	Automatic	
8.	Adjustment	[l=0 h=0.8][b=0 t=1]	
9.	Gamma	1.5	
10.	JPEG Compression	Q=75	
11.	Noise	0.02	

Table 4 Watermark Image after Attacks (Girl Face)

No.	Name	Parameters	Result Image
1.	Watermarked Image		
2.	Gaussian noise	Mean=0 Variance=0. 001	
3.	Low Pass Filtering	(Window Size=3×3)	
4.	Cropping	On bothsides	
5.	Scaling	512×256	
6.	Rotation	20°	
7.	Equalization	Automatic	
8.	Adjustment	[l=0 h=0.8][b=0 t=1]	
9.	Gamma	1.5	
10.	Compression	Q=75	
11.	Noise	(0.02)	

Evaluation Process

In our lab, we evaluated the proposed watermark algorithms by measuring the PSNR, SNR, MAE and RMSE. J's plugin (2016) was used for the evaluation process. This program calculates the PSNR, SNR, MAE and RMSE of the tested images being contingent with the definitions produced by Gonzalez and Woods (2008). The plugin compared a reference image IM (i,j) with a target test image T(i,j). The two images should have the same size of [ni,nj]. The PSNR, SNR, MAE and RMSE are calculated with the given equations:

Peak signal-to-noise ratio (PSNR)

$$PSNR = 20\log_{10}\left(\frac{MAX_f}{\sqrt{MSE}}\right) \quad (1)$$

where the MSE (Mean Squared Error) is:

$$MSE = \frac{1}{mn}\sum_{0}^{m-1}\sum_{0}^{n-1}\|f(i,j) - g(i,j)\|^2 \quad (2)$$

Signal-to-noise ratio (SNR

SNRVoltage=1N∑Ni=1(P2PUp)
i1N′∑N′j=1(STDDown)j

Mean absolute error (MAE)

$$\mathrm{MAE} = \frac{1}{n}\sum_{i=1}^{n} |\boldsymbol{x}_i - \boldsymbol{x}| \qquad (3)$$

n = the number of errors,

Σ = summation symbol (which means “add them all up”),

|xi – x| = the absolute errors

Root mean square error (RMSE)

$$RMS\sqrt{\frac{1}{Ni.Nj}.\sum_{0}^{Ni-1}\sum_{0}^{Nj-1}[IM(i,j)-T(i,j)]^{2}}$$

In our lab, we tested many standard images process test images. Afterwards, we applied our proposed algorithms and a set of attacks. Every test process was applied two times: first, we took the cover image as a reference image; then, we took the watermark image as a reference image. The PSNR, SNR, MAE and RMSE obtained the values shown in Tables 5(a) and (b), Tables 6 (a) and (b), and Tables 7 (a) and (b).

Table 5

Test Image	SNR	PSNR	RMSE	MAE
Wimage.png	49.38	52.76	0.59	0.34
Gaussia.png	26.59	29.97	8.09	6.45
Filter.png	25.20	28.58	9.49	4.02
crop.png	5.57	8.95	91.00	43.35
Resize.png	25.81	29.19	8.85	4.17
Rotate.png	5.56	8.94	91.11	62.27
Equal.png	11.71	15.09	44.87	39.24
Intensit.png	13.03	16.41	38.55	36.26
Gamma.png	16.42	19.79	26.11	24.97
Hostr75.jpg	46.99	50.37	0.77	0.49

Table 6

Test Image	SNR	PSNR	RMSE	MAE
Gaussia.png	26.63	29.99	8.07	6.43
Filter.png	25.20	28.56	9.52	3.94
crop.png	5.55	8.92	91.35	43.39
Resize.png	25.85	29.21	8.83	4.07
Rotate.png	5.56	8.92	91.29	62.36
Equal.png	11.67	15.03	45.20	39.52
Intensit.png	13.12	16.48	38.24	35.91
Gamma.png	16.32	19.68	26.45	25.31
Hostr75.jpg	50.41	53.77	0.52	0.24
Noise.png	18.47	21.83	20.65	2.57

Extraction after Attack: We put our suggested methods to the test in our lab by visually analysing the watermark logo before and after an attack on the MATLAB platform. Using the Muhammad Ali watermarked picture and Logos 3 and 4 in Table 3, Table.8 shows the extraction of the watermark logo before and after an assault (for the original watermarked image, Gaussian, filter, Gamma, Cropping, and Equalization).

5. CONCLUSION

We covered the relevance of digital watermarking, watermark requirements for still pictures, and the most common application area for watermarking approaches throughout this research. In addition, we divided watermarking attacking techniques into groups and explored the link between watermarking attacking strategies and the problem of hazardous communication. In addition, we reviewed relevant work and analysed prior studies on our issue done by a variety of academics, which we categorised into three categories: research studies, integrated algorithms studies, and DWT multi-level investigations.

Furthermore, we created watermarking algorithms based on five places on the cover picture utilising two tagged photos. The first watermelon recommended that it be placed in two places (LL2 and LL4), whereas the second watermark was placed in three places (LL1, LL3 and LL5). We also spoke about how the extraction process worked, and how liquid pictures were subjected to a series of attack tests. The test technique consisted of comparing the values of SNR, PNSR, MAE, and RMSE for watermark pictures taken before and after the assault. Our findings demonstrate that the high-quality pictures produced by our algorithms are reflected by the greatest SNR and PNSR values, outperforming earlier research by Ammar Jameel et al (2015). Furthermore, our suggested methods are very resistant to a variety of assaults, including Compression, Gaussian, Filter, Gamma, Cropping, Resize, Noise Equalization, and so on.

and a rotational assault Our watermark emblem contained in the recorded photos was unaffected by this assault. As a result, we can infer that our suggested algorithm may successfully contribute to the preservation of intellectual property rights and the enhancement of digital asset ownership when travelling via secure channels. The following are some ideas for future projects:

a. Proposing novel watermark methods to increase the amount of data that can be encoded in the hosting picture;

b. Maintaining transparent visibility that does not affect the visibility of capture images when embedding multiple details;

c. Suggesting new watermark techniques that offer better value based on image quality by getting higher SNR and PNSR values;

d. Improving the robustness of a watermark; f. Suggest a powerful new location within the host image to embed more details.

REFERENCES

[1] Amit Kumar Singh. Robust and Imperceptible Dual Watermarking for Telemedicine Applications.

[2] *Wireless Personal Communications*. 2015; 80(4): 1415-1433.

[3] Ammar Jameel, Seda Yüksel, Ersin Elbaşı. Dynamic Binary Location based Multi-watermark Embedding Algorithm in DWT” (Improved). *Journal of Theoretical and Applied Information Technology 20th*, 2015; 78(2).

[4] Barni M, Bartolini F, Cox IJ, Hernandez J, Perez-Gonzalez F. Digital Watermarking for Copyright

Protection: A Communications Perspective. *IEEE Communications Magazine*. August 2001; 39(8): 90-133.

[5] Cox IJ; Miller ML; McKellips AL. *Watermarking as Communications with side Information*. Proceedings of the IEEE. July 1999; 87(7): 1127-1141.

[6] Cox IJ, Kilian J, Leighton T & Shamoon T. Secure Spread Spectrum Watermarking for Multimedia.

[7] *IEEE transactions on image processing*. 1997; 6(12): 1673-1687.

[8] Gunjal BL & Mali SN. Comparative Performance Analysis of Digital Image Watermarking Scheme in DWT and DWT-FWHT-SVD domains. *Annual IEEE India Conference*. 2014.

[9] Hu Y & Jong CC. (), A memory efficient High-Throughput Architecture for Lifting-Based Multi-Level 2D DWT, *IEEE Transactions on Signal Processing*. 2013; 61(20): 4975-4987.

[10] Image plugin to assess the quality of images, Written by Daniel Sage at the Biomedical Image Group, EPFL, Switzerland. Available at: http://bigwww.epfl.ch/

[11] J Cox, ML Miller, JA Bloom. Digital Watermarking. Morgan Kaufmann, 2001.

[12] JY Stein, Digital Signal Processing: A Computer Science Perspective. New York: Wiley. 2000.

[13] K Magai, H Ito, H Mishima, M Suzuki, K Asai. *Watermarking Robust Against Analog VCR Recording*. Image Processing, 2004. ICIP ’04. 2004 International Conference on 2004; 5

[14] Linlin Tang, Yu Tian, Jengshyang Pan, 2015. Applications of Cloud Model in Digital Watermarking. *Chapter Intelligent Data Analysis and Applications volume 370 Series Advances in IntelligentSystems and Computing*. 2015; 370: 371-379.

[15] Malakooti MV, Panah ZF & Hashemi SM. Image Recognition Method based on Discrete Wavelet Transformation (DWT) and Singular Value Decomposition (SVD), SDIWC. 2013: 42-47.

[16] Mohammed Alsultan, Thaer Alramli, Ammar Albayati, Ersin Elbasi. Hough Transform Based Watermark Embedding Algorithm in dct Frequency Domain. *Journal of Theoretical & Applied Information Technology*. 2017; 95(8).

[17] Panchal UH & Srivastava R. A Comprehensive Survey on Digital Image Watermarking techniques. *Fifth International Conference on Communication Systems and Network Technologies*. 2015: 591- 595.

[18] Petitcolas F, Anderson R, Kuhn M. *Information Hiding–a Survey*. Proc. of the IEEE. July 1999; 87(7): 1062-1078.

[19] Podar VM, Han S & Chang E. *A Survey of Digital Image Watermarking Techniques*. 3rd IEEE International Conference on Iindustrial Informatics. 2005: 709-716.

[20] Pu Y, et al. *A Public Adaptive Watermark Algorithm for Color Images Based on Principal Component Analysis of Generalized Hebb*. Proc. of IEEE Int. Conference on Information Acquisition. 2004: 690-695.

[21] R Sugihara et al. *Practical Capacity of Digital Watermark as Constrained by Reliability*. Information Technology: Coding and Computing, 2001. Proceedings. International IEEE Conference. 2001: 85- 89.

[22] RC Gonzalez, RE Woods. Digital Image Processing. 3rd ed., Prentice Hall, 2008.

[23] Saini S. *A Survey on Watermarking Web Contents for Protecting Copyright*. IEEE Sponsored 2nd International conference on Innovations in Information Embedded and Communication Systems. 2015

[24] Sathik MM & Sujatha SS. A Novel DWT Based Invisible Watermarking Technique for Digital Images. *International Arab Journal of e-Technology*. 2012; 02(03): 167-173.

[25] Sharma P & Jain T. Robust Digital Watermarking for Colored Images Using SVD and DWT Techniques. *IEEE*. 2014: 1024-1027.

[26] Swanson MD, Kobayashi M, Tewfik AH. *Multimedia Data-Embedding and Watermarking Technologies*. Proc. of the IEEE. June 1998; 86(6): 1064-1087.

[27] THN Le, KH Nguyen; HB Le. *Literature Survey on Image Watermarking Tools, Watermark Attacks and Benchmarking Tools*. Advances in Multimedia (MMEDIA), 2010, Second International