IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 20 July 2022, accepted 8 August 2022, date of publication 16 August 2022, date of current version 19 August 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3198963

RESEARCH ARTICLE

A Novel Multipurpose Watermarking Scheme Capable of Protecting and Authenticating Images With Tamper Detection and Localisation Abilities

SUNPREET SHARMA, JU JIA ZOU, AND GU FANG, (Member, IEEE)
School of Engineering, Design and Built Environment, Western Sydney University, Penrith, NSW 2751, Australia
Corresponding author: Sunpreet Sharma (sunpreet.sharma@westernsydney.edu.au)

This work was supported by the Western Sydney University Postgraduate Research Award.

ABSTRACT Technologies that fall under the umbrella of Industry 4.0 can be classified into one of its four significant components: cyber-physical systems, the internet of things (IoT), on-demand availability of computer system resources, and cognitive computing. The success of this industrial revolution lies in how well these components can communicate with each other, and work together in finding the most optimised solution for an assigned task. It is achieved by sharing data collected from a network of sensors. This data is communicated via images, videos, and a variety of other signals, attracting unwanted attention of hackers. The protection of such data is therefore pivotal, as is maintaining its integrity. To this end, this paper proposes a novel image watermarking scheme with potential applications in Industry 4.0. The strategy presented is multipurpose; one such purpose is authenticating the transmitted image, another is curtailing the illegal distribution of the image by providing copyright protection. To this end, two new watermarking methods are introduced, one of which is for embedding the robust watermark, and the other is related to the fragile watermark. The robust watermark's embedding is achieved in the frequency domain, wherein the frequency coefficients are selected using a novel mean-based coefficient selection procedure. Subsequently, the selected coefficients are manipulated in equal proportion to embed the robust watermark. The fragile watermark's embedding is achieved in the spatial domain, wherein self-generated fragile watermark(s) is embedded by directly altering the pixel bits of the host image. The effective combination of two domains results in a hybrid scheme and attains the vital balance between the watermarking requirements of imperceptibility, security and capacity. Moreover, in the case of tampering, the proposed scheme not only authenticates and provides copyright protection to images but can also detect tampering and localise the tampered regions. An extensive evaluation of the proposed scheme on typical images has proven its superiority over existing state-of-the-art methods.

INDEX TERMS Image authentication, image copyright protection, cybersecurity, industry 4.0, image watermarking.

I. INTRODUCTION

The present era of the fourth industrial revolution (Industry 4.0) employs information technology to stimulate an industrial change [1]. Herein, the revolution exploits the large-scale machine-to-machine communication (M2M), the cyber-physical system (CPS), and the internet of things (IoT) to increase automation [2]. These attributes are crucial in self-monitoring and communicating the diagnostic issues without human intervention. They are also vital in transforming traditional manufacturing and industrial processes into state-of-the-art practices. The success of this revolution is reliant upon effective and efficient communication amongst the various components in play [3]. This demand is met by a network of sensors that facilitate a constant stream of data flowing between these components that connects them

The associate editor coordinating the review of this manuscript and approving it for publication was Zijian Zhang.

with each other. The data is shared in various signal forms, one such form being an image. Consequently, many images are regularly exchanged in the modern industrial environment, thus safeguarding them is a must. To this end, many techniques, such as, cryptography, steganography, and watermarking that fall under the umbrella of data hiding (DH) are being developed [4]. Steganography and cryptography are means of covert communication, whereas watermarking primarily focuses on media copyright protection and verification, respectively [5]. Moreover, watermark embedding can be visible or invisible, however, the embedded message in steganography and cryptography schemes has to be hidden [6]. This paper *aims* to present a novel watermarking strategy that can authenticate and protect images in an industrial environment, wherein image authentication and copyright protection are necessary. Therefore, the core focus of the remaining discussion will be image watermarking.

The watermarking process consists of an embedding phase, wherein a piece of information known as the ''watermark'' is added to the host signal (an image in this instance). The other phase is that of the extraction, wherein the watermark is extracted or recovered to verify the host image's authenticity and copyright information [6]. A successful extraction validates the integrity of the host image and proves its copyright or ownership. A watermarking scheme needs to address three main requirements [7]. Firstly, in the case of invisible watermarking, the addition of the watermark to the host signal must be imperceptible. This avoids any deformities perceived by the human visual system (HVS). Secondly, the watermark needs to be secure against unauthorised modifications. Thirdly, a watermarking scheme should have a healthy capacity, for example, its ability to embed large watermark(s). These three requirements are closely correlated, and changing one can significantly affect the other. For instance, high capacity can improve security but degrades imperceptibility, whereas the lower the capacity, the better the imperceptibility and the weaker the security. Thus, reaching an equilibrium amongst these requirements is a significant challenge in the field.

In their study, Roy and Pal shared that based on applications, watermarking schemes can be categorised as follows [8]. Firstly, robust watermarking methods are those in which the embedded watermark can withstand watermarking attacks. In other words, the embedded watermark in such processes is resilient to attacks and can be extracted from the watermarked image if attacked. These schemes are mainly used in copyright protection. Secondly, the techniques wherein the embedded watermark has zero-tolerance toward watermarking attacks are known as fragile. In other words, the embedded watermark in these methods is not resilient against attacks and cannot be extracted if the watermarked image is attacked. Fragile watermarking is employed for media authentication or verification as it opposes any modification. Thirdly, caption-based watermarking uses a watermark relevant to the host image, conveying vital information related to that image. For instance, caption watermarks

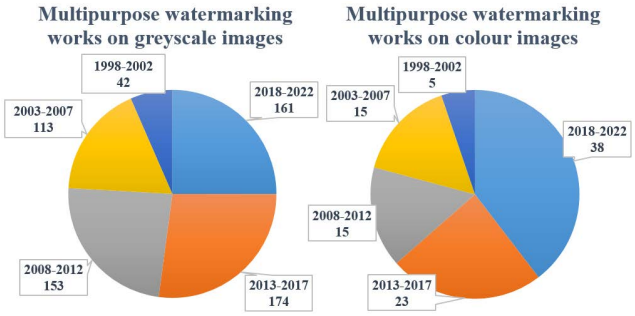


FIGURE 1. Breakdown of the multipurpose watermarking works published in the last 25 years. The left pie chart shows the works that catered to the greyscale images, and the right is for the colour images. Note that the data used for generating these charts is extracted from Scopus®, available at [11]. Best viewed when zoomed-in.

are widely used in medical image watermarking, wherein captions provide helpful information about the patient's health history and contribute to their medical examination [9]. Roy *et al.* also shared that the caption watermarks are generally robust because they are comprised of sensitive information, therefore, their survival is a must. However, caption-based watermarking is out of this study's scope.

This study focuses on achieving copyright protection and authentication in images. It is therefore placed under the multipurpose watermarking category from the application viewpoint. The state-of-art methods (detailed in Section II) in this category use two separate watermarks to achieve multiple goals of copyright protection and authentication in images, one robust and the other fragile [10]. Notwithstanding the successes of existing multipurpose watermarking approaches, they are prone to several limitations outlined below.

Firstly, as outlined above, embedding multiple watermarks can significantly increase capacity, thus degrading imperceptibility. The proposed method bridges this gap by employing novel watermarking strategies, one relating to the robust watermark and the other to the fragile. The watermarked images produced using the proposed method can attain the vital balance amongst the watermarking requirements of imperceptibility, security and capacity. More details on these strategies and their working illustration on typical images, are presented in upcoming Sections III and IV, respectively.

Secondly, most literature covering multipurpose watermarking techniques that use two or more watermarks is focused on greyscale images. Statistically, in the last 25 years, 739 multipurpose watermarking works for images have been published, out of which 643 are for greyscale images and only 96 are for colour ones [11]. As illustrated below in Figure 1, this imbalance needs to be rectified as the greyscale images are rarely used today. Hence, the proposed study addresses this gap by focusing mainly on colour images. However, the proposed scheme is not limited to colour images and can also be implemented on greyscale images. Further details on such operational versatility of the proposed scheme are in Section III.

Thirdly, many of the existing multipurpose watermarking methods are non-blind, which may lead to security issues because the non-blind watermarking techniques require the original signal during the watermark extraction [5], [7], [12], [13]. This shortfall is bridged in this study as the proposed extraction processes are blind. More details are available in subsection III-D.

Fourthly, the majority of the existing approaches employ multiple encryption keys to scramble the watermark [14], [15], [16]. This contributes to the implementation complexity and makes the overall process laborious. This limitation is addressed in this study as only one encryption key is employed by the proposed multipurpose watermarking strategy. More details are in Section III.

Finally, in the case of tampering, many of the existing multipurpose watermarking methods can not detect and localise the affected regions. Even those which can, are not adaptive because they are limited to using only a pixel-based approach or a pixel-block-based approach to achieve tamper detection and localisation. Consequently, this leads to several issues such as, poor tamper detection precision and poor tamper localisation accuracy [17]. This gap is bridged in this study as the proposed tamper detection uses a pixel-based approach, whereas a block-based approach is employed for locating the tampered regions or tamper localisation. More details on these procedures and their working illustration on typical images are present in subsections III-C, III-D1, and IV-D, respectively.

In summary, a novel multipurpose watermarking scheme is presented in this paper. The proposed method is blind, uses only one encryption key for scrambling the watermark(s), and can be employed for watermarking both the greyscale and the colour images. Moreover, the watermarked images produced using the proposed watermarking can attain the vital balance between the watermarking requirements of imperceptibility, security and capacity. In the case of tampering, the proposed scheme has excellent precision in tamper detection and superb accuracy in localising the tampered regions. The proposed scheme can be employed in an industrial environment, wherein image authentication and copyright protection is a necessity. In addition to these advantages, the proposed method has the following contributions.

A. OUR CONTRIBUTIONS

The contributions made by the proposed study are listed below.

1) A novel coefficient selection procedure in the frequency domain is proposed. The procedure is utilised in the robust watermark embedding phase (detailed in subsection III-A), wherein the carefully chosen frequency coefficients are manipulated in equal proportions to achieve robust watermark embedding. To the authors' knowledge, this is the first study wherein such a coefficient selection procedure is proposed and employed. This procedure has the following benefits:
   (i) It uplifts the robust watermark's imperceptibility. The watermarked images produced using the novel coefficient selection procedure have superior imperceptibility performance to state-of-the-art methods [14], [15], [16], [18], [19], [20], [21].
   (ii) It strengthens the overall security of the proposed scheme. The robust watermark embedded using the novel coefficient selection procedure is examined against various geometrical and non-geometrical watermarking attacks (see [6] for an insight into the watermarking attacks). Its resilience to watermarking attacks is higher than many widely-cited methods [14], [15], [16], [18], [19], [20], [21] in the field. Moreover, unlike most of the aforementioned existing watermarking techniques, the security evaluations of the proposed scheme are achieved using a variety of watermarks of different dimensions. Furthermore, the host images used for testing are as small as 128×128 and as large as 2048×1152 in pixel resolution, respectively.
2) A novel least significant bit (LSB) substitution-based strategy is proposed in the spatial domain. This strategy is used for embedding the fragile watermark, presented in subsection III-C. There are two main highlights of this strategy:
   (i) It improves the fragility attribute of the fragile watermark. The fragile watermark(s) used for embedding is self-generated. Specifically, it's the halftone of the colour channel. Once the halftone/binary equivalent of a colour channel is achieved, it is employed to watermark the colour channel itself. The fragility results achieved by such a watermark are superior to the recent works [14], [22], [16], which tend to use foreign logo(s) as the fragile watermark. To the best of the authors' knowledge, this is the first study on *multipurpose* watermarking that uses such a self-generated watermark.
   (ii) It improves the precision of tamper detection and the accuracy in localising the tampered regions. The proposed fragile watermarking uses raster scanning during the embedding and the extraction phases (discussed in subsections III-C and III-D1). In the case of tampering, such scanning allows the proposed scheme to pinpoint and detect the specific pixel that's been tampered with and subsequently fine-tune the localisation of a tampered region. To the best of the authors' knowledge, this study is the first to use this strategy to achieve tamper detection and localisation.

The rest of this discussion is as follows. Section II presents the state-of-the-art literature in the field. Section III covers the proposed methodology. Section IV, is dedicated to the

experimental results, and finally, Section V concludes the article.

II. RELATED WORK

Insight into the state-of-the-art methods which have motivated the proposed study is presented here. Moreover, the pros and cons of the techniques discussed in this section are summarised below in Table 1.

Researchers, Lu and Liao, spearheaded the idea of multipurpose watermarking with their approach, achieving multiple goals of authentication and copyright protection [23]. They used discrete wavelet transform (DWT) and embedded two distinct watermarks, one robust and the other fragile. However, their scheme under-performs in tamper localisation accuracy. These issues are addressed by Liu *et al*. in their study, wherein a multipurpose watermarking scheme for colour images is proposed [10]. In their research, the YC_bC_r colour model is used, where Y, C_b, and C_r are luminance, chrominance blue, and chrominance red channels, respectively. The Y channel is first exposed to the DWT operation, and the robust watermark is then embedded into the low-frequency wavelet coefficients. Subsequently, the robust watermarked image, achieved via the inverse of DWT (IDWT), is split into the red, green, and blue (*RGB*) channels. Each of these channels is thereby embedded with a fragile watermark, thanks to the novel LSB-based embedding method proposed by Liu *et al*. Despite the method's broad acceptance by later works, it has the following disadvantages. Firstly, the approach works only on colour images but not greyscale images. Secondly, the method is solely based on the DWT, therefore suffers from common issues, such as aliasing [24], [25]. These issues are detrimental to the image reconstruction process, thereby affecting the watermark's imperceptibility in the watermarked image.

Several recent studies have shown that the problems DWT may cause are limited, or in some instances eliminated, by combining DWT with other tools. For instance, methods [14], [15], [26], [27] have used discrete cosine transform (DCT), singular value decomposition (SVD), support vector machine (SVM), and neural networks to achieve the required combination, respectively. However, these combination-based approaches also experience challenges. For instance, machine/deep learning based-techniques demand substantial computation power, data collection and training, making them laborious and expensive resources. Hence, combining multiple approaches to achieve the desired outcome is a cumbersome process.

Authors, Hurrah *et al.* presented a dual watermarking framework for privacy protection, and multimedia content authentication in [14]. The study has proposed two methods: scheme 1 and scheme 2. The former is a robust watermarking scheme, the latter is multipurpose. Hence, scheme 2 is more relevant to the topic of this discussion and is expanded upon here. The approach is operable on greyscale and colour images. In the case of a colour image, one of the *RGB* channels is first embedded with the robust watermark via a combination of DWT and DCT. Subsequently, another channel is spatially processed to achieve fragile watermarking. Arnold transform-based encryption is also used for scrambling the logo watermarks, which are further secured using a novel encryption approach proposed by Hurrah *et al.* in the study. Scheme 2 has tamper detection and localisation abilities and can maintain a vital balance between the aforementioned watermarking requirements. However, as the method embeds the fragile watermark in only one of the three colour channels, it fails to explain how it maintains the integrity of the other two channels. So, the question remains, how does it verify if the other two channels have been tampered with or not?

This work by Hurrah *et al.* motivated Kamili *et al.*'s study [16], wherein a novel watermarking scheme known as DWFCAT is proposed using the YC_bC_r colour model. Firstly, the robust logo watermark is encrypted using a combination of chaotic and deoxyribonucleic acid (DNA) encryption techniques. Secondly, the Y channel is embedded with the robust watermark within the transform domain by manipulating the DCT coefficients. Subsequently, the C_b component is divided into the non-overlapping (8×8) blocks in the spatial domain, and a bit from the second binary logo (fragile) watermark is embedded into the LSB of a randomly selected pixel within a block. Moreover, a replica of the already embedded watermark bit is placed in another randomly selected pixel's LSB in the same block. Here, the original bit provides the authentication ability, and the duplicate bit is for tamper detection and localisation. Finally, these steps are repeated and the multipurpose watermarked image is achieved. As the method only uses one colour space instead of two, it is faster than Liu *et al*. and Hurrah *et al*.'s methods [10] and [14]. Moreover, it also outperforms Liu *et al*.'s in terms imperceptibility, i.e., the peak-signal-to-noise ratio *PSNR* performance. However, the method's tamper detection and localisation performances are not quantified using available metrics, such as the false-positive rate (*FPR*), the false-negative rate (*FNR*), the true-positive rate (*TPR*), and the accuracy (*ACC*). Note, these metrics are explained within Section IV.

Inspired by kamili *et al.*'s fragile watermarking, Hurrah *et al.* presented another multipurpose watermarking strategy in 2020 [22]. The scheme caters to medical images only and is implemented in the spatial domain. Although the scheme does not consist of robust watermarking, it is multipurpose and is successful in fulfilling authentication, tamper detection, tamper localisation, and the recovery of the tampered areas. In watermarking, reversibility is a property that allows the watermarking scheme to recover and reconstruct the areas affected by attacks. Even though it is out of this study's scope, author Haghighi *et al.*'s study is a comprehensive read on this topic [28]. Hurrah *et al.*'s method works well in fulfilling multiple purposes, including the ones it is designed to fulfill. However, the method suffers from two major flaws. First, it does not provide copyright protection and so the image can be stolen. Second, it uses a foreign logo as a (fragile) watermark. Here the term ''foreign

logo'' refers to a logo separate from the host image. Such logo is compulsory in robust watermarking to prove the copyright/ownership. However, it is not desired for fragile watermarking because a foreign entity, when added to a host image, is regarded as noise and ultimately degrades the *PSNR*. Hence, most fragile watermarking literature prefers self-embedding watermarks, i.e., those generated from the host image [29]. Moreover, foreign logo-based methods are impossible to apply if no such logo is available.

One of the critical issues in the above-mentioned reversible watermarking method(s) is that there is no backup for the recovery/digest information, and the scheme is no longer reversible if it gets destroyed. This significant shortfall is addressed by Haghighi *et al.*'s in their study [28]. They proposed TRLG, a self-embedding watermarking scheme for image tamper detection and recovery. Their method is blind and uses the lifting wavelet transform (LWT) and halftoning techniques to create four digest (compressed) images. Moreover, genetic algorithm (GA) optimisation is utilised to enhance the quality of the compressed digest images. In the case of tampering, there are four chances to recover a tampered block. To this end, the Chebyshev system is employed in selecting the mapping blocks for embedding, encrypting, and shuffling the information. Subsequently, multiple techniques such as mirror-aside and partner-block are proposed to uplift the recovery of the tampered regions. The method achieves excellent image authentication results and outperforms several state-of-the-art methods (such as Hurrah *et al.*'s scheme 2 in [14]) in tamper detection and localisation performance. Similarly, the technique is high in imperceptibility, which is indicated via the average *PSNR* value of 46 decibels (dB) obtained from the test images. The only shortfall of Haghighi *et al.*'s method is that it cannot provide copyright protection.

Haghighi *et al.* presented WSMN in late 2020 [32] to combat the shortfall of their preceding work. Here, WSMN differs from TRLG as it utilises robust and fragile watermarks to achieve copyright protection and authentication, whereas TRLG is reversible and provides authentication only. However, they both are equipped in their abilities to achieve tamper detection and localisation. WSMN is a multipurpose blind watermarking scheme, based on Shearlet transform, that uses smart algorithms such as multi-layer perception (MLP) and non-dominated sorting genetic algorithm (NSGA-II). In WSMN, quantisation and correlation techniques are used in watermarking the approximate and detail coefficients with robust and authentication watermarks, respectively. Moreover, K-Means clustering is employed to differentiate the suitable embedding blocks from the non-suitable ones. NSGA-II facilitates the optimal selection of the embedding strength parameter, which is vital in achieving a balance between the watermark's imperceptibility and security. Furthermore, MLP's learning ability not only empowers WSMN to withstand the geometrical and non-geometrical attacks, but also to achieve high tamper detection and localisation performances. In other words, it provides immunity to robust watermark(s) against the hybrid attacks and uplifts WSMN's ability to authenticate. In contrast, it also makes the overall scheme laborious and affects the processing time. Moreover, unlike TRLG, the recovery of the tampered regions is not achieved by the WSMN.

In 2022, Sharma *et al.* presented a multipurpose watermarking scheme that targeted copyright protection and authentication [34]. The method is operable across several colour spaces, such as greyscale, *RGB*, and the YC_bC_r. The approach is hybrid, as it utilises both transform and spatial domains. Above all, the method is one of the first to use a single watermark to achieve two goals of copyright protection and authentication. The method has used the Fisher and Yates algorithm for encryption and a combination of DWT-DCT for watermark embedding. The study has also introduced a novel concept of checkpointing; wherein a watermarked image is exposed to a pre-defined set of modifications. After each modification, the energy of the watermarked image is calculated and stored in an array, yielding a modification array. The study defines such an array as the energy vector (EV). Before the watermarked image's transmission, the EV is shared with the receiver along with the secret key. Here, the secret key is the number of iterations used by the Fisher and Yates algorithm to shuffle the logo watermark. Subsequently, once the receiver receives the watermarked image, its energy is calculated and compared against the energy values within the EV. If there is a match, the received watermarked image is deemed authentic, triggering the watermarked extraction process. Otherwise, it is inauthentic, and the extraction process is terminated. Note, embedding and extraction processes are implemented in the transform domain, whereas the checkpointing is executed within the spatial domain. The method is fast, produces imperceptible watermarked images, and can prove their copyright information and verify their integrity. However, the method is not reversible and is unable to achieve tamper detection and localisation. The method is non-blind, i.e., leading to the various security issues caused by such methods [7], [30], [35].

The above discussion has highlighted that *RGB* and YC_bC_r are widely adopted models for watermarking colour images. However, these colour models have their strengths and weaknesses; for instance, the YC_bC_r model is compression friendly but limited in embedding capacity, as Y is the only channel used for watermark embedding. In contrast, the *RGB* model is high in watermarking capacity but not preferred when an application requires image compression [34]. Hence, choosing a colour model is subject to the application by which it is about to be employed. To this end, the proposed method is tailored to utilise YC_bC_r and *RGB* colour models. This way, it can extract the best of both models and illustrate its operational adaptability. Moreover, the success of the DCT-based watermarking methods is in their tolerance to withstand image compression attack, one of the most readily used image manipulations in an industrial environment [36]. DCT's streamlined implementation and application simplicity have made it a popular choice when combining with other

TABLE 1. Summary and comparison of related works. Included in the table are greyscale (GS), foreign logo (FL), self-generated logo (SGL), transform domain (Trans.), and spatial domain (Spa.). A scheme's ability and inability are denoted by ✓ and ×, respectively. The higher the number of +, the stronger the attribute.

Study →	[10]	[30]	[14]	[31]	[28]	[22]	[16]	[32]	[33]	[34]	**Proposed**
Year	2016	2017	2019	2019	2019	2020	2020	2021	2022	2022	2022
Domain(s)	Trans.+Spa.	Trans.+Spa.	Trans.+Spa.	Trans.+Spa.	Spa.	Spa.	Trans.+Spa.	Trans.	Trans.+Spa.	Trans.+Spa.	Trans.+Spa.
Extraction	Blind	Non-blind	Blind	Blind	Blind	Blind	Blind	Blind	Blind	Non-blind	Blind
Host image	Colour	GS	Colour+GS	GS	Colour+GS	GS	Colour	Colour+GS	GS	Colour+GS	Colour+GS
Imperceptibility	+ + +	+ +	+ + + +	+ + + +	+ + + +	+ + +	+ + + +	+ +	+ + +	+ + + +	+ + + +
Robustness	+ +	+ +	+ + +	×	×	×	+ +	+ + + +	×	+ + +	+ + + +
Security	+ +	+ +	+ + +	+ +	+ + +	+ + +	+ +	+ + + +	+ + +	+ + +	+ + + +
Robust watermark	Logo	Logo	Logo	×	×	×	Logo	Logo	×	Logo	Logo
Fragile watermark	SGL	SGL	FL	SGL	SGL	FL	FL	SGL	SGL	FL	SGL
Copyright protection	✓	✓	✓	×	×	×	✓	✓	×	✓	✓
Authentication	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Tamper detection	×	✓	✓	✓	✓	✓	✓	✓	✓	×	✓
Tamper localisation	×	✓	✓	✓	✓	✓	✓	✓	✓	×	✓
Tamper recovery	×	✓	×	✓	✓	✓	×	×	✓	×	×
Optimisation	×	✓	×	×	✓	×	×	✓	×	×	✓

techniques, especially DWT [14], [15], [16], [26], [27]. These insights have also inspired the methodology proposed in this study, presented in the following Section III.

III. METHODOLOGY

The proposed method's overview is in Figure 2. Here, the embedding process is divided into two parts: (1) robust watermark embedding and (2) fragile watermark embedding. Part one is implemented in the transform domain. Here, the host image is converted into the YC_bC_r colour space, and the Y channel is embedded with the robust watermark. Part two is implemented in the spatial domain. Here, the previously attained robust watermarked image is split into *RGB* channels. Each of these channels is then subject to a halftoning operation and subsequently, attained halftones are used in the fragile watermarking of their respective channel. Note, the Y and *RGB* channels are greyscale equivalents with pixel vales ranging from 0 (black) to 255 (white). To this end, the proposed scheme is operable on greyscale and colour images, offering another advantage in terms of its application versatility.

In 2020, Bertini *et al*. have revealed that the image dimensions/size entertained by 13 major industries are in the range of 128×128 to 2048×1152 in pixel resolution [37]. Moreover, the study also pointed out that these industries default to accept an image with dimensions in the powers of two. Bertini *et al.* have also highlighted that when they (industries) encounter an image consisting of an odd number of either rows or columns or both, they use image resizing to align the odd component(s) to its nearest power of two. Here, the proposed method does the same. Furthermore, such resizing is a requirement to perform the DWT decomposition as it yields frequency subbands that are even in size. The rest of the steps in Figure 2 are as follows.

A. ROBUST WATERMARK EMBEDDING

The DWT of an image yields four frequency subbands, which are termed and represented in Figure 3 as low-low (*LL*), low-high (*LH*), high-low (*HL*), and high-high (*HH*). Commonly, the HVS is more receptive to low-frequency modulations. As the *LL* subband is comprised of the low-frequency DWT coefficients, it is not suitable for the watermark embedding.

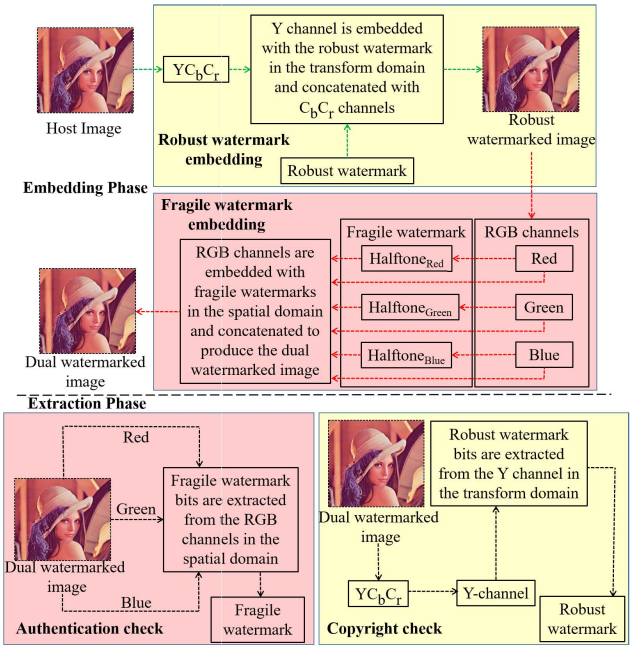


FIGURE 2. Blueprint of the proposed method. Note, the authentication and the copyright checks are independent of each other. To this end, the former check is facilitated by the fragile watermark and the latter by the robust watermark. Best viewed when zoomed-in.

Similarly, the *HH* subband contains high-frequency coefficients, which can easily be victimised by the usual watermarking attacks, such as compression and high-pass filtering, leaving them unsuitable for embedding. Moreover, our previous works [7], [13] are positively influenced by the literature in [38], [39], and [40]. They tend to use the *LH* subband (represented by solid blue in Figure 3) for the watermark embedding due to its ability to limit the flaws associated with *LL* and *HH* subbands. Furthermore, these methods also exploit the wavelet's ability to perform the multi-resolution analysis (MRA), through which an image can be decomposed into multiple levels to extract the DWT coefficients associated with these levels (see [24] and [25] for insight into the MRA).

Investigations by authors Huynh-The *et al.* in [41], [42], [43] have highlighted that as the DWT level increases, the subband size decreases, and so does the watermark-

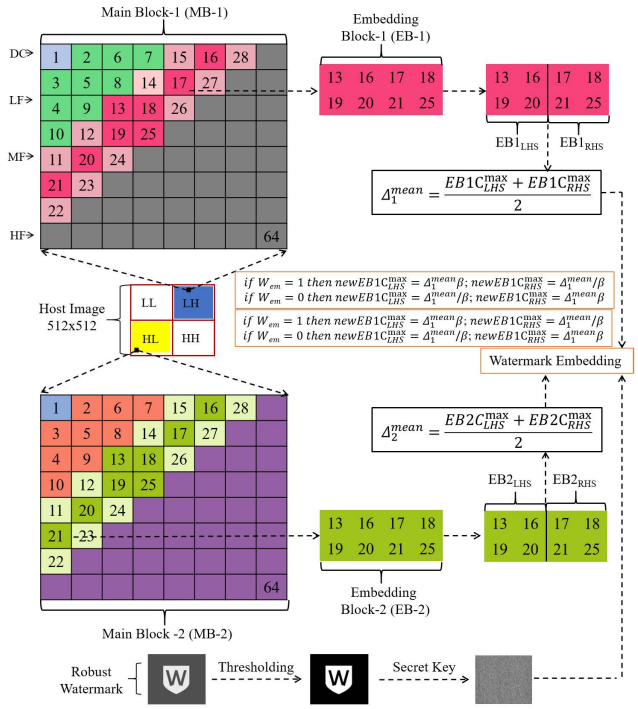


FIGURE 3. Proposed robust watermark embedding process. Digits within main blocks (MB-1 and MB-2) are the numbers allocated to DCT coefficients, where DC being the lowest frequency component is labelled as 1 and 64 is dedicated to the highest frequency component.

ing capacity. Therefore, it is recommended that utilising both *LH* and *HL* subbands (represented by solid yellow in Figure 3) is optimal in the embedding process. In the case of a binary watermark, *LH* and *HL* subbands are preferred due to their symmetry. This allows the black (0) and white (1) bits to be split evenly amongst these two subbands during embedding [34]. Consequently, it makes the watermark more resilient against several attacks, such as rotation, scaling, translation, low-pass and high-pass filtering, whilst also maintaining high capacity and imperceptibility. Convinced by these justifications, the proposed method uses both *LH* and *LH* subbands in the robust watermark embedding process. Moreover, a thorough discussion on watermark embedding in each of these subbands and their behaviour is covered by Islam *et al.* in [40]. A breakdown of the rest of the steps shown in Figure 3 is below.

Firstly, the host image of size $m \times n$ ($rows \times columns$) is decomposed into frequency subbands using DWT. The proposed method can handle images with pixel resolutions ranging from 128×128 to 2048×1152. However, for simplicity, the rest of the proposed method considers a host image which is 512×512 in dimensions.

Secondly, *LH* and *HL* subbands (each composed of the DWT coefficients and 256×256 in size), are divided into 8×8 non-overlapping blocks. Subsequently, the DCT is performed on each of these 8×8 blocks to yield their respective DCT coefficients, and collectively they form the main block that itself is termed as "Main Block" in Figure 3. Moreover, the main blocks associated with the *HL* subband are labelled as "Main Block-1" (MB-1), whereas the ones related to the *LH* block are labelled as "Main Block-2" (MB-2). A magnified illustration of such main blocks is given in Figure 3. The digits within these blocks depict the position numbers associated with the DCT coefficients of which these blocks are constructed. Based on their frequency, DCT coefficients are classified as low-frequency (LF), mid-frequency (MF), and high-frequency (HF), and the very first low-frequency coefficient is known as the direct current (DC) coefficient, respectively (see Figure 3). In this discussion, MF coefficients are selected for the robust watermark embedding, as they allow alterations while maintaining an appropriate balance between imperceptibility and robustness [34].

A complete account of the behaviour of DCT coefficients can be found in [36]. Similar to [26],"Embedding Block" (EB) is constructed by eight of the total MF coefficients in the main block, their allocated position numbers in Figure 3 are 13, 16−21, 25. The selection of these specific coefficients is inspired by Kang *et al.*'s study [26]. The embedding block within MB-1 is termed as EB-1, and the one within MB-2 is labelled as EB-2.

Thirdly, the EB-1 and the EB-2 blocks are vertically split into two halves, forming $EB1_{LHS}$, $EB1_{RHS}$, $EB2_{LHS}$ and $EB2_{RHS}$. Here or at any other instance in this discussion, subscripts *LHS* and *RHS* stand for the "left-hand-side" and the "right-hand-side", respectively. The maximum-valued coefficients in each of these halves are extracted and labelled as $EB1C^{max}_{LHS}$, $EB1C^{max}_{RHS}$, $EB2C^{max}_{LHS}$ and $EB2C^{max}_{RHS}$, respectively. Thereafter, the mean of the $EB1C^{max}_{LHS}$ and the $EB1C^{max}_{RHS}$ is calculated and tagged as Δ_1^{mean}. Similarly, the mean of the $EB2C^{max}_{LHS}$, and the $EB2C^{max}_{RHS}$ is calculated and recorded as Δ_2^{mean}.

Fourthly, the robust watermark is prepared by a series of steps, as shown in Figure 3. It starts by thresholding the watermark to a pixel value of 128. Such thresholding limits the watermark's pixel values to 0 (black) and 255 (white), referred to 0 and 1 in binary. Subsequently, the secret key is used for scrambling the binary watermark. The secret key and watermarked image are shared with authorised personal during the transmission process because the same key is employed to validate the watermark, achieved via watermark extraction (discussed later in subsection III-D). Due to its robust performance and state-of-the-art usage, the Fisher–Yates shuffle algorithm is employed by the proposed method to achieve the watermark scrambling (see [39], [44], and [45] to gain further insight into this shuffling algorithm). Only one secret key is used for scrambling the watermarks throughout this study, this addresses the bridging of the fourth gap, mentioned above in Section I. Once the watermark is scrambled and values of Δ_1^{mean} and Δ_2^{mean} are calculated, the $EB1C^{max}_{LHS}$ and the $EB1C^{max}_{RHS}$ coefficients within the EB-1 block are modified to meet the following criterion.

If the robust watermark bit to be embedded (W_{em}) in the EB-1 block is 1, then;

$$EB1C^{max}_{LHS} = newEB1C^{max}_{LHS} = \Delta_1^{mean}\beta$$

$$EB1C_{RHS}^{max} = newEB1C_{RHS}^{max} = \Delta_1^{mean}/\beta \quad (1)$$

and if it is 0, then;

$$EB1C_{LHS}^{max} = newEB1C_{LHS}^{max} = \Delta_1^{mean}/\beta$$
$$EB1C_{RHS}^{max} = newEB1C_{RHS}^{max} = \Delta_1^{mean}\beta. \quad (2)$$

Here, β stands for the watermark strength factor, also known as the scaling factor in watermarking literature. The value of β in the proposed method is chosen because it attains the vital balance between imperceptibility and robustness. A full account that describes the selection of β is given in the upcoming subsection III-B.

Likewise, the watermark embedding within the EB-2 block can be achieved by rearranging Equations 1 and 2 as Equations 3 and 4, respectively. If the watermark bit to be embedded (W_{em}) in the EB-2 is 1, then;

$$EB2C_{LHS}^{max} = ewEB2C_{LHS}^{max} = \Delta_2^{mean}\beta$$
$$EB2C_{RHS}^{max} = newEB2C_{RHS}^{max} = \Delta_2^{mean}/\beta \quad (3)$$

and if it is 0, then;

$$EB2C_{LHS}^{max} = newEB2C_{LHS}^{max} = \Delta_2^{mean}/\beta$$
$$EB2C_{RHS}^{max} = newEB2C_{RHS}^{max} = \Delta_2^{mean}\beta. \quad (4)$$

The main advantage of the proposed embedding strategy (represented by the orange boundaries in Figure 3) is that it optimizes the imperceptibility as the quantity of coefficient adjustment is divided equally amongst the *HL* and *LH* subbands. Furthermore, the coefficient modifications are carried out in pairs in equal proportions, thus, increasing the robustness and safeguarding the media against several non-geometrical attacks, such as compression. The adopted coefficient modification, in reality, is a coefficient scaling procedure; therefore, if one of the coefficients is scaled up by a factor of β the other coefficient must be scaled down by the same factor. Consequently, the mean values, Δ_1^{mean} and Δ_2^{mean}, are kept unchanged as is the overall imperceptibility. Furthermore, any unauthorised change would cause a shift in the mean values, leading to the degradation of the watermark's imperceptibility in the transmitted watermarked image, ultimately signaling a security breach. This addresses the bridging of the first gap, mentioned above in Section I.

Finally, the aforementioned steps are performed on the remaining 8x8 blocks, selected within *LH* and *HL* subbands. Consequently, the watermark embedding culminates, as does the robust watermark embedding process. This process can be quantised in the form of Equation (5),

$$Y' = Y + \beta W_{Robust} \quad (5)$$

where Y, Y', W_{Robust}, and β stand for the original Y channel, the watermarked Y channel, the robust watermark, and the watermark strength parameter, respectively. Finally, the robust watermarked image is achieved by combining the Y' channel with C_b and C_r channels.

B. SELECTION OF THE WATERMARK STRENGTH PARAMETER

The range of the watermark strength parameter (β) is (0 1], which also specifies the watermark's visibility. To this end, a fully visible watermark is represented by '1' [12]. The value of β directly impacts the watermark's imperceptibility and robustness, its effective selection is therefore vital. The proposed scheme optimises the selection of β by minimising the absolute difference between the imperceptibility and the robustness. It is achieved by fulfilling the following criterion, given in Equation (6).

$$\beta_{optimal} = \underset{\beta\in(0,1]}{\operatorname{argmin}}\{|SSIM(\beta) - NCC(\beta)|\}; \quad (6)$$
$$\text{subject to } PSNR(\beta) \in [34, \infty].$$

Here, the structural similarity index (SSIM) and the *PSNR* represent the imperceptibility, whereas the normalised cross-correlation *NCC* represents the robustness. Note, these performance metrics are explained within the upcoming subsection IV-A. Equation (6) shows that the β's value (where the difference between *SSIM* and *NCC* is minimal and the *PSNR* is greater than 34 dB) is suitable for the robust watermark embedding. The selection of this PSNR's threshold value is presented in [18], [26], and [46], wherein the authors have justified that an image with a *PSNR* greater than 33 dB is imperceptible to the HVS. A working illustration of the proposed β selection is given in Figure 4. Here the plots are generated using *Lenna's* test image; 512 × 512 in size and the *WSU* watermark with varying sizes, respectively. Note, a few examples of the test images and the watermarks used in this discussion are shown below in Section IV. It is vital to acknowledge that the plots in Figure 4 would vary if the size of either the test image or the watermark is changed. However, the proposed β optimisation is well-equipped to deal with such changes and can achieve the desired value of β. This shows the adaptability of the proposed method, which makes it an excellent candidate for a wide range of applications.

C. FRAGILE WATERMARK EMBEDDING

The attained robust watermarked image is split into *RGB* channels. Subsequently, each of these channels is embedded with a fragile watermark. A schematic of the proposed fragile watermark embedding is given in Figure 5. Here, the input is one of the colour channels, equivalent to a greysacle image. The self-generated fragile watermark used for embedding is prepared using a series of steps, outlined below.

(i) *Halftoning*: To begin with, the greyscale equivalent of the colour channel is exposed to a halftoning operation. Floyd-Steinberg (FS) halftoning is employed in the proposed method. Halftones produced using FS closely mimic the original image and are indistinguishable to the HVS [47]. Moreover, out of all the error-diffusion (ED) based halftoning methods, FS is the most widely accepted due to its ability to suppress the blocking

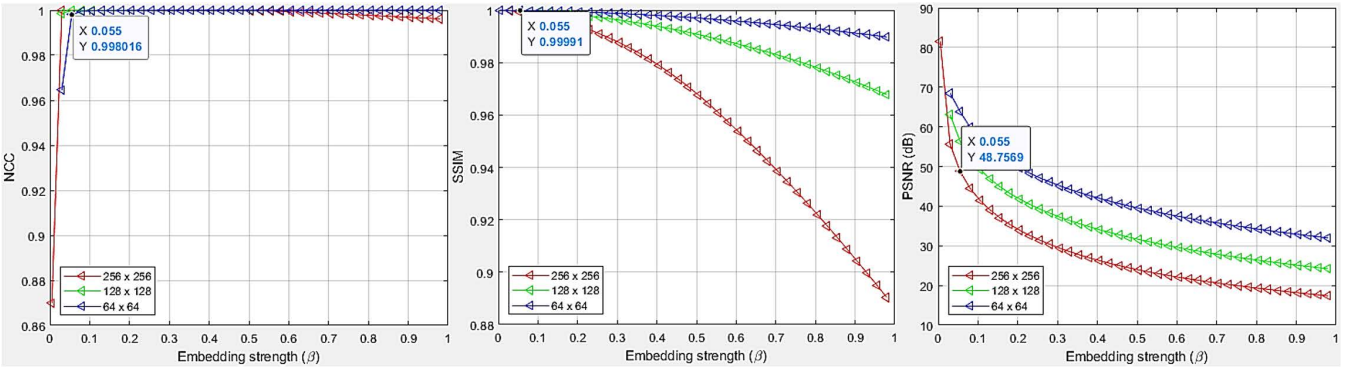


FIGURE 4. Proposed embedding strength (β) selection procedure. Left to right plots: *NCC* Vs. β; *SSIM* Vs. β and *PSNR* Vs. β. Data tips are used to show the best embedding strength factor at $\beta = 0.055$. These plots are generated using *Lenna's* test image; 512 × 512 in size, and the *WSU* watermark with varying sizes, respectively. Best viewed when zoomed-in.

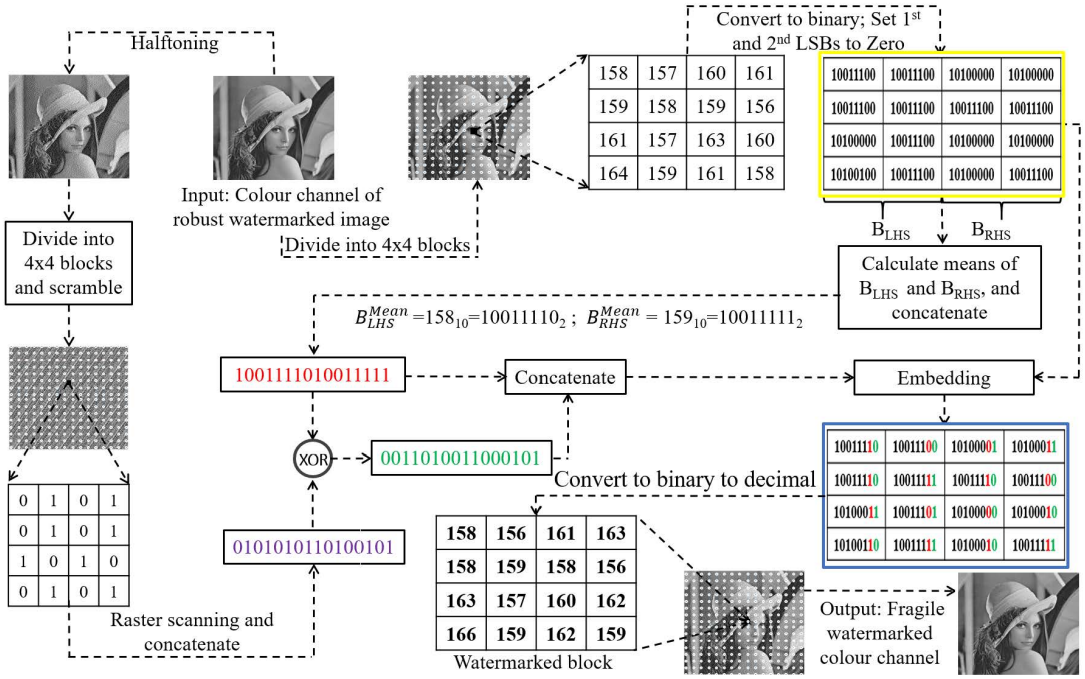


FIGURE 5. Proposed fragile watermark embedding. The purple digits represent the 16-bit watermark seed, the red digits are for the 16-bit mean seed, and the green digits depict the 16-bit XOR-seed. The yellow borders contain the stripped block, and the blue borders are for the embedded block. Best viewed when zoomed-in.

artifacts and minimise the quantisation error. A thorough insight into FS and other halftoning methods can be gained from [48]. Once the halftone image is attained, it is scrambled using the same secret key mentioned above in subsection III-A, and divided into 4 × 4 non-over lapping pixel blocks. Subsequently, the pixel values (0 or 1) of a 4 × 4 block are scanned in the raster scan (left-right; top-bottom) pattern. Finally, these binary values are concatenated to form a 16-bit fragile watermark seed, used in fragile watermarking the colour channel. This watermark seed is depicted by the purple digits in Figure 5. However, the colour channel is prepared before such embedding using the following steps.

(ii) *Colour channel preparation*: To start with, the greyscale equivalent of the colour channel is divided into 4 × 4 non-overlapping pixel blocks. The pixel values of these blocks are then exposed to a decimal to binary conversion. Subsequently, each pixel value is stripped off the LSB and the second bit to the LSB. Note, stripping-off here or anywhere else in this discussion stands for setting the bit value to zero. In Figure 5, the former is depicted as the 1^{st} *LSB*, the latter as the 2^{nd} *LSB* and the stripped block itself is highlighted using yellow borders. The 4 × 4 block is vertically split into two halves; the left-hand side (B_{LHS}) and the right-hand side (B_{RHS}). Thereafter, the mean values of B_{LHS} and B_{RHS} are calculated and labelled as B^{Mean}_{LHS} and B^{Mean}_{RHS}, respectively. Finally, B^{Mean}_{LHS} and B^{Mean}_{LHS} are concatenated to form a 16-bit mean seed, depicted by the red digits in Figure 5. Once the mean seed and the fragile watermark seed are obtained, the actual

fragile watermarking embedding is initiated using the following steps.

(iii) *Embedding*: Firstly, the mean seed and the fragile watermark seed are used in forming a 16-bit exclusive-or (XOR) seed, depicted by the green digits in Figure 5. It is termed as the "XOR-seed" because it is attained by subjecting the mean seed and the fragile watermark seed to an XOR operation.
Secondly, the XOR seed is concatenated with the mean seed to form a 32-bit embedding seed. Subsequently, the stripped block is embedded using the 32-bit embedding seed. Specifically, the 1^{st} *LSB* and the 2^{nd} *LSB* of the stripped block are replaced by the embedding seed. Note, this replacement process also follows a raster scan pattern. In this way, each pixel of a 4×4 block belonging to a colour channel, is embedded with a mean seed bit and an XOR seed bit. Here, the former provides tamper detection and localisation ability, whereas the latter offers authentication/verification. These aspects are discussed within Section III-D, covering the watermark extraction.
Thirdly, the pixel values of the embedded block (contained within the blue borders) are converted to their decimal equivalent, forming the watermarked block. Subsequently, this series of steps is repeated for all other 4×4 blocks of a colour channel.
Finally, the same steps are repeated for the fragile watermark embedding in the other two colour channels. Once all the colour channels are watermarked, they are combined to form a dual watermarked colour image, where the first watermark is robust and the other fragile.

D. WATERMARK EXTRACTION

The proposed method follows the blind watermark extraction procedure, hence it does not require the original signal for the watermark extraction. The discussion in this subsection addresses the bridging of the third gap, mentioned above in Section I. The extraction procedures of robust and fragile watermarks are discussed below.

1) FRAGILE WATERMARK EXTRACTION

The fragile watermark can be extracted to prove the authentication of an image. Figure 6 presents the blueprint of the proposed fragile watermark extraction process. Here, the input image is one of the *RGB* colour channels achieved after splitting the dual watermarked colour image.

Firstly, the input is divided into 4×4 non-overlapping pixel blocks. The pixel values within these blocks are subject to decimal to binary conversion. One such 4×4 block is included within the blue borders in Figure 6. Note, this block is the same as the embedded block from subsection III-C.

Secondly, the block is stripped off its 1^{st} and 2^{nd} LSB, forming a stripped block contained within the yellow boundaries in the exact figure. Note, the pixel values in a 4×4 block are stripped in the raster scan pattern, and the stripped off bits are concatenated to form a 32-bit extracted

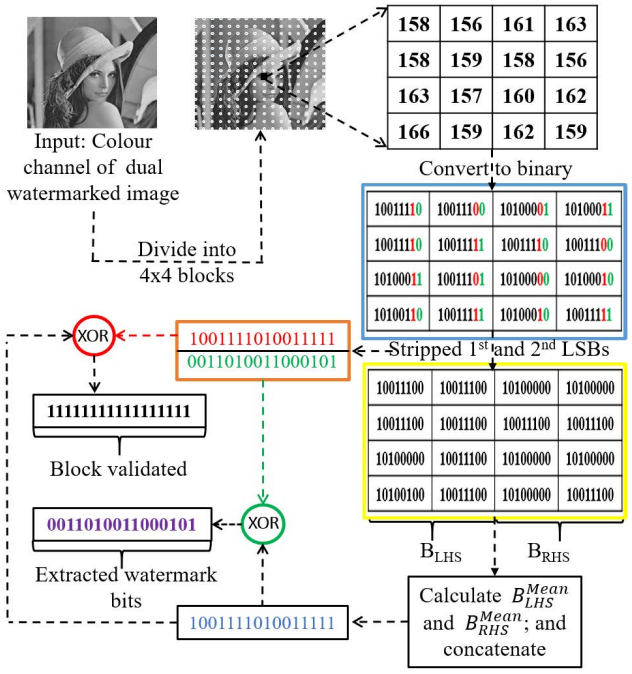


FIGURE 6. Proposed fragile watermark extraction. The green arrow corresponds to the green digits, and the red arrow to the red digits. Best viewed when zoomed-in.

seed. An illustration of an extracted seed is contained within the orange borders in Figure 6.

Thirdly, the stripped-off block is vertically split into two halves; the left-hand-side (B_{LHS}) and the right-hand-side (B_{RHS}). Thereafter, the mean values of B_{LHS} and B_{RHS} are calculated and labelled as B_{LHS}^{Mean} and B_{RHS}^{Mean}, respectively. Subsequently, B_{LHS}^{Mean} and B_{LHS}^{Mean} are concatenated to form a 16-bit mean seed, depicted by the blue digits in Figure 6. In this seed, the first eight digits are from the B_{LHS}^{Mean} and the remaining eight are from the B_{RHS}^{Mean}.

Fourthly, the XOR operation (represented by the green circle in Figure 6) is performed between the 16-bit mean seed and the 16-green digits of the extracted block. These green digits correspond to the 1^{st} *LSBs*. This XOR operation results in the extraction of the 16-bit watermark seed, represented by the purple digits in Figure 6. It can be noticed that the extracted watermark seed is identical to the one embedded above in Figure 5, signifying a successful authentication. Similarly, another XOR-operation (represented by the red circle in Figure 6) is performed between the 16-bit mean seed and the 16-red digits of the extracted block. These red digits correspond to the 2^{nd} *LSBs*. The outcome of this XOR operation proves whether the block is tampered with or not. The tamper detection and localisation processes are discussed within the upcoming subsection III-E.

Finally, each of the 4×4 blocks in each of the three colour channels is processed using these steps. Consequently, the fragile watermark bits are extracted, and each colour channel is validated. Moreover, if any of the colour channels are found to be invalid/tampered, the whole image (in this case) is deemed as tampered. Note, the extracted watermark

bits need to be unscrambled to achieve the actual embedded watermark. This unscrambling is done by using the inverse of the same key that scrambled the watermark during the embedding phase, in the first instance.

2) ROBUST WATERMARK EXTRACTION

The proposed robust watermark extraction process also involves a series of steps. Firstly, the dual watermarked colour image is converted to the YC_bC_r space. The Y channel is selected for the robust watermark extraction, as it is the only channel that was embedded with the robust watermark in the first instance. Specifically, as per the above Equation (5), the Y channel at this particular instance is meant to be Y' because the extraction is only employable on a watermarked channel. Moreover, as the proposed robust watermark embedding is implemented in the frequency domain, its extraction can only be executed in the frequency domain.

Secondly, the 1^{st}-level *DWT* is applied on the Y' channel, which extracts the *LH* and the *HL* subbands. These subbands are then split into 8×8 non-overlapping blocks, each subject to the *DCT* operation. Subsequently, the DCT-coefficients are extracted and processed to form the embedding blocks: EB-1 and EB-2, as stated in subsection III-A. Moreover, Figure 3 (in the same subsection) pictorially represents the same selection procedure and also shows that each of these embedding blocks is 2×4 in size.

Thirdly, the EB-1 and the EB-2 are split vertically to form $EB1_{LHS}$, $EB1_{RHS}$, $EB2_{LHS}$, and $EB2_{RHS}$, respectively. Subsequently, the maximum-valued coefficients in each of these halves; $newEB1C^{max}_{LHS}$, $newEB1C^{max}_{RHS}$, $newEB2C^{max}_{LHS}$ and $newEB2C^{max}_{RHS}$, are extracted. Thereafter, the $newEB1C^{max}_{LHS}$ and the $newEB1C^{max}_{RHS}$ coefficients within an EB-1 block are compared, and the watermark bits are extracted as per Equations (7). Similarly, the $newEB2C^{max}_{LHS}$, and the $newEB2C^{max}_{RHS}$ coefficients within an EB-2 block are compared and the watermark bits are extracted using Equation (8). In an EB-1 block,

$$\begin{aligned} &if \;\; newEB1C^{max}_{LHS} \geq newEB1C^{max}_{RHS}, \;\; then \;\; W_{em} = 1 \\ &if \;\; newEB1C^{max}_{LHS} < newEB1C^{max}_{RHS}, \;\; then \;\; W_{em} = 0. \end{aligned} \quad (7)$$

Similarly, in an EB-2 block,

$$\begin{aligned} &if \;\; newEB2C^{max}_{LHS} \geq newEB2C^{max}_{RHS}, \;\; then \;\; W_{em} = 1 \\ &if \;\; newEB2C^{max}_{LHS} < newEB2C^{max}_{RHS}, \;\; then \;\; W_{em} = 0. \end{aligned} \quad (8)$$

Finally, the remaining watermarked EB-1 and EB-2 blocks are processed using the aforementioned steps within this subsection, and the rest of the watermark bits are extracted. It is essential to realise that Equations (7) and (8) only output the watermark(s) in a scrambled state. To this end, unscrambling the watermark is the last step, achieved by executing the inverse of the aforementioned secret key [39], [40].

E. TAMPER DETECTION AND LOCALISATION

The fragile watermark extraction, facilitates tamper detection and localisation in the proposed method. As mentioned earlier, within subsection III-D, the outcome of the XOR operation (represented by the red circle in Figure 6) decides whether the block is tampered with or not. For instance, when the outcome is a 16-bit seed, wherein each bit has a value of one, the block is considered not-tampered/validated; otherwise it is tampered. In instances when a block is detected as tampered/not-validated, the tampered region is localised as follows.

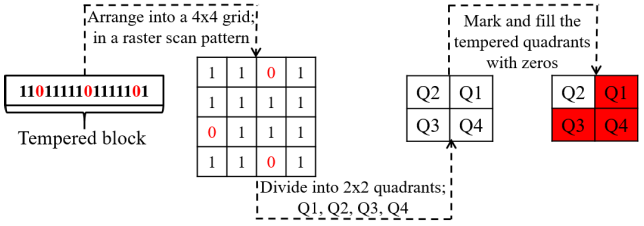


FIGURE 7. Proposed tamper localisation procedure. Here, the red coloured digits represent the tampered bits. Best viewed when zoomed-in.

Firstly, an illustration of a 16-bit seed depicting a tampered block is shown in Figure 7. Here, the tampered or the zero-valued bits are shown using the red colour.

Secondly, bits of a 16-bit seed are arranged to form a 4×4 grid. To increase the precision in localising the tampered area, the grid is further split into four quadrants; Q_1, Q_2, Q_3 and Q_4, each of which is 2×2 in size. Note, the fragile watermark extraction proposed in subsection III-D1 authenticates each pixel, however the proposed tamper localisation is achieved in pixel blocks. It is empirically established that such a combination improves tamper detection precision and tamper localisation accuracy. These results are highlighted and discussed later in the subsection IV-D.

Thirdly, these quadrants are individually checked for the zero-valued bits. Even if a single zero valued bit is present, the quadrant is localised/located as the tampered region; else the following quadrant is processed. Subsequently, the remaining quadrants are treated similarly and the tampered regions are ultimately localised.

Finally, all the bits within a tampered quadrant are replaced with a zero-valued bit. Consequently, the localised region(s) are represented in white in the proposed method.

IV. EXPERIMENTAL RESULTS

The proposed scheme is tested on more than 150 images, publicly available at [49] and [50]. The first two rows of Figure 8 show 12 examples of the total test images, and the third offers a variety of watermarks, all of which are used in simulations. Experiments are conducted using MATLAB (R2021a) on a machine with Intel^{TM} i7-8650U CPU running at 1.9 GHz, 16 GB RAM, and a 64-bit operating system. Note, the experimental analysis presented in this paper is conducted on images as small as 128×128 and as large as 2048×1152 in pixel resolution. Statistically, the experimental simulations were run 25 times. The proposed watermarking scheme is stable and consistently achieves the performance targets implied in this study.

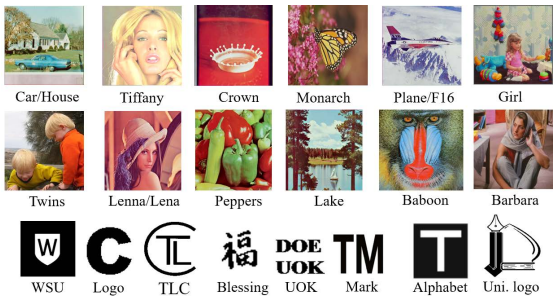


FIGURE 8. Test images (publicly available at [49] and [50]) and a variety of watermarks (row three) used for illustrations in this paper. Best viewed when zoomed-in.

A. PERFORMANCE METRICS AND BASELINE

The evaluations of the proposed method in terms of imperceptibility are contained in Table 2, Figures 9 and 12. Subsequently, Figures 13, 14, 15, and 17 present the security analysis, respectively. To this end, these figures are focused on the robust watermark, demonstrate its robustness against a variety of watermarking attacks, and compare its performance to other state-of-the-art methods. Similarly, Table 5 and Figure 20 cover the performance of the fragile watermark(s) and highlight its sensitivity to various watermarking modifications.

Firstly, the imperceptibility is measured in decibels (dB) through *PSNR* given by Equation (9). The higher the *PSNR*, the better the imperceptibility.

$$PSNR = 10\log_{10}\frac{(255)^2 wh}{\sum_{i=1}^{w}\sum_{j=1}^{h}[I(i,j) - I'(i,j)]^2}; \quad (9)$$

where w and h are the width and height of an image. Moreover, $I(i,j)$ and $I'(i,j)$ indicate pixel values of the host and the watermarked images, respectively.

Secondly, another measure of the imperceptibility is the *SSIM*, calculated as per Equation 10.

$$SSIM(I, I') = l(I, I')c(I, I')s(I, I'); \quad (10)$$

here or at any other instance in this discussion, I and I' stand for the host and the watermarked images, respectively. Moreover, $l(I, I')$, $c(I, I')$, and $s(I, I')$ are the functions comparing the luminance, contrast and the overall structure of the host image and the watermarked image, respectively. To this end, if there is no difference (in terms of luminance, contrast and structural) between I and I' then the value attained by *SSIM* is "1" else, it is less than one. Note, the higher the *SSIM*, the better the imperceptibility. Further insight into *SSIM* can be gained from [51].

Thirdly, the security of the proposed method is tested through *NCC* given by Equation (11), where W and W' stand for the original and the extracted watermarks of dimensions $P \times Q$, respectively.

$$NCC = \frac{\sum_{i=1}^{P}\sum_{j=1}^{Q}(W[i,j] \times W'[i,j])}{\sqrt{\sum_{i=1}^{P}\sum_{j=1}^{Q}(W^2[i,j])} \times \sqrt{\sum_{i=1}^{P}\sum_{j=1}^{Q}(W'^2[i,j])}}. \quad (11)$$

Note, sometimes in the literature, the *NCC* is also addressed as "NC", and for the sake of consistency, the former is adopted throughout this discussion. The *NCC* values should range between [0 1], with '0' being the least in similarity and '1' being the same. Further insight on the *NCC* and its theoretical basis can be gained from [52] and [53]. Moreover, the *NCC*'s selection for assessing the security attribute of the proposed method is motivated by its usage in state-of-the-art works [14], [15], [16], [18], [19], [20], [21], [54], which are also chosen for comparison in this work.

Fourthly, FPR, FNR, and TPR are employed to measure the performance of tamper detection, and tamper localisation attributes, facilitated only by a fragile watermark [55]. The *FPR*, *FNR*, and *TPR* are defined by Equations 12, 13, and 14, respectively.

$$FPR = \frac{FP}{FP + TN}; \quad (12)$$

$$FNR = \frac{FN}{FN + TN}; \quad (13)$$

$$TPR = \frac{TP}{TP + FN}. \quad (14)$$

Here false-negative (FN) is the number of tampered pixels (which should be judged as tampered) that are judged as non-tampered. False-positive (FP) is the number of non-tampered pixels (which should be judged as non-tampered) that are judged as tampered. True-positive (TP) is the number of tampered pixels (which should be judged as tampered) that are judged as tampered. True-negative (TN) is the number of non-tampered pixels (which should be judged as non-tampered) that are judged as non-tampered.

Finally, another metric that measures a watermarking scheme's effectiveness in tamper detection and tamper localisation is known as the accuracy (ACC) [55]. It is defined as per Equation 15.

$$ACC = \frac{TP + TN}{FP + TN + TP + FN}. \quad (15)$$

B. IMPERCEPTIBILITY AND CAPACITY ANALYSIS

The watermarked images in the absence of an attack are shown in Figure 9. Subjectively, it can be noticed that the watermarked images appear to be indistinguishable from the host images. Moreover, as the watermarked images are undistorted, the embedded watermark is imperceptible to the HVS. To this end, the imperceptibility comparisons of the proposed method with existing state-of-the-art methods are shown in Table 2. Note, to fairly compare the proposed with existing state-of-the-art methods, the results in Table 2 are attained from the test image of *Lenna*, 512 × 512 in size. Such fairness is further highlighted as the proposed method uses the aforementioned machine to test all the methods given in the same table. Lastly, the proposed scheme is tested using the same watermarks as used by the existing state-of-the-art methods, and the embedding strength value of 0.005 is selected for all the methods.

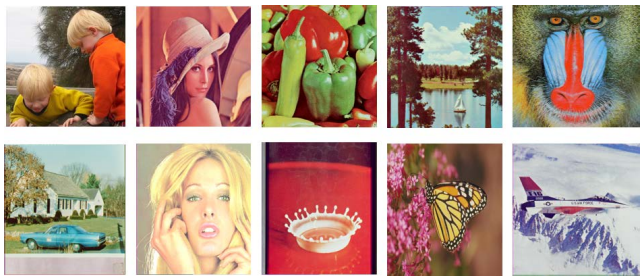
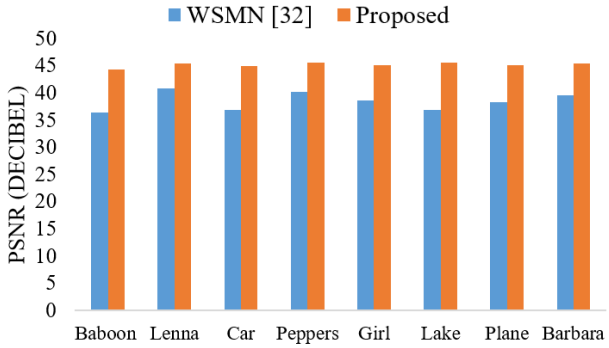


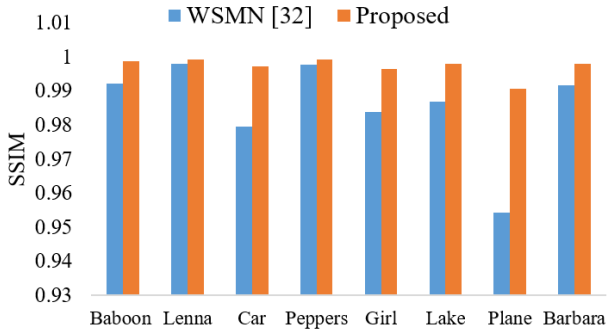
FIGURE 9. Imperceptibility comparisons of the proposed scheme in the absence of an attack. These images are embedded with the *WSU* watermark; 256 × 256 in size, and the value of β is 0.055. Subsequently, each of the *RGB* channels is embedded with a fragile watermark. Best viewed when zoomed-in.

TABLE 2. Imperceptibility analysis. The *PSNR* values are in decibels. Note, the employed test image is that of *Lenna*; 512 × 512 in size.

Method	Watermark type and size	$PSNR$ | $SSIM$
Hurrah *et al.* [14]	UOK: 64 × 64	44.28|0.92
Proposed		49.4|0.98
Loan *et al.* [15]	UOK: 64 × 64	42.54|0.91
Proposed		49.4|0.98
Kamili *et al.* [16]	UOK: 64 × 64	46.4|0.94
Proposed		49.4|0.98
Hurrah *et al.* [18]	UOK: 64 × 64	43.2|0.91
Proposed		49.4|0.98
Koley *et al.* [19]	Logo: 70 × 70	47.2|0.956
Proposed		48.5|0.96
Agarwal *et al.* [20]	Mark: 32 × 32	54.86|0.99
Proposed		63.2|1.0
Yasmeen *et al.* [21]	TLC: 256 × 256	34.8|0.74
Proposed		41.2|0.91
Kumar *et al.* [54]	Alphabet: 64 × 64	45.9|0.98
Proposed		49.1|0.93



(a) PSNR comparison



(b) SSIM comparison

FIGURE 10. *PSNR* and *SSIM* comparisons of WSMN's dual watermarking strategy with the proposed dual watermarking approach.

Firstly, Agarwal and Singh approach uses the *Mark* watermark, 32 × 32 in size [20]. The watermarked image(s) produced by their method is the highest in *PSNR* and *SSIM* values than any other method in Table 2, except the proposed method. This is because the watermark used by Agarwal *et al.*'s approach is the smallest of all the methods in the given table. Moreover, the smaller the watermark, the harder it is to verify. In contrast, Yasmeen and Uddin method [21] uses the biggest watermark i.e., *TLC*; 256 × 256 in dimensions. Consequently, the same table produces the watermarked image with the lowest *PSNR* and *SSIM* values.

Secondly, WSMN's dual watermarking strategy uses *Uni. logo* as a robust watermark to achieve copyright protection [32]. The strategy also employs self-generated fragile watermarks for authentication purposes. Figure 10 shows *PSNR* and *SSIM* comparisons of WSMN's dual watermarking strategy with the proposed dual watermarking approach. Note, the results which correspond to the proposed method in Figure 10 are achieved after using the *Uni. logo* as a robust watermark, 32 × 32 in size. Employing the identical watermark is essential and the only way to justify the proposed method's comparison with WSMN. The figure also highlights that the *PSNR* and *SSIM* values are calculated for various images. It is clear that, in terms of *PSNR* and *SSIM*, the proposed method's performance is superior to that of the WSMN. The superiority of the proposed method can be seen for each image chosen for comparison in Figure 10 and overall. For instance, the overall superiority can be quantified using the mean *PSNR* and *SSIM* values. Here in the comparison, the WSMN attains 38.5 dB and 0.985 as the mean *PSNR* and *SSIM* values, whereas 45.2 dB and 0.997 are the mean values achieved by the proposed method.

In addition to WSMN's dual watermarking approach, its authentication-only approach has also been compared to the proposed authentication-only technique. It is worth re-establishing that authentication-only approaches are solely based on the authentication or fragile watermark(s), and the robust watermark is not utilised. To this end, TRLG [28] and TRLH [56] are state-of-the-art methods within the same category, thereby employed in this comparison. The *PSNR* and *SSIM* analysis in Figure 11 shows that the other methods outperform WSMN's authentication-only approach. This being said, the mean *PSNR* and *SSIM* values achieved by WSMN are 42.38 dB and 0.9936, respectively. Such high values indicate that the watermarked images produced by WSMN's authentication-only approach are still imperceptible and on par with many state-of-the-art methods mentioned in this discussion. However, the watermarked images attained by TRLG and TRLH have better imperceptibility than those achieved by the WSMN. To this end, TRLG and TRLH are almost identical in their imperceptibility performance, and the similarity is evident in Figure 11. Moreover, the mean *PSNR* and *SSIM* values quantify the

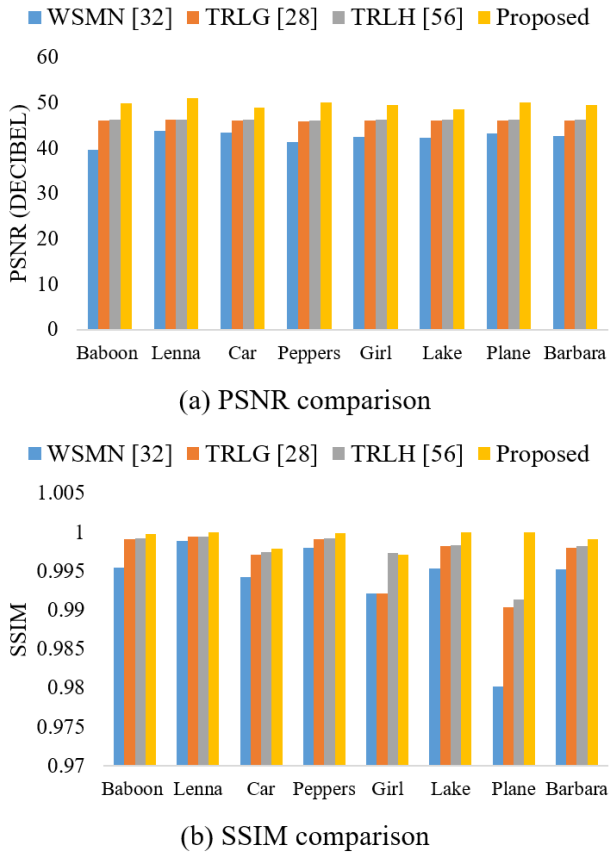


FIGURE 11. ***PSNR*** **and** ***SSIM*** **comparisons of the proposed authentication approach with similar state-of-the-art methods.**

imperceptibility performance of TRLG and TRLH. Here, the calculated mean values of TRLG are 46.13 dB and 0.996, and that of TRLH are 46.33 dB and 0.997. Notwithstanding the successful imperceptibility performances of the state-of-the-art methods in Figure 11, they are surpassed by the proposed authentication-only approach in this context. It can be observed in Figure 11 that the proposed approach achieves higher *PSNR* and *SSIM* values than any other method. Moreover, the claim is further justified via the mean *PSNR* and *SSIM* values of 49.70 dB and 0.999, respectively.

Thirdly, the schemes by the authors in [14], [15], [16], and [18] are tailored to balance the shortfalls of the aforementioned schemes with the highest and the lowest watermark capacity, respectively. As can be observed from Table 2, methods [14], [15], [16], [18] utilise a medium-sized *DOE* watermark, 64 × 64 in dimensions. Moreover, these methods can handle greyscale and colour images, excluding Kamili *et al.*'s method [16], which is only operable in the YC_bC_r colour-space. While operating on the greyscale images, Loan *et al.*'s [15] method is slightly better than Hurrah *et al.*'s method [18], in terms of imperceptibility. However, Hurrah *et al.*'s other method [14] is higher in *PSNR* and *SSIM* values. To this end, the difference in the watermark's imperceptibility amongst these three methods is not significant and they all share the same capacity. Moreover, when embedded with the same *DOE* watermark, the proposed method achieves better *PSNR* and *SSIM* values than its three counterparts. Here, Kamili *et al.*'s method outperforms [15] and [18] in terms of the imperceptibility attribute but not the proposed method. Similarly, the proposed method has the best *PSNR* and *SSIM* values, followed by Kumar and Singh method [54], another that uses a watermark that is also 64 × 64 in size.

Fourthly, the watermark used by Koley is *Logo*; 70 × 70 in size [19]. Notwithstanding the watermark size, their method outperforms other methods [14], [15], [16], [18] in terms of imperceptibility. This is thanks to the adaptive coefficient blending technique that Koley used in their study. To this end, after being embedded with the same *Logo* watermark, the watermarked images produced by the proposed method exhibit better imperceptibility traits by achieving higher *PSNR* and *SSIM* values than Koley *et al.*'s method.

Finally, Figure 12 further illustrates the *PSNR* and the *SSIM* performance of the proposed method. Here, the imperceptibility performance of the proposed method on different test images is illustrated, wherein various host images of different sizes are embedded with the *WSU* watermark. Moreover, the same figure and Figure 13 also highlight the effects of the change in the capacity or the embedded watermark's size. To this end, Figure12 shows, as the watermarking capacity decreases, the *PSNR* and the *SSIM* values increase and vice-versa. Similarly, in the case of Figure 13, it is illustrated that the smaller the watermark, the weaker is its immunity to the watermarking attacks. To sum up, the proposed method's superiority in Table 2 and performance in Figures 9 and 12 collectively justify and illustrate the bridging of the first gap mentioned above in Section I.

C. ROBUST WATERMARK's ROBUSTNESS ANALYSIS

The *NCC* plots are generated using different images after they are exposed to various StirMark attacks (available at [57]) are shown in Figure 14. These plots are achieved using the *WSU* watermark; 256 × 256 in size. Moreover, watermarks of different dimensions are used in Figure 15, wherein the robustness performance of the watermarks extracted using the proposed method is compared with those extracted using state-of-the-art methods.

The results within Figure 15 are attained by using the host image of *Lenna*, which is 512 × 512 in size. The same host image with similar dimensions is employed by each state-of-the-art method, chosen for comparisons in Figure 15. Moreover, the same figure illustrates that the robustness of the proposed method is tested using a variety of watermarks used by the existing state-of-the-art methods. Each of these comparisons is made using like-for-like watermark images, as below.

Firstly, Yasmeen and Uddin 's method [21] uses the *TLC* watermark; 256 × 256 in size. Their method has superior robustness over the proposed method's when tested against the median and the Gaussian low-pass filtering (LPF) and the histogram equalization (HE). However, the proposed method

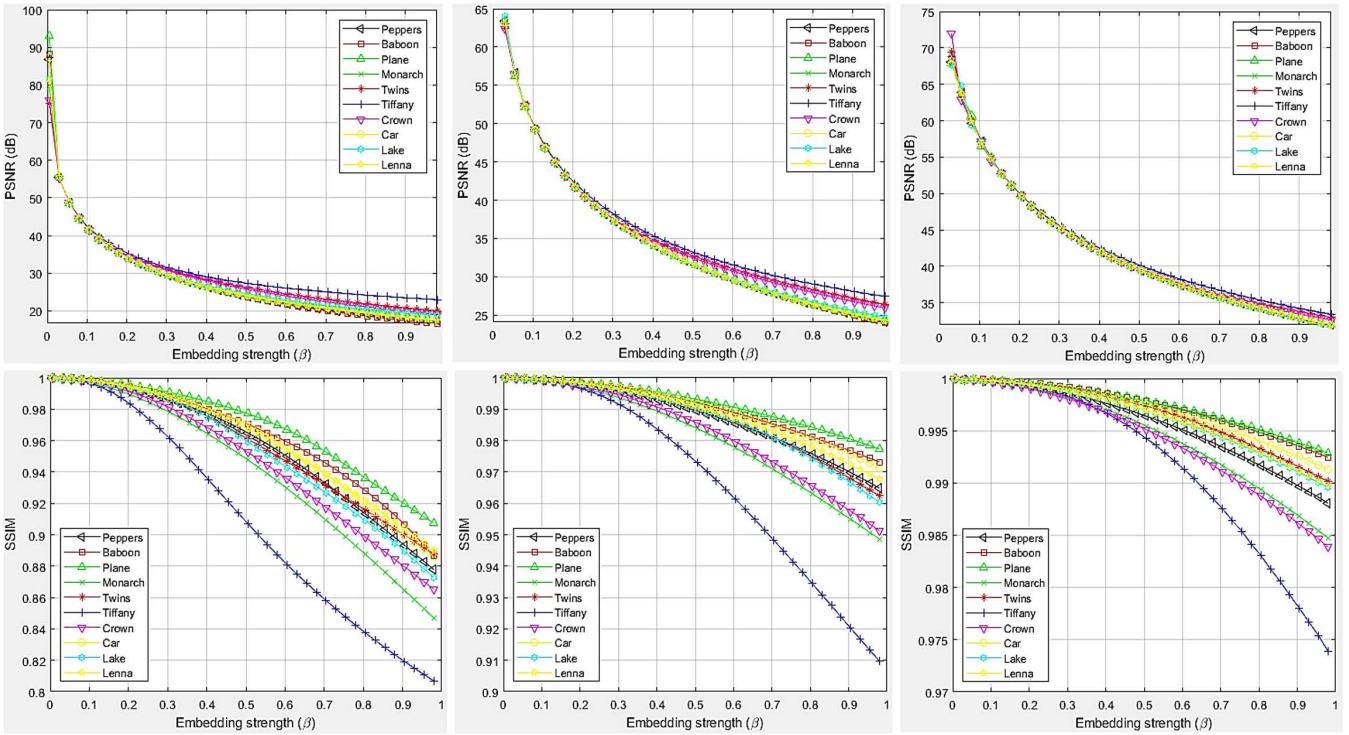


FIGURE 12. Imperceptibility comparisons of the proposed scheme in the absence of an attack. Here, different host images of different sizes are embedded with the *WSU* watermark. In the 1st column the *WSU* watermark, 256 × 256 in size is used, whereas the plots within 2nd and 3rd columns are generated using the *WSU* watermark, 128 × 128, and 64 × 64 in size, respectively. Moreover, each of the *RGB* channels in each of the host images is also embedded with the fragile watermarks. Best viewed when zoomed-in.

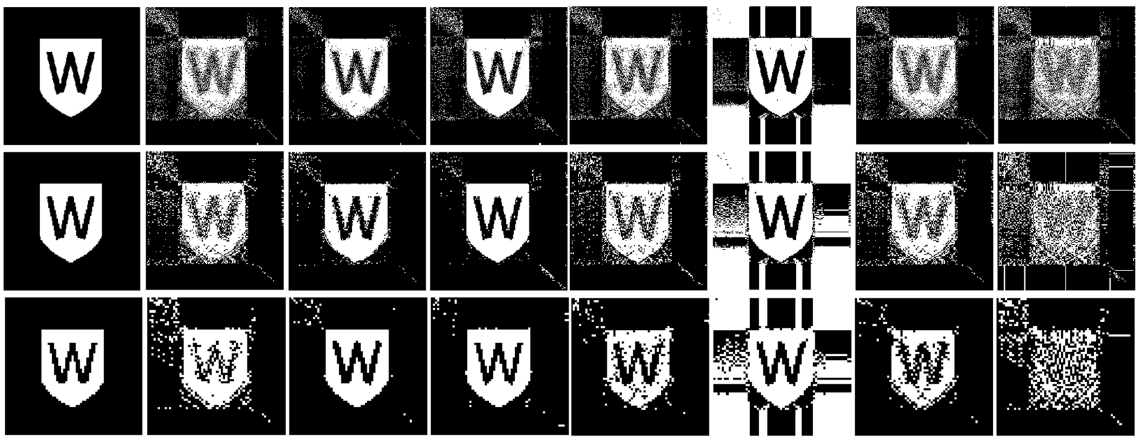


FIGURE 13. Behaviour of the robust watermark in response to the change in the capacity or the watermark's size. The 1st row shows the response of the *WSU* watermark, 256 × 256 in size, to various watermarking attacks. Left to right: no attack, Gaussian LPF, median filter, Gaussian noise, sharpening, histogram equilization, average filter, motion blurring. Similarly, 2nd and 3rd rows illustrate the same response to the aforementioned attacks but on the *WSU* watermark, 128 × 128 and 64 × 64 in size, respectively.

outperforms its opponent against numerous other watermarking attacks, as shown in Figure 15.

Secondly, Koley's method [19] utilises the *Logo* watermark; 70 × 70 in dimensions. Their method exhibits excellent robustness when tested against Gaussian LPF, median filtering, and HE. However, it has the worst performance against JPEG compression, one of the most commonly used manipulations in the whole image/video processing space. Moreover, the proposed method has outperformed Koley's method in the majority of the other watermarking attacks mentioned in Figure 15.

Thirdly, Kumar *et al.*'s method uses the *Alphabet* watermark; 64 × 64 in size [58]. Their method achieved better *NCC* values than the proposed method when tested against the sharpening, GN, and HE attacks, respectively. However, the proposed method performed better than its counterpart in the remainder of the attacks mentioned in Figure 15. Subsequently, Agarwal and Singh 's method [20] employs the *Mark* watermark; 32 × 32 in size. Its robustness performance is overshadowed by the proposed method when tested against any of the attacks mentioned in Figure 15. Moreover, another main shortfall associated with Agarwal *et al.*'s method is that

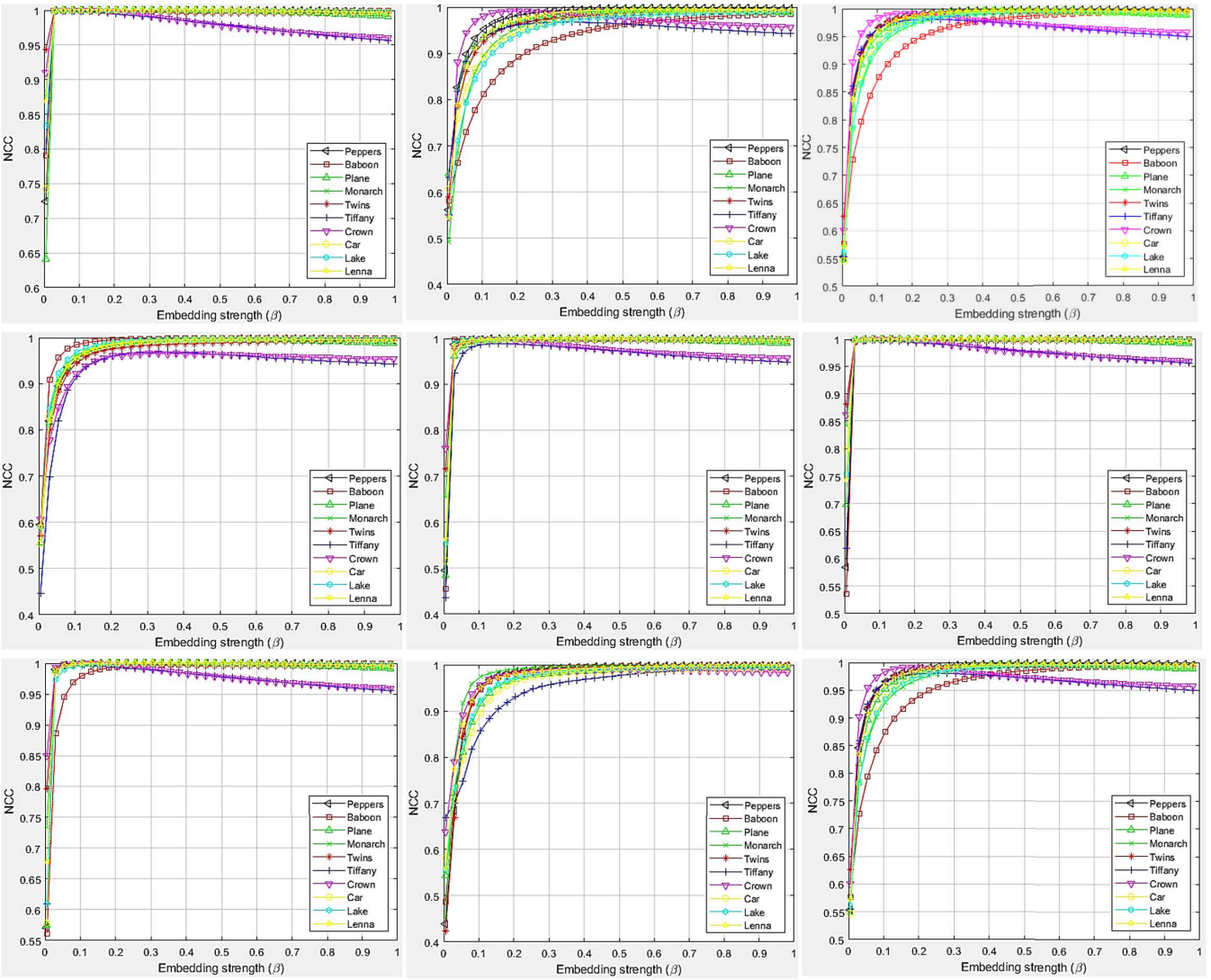


FIGURE 14. Robustness/*NCC* comparisons of the proposed scheme on different images under various attacks. The *WSU* watermark; 256 × 256 in size, is used in this analysis. Attacks performed are as follows. The 1st row (left to right): No attack, median filter (7 × 7), Gaussian low-pass filter (3 × 3). The 2nd row (left to right): Gaussian noise (0.003), speckle noise (0.003), JPEG compression (*QF* = 40). The 3rd row (left to right): JPEG2000 compression (*CR* = 14), rotation (2°), and the average filter (3 × 3). Best viewed when zoomed-in.

it is unequipped to deal with the geometrical attacks, such as rotation and scaling. Hence, not an ideal candidate for real-time applications.

WSMN is another method that uses *Uni. logo*, a 32 × 32 robust watermark [32]. Out of all the state-of-the-art techniques in Figure 15, WSMN is the only method that has tested the watermark's robustness against every attack mentioned in Figure 15. The robustness of the watermark embedded using WSMN is on par with the watermark embedded using the proposed method when tested against attacks, such as Gaussian LPF, median filtering, and sharpening. The similar is the case when tested against JPEG and JPEG 2000 compression. However, the robustness favors the proposed method when tested against other attacks in Figure 15. Such superiority is further highlighted in Figure 16, wherein the *NCC* values achieved by WSMN under several attacks are compared to the *NCC* values attained by the proposed method. Note that the comparison consistency between the proposed method and WSMN is ensured as both methods have used the same watermark, *Uni. logo*, 32 × 32 in size and the test image of *Lenna*, 512 × 512 in dimensions.

Fourthly, in Figure 15, watermarks of size 64 × 64 are used by methods [14], [15], [18]. The best *NCC* value regarding the sharpening attack is achieved by Loan *et al.*'s method [15]. Its immunity to the JPEG comparison, specifically at higher quality factors (QFs) is also superior to other methods. Moreover, Hurrah *et al.*'s methods [14] and [18] are better than Loan *et al.*'s in resisting the geometrical attacks. To this end, Hurrah *et al.*'s method [18] surpasses other method in [14] in terms of the overall *NCC* performance. Even after being exposed to various noise attacks, the proposed method achieves higher *NCC* values than all three of its counterpart methods. The same is true when resisting the majority of the JPEG compression attacks. The

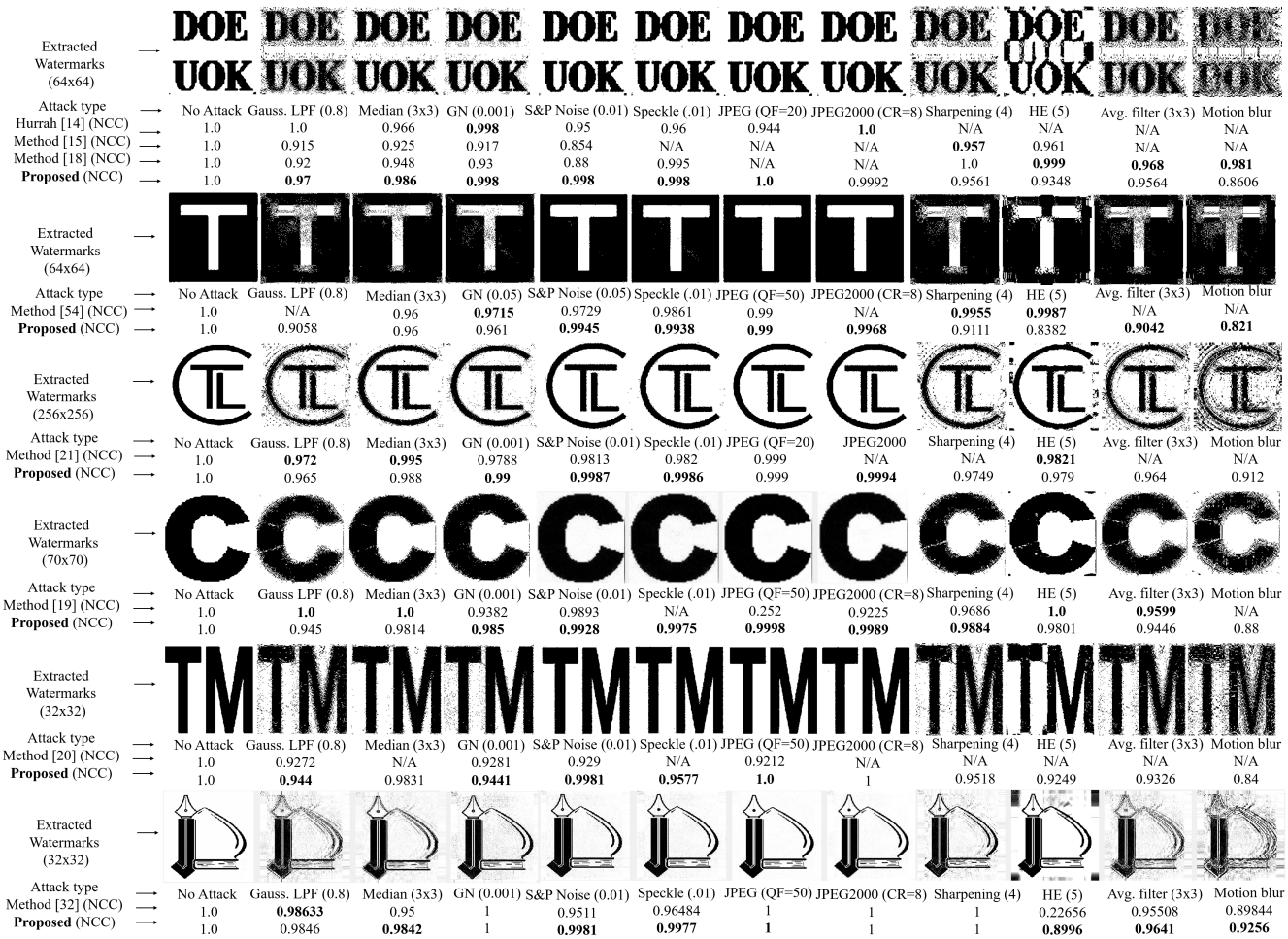


FIGURE 15. **Robustness performance of the robust watermarks extracted using the proposed method compared with state-of-the-art methods. These watermarks are extracted from the test image of *Lenna*, once it's been exposed to a variety of attacks. The test image is 512 × 512 in size. Best viewed when zoomed-in.**

proposed method operates as skillfully as method [14] under Gaussian noise and scaling attacks. Moreover, it outperforms [14] and all other methods in Figure 15 relating to the overall *NCC* performance, making it superior in overall robustness.

Finally, some of the results in Figures 14 and 15 are obtained using the static parameters. Specifically, the *NCC* results against JPEG compression, JPEG 2000 compression, median filtering and so on, are obtained at a particular *QF*, compression ratio (*CR*) and the window size, respectively. Such comparisons are vital when comparing the proposed method with existing methods, however in reality, many of these attacks are dynamic. In other words, JPEG compression, JPEG 2000 compression, median filtering, etc., can be performed over a wide range of *QFs*, *CRs*, and different window sizes, respectively. To this end, the proposed method is also tested against these attacks over a range of parameters, and the results are shown in Figure 17. These results prove the versatility of the proposed method to operate on a wide range of dynamic attacks, and highlight its robustness against such adversaries.

D. FRAGILE WATERMARK's FRAGILITY ANALYSIS

The fragility analysis of the proposed method is covered in Table 3. Results in Table 3 indicate that the *NCC* values are less than 0.025, and according to Thanki and Borra this is the threshold value below which the extracted watermark is meaningless [46]. In other words, if hackers make any change to the watermarked image, the proposed fragile watermark extraction yields a non-readable watermark, signaling the existence of tampering. To this end, an illustration of the extracted (fragile) watermarks from an attacked watermarked image is provided in Figure 18. Here, the extracted watermarks are scrambled, an indication of tampering. In contrast, the same figure also shows an illustration of successfully extracted fragile watermarks. Here, the unharmed watermarks are extracted from *RGB* channels, which signify the absence of an attack.

As mentioned earlier in the discussion, tamper detection and localisation are attributes facilitated only by the fragile watermark. A thorough analysis of these attributes is presented below in Figure 20. Here, the watermarked images are manipulated using a variety of watermarking attacks and

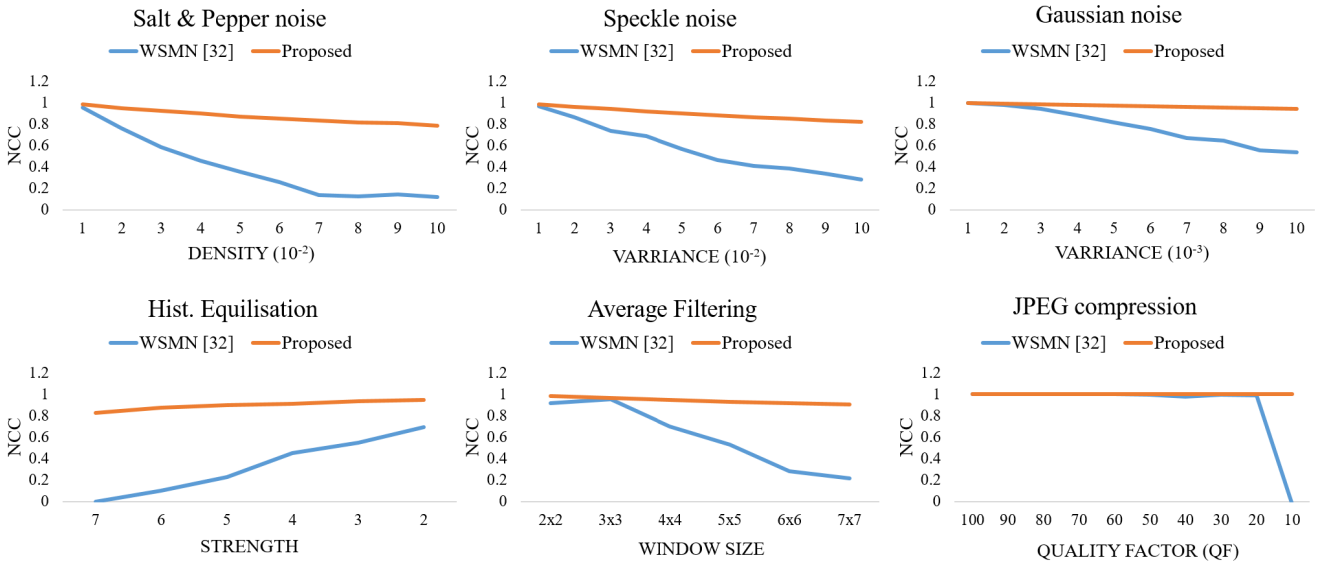


FIGURE 16. Robustness comparison of the robust watermarks processed via the proposed method and WSMN [32]. Note, both methods have used the same watermark, *Uni. logo*, 32 × 32 in size and the test image is that of *Lenna*, 512 × 512 in dimensions.

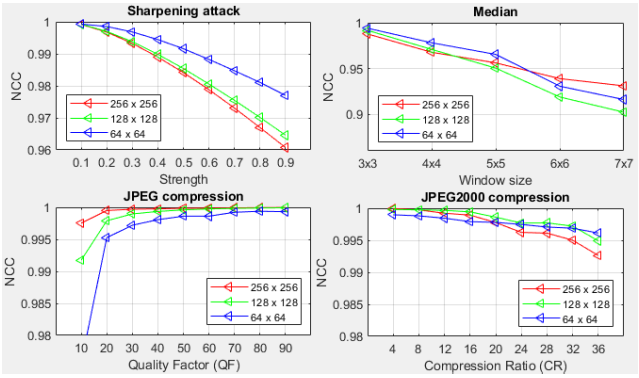


FIGURE 17. Watermark's robustness performance against the attacks which dynamic in nature. These plots are achieved from the host image of *Lenna's*; 512 × 512 in size and the *WSU* watermark with varying sizes. Best viewed when zoomed-in.

FIGURE 18. First row shows fragile watermarks extracted from *Lenna's* dual watermarked image in the absence of an attack. Here, the left-most impression is of the fragile watermark extracted from the red colour channel. The middle and the right-most images are the fragile watermarks extracted from the green and blue channels, respectively. In contrast, the second row shows fragile watermarks extracted from *Lenna's* dual watermarked image after it's been exposed to the median filtering attack. Best viewed when zoomed-in.

subsequently are exposed to the proposed tamper detection and localisation strategy. Consequently, both the subjective and the objective evaluations are provided in the given figure.

In Figure 20, the manipulated images are dually watermarked images i.e., watermarked with the robust and the fragile watermarks. Note, the robust watermark used for the illustration in the given figure is *Blessings*; 64 × 64 in size. The manipulated dually watermarked images are in 1^{st}, 4^{th}, 7^{th}, 10^{th} and 13^{th} rows. The subjective results of the proposed tamper detection and localisation strategy are in 2^{nd}, 5^{th}, 8^{th}, 11^{th} and 14^{th} rows. Similarly, the objective results; given via *ACC*, are in 3^{rd}, 6^{th}, 9^{th}, 12^{th} and 15^{th} rows. Moreover, the subjective results of the robust watermark extracted from the manipulated images are also shown in the same figure. Regarding the objective evaluations, it can be observed that the proposed scheme exhibits excellent *FPR*, *FNR*, and *TPR* results. Consequently, the method achieves high *ACC* values, some of which are as follows. The median of the *ACC* values given in the 3^{rd} row is 0.9654, in the 6^{th} row is 0.9511, in the 9^{th} row is 0.94395, in the 12^{th} row is 0.9626, and in the 15^{th} row is 0.9119, respectively. Such high values are indicative of the proposed method's precision and accuracy in terms of tamper detection and localisation. Moreover, they also highlight its ability to recognise a wide range of image manipulations which often happen in an industrial environment.

The proposed method's accuracy and precision in tamper detection and localisation is compared with existing state-of-the-art methods in Figure 19. Here, the 1^{st} column shows *Lenna's* watermarked image, which has been exposed to a variety of attacks. The 2^{nd} column shows tamper detection and localisation results obtained by the proposed method, and similar results obtained by existing state-of-the-art-methods [14], [15], [16] are in 3^{rd}, 4^{th} and

TABLE 3. Fragility analysis of the fragile watermarks under different attacks.

Red component										
Attacks ↓ | NCC ↘ | Images →	Twins	Lenna	Baboon	Peppers	Crown	Lake	Tiffany	Plane	Monarch	Car
Attack-free	1	1	0.98	1	0.99	1	0.98	0.99	1	1
Rotation 45°	0.018	0.023	0.019	0.014	0.013	0.017	0.013	0.011	0.023	0.011
Median filtering (3×3)	0.013	0.02	0.019	0.014	0.018	0.016	0.022	0.021	0.023	0.017
Gamma correction at ($\gamma = 0.50$)	0.019	0.013	0.011	0.021	0.018	0.023	0.0198	0.024	0.021	0.019
Salt & Pepper noise (0.02)	0.02	0.023	0.012	0.014	0.022	0.024	0.015	0.023	0.018	0.019
Gaussian noise (0.001)	0.024	0.022	0.02	0.018	0.021	0.014	0.013	0.017	0.023	0.021
Histogram equilization	0.014	0.021	0.021	0.015	0.024	0.021	0.023	0.016	0.014	0.022
Blurring (5%)	0.013	0.015	0.021	0.021	0.024	0.023	0.012	0.016	0.022	0.019
Sharpening (25%)	0.014	0.018	0.014	0.015	0.016	0.024	0.012	0.022	0.023	0.019
Scaling (50%)	0.017	0.019	0.021	0.014	0.024	0.019	0.022	0.015	0.022	0.017
Compression (QF= 40)	0.019	0.014	0.022	0.017	0.024	0.017	0.022	0.018	0.018	0.013
Compression (QF= 50)	0.022	0.024	0.012	0.021	0.016	0.023	0.016	0.014	0.024	0.022
Green component										
Attack-free	1	0.99	1	1	1	1	1	0.98	0.99	0.96
Rotation 45°	0.021	0.021	0.02	0.022	0.012	0.024	0.021	0.023	0.014	0.011
Median filtering (3×3)	0.017	0.019	0.021	0.017	0.011	0.013	0.021	0.012	0.011	0.019
Gamma correction at ($\gamma = 0.50$)	0.012	0.014	0.012	0.018	0.024	0.018	0.017	0.021	0.022	0.014
Salt & Pepper noise (0.02)	0.013	0.019	0.016	0.015	0.013	0.015	0.018	0.016	0.013	0.022
Gaussian noise (0.001)	0.015	0.016	0.013	0.017	0.016	0.012	0.022	0.012	0.012	0.022
Histogram equilization	0.016	0.022	0.012	0.021	0.022	0.011	0.021	0.013	0.015	0.012
Blurring (5%)	0.012	0.016	0.017	0.022	0.016	0.021	0.016	0.011	0.016	0.015
Sharpening (25%)	0.004	0.015	0.021	0.012	0.016	0.005	0.015	0.009	0.021	0.006
Scaling (50%)	0.016	0.015	0.023	0.009	0.022	0.019	0.017	0.016	0.024	0.011
Compression (QF= 40)	0.014	0.019	0.021	0.016	0.023	0.018	0.023	0.006	0.019	0.011
Compression (QF= 50)	0.023	0.021	0.018	0.019	0.017	0.021	0.012	0.017	0.024	0.019
Blue component										
Attack-free	1	0.97	1	0.96	0.98	0.97	1.0	0.95	1	1
Rotation 45°	0.0130	0.021	0.009	0.023	0.011	0.018	0.015	0.023	0.017	0.009
Median filtering (3×3)	0.02	0.023	0.011	0.019	0.015	0.019	0.021	0.012	0.021	0.013
Gamma correction at ($\gamma = 0.50$)	0.023	0.017	0.02	0.021	0.013	0.016	0.014	0.018	0.017	0.021
Salt & Pepper noise (0.02)	0.013	0.023	0.016	0.021	0.014	0.012	0.013	0.019	0.015	0.018
Gaussian noise (0.001)	0.012	0.017	0.016	0.023	0.019	0.011	0.017	0.023	0.021	0.013
Histogram equilization	0.011	0.019	0.017	0.021	0.022	0.014	0.019	0.013	0.021	0.016
Blurring (5%)	0.017	0.023	0.011	0.02	0.013	0.017	0.019	0.022	0.009	0.012
Sharpening (25%)	0.008	0.024	0.019	0.016	0.015	0.006	0.012	0.022	0.016	0.013
Scaling (50%)	0.009	0.006	0.019	0.011	0.009	0.014	0.016	0.012	0.019	0.012
Compression (QF= 40)	0.009	0.011	0.007	0.012	0.009	0.014	0.016	0.012	0.018	0.009
Compression (QF= 50)	0.014	0.012	0.011	0.016	0.013	0.018	0.019	0.021	0.023	0.014

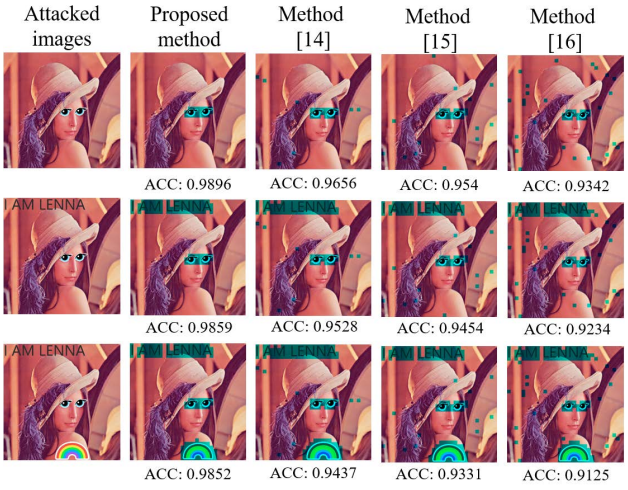


FIGURE 19. Proposed method's tamper detection and localisation comparison with existing state-of-the-art methods. Best viewed when zoomed-in.

5^{th} columns, respectively. In regards to the *ACC* performance, Kamili *et al.*'s method [16] has under-performed when compared to the proposed method, and other methods in [14] and [15]. Similarly, Loan *et al.*'s method [15] is objectively outperformed by Hurrah *et al.*'s method [14] and the proposed method. To this end, the proposed method has better *ACC* performance than its counterparts. Subjectively, Figure 19 shows that the proposed method's tamper detection and localisation results are excellent. In contrast, other methods regularly misinterpret the non-tampered area as tampered, which goes to their detriment. In short, the proposed method exhibits superior objective and subjective performances in terms of tamper detection and localisation attributes than existing state-of-the-art methods. Moreover, Figures 19 and 20, and the discussion in this subsection illustrate and justify the bridging of the fifth gap, mentioned above in Section I, respectively.

E. PERFORMANCE AGAINST THE VQ, COPY-MOVE AND PROTOCOL ATTACKS

In addition to the aforementioned watermarking attacks, the proposed method's performance against other well-known manipulations is covered here. (VQ), copy-move and protocol attacks are some of the attacks in the limelight over the last few years. Due to space constraints, this discussion does not elaborate on the intricacies of these attacks, and only an brief overview is provided here. However, TRLG provides an excellent insight into these attacks [28].

- In the VQ attack, a part of a watermarked image(s), achieved by a particular watermarking method is

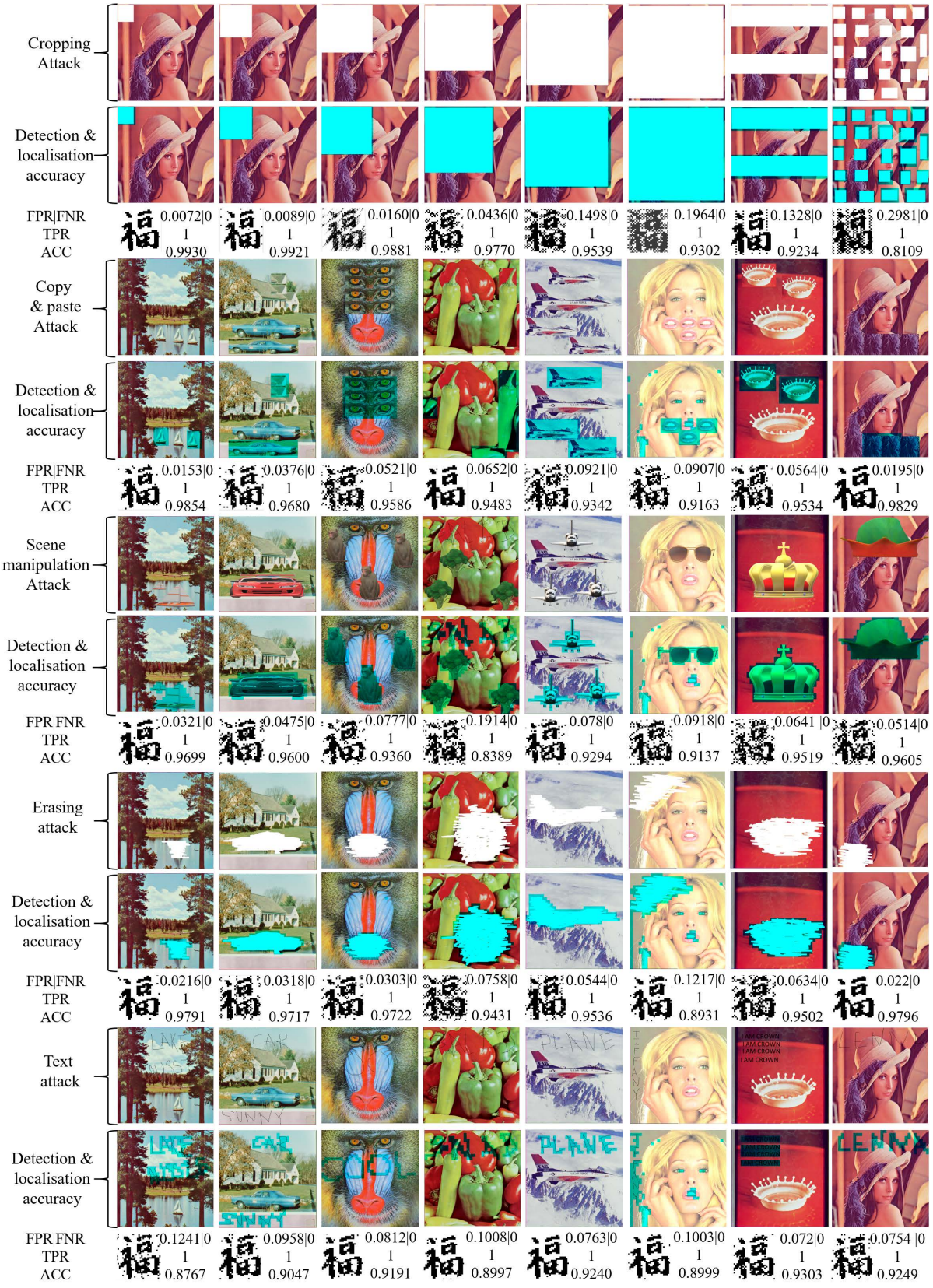


FIGURE 20. Illustration of different attacks when performed on the watermarked images which are achieved using the proposed method. Here, the robust (*Blessings*) watermark's immunity to attacks is depicted via the successfully extracted impressions of the robust watermark. Note that in this instance, the *FPR, FNR, TPR*, and *ACC* values are not to be associated with the robust watermark. Instead, these values represent the proposed method's performance in tamper detection and localisation attributes, facilitated only by the authentication or fragile watermark(s). Best viewed when zoomed-in.

FIGURE 21. Proposed method's performance against the VQ, copy-move and protocol attacks. Best viewed when zoomed-in.

inserted into another watermarked or target image, acquired by the same method. Illustrations within the red boundaries in Figure 21 depict images exposed to the VQ attack. Here, the attacked watermarked images are achieved via the proposed method.

- In the copy-move attack, a part(s) of the watermarked image is copied and subsequently placed within the same watermarked image. Illustrations within the orange boundaries in Figure 21 show a few examples of the images attacked via copy-move. Here the employed watermarked images are achieved using the proposed method.
- The protocol attack, also known as the watermark copy or ambiguity attack, is one of the significant watermarking manipulations. In this attack, external information is inserted into a target image so that the LSBs of the target image remain unaltered. Consequently, the attack often leads to ambiguity during the watermark extraction process, and the attack may remain unnoticed. Despite the attack's effectiveness, many state-of-the-art methods have not been tested against this attack. The same is not the case for this discussion, as the effects of the protocol attack are evident from illustrations within the green boundaries of Figure 21.

Figure 21 shows the performance of the proposed method against the VQ, copy-move, and protocol attacks when performed over various images. Here, embedded with robust and fragile watermarks, the watermarked images are exposed to attacks, whereby their robustness and fragility performance is also presented. It is evident from the figure that the robust watermark has survived each of these attacks and the *NCC* values are excellent. The primary reason for such pronounced robustness is that the robust watermark is embedded within the frequency domain in the proposed method. In contrast, these attacks are executed predominantly in the spatial domain. Hence, it is improbable for the spatial domain-based attacks to abolish the frequency coefficients representing the robust watermark's information.

Figure 21 also highlights the proposed method's tamper detection and localisation performance against the VQ, copy-move, and protocol attacks. Here, it is evident that the *FPR* and *FNR* values are almost negligible, whereas the *TPR* and *ACC* values are high. These attributes highlight that the proposed method's tamper detection and localisation performance is on par with several state-of-the-art methods [28], [32], [56], if not better. The reason for such high performance of the proposed method is that the fragile watermark(s) employed by the proposed method is self-generated, and before embedding in a block, it is concatenated with the block's mean value. The concatenation results in a dependency of the block information on the fragile watermark and vice-versa. Consequently, harming one harms the other, making it challenging for the watermarking attacks to break the dependency. Hence, in the proposed method, the watermark and block information work hand-in-hand to provide authentication and achieve tamper detection and localisation.

F. PROCESSING TIME ANALYSIS

The processing time (PT) of the proposed multipurpose watermarking scheme is dependent on the dimensions of the host image and that of the watermark. The larger these sizes, the longer the processing time. In the case of embedding, the processing time ($PT_{Embedding}$) is calculated in Equation 16, below.

$$PT_{Embedding} = Time_{Robust} + Time_{Fragile}. \tag{16}$$

Here, $Time_{Robust}$ and $Time_{Fragile}$ are the times taken for embedding the robust and the fragile watermark(s). Similarly, in the case of the extraction, the processing time ($PT_{Extraction}$) is calculated in Equation 17, below.

$$PT_{Extraction} = Time'_{Robust} + Time'_{Fragile}. \tag{17}$$

TABLE 4. Processing time evaluation (in Seconds).

Robust watermark is *WSU*: 64×64			
Host: *Lenna*	$PT_{Embedding}$	$PT_{Extraction}$	PT_{Total}
2048×2048	6.1	7.4	13.5
1024×1024	5.6	6.7	12.3
512×512	5.1	6.1	11.2
256×256	4.8	5.2	10.0
128×128	4.3	4.8	9.1
Robust watermark is *WSU*: 128×128			
Host: *Lenna*	$PT_{Embedding}$	$PT_{Extraction}$	PT_{Total}
2048×2048	7.8	8.7	16.5
1024×1024	7.2	7.9	15.1
512×512	6.7	7.2	13.9
256×256	5.8	6.3	12.1
Robust watermark is *WSU*: 256×256			
Host: *Lenna*	$PT_{Embedding}$	$PT_{Extraction}$	PT_{Total}
2048×2048	9.1	9.8	18.9
1024×1024	8.4	8.9	17.3
512×512	7.1	7.8	14.9

TABLE 5. Processing time comparison (in Seconds). The host image is *Lenna*; 512 × 512 in size, and the robust watermark is 64 × 64.

Methods	$PT_{Embedding}$	$PT_{Extraction}$	PT_{Total}
Method [10]	6.3	6.8	13.2
Method [14]	5.6	6.4	13.0
Method [16]	3.42	2.99	6.41
Ours	5.1	6.1	11.2

Here, $Time'_{Robust}$ and $Time'_{Fragile}$ are the times taken for extracting the robust watermark and the fragile watermark(s). Ultimately, the total PT (PT_{Total}) is calculated in Equation 18, below.

$$PT_{Total} = PT_{Embedding} + PT_{Extraction}. \tag{18}$$

Note, in the case of the fragile watermark, tamper detection and localisation impose an overhead to the $PT_{Extraction}$. However, as these procedures happen in the spatial domain, their impact on the overall extraction time is insignificant. A glimpse into the execution timings of the proposed method is presented in Table 4. The given table illustrates the PT's dependency on the sizing of the host image and the embedded watermarks.

Table 5 illustrates that when compared to the existing multipurpose watermarking methods [10], [14], [16], the proposed method is faster than methods in [10] and [14]. However, it is outperformed by kamili *et al.*'s method in the similar context [16]. Moreover, kamili *et al.*'s method [16] is the fastest of all the methods discussed here, because it is implemented only within the YC_bCr colour space. In contrast, the proposed method, and others [10], [14] are implemented using the YC_bCr and the *RGB* colour-spaces. Although kamili *et al.*'s method is the most time efficient, it does lack in terms of the *ACC* performance when compared to the proposed method and Hurrah *et al.*'s method [14]. This being said, the proposed method is very much employable for the real-time applications in its current state. However, our future work will be focused on further optimising the processing time analysis of the proposed method.

V. CONCLUSION AND FUTURE WORKS

A novel image watermarking scheme with its potential applications in Industry 4.0 is presented. The proposed scheme is multipurpose as it both authenticates and protects the copyright of images, transmitted within an industrial environment. To this end, two new watermarking methods are presented; one is for embedding the robust watermark, and the other is related to the fragile watermark. The robust watermark's embedding is achieved in the frequency domain, wherein the frequency coefficients are selected using a novel mean-based coefficient selection procedure. Subsequently, the selected coefficients are manipulated in equal proportion to embed the robust watermark. The fragile watermark's embedding is achieved in the spatial domain, wherein a self-generated fragile watermark is embedded by directly altering the pixel bits of the image that is meant for transmission. The following conclusions are drawn from this study.

- The watermarked images produced using the proposed method are excellent in imperceptibility and achieve high *PSNR* and *SSIM* values. For instance, when a watermark as large as 256×256 in dimensions is embedded in the host image that is 512×512 in size, the smallest *PSNR* and *SSIM* values achieved by the proposed method are > 41 dB and > 0.9, respectively. In similar context, the proposed scheme has outperformed the existing state-of-art-methods [14], [15], [16], [18], [19], [20], [21], [54], when tested on datasets, available at [49] and [50]. Moreover, the resourcefulness of the proposed scheme is demonstrated by its ability to handle images as small as 128×128 and as large as 2048×1152 in pixel resolution.
- The robustness performance of the robust watermark embedded using the proposed method is higher than the existing state-of-the-art methods. Considering the smaller the watermark, the weaker the *NCC* value, a 32×32 robust watermark embedded using the proposed method achieves the median *NCC* value of > 0.95. Note, this median value is the median of all the *NCC* values attained by the robust watermark after it is exposed to > 70 variations of watermarking attacks. Similarly, the fragility of the fragile watermark(s) is tested over a large variety of such attacks. When attacked, the lower the *NCC* value, the better the fragility of the fragile watermark. In the case of an attack, the *NCC* values of < 0.025 are achieved by the fragile watermark(s), embedded using the proposed method. In terms of the overall security (robustness and fragility), the proposed method has demonstrated its superiority over the existing state-of-the-art methods.
- The proposed method's precision and accuracy in tamper detection and localisation are high. To this end, the average value of such accuracy (*ACC*) achieved by the proposed method in this study is 0.9394 or 93.94%. Such high accuracy value highlights the proposed method's ability to recognise a wide range of image manipulations which often happen in an industrial environment. Moreover, in the terms of the *ACC* performance, the proposed methods has outperformed widely-cited methods [14], [15], [16].

The main limitation of the proposed method is that it is not reversible. In other words, it cannot restore or recover the tampered regions. This shortfall will be addressed in the subsequent work, which will be inspired by the state-of-the-art methods in the category, such as TRLG and [28] and TRLH [56], respectively. In the future, the proposed method will also aim to explore the machine learning (ML) domain. Its potential extension will align with the widely cited works that employed ML to achieve watermarking, such as WSMN [32]. To the best of our knowledge, no specific image models exist within the Industry 4.0 environment. Hence, another aspect in the future that will be inspected is the potential of the image model development for the proposed watermarking within Industry 4.0. Last but not least, the proposed study will explore the effects of incorporating other transform domain-based techniques or tools. For instance, techniques such as curvelets or contourlets, shearlet transform, and others will be used instead of DCT or DWT. To this end, a thorough analysis of the results achieved after employing these techniques will be done and compared with the experimental results presented in the proposed study.

ACKNOWLEDGMENT

Thanks to Jessica Johnston for editing and proofreading the manuscript. The authors are thankful to the anonymous reviewers for their helpful comments and suggestions.

REFERENCES

[1] F. Xie, Z. Pang, H. Wen, W. Lei, and X. Xu, "Weighted voting in physical layer authentication for industrial wireless edge networks," *IEEE Trans. Ind. Informat.*, vol. 18, no. 4, pp. 2796–2806, Apr. 2022.

[2] J. Gao, B. Zhang, X. Guo, T. Baker, M. Li, and Z. Liu, "Secure partial aggregation: Making federated learning more robust for industry 4.0 applications," *IEEE Trans. Ind. Informat.*, vol. 18, no. 9, pp. 6340–6348, Sep. 2022.

[3] Y. Sharma, J. Taheri, W. Si, D. Sun, and B. Javadi, "Dynamic resource provisioning for sustainable cloud computing systems in the presence of correlated failures," *IEEE Trans. Sustain. Comput.*, vol. 6, no. 4, pp. 641–654, Oct. 2021.

[4] I. J. Kadhim, P. Premaratne, P. J. Vial, and B. Hallorana, "Comprehensive survey of image steganography: Techniques, evaluations, and trends in future research," *Neurocomputing*, vol. 335, pp. 299–326, Mar. 2019.

[5] 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.

[6] S. Sharma, J. J. Zou, and G. Fang, "Recent developments in halftone based image watermarking," in *Proc. Int. Conf. Electr. Eng. Res. Pract. (ICEERP)*, Nov. 2019, pp. 1–6.

[7] S. Sharma, J. J. Zou, and G. Fang, "A novel signature watermarking scheme for identity protection," in *Proc. Digit. Image Comput., Techn. Appl. (DICTA)*, Nov. 2020, pp. 1–5.

[8] S. Roy and A. K. Pal, "A blind DCT based color watermarking algorithm for embedding multiple watermarks," *AEU, Int. J. Electron. Commun.*, vol. 72, pp. 149–161, Feb. 2017.

[9] A. Giakoumaki, S. Pavlopoulos, and D. Koutsouris, "Multiple image watermarking applied to health information management," *IEEE Trans. Inf. Technol. Biomed.*, vol. 10, no. 4, pp. 722–732, Oct. 2006.

[10] X. L. Liu, C. C. Lin, and S. M. Yuan, "Blind dual watermarking for color images' authentication and copyright protection," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 28, no. 5, pp. 1047–1055, May 2018.

[11] *Scopus*. Accessed: Jul. 16, 2022. [Online]. Available: https://www.scopus.com/search/form.uri?

[12] D. Bhowmik and C. Abhayaratne, "Embedding distortion analysis in wavelet-domain watermarking," *ACM Trans. Multimedia Comput., Commun., Appl.*, vol. 15, no. 4, pp. 1–24, Nov. 2019.

[13] S. Sharma, J. J. Zou, and G. Fang, "Significant difference-based watermarking in multitoned images," *Electron. Lett.*, vol. 56, no. 18, pp. 923–926, Sep. 2020.

[14] N. N. Hurrah, S. A. Parah, N. A. Loan, J. A. Sheikh, M. Elhoseny, and K. Muhammad, "Dual watermarking framework for privacy protection and content authentication of multimedia," *Future Gener. Comput. Syst.*, vol. 94, pp. 654–673, May 2019.

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

[16] A. Kamili, N. N. Hurrah, S. A. Parah, G. M. Bhat, and K. Muhammad, "DWFCAT: Dual watermarking framework for industrial image authentication and tamper localization," *IEEE Trans. Ind. Informat.*, vol. 17, no. 7, pp. 5108–5117, Jul. 2021.

[17] F. Tohidi, M. Paul, and M. R. Hooshmandasl, "Detection and recovery of higher tampered images using novel feature and compression strategy," *IEEE Access*, vol. 9, pp. 57510–57528, 2021.

[18] N. N. Hurrah, S. A. Parah, J. A. Sheikh, F. Al-Turjman, and K. Muhammad, "Secure data transmission framework for confidentiality in IoTs," *Ad Hoc Netw.*, vol. 95, Dec. 2019, Art. no. 101989.

[19] S. Koley, "A feature adaptive image watermarking framework based on phase congruency and symmetric key cryptography," *J. King Saud Univ., Comput. Inf. Sci.*, vol. 34, no. 3, pp. 636–645, Mar. 2022.

[20] N. Agarwal and P. K. Singh, "Discrete cosine transforms and genetic algorithm based watermarking method for robustness and imperceptibility of color images for intelligent multimedia applications," *Multimedia Tools Appl.*, vol. 81, pp. 19751–19777, Jan. 2022.

[21] F. Yasmeen and M. S. Uddin, "An efficient watermarking approach based on LL and HH edges of DWT–SVD," *Social Netw. Comput. Sci.*, vol. 2, no. 2, pp. 1–16, Apr. 2021.

[22] N. N. Hurrah, S. A. Parah, and J. A. Sheikh, "Embedding in medical images: An efficient scheme for authentication and tamper localization," *Multimedia Tools Appl.*, vol. 79, nos. 29–30, pp. 21441–21470, Aug. 2020.

[23] C.-S. Lu and H.-Y. M. Liao, "Multipurpose watermarking for image authentication and protection," *IEEE Trans. Image Process.*, vol. 10, no. 10, pp. 1579–1592, Oct. 2001.

[24] I. Daubechies, B. Han, A. Ron, and Z. Shen, "Framelets: MRA-based constructions of wavelet frames," *Appl. Comput. Harmon. Anal.*, vol. 14, no. 1, pp. 1–46, 2003.

[25] I. W. Selesnick, R. G. Baraniuk, and N. C. Kingsbury, "The dual-tree complex wavelet transform," *IEEE Signal Process. Mag.*, vol. 22, no. 6, pp. 123–151, Nov. 2005.

[26] X.-B. Kang, F. Zhao, G.-F. Lin, and Y.-J. Chen, "A novel hybrid of DCT and SVD in DWT domain for robust and invisible blind image watermarking with optimal embedding strength," *Multimedia Tools Appl.*, vol. 77, no. 11, pp. 13197–13224, 2018.

[27] A. K. Singh, B. Kumar, S. K. Singh, S. P. Ghrera, and A. Mohan, "Multiple watermarking technique for securing online social network contents using back propagation neural network," *Future Gener. Comput. Syst.*, vol. 86, no. 1, pp. 926–939, 2018.

[28] B. B. Haghighi, A. H. Taherinia, and A. H. Mohajerzadeh, "TRLG: Fragile blind quad watermarking for image tamper detection and recovery by providing compact digests with optimized quality using LWT and GA," *Inf. Sci.*, vol. 486, pp. 204–230, Jun. 2019.

[29] K. Sreenivas and V. K. Prasad, "Fragile watermarking schemes for image authentication: A survey," *Int. J. Mach. Learn. Cybern.*, vol. 9, no. 7, pp. 1193–1218, Jul. 2018.

[30] I. A. Ansari and M. Pant, "Multipurpose image watermarking in the domain of DWT based on SVD and ABC," *Pattern Recognit. Lett.*, vol. 94, pp. 228–236, Jul. 2017.

[31] N. Daneshmandpour, H. Danyali, and M. S. Helfroush, "Image tamper detection and multi-scale self-recovery using reference embedding with multi-rate data protection," *China Commun.*, vol. 16, no. 11, pp. 154–166, Nov. 2019.

[32] B. B. Haghighi, A. H. Taherinia, A. Harati, and M. Rouhani, "WSMN: An optimized multipurpose blind watermarking in shearlet domain using MLP and NSGA-II," *Appl. Soft Comput.*, vol. 101, Mar. 2021, Art. no. 107029.

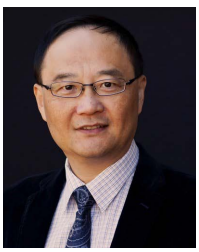
[33] R. Sinhal, S. Sharma, I. A. Ansari, and V. Bajaj, "Multipurpose medical image watermarking for effective security solutions," *Multimedia Tools Appl.*, vol. 81, no. 10, pp. 14045–14063, Apr. 2022.

[34] S. Sharma, J. J. Zou, and G. Fang, "A single watermark based scheme for both protection and authentication of identities," *IET Image Process.*, pp. 1–20, Jun. 2022, doi: 10.1049/ipr2.12542.

[35] S. Sharma, J. J. Zou, and G. Fang, "A dual watermarking scheme for identity protection," *Multimedia Tools Appl.*, pp. 1–30, Jun. 2022, doi: 10.1007/s11042-022-13207-1.
[36] S. A. Parah, J. A. Sheikh, N. A. Loan, and G. M. Bhat, "Robust and blind watermarking technique in DCT domain using inter-block coefficient differencing," *Digit. Signal Process.*, vol. 53, pp. 11–24, Jun. 2016.
[37] F. Bertini, R. Sharma, and D. Montesi, "Are social networks watermarking us or are we (unawarely) watermarking ourself?" 2020, *arXiv:2006.03903*.
[38] W.-H. Lin, S.-J. Horng, T.-W. Kao, P. Fan, C.-L. Lee, and Y. Pan, "An efficient watermarking method based on significant difference of wavelet coefficient quantization," *IEEE Trans. Multimedia*, vol. 10, no. 5, pp. 746–757, Aug. 2008.
[39] V. S. Verma, R. K. Jha, and A. Ojha, "Significant region based robust watermarking scheme in lifting wavelet transform domain," *Expert Syst. Appl.*, vol. 42, no. 21, pp. 8184–8197, Nov. 2015.
[40] M. Islam, A. Roy, and R. H. Laskar, "SVM-based robust image watermarking technique in LWT domain using different sub-bands," *Neural Comput. Appl.*, vol. 32, no. 5, pp. 1379–1403, Mar. 2020.
[41] T. Huynh-The, C.-H. Hua, N. A. Tu, and D.-S. Kim, "Robust image watermarking framework powered by convolutional encoder–decoder network," in *Proc. Digit. Image Comput., Techn. Appl. (DICTA)*, Dec. 2019, pp. 1–7.
[42] T. Huynh-The, O. Banos, S. Lee, Y. Yoon, and T. Le-Tien, "Improving digital image watermarking by means of optimal channel selection," *Expert Syst. Appl.*, vol. 62, pp. 177–189, Nov. 2016.
[43] T. Huynh-The, C.-H. Hua, N. A. Tu, T. Hur, J. Bang, D. Kim, M. B. Amin, B. H. Kang, H. Seung, and S. Lee, "Selective bit embedding scheme for robust blind color image watermarking," *Inf. Sci.*, vol. 426, pp. 1–18, 2018.
[44] F. Musanna and S. Kumar, "A novel fractional order chaos-based image encryption using Fisher Yates algorithm and 3-D cat map," *Multimedia Tools Appl.*, vol. 78, no. 11, pp. 14867–14895, Jun. 2019.
[45] A. Karawia, "Image encryption based on Fisher–Yates shuffling and three dimensional chaotic economic map," *IET Image Process.*, vol. 13, no. 12, pp. 2086–2097, Oct. 2019.
[46] R. Thanki and S. Borra, "Fragile watermarking for copyright authentication and tamper detection of medical images using compressive sensing (CS) based encryption and contourlet domain processing," *Multimedia Tools Appl.*, vol. 78, no. 10, pp. 13905–13924, 2019.
[47] Y. Guo, O. C. Au, R. Wang, L. Fang, and X. Cao, "Halftone image watermarking by content aware double-sided embedding error diffusion," *IEEE Trans. Image Process.*, vol. 27, no. 7, pp. 3387–3402, Jul. 2018.
[48] S. Sharma, "Detail and contrast enhancement in images using dithering and fusion," Western Sydney Univ., Sydney, NSW, Australia, Tech. Rep., 2018. [Online]. Available: http://hdl.handle.net/1959.7/uws:50866
[49] *CVG—UGR Image Database*. Accessed: Jul. 16, 2022. [Online]. Available: http://decsai.ugr.es/cvg/dbimagenes/g512.php
[50] *The Waterloo Fractal Coding and Analysis Group*. Accessed: Jul. 16, 2022. [Online]. Available: http://links.uwaterloo.ca/Repository.html
[51] A. Alzahrani and N. A. Memon, "Blind and robust watermarking scheme in hybrid domain for copyright protection of medical images," *IEEE Access*, vol. 9, pp. 113714–113734, 2021.
[52] J.-C. Yoo and T. H. Han, "Fast normalized cross-correlation," *Circuits, Syst. Signal Process.*, vol. 28, no. 6, pp. 819–843, Dec. 2009.
[53] *NCC Calculations on MATLAB*. Accessed: Jul. 16, 2022. [Online]. Available: https://www.mathworks.com/help/images/ref/normxcorr2.html
[54] S. Kumar and B. K. Singh, "An improved watermarking scheme for color image using alpha blending," *Multimedia Tools Appl.*, vol. 80, no. 9, pp. 13975–13999, Apr. 2021.
[55] S. Prasad and A. K. Pal, "A tamper detection suitable fragile watermarking scheme based on novel payload embedding strategy," *Multimedia Tools Appl.*, vol. 79, nos. 3–4, pp. 1673–1705, Jan. 2020.
[56] B. B. Haghighi, A. H. Taherinia, and A. Harati, "TRLH: Fragile and blind dual watermarking for image tamper detection and self-recovery based on lifting wavelet transform and halftoning technique," *J. Vis. Commun. Image Represent.*, vol. 50, pp. 49–64, Jan. 2018.
[57] F. A. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Attacks on copyright marking systems," in *Proc. Int. Workshop Inf. Hiding*. Berlin, Germany: Springer, 1998, pp. 218–238.
[58] C. Kumar, A. K. Singh, and P. Kumar, "A recent survey on image watermarking techniques and its application in e-governance," *Multimedia Tools Appl.*, vol. 77, no. 3, pp. 3597–3622, 2018.

SUNPREET SHARMA received the B.Eng. degree (Hons.) in computer systems engineering and the M.Sc. degree in mobile and satellite communications from London Metropolitan University, U.K., in 2014 and 2015, respectively, and the M.Phil. degree in computer engineering from Western Sydney University (WSU), Australia, where he is currently pursuing the Ph.D. degree. Moreover, he is also working as a Research Assistant (RA) to support the Robotic Automation in Greenhouse Pollination (RAGP) Project at WSU. His current research interests include multimedia watermarking, cybersecurity, machine learning, and image and signal processing.

JU JIA ZOU received the Ph.D. degree in digital image processing from the University of Sydney, Australia. He joined Western Sydney University, in 2003, where he is currently a Senior Lecturer. His current research interests include image processing, pattern recognition, computer vision, and their applications. Some of his research projects have been funded by the Australian Research Council and industry. He is an Associate Editor of *IET Image Processing*.



GU FANG (Member, IEEE) received the B.E. degree in mechanical automation from the Shanghai University of Technology, China, and the Ph.D. degree from The University of Sydney, Australia. He is currently a Professor of mechatronic engineering with Western Sydney University. He has co-edited two research books. He has published many refereed papers in book chapters, international journals, and conferences. His current research interests include robotics, computer vision, control systems, and artificial intelligence. He had many research grants from the Australian Research Council (ARC), the National Natural Science Foundation of China, and from industries. He had a Visiting Scholar appointments in UTS, Australia, and Shanghai Jiao Tong University, China. He is a regular referee for various international journals and conferences. He is a member of Engineers Australia.