Bulletin of Electrical Engineering and Informatics
Vol. 13, No. 3, June 2024, pp. 1877~1896
ISSN: 2302-9285, DOI: 10.11591/eei.v13i3.6337

A hybrid steganography and watermark algorithm for copyright protection by using multiple embedding approaches

Nasharuddin Zainal[1], Alaa Rishek Hoshi[1], Mahamod Ismail[1], Abd Al-Razak T. Rahem[2], Salim Muhsin Wadi[3]

[1]Department of Electrical, Electronic, and Systems Engineering, Faculty of Engineering and Built Environment, Universiti Kebangsaan Malaysia, Bangi, Malaysia
[2]Department Electrical Engineering Technical College, Middle Technical University, Baghdad, Iraq
[3]Department Communication Techniques Engineering, Al-Furat Al-Awsat Technical University, Najaf, Iraq

Article Info

Article history:

Received Mar 28, 2023
Revised Jul 13, 2023
Accepted Aug 30, 2023

Keywords:

Copyright protection
Discrete cosine transform
Discrete wavelet transform
One-time pad
Playfair
Steganography
Watermarking

ABSTRACT

In this modern era, it has become much simpler to replicate, sell, and copy the copyright owners' works without their permission as a result of the expansion of digitalization, and it is difficult to identify such violations, posing a threat to the creators' and copyright owners' rights. For many years, the internet has been regarded as one of the most serious threats to copyright, and the content available has varying levels of copyright protection. On the internet, there are numerous copyrighted works, including e-books, movies, news, and so on. Therefore, by using watermarking and steganography techniques, these issues can be solved, which are based on the author's signature information or logo. This paper concluded that the techniques of discrete cosine transform (DCT), discrete wavelet transform (DWT), one-time pad (OTP), and playfair are highly effective when used together to watermark an image or embed a secret message, our lab results validate that our algorithm scheme is robust against several sets of attacks, where the algorithm was assessed by computation of many evaluation metrics such as mean square error (MSE), signal-to-noise ratio (SNR), and peak signal-to-noise ratio (PSNR).

This is an open access article under the CC BY-SA license.

Corresponding Author:

Alaa Rishek Hoshi
Department of Electrical, Electronic, and Systems Engineering
Faculty of Engineering and Built Environment, Universiti Kebangsaan Malaysia
43600 UKM, 43600 Bangi, Selangor, Malaysia
Email: alaa.wn@gmail.com

1. INTRODUCTION

Digital distribution of documents over open channels through information and communication technology (ICT) is considered to be a cost-effective and indispensable technique for the distribution and dissemination of digital media files. Nevertheless, ownership identification, prevention of copyright violation, and identity have been major challenges because of hacking of information channels and attempts of malicious attacks. The key objective behind attacks is to delete or modify and change the document watermark to prevent the information transfer to a receiver or claiming illegal ownership. Hence, addressing such challenges remains an interesting problem for scholars [1].

Over the past few decades, the advancement in science has introduced several branches used for securing secret communication, including steganography, watermarking, and cryptography. Data delivery via public media like online mediums (e.g., the internet) leads to the chances of data manipulation and theft. Hence, this science is developed from the perspective of the need for security. Watermarking and steganography are common techniques are hiding or protecting secreting messages in a cover file [2]. It is believed that the significance of securing digital data is high, and one way to maintain its security is to use digital watermarking and steganography techniques. This is especially suitable for different multimedia data, like video files, audio recordings, and images. Concealing information using digital watermark embedding and steganography is an established and developing scientific field [3].

Nevertheless, the difference between the two is the purpose, as watermarking looks to protect the copyright, whereas steganography hides the messages. Normally, human senses cannot detect messages, so it is challenging to differentiate between the original or normal data involving the message or file [4]. On the other hand, cryptography works to change the message or file to an irregular one to make it look damaged. There are two kinds of domains normally applied in steganography, spatial domain, and namely domain transformation [5], [6]. Domain transformation is beneficial in spreading the message to the whole file cover, while on the contrary, spatial domains work best in simpler operations. Discrete wavelet transform (DWT) and discrete cosine transform (DCT) are the highly popular transformation domains in steganography [7]-[9]. DCT has potential in computing and compact energy and is comparatively quicker than DWT, while DWT, on the other hand, is an algorithm with comparatively low resistance alteration and error rate [7], [10].

Another importance of DCT is its application as the standard transformation of DWT and joint photographic experts group (JPEG) as a normal alteration of JPEG 2000 [11]. Several types of research [12]-[14] showed that the amalgamation of this transformation in a steganography scheme could be more improved. Others including [15]-[17], associate steganographic and cryptography techniques to improve the security of private messages. There are different cryptographic techniques, including one time pad (OTP), advanced encryption standard (AES), rivest-shamir-adleman (RSA), data encryption standard (DES), and blowfish [16], [18], [19]. OTP is a technique that is simplest and managed per block in comparison to other techniques. OTP is a famous algorithm normally applied via cryptographic techniques. It is a part of a symmetric cryptographic algorithms group where a single key is used for decryption and encryption [20], [21].

Emphasizing steganography, it is discussed that steganography comprises the protection of a few additional pieces of information inserted in digitally protected objects. The cover object and the information itself can both be different digital objectives. The key concept of steganographic methods is to make embedded information secure against an attacker. The secret information due to this statement could be transmitted safely via open communication channels as the receiver and sender will know its existence in a transmitted over the objective [3]. Hybrid and blind steganographic processes can increase the security of steganography as private information can be retrieved from the stego-image [22]. Empirically, there are studies, which use used steganography techniques for a color image. For example, Thanki *et al.* [23], in their study, proposed a steganography technique based on DWT and finite ridgelet transform (FRT) for securing secret color images for securing the secret image in a color image. It is known that this technique is hybrid, and it satisfies the security needs of color image alteration over communication medium by enabling high entrenching capacity and giving high security and safety for a color image. This technique, as proposed by the scholars with comparable with previous techniques concerning different features. However, it is observed after comparison that this technique using DWT and FRT performs exceptionally well compared to other techniques in relation to hiding capacity and imperceptibility.

Likewise, Thanki and Borra [24] proposed a color image steganography centered on DWT and FRT. The FRT is used on the cover color image to attain ridgelet constants of the color image, and a DWT was used to acquire various wavelet constants, which were further changed by coded channel values of a secret color image to acquire a stego-color image.

According to Borra *et al.* [25], color images are used in different social media sites, including Instagram, WhatsApp, and Facebook. These images are moved from one server, network, or computer to another via open networks like wireless networks and the internet, in which they can face different attacks and manipulations [26], [27]. In such circumstances, different techniques for securing color images have been proposed; for example, Phadikar *et al.* [28], put forward blind watermarking techniques based on wavelet transform for color image security. The binary logo in this technique is inserted in the wavelet sub-bands region of interest (ROI) of the color image. Eswaraiah and Reddy [29] recommended DCT and DWT focused on watermarking techniques for color image security in a similar context. Initially, a two-level DWT in this technique was used for the blue channel for the color image to acquire wavelet constants; later, to get DCT constants, DCT was used for LH2 sub-band coefficients.

Nevertheless, there is a lack of evidence to support that watermarking techniques can attain the required objective to recover the correct information from the data after different sorts of content-preserving manipulations. Due to reliability restraints, watermarks can be embedded only in a small space in multimedia data. In this case, a biased edge is always there for attackers to target and remove the watermarks by misusing different manipulations in the limited watermarking space. Different solutions are proposed, including watermarking, steganography, and cryptography; however, watermarking provides the best solution. In this reference, Thanki *et al*. [23] add that digital watermarking is applied in different applications like ownership authentication and copyright protection. The goal behind its application in copyright protection is to protect digital information over networks like communication channels and the internet.

2. WATERMARKING AND STEGANOGRAPHY TECHNIQUES

The attention of the researchers has been gained by the digital watermarking and steganography techniques because of their effective distribution of redundant information and availability. Digital content is protected by such techniques from manipulation and authorized access, and they are needed for distinct applications like trademark protection, authentication, material security, and operator acknowledgment [30]. Though watermarking and steganography are two distinct techniques, some of the similar qualities are shared by both for instance, the same model is followed by both techniques where two inputs go into an embedder. Also, steganographic methods are applied by both techniques for embedding data covertly within noisy signals. Thus, it could be stated that digital watermarking is itself one of the major techniques of steganography. The classification of digital watermarking techniques is grounded upon multi-media types (i.e., video, audio, or image), human perception (i.e., invisibility or visibility), working domain (i.e., hybrid, frequency, or spatial), application type (i.e., destination or source-based), an algorithm's nature (i.e., parallel or sequential).

Concerning working-domain, the spatial technique of watermarking is defined as a method in which watermark information is inserted into the host image, which an owner describes within the time or spatial domain with the help of distinct ways that include significant intermediate bits (ISB) algorithms, patchwork algorithms, and least significant bits (LSB) algorithms. Such techniques are directly applied to the original pixels of an image as the watermark is possible to be inserted through manipulating the values of the pixel, which is based upon signature information or logo given by the author. Spatial watermarking techniques have improved efficacy, rapid execution, and low complexity [31]. However, the paper of Begum and Uddin [30] explored that the techniques associated with spatial domain watermarking are easy to manipulate, and they are too fragile, which makes them lead strongly against distinct attack types in comparison with frequency-domain algorithms. This is why the focus of the researchers has drawn towards frequency domain watermarking techniques as they effectively hide data of a picture through a pre-defined transformation to show an image within the frequency domain. Then, the watermark is embedded with the help of altering the transform-domain coefficients of a picture by utilizing various transforms involving discrete fourier transform (DFT), singular value decomposition (SVD), DWT, and DCT as shown in Figure 1.

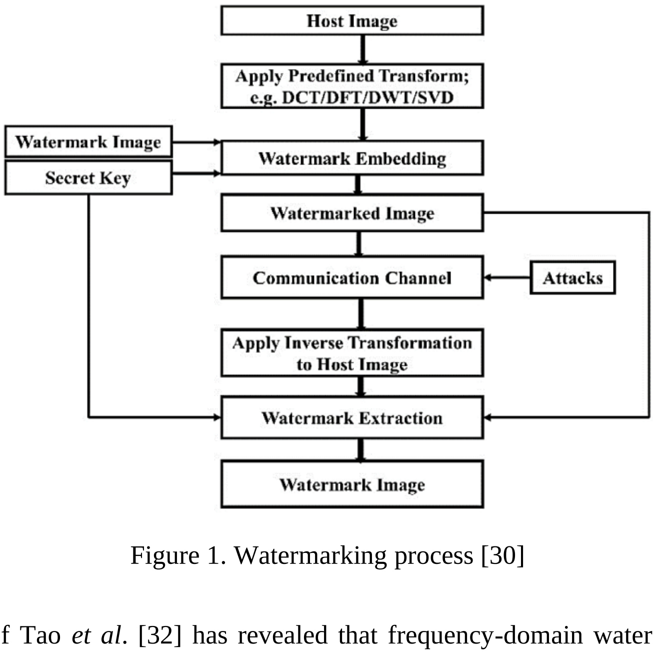


Figure 1. Watermarking process [30]

The research of Tao *et al*. [32] has revealed that frequency-domain watermarking provides better security, imperceptibility, and robustness against several attacks, for instance, cutting, rotation, compression, filtering, and noise. Moreover, the capability of hiding data and the frequency domain's computational capacity is greater than the spatial domain, which makes it more preferable. For this paper, two main techniques attached to frequency domain image watermarking are selected, i.e., DCT and DWT, which are then combined with two cryptographic techniques, which are (OTP) and Playfair to identify their impact on protecting copyright on social media.

2.1. Discrete cosine transform

DCT is a well-known kind of frequency-domain transformation. A digital image is divided into sine and cosine frequencies that contain dissimilar amplitudes. Because of such ability, this technique is mostly utilized in the field of data compression as well as pattern recognition [33]. Also, the digital image is transformed by DCT with the use of fourier transformation into frequencies' easy segments. The algorithm then splits the image into 8×8 non-overlying blocks, then embeds the hidden information into the image coefficients. With the help of this process, the data is represented by DCT in frequency space rather than within the amplitude space, which makes such a technique more robust compared to other operations of digital image processing, for example, filtering, contrast adjustments, and brightness. But, as per the study of Yadav *et al.* [34], they are computationally expensive as well as not easy to apply. Additionally, they are exposed to geometric attacks, which include rotation, cropping, and scaling. Despite various limitations, finite data point sequences are expressed by DCT at oscillating frequencies, making this technique very effective within distinct applications, such as plummeting network bandwidth, looking for solutions of incomplete differential equations, and digital signal processing [33].

When the watermark is embedded within an image using DCT, middle and low frequencies are taken as during the procedure of image compression, the disappearance of high frequencies is experienced. Utilizing DCT for image watermarking, the calculation of the DCT coefficient associated with the original image is performed. As Kulkarni *et al.* [35] discussed, after computing this, the watermark image's DCT coefficient is computed. Then, different values of Beta, as well as Alpha, are assigned towards this coefficient correspondingly. When the watermark image is embedded into the original one, a watermark picture is then got as an output within the frequency domain. Therefore, in order to attain a watermarked picture within the time (image) domain, there is a need to calculate the watermarked image's DCT. The above-discussed DCT method to embed the watermark is implemented on the image by partitioning the original picture into several blocks. Then the allocation of Beta along with Alpha value is done toward every block.

As per the research of Singh *et al.* [36], the DCT-based technique is effective in comparison with spatial domain methods. The reason behind this is because the watermark embedded into the image under such a technique is not possibly destroyed by any attach as the middle-frequency coefficients are used for embedding, and thus the image's visibility is not impacted. On the other hand, it is argued by Shaikh and Deshmukh [37] that due to block-wise DCT, the system's invariance property is sometimes destroyed. Moreover, when the quantization is performed, some components of higher frequency get stifled.

2.2. Discrete wavelet transform

DWT is defined by Hoshi *et al.* [33] as a modern and widely utilized technology, which supports numerous operations, such as digital signal processing, watermarking, and image compression. Due to its excellent characteristics associated with spatial localization as well as multi-resolution, this technique is mostly used within digital watermarking. Along with that, it is denoted as an effective mathematical tool, which is best for the hierarchical decomposition of digital pictures. Moreover, DWT is also defined as a theory of information analysis known for the past few years. This technique contains several scales within the frequency and space, whose image decomposition could be carried out constantly from low to high resolution. When DWT watermarking technique is used, the image is split into four different components, which are high-high (HH), high-low (HL), low-low (LL), and low-high (LH), as shown in Figure 2. The 1st letter corresponds towards implementing the operation of a high pass or low pass frequency to the rows and the 2nd letter denotes the filter, which is implemented to the columns [35]. In such an algorithm, the embedding of the watermark is done into the host image with the modification of the coefficients attached to the banks of high frequency, i.e., HH sub-band.

The parts related to higher frequency are extensively utilized for digital marketing, whereas the parts linked with lower frequency play an important role in extracting watermarks. Hence, the wavelet filters are incorporated by DWT, which possesses floating-point coefficients, and they are developed through dilations as well as translations of a static mother wavelet function. Thus, as per the study of Zhang and Wei [38], both the frequency and spatial description of a specific image are provided by the wavelets. Their decomposition's significance rests on the ability to decompose the matrix of an image at a dynamic scale. Because of such a capability, DWT is optimal for analyzing multi-resolution, which is possible to be compared with the characteristics of energy compression and standards of compression, making Distinct Wavelet Transform effective against noise attacks and compressions [33].

DWT technique of digital watermarking is efficient towards attacks like cropping, scaling, salt and pepper attack, deblurring, and JPEG compression. This technique is extensively utilized in numerous applications of signal processing, for example, wireless antenna distribution stimulation, compression of video and audio, and noise removal within audio [39]. The preference given to DWT is simply because of its benefit of providing both similar frequency spread and spatial localization of the watermark in the host image. The technique's key idea within the procedure of an image is to decompose an image into a sub-image of distinct, independent frequencies and spatial domains.

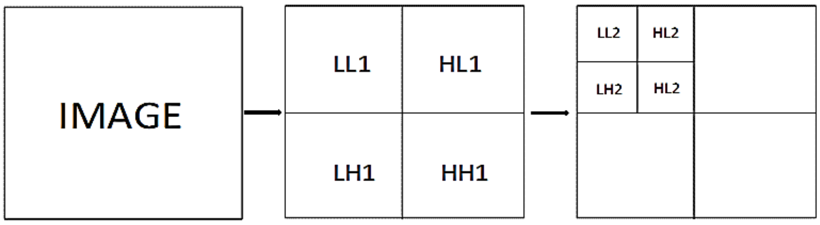


Figure 2. DWT mechanism [33]

2.3. One-time pad

The one-time pad (OTP) is a robust and hybrid encryption and watermarking method/algorithm. It is based on a new chaotic map approach [40] It is considered one of the unique inventions related to encryption and watermarking. OTP is an encryption technique that is difficult to decipher. This is because the key which is generated to encrypt the message is only generated once [41]. After its usage, the key expires, and hence, the system cannot be cracked again. This type of cryptography has been the key feature of security agencies. As noted by Deng and Long [42], the OTP traces its roots to the USSR and the era of Stasi, where the communication of information was very sensitive due to the presence of enemies. This type of situation encouraged the development of a code that would make it very difficult to decipher. In fact, the study of Matt and Maurer [43] relates the development of OTP to Frank Miller in 1882. However, with the evolution of time and technology, a fully developed OTP was launched in 1917 with the idea of having a code that is truly and mathematically unbreakable.

The working mechanism of OTP is defined by Rubin [44], who states that in a standard OTP, each character is combined with a character generated by a random keystream. It is important to mention that the length of an OTP is equal to the length of the original message. Because numbers are assigned to each code, it makes no sense unless the reader has the key to decipher it. OTP also has to follow a certain logic. This logic includes: a standard OTP must contain truly random characters, the length of OTP should correspond to the length of the original text, the copies of OTP must be limited to a minimum number which is 2, it must be used only once, and finally, the key must be destroyed after the usage. The inclusion of the last theory, i.e., its key must be destroyed, is very important because this feature makes OTP unique. Moreover, it is also important to shed light on the mechanism of OTP. It implies the use of the key that the receiver must possess in order to encipher the message. This is normally described as a "100 percent noise source," meaning that regardless of the noise present in the externality, OTP can only be deciphered through the use of the key. For this, the parties that have to use the code must start off from the same location. It is to say that both the receiver and sender must possess the knowledge of the key unless OTP is conveyed through computer technology [44].

It is important to note that digital watermarking interest is motivated by multimedia security, which has led to many cryptographic analogies, such as OTP, being applied to watermarking. It is argued that these analogies could be incorrect or misleading since keys used in both watermarking and cryptography have different properties. Moreover, watermarking is fundamentally communication and relies on the reliable delivery of bits. Still, in the development of watermarking applications, cryptography plays an important role [45]. OTP has risen to success and has become a popular use in secrecy communication because it is theoretically impenetrable. It means that it cannot be broken unless the user has the key. It means that it can be distributed and encrypted without the use of computer technology. OPT was conceived in the pre-computer age and continues to remain a success because it does not rely on information technology. Lastly, the future of OTP needs to be mentioned as well. As per Rijmenants [46] study, it is the only encryption technique that has a future. This is because almost all code-breaking technology can be deciphered, but OTP is difficult to decipher. Its future hinges on the method of key distribution. Because it is the key that lays the solution to the code needs to be sent in a perfectly secured environment and should not be accessed by rivals. This type of technology will undoubtedly have a bright future, especially when all types of technology have been developed to encrypt the protocols and get a deeper insight into the enemies' communication. This is also the reason why, in the study of Borowski and Leśniewicz [47], it is mentioned that aircraft carriers and armed forces still rely on OTP to distribute information. In order to ensure the operations, trusted data management along with the couriering system is used, which can be fully trusted to process the key to the code.

2.4. Playfair

Playfair is among the most archaic forms of encryption and watermarking tools that is still being used. It was first invented by Charles Wheatstone in 1854. Since then, the technique has been fairly developed. This encryption technique is further studied by Shakil and Islam [48]. As per the authors, Playfair is built on a symmetric polyalphabetic encryption system that uses block substitution. A standard Playfair cipher is built on a 5×5 matrix. The reason why this technique is still studied or employed is that it is very complex to break this code. This is primarily due to the pairing of encrypted letters, which is done in pairs. It is opposed to the substitution cipher, which is rather conducted on single letters.

The study of R. [49] also highlights the complicated history of the encryption technique. As per the author, because the technique employed by Playfair was so complex and harder to understand, the British Foreign Secretary rejected the use of Playfair in its official communication. Nevertheless, the technique was famously employed in WWII. The reason for its prestige was that it depended on simple paper and pencil to decipher, which came in handy in the second world war.

The study of Dooley [50] also shows how important the Playfair cipher has been over history. The Britishers first used it in the Second Boer War (1899-1902) and world war I. The claim to its success was because Playfair was so complex and harder to break, it became a standard cyphering technique that would be employed even after the war. However, with the development of technology and the evolution of time, the complex code did not continue to remain that complicated and eventually had to be replaced with a better and more sophisticated cipher technique. The cyphering technique especially faced a decline when computer machines were invented and became the most popular communication device. It was because computer machine was built on algorithms that could solve a Playfair code in seconds, and hence, since then, the Playfair technique was rendered irrelevant and became a part of history.

3. PROPOSED ALGORITHM

The embedding and extraction schemes follow the diagrams shown in Figure 3. The embedding process is the process by which the hidden is watermarked in the cover image. It needs two images, namely, a cover image to hide the image on and a hidden image to be hidden inside it. The embedding process of the proposed work starts by calculating the 8-by-8 block DCT of the cover image, which is done by processing the image into 8-by-8 blocks and performing the DCT in each block individually. Then the DC component, which is the first coefficient from the top left of each 8-by-8 block, having computed the DC image, it is then transformed using 2 levels of DWT. The DWT has 4 resultant images based on its frequency content and the direction of computing, namely, the LL, LH, HL, and HH. Where L stands for low-frequency content and H for high-frequency content. Two-level DWT was computed throughout this work; the second level is computed from the LL component. When concatenating the 4 images of the second level, we get 32-by-32-by-3 which should be the maximum size of the hidden image. The hidden image is encoded using two methods, firstly, the OTP and secondly, the Playfair ciphering algorithm. The algorithms are simple and straightforward. The second logo image was also embedded in the cover image in 5-level DWT in three different locations, which are LL1, LL3, and LL5.

In the end, we reconstruct the final watermarked image that results from this process. Then we apply 10 types of selected attacks and measure the MSE, SNR, and PSNR for the extraction process before and after attacks. Decoding before and after attacks is performed, as shown in Figure 3. The images that were tested in this paper were taken from the image database located on the website of the University of (Southern California).

3.1. Encoding process

The hidden image is encoded using two methods, firstly, the OTP and secondly, the Playfair ciphering algorithm. The algorithms are simple and straightforward, whereas the keys for each method are defined in the following subsections. The OTP key should have the same size as the original image because the OTP ciphering process is done by bitwise XOR operation. Therefore, each pixel in the original image must have a corresponding key in the cover image; that's why the two images must have the same size. The key is generated by using as:

$$OTP\ key = round(255 \times random(image\ size))$$

Where the rounding process to eliminate the fractions as maximum image intensity is 255.

The Playfair key, on the other hand, must be a squared matrix containing every possible pixel intensity in the input image. The Playfair key also should not contain duplicate entries. The following encryption and decryption algorithms are used for image encryption and reconstruction.

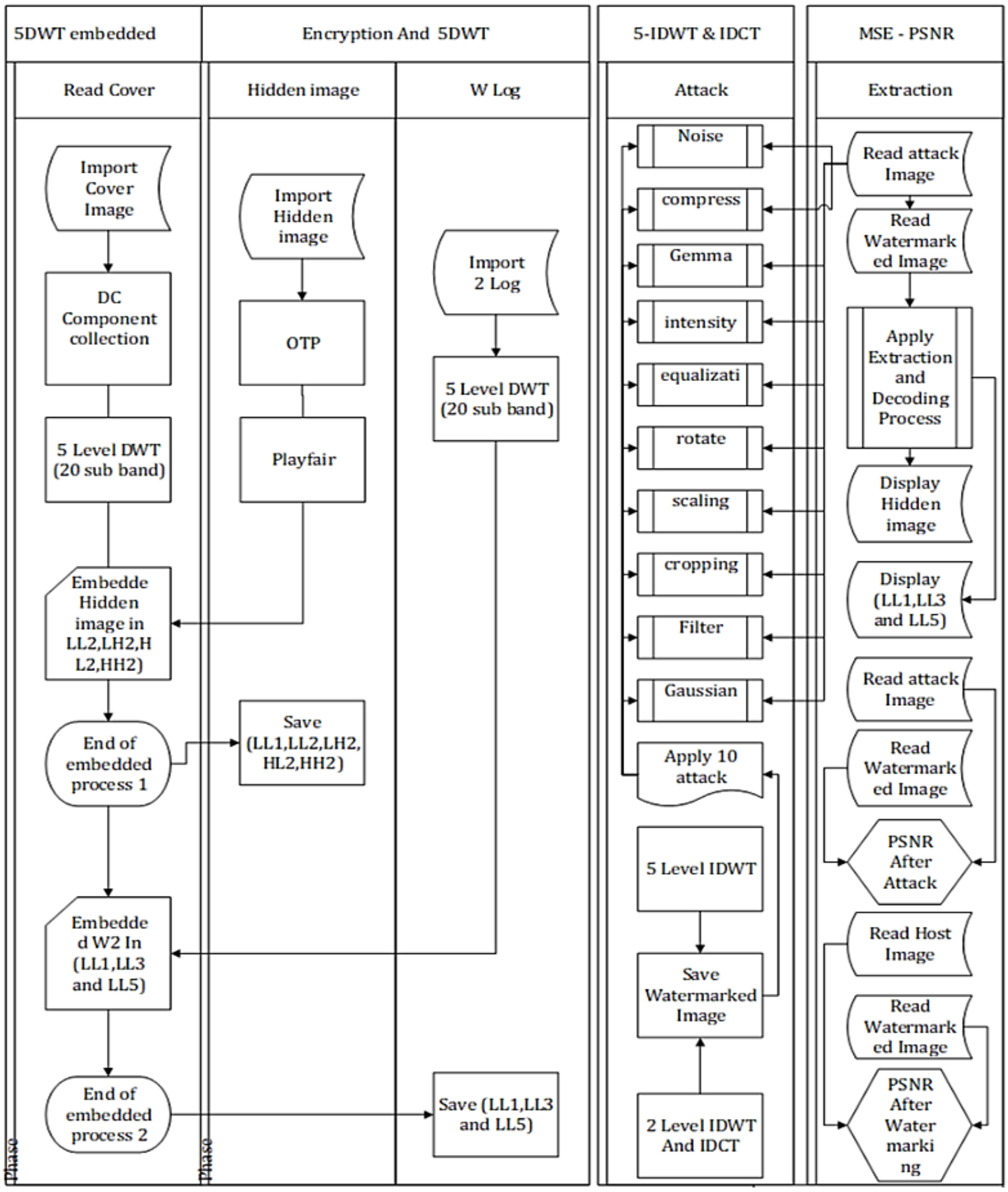


Figure 3. Proposed algorithm

3.2. The embedding scheme

Assume we have a host image Hi (i,j) (512×512) this host image is considered as a cover host image, and assume that we have a Ci (i,j) (32×32) as a hidden image and Li (i,j) (512×512) as a logo image, the first process is to obtain the image Wi1 (i,j) (512×512) where DCT– 2 level DWT watermarking apply and hidden where embedded in certain location-based in our suggestion algorithm (LL, LH, HL, and HH) after OTP and Playfair were used to cipher the hidden image, this will result our first Watermarked/Cipher image WCi1(i,j), while the 5 level DWT watermarking used to embed the log image WCi2 (i,j) in certain location-based in our suggestion algorithm (LL1, LL3, and LL5) as well (see Figure 4). Therefore, the summation of WCi1 (i,j) and WCi2 (i,j) resulted in our final watermarked image WCi (i,j) following mathematical in (1) to (3) representing our first process. In contrast, in (4) is used in the embedding process in the second process. In (5) represent the equations for the final watermarked image.

$$\mathrm{WCi}(i,j) \;=\; (1-\beta) + \left(\frac{Ci(i,j)}{255} * (1(1-\beta))\right) \tag{1}$$

$$WCi0(i,j) = (Hi(i,j) + \epsilon) * WCi(i,j) \tag{2}$$

$$WCi1(i,j) = Hi(i,j) + WCi0(i,j) \quad (3)$$

$$WCi2(i,j) = Hi(i,j) + Li(i,j) \quad (4)$$

$$\mathrm{WCi}(i,j) = WCi1(i,j) + WCi2(i,j)/2 \quad (5)$$

where β is the scaler factor in reducing the effect of the embedding process and ϵ is floating-point relative accuracy.

The purpose of this equation is to let the ciphered image be in the range of (1-β) to 1 so that it does not affect the plane value heavily and produces an image with reasonable PSNR. For example, if β value was 0.001, the hidden image would be in the range of 0.990 to 1 when this is multiplied by the original plane image; it will not affect the plane heavily but would produce the required embedding.

The final watermarked image is calculated by reversing the operations of the encoding process starting from the end to the beginning. Namely, replacing the 2nd level plane with the ciphered plane, then performing the two-level inverse wavelet transform to get back the watermarked DC image. Then, these watermarked DC components were restored back to the DC component's original image, and the inverse discrete cosine transform (IDCT) was performed to get back the final watermarked image.

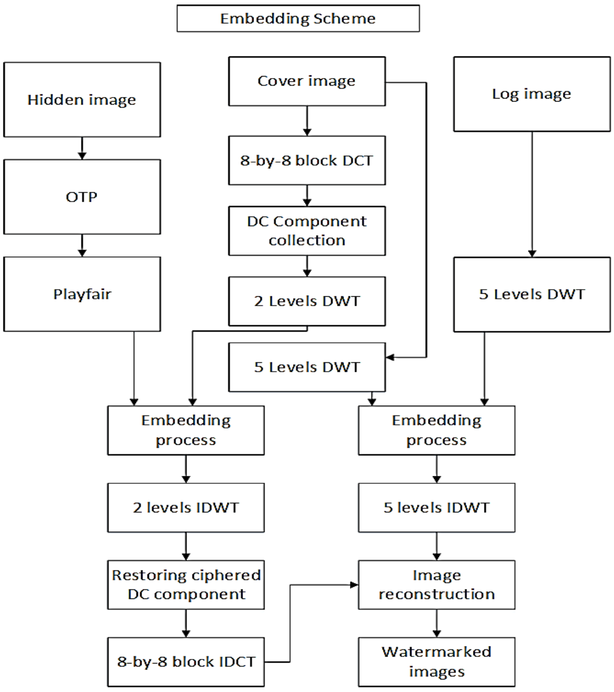


Figure 4. Embedding scheme

3.3. The extraction scheme

Assume we have both host image Hi (i,j) (512×512), and watermarked image WCi (i,j), then the extraction scheme is done to retrieve the hidden image, two images must be present to get the image back, the watermarked image alongside with the original cover image as shown in Figure 5. The same steps taken to extract the 2nd level DWT are also taken here; namely, the DCT transform, then collecting the DC components from both of the images (original cover and watermarked) then applying the 2 levels. In (6) to (8) represent the extraction process for hidden images, while subtraction is applied to extract the logo image using 5 levels DWT also from (original cover and watermarked), which is represented in (9).

$$WCi0(i,j) = Hi(i,j) + WCi1(i,j) \quad (6)$$

$$WCi(i,j) = \frac{WCi0(i,j)}{Hi(i,j) + \epsilon} \quad (7)$$

$$Ci(i,j) = round\left(\frac{WCi(i,j)-(1-\beta)}{1-(1-\beta)} * 255\right) \quad (8)$$

$$WCi2(i,j) = Hi(i,j) - WCi(i,j) \quad (9)$$

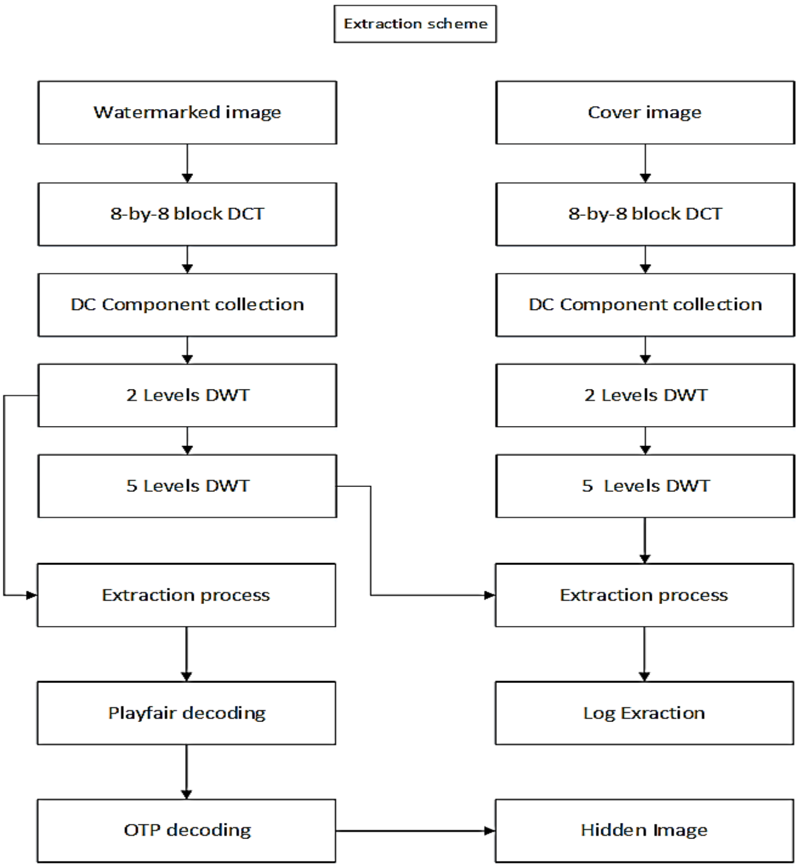


Figure 5. Extraction scheme

3.4. Decoding process

This is the reverse of the process that was performed earlier. The extracted image is ciphered using the Playfair algorithm combined with the OTP. Hence, the decoding algorithm for both must be used to get the original hidden image back. Note that it's important to use the same key as encoding to decode the image back; otherwise, no information can be retrieved.

3.5. Image quality evaluation

Mean squared error (MSE) indicates the closeness of a regression line to a set of points. It accomplishes this by squaring the distances between the points and the regression line (these distances are the "errors"). Squaring is required to eliminate any negative signals. It also gives significant discrepancies more weight. Because you're calculating the average of a series of errors, it's termed the mean squared error. The better the forecast, the lower the MSE. In (10) was used in this paper to calculate MSE [51]:

$$MSE = \frac{1}{n}\sum_{i=1}^{n}(y_i - \tilde{y_i})^2 \quad (10)$$

Signal to noise ratio (SNR) is defined as the ratio between the desired information or signal power and the undesirable signal or background noise power. SNR is also a scientific and technical measurement parameter that compares the level of the desired signal to the amount of background noise. In other terms, SNR is the ratio of signal to the noise power, with decibels as the standard unit of measurement (dB). Furthermore, a SNR larger than 0 dB or greater than 1:1 indicates that there is more signal than noise. This parameter is also related to image quality as it measures the level of noise/distortion in the image. In (11) is used to calculate the SNR value [51]:

$$SNR = 10.log\,10\left[\frac{\sum_{0}^{Na-1}\sum_{0}^{Nb-1}[Ri(a,b)]^2}{\sum_{0}^{Na-1}\sum_{0}^{Nb-1}[Ri(a,b)-Ti\,(a,b)]^2}\right] \qquad (11)$$

Peak signal-to-noise ratio (PSNR) is the ratio of a signal's maximum possible value (power) to the strength of distorting noise that influences its representation quality. The PSNR is commonly stated in terms of the logarithmic decibel scale since many signals have a very wide dynamic range (the ratio between the biggest and smallest possible values of a variable quantity). Improving the visual quality of a digital image, often known as image augmentation, is a subjective process. Whether or whether one method produces a higher-quality image depends on the individual. As a result, quantitative/empirical metrics to compare the effects of image enhancement algorithms on image quality are required. This value is calculated in this paper to evaluate the quality of the image. In (12) was used to evaluate this parameter [51]:

$$PSNR = 10.log\,10\left[\frac{Max\,(Ri(a,b))^2}{\frac{1}{N_aN_b}.\sum_{0}^{Na-1}\sum_{0}^{Nb-1}[Ri(a,b)-Ti(a,b)]^2}\right] \qquad (12)$$

4. RESULT AND DISCUSSION

This section presents the results and discussion of this paper after running the proposed algorithm. The embedding process was performed as shown in Figure 6. A 5-level DWT was performed that was embedded into the image of Lena using the 8×8 block DCT. Also, the technique of ciphered OTP was used to image. The results of this process noted that this method of copyrighting is highly secure as it completely hides the watermark, making the image safe from any security threat. OTP is the only encryption technique that has a future, according to Rijmenant's [46] analysis. It's because practically all code-breaking technology can be read, but OTP is particularly tough to crack. Its future is dependent on how keys are distributed. Because it is the key that contains the solution to the code, it must be sent in a highly secure environment and must not be accessible by competitors. This idea can also be noted from the result of this study, as the image that has been embedded with the watermark through OTP is unable to be deciphered through traditional methods.

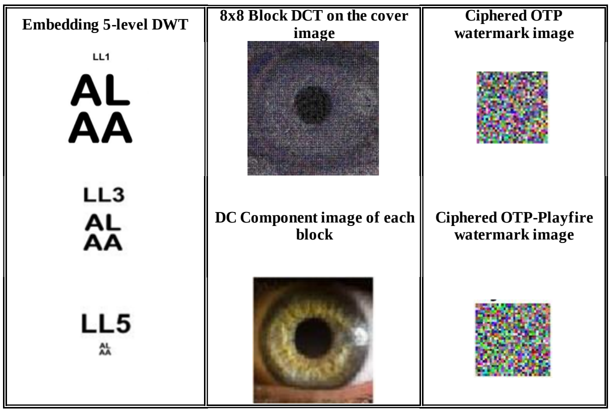
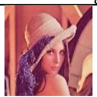

Embedding 5-level DWT
LL1
AL
AA
LL3
AL
AA
LL5
AL
AA
8x8 Block DCT on the cover image
Ciphered OTP watermark image
DC Component image of each block
Ciphered OTP-Playfire watermark image

Figure 6. Embedding results

Moreover, during the experiment, DCT, DWT, and OTP methods were used to transform the images into digital blocks and watermark them. Different images were watermarked through these methods, as shown in Table 1. One of the key points to note is that the use of these digital watermarking techniques did not bring any negative impact on the quality of the image. Also, it can be noted that the secret messages embedded in these images could not be deciphered accurately. In addition to this, wavelets provide both the frequency and spatial description of a specific image, according to Zhang and Wei [38]. The relevance of their decomposition is based on the ability to deconstruct an image's matrix at a dynamic scale. Because of this, DWT is ideal for assessing multi-resolution data, which can be compared to energy compression characteristics and compression standards, making the distinct wavelet transform effective against noise attacks and compressions [33]. These concepts can be noted from the image results as DWT has significantly reduced the image noise and compressed the hidden message into the covered image without harming its quality.

Table 1. Experimental results

Covered image	Watermarked image	Logo	Hidden image
		AL AA	Secret Message
		AL AA	Secret Message
		AL AA	Secret Message
		AL AA	Secret Message
		AL AA	Secret Message

4.1. Human visual quality

Moreover, human visual quality is an important aspect of images as it defines the ways humans are able to perceive images. Different factors affect the human visual quality including noise, filter, intensity, and size. Various factors of images were analyzed during this paper that has been presented in Tables 2 and 3. These results depict the findings after the attack that the image watermark was unharmed. Various techniques like crop, noise, resizing, and adjustments were made to check the impact on the human visual quality. It was noted that although the hidden image was affected a bit, the watermark logo remained the same. Therefore, it can be interpreted based on these results that the use of DWT, DCT, and OTP for watermarking the images is highly effective as any changes to the image do not harm the watermark. The DCT-based strategy is more effective than spatial domain methods [36]. The reason for this is that the watermark implanted in the image using this technique cannot be erased by any attach since middle-frequency coefficients are utilized for embedding; hence the image's visibility is unaffected. Therefore, these results also depict a similar outcome as the visibility remains unaffected due to the attacks as the images were converted using the DCT approach. Both Tables 2 and 3 show similar results.

Table 2. Human visual quality results on Lena

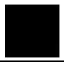
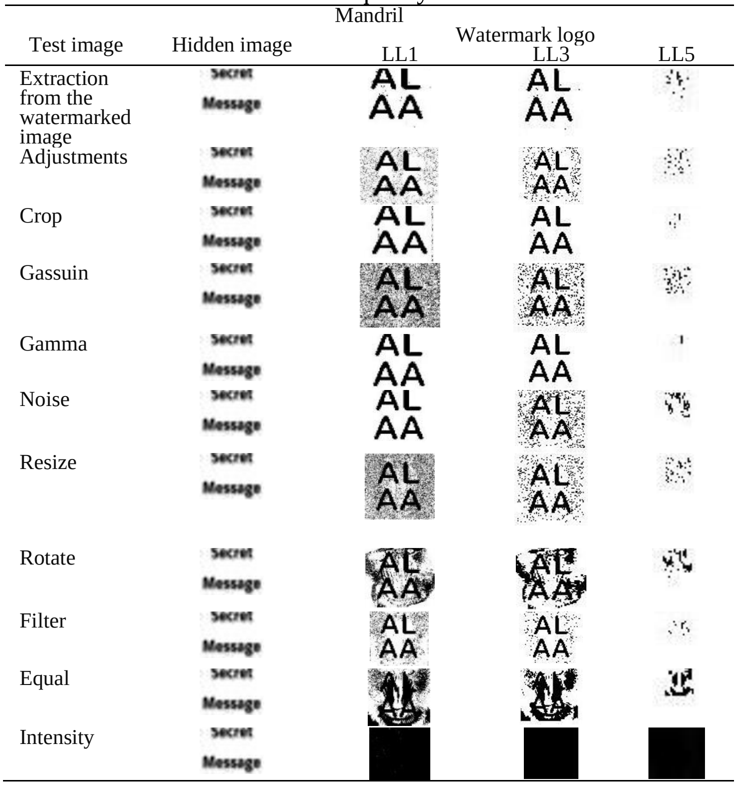
	Lena			
Test image	Hidden image	Watermark logo LL1	 LL3	 LL5
Extraction from the watermarked image	Secret Message			
Adjustments	Secret Message			
Crop	Secret Message			
Gassuin	Secret Message			
Gamma	Secret Message			
Noise	Secret Message			
Resize	Secret Message			
Rotate	Secret Message			
Filter	Secret Message			
Equal	Secret Message			
Intensity	Secret Message			

Table 3. Human visual quality results on Mandril



Test image	Hidden image	Mandril LL1	Watermark logo LL3	LL5
Extraction from the watermarked image				
Adjustments				
Crop				
Gassuin				
Gamma				
Noise				
Resize				
Rotate				
Filter				
Equal				
Intensity				

However, research by Shaikh and Deshmukh [37], the system's invariance property is sometimes destroyed owing to block-wise DCT. Furthermore, when quantization is applied, some higher-frequency components are repressed. This change in the visual quality was noted in the results for Lena and Mandril after an attack for equal, and intensity was applied. This paper observed that the watermark logo completely blackened which destroyed the hidden message in the image. Therefore, it can be stated that there are conditions where the watermarked image can lose its digital watermark when it is attacked.

Another important difference that is noted during this paper between the images of Mandril and Lena is that the watermark logo with LL5 was more visually prominent in the Lena image as compared to the Mandril image (see Tables 2 and 3). Therefore, the watermark logo in the Mandril image is more prone to be destroyed as compared to the image of Lena. An important interpretation that can be made from these results is that the watermarking security might change from one image to another based on its visual characteristics. Watermarking invisibly or obviously embeds the ownership symbol within movies and photos, whereas steganography hides the information's little parts [52] However, hidden image is sometimes harmed when the image is attacked. Although these digital watermarking techniques are highly effective against most attacks, they can still be breached in some circumstances. Thus, the integrity of these images must be protected through the use of more than one watermarking technique.

4.2. Experimental results: after apply set of attacks

The results noted that after the application of attacks on the images with watermarks, there was no impact on the hidden message and watermark logo. Although little changes to both can be noted in Tables 2 and 3, the secret message was still preserved. Therefore, this is a very critical observation as it shows the high effectiveness of DCT, DWT, OTP, and Playfair methods. As per the study of Dooley [50], the Playfair technique is one of the most complex and complicated methods of watermarking. However, it also has strong results that do not allow the attacker to break the code. In this study, DCT, DWT, and OTP were used along with the Playfair method to reduce the complexity offered by the latter. This brought various benefits that included highly secure digital watermarks for the test images. Therefore, the results noted that the visual quality of the images, along with their watermarks, remained unharmed when different sets of attacks were applied to the test images.

5. EVALUATION

MSE, SNR, and PSNR values were calculated for the Lena cover image which is shown in Table 4. It can be noted that with reference to the original image, the watermarked image had a higher PSNR, which means that the quality of the image improved after the application of watermarking techniques. Also, it can be noted that the value of SNR shows that there is minimal noise in the watermarked image. Therefore, the image quality is higher.

Table 4. Lena's cover image references

Lena cover image				
Ref. image	Test image	MSE	SNR (dB)	PSNR (dB)
Original image	Watermarked image	0	0.07	32.8
Original image	Adjustments	0.03	1.34	14.56
Original image	Crop	0.08	-1.45	10.75
Original image	Equal	0	0.39	22.52
Original image	Gamma	0.01	-1.7	17.71
Original image	Gassuin	0	-0.06	31.08
Original image	Intensity	0.01	1.57	18.66
Original image	Noise	0	-0.05	24.37
Original image	Resize	0	-0.07	29.29
Original image	Rotate	0.07	-0.58	11.17
Original image	Filter	0	-0.07	32.61

The image quality evaluation was then performed in reference to the watermarked image while making different changes. The results have noted that the application of changes like adjustments, gamma, noise, and filter, did not change the image quality (see Table 5). Therefore, it can be interpreted that the use of DCT and other watermarking techniques did not harm the image quality.

Table 5. Lena's watermark references

Lena watermark image				
Ref. image	Test image	MSE	SNR (dB)	PSNR (dB)
Watermarked image	Adjustments	0.03	1.41	14.45
Watermarked image	Crop	0.08	-1.39	10.83
Watermarked image	Equal	0	0.46	23.23
Watermarked image	Gamma	0.01	-1.63	18.25
Watermarked image	Gassuin	0	0	35.91
Watermarked image	Intensity	0.01	1.64	18.46
Watermarked image	Noise	0	0	25
Watermarked image	Resize	0	-0.01	30.37
Watermarked image	Rotate	0.07	-0.52	11.17
Watermarked image	Filter	2.4	-0.01	46.19

The same procedures were then applied to the Mandril cover image and Peppers's cover image. Table 6 shows the results for the original Mandril cover image. Again, the results are similar to the Lena cover image. However, in the Mandril watermarked image, the noise reduction is more as compared to that in the Lena watermarked image, as can be seen from the greater negative value of SNR. Similarly, the value of PSNR is higher in the Lena cover image, which shows that the image is of high quality. Table 7 shows the results for the watermarked image being applied with different variations. It was noted that the results of this process were very similar to that of the Lena watermarked image.

Table 6. Mandril cover image references

Mandril cover image				
Ref. image	Test image	MSE	SNR (dB)	PSNR (dB)
Original image	Watermarked image	0	0.15	25.53
Original image	Adjustments	0.03	0.56	14.46
Original image	Crop	0.06	-0.86	12.38
Original image	Equal	0.01	1	19.95
Original image	Gamma	0.01	-1.66	18.04
Original image	Gassuin	0	0.15	25.12
Original image	Intensity	0.02	1.84	17.19
Original image	Noise	0	0.17	22.47
Original image	Resize	0	0.02	21.08
Original image	Rotate	0.08	-0.37	10.88
Original image	Filter	0	0.13	25.39

Table 7. Mandril watermark image references

Mandril watermark image				
Ref. image	Test image	MSE	SNR (dB)	PSNR (dB)
Watermark image	Adjustments	0.03	0.41	14.82
Watermark image	Crop	0.05	-1.02	12.37
Watermark image	Equal	0.01	0.82	22.16
Watermark image	Gamma	0.01	-1.81	18.18
Watermark image	Gassuin	0	0	35.62
Watermark image	Intensity	0.01	1.68	18.56
Watermark image	Noise	0	0.02	25.34
Watermark image	Resize	0	-0.13	21.71
Watermark image	Rotate	0.08	-0.52	10.83
Watermark image	Filter	0	-0.01	38.92

Similarly, the tests were performed on Pepper's original and watermarked images. The results noted that the value of SNR for the watermarked image was lower than that of the watermarked image of the Mandril. However, the value of PSNR was high (see Table 8). This shows that the quality of the image was high with some noise. Likewise, other, Peppers's watermarked image was tested with different variations, and their results also aligned with that mentioned above (see Table 9).

Table 8. Peppers cover image references

Peppers cover image				
Ref. image	Test image	MSE	SNR (dB)	PSNR (dB)
Original image	Watermarked image	0	0	33.28
Original image	Adjustments	0.04	1.33	13.45
Original image	Crop	0.05	-1.23	12.31
Original image	Equal	0.01	1.51	20.27
Original image	Gamma	0.01	-1.93	18.65
Original image	Gassuin	0	0	31.39
Original image	Intensity	0.01	1.88	18.35
Original image	Noise	0	0.03	24.34
Original image	Resize	0	-0.02	29.21
Original image	Rotate	0.09	-0.76	10.25
Original image	Filter	0	-0.01	33

Table 9. Peppers watermark image references

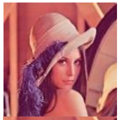
Peppers watermark image				
Ref. image	Test image	MSE	SNR (dB)	PSNR (dB)
Watermarked image	Adjustments	0.04	1.34	13.51
Watermarked image	Crop	0.06	-1.22	12.34
Watermarked image	Equal	0.01	1.51	20.51
Watermarked image	Gamma	0.01	-1.93	18.79
Watermarked image	Gassuin	0	0.01	36
Watermarked image	Intensity	0.01	1.89	18.5
Watermarked image	Noise	0	0.03	24.93
Watermarked image	Resize	0	-0.02	30.52
Watermarked image	Rotate	0.09	-0.76	10.27
Watermarked image	Filter	3.08	-0.01	45.11

The test result shows very good and high value which mean that our suggestion algorithm used is robust enough to preserve image quality against different type of attacks, based on these results, it can be stated that the image quality is affected by the processes like crop, gamma, Gaussian, filter, and rotation. These processes change the values of MSE, SNR, and PSNR, which shows changes in the image quality and noise levels. However, it is also important to note that the changes in quality are not major, which means the watermarks are preserved during these processes. Nevertheless, it is important to note that different images might behave differently when they undergo similar procedures. For instance, applying the intensity process to Mandril, Lena, and Pepper images brought different results.

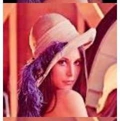
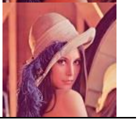
5.1. Experimental results after attacks

The results for this section are obtained through extraction after attacks. It can be noted that the resulting image does not lose its quality during the process, which means that the watermark and secret message are safely embedded. Different attacks like Gaussian, Gamma, and adjustment didn’t change the characteristics of the resultant image (see Table 10). However, they did not raise the noise levels significantly. This shows that the images are not destroyed and can be used to retrieve the secret message that was embedded. Therefore, these images can be used for the communication of hidden messages. The results of this paper have proved the high security offered by these methods for digital watermarking and hiding the image through the embedding process in the images. It has been noted that in most attacks, the integrity of the watermarks and hidden images will not be violated.

Table 10. Lena's image results

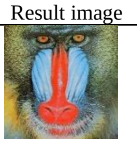
		Lena	
No.	Name	Parameters	Result image
1.	Watermarked image	Logo image + Hidden image	

2.	Gaussian	Mean=0
		Variance=0.001	

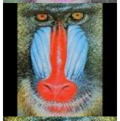
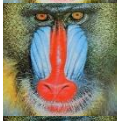
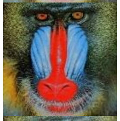
3.	Intensity	1.5	
4.	Noise	0.02	
5.	Rotate	512×256	
6.	Adjustment	[l=0 h=0.8] [b=0 t=1]	
7.	Crop	On both sides	
8.	Equal	20°	
9.	Filter	Window size=3×3	
10.	Gamma	[l=0 h=0.8] [b=0 t=1]	
11.	Resize	Automatic	

The watermarked images were put to the test using a variety of attacks in MATLAB to evaluate the effectiveness and robustness of the suggested algorithm. Attacks like Gaussian, intensity, noise, rotate, adjustment, crop, gamma, equal, filter, and resize. We can infer from the values obtained above that the algorithm was effective in fending off various forms of attacks, and the image quality obtained is still suitable for visual observation. Similarly, when the attacks were applied to the Mandril image and the extraction process was performed, the following results were obtained (see Table 11). Like the Lena image, the integrity of these images was not violated, and all the images had a high quality. Also, they have very little noise, which shows that the hidden image and logo image are safely embedded and can be deciphered with the key to read the message when needed. In the evaluation results, Lina's image shows a very good and high value compared to Mandril's image. The results of this paper also validate these assertions as different attacks did not allow a change in the quality of the image. Therefore, based on these findings, it can be stated that the methods of DCT, DWT, OTP, and Playfair are highly effective in digital watermarking images and embedding secret messages.

Table 11. Mandril image results

		Mandril	
No:	Name	Parameters	Result image
1.	Watermarked image	Logo image+Hidden image	

2.	Gaussian	Mean=0
		Variance=0.001	

3.	Intensity	1.5	
4.	Noise	0.02	
5.	Rotate	512×256	
6.	Adjustment	[l=0 h=0.8] [b=0 t=1]	
7.	Crop	On both sides	
8.	Equal	20°	
9.	Filter	Window size=3×3	
10.	Gamma	[l=0 h=0.8] [b=0 t=1]	
11.	Resize	Automatic	

The findings of this paper demonstrated the excellent level of security provided by these technologies for digital watermarking and picture concealment via the embedding process in photographs. Therefore, it is recommended that these methods are adopted for secure communication of messages as it is very hard to break these security protocols as none of the attacks have been proven to be effective in deciphering the embedded message.

In the end, it can be concluded that the techniques of DCT, DWT, OTP, and Playfair are highly effective when used together to watermark an image or embed a secret message. These methods of copyrighting can solve various problems that have arisen due to the emergence of the internet and technology. In this modern era, it has become much simpler to replicate, sell, and copy the copyright owners' works without their permission as a result of the expansion of digitalization, and it is difficult to identify such violations, posing a significant threat to the creators' and copyright owners' rights. For many years, the internet has been regarded as one of the most serious threats to copyright, and the content available has varying levels of copyright protection. On the internet, there are numerous copyrighted works, including stories, e-books, graphics, movies, news, screenplays, and so on. Therefore, by using watermarking and steganography techniques, these issues can be solved. Such techniques are directly applied to an image's original pixels since the watermark can be added by modifying the pixel's values, which are based on the author's signature information or logo. Therefore, to improve the image quality and safety of watermarks, this paper examined the use of DCT, DWT, OTP, and Playfair methods to watermark the images digitally. An algorithm was proposed that used embedding and extraction processes to gather the results and data. These results were then analyzed to produce the findings.

6. CONCLUSION

This paper has used DCT, DWT, OTP, and Playfair methods simultaneously. This collaboration of methods allowed the images to be of high quality and safer for watermarks. It was noted that being used alone, each of these methods can have various limitations that might not bring the desired watermarking results. For instance, it was observed that DCT represents the data in frequency space rather than amplitude space, which makes this technique more robust than other digital image processing operations like filtering, contrast changes, and brightness. However, they are computationally expensive and difficult to implement. They are also vulnerable to geometric attacks such as rotation, cropping, and scaling. In addition to this, the Playfair method is no longer used extensively in watermarking. This is primarily due to the system's ease of use and understanding, which allows an official to break it in a short period of time. Because of its simplicity, the technique has become obsolete in current times. Therefore, it can be noted that these methods also have their limitations. Nonetheless, their use together to watermark and embed an image has overcome their weaknesses and optimized the process of watermarking.

More advantage of this paper is that the new algorithm has also found that by using these methods, there is no impact on the quality of the image when they are under different attacks like cropping, resizing, and rotation, Therefore, this means that the watermark images and their embedded messages are secure, even after the attacks. It's worth noting that the final image obtained after the attacks in this paper maintained its quality throughout the process analyzed in standard traditional metrics MSE, SNR, and PSNR. implying that the watermark and secret message are securely inserted with a high-quality image.

ACKNOWLEDGEMENTS

This research has been conducted in the Vision Research Laboratory in UKM and is supported by the Ministry of Education (MOE) Grant fund: FRGS/1/2018/TK04/UKM/02/16.

REFERENCES

[1] A. K. Singh, “Improved hybrid algorithm for robust and imperceptible multiple watermarking using digital images,” *Multimedia Tools and Applications*, vol. 76, no. 6, pp. 8881–8900, Mar. 2017, doi: 10.1007/s11042-016-3514-z.

[2] A. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, “Digital image steganography: Survey and analysis of current methods,” *Signal Processing*, vol. 90, no. 3, pp. 727–752, Mar. 2010, doi: 10.1016/j.sigpro.2009.08.010.

[3] O. Evsutin, A. Melman, and R. Meshcheryakov, “Digital steganography and watermarking for digital images: A review of current research directions,” *IEEE Access*, vol. 8, pp. 166589–166611, 2020, doi: 10.1109/ACCESS.2020.3022779.

[4] K. Joshi and R. Yadav, “A new LSB-S image steganography method blend with Cryptography for secret communication,” in *Proceedings of 2015 3rd International Conference on Image Information Processing, ICIIP 2015*, pp. 86–90, Dec. 2016, doi: 10.1109/ICIIP.2015.7414745.

[5] V. Kumar and D. Kumar, “Performance evaluation of DWT based image steganography,” in *2010 IEEE 2nd International Advance Computing Conference, IACC 2010*, pp. 223–228, Feb. 2010, doi: 10.1109/IADCC.2010.5423005.

[6] S. Kumar and S. K. Muttoo, “A Comparative Study of Image Steganography in Wavelet Domain,” *International Journal of Computer Science and Mobile Computing*, vol. 2, no. 2, pp. 293–297, 2013.

[7] A. Susanto, D. R. I. M. Setiadi, C. A. Sari, and E. H. Rachmawanto, “Hybrid method using HWT-DCT for image watermarking,” in *2017 5th International Conference on Cyber and IT Service Management, CITSM 2017*, pp. 1–5, Aug. 2017, doi: 10.1109/CITSM.2017.8089252.

[8] D. R. I. M. Setiadi, T. Sutojo, E. H. Rachmawanto, and C. A. Sari, “Fast and efficient image watermarking algorithm using discrete tchebichef transform,” in *2017 5th International Conference on Cyber and IT Service Management (CITSM)*, pp. 1–5, Aug. 2017, doi: 10.1109/CITSM.2017.8089229.

[9] A. Winarno, D. R. I. M. Setiadi, A. A. Arrasyid, C. A. Sari, and E. H. Rachmawanto, “Image watermarking using low wavelet subband based on 8×8 sub-block DCT,” in *Proceedings - 2017 International Seminar on Application for Technology of Information and Communication: Empowering Technology for a Better Human Life, iSemantic 2017*, vol. 2018, pp. 11–15, Oct. 2017, doi: 10.1109/ISEMANTIC.2017.8251835.

[10] P. Bedi, V. Bhasin, and T. Yadav, “2L-DWTS - Steganography technique based on second level DWT,” in *2016 International Conference on Advances in Computing, Communications and Informatics, ICACCI 2016*, pp. 1533–1538, Sep. 2016, doi: 10.1109/ICACCI.2016.7732266.

[11] L. C. Schaupp and L. Carter, “E-voting: from apathy to adoption,” *Journal of Enterprise Information Management*, vol. 18, no. 5, pp. 586–601, Oct. 2005, doi: 10.1108/17410390510624025.

[12] M. A. Faizal, H. B. Rahmalan, E. H. Rachmawanto, and C. A. Sari, “Impact Analysis for Securing Image Data using Hybrid SLT and DCT,” *International Journal of Future Computer and Communication*, pp. 309–311, 2012, doi: 10.7763/ijfcc.2012.v1.83.

[13] A. Goswami and S. Khandelwal, “Hybrid DCT-DWT Digital Image Steganography,” *International Research Journal of Engineering and Technology (IRJET)*, vol. 4, no. 6, pp. 228–233, 2017, doi: 10.17148/IJARCCE.2016.5649.

[14] A. Nambutdee and S. Airphaiboon, “Medical image encryption based on DCT-DWT domain combining 2D-DataMatrix Barcode,” in *BMEiCON 2015 - 8th Biomedical Engineering International Conference*, pp. 1–5, Nov. 2016, doi: 10.1109/BMEiCON.2015.7399508.

[15] M. R. PourArian and A. Hanani, “Blind steganography in color images by double wavelet transform and improved arnold transform,” *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 3, no. 3, pp. 586–600, 2016, doi: 10.11591/ijeecs.v3.i2.pp586-600.

[16] P. Patel and Y. Patel, “Secure and authentic DCT image steganography through DWT - SVD based digital watermarking with RSA encryption,” in *Proceedings - 2015 5th International Conference on Communication Systems and Network Technologies, CSNT 2015*, pp. 736–739, Apr. 2015, doi: 10.1109/CSNT.2015.193.

[17] M. Jain and S. K. Lenka, “Secret data transmission using vital image steganography over transposition cipher,” in *Proceedings of the 2015 International Conference on Green Computing and Internet of Things, ICGCIoT 2015*, pp. 1026–1029, Oct. 2016, doi: 10.1109/ICGCIoT.2015.7380614.

[18] N. Nagaraj and P. G. Vaidya, “One-Time Pad, Arithmetic Coding and Logic Gates: An unifying theme using Dynamical Systems,” 2008, doi: 10.48550/arXiv.0803.0046.

[19] J. Thakur and N. Kumar, “DES, AES and Blowfish: Symmetric key cryptography algorithms simulation based performance analysis,” *International journal of emerging technology and advanced engineering*, vol. 1, no. 2, pp. 6–12, 2011.

[20] O. Tornea, M. E. Borda, V. Pileczki, and R. Malutan, “DNA Vernam cipher,” *2011 E-Health and Bioengineering Conference, EHB 2011*, 2011.

[21] W. S. Sari, E. H. Rachmawanto, D. R. I. M. Setiadi, and C. A. Sari, “A Good Performance OTP encryption image based on DCT-DWT steganography,” *Telkomnika (Telecommunication Computing Electronics and Control)*, vol. 15, no. 4, pp. 1987–1995, Dec. 2017, doi: 10.12928/TELKOMNIKA.v15i4.5883.

[22] J. Kodovský, J. Fridrich, and V. Holub, “Ensemble classifiers for steganalysis of digital media,” *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 2, pp. 432–444, Apr. 2012, doi: 10.1109/TIFS.2011.2175919.

[23] R. Thanki, A. Kothari, and D. Trivedi, “Hybrid and blind watermarking scheme in DCuT – RDWT domain,” *Journal of Information Security and Applications*, vol. 46, pp. 231–249, Jun. 2019, doi: 10.1016/j.jisa.2019.03.017.

[24] R. Thanki and S. Borra, “A color image steganography in hybrid FRT–DWT domain,” *Journal of Information Security and Applications*, vol. 40, pp. 92–102, Jun. 2018, doi: 10.1016/j.jisa.2018.03.004.

[25] S. Borra, H. R. Lakshmi, N. Dey, A. S. Ashour, and F. Shi, “Digital image watermarking tools: State-of-the-art,” *Frontiers in Artificial Intelligence and Applications*, vol. 296, pp. 450–459, 2017, doi: 10.3233/978-1-61499-785-6-450.

[26] B. Surekha and G. N. Swamy, “Sensitive digital image watermarking for copyright protection,” *International Journal of Network Security*, vol. 15, no. 2, pp. 113–121, 2013.

[27] A. S. Ashour and N. Dey, “Security of multimedia contents: A brief,” in *Studies in Computational Intelligence*, vol. 660, pp. 3–14, 2017, doi: 10.1007/978-3-319-44790-2_1.

[28] A. Phadikar, B. Verma, and S. Jain, “Region Splitting Approach to Robust Color Image Watermarking Scheme in Wavelet Domain,” *Asian Journal of Information Management*, vol. 1, no. 2, pp. 27–42, 2007, doi: 10.3923/ajim.2007.27.42.

[29] R. Eswaraiah and E. S. Reddy, “Robust watermarking method for color images using DCT coefficients of watermark,” *Global Journal of Computer Science and Technology*, vol. 12, no. 12-F, 2012.

[30] M. Begum and M. S. Uddin, “Digital image watermarking techniques: A review,” *Information (Switzerland)*, vol. 11, no. 2, p. 110, Feb. 2020, doi: 10.3390/info11020110.

[31] N. I. Wu and M. S. Hwang, “Data hiding: Current status and key issues,” *International Journal of Network Security*, vol. 4, no. 1, pp. 1–9, 2007.

[32] H. Tao, L. Chongmin, J. M. Zain, and A. N. Abdalla, “Robust image watermarking theories and techniques: A review,” *Journal of Applied Research and Technology*, vol. 12, no. 1, pp. 122–138, Feb. 2014, doi: 10.1016/S1665-6423(14)71612-8.

[33] A. R. Hoshi, N. Zainal, M. Ismail, A. A.-R. T. Rahem, and S. M. Wadi, “A robust watermark algorithm for copyright protection by using 5-level DWT and two logos,” *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 22, no. 2, pp. 842-856, May 2021, doi: 10.11591/ijeecs.v22.i2.pp842-856.

[34] U. Yadav, J. P. Sharma, D. Sharma, and P. K. Sharma, “Different Watermarking Techniques &amp; its Applications: A Review,” *International Journal of Scientific & Engineering Research*, vol. 5, no. 4, pp. 1288–1294, 2014.

[35] P. Kulkarni, S. Bhise, and S. Khot, “Review of Digital Watermarking Techniques,” *International Journal of Computer Applications*, vol. 109, no. 16, pp. 40–44, Jan. 2015, doi: 10.5120/19275-1029.

[36] R. S. C. P. Singh, P. Singh, and R. S. Chadha, “A survey of digital watermarking techniques, applications and attacks,” *International Journal of Engineering and Innovative Technology (IJEIT)*, vol. 2, no. 9, pp. 165–175, 2013.

[37] S. Shaikh and M. Deshmukh, “Digital Image Watermarking in DCT Domain,” *International Journal of Emerging Technology and Advanced Engineering*, vol. 3, no. 4, pp. 3–7, 2013.

[38] L. Zhang and D. Wei, “Dual DCT-DWT-SVD digital watermarking algorithm based on particle swarm optimization,” *Multimedia Tools and Applications*, vol. 78, no. 19, pp. 28003–28023, Oct. 2019, doi: 10.1007/s11042-019-07902-9.

[39] K. L. H. N. H. Barnouti and Z. S. Sabri, “Digital Watermarking Based on DWT (Discrete Wavelet Transform) and DCT (Discrete Cosine Transform),” *International Journal of Engineering and Technology (UAE)*, vol. 7, no. 4, pp. 3835–3842, 2018, doi: 10.14419/ijet. v7i4.25085.

[40] M. AlShaikh, L. Laouamer, L. Nana, and A. C. Pascu, “Efficient and robust encryption and watermarking technique based on a new chaotic map approach,” *Multimedia Tools and Applications*, vol. 76, no. 6, pp. 8937–8950, Mar. 2017, doi: 10.1007/s11042-016-3499-7.

[41] S. M. Bellovin, “Frank Miller: Inventor of the one-time pad,” *Cryptologia*, vol. 35, no. 3, pp. 203–222, Jul. 2011, doi: 10.1080/01611194.2011.583711.

[42] F.-G. Deng and G. L. Long, “Secure direct communication with a quantum one-time pad,” *Physical Review A*, vol. 69, no. 5, p. 052319, May 2004, doi: 10.1103/PhysRevA.69.052319.

[43] C. Matt and U. Maurer, “The one-time pad revisited,” in *IEEE International Symposium on Information Theory - Proceedings*, Jul. 2013, pp. 2706–2710. doi: 10.1109/ISIT.2013.6620718.

[44] F. Rubin, “One-time pad cryptography,” *Cryptologia*, vol. 20, no. 4, pp. 359–364, Oct. 1996, doi: 10.1080/0161-119691885040.

[45] I. J. Cox, G. Doërr, and T. Furon, “Watermarking is not cryptography,” in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 4283 LNCS, pp. 1–15, 2006, doi: 10.1007/11922841_1.

[46] D. Rijmenants, “Is One-time Pad History ?,” *Cipher Machines & Cryptology*, pp. 1–4, 2009, [Online]. Available: http://users.telenet.be/d.rijmenants.

[47] M. Borowski and M. Lesniewicz, “Modern usage of ‘old’ one-time pad,” *2012 Military Communications and Information Systems Conference, MCC 2012*, pp. 243–247, 2012.

[48] M. A. T. Shakil and M. R. Islam, “An efficient modification to Playfair cipher,” *ULAB Journal of Science and Engineering*, vol. 5, no. 1, pp. 26–30, 2014.

[49] H. E. R., “Memoirs and Correspondence of Lyon Playfair, First Lord Playfair of St. Andrews, P.C., G.C.B., LL.D., F.R.S,” *Nature*, vol. 61, no. 1571, pp. 121–122, 1899, doi: 10.1038/061121a0.

[50] J. F. Dooley, “Crypto and the war to end all wars: 1914–1918,” in *SpringerBriefs in Computer Science*, pp. 43–51, 2013, doi: 10.1007/978-3-319-01628-3_5.

[51] D. Asamoah, E. Ofori, S. Opoku, and J. Danso, “Measuring the Performance of Image Contrast Enhancement Technique,” *International Journal of Computer Applications*, vol. 181, no. 22, pp. 6–13, 2018, doi: 10.5120/ijca2018917899.

[52] S. Ramakrishnan, “Introductory Chapter: Digital Image and Video Watermarking and Steganography,” in *Digital Image and Video Watermarking and Steganography [Working Title]*, IntechOpen, 2019, doi: 10.5772/intechopen.84984.

BIOGRAPHIES OF AUTHORS

Nasharuddin Bin Zainal he is an esteemed academic and prominent researcher in the field of Computer Engineering. He holds a Doctor of Engineering (Dr.Eng.) degree in International Development from the Tokyo Institute of Technology. Additionally, he has completed his Master of Engineering (M.Eng.) in Communication and Computer from Universiti Kebangsaan Malaysia, and a Bachelor of Engineering (B.Eng.) in Information Engineering (Computer Engineering) from Tokyo Institute of Technology. His research interests span a wide range of cutting-edge domains, including image and video processing, pattern recognition, and robotics. His valuable contributions in these areas have been notably associated with Universiti Kebangsaan Malaysia. With his extensive academic achievements and expertise, He has become a respected Associate Professor, inspiring both students and fellow researchers alike. He actively contributes to the advancement of knowledge and technology in his field. He can be contacted at email: nasharuddin.zainal@ukm.edu.my.

Alaa Rishek Hoshi he is a dedicated and accomplished scholar with a profound educational background in the field of Software Engineering and Information Technology. In 2001, he obtained his Bachelor of Science (B.Sc.) degree in Software Engineering from Rafidain University College, Iraq/Baghdad, marking the beginning of his academic journey. Driven by a passion for continuous learning, he pursued further specialization in the field of Website Technology, earning a Higher Diploma from the Informatic Institution for Postgraduate Studies, Iraq/Baghdad, in 2010. In 2016, he expanded his horizons and obtained a Master's degree in Information Technology from Cankaya University, Turkey/Ankara. This program further honed his skills in advanced Information Technology concepts, contributing to his diverse expertise. Continuing his pursuit of academic excellence, he embarked on a Ph.D. journey at (Universiti Kebangsaan Malaysia) in 2019. As a Ph.D. student, he delves deeper into research and exploration within his chosen field. ALAA's educational achievements highlight his commitment to the advancement of knowledge and expertise in software engineering and information technology. His diverse academic background, ranging from software engineering to website technology and information technology, demonstrates his versatility and depth of understanding. He can be contacted at email: alaa.wn@gmail.com.

Mahamod Ismail he is a distinguished academic and researcher renowned for his expertise in the field of Wireless Communication and Networking. With a prolific career, he has served as a Professor at the Department of Electrical, Electronics and System Engineering, Faculty of Engineering and Built Environment, Universiti Kebangsaan Malaysia, and now he is retired. Throughout his illustrious academic journey, he has made significant contributions to the advancement of wireless communication and networking technologies. His extensive research and profound knowledge have garnered him widespread recognition in the academic community. As a dedicated educator, he mentored numerous students, inspiring them to excel in the domain of electrical engineering and communication systems. His influence and impact continue to resonate within academic circles. His research interests encompass a broad spectrum of wireless communication and networking areas, reflecting his passion for exploring cutting-edge technologies and applications. Upon his retirement, he remains actively engaged in the academic landscape, sharing his expertise and insights with peers and researchers worldwide. He welcomes collaborations and inquiries from the academic and professional community. For any communications or collaboration opportunities, He can be contacted at email: mahamod@gmail.com.

Abd Al-Razak T. Rahem he is an accomplished engineer and dedicated educator in the fields of electrical, electronics, and systems engineering. He holds a Ph.D. from the Faculty of Engineering and Built Environment at Universiti Kebangsaan Malaysia, Malaysia, which he obtained from 2013 to 2016. From 2010 to 2012, He pursued a Master of Science in Technology (Information Technology) at the College of Engineering, Bharati Vidyapeeth Deemed University, India/Pune. This program provided him with a profound understanding of information technology and its applications. In his formative years, from 1998 to 2002, He completed his Bachelor of Science in Computer Engineering and Information Technology from the distinguished University of Technology, Iraq/Baghdad. This foundational education equipped him with essential skills and knowledge in the realm of computer engineering. Currently, He serves as an esteemed Instructor at the Department of Computers, Faculty of Engineering, Middle Technical University (government). In this role, he passionately imparts his extensive expertise to nurture and guide the next generation of engineers. He can be contacted at email: abdtareq@gmail.com.

Salim Muhsin Wadi he is an esteemed scholar and educator with a strong foundation in Communication Engineering. His educational journey has been marked by significant academic accomplishments and contributions to the field. Salim's academic pursuits began with a Bachelor of Science (B.Sc.) degree in Communication Techniques Engineering from AL-Najaf Technical College in 2002. Eager to expand his expertise, he pursued a Master of Science (M.Sc.) in Communication Engineering from the Department of Electric and Electronic at the University of Technology in 2005. His dedication to advanced knowledge continued as he successfully earned a Ph.D. in Communication Engineering from the Department of Electrical, Electronic, and System Engineering at The National University of Malaysia in 2015. Currently, he holds the esteemed position of Senior Lecturer at Technical College-Najaf, specifically within the Communications Techniques Engineering Department in Najaf, Iraq. In this role, he imparts his extensive knowledge and expertise to shape the future generation of engineers. His dedication to enhancing the understanding and applications of communication technologies underscores his commitment to progress and innovation. He can be contacted at email: salim2007555@yahoo.com.