Hindawi
Mathematical Problems in Engineering
Volume 2023, Article ID 5060564, 11 pages
https://doi.org/10.1155/2023/5060564

Research Article

Maximize the Security for Image Processing Using an Improved Watermarking Approach

Manoj Kumar Tyagi,[1] Cuddapah Anitha,[2] R. Ramyadevi,[3] Sunita Pachar,[4] Ravi Kumar Tata,[5] Preetam Suman,[6] and Fardin Ahmadi [7]

[1]*Computer Science and Information Technology, KIET Group of Institutions, Delhi-NCR, Muradnagar, Ghaziabad, Uttar Pradesh, India*
[2]*School of Computing, Computer Science and Engineering, Mohan Babu University (Erstwhile Sree Vidyaniketan Engineering College), Tirupati 517102, Andhra Pradesh, India*
[3]*Department of Computer Science and Engineering, Saveetha Engineering College, Chennai, India*
[4]*IBM Department, GLA University, Mathura, Uttar Pradesh, India*
[5]*Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Andhra Pradesh, India*
[6]*School of Computing Science and Engineering, VIT Bhopal University, Bhopal-Indore Highway, Kothrikalan, Sehore, Madhya Pradesh 466114, India*
[7]*Rana University, Kabul, Afghanistan*

Correspondence should be addressed to Fardin Ahmadi; fardin.ahmadi@bcs.ru.edu.af

Received 31 July 2022; Revised 29 September 2022; Accepted 24 November 2022; Published 27 September 2023

Academic Editor: Savita Gupta

Creating a dependable and effective digital image watermarking (WM) method necessitates balancing imperceptibility, resilience, capacity, and security. Several studies have combined spatial and transform domains to meet these needs. We investigated the current state of hybrid digital image WM. When developing a hybrid WM strategy, it is critical to consider software compatibility. Following a brief review of the literature, we used a table to analyse and evaluate current hybrid approaches. Furthermore, the limitations and possibilities of these approaches are discussed. We investigated the limitations of current research methodologies and proposed new research directions. The internet's role in distributing digital material has resulted in more digitalisation and more complex copyright concerns. Copyright breaches are being reduced through the deployment of innovative digital WM techniques. As a result of this research, a WM system capable of dealing with a wide range of threats is being developed. The goal of this study is to maximise security while maintaining visibility and resilience. Discrete wavelets transform (DWT) and singular value decomposition (SVD) were used to investigate covert operations; DWT was used to isolate each level of the host image, which was then processed using SVD. At the time, normalized correlation was the best method for measuring watermarked images. In research, DWT–SVD was more accurate in detecting assaults; it shows structural similarity index and normalized correlation are 98.4 and 98.35, respectively. Watermarked images can withstand a variety of assaults due to their invisibility and resilience; this system repels assaults that alter pixel values better than traditional methods.

1. Introduction

The following sections summarise the main points, every day, multimedia advances without sacrificing quality, digital images can be instantly modified, copied, reproduced, and transmitted over local networks and the Internet. The multimedia revolution has an impact on image security and privacy. Digital image watermarking (WM) has become an important way to protect multimedia content and determine who owns its use in recent years. The watermark information is implanted in a media item (text, image, sound, and video), then recovered or recognised to approve the item's genuineness [1]. An eavesdropper cannot change or replace the watermark data in the host data, thus protecting it. By using this strategy, you can be confident that the content you are using is genuine, that its integrity has been verified, and that your images have

been safeguarded. A watermark safeguards the image quality and aesthetic appeal of the cover. Several spatial or transform-based approaches have been developed in recent years. The study made the following contributions: we exposed flaws in existing hybrid digital image WM methods. The protection of sensitive electronic information has been and will continue to be one of the most important problems facing research in the scientific community. Because of the proliferation of Internet-connected gadgets, it is now simpler to make unauthorised copies of digital information, authenticate it, and distribute it to third parties. These applications include broadcasting and tracking. Since electronic information has been widely published and distributed via the Internet, there has been an increase in the frequency of various violations of copyright, including unauthorised use and copying, as well as theft of online content. The Internet is the distinguishing technology of the information age, just like the electrical engine was the push for technical growth during the industrial age. Users may engage in a wide range of communications in several ways from any location on Earth due to the linked structure of these networks and the fact that the bulk of them are backed by technology that allows wireless transmission. This immediately affects a user's ability to connect to the internet. The Internet is the distinguishing technology of the information age, just like the electrical engine was the push for technical growth during the industrial age. Users may engage in a wide range of communications in several ways from any location on Earth due to the linked structure of these networks and the fact that the bulk of them are backed by technology that allows wireless transmission. This immediately affects a user's ability to connect to the internet. If digital images are ever going to be worth a significant amount of money in the future, it is imperative that their intellectual property rights be safeguarded. It is possible to safeguard these images by utilising the cutting-edge method of digital WM [2, 3], which is not only efficient but also feasible using the WM approach; any data belonging to the owner that is going to be preserved or shared over the internet may be encrypted. The demonstration of ownership may be accomplished by the acquisition of encoded watermark data at the appropriate time using a variety of technologies, application domains, and many other online platform-based systems. There have been very few investigations exploring the use of digital WM as a technique of protecting images that were captured with a digital camera. Over the course of the past several years, several various alternative WM techniques have been created and implemented. The WM of a digital image may be extracted with the use of algorithms, which can then be modified [3–6]. In the context of WM in general, attacks that seek to erase or otherwise damage encoded watermark data could be a real possibility. These kinds of attacks might be a concern. There is a possibility that the WM process might be affected inadvertently by actions that are essential to the maintenance or distribution of the content. The word "unintentional" could be used to describe attacks of this kind. This may be achieved in one of two ways: either computationally or physically. Both approaches are viable options. However, to extract WM, it is necessary to fulfil several additional prerequisite requirements. Both intentional and accidental assaults have the potential to corrupt the data kept on the host as well as the data that is encoded in WM. Therefore, it's possible that taking a statistical approach will produce better results than trying to extract WM in an organised and planned method.

To create a form of semisequence that may be used to integrate many watermark images into one, a cryptographic approach that uses pseudorandom data may be utilised to build the sequence. As a watermark, you have the option of using either a monochromatic or two-color image [7–11]. Approaches for the protection of digital material can be implemented in WM methods. Two examples of these techniques are scatter-spectral (SS) and quantisation index manipulation (QIM). The abbreviations SS and QIM refer to the procedures of SS manipulation and QIM, respectively. Both alternative and cumulative methods are referred to in a manner that is virtually equivalent when they are referred to in this manner. Spatial domain watermarking (STDM) is a procedure that takes both the dependability of SS and the efficiency of QIM and combines them. Systems for WM anything need to have a payload in addition to being reliable and valid. Images that were processed in the spatial domain utilising filtering techniques such as brightness, softness, and noise reduction are substantially more trustworthy than those that were processed using discrete cosine transform (DCT). The ability of discrete wavelets transform (DWT) to edit digital images that have been watermarked has contributed to the broad use of the tool. An initial set of processes will work their way down, beginning with the DWT domain [12–15], going from the domain with the highest resolution all the way down to the domain with the lowest resolution. When creating digital images, it is important to make sure that the intensity of the watermark masking is raised throughout the process. This ensures that the product will last for a longer period. Currently, the use of singular value decomposition (SVD) as a method for adding a watermark to digital images is already regarded to be standard practise. Even if the user is attacked in a variety of ways while SVD is running, the concealed image will not be corrupted since it will still be protected. Companies are already utilising testing platforms to develop algorithms that can interact with their surroundings in a manner that is more helpful and to glean insights that have never been discovered before.

The removal of noise and an enhancement in the image's overall clarity are two examples of how digital image processing may enhance the overall quality of an image. The use of neural networks to construct mappings between clear and distorted images to enhance deblurring has been increasingly popular in recent years [16, 17]. To improve the effectiveness of the deblurring process, this step has been taken. The images that were sharp and clear were contrasted with those that were fuzzy or otherwise misleading in some other way. Convolutional neural network (CNN) has the potential to offer excellent results in image denoising because of its vast modelling capacity as well as major network and architectural advancements. CNN makes use of a deep structure model, which can make greater use of visual information in both its training and its noise reduction processes. To

do this, the use of a CNN is necessary; batch normalisation and the rectified linear unit, both of which have witnessed significant advancements in recent years, are currently considered to be two of the most essential learning approaches to produce CNNs, as well as the teaching of those methodologies. It is dangerous to employ this method of reducing noise on an image that has a watermark since the watermark itself is nothing more than a string of noise. Digitized watermark images, particularly those whose level of noise has been increased or lowered, offer a lot of room for attack [18–20]. This is especially true for images in which the noise level has been altered. Because of this, the starting value of each pixel in an image is the same for both procedures. An image is composed of a very large number of individual dots called pixels. Researchers conducted tests using Fully Convolutional Neural Networks (FCNNs) to see whether the FCNNs could recognise watermarks in images that already included watermarks. In the course of this study, a noteworthy discovery emerged: the normalization of denoising could potentially serve as an independent avenue for launching attacks when implementing computerized digital WM on images.

Images that have been digitally watermarked are susceptible to a broad variety of different attacks. These assaults make use of a range of tactics, some of which include backdrop removal, geometric alteration, loss compression, and additive noise. Any one of these methods will do the trick in removing watermarks from digital images. The properties of the noise include both salt-and-pepper noise as well as multiplicative noise. The most common type of attack used against digital WM images is one that involves the introduction of Gaussian noise. The use of salt-and-pepper sounds may take a greyscale image with 8 bits that appear to be white and white. The build-up of Gaussian noise results in a decline in both the image's quality and its look. Image filtering methods such as averaging, Wiener, median, and Gaussian filtration can be utilised to remove a watermark from a digital image. Other techniques of image filtration, such as median and Gaussian filtration, are also available. The median filter is an adaptive nonlinear filtering method that may be utilised to retain the borders of the image while simultaneously minimising the amount of noise that is present in the image. The Wiener filter is widely utilised as a means of reducing the overall impression of blur in the images they capture. When an averaging filter is used, the value of each pixel is replaced with a weighted average of the values of its near neighbours as well as itself. This new value is then used to represent the pixel. As a direct consequence of this, there is less variation in the brightness of individual pixels. It is usual practise to blur images, as doing so lessens both the intensity of the image and the amount of distortion it includes when using a Gaussian filter to process the image. Image modification techniques such as scaling, rotating, clipping, and translating may be used to change images that were created using geometric assaults [21, 22]. Other image modification techniques that can be used include skewing and blurring. It is possible to speak about "local" geometric assaults while referring to both "local" and "global" attacks. Attackers armed with chainsaws are only able to completely wipe off a small area of the final image.

To produce a wavelet tree quantisation-based blind image that is more resistant to geometric distortions like rotation, scaling, or cutting, stenographic techniques were utilised in the creation process. This method was developed to address the challenges using this strategy; it is simple to avoid being caught by cropping and rotating assaults. A method of image WM that is immune to several forms of cryptographic assaults, such as translation and rotation [23]. His method is described in more detail in the reference. Together with his colleagues, he came up with a method for mathematically sound image WM [24] that was founded on the change of histograms. This method was mathematically sound. This method considers the image's translations as part of the total transformation, in addition to rotation, cropping, and scaling, which are the other components of the transformation. In order to protect their images from being stolen using geometrical approaches [25], a method of WM for persistent images. It is not necessary to use DCT to embed a host image; in fact, you can choose from a variety of different methods. There are two other methods for modifying watermark information that may be used in addition to the JPEG compression strategy and the continuous gain attack (CGA). CGA attack settings were utilised to adjust the levels of brightness and darkness in digital images that had been watermarked. By utilising a model that considers the user's point of view [26] were able to make the STDM WM approach more resistant to JPEG compression. Other researchers [27] have demonstrated how they improved a JPEG compression approach [28] that is utilised in image WM systems. The findings of this research were presented in a report that was published in Computer Graphics Forum. In the previous few years, the utilisation of CNNs has become an increasingly crucial component in the process of the generation of an image prior to [29] designed the method known as deep network CNN (DnCNN) with the intention of removing noise from images. In this framework, you should make use of the convolutional kernels that are utilised in the process of identifying attacks on image watermarks. To construct a network with this level of complexity, it is required to use a broad array of architecture and many convolutional layers. Since they are all components of the hidden layer, Convolution, BatchNorm, and Relu are all utilised in the last phase of the downsampling process. The network was taught to perform blinded denoising in conjunction with cumulative Gaussian denoising. With the use of these methods, it is conceivable that the identification of attacks that make use of images with watermarks might be significantly enhanced [30] FFDNet. This apparatus can function normally in a broad variety of loud environments, including those with exceptionally high noise levels. FFDNet utilises a CNN model that is superior in both speed and accuracy compared to that of DnCNN, which uses a CNN model that is equal to FFDNet's. When it comes to precisely detecting specific sounds, this approach falls short, even though it is often believed to be accurate. These images can be utilised in CNN layers. To be able to see images that have been watermarked,

one must first come to terms with the fact that watermarks are both imperceptible and permanent over the course of time [31]. Researchers have investigated the concept of a trade-off or compromise to develop a solution that satisfies both the need for invisibility and the requirement for resistance. Among the numerous important results and discoveries that came out of this research are the following: by employing a hybrid model that can recognise a broad variety of attacks on watermarked images, the WM approach was given an increased level of protection. Through the utilisation of a scaling factor, we were successful in locating a medium between the invisibility and robustness linkages. If this capability is developed, controlling images that have been watermarked may become much simpler. This paper discusses the challenges and potential solutions for future researchers. Part 2 looks at the literature review part. Section 3 shows the proposed hybrid method for the digital WM of images. Section 4 goes into detail about the results, the conclusion is shared in Section 5.

2. Literature Review

The study proposes a copyright-protecting digital image WM approach based on DWTs and DCTs. Watermark images are encrypted using the Arnold transform; the image is more aesthetically pleasing after the system computes DWT LL sub-band block-based DCT. In this situation, a watermark created from the DCT coefficient midfrequency is used. After the host image has been processed with a 2L DWT subband, the watermark is added to the unique values recorded in the HL/LH format. The DWT–SVD digital WM approach can be built using DWT and SVD wavelet fusion techniques. It enables them to do more with less resources while limiting their exposure. The watermark can be understood even if the original image is lost. WM techniques, such as DWT–SVD hybrid WM [32–34], can be utilised to successfully integrate data into an image. Images with watermarks have noticeable changes in their diagonal singular value coefficients. When DWT–DCT–SVD was made, both the privacy of medical imaging and the protection of intellectual property rights were considered. To improve the approach's performance, the proposed WM method employs discrete wavelet transforms, DCTs, and SVDs. The DWT improves the accuracy of potentially uncovered crucial data by basing its analysis on aspects of the human visual system. This is because the DWT based its analysis on these characteristics. As a result, it is easier to select solutions that are beneficial to you. The DCT will remain unknown for an extended period. Finally, the major advantage of employing this technique is that it assures the SVD's single values are accurate. When a small amount of data, known as perturbations, is introduced to an image, it indicates that the values of the individual pixels do not fluctuate much. Several independent analyses have proved that the approach we describe is effective. It is not only easy to add a substantial amount of information without sacrificing image quality (using a 512×512 watermark), but it is also resistant to a wide range of various forms of attacks. As a result, employing this method to safeguard sensitive information is a wise decision.

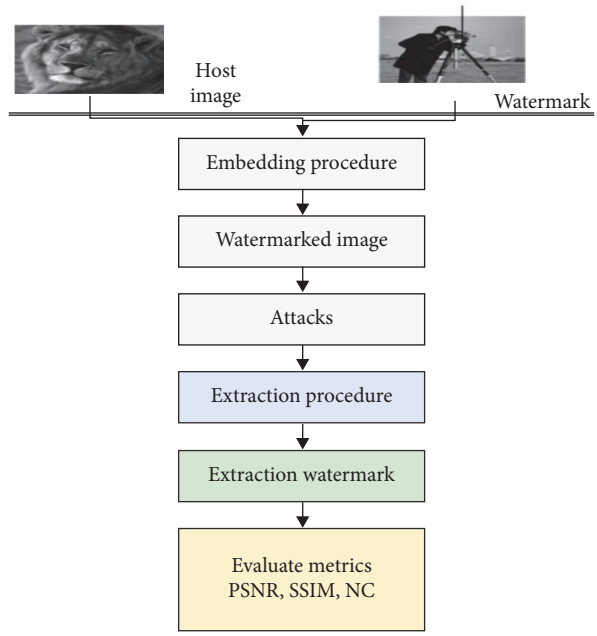

Figure 1: Watermarking procedure.

WM can be used to increase the signal-to-noise ratio (PSNR) of an image; steps for WM are shown in Figure 1. There are no scaling, filtering, cropping, or rotating issues with the approach provided. Another study suggests a method for preserving telemedicine medical data. To safely transmit medical data over a network, this study employs both DWT and DCT. In this medical host scenario, the region of interest (ROI) and non-region of interest (NROI) are distinct concepts (the ROI). In ROI and NROI, the image has both image and text watermarks. To add security before embedding a text watermark, the Rivest–Shamir–Adleman method is used. When adding a watermark, this hybrid method has no effect on the image's visual quality. A hybrid DCT–DWT technique with auto thresholding is another option. Before DWT, the host image is DCT-transformed. DWT and DCT can be combined to create a robust and unnoticed method [35]. The watermark is embedded in this study using DWT–DCT coefficients. This method is illustrative. According to studies, this method is resistant to histogram equalisation, compression, cropping, and noise addition. DWT combines DWT, DCT, and SVD to improve the safety of medical images. This medical image contains a hidden watermark. The medical host image has been 3L DWT. Finally, the host image is DCT and SVD transformed. The system reduces the visibility and resilience of Gaussian, salt-and-pepper, and Wiener noise addition, as well as Wiener, average, and median filtering. Edge detection replaces older methods for determining the best location to include a watermark [36]. To balance imperceptibility and resilience, particle swarm optimisation is used. If you require more storage, consider [37], which describes a frequency domain DCT–SVD hybrid technique. Arnold is used in this method to texture the watermark logo. Both watermark logo symbol vector decomposition and host image

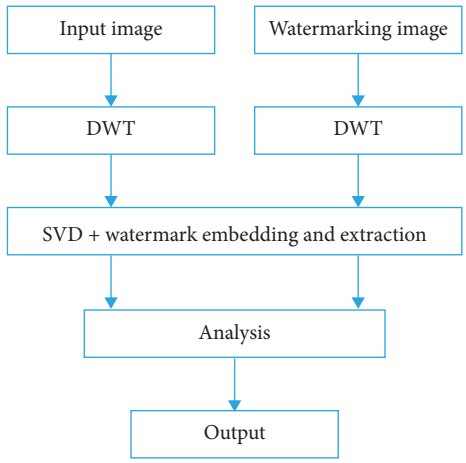

Figure 2: The watermark embedding procedure.

DCT processing are completed at this stage. Weights are chosen based on the host image's lowered singular values for the best results and the least distortion. To protect copyrighted material, this method [38] employs DFT and DCT. The demonstration demonstrates that the watermarked and host images are identical. The system can withstand more severe attacks. The new method improved imperceptibility and resilience. Another study employs DCT and DWT to secure watermark colour images. A three-component RGB host image must be split into red, blue, and green before DCT and DWT can be applied. Arnold secures the watermarked image. The encrypted watermark's DCT coefficient is calculated after it has been divided into equal-sized subsets. The system is more imperceptible than other methods. WM technologies that are blind and nonblind are recommended, with the former used on the inside and the latter on the outside. In 2020, researchers published a watermark reinforcement learning approach. *Q* learning and matrix factorisation were used. To determine which host blocks to integrate, *Q* learning employs trial-and-error learning. It is more resilient and undetectable than random embedding. It lacks the ability to withstand repeated attacks. Another paper [39] employs a genetic algorithm and SVM to select relevant regions and generate low-frequency regions; fuzzy entropy is used to improve the performance. A genetic algorithm is used to optimise the watermark strength in this case [40]. To find the best embedding function or block, use a genetic algorithm, ant colony optimisation, or the firefly algorithm. Machine learning and neural networks are more popular than ever [41, 42], and we present a less time-consuming DWT-based Spiking Neural Network (SNN). Extraction is viewed as an SNN-solvable optimisation problem by this network. Contourlet transforms, Kurtosis coefficients, and YCbCr spaces have all been implemented using neural networks.

Figure 2 depicts embedded watermarking process, to apply a watermark to an image, you must first do the following steps: a personalised watermark for your work might be created using this approach. After that, the watermark will be applied.

3. Hybrid Method for the Digital Watermarking of Images

One way for securing multimedia material is to use digital watermarks, which can obscure the data's original source [28]. Everything works out in the end, using an embedding strategy and a secret key, a watermark has been imprinted on the host's image. Following that, folks will swap watermarked images to remove the watermark image from the system; a certain technique and key must be used, Figure 3 depicts the hybrid method.

Procedures in space are vulnerable to attacks and manipulation [29]; as a result, transform domain solutions for multimedia security have gained traction [30]. Because of the payload limitations of transform domain methods [31], hybrid domain approaches have emerged. Two or more photo changes are required for hybrid domain WM, and transformation domain methods benefit from hybrid domain strategies [32]. These approaches are most used to protect copyrights and multimedia content, but there are other applications available. An image will first go through the DCT, DFT, DWT, and SVD editing stages before commencing the hybrid digital image WM process. It is most likely the consequence of some form of hybridisation. The *n*-blocks are then split down into a lower number of bits once the watermark image has been encrypted [43, 44]. Following this, a watermark image is encrypted using a block-based watermark that can be found dispersed across the image in entirely random areas. Each chunk has *N* bytes at this point, and the previously specified watermark will be applied to the image. Reverse the process to remove the watermark, and the hybrid watermark embedding scheme is depicted in Figure 4.

When working with watermarked images, having a mechanism for extracting features is critical. It is critical to extract characteristics from the watermarked image to determine which elements are the most important. When discussing watermarked images, it is customary to refer to both the image-maker and the result. Figure 5 depicts the steps that must be taken to remove watermarks from previously watermarked images.

WM images makes it more difficult to sell or share them since they cannot be modified or removed after capture. This method can help to avoid data theft and unauthorised use, both transforms and steganographic approaches must be used for hybrid WM to operate. Standards for digital image WM in hybrid systems because of the confluence of multimedia and the Internet, digital images may now be printed, transferred, and published over a private network or the Internet. WM digital images are accomplished by adding extra data to the host medium. This allows you to limit who can see a piece of information, and it is critical that the system works properly. The hybrid digital image WM technique can only be carried out effectively if certain parameters are met. It is critical that the system stays undiscovered while being robust, scalable, and secure. We have included a graphic illustration of their components in Figure 6 for your consideration.

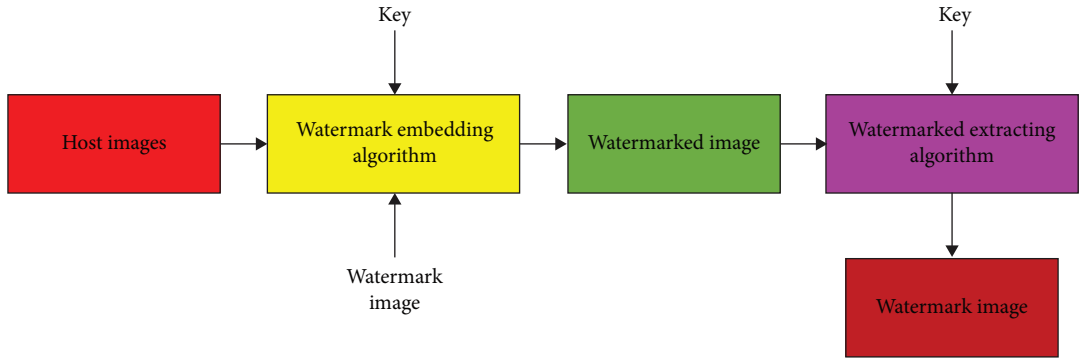

Figure 3: Watermark embedding and extraction is a two-step technique.

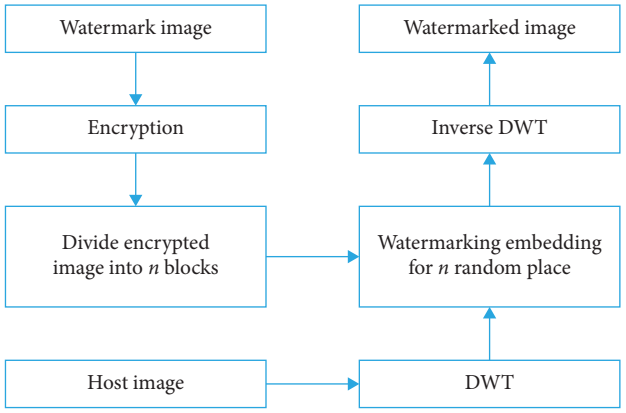

Figure 4: Digital image watermark embedding framework for hybrid techniques.

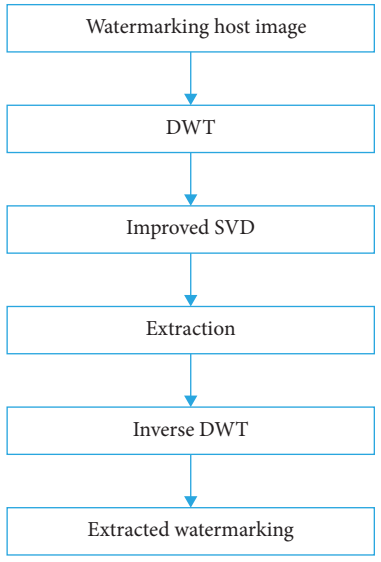

Figure 5: Feature extracting procedure.

The performance of hybrid digital image WM solutions is evaluated using imperceptibility. The watermarked and host images look identical. Human eyes cannot distinguish between dimmed brightness and contrast [28–33]. Because of the durability of the watermark, the watermarked image may still be

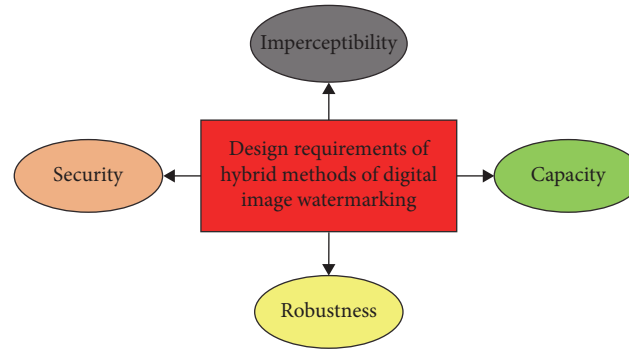

Figure 6: Specifications necessity for hybrid watermarking approach.

traceable to its owner after standard image processing. Using this method aids in the retention of the watermark. In addition to "robustness," the word "fragility" and "semi-fragility" can be used to denote it. The amount of data that may be stored inside an image is known as its payload capacity. A host image can only store so much data. It may be challenging to incorporate more watermark bits into the image being stored. Each one of these conditions must be met before the fingerprinting procedure can begin. As a preventive step, the image containing the watermark has been encrypted. Images containing watermarks can be hidden in a variety of ways.

When it comes to digital photo WM, you may choose between a spatial or transformational watermark technique that can be used simultaneously. These approaches are classified as spatial domain techniques and include patchwork, LSB, and ISB. DCT, DFT, DWT, and SVD are a few transformation-domain techniques that may be employed in this sector. The hybrid approach to domains integrates a variety of approaches within its overarching framework. Algorithms of this type include DCT/DFT/DWT/SVD. As seen in Figure 7, there are several techniques for WM images.

The efficacy of assaults like image manipulation and sharpening are greatly decreased when hybrid digital photo WM technologies are utilised. These various techniques are getting increasingly computationally intensive (time and space). It is physically impossible for them to have all these attributes at the same time. Concerns about users' capacity to retain their privacy have directly resulted from the introduction of this technology. Computers, on the other hand, rely on more complex

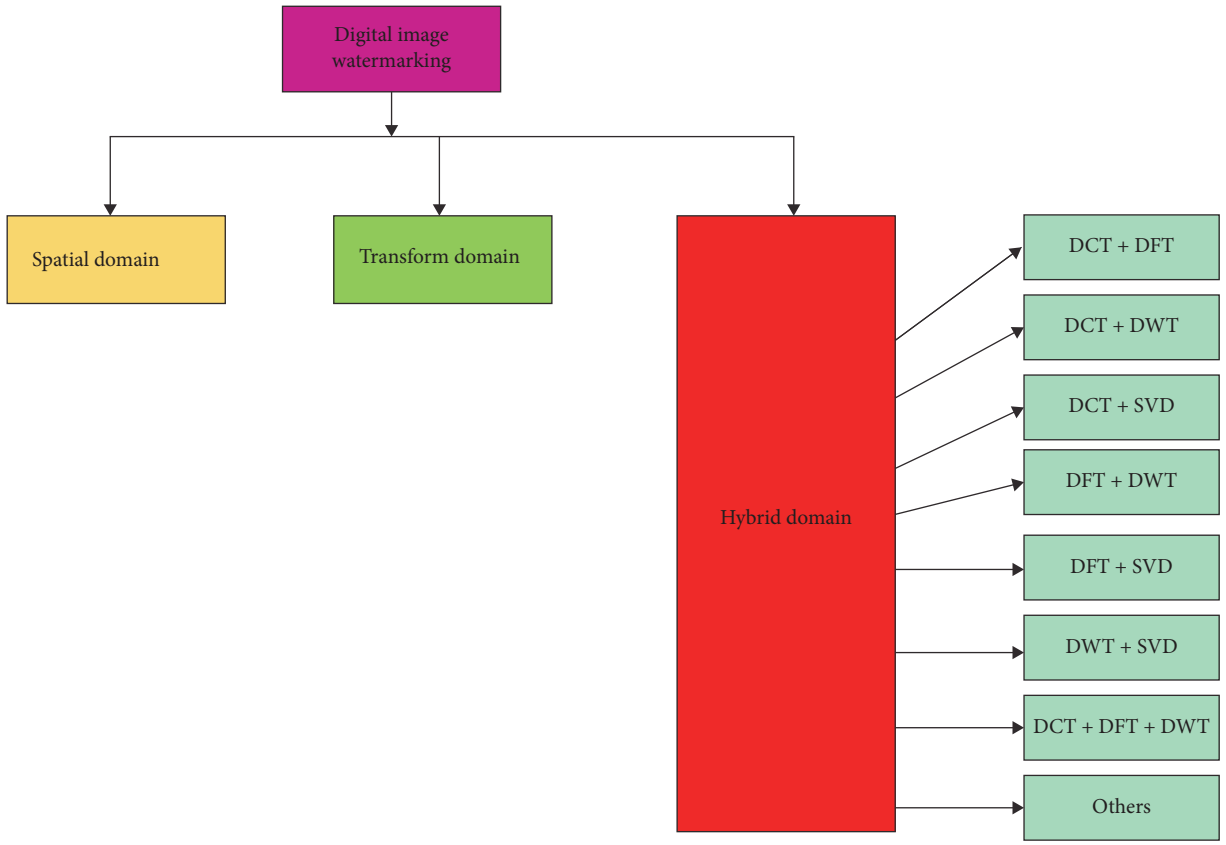

Figure 7: Watermarking hybrid domain possibilities.

algorithms for security, whereas internet-connected devices use simpler approaches. The Internet of Things (IoT) necessitates less storage space and processing power [36]. Blockchain technology allows for decentralised authentication. A blockchain is a decentralised digital ledger made up of encrypted, linked data chunks that are protected by encryption. The digital signature of the host photo is saved using blockchain technology. An attacker cannot alter the host's appearance. The updated area and host image can be validated using the blockchain signature. Near-field communication can be used to authenticate pharmaceuticals on the IoT [38]. ROR is used to secure session keys (real-or-random). This model saves money on computers and transmission. Content-based image retrieval does not require information about cloud servers. Photos in this demo are feature vectors, not bitmaps. The feature vector is protected by k-neighbors. LBRAPS, a lightweight authentication technique for RFID data based on blockchain, will benefit 5G mobile supply chains. The method defends against multiple attackers [40]. Outsiders can examine cloud server data from here. Cloud server and smart metre authentication allow for the secure exchange of cloud server data. Bitwise XOR and cryptographic hash algorithms have been shown in experiments to make the procedure more secure.

4. Results

It is required to use a range of sizes when computing the scaling factor, and this information must subsequently be provided to optimal edge detection. Using watermarked images within the suggested framework allows for the management of image invisibility and the strengthening of images against various forms of assaults. Lions, just like filmmakers, have certain requirements when it comes to the size of their images and the values of their important qualities; we are aware of both requirements due to our familiarity with each of these professions. By keeping an eye on this connection, one can gain control over image invisibility and durability. The normalized correlation measure is used to show the relative importance of a variety of unique elements in connection to assaults (Figure 8).

For example, it was revealed that motion blur and average filters had exceptionally low PSNR values. The PSNR values that have been measured are shown on an axis. All the attack scale variables are presented along the labelled axis, which reads. Most of the watermark images that we looked at displayed symptoms associated with a wide range of diseases. These techniques were used to address difficulties such as motion blur, spherical noise compression, and histogram equivalency. These criteria were used to assess the watermark image's resilience to a variety of attacks. Using this approach, you may assess how resistant the watermark image is to various assaults. An assault was carried out on the watermark images to establish how well they would survive the normalized correlation measure.

Figure 9 summarises the experiment's findings because of technological developments; the screening procedure for

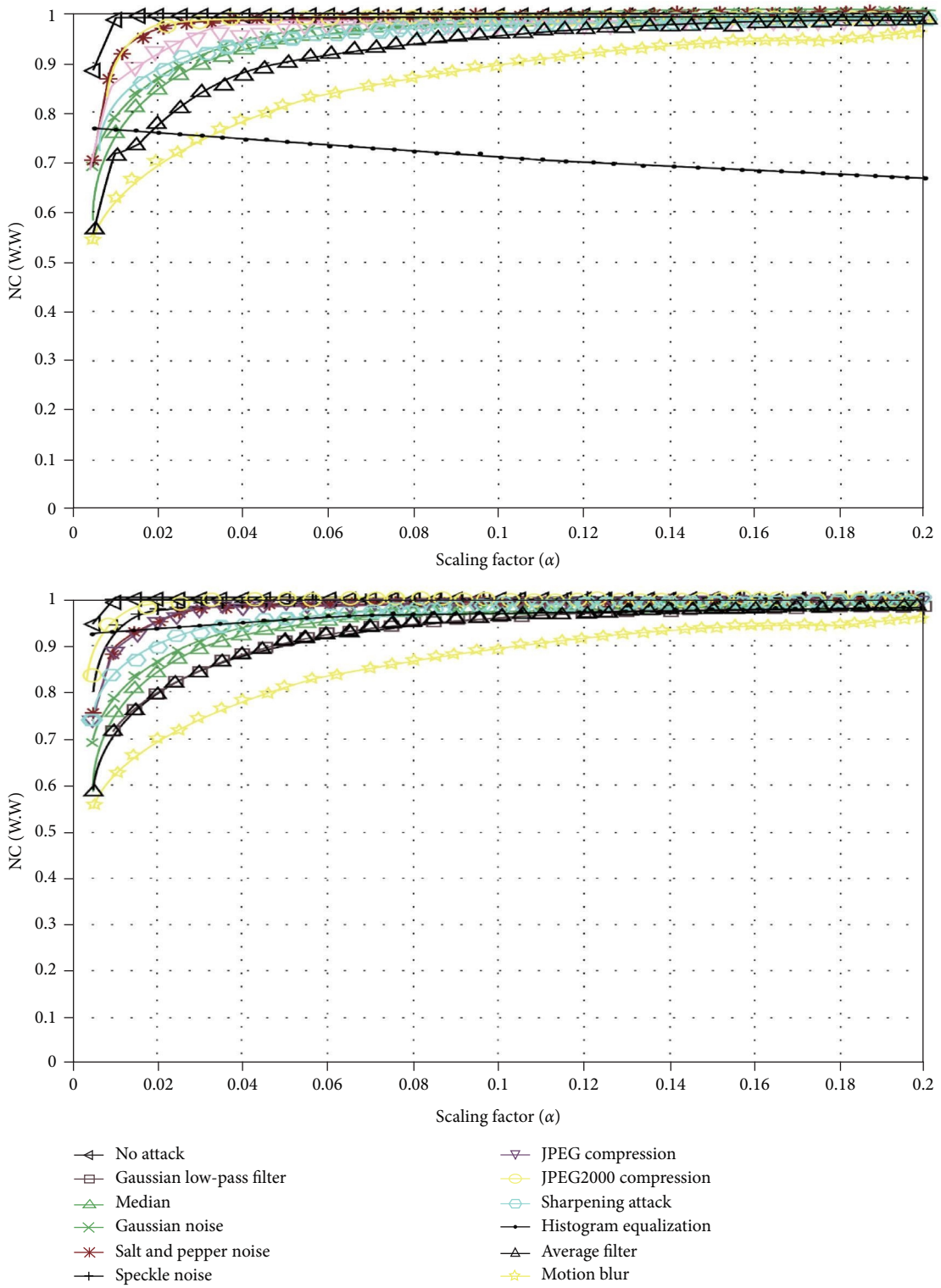

Figure 8: The NC approach was utilised to scale both the lion image and the image of Lina.

averting various forms of assaults proceeded quite successfully. Following the assaults, watermarked images were gathered and analysed using DWT–SVD. Table 1 depicts the study's findings; the values offered by NC are superior to the bulk of attacks.

The researchers used a total of six distinct procedures, some of which were rather difficult and included the use of techniques such as Gaussian filtering and median filtering. As a direct result of the investigation, the quality of previously wrecked images has greatly improved. Multiple attacks revealed that the proposed strategy was significantly more successful than the present one. According to the study's findings, this strategy had a considerable influence on the

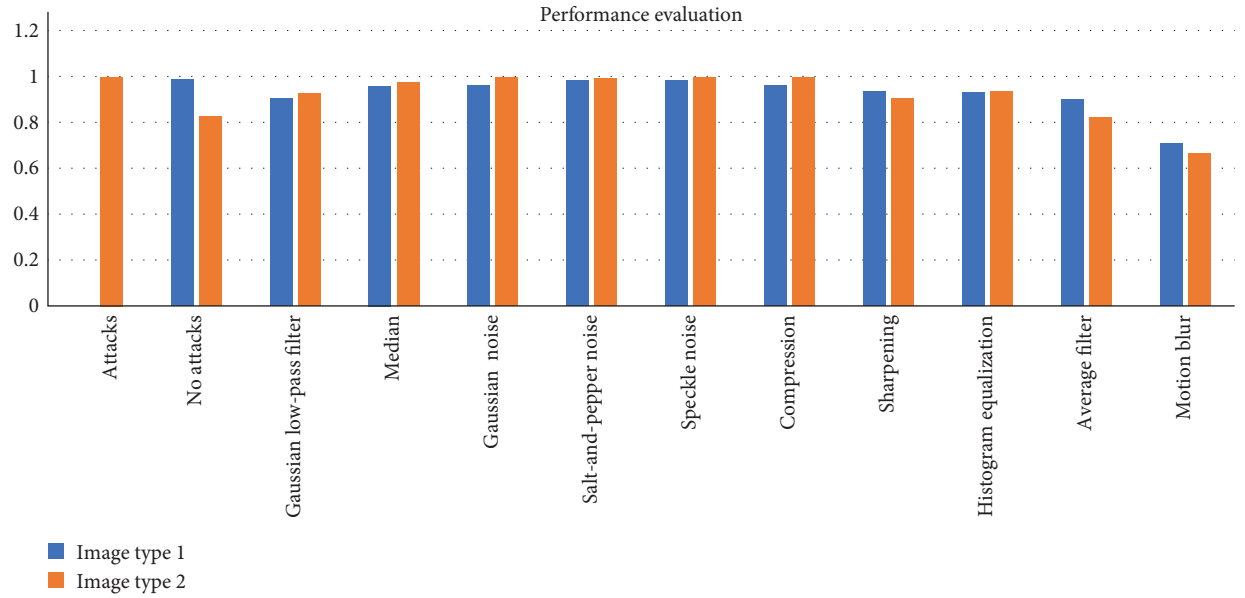

Figure 9: Performance evaluation of the proposed method.

Table 1: Performance evaluation of the proposed method with traditional methods.

Attacks or noises	Proposed system		Existing system	
	Normalized correlation	Structural similarity index	Normalized correlation	Structural similarity index
Motion blur	96.90	98.2	94.4	86.7
Gaussian noise	98.35	98.4	88.9	62.3
Speckle noise	91.71	97.7	83.1	42.9

desired objectives. When analysing watermarked photos, Structural Similarity Index (SSIM) and PSNR were used to determine their invisibility, whereas normalized correlation was utilised to determine their resistance to the assaults that were employed. The study's empirical data revealed that normalized correlation performed admirably in analysing each of the assaults used. When the suggested system was compared to those currently in existence, it was discovered to have greater performance. This approach may help digital image WM since it allows unfettered mobility of the WM information as well as WM on the host image without causing any damage to either of them.

5. Conclusion

Images are included in multimedia data sets. Image authentication becomes difficult due to Internet traffic. IoT technologies and interactive multimedia data transfer make it easier to copy and distribute information. Making the system invisible, resilient, and data-embedding capable is just as important as ensuring the privacy of image data. Keep these difficulties in mind when WM digital images. To address these challenges, we concluded that existing hybrid techniques must be improved. Because of the dynamic nature of digital multimedia data transmission, it is now possible to easily regenerate information. The DWT–SVD approach will be used in this study to investigate a range of watermark assaults. We used scaling variables to study the relationship between being invisible and having a resilient character. Watermarks were expected to be implanted and removed in a manner that was both undetectable and resistant to numerous attacks for the purposes of the study. The following are some of the study's most notable findings: the DWT–SVD technique was utilised to extract a wide range of relevant data to identify all watermark attacks. To put the proposed approach to the test, hybrid DWT–SVD was applied to watermarked images. The SSIM, PSNR, and normalized correlation data were used to evaluate the proposed system's efficacy. When analysing watermarked photos, SSIM and PSNR were used to determine their invisibility, whereas normalized correlation was utilised to determine their resistance to the assaults that were employed. The study's empirical data revealed that normalized correlation performed admirably in analysing each of the assaults used. When the suggested system was compared to those currently in existence, it was discovered to have greater performance. This approach may help digital image WM since it allows unfettered mobility of the WM information as well as WM on the host image without causing any damage to either of them. Using the suggested approach, invisibility and resilience may be increased and regulated, allowing the system to respond to a wide range of threats at its best. Our aim is to

perfect this technology to the point where there is scarcely any quality loss in the watermarked image, and the restored watermark is almost immaculate. Watermark extraction accuracy should improve dramatically with the addition of this additional information. If the massive over dictionary was the primary focus of the investigation, other feature learning methodologies or training models might be used in possible future research paths.

Data Availability

ImageNet data is publicly available at the following URL: https://www.image-net.org/.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] P. Morasso, "Spatial control arm movements," *Experimental Brain Research*, vol. 42, pp. 223–227, 1981.

[2] Y. Uno, M. Kawato, and R. Suzuki, "Formation and control of optimal trajectory in human multijoint arm movement," *Biological Cybernetics*, vol. 61, pp. 89–101, 1989.

[3] L. P. Feng, L. B. Zheng, and P. Cao, "ADWT-DCT based blind watermarking algorithm for copyright protection," in *Proceedings of 3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT)*, pp. 455–458, Chengdu, China, July 2010.

[4] X. Zhou, J. Ma, and W. Du, "SoW: a hybrid DWT-SVD based secured image watermarking," in *Proceedings of the International Conference on Sensor Network Security Technology and Privacy Communication System (SNS & PCS)*, pp. 197–200, Nangang, China, May 2013.

[5] E. E.-D. Hemdan, N. El-Fishaw, G. Attiya, and F. Abd El-Samii, "C11. Hybrid digital image watermarking technique for data hiding," in *Proceedings of the 30th National Radio Science Conference*, pp. 220–227, Cairo, Egypt, April 2013.

[6] R. Nair and A. Bhagat, "An application of big data analytics in road transportation," in *Advances in Systems Analysis, Software Engineering, and High Performance Computing*, pp. 39–54, IGI Global, Hershey, PA, USA, 2018.

[7] R. Nair and A. Bhagat, "An introduction to clustering algorithms in big data," in *Encyclopedia of Information Science and Technology*, pp. 559–576, IGI Global, Hershey, PA, USA, 5th edition, 2021.

[8] R. Nair, S. N. Zafrullah, P. Vinayasree et al., "Blockchain-based decentralized cloud solutions for data transfer," in *Computational Intelligence and Neuroscience*, vol. 2022, pp. 1–12, Hindawi Limited, 2022.

[9] R. Kashyap, "Applications of wireless sensor networks in healthcare," in *Advances in Wireless Technologies and Telecommunication*, pp. 8–40, IGI Global, Hershey, PA, USA, 2020.

[10] R. Nair, S. Gupta, M. Soni, P. K. Shukla, and G. Dhiman, "An approach to minimize the energy consumption during blockchain transaction," in *Materials Today: Proceedings*, Elsevier, 2020.

[11] N. Waoo, R. Kashyap, and A. Jaiswal, "DNA nano array analysis using hierarchical quality threshold clustering," in *2010 2nd IEEE International Conference on Information Management and Engineering*, pp. 81–85, IEEE, Chengdu, China, 2010.

[12] R. Kashyap and A. Piersson, "Big data challenges and solutions in the medical industries," in *Advances in Systems Analysis, Software Engineering, and High Performance Computing*, pp. 1–24, IGI Global, Hershey, PA, USA, 2018.

[13] R. Kashyap, "Big data analytics challenges and solutions," in *Big Data Analytics for Intelligent Healthcare Management*, pp. 19–41, IGI Global, Hershey, PA, USA, 2019.

[14] I. Assini, A. Badri, K. Safi, A. Sahel, and A. Baghdad, "A robust hybrid watermarking technique for securing medical image," *International Journal of Intelligent Engineering and Systems*, vol. 11, no. 3, pp. 169–176, 2018.

[15] T. T. Takore, P. R. Kumar, and G. L. Devi, "A new robust and imperceptible image watermarking scheme based on hybrid transform and PSO," *International Journal of Intelligent Systems and Applications*, vol. 10, no. 11, pp. 50–63, 2018.

[16] P. Jain and U. Ghanekar, "Robust watermarking technique for textured images," in *Proceedings of the 6th International Conference on Smart Computing and Communications (ICSCC)*, pp. 179–186, Kurukshetra, India, December 2018.

[17] M. Hamidi, M. E. Haziti, H. Cherifi, and M. E. Hassouni, "Hybrid blind robust image watermarking technique based on DFT-DCT and Arnold transform," *Multimedia Tools and Applications*, vol. 77, no. 20, pp. 27181–27214, 2018.

[18] Y. Zhang, Y. Li, and Y. Sun, "Digital watermarking based on Joint DWT-DCT and OMP reconstruction," *Circuits, Systems and Signal Processing*, vol. 38, no. 11, pp. 5135–5148, 2019.

[19] A. K. Abdulrahman and S. Ozturk, "A novel hybrid DCT and DWT based robust watermarking algorithm for color images," *Multimedia Tools and Applications*, vol. 78, pp. 17027–17049, 2019.

[20] D. G. Savakar and A. Ghuli, "Robust invisible digital image watermarking using hybrid scheme," *Arabian Journal for Science and Engineering*, vol. 44, no. 4, pp. 3995–4008, 2019.

[21] M. Alizadeh, H. Sajedi, and B. Babaali, "Image watermarking by Q learning and matrix factorization," in *Proceedings of the International Conference on Machine Vision and Image Processing (MVIP)*, Qom, Iran, February 2020.

[22] R. Mehta, K. Gupta, and A. K. Yadav, "An adaptive framework to image watermarking based on the twin support vector regression and genetic algorithm in lifting wavelet transform domain," *Multimedia Tools and Applications*, vol. 79, no. 25-26, pp. 18657–18678, 2020.

[23] G. Dubey, C. Agarwal, S. Kumar, and H. P. Singh, "Image watermarking scheme using cuckoo search algorithm," in *Advances in Data and Information Sciences*, vol. 94 of *Lecture Notes in Networks and Systems*, Springer, Singapore, 2020.

[24] R. A. Dobre, R. O. Preda, C. C. Oprea, and L. Pirnog, "Authentication of JPEG images on the blockchain," in *Proceedings International Conference on Control, Artificial Intelligence, Robotics & Optimization (ICCAIRO)*, pp. 211–215, Prague, Czech Republic, May 2018.

[25] Y. Guo, B.-Z. Li, and N. Goel, "Optimised blind image watermarking method based on firefly algorithm in DWT-QR transform domain," *IET Image Processing*, vol. 11, no. 6, pp. 406–415, 2017.

[26] Y.-H. Chen, H.-C. Huang, C.-H. Lai, and T.-Y. Chang, "An image watermarking approach based on artificial fish swarm algorithm," in *Proceedings of Analysis of Watermarking Framework for Color Image Through*, pp. 46–50, Kyoto, Japan, March 2020.

[27] M. F. Kazemi, M. A. Pourmina, and A. H. Mazinan, "Analysis of watermarking framework for color image through a neural

network-based approach," *Complex & Intelligent Systems*, vol. 6, no. 1, pp. 213–220, 2020.

[28] M. F. Kazemi, M. A. Pourmina, and A. H. Mazinan, "Novel neural network based CT-NSCT watermarking framework based upon Kurtosis coefficients," *Sensing and Imaging*, vol. 21, no. 1, Article ID 7, 2020.

[29] A. K. Yadav and R. Mehta, "Local coupled extreme learning machine based image watermarking using DCT in YCbCr space," in *Proceedings of the Amity International Conference on Artificial Intelligence (AICAI)*, pp. 527–532, Dubai, UAE, February 2019.

[30] M. Naseri, M. Abdolmaleky, A. Laref et al., "A new cryptography algorithm for quantum images," *Optik*, vol. 171, pp. 947–959, 2018.

[31] S. Heidari, M. M. Abutalib, M. Alkhambashi, A. Farouk, and M. Naseri, "A new general model for quantum image histogram (QIH)," *Quantum Information Processing*, vol. 18, no. 6, pp. 1–20, 2019.

[32] R. Krishnamoorthi, S. Joshi, H. Z. Almarzouki et al., "A novel diabetes healthcare disease prediction framework using machine learning techniques," *Journal of Healthcare Engineering*, vol. 2022, Article ID 1684017, 10 pages, 2022.

[33] I. Ahmad, S. H. Serbaya, A. Rizwan, and M. S. Mehmood, "Spectroscopic analysis for harnessing the quality and potential of gemstones for small and medium-sized enterprises (SMEs)," *Journal of Spectroscopy*, vol. 2021, Article ID 6629640, 12 pages, 2021.

[34] H. Z. Almarzouki, H. Alsulami, A. Rizwan, M. S. Basingab, H. Bukhari, and M. Shabaz, "An internet of medical things-based model for real-time monitoring and averting stroke sensors," *Journal of Healthcare Engineering*, vol. 2021, Article ID 1233166, 9 pages, 2021.

[35] D. Delannay and B. Macq, "Generalized 2-D cyclic patterns for secret watermark generation," in *Conference Proceedings 2000 International Conference on Image Processing (Cat. no. 00ch37101)*, vol. 2, pp. 77–79, Vancouver, BC, Canada, September 2000.

[36] 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, 2014.

[37] N. A. Loani, N. N. Hurrahi, S. A. Parah, J. W. Lee, J. A. Sheikhi, and G. M. Bhat, "Secure and robust digital image watermarking using coefficient differencing and chaotic encryption," *IEEE Access*, vol. 6, pp. 19876–19897, 2018.

[38] T. Yang, G. H. Zhang, L. Liu et al., "New features of authentication scheme for the IoT: a survey," in *Proceedings of the 2nd International ACM Workshop on Security and Privacy for the Internet-of-Things*, pp. 44–49, London, UK, November 2019.

[39] M. Wazid, A. K. Das, M. K. Khan, A. A.-D. Al-Ghaiheb, N. Kumar, and A. V. Vasilakos, "Secure authentication scheme for medicine anti-counterfeiting system in IoT environment," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1634–1646, 2017.

[40] Z. Xia, N. N. Xiong, A. V. Vasilakos, and X. Sun, "EPCBIR: an efficient and privacy-preserving content-based image retrieval scheme in cloud computing," *Information Sciences*, vol. 387, pp. 195–204, 2017.

[41] C. Lin, D. He, X. Huang, K.-K. R. Choo, and A. V. Vasilakos, "BSeIn: a blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0," *Journal of Network and Computer Applications*, vol. 116, pp. 42–52, 2018.

[42] S. Jangirala, A. K. Das, and A. V. Vasilakos, "Designing secure lightweight blockchain-enabled RFID-based authentication protocol for supply chains in 5G mobile edge computing environment," *IEEE Transactions on Industrial Informatics*, vol. 16, pp. 7081–7093, 2019.

[43] S. Challa, A. K. Das, P. Gope, N. Kumar, F. Wu, and A. V. Vasilakos, "Design and analysis of authenticated key agreement scheme in cloud-assisted cyber-physical systems," *Future Generation Computer Systems*, vol. 108, pp. 1267–1286, 2020.

[44] M. Wazid, A. K. Das, K. V. Bhat, and A. V. Vasilakos, "LAM-CIoT: lightweight authentication mechanism in cloud-based IoT environment," *Journal of Network and Computer Applications*, vol. 150, Article ID 102496, 2020.