Received: 20 October 2021 | Revised: 15 February 2022 | Accepted: 4 April 2022

IET Image Processing

DOI: 10.1049/ipr2.12542

The Institution of Engineering and Technology WILEY

ORIGINAL RESEARCH

A single watermark based scheme for both protection and authentication of identities

S. Sharma | J.J. Zou | G. Fang

School of Engineering, Design and Built Environment, Western Sydney University, Penrith, NSW, Australia

Correspondence
S. Sharma, School of Engineering, Design and Built Environment, Western Sydney University, Locked Bag 1797, Penrith 2751, NSW, Australia.
Email: sunpreet.sharma@westernsydney.edu.au

Abstract

The security of a watermarking scheme is mainly categorised as either robust or fragile. The former can withstand an authorised alteration/attack, primarily used in copyright protection. The latter follows a zero tolerance towards any modification, used primarily in content authentication processes. The existing literature in the field projects that two separate watermarks are required to make a watermarking scheme robust and fragile, thus making the overall process cumbersome and complex. A novel image watermarking scheme that uses only one watermark while achieving both goals of copyright protection and authentication of identities is presented. An unconventional concept of checkpointing is introduced, which equips the proposed scheme to be either robust or fragile, making it superior in its application versatility. First, watermark embedding within the host/original image is achieved by a combination of transform domain techniques along with a novel median-based embedding block selection procedure. Second, checkpointing is performed in the spatial domain. The watermarked image in the absence of an attack is correlated to the one that is being attacked, using the template energy comparison-based approach. In the case of the robust watermark, such checkpointing can establish whether the carried out attack is authorised or not, determining the successful recovery of the watermark or vice-versa. Moreover, in the case of the fragile watermark, a sole confirmation of the occurrence of an attack is sufficient to make the watermark recovery impossible. Finally, the experimental analysis of the proposed scheme illustrates its excellent performance and superiority over state-of-the-art methods within the field.

1 | INTRODUCTION

In this era of technology, as more people and businesses are transitioning towards being digital, safeguarding their identity is the prime focus of any information security system. This being said, the year 2020 presented several unprecedented scenarios as COVID-19 has reshaped both the personal and the professional lives of people across the globe. It has altered the way businesses/organisations operate as the use of physical office space(s) has declined dramatically, forcing them to run from online. Consequently, internet usage has maximised, and many online platforms such as Zoom™, Webex™ are in the limelight. Furthermore, social networks (SNs) activity has hiked as more people tune in to these avenues. These mediums are beneficial as they have made it possible to stay connected in these isolating times; however, their other side is not that captivating as hacking and cyber-crimes have also skyrocketed. The affects of such adversaries are felt worldwide; for instance, in May 2020, Zoom faced an alarming trend known as "Zoom bombing", in which intruders hijacked the live video sessions and created nuisance [1]. Subsequently, in June, the information systems of services New South Wales (NSW), Australia, were infiltrated and numerous sensitive documents were stolen. Consequently, almost a quarter of a million Australians' ended up losing their personal information in the form of driver's licences, handwritten signatures, marriage and birth certificates [2]. Last but not least, the severity of such attacks is evident when performed on the SNs; for instance, the facebook™ security breach at the beginning of 2020 impacted its 50 million users. These users had their email accounts compromised, pictures/images stolen and the same

goes for the twitter™ breach of July 2020 [3]. These are only a handful of snippets of the wide range of persisting cyber-attacks and thus, thwarting them is pivotal. Watermarking in this context is an effective and reliable tool, specifically for the platforms that use images/videos.

The watermarking process includes an addition of subtle information known as the "watermark" to a host signal (an image in this paper). The added watermark can successively be extracted/recovered to verify the host image's authenticity and copyright information [4]. A successful extraction validates the integrity of the host image. A watermarking scheme needs to address three main requirements [5]. First, the addition of the watermark to a host signal has to be imperceptible. This avoids any deformities that may be perceived by the human visual system (HVS). Second, the watermark needs to be secured against unauthorised modifications. Lastly, a watermarking scheme should have a healthy capacity, that is, its ability to embed large watermark(s). However, these three requirements are closely correlated and changing one of these can significantly affect the other. For instance, high capacity can improve security but degrades imperceptibility. Whereas the lower the capacity, the better the imperceptibility, the weaker the security. Thus, reaching a balance among these requirements is a significant challenge in the field of watermarking.

The security within watermarking is further sub-divided into two categories: robust and fragile [6]. The former can entertain a set of authorised modifications/attacks and is primarily used in copyright protection or similar applications. The latter is mainly used for authentication purposes as it simply opposes any modification. To achieve both goals of image authentication and copyright protection, two separate watermarks are being embedded in state-of-the-art methods. One is robust and the other fragile [7]. Notwithstanding the success of embedding multiple watermarks, the approach is prone to several limitations. First and foremost, as per the aforementioned discussion, embedding multiple watermarks can lead to a significant increase in capacity, thus, degrading the imperceptibility. Second, the addition of multiple watermarks is an uphill task, not preferred by the real-time applications. Finally, due to the increased capacity, the majority of these multipurpose techniques happen to be blind, thus, giving rise to security issues because in the blind watermarking technique, the original image is absent at the time of extraction. Such an absence makes it impossible to verify the extracted watermark against the original watermark. That is why the non-blind watermarking schemes are considered the most secured ones in the literature [5, 6, 8, 9]. To this end, this paper *aims* to present a non-blind watermarking scheme that uses only one watermark to achieve both goals of image authentication and copyright protection.

A watermarking scheme can be robust or fragile, depending on the requirement of the practical application for which it is about to be employed. The proposed method uses a novel concept of checkpointing (discussed in Section 3.3) that makes the proposed scheme adapt to the requirement of either being robust or fragile. This concept highlights the versatility of the proposed method, and an insight into its application background can be gained from the following examples. First, many artists today use social network (SN) platforms to showcase their art. Unfortunately, these platforms are also the primary source of information leaks, and according to Bertini et al. [10], only one out of 13 main SNs uses watermarking technology Before uploading an image of their work on a SN, artists can embed the electronic version of their art with a robust watermark. This means, if an artist comes across a stolen version of their work, they can alert the relevant SN, and prove the copyright of their work via the robust watermark. Ultimately, they can have the stolen version of their work removed from the internet. Second, sensitive data, such as medical and military images, are not to be altered as it can result in severe consequences. To keep the authenticity of such images intact, they are embedded with a fragile watermark that can easily be broken even by the slightest change. Subsequently, the intactness of these images can be verified during the extraction process (discussed in Section 3.2). To this effect, if the watermark is successfully extracted, an image is considered legitimate else, it is illegitimate. The application versatility of the proposed method is further highlighted as the discussion in this paper progresses

1.1 | Our contributions

The main contributions of the proposed scheme are listed below.

1. A novel median-based coefficient selection procedure in the frequency domain is proposed. This procedure is employed during the watermark embedding phase of this study (discussed in detail in the upcoming Section 3.1), wherein the carefully selected frequency coefficients are modified in equal proportions. To the best of the authors' knowledge, this is the first study wherein such a coefficient selection procedure is developed and employed. This procedure has two main benefits, as outlined below.

    It improves the watermark's imperceptibility. To this end, while operating on the greyscale images, the proposed watermarking is superior to existing state-of-the-art methods [5, 11–17] and also outperforms [18] and [19] while operating on the colour images.

    It improves the overall security attribute of the proposed scheme. The robustness of the watermark, embedded using the proposed novel median-based coefficient selection procedure, is tested against various geometrical and non-geometrical watermarking attacks (see [4] to gain an insight in the watermarking attacks). Its immunity is higher to such attacks than widely-cited methods [5, 11–20] in the field. Moreover, unlike most of the aforementioned existing watermarking techniques, the security evaluations of the proposed scheme are achieved using various watermarks of different dimensions, and the host images as small as 128×128 and as large as 2048×1152 in pixel resolution, respectively.

TABLE 1 Summary and comparison of related works

Method	Watermark (s)	Colour map	Technique (s)	Copyright protection	Authentication	Security	Imperceptibility	Capacity
Sharma et al. [5]	1	Greyscale	DWT	✓	×	High	High	Medium
Hurrah et al. [11]	2	Colour+Greyscale	DWT+DCT	✓	✓	High	Medium	High
Kang et al. [12]	1	Greyscale	DWT+DCT+SVD	✓	×	High	Low	Low
Verma et al. [13]	1	Greyscale	DWT	✓	×	HIgh	Medium	Low
Islam et al. [14]	1	Greyscale	DWT+SVM	✓	×	High	Medium	Low
Barr et al. [18]	2	Colour	DWT	✓	×	Lowest	Lowest	Lowest
Loan et al. [15]	2	Colour+Greyscale	DWT+DCT	✓	✓	High	Medium	**Highest**
Singh et al. [29]	2	Colour	DWT+DCT+BPNN	✓	×	Medium	Low	High
Kamili et al. [19]	2	Colour	DWT+DCT	✓	✓	High	Medium	High
Hurrah et al. [16]	1	Greyscale	DWT	✓	✓	High	High	High
Kang et al. [17]	1	Greyscale	DWT+DCT+SVD	✓	×	High	Medium	Low
Proposed	1	Colour+Greyscale	DWT+DCT	✓	✓	**Highest**	**Highest**	High

2. A novel concept that works in the spatial domain, which is termed by the authors as *checkpointing*, is introduced. The main benefit of this concept is that it empowers the proposed watermarking scheme to be adaptable to the requirement of being either robust or fragile. To the best of the authors' knowledge, checkpointing is the first of its kind concept that uses only one watermark to achieve both copyright protection and authentication goals. More details on checkpointing can be found in Section 3.3.

The rest of this paper is organised as follows. Section 2 covers state-of-the-art literature in the field. Section 3 is dedicated to the proposed methodology. Section 4 covers the experimental results and finally, Section 5 is the conclusion.

2 | RELATED WORK

The term "Digital Watermarking" had its dawn in 1992 and since then it has been an active topic of research [21]. Its applications are continuously branching out to new advents in technology; for example, the process of watermarking a neural network is known as "passporting" [22, 23], security in cloud storage systems [24, 25], electronic money transfers, e-governance [26]. However, the use of watermarking for purposes of copyright protection and authentication has always been a key focus ever since its arrival [27, 28], thus is also the focus of this discussion. The state-of-the-art methods that have influenced the proposed scheme are discussed and summarised in this section and Table 1, respectively.

A discrete wavelet transform (DWT) coefficient difference-based watermarking approach was developed by Lin et al. in [30]. Their technique is extensively used and embraced by many later works such as [13, 14]. Although their method successfully achieved very high imperceptibility with moderate capacity, it struggled from the security aspect [31]. The strategy of embedding multiple watermarks rectified this shortfall and is currently being used in identity (ID) protection or similar applications [18, 32, 33]. Lu and Liao pioneered the idea of multipurpose watermarking that achieved both authentication and copyright protection [34]. They successfully used DWT for embedding two separate watermarks to make their scheme both robust and fragile. Their method was only applicable to greyscale images and suffered from the tamper localisation issues, rectified by Liu et al. through a dual watermarking scheme on colour images [7]. They employed DWT in YC_bC_r colour model, where Y, C_b and C_r are luminance, chrominance blue and chrominance red channels of a colour image, respectively. Subsequently, they used Y channel for robust watermark embedding in the transform domain and manipulated the least significant bits (LSB) for fragile watermark insertion in the spatial domain. Disadvantages associated with methods that are solely based on DWT are restricted if not nullified by pairing them with other techniques such as discrete cosine transform (DCT), singular value decomposition (SVD), support vector machine (SVM) and back propagation neural network (BPNN) [11, 12, 15, 20, 29, 35]. Moreover, these hybrid methods have their own flaws. For instance, BPNN or any other machine/learning-based technique initially requires intense computation power, data collection and training, making such methods expensive in terms of resource and processing time. Hence, integrating multiple processes into one is a cumbersome task. In addition to its fast processing ability and application simplicity, the main merit of DCT-based watermarking methods is their resilience to the image compression attack method, one of the most effective and widely used attacks [35, 36].

Hurrah et al. presented a dual watermarking framework for privacy protection and multimedia content authentication in [11]. Their method is employable across different colour spaces: greyscale and *RGB* (red-blue-green channels). Subsequently, they used DWT-DCT based embedding scheme along with Arnold transform-based encryption key. Their work motivated Kamili et al., who have recently proposed DWFCAT: a watermarking strategy for colour images. Unlike [11], DWFCAT

employs YC_bC_r colour-space. It exploits the energy compaction property of DCT coefficients for robust watermark embedding and fast processing is achieved by embedding fragile watermark bits in the spatial domain [19]. Their technique employs chaotic and deoxyribonucleic acid (DNA) encryption keys as a measure to ensure extra security. Although Kamili et al.'s method has high capacity, it under-performed in peak-signal-to-noise-ratio (PSNR) values. Subsequently, Hurrah et al. successfully proposed another dual watermarking strategy in [37], through which they were able to surpass the PSNR values attained by their preceding method in [11] and Kamili et al.'s method.

The methods mentioned above motivate the proposed approach to use both DWT and DCT for the watermark embedding. Their combination leads to better imperceptibility and security; however, the proposed method is also outstanding in the following aspects. First, the majority of these aforementioned methods use at least two if not more encryption keys. This not only adds to the implementation complexity but also makes the whole process time-consuming. In contrast, the proposed method uses only one encryption key (discussed in detail in the upcoming section). Second, a dual watermarking technique can be tedious as it performs twice the watermark embedding and extraction procedures. The proposed method eradicates this issue as it uses only one watermark to achieve both copyright protection and media authentication goals. Finally, in addition to using both DWT and DCT, the proposed watermark embedding incorporates a novel median-based embedding block selection procedure. This block selection procedure is adaptive, thus, eliminates any errors that may occur in manual thresholding. The rest of the proposed methodology is covered in the following section.

3 | METHODOLOGY

An overview of the proposed method is given in Figure 1, in which the original image is divided into multiple frequency subbands through DWT. Note, the proposed scheme can be applied to both greyscale and colour images; for simplicity, discussion in this section is done by employing the greyscale colour-space. A separate subsection that presents the application on the colour images is dedicated to this paper's latter part.

Precisely, the DWT of an image yields four frequency subbands, which are termed and represented in Figure 1 as *LL* (Low-Low), *LH* (Low-High), *HL* (High-Low) and *HH* (High-High). 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. 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 unfit for embedding. Moreover, our previous works in [5, 9] are positively influenced by the literature in [13, 14, 30]. They tend to use the *LH* (represented by solid blue in Figure 2) subband for the watermark embedding due to its ability to limit the flaws above, linked with *LL* and *HH* subbands.

TABLE 2 Default image sizes accepted by SNs

Index	SN	Pixel resolution
1	Facebook	2048 × 1152
2	Flickr	2048 × 1152
3	Google+	2048 × 1152
4	Instagram	1080 × 1080
5	LinkedIn	2048 × 1152
6	Pinterest	2048 × 1152
7	Telegram	1280 × 720
8	Tumblr	1280 × 720
9	Twitter	2048 × 1152
10	Viber	1280 × 720
11	VK	2560 × 1440
12	WeChat	1280 × 720
13	WhatsApp	1600 × 1200

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 [38, 39] to gain an insight on the MRA).

Notwithstanding the success of these methods in their application simplicity and faster processing, it is well-known that the MRA, specifically at levels higher than three, can lead to a number of issues, such as, aliasing which could be detrimental during the image reconstruction process and ultimately sacrifice the imperceptibility of the watermarked image. Further investigations by Thien et al. in [40–42] have highlighted that as the DWT level increases, the subband size decreases, and so is the watermark capacity. Therefore, it is recommended that utilising both *LH* and *HL* (represented by solid yellow in Figure 2) subbands is optimal in the embedding process. Additionally, it is suggested that as *LH* and *HL* are symmetrical in nature, therefore, while embedding a binary watermark, black (0) and white (1) bits can be evenly split amongst these two subbands. Consequently, it makes the watermark more resilient against several attacks such as the low-pass and high-pass filtering, rotation, scaling, translation while being high in capacity and imperceptibility. Convinced by these justifications, the proposed method uses both *LH* and *LH* subbands in the embedding process. Moreover, a thorough discussion on the watermark embedding in each of these subbands and their behaviour is covered by Islam et al. in [14].

Note, the default image dimensions/size accepted by 13 prominent SNs, recently studied by Bertini et al. in [10], are given in Table 2. This table shows that all of these SNs are defaulted to accept an image with dimensions in the power of two. Bertini et al. have also addressed that these SNs when presented with an image, consisting of an odd number of either rows or columns or both, perform a resizing operation that aligns the given image to its nearest power of two, thus, making it acceptable. The proposed method in this paper follows the same trajectory. Furthermore, such resizing is also essential to

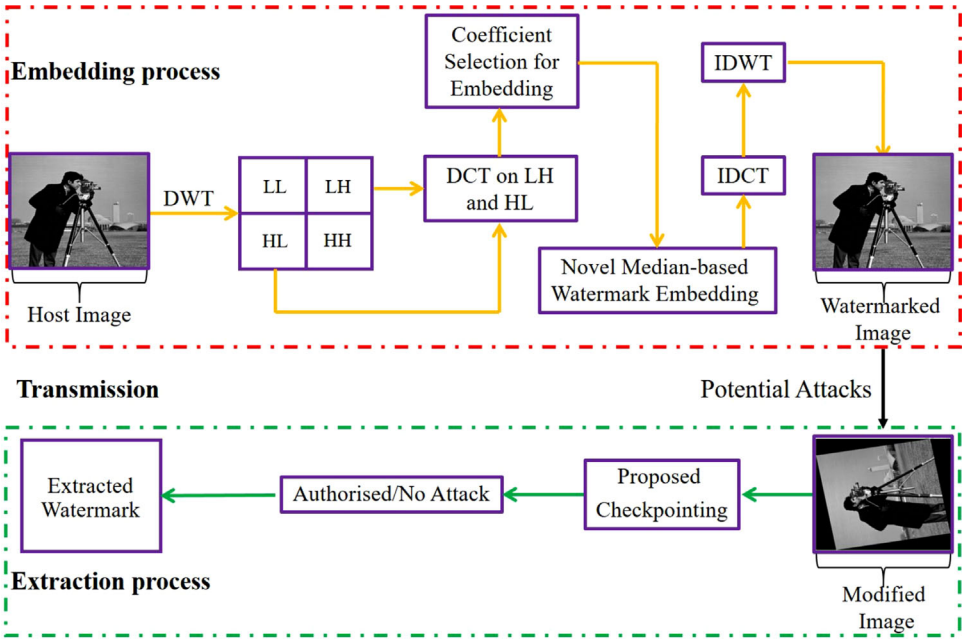

FIGURE 1 Blueprint of the proposed method. The yellow arrows represent steps within the embedding phase and the green arrows are for the extraction process

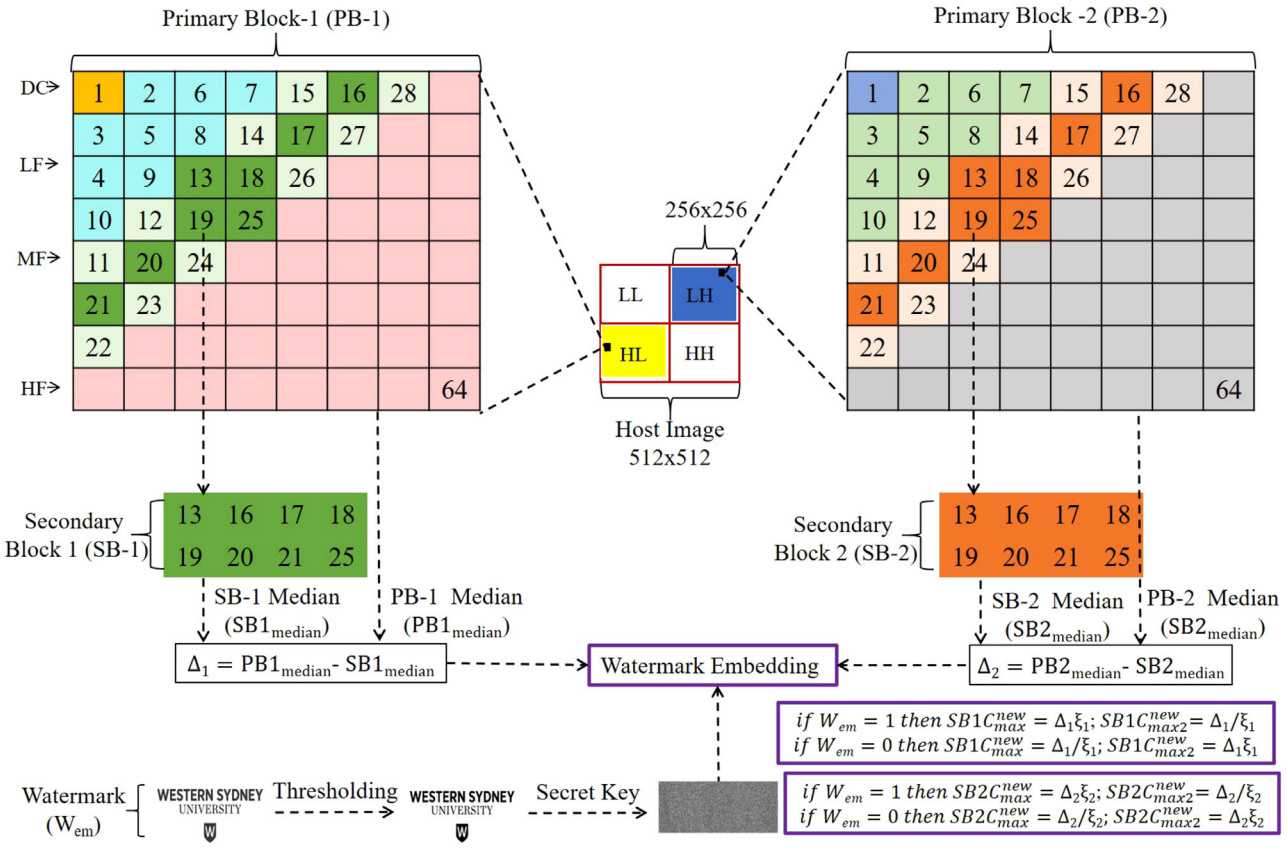

FIGURE 2 The proposed watermark embedding process. Digits within Primary Blocks (PB-1 and PB-2) are the numbers allocated to DCT coefficients, where DC being the lowest frequency component is labelled as 1 and 64 is dedicated to the highest frequency component

carry forward a DWT operation as it yields frequency subbands that are even in size. Subsequent steps shown in Figure 1 are discussed in the upcoming subsections, covering the proposed watermark embedding and extraction, respectively.

3.1 | Watermark embedding

A breakdown of the proposed embedding strategy is provided in Figure 2. First, the host image of size $m \times n$ (*rows*×*columns*) is decomposed into frequency subbands using DWT. The proposed method is fully able to handle images with pixel resolutions mentioned in Table 2; however, for the sake of explanation simplicity, the rest of the proposed method is elaborated by considering a host image of dimensions 512×512 in pixels. Second, *LH* and *HL* subbands, composed of the DWT coefficients and each having 256×256 pixels 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 a primary block that is termed "Primary Block" in Figure 2. Moreover, the primary block associated with the *HL* subbands is labelled as "Primary Block-1" (PB-1), whereas the one related to the *LH* block is labelled as "Primary Block-2" (PB-2). A magnified illustration of these primary blocks is presented in Figure 2. 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 2). In this paper, MF coefficients are selected for the watermark embedding as these coefficients, unlike their counterparts (LF and HF coefficients), allow alterations while maintaining a harmonious balance between imperceptibility and robustness. Furthermore, a full account on the behaviour of DCT coefficients can be found in [36]. Similar to [12], a "Secondary Block" (SB), is constructed by eight of the total MF coefficients in a primary block; their allocated position numbers in Figure 2 are $13, 16-21, 25$. The secondary block contained within PB-1 is termed as SB-1 and the one within PB-2 is labelled as SB-2. Third, the individual median values of PB-1 and PB-2 are calculated and successively, tagged as $PB1_{median}$ (Primary Block-1 Median) and $PB2_{median}$ (Primary Block-2 Median) and so are the medians of secondary blocks with $SB1_{median}$ (Secondary Block-1 Median) and $SB2_{median}$ (Secondary Block-2 Median). Thereafter, the difference between $PB1_{median}$ and $SB1_{median}$ is calculated and depicted as Δ_1. Similarly, the difference between $PB2_{median}$ and $SB2_{median}$ is docketed as Δ_2. Figure 3 provides the pictorial representation of median calculations and literature in [15] and [43] provides further insight on these median estimations.

Subsequently, the watermark (W_1) is prepared by a series of steps, as shown in Figure 2. The first step is thresholding the watermark to a pixel value of 128. It yields its binary equivalent and limits it to 0 (Black) and 255 (White) in values, referred to as 0 and 1 in binary. Second, the secret key is used to scramble the binary watermark. Such a secret key is vital during the transmission of the watermarked image because this very key is employed at the time of its validation, achieved via watermark extraction (discussed later in this paper). Due to its robust performance and state-of-the-art usage, the Fisher-Yates shuffle algorithm is employed in this paper to achieve watermark scrambling (see [13, 44, 45] to gain further insight on this shuffling algorithm). Once the watermark is prepared and values of Δ_1 and Δ_2 are calculated, the maximum ($SB1C_{max}$) and second-maximum ($SB1C_{max2}$) valued coefficients within a secondary block, SB-1 are modified to meet the following criterion.

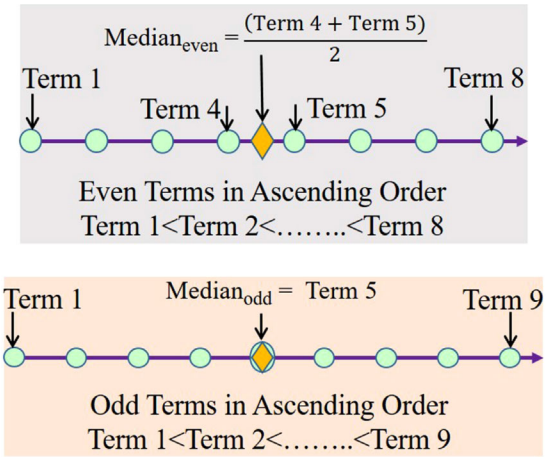

FIGURE 3 Median value calculations

If the watermark bit to be embedded (W_{em}) in the SB-1 is 1, then,

$$\begin{aligned} SB1C_{max} &= SB1C^{new}_{max} = \Delta_1 \xi_1 \\ SB1C_{max2} &= SB1C^{new}_{max2} = \Delta_1 / \xi_1 \end{aligned}, \tag{1}$$

and if it is 0, then,

$$\begin{aligned} SB1C_{max} &= SB1C^{new}_{max} = \Delta_1 / \xi_1 \\ SB1C_{max2} &= SB1C^{new}_{max2} = \Delta_1 \xi_1 \end{aligned}, \tag{2}$$

where ξ_1 stands for the average median value of selected SB-1 blocks from the total SB-1 blocks. ξ_1 is calculated as per Equation 3 in which $\lfloor . \rfloor$ or anywhere else in this paper stands for the floor function. Similarly, M_b stands for the aforementioned selected SB-1 blocks, selected as per Figure 4.

$$\xi_1 = \left\lfloor \frac{\sum_{i=1}^{M_b} SB1^i_{median}}{M_b} \right\rfloor. \tag{3}$$

Likewise, in the case of embedding in the secondary block, SB-2, Equations (1) and (2) can be rewritten as Equations (4) and (5), respectively. If the watermark bit to be embedded (W_{em})

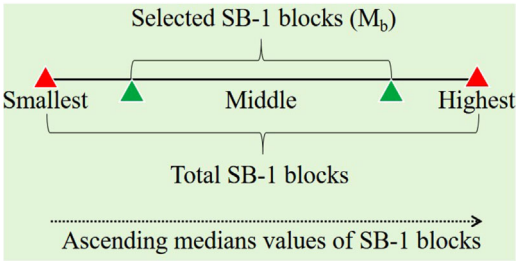

FIGURE 4 Block selection procedure. The selected SB-1 blocks are between the green labels

in the SB-2 is 1, then,

$$\begin{aligned} SB2C_{max} &= SB2C^{new}_{max} = \Delta_2\xi_2 \\ SB2C_{max2} &= SB2C^{new}_{max2} = \Delta_2/\xi_2 \end{aligned}, \tag{4}$$

and if it is 0, then,

$$\begin{aligned} SB2C_{max} &= SB2C^{new}_{max} = \Delta_2/\xi_2 \\ SB2C_{max2} &= SB2C^{new}_{max2} = \Delta_2\xi_2 \end{aligned}, \tag{5}$$

with ξ_2 as the average median value of selected SB-2 blocks from the total SB-2 blocks. ξ_2 is calculated as per Equation 6, where N_b stands for the aforementioned selected SB-2 blocks, calculated in the same way as M_b in Figure 4.

$$\xi_2 = \left\lfloor \frac{\sum_{i=1}^{N_b} SB2^i_{median}}{N_b} \right\rfloor. \tag{6}$$

The main advantage of the proposed embedding strategy (represented by the purple boundaries in Figure 2) 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 unwanted 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 ξ the other coefficient must be scaled down by the same factor. Consequently, the median values of primary blocks, PB-1 and PB-2 are kept intact and so is the overall imperceptibility. Furthermore, any unauthorised change would cause a shift in the median values that can degrade the appearance of the transmitted watermarked image, confirming a security breach.

Finally, the steps above are carried out on the rest of the selected 8x8 blocks within *LH* and *HL* subbands and as a result, the watermark embedding culminates, and so is the overall embedding process. The proposed embedding process can be quantized in the form of Equation (7).

$$WI_{Final} = HI_{Original}(1 + \beta W_{Total}); \tag{7}$$

ALGORITHM 1 The proposed watermark extraction process.

Input: The original host image ($HI_{Original}$), the final watermarked image (WI_{Final}) and the embedding strength factor (β).

Output: The employed watermark (W_{em}).

Step 1: Apply 1-level DWT on $HI_{Original}$, extract its *LH* and *HL* subbands: $LH_{Original}$ and $HL_{Original}$, respectively.

Step 2: Apply 1-level DWT on WI_{Final}, extract its *LH* and *HL* subbands: LH_{Final} and HL_{Final}, respectively.

Step 3: Apply DCT on $LH_{Original}$ and $HL_{Original}$: $LH^{DCT}_{Original}$ and $HL^{DCT}_{Original}$, respectively.

Step 4: Apply DCT on LH_{Final} and HL_{Final} : LH^{DCT}_{Final} and HL^{DCT}_{Final}, respectively.

Step 5: Compute the following:

$$W_1 = \frac{LH^{DCT}_{Final} - LH^{DCT}_{Original}}{\beta LH^{DCT}_{Original}};$$

$$W_2 = \frac{HL^{DCT}_{Final} - HL^{DCT}_{Original}}{\beta HL^{DCT}_{Original}}.$$

Step 6: $W_{Scrambled}$ is extracted by concatenating (++) W_1 and W_2 as following:

$$W_{Scrambled} = W_1 ++ W_2.$$

Step 7: Execute the inverse of DCT and DWT.

Step 8: Unscramble $W_{Scrambled}$ by applying the secret key's inverse and extract the employed watermark (W_{em}).

where WI_{Final}, $HI_{Original}$, W_{Total} and β stand for the final watermarked image, the original/host image, the total watermark embedded and the watermark strength/scaling parameter, respectively. The range of β is (0 1] that also specifies the watermark's visibility. To this end, an obvious watermark is represented by '1' and vice-versa [8]. It is established empirically that the proposed scheme yields the best results when β is between [0.03–0.06]. Similar to [13] and [14], β equal to 0.04 is chosen for the experimental simulations in this paper.

3.2 | Watermark extraction

The non-blind watermarking requires the host and the watermarked signals at the time of extraction. Such extraction within the spatial domain can be achieved by using Equation (8). Note, as the proposed embedding strategy is implemented in the frequency domain, the relevant extraction process can therefore only be executed in the frequency domain. A step-by-step breakdown of the employed extraction process in the frequency domain is provided in Algorithm 1. It is essential to realise that Equation (8) only outputs the watermark(s) in a scrambled state. To this end, unscrambling the watermark is the final step, achieved by executing the inverse of the aforementioned secret

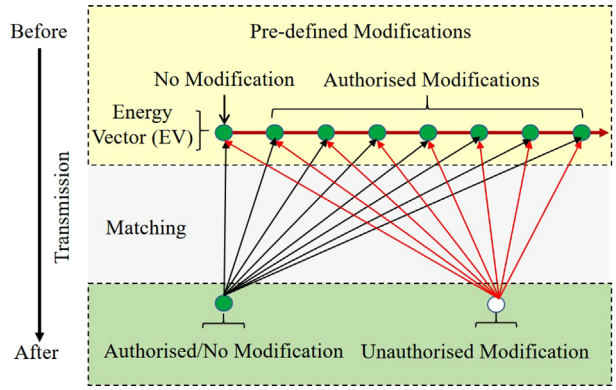

FIGURE 5 The proposed checkpointing operation. The red arrows show a mismatch due to unequal energy values, whereas, the black arrows show a match and equal energy values. Note, all values within EV are sorted in an ascending order, a prerequisite for the binary search

key [13, 14].

$$W_{Total} = \frac{WI_{Final} - HI_{Original}}{\beta HI_{Original}}. \tag{8}$$

Note, the given extraction process is only feasible once the validity of the watermarked image is assured. It is achieved through the process of checkpointing that is discussed in the upcoming subsection.

3.3 | Checkpointing

An overview of the proposed checkpointing is presented in Figure 5.

In this process, the energy of the watermarked image before transmission is computed under various scenarios, such as, in the absence of an attack and under an authorised attack(s). Equation (9) contains the general formulation of the adopted energy calculations, where WI stands for the watermarked image, $B \times H$ in size,

$$Energy = \sum_{i=1}^{B} \sum_{j=1}^{H} WI_{i,j}. \tag{9}$$

Once calculated, these energy values are stored in the form of a vector, depicted as the "Energy Vector" (EV) in Figure 5. In this process, EV can be perceived as a dictionary, which comprises all modifications authorised by an individual or an organisation for a watermarked image. After transmission, once the watermarked image is received at the receiver's end, it is successively matched against these predefined modifications stored within EV. Matching in the proposed method follows the principle of the binary search, covered extensively in [46, 47]. Apart from its precision in searching for the required element, the main advantage of binary search is its ability to save the processing time (discussed later in detail in the processing time analysis section). A successful match initiates the extraction process given in Equation (8), validating the watermarked image and vice versa. Note, the proposed checkpointing process varies in robust watermarking from its fragile counterpart, discussed below.

3.3.1 | Robust and fragile checkpointing

In robust watermarking, the watermarked image before (WI_{Before}) and after transmission (WI_{After}) is matched using Equation (10).

$$WI_{After} = \begin{cases} WI_{Before}, & if\ Energy(WI_{Before} = WI_{After}) \in EV \\ Error, & otherwise. \end{cases} \tag{10}$$

$Energy(WI_{Before})$ and $Energy(WI_{After})$ in Equation (10) are energies associated with the watermarked image, before and after transmission, respectively. Equation (10) shows that WI_{After} and WI_{Before} are the same if and only if they share the common energy value, which is also present within EV. This confirms the authenticity and extracts the robust watermark, else an error message is displayed by the proposed method.

In fragile watermarking as there is no room for modifications, thus, WI_{After} and WI_{Before} are considered as same if their energy values are equal and identical to only one element in EV, shown as "No Modification" in Figure 5. Subsequently, its matching criteria are given in Equation (11). The fulfillment of criteria in Equation (11), leads to an extraction of the fragile watermark, else an error message is displayed.

$$WI_{After} = \begin{cases} WI_{Before}, & if\ Energy(WI_{Before} = WI_{After}) = EV_{No\ Modification} \\ Error, & otherwise. \end{cases} \tag{11}$$

3.4 | Application to colour images

The proposed methodology can effortlessly be applied to colour images. There are various models in which a colour image can be represented; however, as discussed earlier in the literature review section, RGB and YC_bC_r are the prominent models used in watermarking of colour images. Each of these colour models has its pros and cons; for instance, YC_bC_r model is compression friendly but limited in embedding capacity, as Y is the only channel used for watermark embedding. On its flip side, RGB model is high in capacity but not preferable when an application requires image compression [48]. This being said, choosing a colour model is entirely subject to the application by which it is about to be employed. Tan et al. [49] and Roy et al. [48] are among a few researchers working towards further improvising these colour spaces. For instance, their studies use both Y and C_b channels for embedding watermark(s), thereby improving the balance between the watermark imperceptibility and security. Notwithstanding the merits of their work, they

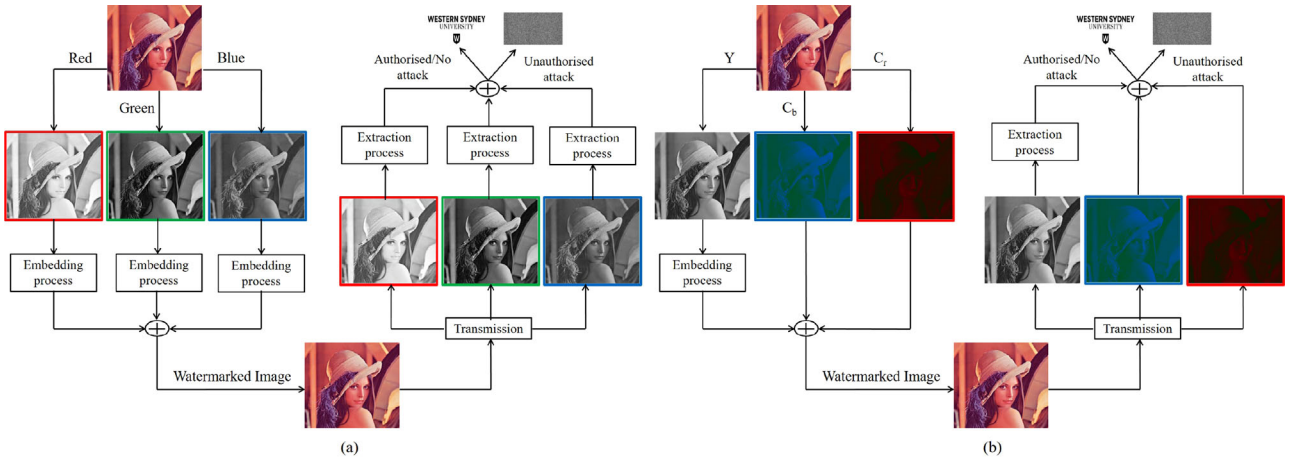

FIGURE 6 Application of the proposed method to colour images. (a): Represents the *RGB* model and (b): Represents the YC_bC_r model

did not expand their embedding strategies from YC_bC_r to the *RGB*, thus lacking a comparison between the former and the latter. To this end and similar to methods in [11, 15], the proposed method is outstretched to both YC_bC_r and *RGB* models. This is not only necessary to gain a fair compression between the proposed method and others but also shows its operational versatility and adaptability.

The *RGB* model is shown in Figure 6a, in which a colour host image is split into *R*, *G* and *B* channels. Each of these channels is a greyscale equivalent with pixel values between [0–255]. Thereafter, these channels are individually watermarked using the same embedding strategy presented within the aforementioned section on watermark embedding. Note, the proposed watermark embedding manipulates each of these channels in equal proportions. Such manipulation keeps the inter-channel correlation intact: vital for maintaining the imperceptibility. An insight on the inter-channel correlation of an *RGB* model and other colour models is provided by Su et al. in [50]. Once watermarked, these channels are concatenated to produce the final watermarked image. Subsequently, steps involved in the extraction process are similar to the ones discussed earlier in the watermark extraction section, the only exception is that in the *RGB* model, the extraction process is performed across three colour channels. Although the availability of three separate channels for embedding facilitates the *RGB* model's high capacity attribute, the same also contributes to its main set back of prolonged processing time. Note, the time complexity is covered in the upcoming section on the processing time analysis. This time complexity issue can be eradicated by using the YC_bC_r model given in Figure 6b.

In the YC_bC_r model, a colour host image is divided into a luminance and two chrominance channels. The luminance channel is equivalent to a greyscale scale image, an appropriate candidate for the proposed watermark embedding. Once watermarked, the luminance channel is concatenated with chrominance channels and a colour watermarked image is achieved. Subsequently, the inserted watermark can be extracted at the receiver's end by splitting the watermarked image and performing the aforementioned extraction process on the luminance channel. The overall approach in YC_bC_r model is streamlined as traditionally it is limited to one channel instead of three channels employed by its counterpart *RGB* model.

FIGURE 7 Test images (publicly available at [51] and [52]) and a variety of watermarks used for illustrations in this paper. Best viewed when zoomed in

4 | EXPERIMENTAL RESULTS

The versatility of the proposed scheme is tested on 200 images. Datasets used are publicly available at [51] and [52].

The first three rows of Figure 7 show 15 examples of the total test image and the last two shows a variety of watermarks, all of which are used in simulations. Experiments are carried out using MATLAB (R2021a) on a machine with Intel™ i7-8650U CPU running at 1.9 GHz, 16 GB RAM and 64-bit operating system.

TABLE 3 Imperceptibility and capacity analysis. The PSNR values are in decibels (dB) and the capacity is measured in the total number of bits, which can be embedded within the host image. Note, the employed test images are *Lenna* and *Lenna_colour*, each of which is 512 × 512 in size. "N/A" in this table or at any other instance in this discussion stands for "Not Available"

Methods ↓		Imperceptibility (PSNR)			Maximum capacity (in bits)	
Colour-space →	Watermark type and size	Greyscale	YC_bC_r	*RGB*	Greyscale|YC_bC_r	*RGB*
Sharma et al. [5]	DICTA: 32 × 16	44.1	N/A	N/A	2048|N/A	N/A
Proposed		47.2	46.1	45.2	4096	12288
Hurrah et al. [11]	UOK: 64 × 64	40.45	N/A	43.28	4096	12288
Proposed		45.6	44.7	43.4	4096	12288
Kang et al. [12]	Xi'an: 32 × 32	40.07	N/A	N/A	1024|N/A	N/A
Proposed		46.8	45.7	44.8	4096	12288
Verma et al. [13]	CSIE: 32 × 16	41.89	N/A	N/A	1024|N/A	N/A
Proposed		47.4	46.3	45.4	4096	12288
Islam et al. [14]	Crown: 32 × 16	42.95	N/A	N/A	1024|N/A	N/A
Proposed		46.9	46.1	45.3	4096	12288
Barr et al. [18]	TEST: 50 × 20	N/A	N/A	37.24	1210|N/A	N/A
Proposed		47.4	46.3	45.7	4096	12288
Loan et al. [15]	UOK: 64 × 64	42.65	41.24	42.54	4096	12288
Proposed		45.6	44.7	43.4	4096	12288
Singh et al. [20]	CM_WM: 128 × 128	52.34	N/A	N/A	16384|N/A	N/A
Proposed		47.1	45.9	44.7	4096	12288
Kamili et al. [19]	UOK: 64 × 64	N/A	42.44	N/A	N/A|8192	N/A
Proposed		45.6	44.7	43.4	4096	12288
Hurrah et al. [16]	UOK: 64 × 64	42.69	41.29	N/A	4096	N/A
Proposed		45.6	44.7	43.4	4096	12288
Kang et al. [17]	Print: 32 × 32	41.97	N/A	N/A	1024|N/A	N/A
Proposed		46.5	45.9	45.1	4096	12288

Note, the experimental analysis presented in this paper is conducted on images as small as 128x128 and as large as 2048x1152 in pixel resolution. Statistically, the experimental simulations were run 25 times using the machine above. The proposed watermarking scheme is stable and achieves confidence of 98% in PSNR and normalised cross-correlation (NCC) values. In terms of execution, the proposed method works 100% in watermark embedding and checkpointing, respectively.

4.1 | Performance matrices and baseline

A quantitative evaluation of the proposed method in terms of imperceptibility and capacity is contained in Table 3 and Figure 9. Subsequently, Tables 4 and 5 present the security analysis. The former is for the watermark robustness and compares the effect of various attacks on watermarked images achieved by the proposed method and other state-of-the-art methods. The latter covers the watermark fragility and shows the watermark's sensitivity towards various modifications. The imperceptibility is measured in decibels (dB) through PSNR given by Equation (12). A high PSNR value indicates high imperceptibility.

$$PSNR = 10\log_{10}\frac{(255)^2 wh}{\sum_{i=1}^{w}\sum_{j=1}^{h}(x[i,j]-y[i,j])^2}, \quad (12)$$

where w and h stand for the width and height of an image. Furthermore, $x(i,j)$ and $y(i,j)$ indicate pixel values of the host image and the watermarked image produced due to the proposed watermark embedding, respectively. Subsequently, the security of the proposed method is tested using NCC given by Equation (13), where W and W' stand for the original and the extracted watermarks of dimensions $P \times Q$, respectively.

$$NCC = \frac{\sum_{i=1}^{P}\sum_{j=1}^{Q}(W[i,j]\times W'[i,j])}{\sqrt{\sum_{i=1}^{P}\sum_{j=1}^{Q}(W^2[i,j])}\times\sqrt{\sum_{i=1}^{P}\sum_{j=1}^{Q}(W'^2[i,j])}}. \quad (13)$$

Note, sometimes in the literature, the NCC is also addressed as NC, and for consistency's sake, the former is adopted throughout this discussion. The NCC values should range

TABLE 4 Robustness comparison with state-of-the-art methods. Note, the employed test image is *Lenna*, which is 512 × 512 in size. The only exception is Barr et al.'s method [18], as it has used *Lenna_colour* as the host image and so does the proposed method, while comparing the two. "N/A" in this table or at any other instance in this discussion stands for "Not Available"

Watermark →	**TEST: 50 × 20**		**UOK: 64 × 64**			
Attacks ↓ | Method →	**Barr et al. [18]**	**Proposed**	**Hurrah et al. [11]**	**Loan et al. [15]**	**Hurrah et al. [16]**	**Proposed**
Attack-free	1.0	1.0	1.0	1.0	1.0	1.0
Rotation 10°	N/A	0.954	0.94	0.953	**0.98**	**0.98**
Rotation 45°	0.93	**0.967**	0.966	0.96	0.978	**0.98**
Gamma correction ($\gamma = 0.50$)	N/A	0.967	N/A	N/A	**1.0**	0.96
Scaling (50%)	**0.9**	0.881	**0.99**	0.987	**0.99**	**0.99**
Compression (QF= 50)	N/A	0.976	0.944	N/A	0.9821	**0.991**
Compression (QF= 60)	N/A	0.979	0.967	**1.0**	0.9981	0.996
Compression (QF= 90)	N/A	0.984	**1.0**	**1.0**	**1.0**	**1.0**
Watermark →	**CSIE: 32 × 16**		**Crown: 32 × 16**		**DICTA: 32 × 16**	
Attacks ↓ | Method →	**Verma et al. [13]**	**Proposed**	**Islam et al. [14]**	**Proposed**	**Sharma et al. [5]**	**Proposed**
Attack-free	1.0	1.0	1.0	1.0	1.0	1.0
Compression (QF= 20)	0.94	**0.978**	0.943	**0.981**	0.959	**0.982**
Compression (QF= 30)	**0.99**	0.976	0.9424	**0.986**	0.976	**0.996**
Compression (QF= 40)	**1.0**	0.985	0.9591	**0.992**	0.987	**0.991**
Compression (QF= 50)	**1.0**	0.991	0.9640	**0.995**	0.991	**0.993**
Scaling (50%)	0.98	**0.984**	N/A	0.972	0.962	**0.977**
Scaling (75%)	N/A	0.952	**0.9851**	0.979	**0.975**	0.968
Watermark →	**Xi'an: 32 × 32**		**Print: 32 × 32**		**WSU: 64 × 64**	
Attacks ↓ | Method →	**Kang et al. [12]**	**Proposed**	**Kang et al. [17]**	**Proposed**	**Proposed**	
Attack-free	1.0	1.0	1.0	1.0	1.0	
Compression (QF= 10)	0.8382	**0.886**	0.6920	**0.873**	0.926	
Compression (QF= 20)	0.8502	**0.913**	0.7320	**0.922**	0.941	
Compression (QF= 30)	0.8867	**0.942**	0.8444	**0.954**	0.978	
Compression (QF= 50)	0.9449	**0.977**	**0.9371**	0.936	0.99	
Compression (QF= 70)	0.9859	**0.991**	**0.9883**	0.962	1.0	
Rotation 45°	N/A	0.989	N/A	0.984	0.986	
Gamma correction ($\gamma = 0.50$)	N/A	0.985	N/A	0.981	0.98	
JPEG2000 compression (CR= 2)	**0.998**	0.991	**0.998**	0.998	0.999	
JPEG2000 compression (CR= 4)	**0.989**	**0.989**	0.976	**0.981**	0.986	
JPEG2000 compression (CR= 8)	**0.949**	0.946	**0.969**	0.962	0.9801	

between [0 1], with '0' being the least in similarity and '1' being the highest. Further insight on the NCC and its theoretical basis can be gained from [53, 54]. 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 [5, 11–20], which are also chosen for comparison in this work.

The watermark extraction error is a factor of the watermark embedding strength factor (β), also known as the scaling factor and the type of watermarking attack. Overall, the extraction process is stable with a maximum error rate of 0.14%, illustrated by Figure 8. The error rate is calculated as the bit-error-rate (BER), using Equation (14);

$$BER = \left(\frac{\sum_{i=1}^{P} \sum_{j=1}^{Q} [(W[i,j] - W'[i,j])^2]}{P \times Q} \right) \times 100. \quad (14)$$

The BER value lies between 0 and 1. The watermark extraction is considered perfect if the BER is '0'. In such a case, the

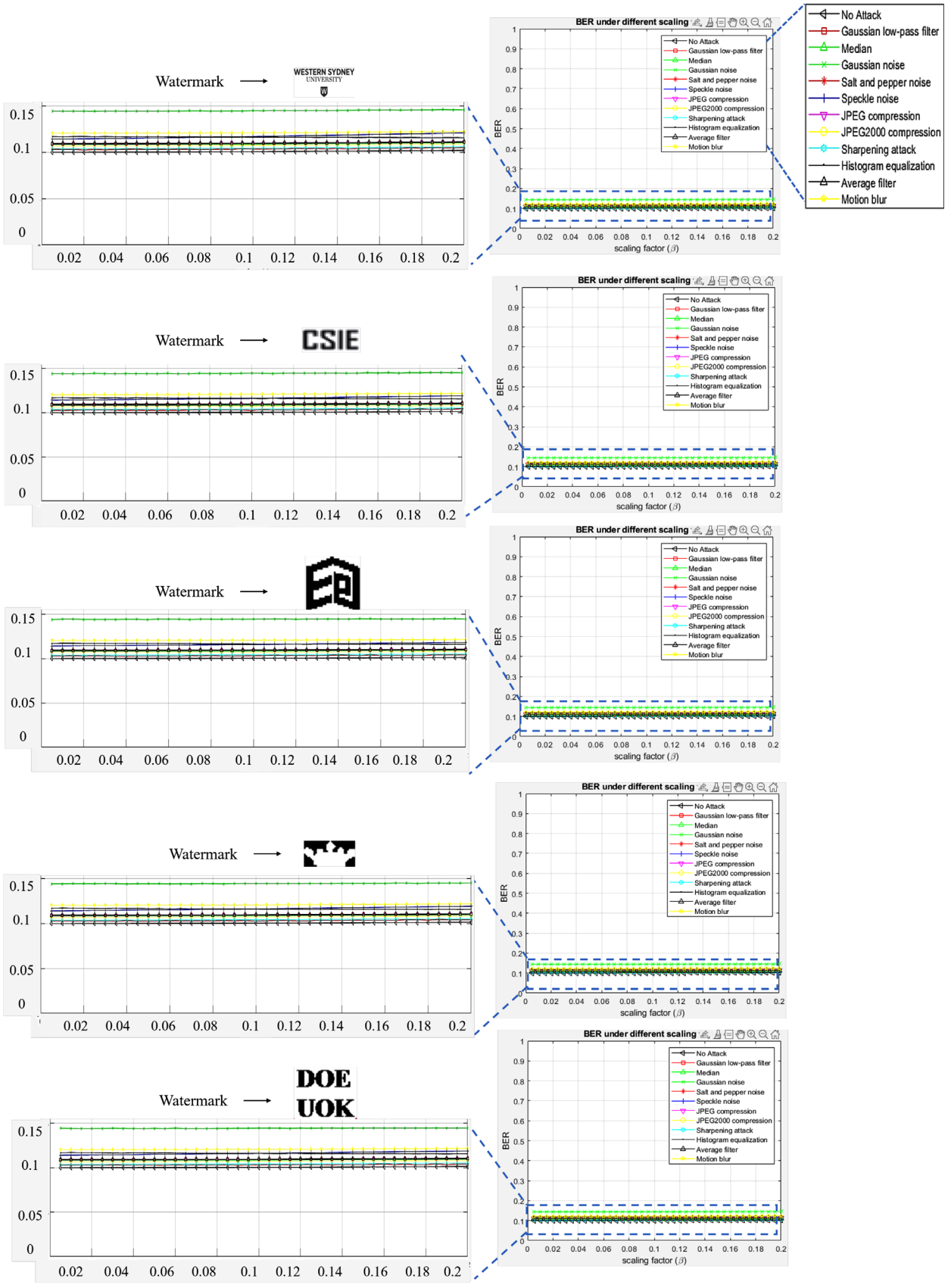

FIGURE 8 BER vs. scaling factor (β) plots. Illustrate the watermark extraction error rate under the influence of different attacks. The test image of *Lenna* is greyscale and 512 × 512 in size. The dimensions of the individual watermarks are given in Table 3. Best viewed when zoomed in

TABLE 5 Watermark fragility analysis under different attacks. The employed test and the watermark images are *Lenna* and WSU, respectively. The former is 512 × 512 in size and the latter is 64 × 64

Attacks ↓ /Images →	Goldhill	Lenna	Baboon	Pirate	Zelda	Barb	Tiffany	Boat	Cameraman	Lady
Attack-free/ NCC→	1	1	0.98	1	0.99	1	0.98	0.99	1	1
Rotation 45°	0.0180	0.013	0.009	0.011	0.023	0.015	0.018	0.017	0.023	0.019
Median filtering (3×3)	0.023	0.02	0.019	0.017	0.019	0.015	0.012	0.021	0.013	0.021
Gamma correction at ($\gamma = 0.50$)	0.017	0.023	0.021	0.02	0.016	0.013	0.018	0.014	0.021	0.017
Salt & Pepper noise (0.02)	0.01	0.013	0.021	0.016	0.012	0.014	0.019	0.013	0.016	0.015
Gaussian noise (0.001)	0.014	0.012	0.023	0.016	0.011	0.019	0.023	0.017	0.013	0.021
Histogram equilization	0.019	0.011	0.021	0.017	0.014	0.022	0.013	0.019	0.016	0.021
Blurring (5%)	0.023	0.017	0.02	0.011	0.014	0.013	0.022	0.019	0.012	0.009
Sharpening (25%)	0.024	0.008	0.016	0.019	0.006	0.015	0.022	0.012	0.013	0.016
Scaling (50%)	0.0066	0.009	0.011	0.019	0.014	0.009	0.012	0.016	0.012	0.019
Compression (QF= 40)	0.009	0.004	0.012	0.007	0.014	0.007	0.012	0.016	0.008	0.018
Compression (QF= 50)	0.012	0.014	0.016	0.011	0.018	0.013	0.018	0.019	0.014	0.021

extracted watermark bits are identical to the embedded/original watermark bits. In contrast, the BER value of '1' indicates a total mismatch between the former and the latter [11–19]. The symbols in Equation (14) are similar to the ones in Equation (13). that is, W and W' stand for the original and extracted watermarks of dimensions P and Q, respectively. Note, the simulation results in Figure 8 are obtained from the test image of *Lenna*.

4.2 | 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 contained within the solid green boundaries (see Figure 9), appear to be serene and indistinguishable from the host images. Furthermore, watermarked images display a smooth transition between the grey or the *RGB* colour levels, making them imperceptible to the HVS. Subsequently, the same figure also illustrates the PSNR values and the imperceptibility performance of the proposed method on different test images. The PSNR results presented within Figure 9 are achieved using the WSU watermark, which is 64 × 64 in size. Moreover, the imperceptibility and capacity comparisons of the proposed method with state-of-the-art methods are shown in Table 3. Note, to gain a fair comparison between the proposed and state-of-the-art methods, the results in Table 3 are attained from the test images, *Lenna* and *Lenna_colour*, each of which is 512 × 512 in size. Such fairness is further highlighted as the proposed method uses the same watermarks as used by the state-of-the-art methods to achieve the PSNR values.

First, Table 3 shows that the watermark of size 32 × 16 is used by the methods in [5, 13] and [14]. The methods by Verma et al. [13] and Islam et al. [14] have the same embedding capacity but the former is outperformed by the latter in the context of the PSNR values. These methods are surpassed by Sharma et al.'s method [5] in terms of the PSNR and the embedding capacity. When the proposed method is embedded with a watermark that's 32 × 16 in size, it outperforms the method [5] in every aspect. In the similar context, Singh et al.'s method [20] achieves the best PSNR and has the highest capacity, but their method operates only on the grayscale images. In contrast,

FIGURE 9 Imperceptibility comparisons of the proposed scheme in the absence of an attack. The greyscale, the *RGB* and the YC_bC_r model-based watermarked images are in the solid: green, orange and blue boundaries, respectively. Subsequently, the extracted watermarks are in the dashed: green, orange and blue boundaries, respectively. Best viewed when zoomed in

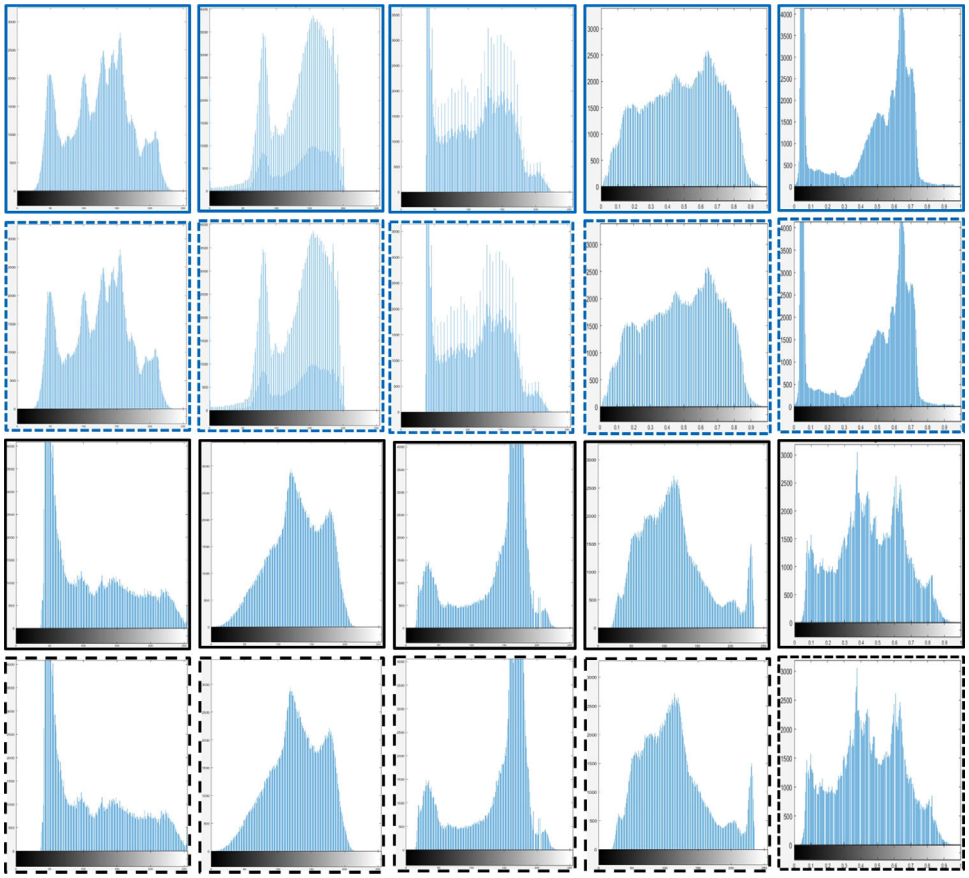

FIGURE 10 Histogram comparison of host images (first and third rows) with watermarked images (second ad fourth rows). Note, a top and a bottom image jointly makes a pair. Left to Right pairs (blue boundaries): *Lenna, Tiffany, Pirate, Zelda* and *Cameraman*. Left to Right pairs (black boundaries): *Lady, Baboon, Boat, Goldhill, Cameraman* and *Barb*. Best viewed when zoomed in

the method by Barr et al. [18] is only operable on the colour images.

Second, Barr et al.'s approach uses the *RGB* colour-space and is tested using two separate watermarks. The *TEST* watermark, that's 50×20 in size, is one of the two watermarks. Even though Barr et al. have tested their method only on six-test images, their scheme is imperceptible and has a higher capacity than the aforementioned methods in [5, 13] and [14]. Once embedded with the *TEST* watermark (50×20 in size), the watermarked images produced by the proposed method are higher in imperceptibility than Barr et al.'s method. In addition to the *RGB* colour-space, Table 3 also shows the proposed method's PSNR results, achieved after employing the *TEST* watermark in both the greyscale and the YC_bCr colour spaces. This not only highlights the superiority of the proposed method over Barr et al.'s method but also its operability in different colour spaces.

Third, the watermarks used by Kang et al. in [12] and [17] are 32×32 in size. Although both of their studies are the same in the embedding capacity, the watermarks used for illustrations in each of them are different. For instance, the study in [12] has used the *Xi'an* watermark, whereas the study in [17] has used the *Print* watermark. Moreover, the former study is outperformed by the latter in terms of the PSNR values.To this end, after being embedded with each of these watermarks, the watermarked images processed by the proposed method exhibit better imperceptibility traits and achieve higher PSNR values than each of Kang et al.'s methods.

Fourth, it is well known that the security of a watermarking scheme suffers when the embedding capacity is reduced. Additionally, the smaller the watermark, the harder it is to verify. Therefore, the schemes by [11, 15, 19] and [16] are higher in capacity than most methods in Table 3. Each of these methods has utilised the *DOE* watermark, 64×64 in dimensions, for illustrations. Moreover, except Kamili et al.'s method, which is only operable in the YC_bC_r colour-space, each of these methods can handle the greyscale and the colour images. While operating on the greyscale images, Hurrah et al.'s method [16] is better in imperceptibility than Loan et al. [15], but the latter outperforms the method [11] in the PSNR performance. The PSNR difference amongst these three methods is not significant and they all share the same capacity while operating on the greyscale images. As illustrated in Table 3, this capacity value is the same for the proposed method. Still, when when embedded with the same *DOE* watermark, the proposed method achieves better PSNR values than its three counterparts. In the YC_bCr colour-space, Kamili et al.'s method has the highest embedding capacity. It

FIGURE 11 Robustness comparisons of the proposed scheme on the continuous-tone images under various attacks. The Solid red, yellow, green, orange and blue boundaries contain the watermarked images under the rotation attack at 45°, Gaussian noise (GN) at 0.001 and gamma correction at 0.75, salt & pepper (S&P) noise at 0.02 and histogram equalization (HE), respectively. The dashed boundaries represent the extracted watermarks from the attacked watermarked images. Best viewed when zoomed in

also outperforms the PSNR values attained by methods [16] and [15] but not by the proposed method. Similarly, in the *RGB* colour-space, the proposed method shares the same capacity as the methods in [15] and [11]. However, the proposed method has the best PSNR, followed by Hurrah et al.'s method and Loan et al.'s method. While operating on the greyscale images, the proposed method is superior to methods [5, 11–17] in Table 3 from the imperceptibility viewpoint by a margin of 3.1%, 5.15% , 6.73%, 5.51%, 3.95%, 2.95%, 2.91%, 4.53%, respectively. Similarly, in the *RGB* and the YC_bCr colour-space, it is superior to methods [18] and [19] by 8.46% and 2.26%, respectively.

Finally, the authors in [37, 55, 56] have used histograms to prove the effectiveness of their embedding strategies. Similarly, histogram comparisons in Figure 10 suggest a cumulative resemblance of 98.4% between image pairs. Note, in Figure 10, a top and a bottom image (the host image and its watermarked version) jointly makes a pair. Moreover, the watermark employed to generate these histograms is WSU: 64 × 64. Subsequently, the histogram pair of the test image, *Tiffany*, has the least histogram similarity, that is, 97.9 %, whereas the highest similarity is attained by the test image of *Lenna* with 98.6%. Similar to the method in [55], histograms of the processed images achieved by the proposed method show a great degree of similarity. For instance, in [55] the histogram similarity for the test image: *Lenna* is 98.11%. This indicates a successful embedding strategy as the watermarked images are imperceptible and indistinguishable from the host images to the HVS.

4.3 | Security: Robustness and fragility analysis

The watermarked images under various StirMark attacks (available at [57]) such as rotation attack at 45°, Gaussian noise (GN) at 0.001, JPEG compression at different quality factors (QF) etc. and the extracted watermarks are shown in Figure 11. These illustrations are achieved using the WSU watermark, 64 × 64 in size. Moreover, watermarks of different dimensions are used in Figure 12, wherein the robustness performance of the watermarks extracted using the proposed method is compared with those extracted using state-of-the-art methods. The NCC values in Tables 4 and 5 demonstrate the similarity between the embedded and extracted watermarks, respectively.

The results within Figure 12 and Table 4 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 12 and Table 4, respectively. However, the only exception is Barr et al.'s method [18], as it has used *Lenna_colour* as the host image, which is also 512 × 512 in size. Therefore, the same image is used by the proposed method to achieve a comparison with Barr et al.'s method [18]. Moreover, as illustrated in Figure 12 and Table 4, the robustness of the proposed method is tested using a variety of watermarks- as used by state-of-the-art methods. Each of these comparisons is made using like-for-like watermark images as below.

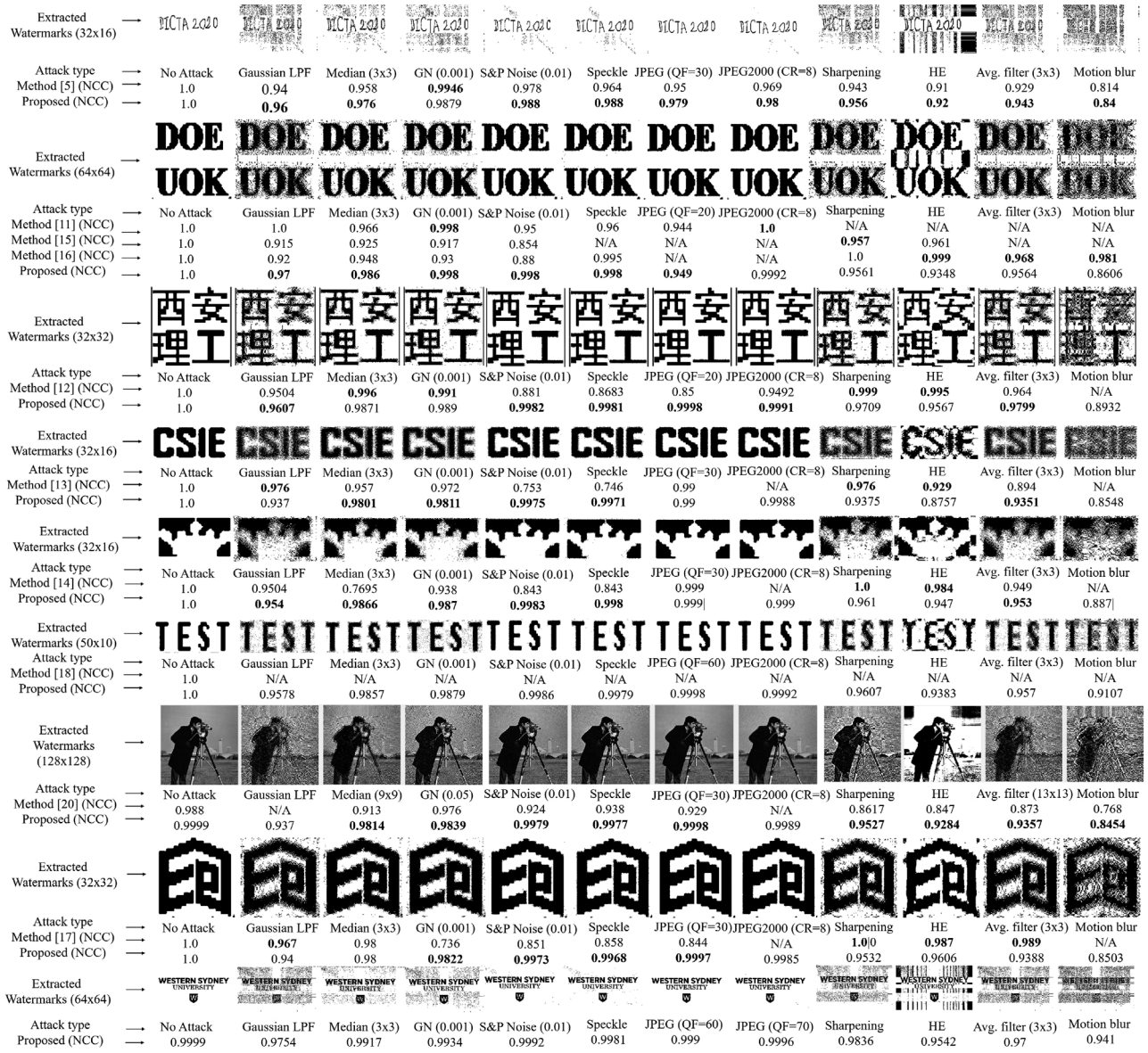

FIGURE 12 Robustness performance of the watermarks extracted using the proposed method and their comparison with state-of-the-art methods. These watermarks are extracted from the test image of *Lenna*, once it's been exposed to a variety of attacks. The test image is greyscale and 512 × 512 in size. The only exception is Barr et al.'s method [18], as it has used *Lenna_colour* as the host image, which is also 512 × 512 in size. The same image, therefore, is used by the proposed method to achieve a comparison with Barr et al.'s method [18]. Best viewed when zoomed in

TABLE 6 Processing time evaluation (in seconds) and comparisons for a 512 × 512 image. The machine used by the proposed method in this analysis has an i7-8650U CPU, running at 1.9 GHz and 16 GB RAM

Methods	Machine	Watermark	Colour-space	$Time_{Embedding}$	$Time_{Extraction}$	$PT_{NoAttack}$
Sharma et al. [5]	Same as the proposed method	DICTA: 32 × 16	Greyscale	4.9	0.23	**5.13**
Proposed				5.1	1.1	6.2
Barr et al. [18]	Intel™ i7 microprocessor running at 2.2 GHz, 16 GB DDR3 RAM, and Iris Pro 1536 MB graphics card.	TEST: 50 × 10	*RGB*	90	55	145
Proposed				15.3	3.3	**18.6**
Kamili et al. [19]	Intel™ Core Duo CPU T5870, running at 2.00 GHz	UOK: 64 × 64	YC_bC_r	2.28	0.92	**3.2**
Proposed				5.1	1.1	6.2

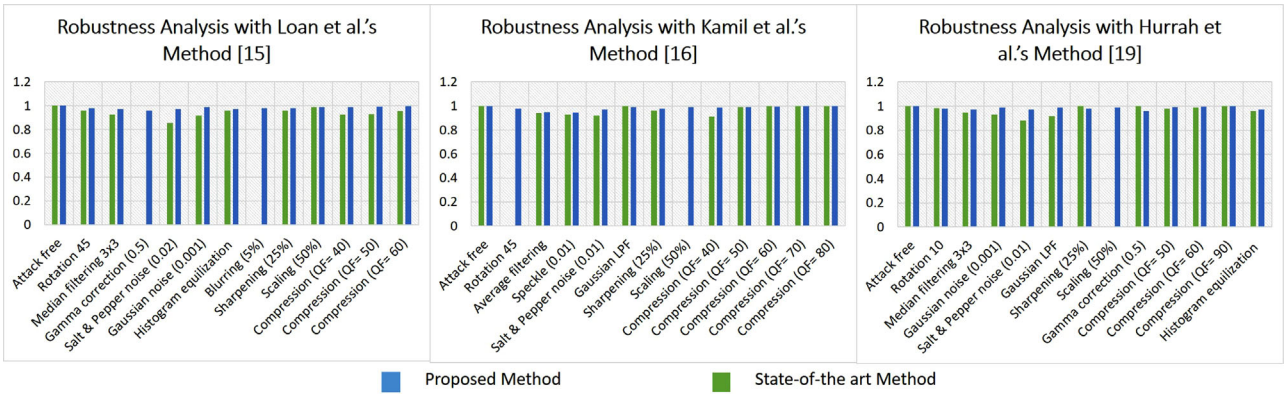

FIGURE 13 Robustness comparisons of the proposed method with state-of-the-art methods [15, 16, 19], within the YC_bC_r colour-space. Best viewed when zoomed in

First, in Figure 12 and Table 4, watermarks of size 32×16 are used by methods [5, 13] and [14]. Verma et al.'s method achieves the best NCC value under the Gaussian low-pass-filtering (LPF) attack. It's also the most resilient towards the JPEG compression attacks. Islam et al.'s method is the best in resisting the sharpening, the HE and the scaling (75%) attacks, respectively. However, Sharma et al.'s method outperforms Islam et al.'s method in terms of resisting the JPEG compression attacks. Sharma et al.'s method also achieves better NCC values in terms of the noise (GN, S&P, speckle) attacks when compared to its counterpart methods by Verma et al. [13] and Islam et al. [14]. In a similar context, these three methods [5, 13, 14], are outperformed by the proposed method. Additionally, as illustrated within Figure 12 and Table 4, the watermarks extracted using the proposed method attain the highest NCC values when exposed to the majority of the watermarking attacks.

Second, in Figure 12 and Table 4, watermarks of size 32×32 are used by methods [12] and [17]. These methods withstand the JPEG compression effectively and have excellent resistance to the JPEG2000 compression attack. In case of the latter attack, both of these methods are either on-par with the proposed method or outperform it. Figure 12 illustrates some other instances where these methods can also outshine the proposed method concerning the NCC values. However, in most cases, the highest NCC values favor the proposed method. Moreover, two main shortfalls are associated with methods [12] and [17]. First, these methods are unequipped to deal with geometrical attacks, such as rotation and scaling. Second, these methods can only operate on grey scale images that are hardly used nowadays. In contrast, the proposed method can bridge both of these gaps.

Third, in Figure 12 and Table 4, watermarks of size 64×64 are used by methods [11, 15] and [16]. Loan et al.'s method [15] achieves the best NCC value concerning the sharpening attack. It is also superior in resisting the JPEG comparison, specifically at higher QFs. Moreover, Hurrah et al.'s methods [11] and [16] are better than Loan et al.'s in resisting the scaling, rotation, and gamma-correction attacks, respectively. To this end, the overall NCC value performance of Hurrah et al.'s method [16] surpasses other method in [11]. 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 proposed method operates as skillfully as method [11] under Gaussian noise and scaling attacks. Moreover, it outperforms [11] and all other methods in Table 4 concerning the overall NCC performance, making it superior in overall robustness.

Fourth, in Figure 12 and Table 4, Barr et al.'s method uses a watermark of size 50×20 [18]. Table 4 shows that Barr et al.'s work is limited in robustness evaluations. Their method is tested under the scaling and the rotation attacks, respectively. In the case of the scaling attack, it outperforms the proposed method, whereas it is the other way around in the case of the rotation attack. The proposed method outshines Barr et al.'s method in the overall NCC performance method. Finally, the robustness performance of the proposed method within the YC_bC_r colour-space is presented in Figure 13. The exact figure also highlights the robustness performances of other state-of-the-art methods [15, 16, 19], all of which are operable with the YC_bC_r colour-space.

Likewise, the fragility analysis of the proposed method is covered in Figure 14 and Table 5. In Figure 14, the solid red colour boundaries contain the modified/attacked watermarked images and the solid green boundaries carry images with no modification. Subsequently, the successively extracted watermarks from these watermarked images are contained within their corresponding coloured dashed boundaries. Subjectively, it can be noticed that in case of a modification, the extraction process yields a non-readable watermark, indicating tamper existence. Results in Table 5, indicate that the NCC values are less than 0.025 and as per Thanki et al. this is the threshold, below which the extracted watermark is meaningless [58]. Consequently, it verifies that if any change is made to the watermarked image by the hackers, the proposed extraction process prohibits the watermark from being extracted, signifying tamper detection.

4.4 | Processing time analysis

The processing time (PT) of the proposed scheme is dependent on the size of the host image and that of the watermark. The larger these sizes are, the longer is the processing time.

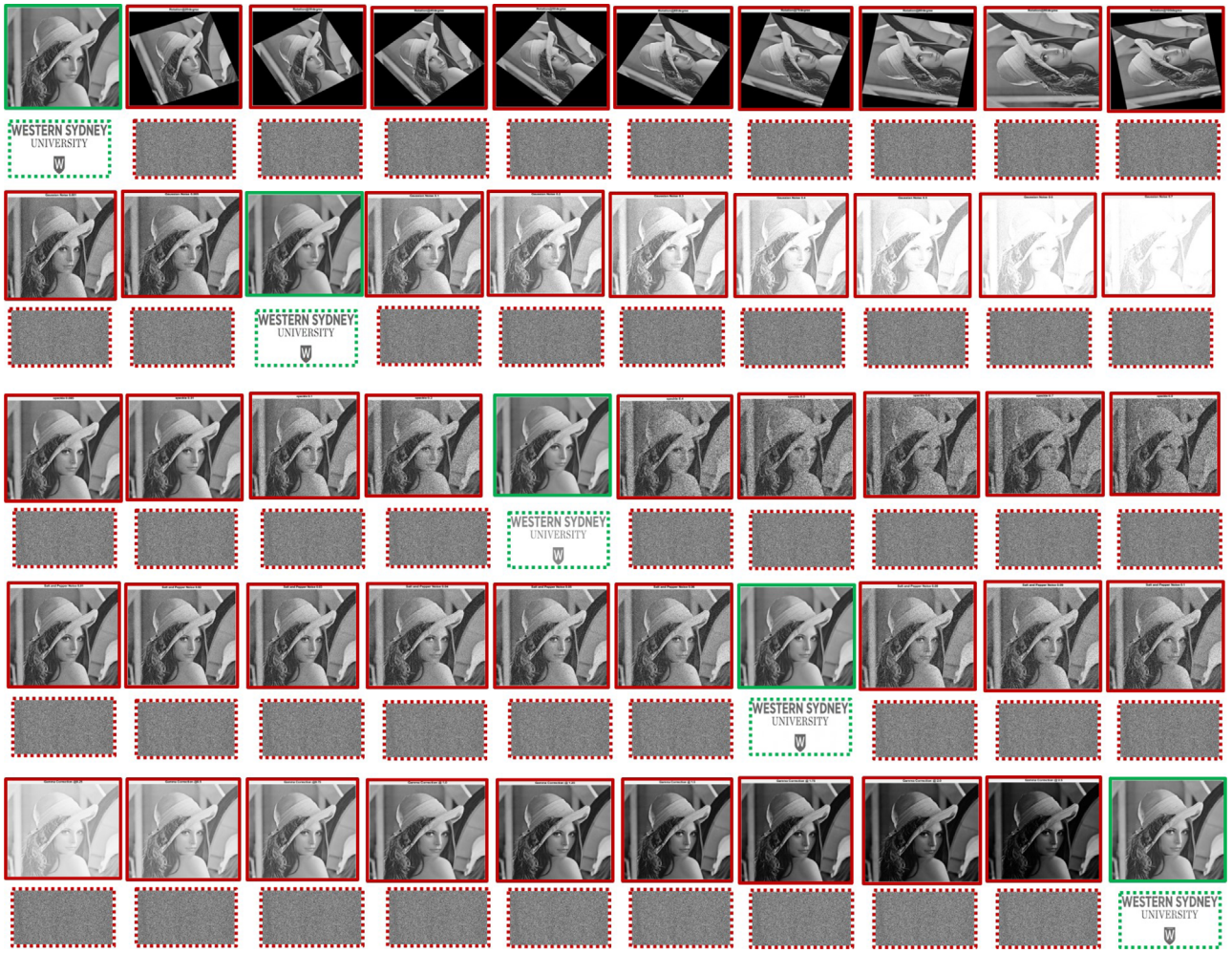

FIGURE 14 Fragility analysis of the proposed scheme. The solid red boundaries contain watermarked images after modifications and the solid green boundaries contain the watermarked images with no modification. Subsequently, the extracted watermarks from these images are contained within their corresponding coloured dashed boundaries. Best viewed when zoomed in

Furthermore, in the proposed watermarking process, the processing time in the absence of an attack ($PT_{NoAttack}$) is measured as a sum of the time taken by the embedding ($Time_{Embedding}$) and the extraction ($Time_{Extraction}$) processes, respectively. In this paper, $PT_{NoAttack}$ is calculated via Equation (15). Similarly, the processing time in the occurrence of an attack (PT_{Attack}) is calculated as per Equation (16), where $Time_{Checkpointing}$ is the time taken by the proposed checkpointing process.

$$PT_{NoAttack} = Time_{Embedding} + Time_{Extraction}, \tag{15}$$

$$PT_{Attack} = PT_{NoAttack} + Time_{Checkpointing}. \tag{16}$$

The objective evaluation of the proposed method's PT and its comparison with other methods is presented in Table 6. The given table shows the time taken by different methods in the absence of an attack. It can be noticed that Barr et al.'s method [18] has the highest PT, whereas Kamili et al.'s method [19] has the lowest. Although their results are not included within Table 6, but methods by Verma et al. and Islam et al. are also faster than the proposed method. However, these methods are limited to robust watermarking, whereas the proposed method is adaptable to robust and fragile watermarks.

In the case of the robust watermarking, $Time_{Checkpointing}$ in the proposed method is dependent on a few factors. The first is the EV's size and the second is the number of iterations performed to find the target element within EV. Note, from Equation (10), the target element of robust watermarking proves $Energy(WI_{Before})$ equals $Energy(WI_{After})$. As the proposed checkpointing is based on the binary search algorithm, its time complexity is defined as $\mathcal{O}(log_2 N)$, where N is the size of EV or the number of elements present within EV. To this end, the fastest or best scenario for the proposed checkpointing is when the first element to be matched within EV is the target element.

In contrast, the worst-case occurs if the target element is located at the end of EV, as it will be the last element to be matched or the target element is not at all present in EV. Objective evaluations have demonstrated that when the size of EV is eight, $Time_{Checkpointing}$ in the worst-case scenario, imposes a 9%

of $PT_{NoAttack}$ overhead. Moreover, if the watermark is fragile, the process is streamlined as per Equation (11), which consists of matching only one element in EV: $EV_{NoModification}$ with $Energy(WI_{After})$ and $Energy(WI_{Before})$ to establish its being as the target element. Note, the aforementioned time complexity analysis is valid when an image is either in the greyscale or in the YC_bC_r colour-space. In contrast, this time complexity becomes three times when the proposed method is implemented within the *RGB* colour-space. Illustrations of the proposed method's processing time, in each of the colour-spaces (greyscale, YC_bC_r and *RGB*) are presented within Table 6.

5 | CONCLUSION

A novel image watermarking scheme that uses only one watermark for achieving both protection and authentication of identities is presented. First, the proposed watermark embedding approach uses DWT, DCT and a novel median-based embedding block selection procedure. Combining these techniques enables the proposed watermarking scheme to outperform the existing methods concerning imperceptibility and security. Second, an unconventional concept of checkpointing is introduced in the spatial domain which streamlines the overall process and equips the proposed scheme to be either robust or fragile, making it superior in its application versatility. Furthermore, the proposed scheme has a high watermark embedding capacity, on par with state-of-the-art methods. Third, 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. Moreover, the proposed method is compatible with different colour spaces, thus, it can be deployed on greyscale and colour images. Finally, the proposed scheme objectively outperforms the state-of-the-art methods in imperceptibility and security attributes, measured via PSNR and NCC values, respectively.

ACKNOWLEDGEMENTS

This work is supported by the Western Sydney University Postgraduate Research Award. Thanks to Jessica Johnston for proofreading this work. The authors are thankful to the anonymous reviewers for their helpful comments and suggestions.

CONFLICT OF INTEREST

The authors have declared no conflict of interest.

DATA AVAILABILITY STATEMENT

The data that support the findings of this study are available from the corresponding author upon reasonable request.

ORCID

S. Sharma https://orcid.org/0000-0002-3185-6149

REFERENCES

1. Mohanty, M., Yaqub, W.: Towards seamless authentication for zoom-based online teaching and meeting. arXiv preprint, arXiv:2005.10553 (2020)
2. Service nsw cyber incident. https://www.service.nsw.gov.au/cyber-incident
3. van der Schyff, K., Flowerday, S., Furnell, S.: Duplicitous social media and data surveillance: An evaluation of privacy risk. Comp. Security 94, 101822 (2020)
4. Sharma, S., Zou, J.J., Fang, G.: Recent developments in halftone based image watermarking. In: 2019 International Conference on Electrical Engineering Research & Practice (ICEERP), pp. 1–6. IEEE, Piscataway (2019)
5. Sharma, S., Zou, J.J., Fang, G.: A novel signature watermarking scheme for identity protection. In: 2020 Digital Image Computing: Techniques and Applications (DICTA), pp. 1–5. IEEE, Piscataway (2020)
6. Evsutin, O.O., Melman, A.S., Meshcheryakov, R.V.: Digital steganography and watermarking for digital images: A review of current research directions. IEEE Access 8, 166589–166611 (2020).
7. Liu, X.-L., Lin, C.-C., Yuan, S.-M.: Blind dual watermarking for color images' authentication and copyright protection. IEEE Trans. Circuits Syst. Video Technol. 28(5), 1047–1055 (2016)
8. Bhowmik, D., Abhayaratne, C.: Embedding distortion analysis in wavelet-domain watermarking. ACM Trans. Multim. Comp. Commun. Appl. (TOMM) 15(4), 1–24 (2019)
9. Sharma, S., Zou, J., Fang, G.: Significant difference-based watermarking in multitoned images. Electron. Lett. 56(18), 923–926 (2020)
10. Bertini, F., Sharma, R., Montesi, D.: Are social networks watermarking us or are we (unawarely) watermarking ourself? arXiv preprint, arXiv:2006.03903 (2020)
11. Hurrah, N.N., Parah, S.A., Loan, N.A., Sheikh, J.A., Elhoseny, M., Muhammad, K.: Dual watermarking framework for privacy protection and content authentication of multimedia. Future Gener. Comput. Syst. 94, 654–673 (2019)
12. Kang, X.-b., Zhao, F., Lin, G.-f., Chen, Y.-j.: A novel hybrid of dct and svd in dwt domain for robust and invisible blind image watermarking with optimal embedding strength. Multim. Tools Appl. 77(11), 197–224 (2018)
13. Verma, V.S., Jha, R.K., Ojha, A.: Significant region based robust watermarking scheme in lifting wavelet transform domain. Expert Syst. Appl. 42(21), 8184–8197 (2015)
14. Islam, M., Roy, A., Laskar, R.H.: Svm-based robust image watermarking technique in lwt domain using different sub-bands. Neural Comput. Appl. 32(5), 1379–1403 (2020)
15. Loan, N.A., Hurrah, N.N., Parah, S.A., Lee, J.W., Sheikh, J.A., Bhat, G.M.: Secure and robust digital image watermarking using coefficient differencing and chaotic encryption. IEEE Access 6, 876–897 (2018)
16. Hurrah, N.N., Parah, S.A., Sheikh, J.A., Al-Turjman, F., Muhammad, K.: Secure data transmission framework for confidentiality in iots. Ad Hoc Netw. 95, 101989 (2019)
17. Kang, X., Chen, Y., Zhao, F., Lin, G.: Multi-dimensional particle swarm optimization for robust blind image watermarking using intertwining logistic map and hybrid domain. Soft Comput. 24(14), 561–584 (2020)
18. Barr, M., Serdean, C.: Wavelet transform modulus maxima-based robust logo watermarking. IET Image Proc. 14(4), 697–708 (2019)
19. Kamili, A., Hurrah, N.N., Parah, S.A., Bhat, G., Muhammad, K.: Dwfcat: Dual watermarking framework for industrial image authentication and tamper localization. IEEE Trans. Ind. Inf. 17(7), 5108–5117 (2020)
20. Singh, D., Singh, S.K.: Dwt-svd and dct based robust and blind watermarking scheme for copyright protection. Multim. Tools Appl. 76(11), 001–024 (2017)
21. Van Schyndel, R.G., Tirkel, A.Z., Osborne, C.F.: A digital watermark. In: Proceedings of 1st International Conference on Image Processing, vol. 2, pp. 86–90. IEEE, Piscataway (1994)
22. Uchida, Y., Nagai, Y., Sakazawa, S., Satoh, S.: Embedding watermarks into deep neural networks. In: Proceedings of the 2017 ACM on International Conference on Multimedia Retrieval, pp. 269–277. ACM, New York (2017)
23. Boenisch, F.: A survey on model watermarking neural networks. arXiv preprint, arXiv:2009.12153 (2020)
24. Sharma, Y., Taheri, J., Si, W., Sun, D., Javadi, B.: Dynamic resource provisioning for sustainable cloud computing systems in the presence of correlated failures. IEEE Trans. Sustain. Comput. 6(4), 641–654 (2020)

25. Sharma, Y., Javadi, B., Si, W., Sun, D.: Reliable and energy efficient resource provisioning and allocation in cloud computing. In: Proceedings of the10th International Conference on Utility and Cloud Computing, pp. 57–66. IEEE Computer Society, Los Alamitos (2017)
26. Kumar, C., Singh, A.K., Kumar, P.: A recent survey on image watermarking techniques and its application in e-governance. Multim. Tools Appl. 77(3), 3597–3622 (2018)
27. Anand, A., Singh, A.K.: Watermarking techniques for medical data authentication: A survey. Multim. Tools Appl. 80, 30165–30197 (2020)
28. Menendez-Ortiz, A., Feregrino-Uribe, C., Hasimoto-Beltran, R., Garcia-Hernandez, J.J.: A survey on reversible watermarking for multimedia content: A robustness overview. IEEE Access 7, 662–681 (2019)
29. Singh, A.K., Kumar, B., Singh, S.K., Ghrera, S., Mohan, A.: Multiple watermarking technique for securing online social network contents using back propagation neural network. Future Gener. Comput. Syst. 86, 926–939 (2018)
30. Lin, W.-H., Horng, S.-J., Kao, T.-W., Fan, P., Lee, C.-L., Pan, Y.: An efficient watermarking method based on significant difference of wavelet coefficient quantization. IEEE Trans. Multim. 10(5), 746–757 (2008)
31. Meerwald, P., Koidl, C., Uhl, A.: Attack on watermarking method based on significant difference of wavelet coefficient quantization. IEEE Trans. Multimedia 11(5), 1037–1041 (2009)
32. Bobkowska, K., Nagaty, K., Przyborski, M.: Incorporating iris, fingerprint and face biometric for fraud prevention in e-passports using fuzzy vault. IET Image Proc. 13(13), 2516–2528 (2019)
33. Haddada, L.R., Dorizzi, B., Amara, N.E.B.: A combined watermarking approach for securing biometric data. Signal Process. Image Commun. 55, 23–31 (2017)
34. Lu, C.-S., Liao, H.-Y.: Multipurpose watermarking for image authentication and protection. IEEE Trans. Image Process. 10(10), 1579–1592 (2001)
35. Abdulrahman, A.K., Ozturk, S.: A novel hybrid dct and dwt based robust watermarking algorithm for color images. Multim. Tools Appl. 78(12), 027–049 (2019)
36. Parah, S.A., Sheikh, J.A., Loan, N.A., Bhat, G.M.: Robust and blind watermarking technique in dct domain using inter-block coefficient differencing. Digital Signal Process. 53, 11–24 (2016)
37. Hurrah, N.N., Parah, S.A., Sheikh, J.A.: Embedding in medical images: an efficient scheme for authentication and tamper localization. Multim. Tools Appl. 79(5) (2020)
38. Selesnick, I.W., Baraniuk, R.G., Kingsbury, N.C.: The dual-tree complex wavelet transform. IEEE Signal Process Mag. 22(6), 123–151 (2005)
39. Daubechies, I., Han, B., Ron, A., Shen, Z.: Framelets: Mra-based constructions of wavelet frames. Appl. Comput. Harmon. Anal. 14(1), 1–46 (2003)
40. Huynh-The, T., Hua, C.-H., Tu, N.A., Kim, D.-S.: Robust image watermarking framework powered by convolutional encoder-decoder network. In: 2019 Digital Image Computing: Techniques and Applications (DICTA), pp. 1–7. IEEE, Piscataway (2019)
41. Huynh-The, T., Banos, O., Lee, S., Yoon, Y., Le-Tien, T.: Improving digital image watermarking by means of optimal channel selection. Expert Syst. Appl. 62, 177–189 (2016)
42. Huynh-The, T., Hua, C.-H., Tu, N.A., Hur, T., Bang, J., Kim, D., Amin, M.B., Kang, B.H., Seung, H., Lee, S.: Selective bit embedding scheme for robust blind color image watermarking. Inf. Sci. 426, 1–18 (2018)
43. Median calculations. https://www.mathworks.com/help/matlab/ref/median.html
44. Musanna, F., Kumar, S.: A novel fractional order chaos-based image encryption using fisher yates algorithm and 3-d cat map. Multim. Tools Appl. 78(11), 867–895 (2019)
45. Karawia, A.: Image encryption based on fisher-yates shuffling and three dimensional chaotic economic map. IET Image Proc. 13(12), 2086–2097 (2019)
46. Bentley, J.L.: Multidimensional binary search trees used for associative searching. Commun. ACM 18(9), 509–517 (1975)
47. Binary search using matlab. https://www.mathworks.com/matlabcentral/fileexchange/56271-binarysearch-a-n-num
48. Roy, A., Maiti, A.K., Ghosh, K.: An hvs inspired robust non-blind watermarking scheme in ycbcr color space. Int. J. Image Graph. 18(03), 1850015 (2018)
49. Tan, Y., Qin, J., Xiang, X., Ma, W., Pan, W., Xiong, N.N.: A robust watermarking scheme in ycbcr color space based on channel coding. IEEE Access 7, 026–036 (2019)
50. Su, F., Fang, G., Zou, J.J.: A novel colour model for colour detection. J. Mod. Opt. 64(8), 819–829 (2017)
51. Cvg - ugr image database. http://decsai.ugr.es/cvg/dbimagenes/g512.php
52. The waterloo fractal coding and analysis group. http://links.uwaterloo.ca/Repository.html
53. Yoo, J.-C., Han, T.H.: Fast normalized cross-correlation. Circuits Syst. Signal Process. 28(6), 819–843 (2009)
54. Ncc calculations on matlab. https://www.mathworks.com/help/images/ref/normxcorr2.html
55. Yan, X., Wang, S., Abd El-Latif, A.A., Niu, X.: New approaches for efficient information hiding-based secret image sharing schemes. Signal Image Video Process. 9(3), 499–510 (2015)
56. Singh, S.P., Bhatnagar, G.: A new robust watermarking system in integer dct domain. J. Visual Commun. Image Represent. 53, 86–101 (2018)
57. Petitcolas, F.A., Anderson, R.J., Kuhn, M.G.: Attacks on copyright marking systems. In: International Workshop on Information Hiding, pp. 218–238. Springer, Berlin Heidelberg (1998)
58. Thanki, R., Borra, S.: Fragile watermarking for copyright authentication and tamper detection of medical images using compressive sensing (cs) based encryption and contourlet domain processing. Multim. Tools Appl. 78(10), 905–924 (2019)

How to cite this article: Sharma, S., Zou, J.J., Fang, G.: A single watermark based scheme for both protection and authentication of identities. IET Image Process. 16, 3113–3132 (2022). https://doi.org/10.1049/ipr2.12542