IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

SPECIAL SECTION ON INFORMATION SECURITY SOLUTIONS FOR TELEMEDICINE APPLICATIONS

Received January 4, 2018, accepted February 7, 2018, date of publication March 16, 2018, date of current version April 25, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2808172

Secure and Robust Digital Image Watermarking Using Coefficient Differencing and Chaotic Encryption

NAZIR A. LOAN[1], (Student Member, IEEE), NASIR N. HURRAH[1], (Student Member, IEEE), SHABIR A. PARAH[1], (Student Member, IEEE), JONG WEON LEE[2], (Member, IEEE), JAVAID A. SHEIKH[1], (Student Member, IEEE), AND G. MOHIUDDIN BHAT[3]

[1]Department of Electronics and Instrumentation Technology, University of Kashmir, Srinagar 19006, India
[2]Department of Digital Contents, Sejong University, Seoul 143-747, South Korea
[3]Department of Electronics Engineering, Institute of Technology Zakoora, Srinagar 19006, India

Corresponding authors: Shabir A. Parah (shabireltr@gmail.com) and Jong Weon Lee (jwlee@sejong.ac.kr)

This work was supported in part by the Department of Science and Technology (DST), New Delhi, and DeitY, Government of India, through the DST Inspire Fellowship Scheme and Visvesvaraya Ph.D. Scheme, respectively, and in part by the Ministry of Science and ICT (MSIT), South Korea, under the Information Technology Research Center (ITRC) support program supervised by the Institute for Information & communications Technology Promotion (IITP) under Grant IITP-2017-2016-0-00312.

ABSTRACT This paper presents a chaotic encryption-based blind digital image watermarking technique applicable to both grayscale and color images. Discrete cosine transform (DCT) is used before embedding the watermark in the host image. The host image is divided into 8×8 nonoverlapping blocks prior to DCT application, and the watermark bit is embedded by modifying difference between DCT coefficients of adjacent blocks. Arnold transform is used in addition to chaotic encryption to add double-layer security to the watermark. Three different variants of the proposed algorithm have been tested and analyzed. The simulation results show that the proposed scheme is robust to most of the image processing operations like joint picture expert group compression, sharpening, cropping, and median filtering. To validate the efficiency of the proposed technique, the simulation results are compared with certain state-of-art techniques. The comparison results illustrate that the proposed scheme performs better in terms of robustness, security, and imperceptivity. Given the merits of the proposed scheme, it can be used in applications like e-healthcare and telemedicine to robustly hide electronic health records in medical images.

INDEX TERMS Electronic healthcare, Arnold transform, blind watermarking, chaos, DCT, encryption, and robustness

I. INTRODUCTION

We are living in an age where the Internet has such a great impact on our lives, that we are dependent on it in every aspect. This internet has transformed the entire world into a global village and in last few years, there has been an extraordinary increase in the transfer and sharing of digital data like text, videos, images, audio, etc. over it. However, with the advent of modern access technology, multimedia data is more prone to security risks as data can be modified or redistributed without prior permission. The security risks may include copyright violations, piracy, hacking, unapproved production and distribution, information theft and several other statistical and differential attacks [1]–[4]. According to the Motion Picture Association of America (MPAA) and the Institute of Policy Innovation (IPI), billions of dollars and thousands of jobs are lost annually due to piracy and copyright violation faced by movie, music and software industries. In May 2014 'Guardian' reported an annual loss of 20.5 billion US dollars to movie industry alone. To check these losses, US congress came up with the Stop Online Piracy Act (SOPA) and Protect IP Act (PIPA) bills. Besides copyright and copy protection of multimedia objects, their privacy and security is of supreme importance. For example, in the case of medical images used in an e-healthcare system, the image data and Electronic Patient Record (EPR) is sent to desired locations via insecure channels of Internet [5]–[13]. A minute alteration of these medical images could result in a wrong diagnosis and

2169-3536 © 2018 IEEE. Translations and content mining are permitted for academic research only.
Personal use is also permitted, but republication/redistribution requires IEEE permission.
See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

thus result in a fatal health problem. In such a scenario, development of state of the art algorithms for secure and reliable multimedia content is desperately needed. Though cryptography has been used as a potential tool to tackle some of the issues but cryptographic methods involve the modification of data visually and statistically, which often arouses suspicion and invite attacks [14]–[16]. Information hiding, which involves steganography [17]–[20] and watermarking [21]–[23], has flourished as an effective and alternative method for security, authentication, and IPR issues in multimedia images.

Digital watermarking has been shown to be one of the best solutions for protecting IPR and authenticating the content. Digital watermarking is a technique of hiding information in host media like video, images, etc., in a way that it is unnoticeable to human visual system (HVS). It ensures the security of the information hidden in the images/videos and acts as an important tool to take care of various multimedia related IPR issues. A digital watermark can be an institute logo, signature of a doctor, case history, someone's personal logo, etc. The efficiency of a watermarking technique is decided by various important parameters like robustness, payload, imperceptibility, and security [24]. A watermark is said to be robust if it survives the image processing attacks i.e., a recognizable watermark is extracted from an attacked image. The number of bits of secret data that can be embedded into a given host media is termed as payload. A watermark is said to be highly imperceptible if the human visual system (HVS) cannot detect the presence of the watermark in a host media while maintaining the quality of the host media. The watermark is secure if an adversary somehow extracts the watermark but is not possible for him to put it in a recognizable form without the encryption key. There is always a trade-off between these parameters as described by the famous conflict triangle [25].

Digital watermarking techniques are divided into three types on the basis of degree of robustness of watermark to attacks: robust, fragile or semi-fragile technique [26]–[29]. Robust watermarks survive most of the image processing operations and are best suited for copyright protection and ownership verification, while fragile watermarks vanish when the watermarked media experiences a slight modification and are best suited for authentication and integrity. Watermarks are generally embedded in two domains: pixel domain and transform coefficient domain. In pixel domain watermarking, the host image pixels are directly altered in accordance with that of watermark bits. Pixel domain techniques are easy to implement, having high payload and less computational cost. However, most of the pixel domain methods offer least robustness. In coefficient domain methods, the frequency coefficients of any transform are altered according to the watermark bits. Most of the coefficient domain watermarking methods offer high robustness at the cost of increased computational complexity and reduced payload. Discrete Wavelet Transform (DWT) and Discrete Cosine transform (DCT) are most commonly used transforms for the coefficient domain watermarking methods [30]–[32]. The pixel domain and coefficient domain methods are respectively called spatial domain and transform domain methods. A genetic algorithm based multiple watermarking techniques utilizing DWT and SVD has been presented in [33]. Though the scheme has been shown to be robust and has better imperceptivity, it has no provision for security of the watermark and the scheme is computationally complex. Among the various transform domain techniques, DCT has proven to be efficient as it favors low hardware design cost. There are usually three methods for computing DCT of an image. DCT is computed either on the whole image or is computed on the blocks of the image or only the DC coefficient of blocks of image are computed directly in spatial domain [55]. In each method, watermark embedding is done by altering the DCT coefficients. DCT of a digital image is broadly classified into three bands of frequency coefficients (DC, Middle and Higher). For copyright protection, a watermark must resist most of the image processing attacks and, therefore, can be achieved by embedding it in low frequency coefficients. Since low frequency coefficients contain most of the visual information of an image, therefore, modification of these coefficients may lead to a low quality watermarked image. For authentication purposes, one can embed watermark in high-frequency coefficients because a slight alteration to image would modify the high-frequency coefficients by a significant amount. For the optimal value of robustness and imperceptivity, one can embed the watermark in mid-frequency coefficients [34], [35].

The security of a watermark is one of the major concerns regarding digital image watermarking techniques. For security purposes, cryptographic methods have proven to be a demanding factor, especially for images from defense and medical applications, where privacy is a critical parameter [36], [37]. The conventional data encryption algorithms like data encryption standard (DES), AES, etc. have been shown to perform poorly in case of digital images due to correlation and redundancy problems. Chaos based encryption algorithms, on the other hand, show highly efficient results due to their excellent characteristics viz. initial condition sensitiveness, periodicity, pseudorandom behavior, and ergodic nature. Due to these properties, the adoption of chaotic methods has been considered widely in recent years. Chaotic map based, different image encryption methods have been proposed, and could be seen in [38]–[41]. Numerous watermarking techniques have been reported with the aim of tackling IPR and security issues. Some of the state of art work in this regard could be found in [42]–[62]. A thorough survey of the mentioned work leads to the fact that most of the reported work focuses only on improvement of only one parameter viz. security, payload, imperceptivity, robustness or computational efficiency.

To the best of our knowledge, we did not come across any work that presents an optimal solution that could lead to a secure, imperceptible, robust and computationally efficient technique. This is due to the following presented facts:

1. Either no security mechanism or a poor encryption tool has been utilized, which leads to security issues.
2. Complex mathematical tools for image transformation or complex data hiding approach has been utilized, leading to computational complexity.
3. The systems fail to utilize and/or use only a portion of transformed image for data embedding. In addition, some reported scheme uses bigger block sizes, resulting in low embedding capacity.
4. Modification of low frequency coefficients, or modifying pixels of cover image by a large amount, leading to low imperceptivity.
5. Modification of high frequency coefficients or modifying a pixel by a very small amount, resulting in less robustness of the watermark towards signal processing attacks.

In this paper we have tried to come up with an optimal solution by proposing a novel watermarking technique that takes care of various issues like payload, security, imperceptivity, and robustness, etc. The main contributions of this work are:

1. The scheme is adaptive as there is an option for embedding a single watermark (in case of grayscale images or in luminance component of color image) or multiple watermarks (using R, G, B components of color image) as per need of the application.
2. Inter-block coefficient correlation has been exploited for watermark embedding to facilitate better robustness and payload.
3. Watermark bits have been embedded by altering the difference between two preselected DCT coefficients of the two adjacent blocks. The modification is done in such a way that even various image processing and geometric attacks are successfully resisted by our system making our system highly robust.
4. Nonlinear dynamics of chaos and Arnold transform have been put to use for improving watermark security.

The broad sections of this paper are arranged as follows. A detailed literature review is presented in the Section II. The proposed watermarking algorithm is discussed in the Section III. The simulation results of the proposed scheme have been presented in Section IV to Section VI. The paper concludes in Section VIII.

II. LITERATURE REVIEW

Numerous watermarking techniques for IPR protection, content authentication and/or security of hidden information have been proposed in various works either implemented in the pixel or coefficient domain [42]–[49]. For real-time applications, a watermark is inserted into an image at the time of its capture. The cost of the hardware implementation of an algorithm is of critical importance; SVD, DWT, and Ridgelet transform are not a good choice as far as cost, computational efficiency and hardware complexity is concerned. Embedding using DCT has proven to be better choice for real-time implementation. Furthermore, the popularity of embedding in the DCT domain also gained momentum as Joint Picture Expert Group (JPEG) compression is inherent in most of the image capturing modules, wherein DCT is the opening step of this compression [50], [51].

Bio-inspired optimization principle based DWT domain watermarking technique for RGB images has been presented in [52], where watermark embedding has been done in three level DWT coefficients of the host image. About 25% of the watermark is embedded four times in the LL3 sub-band coefficients of the 3-level DWT while the 75% of watermark is embedded in rest of the three components 3-level DWT coefficients. This technique offers a high degree of robustness while maintaining the quality of the marked image. The disadvantage of this technique is that it is very slow and hence not suited for real-time applications. Further, it offers low payload and imperceptibility.

A watermarking approach for ownership verification and copyright protection has been reported in [53]. Watermark embedding is achieved by using Principal Component Analysis (PCA) and Gray Level Co-occurrence Matrix (GLCM). The scheme has limitation of low embedding capacity.

A watermarking technique for monochrome images has been reported in [54]. This scheme has been shown to have better performance in terms of imperceptibility and robustness, but it offers low capacity. In [55], a blind RGB image watermarking approach is presented by integrating the features of both spatial and frequency domain. In the first stage of the embedding process, the luminance component (Y) of the host image is divided into 8×8 sub-blocks followed by calculation of DC coefficients of each block without using DCT. Watermark embedding has been carried out by modifying the calculated DC coefficients according to the watermark bits. The imperceptivity and robustness of the technique is low, and security analysis of the watermark has not been carried out. In [56], a blind watermarking scheme has been proposed wherein embedding has been done in DCT domain by correlating the two DCT coefficients lying in the same position of adjacent blocks. The technique has been proven resilient to different attacks like rotation, Cropping, JPEG Compression, and few combined attacks. The drawback of this technique is that it is unable to embed a watermark bit in all the blocks, resulting in reduced capacity. In [57], an improved technique has been presented using the concept of coefficient correlation wherein all the blocks are used for the embedding purpose which improves the payload capacity. The results show improved robustness and imperceptibility in addition to increased capacity. But the algorithm has the limitation of increased complexity and computation time. Also, there is no provision for providing confidentiality to the watermark.

There are several applications like data authentication, copyright protection and digital content tracking for illegal distribution where the watermarking algorithms which are not secure cannot be used [1]. Numerous encryption methods have been used to ensure confidentiality and security of embedded watermarks. Chaos has been at center of attraction

for researchers to secure the information prior to embedding to facilitate a double layer security mechanism.

In [58], an encryption technique based on chaos is presented for both standard and medical images. Although security analysis of the scheme shows better results, other parameters like payload and imperceptivity have not been discussed in the proposed work.

In [59], DCT and logistic map based encryption technique is used for securing the medical images through watermarking algorithm. The authors have done ROI based watermarking and tested the design for various attacks. Although the scheme has been found to be secure, the imperceptivity is poor and payload has not been properly considered.

Mathematical remainder based watermarking scheme has been reported in [60], in which watermark embedding is done in low-frequency coefficients of the DCT domain. This approach is robust against common processing attacks but its imperceptivity and payload is low. A DCT domain based watermark embedding algorithm has been proposed by Lin and Chen [61], wherein embedding of watermark information has been done by Least Significant Substitution (LSB). As quantization has been carried on low-frequency coefficients so this system of watermark embedding compromises the robustness in case of JPEG compression.

In [62], a watermark embedding algorithm for monochrome images has been presented, which offers high security for the watermark through encryption, but the robustness of this scheme against image processing operations is not up to the mark. The authors have used a hybrid combination of DCT and DWT to enhance the robustness of the scheme implemented using encryption domain technique. The proposed algorithm has, however, high computational cost. Further, the imperceptivity and payload of the scheme is not up to the mark.

To detect cyber-attacks in the devices used in Internet of Things (IOT), Ferdowsi and Saad [63] proposed a new deep learning algorithm for watermarking of IOT signals utilizing long short-term memory (LSTM) blocks. The authors showed that their method is best suited for IOT security because of its high accuracy, less delay and low complexity. Based on neural networks (NN) and GA, Maity *et al.* [64] proposed perceptually adaptive watermarking technique where embedding is done in the mutually independent host components. For partitioning of the host image, gradient thresholds are properly selected via GA while the weight factor is calculated in minimum mean square error combining (MMSEC) decoder by using NN which ensures stable decision variables that result to improved watermark extraction and interference cancelation. The technique is robust to fading like gain operation but its main drawbacks are low capacity, low imperceptibility, low robustness and very high computational complexity. Mun *et al.* [65] proposed a convolutional neural network (CNN) based watermarking approach using iterative learning framework. Each loop of learning process comprises of watermark embedding, attack simulation and weight update. Although the robustness of this scheme high against common signal processing operations but its performance against jpeg compression of this method is poor.

As discussed, several techniques exist which offer robustness or security or adaptivity in a standalone mode, but as per the best of our knowledge, no such a technique exists which offers better robustness, imperceptivity, adequate payload and sufficient security simultaneously. Further, most of the reported techniques are seen to be applicable either for grayscale or medical or color images. In addition, they only provide facility for embedding single or multiple watermarks. Keeping all the discussed facts in mind, the most pressing need is to develop a secure watermarking scheme that offers high imperceptibility besides having the features of high payload and robustness to single and simultaneous attacks. Towards this end, we present a robust and secure watermarking technique utilizing neighboring block correlation for watermark embedding. The proposed scheme is capable of embedding a watermark in color/grayscale image and also supports embedding multiple watermarks. The proposed scheme promises to be a better solution as we obtain better subjective and objective quality parameters as a result of the facts below.

The imperceptivity is better because we embed a watermark bit by modifying the difference between two mid-frequencies DCT coefficients of the adjacent blocks by an adaptive modification factor. Further, it is worth mentioning here that the modification of difference is done in such a way that it is brought to its nearest predefined zone, which results in less degradation to host image.

The improved payload of our scheme is a result of the fact that we utilize all the blocks of image for data embedding. Further, there is a choice for embedding the number of watermarks. For instance, in the case of an RGB image, if only one watermark is to be embedded, then we embed the watermark in the luminance component. As for inserting multiple watermarks, R, G, B planes of the image are used as cover medium.

The proposed scheme shows better robustness to singular and simultaneous attacks as a result of guard bands utilized in extraction process. This is due to the fact that, when the watermarked media experiences an attack, then the difference between the coefficients may be modified; but this difference has to cross the guard bands on either side of the difference zone to extract a wrong bit

To ensure a better security, the watermark is encrypted at two levels, it is first encrypted by using Chaos and then by using Arnold transform, which results in enhanced security to the embedded watermark.

III. PROPOSED METHOD

The proposed watermarking system could be described by the block diagram shown in Figure 1. The watermark embedding unit and watermark security unit form two important subsystems of the proposed system. The watermark security unit is aimed at improving the security of the embedded

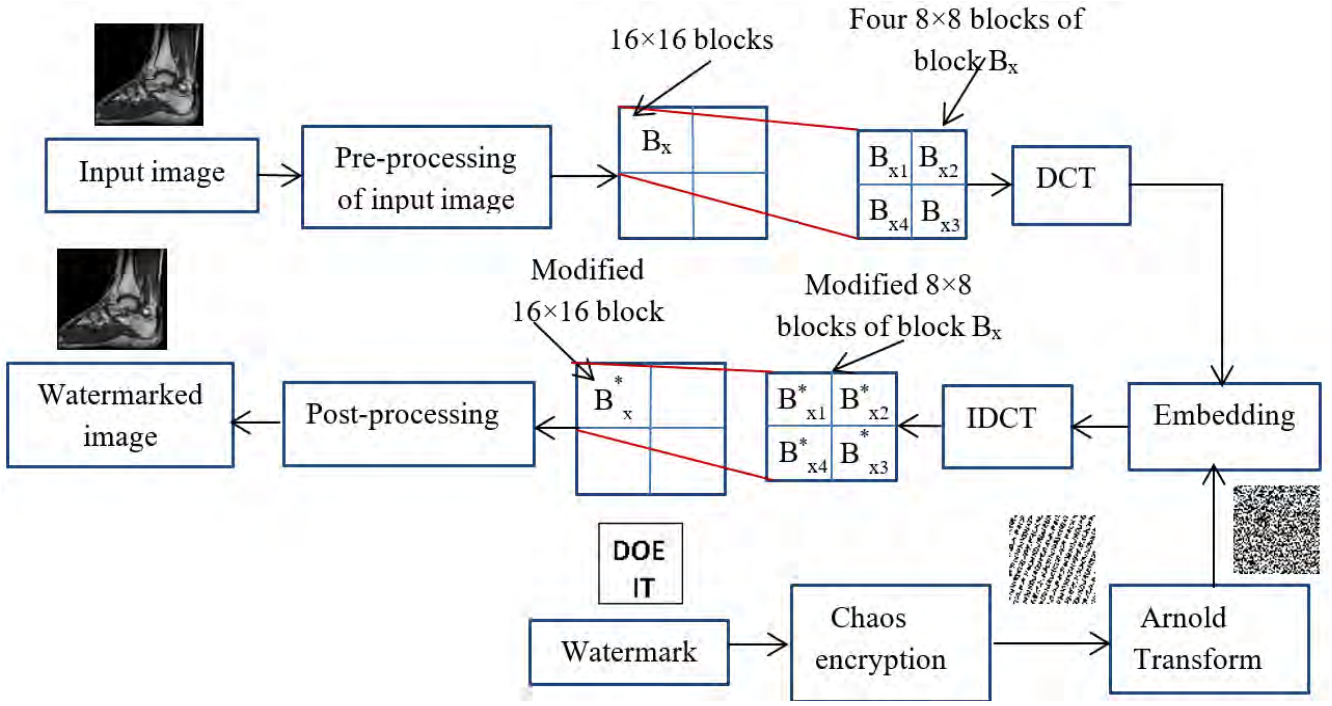


FIGURE 1. Block diagram of the proposed technique.

watermark so as to make it impossible for an adversary to get the exact watermark even if it has the knowledge of embedding algorithm. Chaotic theory and Arnold encryption have been used to achieve a better security. The mathematical preliminaries of Chaos and Arnold encryption are presented in the following sub-section.

A. CHAOS AND ARNOLD ENCRYPTION

A chaotic based encryption algorithm is an effective method for data encryption. Chaos signals possess the qualities of pseudo-randomness, irreversibility and dynamic behavior. The systems having chaotic nature possess high sensitivity to initial parameters. The output chaotic sequence is similar to white noise having random behavior with improved correlation and complexity and is defined as reported in [34] and [35] and given by:

$$C_{n+1} = \mu \times C_n \times (1 - C_n) \tag{1}$$

where $0 < \mu < 4$ typically μ is set to value 3.9 in order to achieve highest randomness and $0 < C_n < 1$ is the nth value generated from Eqn. 1. Different values of C_n could be obtained by varying the value of n from 0 to L-1. Here, L is the maximum number of chaotic values. By setting the initial values of μ and C_0, we can get the required chaotic signal.

As it offers the joint advantage of speed and security, the use of chaotic encryption has been shown to offer increased security [63]. The security of information can be increased by using various encryption techniques, and one of the effective techniques is Arnold transform [66]–[68]. This encryption method, is two dimensional and works well in applications for encrypting images of type N × N. The Arnold transformation is mathematically represented as

$$\begin{bmatrix} x_n \\ y_n \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} (\mathrm{mod} N) \tag{2}$$

where (x_n, y_n) and (x, y) respectively represent the input image and encrypted image pixel coordinates represented as 2D matrices. The transform results in the change of the pixel positions to generate an image which is disordered and different from original one. The result of Arnold transform is an encrypted image which has a one-to-one correspondence with the original image. The pseudo-random nature of the Arnold encryption results in a scrambled image which is not possible to be cracked down without knowing the sequence used [70], [71]. The strength of encryption depends on the number of iterations, which can be defined at the start of the process. Inverse Arnold transform is used to decrypt the encrypted message by using the equation (3). For further details, please refer to [75] and [76].

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 2 & -1 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} (\mathrm{mod} N) \tag{3}$$

B. WATERMARK AND COVER GENERATION

As shown in Figure 1, the input image 'I' is passed through the pre-processing unit which acts as a buffer for grayscale images and as a converter for color images. To carry out watermark embedding into the luminance part of the image the pre-processing unit converts the input RGB image into YCbCr image, where Y stands for luminance information, Cb stands for chrominance blue information and Cr stand for

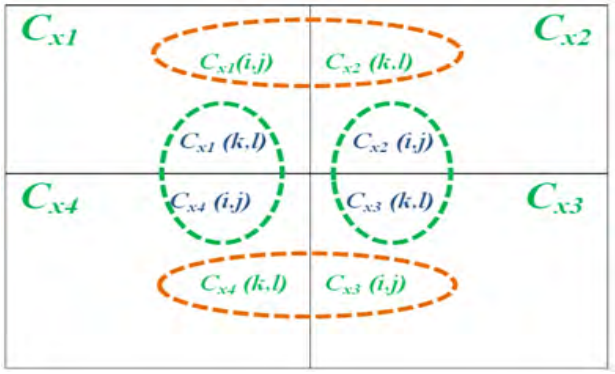


FIGURE 2. Coefficient selection from a pair of neighboring DCT blocks for difference purpose.

chrominance red information of the image. The luminance part 'Y' is put forward as cover for the watermark because modification of this part of the image brings less noticeable changes to actual image compared to the chrominance information. On the other hand, if one wants to embed three watermarks into an RGB image, one in each plane, then the pre-processing unit extracts the RGB planes and then arranges all the three planes in a two-dimensional matrix so that each plane could be treated by the system as a P × Q grayscale plane, where P and Q respectively denote rows and columns of cover image. The resulting matrix values are brought in a range of −128 to 127 by subtracting 128 from the matrix.

After pre-processing the resultant matrix is divided into 16 × 16 blocks. For an input image of dimensions P × Q, the number of blocks will be $\frac{P}{16} \times \frac{Q}{16}$. Let an arbitrary block be represented by B_x. The block B_x is further divided into 8 × 8 blocks. The four 8 × 8 blocks of block B_x are represented by B_{x1}, B_{x2}, $B_{x3,}$ and B_{x4} as shown in Figure 1. Therefore, the total number of 8×8 blocks will be equal to $4 \times (\frac{P}{16} \times \frac{Q}{16})$. The total number of bits that could be inserted into a host image is equal to the total number of 8 × 8 blocks. The proposed technique utilizes the advantages of the DCT coefficient correlation of adjacent blocks. Therefore, DCT of each block (8 × 8) is calculated. Let the DCT coefficient blocks corresponding to block B_x be represented by C_{x1}, C_{x2}, C_{x3}, and C_{x4} (respectively for B_{x1}, B_{x2}, $B_{x3,}$ and B_{x4}) as shown in Figure 2. To embed a watermark bit, the difference between two preselected DCT coefficients of two neighboring blocks is calculated and is given as

$$D = C_{xy}(i, j) - C_{xy+1}(k, l) \tag{4}$$

where (i, j) ≠ (k, l), gives the position of the selected coefficient within a sub-block and 1≤i,j,k,l≤8. x = 1,2,3,4, …., P/16×Q/16; whose value represents to which 16 × 16 pixel block the coefficient belongs while as y = 1,2,3,4 (whose value represents the 8 × 8 DCT block to which the coefficient belongs). For the current work i, j, k and l are respectively taken as 3, 3, 3 and 2. Note that $C_{x5} = C_{x1}$ as 4 Mod y = 0 as is clear from Figure 2.

From Equation (3) and Figure 2, it is clear that for embedding the first watermark bit the difference between coefficient chosen from Block C_{x1} and a coefficient chosen from block C_{x2} is calculated. Similarly, to embed the second watermark bit, the coefficients from the block C_{x2} and the block C_{x3} are chosen for the difference, for embedding third bit in block B_x the coefficients from block C_{x3} and block C_{x4} are chosen and for embedding fourth bit the blocks Cx4 and C_{x1} are taken for difference purpose. The difference 'D' is modulated according to the information bit to be embedded and the 'D' itself.

The difference is changed by adding one coefficient and subtracting another coefficient by a value of Δ/2, where Δ is the amount of modification that needs to be brought between the two DCT coefficients iteratively until the difference reaches a particular zone as described by Figure 3. This is done to ensure that the two coefficients are modified by an optimal value rather than by modifying only one coefficient by a large amount. In Figure 3, the regions defined above axis are for bit '1,' while the regions defined below the axis are for bit '0'. The modification factor is calculated as

$$\Delta_{xy} = \alpha \times \frac{DC(C_{xy}) - Median(C_{xy})}{DC(C_{xy})} \tag{5}$$

where α (ranges from 0.2 to 2.5) is the multiplication factor which decides the robustness of the system i.e., higher the value of α higher the degree of robustness and vice versa, $DC(C_{xy})$ is DC coefficient of DCT block C_{xy} and $Median(C_{xy})$ is median of first thirteen low-frequency coefficients [57].

From Equation (5), it is clear that the modification factor Δ is adaptive that means it is different to different blocks and hence results into high-quality watermarked images.

Before embedding watermark 'w', two-level encryption of the watermark is performed to boost its security. First, chaos encryption is applied to the watermark according to the following equations:

$$C'(x) = round(C(x) \times 10^4) \tag{6}$$

$$C''(x) = binary(C'(x)) \tag{7}$$

$$b(x) = xor\ of\ all\ the\ bits\ of\ C''(x) \tag{8}$$

where 'C' is the sequence generated by using chaos equation (1), $C'$is a four digit integer obtained by multiplying C with 104 and then rounded towards the nearest integer, C'' is the binary representation of sequence C' and 'b(x)' is the binary bit generated from $C''(x)$ as per equation (7), by XOR-ing all the bits of $C''(x)$. The length of chaos sequence has been taken about one lakh, and out of this sequence only preselected 4096 values have been used. The first level encryption of the watermark is achieved by performing XOR operation between the sequences 'w' and 'b' as given by equation (9).

$$w_{e1} = w(x)\, XOR\, b(x) \tag{9}$$

Where 'w_{e1}' is the watermark, after the first level of encryption. Secondly, the Arnold transform is performed on

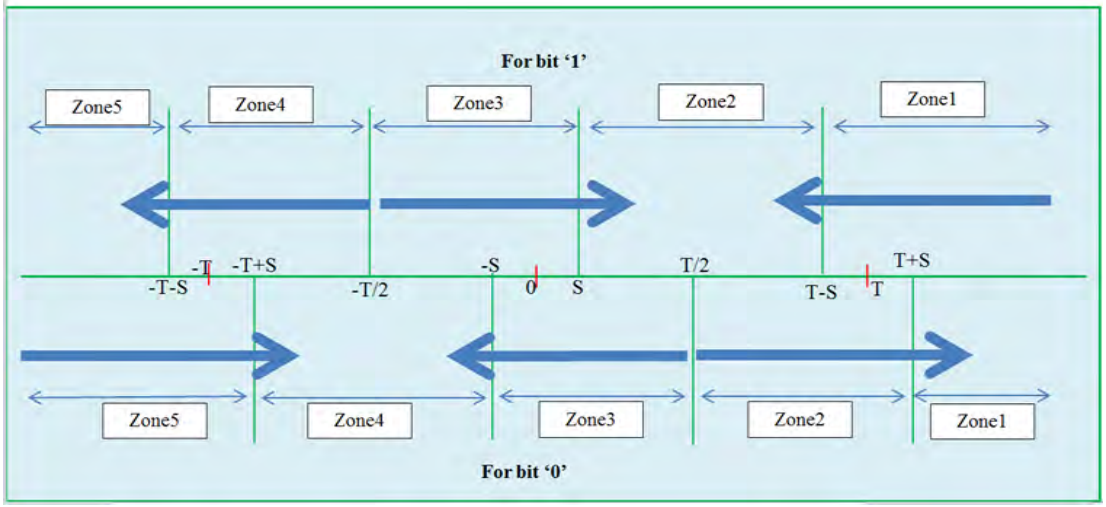


FIGURE 3. Zones and modification.

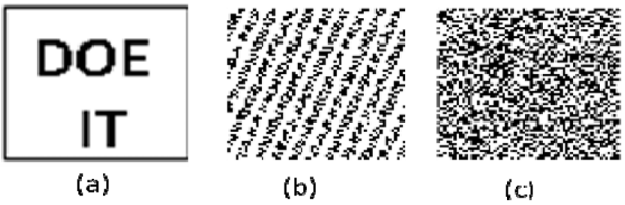


FIGURE 4. (a) Original watermark, (b) first level encrypted watermark and (c) second level encrypted watermark.

the sequence 'w_{e1}' to get the second level encrypted watermark 'w_e'. The input and encrypted watermarks are presented in Figure 4. The principle advantage of these two encryption methods is that we do not need a large overhead of keys. The number of iterations, initial value, and the logistic mapping parameter are the only keys that have to be used at the receiver to decrypt the encrypted data. However, the security of watermark, in this case is not so high because once we know the values of μ, C_0, and L, we can generate the exact sequence by using equation 1 and hence decrypt the watermark easily. To secure the parameters we have used different keys for the selection of different parameters in equation 1. The logistic parameter 'μ' is restricted to a range of 1.34 to 3.9 and is calculated by using an 8-bit key as given below:

$$\mu = 1.35 + \frac{decimal(K_1)}{100} \tag{10}$$

Where K_1 is an 8-bit key and gives security to the logistic parameter. Similarly, the initial value C_0 calculated by using a four-bit key K_2 is given by the following equation:

$$C_0 = 0.1 + \frac{decimal(K_2)}{17} \tag{11}$$

The value of C_0 ranges between 0.1 and 0.9. The number of chaotic values 'L' in the chaotic sequence is calculated by using a 19-bit key K_3, as given by the following equation:

$$L = 4096 + decimal(K_3) \tag{12}$$

The chaotic sequence 'C' is divided into chunks, each chunks of 2048 sample long. Let the total number of chunks be n_c. Out of these chunks only two chunks are selected and eight bits are used to select each chunk. Therefore, a total of 16 bits are required to select the two chunks. Let K_4represent the address of one chunk then the address of second chunks is calculated as

$$K_5 = n_c - decimal(K_4) \tag{13}$$

where K_5 represents the address of the second chunk. These two chunks are combined to form a sequence of 4096 value which is exactly the length of our watermark. The equations 5-8 are used to encrypt the watermark at the first level. At the second level of encryption, the only key for Arnold transform is the number of iterations which is selected by using a 6-bit key K_6. Therefore, a master key K of 53 bits is used to enhance the security of our watermark, where

$$K = K_1 : K_2 : K_3 : K_4 : K_5 : K_6 \tag{14}$$

C. JUSTIFICATION ABOUT THE PARAMETERS 'μ', AND 'C0'

The logistic parameter 'μ' in equation (10) is restricted to a range of 1.35 to 3.9 because this range of 'μ' produces the chaotic values with highest chaotic behavior at 3.9 which in turn provides high security to the watermark that is why we have chosen 'μ' between 1.35 to 3.9. The initial value C_0 in equation (11) can be any value between 0 and 1 that is why we chosen this by using a key in order to improve the security of the watermark.

D. WATERMARK EMBEDDING

For a given 16 × 16 block, we have to embed four bits of encrypted watermark 'we', one between each pair of

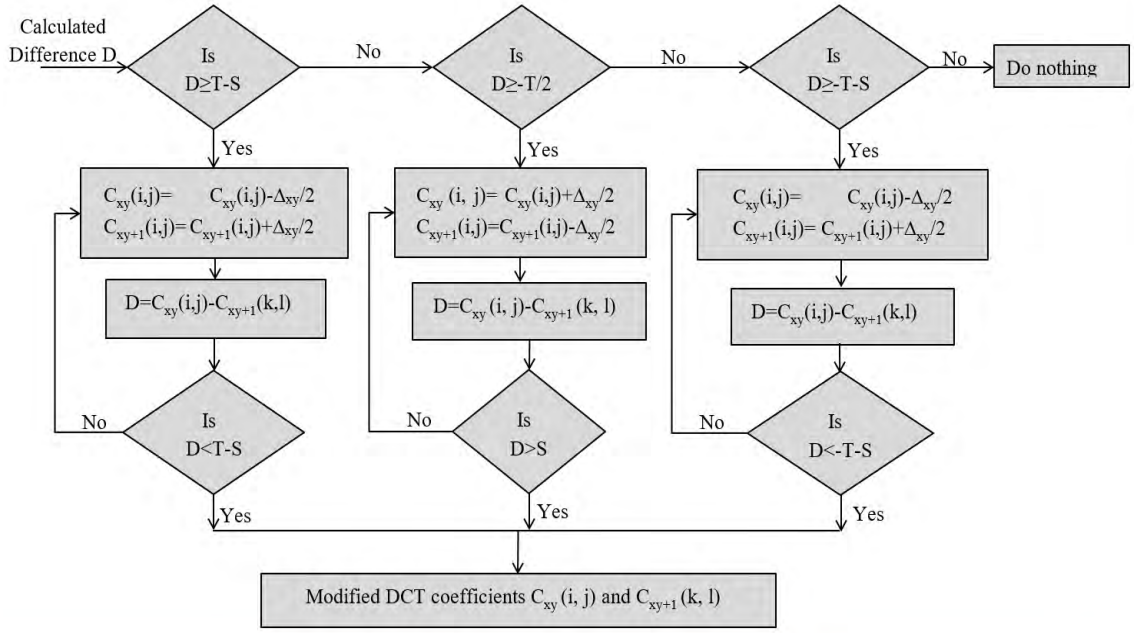


FIGURE 5. Flow chart for embedding bit '1'.

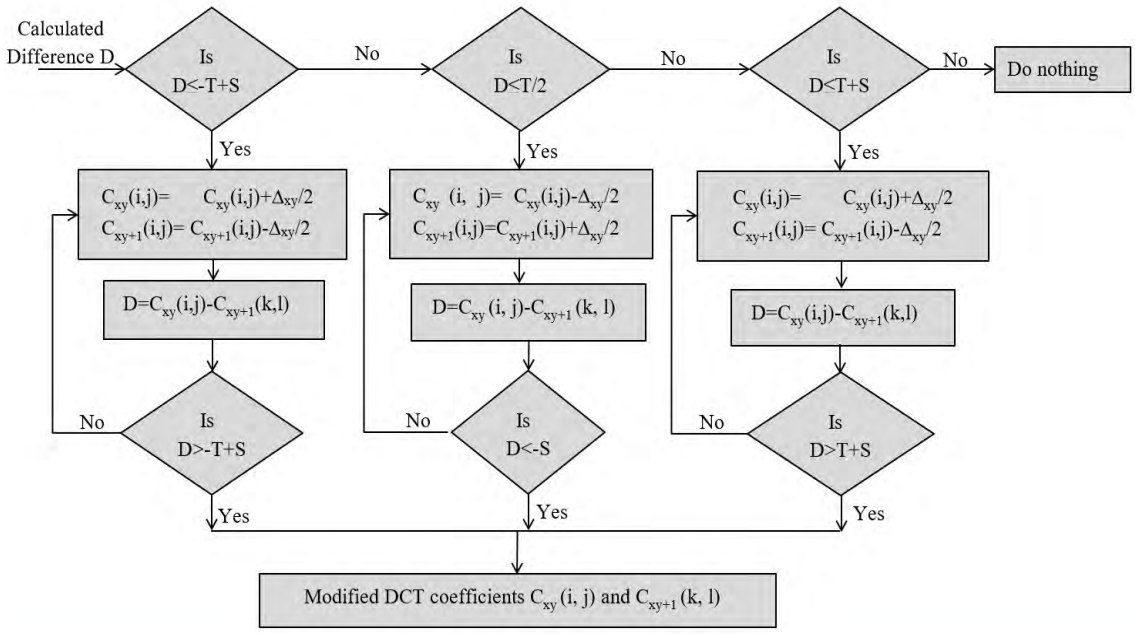


FIGURE 6. Flow chart for embedding bit '0'.

DCT blocks as shown in Figure 2. Figures 5 and 6 respectively show flow chart for embedding bits '1' and '0'.

For hiding bit '1', the 'D' is to be taken either to zone 2 or zone 5 depending upon the pre-embedding difference between two coefficients. If 'D' lies in zone 1 or 3 then the coefficients $C_{xy}(i, j)$ and $C_{xy+1}(k, l)$ are modified in such a way that the difference between them reaches to zone 2, which is the nearest zone. If the difference 'D' lies in zone 4 then the two selected coefficients are modified so that the difference reaches to zone 5. Thus, either zone 2 or zone 5 would carry the information about bit '1'. By modifying the difference to the nearest zone degrades the quality of the image by a small amount compared to its counterpart where the difference is modified to the farthest zone. Similarly, to embed bit '0', if the difference lies in zone 2, then it is modified to zone 1, and if it lies either in zone 3 or

zone 5, then it is modified to zone 4. This implies bit '0' information is stored either in zone 1 or zone 4. It is clear from Figures 3, 5 and 6 that the difference zones for a particular bit (zone 2, zone 5 for bit 1: or zone 1, zone 4 for bit 0) are separated by a guard band of 2S where S is the embedding strength which decides the robustness of the proposed watermarking system. This guard band brings extra robustness to our watermark, which has been discussed in the extraction part. The value of S in our work has been chosen in a range from 5 to 20. Robustness of the system is directly proportional to the value of S, while imperceptivity is inversely proportional to S. After complete embedding, inverse DCT (IDCT) of each modified DCT blocks is computed as shown in Figure 1. IDCT is followed by post-processing operations, which include addition of 128 to each element of the modified Blocks B∗x so that the pixel intensities ranging from 0 to 255. It also includes YCbCr to RGB conversion in case of luminance component embedding and conversion of a resulted matrix into three planes, which are basically the three-color planes for watermarked color image in case of RGB plane (i.e. one logo in each plane) embedding. The completion of post-processing operations produces the final watermarked image.

E. JUSTIFICATION ABOUT THE PARAMETERS A, S, AND T

From equation 5 and Figure 5, it is clear that the value of α plays a significant role in the calculation of the modification factor Δ_{xy} which is incremented to one predefined DCT coefficient and decremented from other coefficient iteratively, until the difference between these coefficient reaches to a specified zone which is decided by the threshold (T) and the embedding strength (S). The value of α can be chosen anything greater than zero but to prevent difference zones to overlap we have chosen it between 0.2 to 2.5. For this range the guard band of 2S is maintained between two information carrying difference zones that leads to the correct extraction of watermark.

The value of embedding strength (S) decides the width of an information carrying zone and has been chosen from 5 to 20 because of the reason that for such range of S the quality of the watermarked images is maintained to an acceptable level. The highest quality is obtained at at $S = 5$ and it reduces as S is increased while robustness is directly proportional to S. Beyond $S = 20$, the quality of the images is degraded by a large amount while robustness is increased by very small amount compared to the range $5 \leq S \leq 20$.

F. WATERMARK EXTRACTION

Watermark extraction involves steps like pre-processing, the partition of the watermarked image into 16×16 blocks and 8×8 blocks; DCT computation is carried out in exactly the same way as in case of the watermark embedding process. Only those DCT coefficients which are modified during embedding are used for watermark extraction. A watermark bit is obtained by analysing the difference between the two predefined coefficients. If the difference lies anywhere in zone 2 or zone 5, bit '1' is obtained while bit '0' is obtained if the difference lies either in zone 1 or zone 4. As already discussed that between the information carrying zones there exists a guard band of 2S which is separating them from each other; hence, for extraction, S is considered as zero (i.e., each difference zone is extended on either side by S) so that a transition of difference from zone boundaries due to image processing operations may not lead to wrong bit extraction. This, in turn, makes our system more robust. After extracting all the bits from the marked image, the decryption process is utilized to obtain the original watermark.

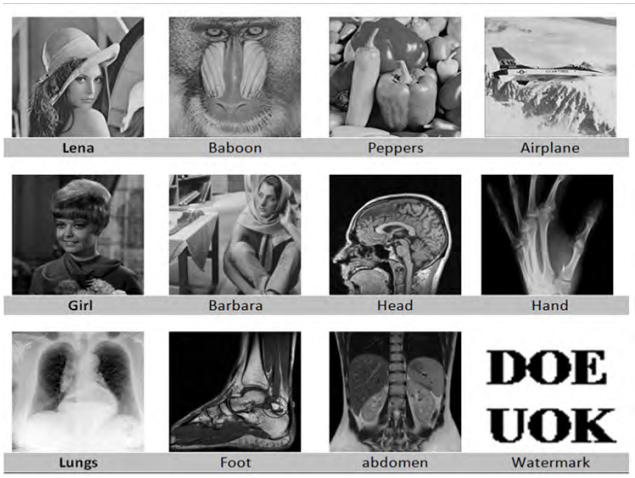


FIGURE 7. Grayscale images and a binary watermark.

IV. RESULTS AND DISCUSSIONS

The proposed watermark embedding algorithm has been examined for different grayscale and color images, each 512 × 512 in size as shown in Figures 7 and 8. The logo, as shown in Figure 7, has been used as the watermark for grayscale images while as the logos shown in the Figure 8 have been used for color images. All the three binary logos are 64×64 in size.

The objective performance of the proposed technique has been analyzed by using different objective image quality indices like Peak Signal to Noise Ratio (PSNR), Bit Error Rate (BER) and Normalized Cross-Correlation (NCC) defined as under:

$$BER = \frac{1}{mn}\left[\sum_{i=1}^{m}\sum_{j=1}^{n} w_o(i,j) \oplus w_x(i,j)\right] \tag{15}$$

$$NCC = \frac{\sum_{i=1}^{m}\sum_{j}^{n} w_o(i,j)w_x(i,j)}{\sum_{i=1}^{m}\sum_{j=1}^{n}[w_o(i,j)]^2} \tag{16}$$

where w_o(i ,j) is actual embedded logo bit at coordinates (i, j) and w_x(i,j) is the extracted logo bit at coordinates (i,j) and m×n is dimensions of logo. The values of BER and NCC of the system decide how robust the system is to image processing operations. Higher NCC and lower BER show that

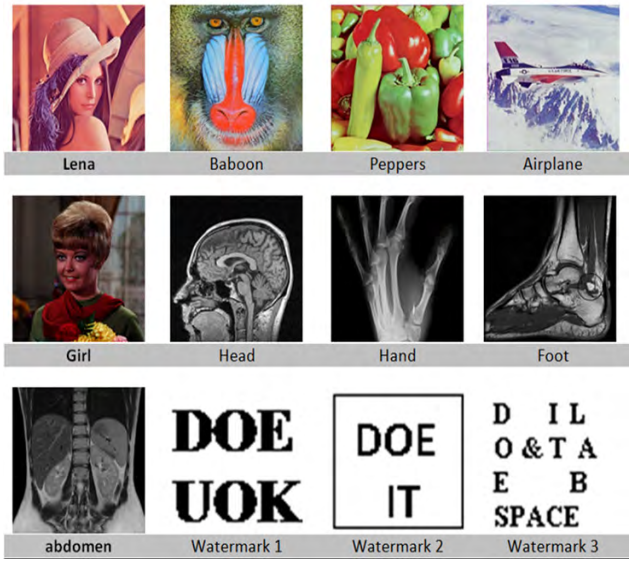


FIGURE 8. Color images and the watermarks.

the system is highly resilient to attacks.

$$PSNR = 10 \log \frac{(2^v - 1)^2}{MSE} \tag{17}$$

$$MSE = \frac{1}{MN} \sum_{l=1}^{M} \sum_{k=1}^{N} (H_{l,k} - E_{l,k})^2 \tag{18}$$

Here, 'v' is the minimum number of bits that can represent possible maximum intensity in a given image, H and E represent the host and marked image respectively and M and N respectively represent the number of rows and columns of the host image. PSNR is calculated to examine the quality of the watermarked image. Further, the quality of the watermarked images has also been evaluated using the structural similarity index SSIM as defined in [72] and [73].

A. PAYLOAD ANALYSIS

In this sub-section, we evaluate our technique for payload capability. The proposed technique is able to embed four bits of the logo in every 16 × 16 block. Consequently, the maximum number of logo bits that can be hidden in a 512 × 512 grayscale image is 4 × (512/16 × 512/16) = 4096 bits. The same number of bits could be hidden into an R, G, B image of the same size when embedding is carried in luminance component of the image; however, the payload is increased three times (i.e., 3 × 4096 = 12288 bits) when watermark is embedded into constituent channels: Red(R), Green (G) and Blue (B). A comparison of the payload of our technique with some existing schemes has been carried out. The results obtained are shown in Figures 9a and 9b, respectively for grayscale and color images. From the results, it is apparent that our technique performs better especially when watermark embedding is done in three channels (R, G, B) of the color image. In [54], for a N×N image, the maximum number of bits that can be embedded is N/4 because in general, a single bit is embedded in 4 rows and 4 columns of the image while

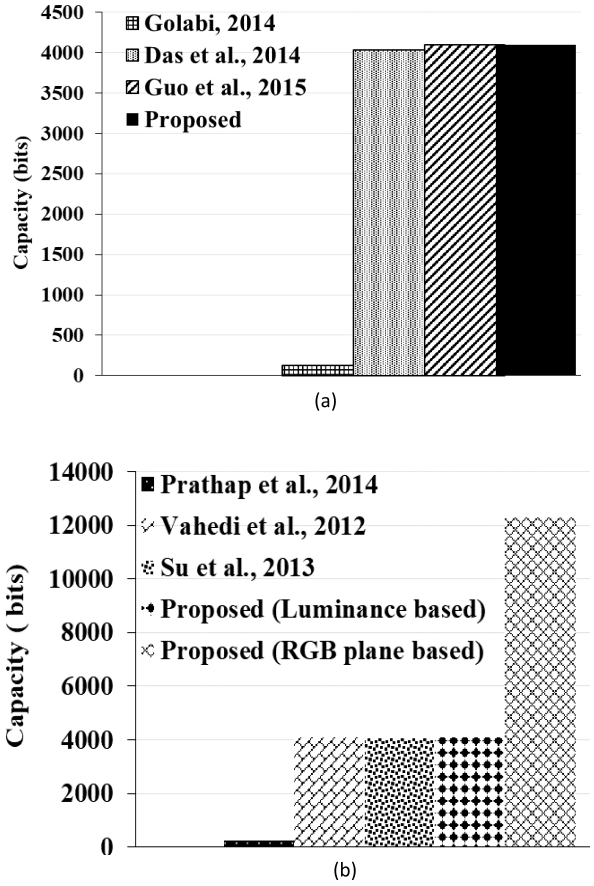


FIGURE 9. Payload comparison (a) for grayscale images and (b) for color images.

Das *et al.* [56] fail to embed the watermark bits in all the blocks which lead to the reduced payload. In [53], the watermark embedding is carried out only in less correlated high and low-frequency bands, while in [55] watermark embedding is done only in the luminance component of host image, which leads to reduced payload compared to our scheme where three copies of the watermark can be embedded in an RGB image.

B. IMPERCEPTIBILITY ANALYSYIS

This sub-section evaluates the quality of the marked images obtained after utilizing the proposed method of embedding. To examine the quality of watermarked images, SSIM and PSNR have been adopted as objective parameters. The proposed system produces high-quality images with high PSNR ranging from 39dB to 47.7dB in case of general test images, and 40.6 dB to 51 dB in case of medical images. The various grayscale watermarked images and respective extracted at S = 15 are presented in Figure 10.

The objective performance metrics for grayscale images have been reported in Table 1 and 2 for different values of 'S' when no attack is applied on the marked media. From Figure 10 and Table 1 and 2, it is clear that the subjective quality as well as objective quality of the watermarked images is high.

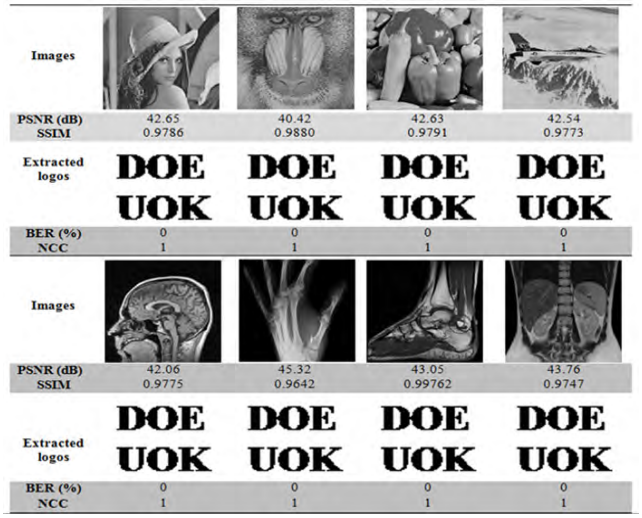


FIGURE 10. Watermarked images and extracted logos at S = 15.

TABLE 1. Objective image quality metrics for grayscale image at S = 5,10.

Images	S=5				S=10			
	PSNR (dB)	SSIM	BER (%)	NCC	PSNR (dB)	SSIM	BER (%)	NCC
Lena	46.31	0.9927	0	1	44.39	0.9868	0	1
Pepper	46.30	0.9924	0.02	0.99	44.37	0.9835	0	1
Plane	46.10	0.9935	0	1	44.23	0.9857	0	1
Barbara	44.16	0.9920	0	1	42.73	0.9823	0	1
Baboon	42.72	0.9940	0	1	41.55	0.9870	0	1
Girl	47.77	0.9920	0	1	45.41	0.9845	0	1
Hand	51.37	0.9905	0	1	47.90	0.9832	0	1
Head	45.40	0.9958	0	1	43.66	0.9856	0	1
Lungs	48.02	0.9920	0	1	45.57	0.9842	0	1
Foot	46.79	0.9934	0.02	0.99	44.16	0.9823	0	1
Abdomen	47.75	0.9916	0	1	45.68	0.9913	0	1

Further, logos are extracted from the marked media without any error, which validates the correctness of extraction algorithm. The value of embedding strength S has a great effect on the PSNR of watermarked images as is clearly seen in Tables 1 and 2.

A comparison of PSNR has been made with certain existing techniques as shown in Figure 11. The comparison results show that our technique produces high-quality grayscale images compared to the schemes under comparison. Figures 12 and 13 respectively show the watermarked images and the corresponding extracted logos for luminance component based embedding and RGB plane based embedding at $S = 15$. Besides high objective and subjective quality of color images, the proposed schemes are successfully able to extract the logos without any error as is evident from Figures 12 and 13.

A PSNR comparison has also been made with some deep learning methods [64] and [65] and results are reported

TABLE 2. Objective image quality metrics for grayscale image at S = 15, 20.

Images	S=15				S=20			
	PSNR (dB)	SSIM	BER (%)	NCC	PSNR (dB)	SSIM	BER (%)	NCC
Lena	42.65	0.9786	0	1	41.11	0.9681	0	1
Pepper	42.65	0.9772	0	1	41.10	0.9692	0	1
Plane	42.54	0.9805	0	1	41.04	0.9723	0	1
Barbara	41.37	0.9777	0	1	40.10	0.9689	0	1
Baboon	40.42	0.9856	0	1	39.34	0.9767	0	1
Girl	43.36	0.9736	0	1	41.64	0.9599	0	1
Hand	45.32	0.9576	0	1	43.29	0.9419	0	1
Head	42.06	0.9763	0	1	40.63	0.9657	0	1
Lungs	43.43	0.9724	0	1	41.67	0.9580	0	1
Foot	42.78	0.9750	0	1	41.30	0.9627	0	1
Abdomen	43.76	0.9747	0	1	41.93	0.9610	0	1

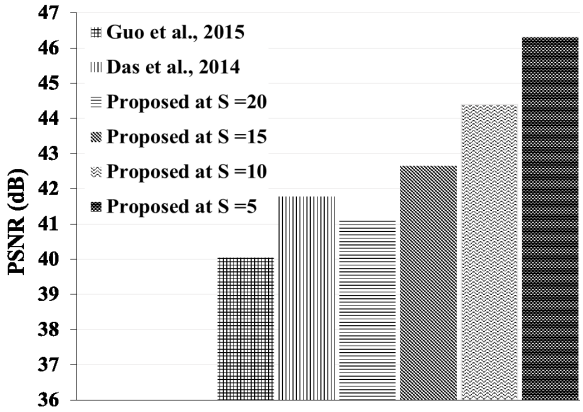


FIGURE 11. Comparison of PSNR for grayscale Lena image.

TABLE 3. PSNR comparison with deep learning methods.

Images	PSNR (dB)			
	Proposed Scheme1 (S=15)	[64]	Proposed Schene2 (S=15)	[65]
Lena	42.65	41.25	41.24	39.2
Baboon	41.37	41.67	38.89	35.9
Peppers	42.65	40.96	41.38	38.9

in Table 3 which clearly reveals that the proposed technique produces better quality watermarked images compared to those under comparison.

We also computed and compared the SSIM of our technique. The SSIM comparison for the two embedding approaches, for various test images (with different values of S), is presented in Figure 14.

A comparison of SSIM with [52] and [55] for color images is shown in Figure 15. The comparison results prove that our schemes outperform the schemes under comparison. Thus, the proposed scheme offers better quality watermarked

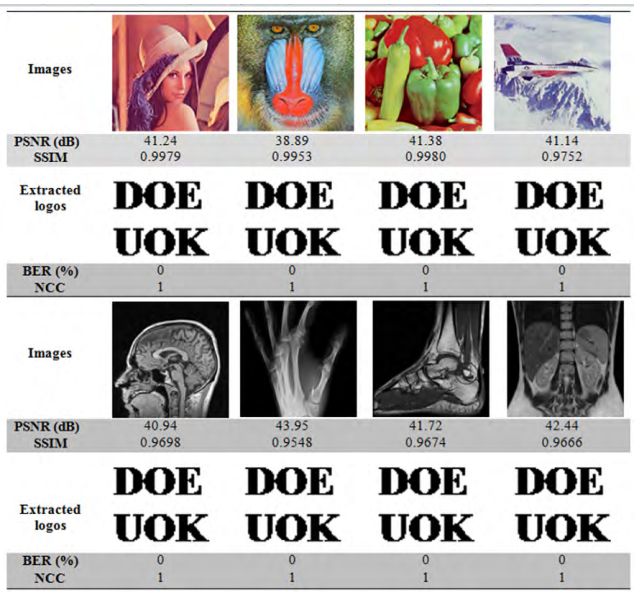


FIGURE 12. Watermarked images and the corresponding extracted logos for luminance component embedding scheme.

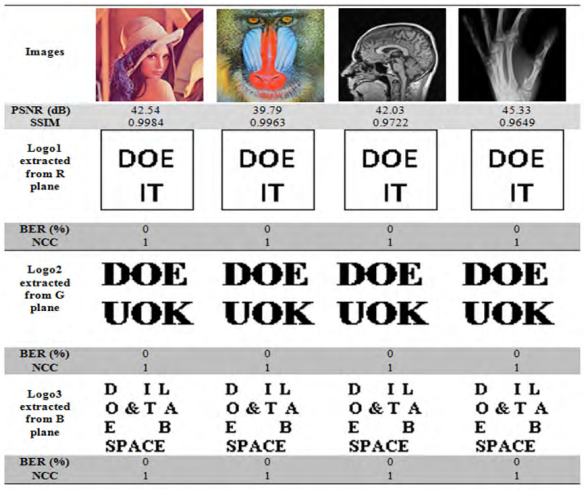


FIGURE 13. Watermarked images and the corresponding extracted logos for RGB plane based embedding scheme.

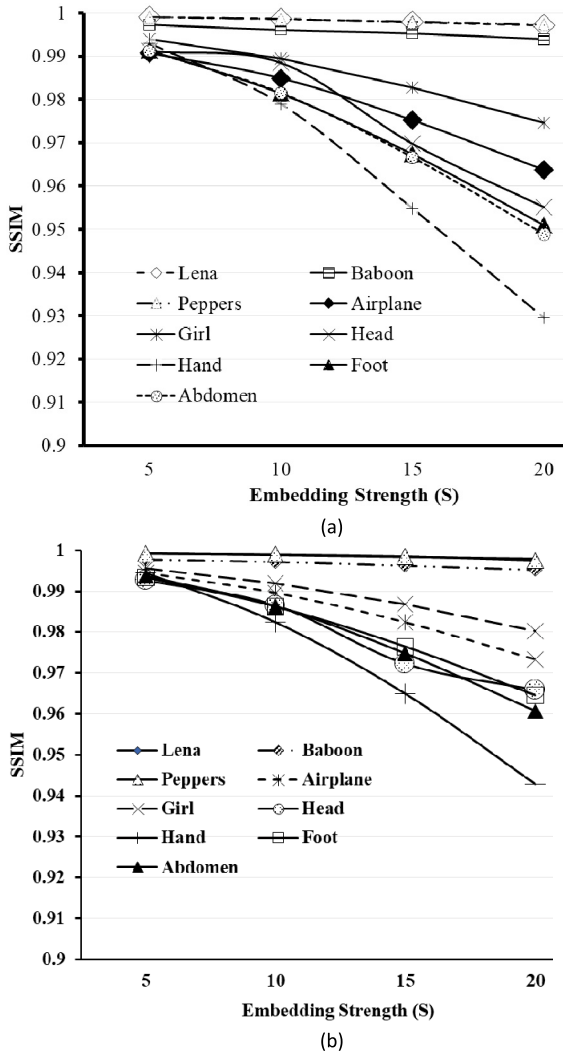


FIGURE 14. Comparison of SSIM for different images for different values of S: (a) luminance component based embedding scheme and (b) RGB plane based embedding scheme

images in both the cases, whether embedding is carried on grayscale images or on color images. Because in our watermarking system a watermark bit is embedded by modifying the two mid-frequency DCT coefficients of adjacent blocks by an optimal value which in turn leads to a small change in pixel domain compared to the techniques under comparison. In [52] and [62] watermark embedding is done in LL sub-band of DWT of the host image, which contains most of the visual information. Modification of the LL sub-band coefficients leads to a significant change in the pixel domain. In [52], 25% of the watermark is 4 times embedded in the LL3 sub-band coefficients of the 3-level DWT, while the 75% of watermark is embedded in rest of the three components of 3-level DWT coefficients. In [56] mid-frequency DCT coefficient of a block is modified by a large amount, which in turn reduces the quality of the watermarked image.

V. ROBUSTNESS ANALYSIS

A watermarking system is said to be robust if a recognizable watermark is obtained after applying an attack on the watermarked media. To investigate the robustness of our schemes, different attacks such as rotation, cropping, resizing, filtering, the addition of noise, etc. were applied on the watermarked images. The objective metrics like NCC and BER were adopted to evaluate the robustness of the system. Further, it is worth mentioning here that we attacked the watermarked images using two approaches: (a) single attack at a time and (b) a combination of two or more different attacks simultaneously. To make robustness analysis more exhaustive we considered three variants of the proposed scheme. The variants names are as per the Table 4.

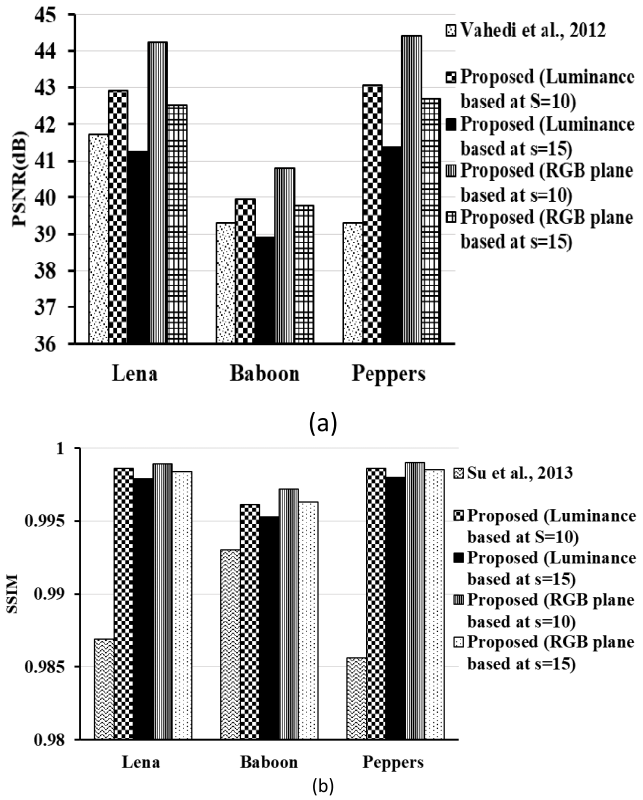


FIGURE 15. Comparison of objective quality metrics: (a) PSNR comparison for luminance component embedding scheme and (b) SSIM comparison for RGB plane based embedding scheme.

TABLE 4. Different variants of proposed scheme.

Name of the Proposed Scheme	Description of the Scheme
Proposed Scheme 1	When embedding is carried out in a grayscale image: No pre-processing of the image is required
Proposed Scheme 2	When embedding is carried out in a color image: The color image is transformed into YCbCr model and one logo is embedded in it.(this is also called as luminance component based embedding)
Proposed Scheme 3	When embedding is carried out in a color image: The color image is converted into three constituent Planes and each plane is considered as a monochrome image, thus three logos are embedded in it.

A. ANALYSIS FOR ROTATION ATTACK

The watermarked images are rotated by 1, 5, 10, 30 and 45 degrees. The watermarked images and the corresponding extracted watermarks after rotation of 10 degrees are shown in Figure 16 at $S = 15$.

It is evident from Figure 16 that recognizable logos are obtained from the rotated images, and the BER obtained is also less which implies that our system is resilient to rotation attacks. Further, BER of logos, extracted from rotated Lena image at different values of S is compared so that the effect of S on robustness could be seen. The comparison results are presented in Figure 17. The results clearly state that BER significantly reduces as the value of S increase which means robustness increases as value of S increases. Further, the results obtained have been compared with some related state of art techniques as shown in Figure 18. The comparison results clearly show the superiority of our technique.

TABLE 5. NCC comparison for cropping attack.

Algorithm	Cropping			
	25 % at top left corner	25 % at top right corner	25 % at bottom left corner	25 % at bottom right corner
Proposed scheme 1	0.9000	0.9027	0.9000	0.8976
Das et a1., 2014 [56]	0.9954	0.9973	0.9924	0.9981

B. ANALYSIS FOR CROPPING AND RESIZING ATTACK

Image cropping was done in such a way that 25% of the watermarked Lena image is cropped at different corners (i.e., bottom left, bottom right, top left and top right). A well identifiable logo is obtained from the cropped images as shown in Figure 19. The NCC results obtained are reported in Table 5. Although the objective analysis shows a lesser robustness but the subjective quality of the watermarked images obtained is good and are quite recognizable. Robustness of the system has also been tested for the resizing attack where the watermarked Lena image is resized to 0.5, 0.8, 1.2 and 1.6 times to that of original dimensions of the image. The images resized to 0.5 times and the watermarks obtained from them are presented in Figure 19. The figure clearly states that recognizable logos are obtained from the resized images which imply that our schemes are resilient to resizing as well.

The NCC results obtained for resizing attack are compared with some related techniques as given in Table 6. From the Table 6, it is clear that our schemes (1-3) outperform the techniques under comparison.

C. ANALYSIS FOR JPEG COMPRESSION ATTACK

JPEG compression is the most commonly used image processing operation to compress the image so that its storage requirement and its transmission time are reduced. Sometimes adversaries try to compress the watermarked images so that the copyright holder fails to prove his ownership. This is because of the fact that by compressing watermarked

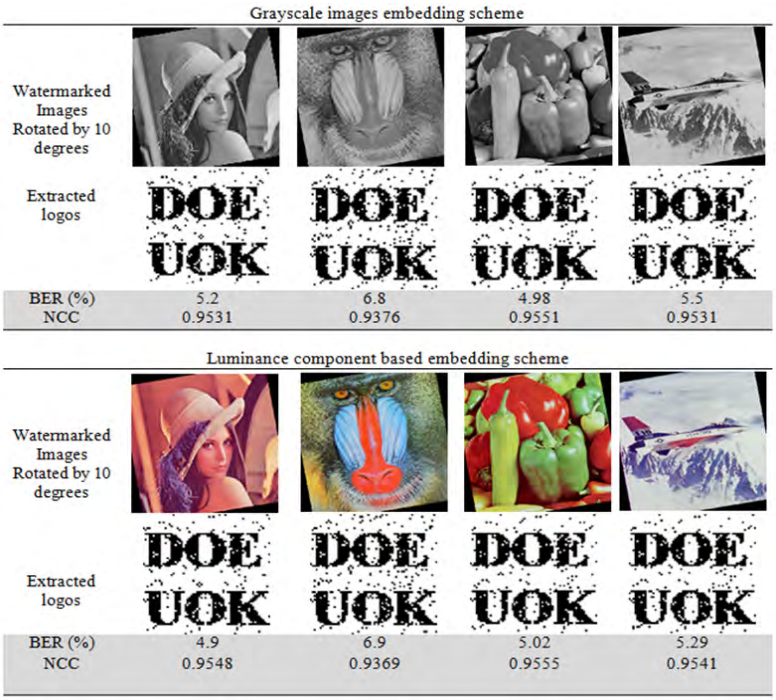


FIGURE 16. Rotated images and corresponding extracted watermarks.

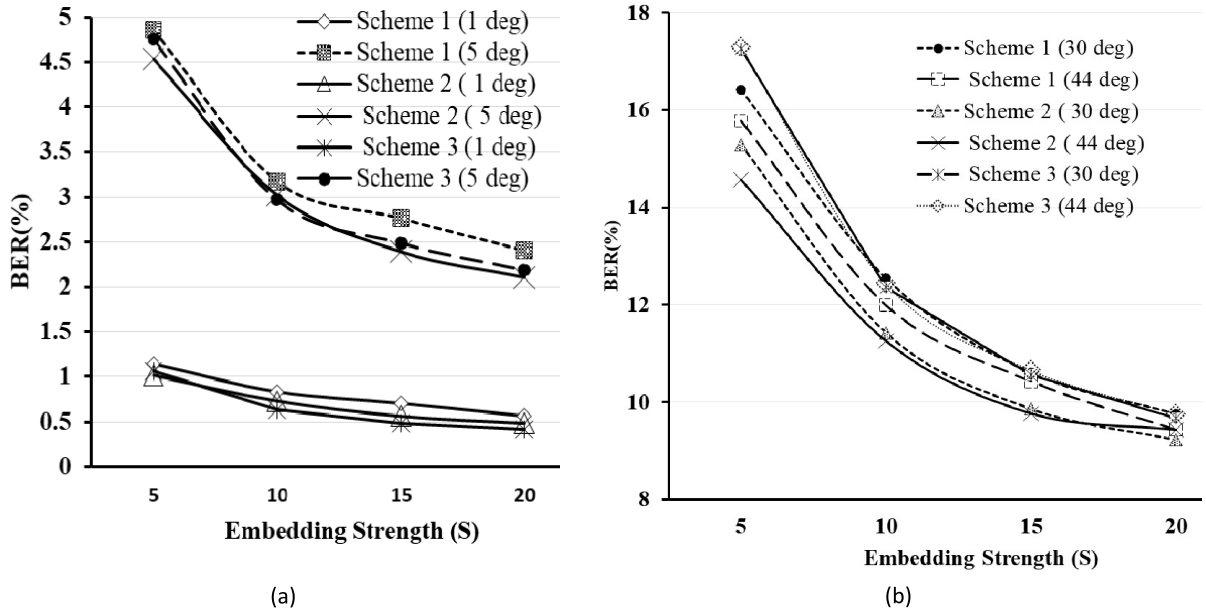
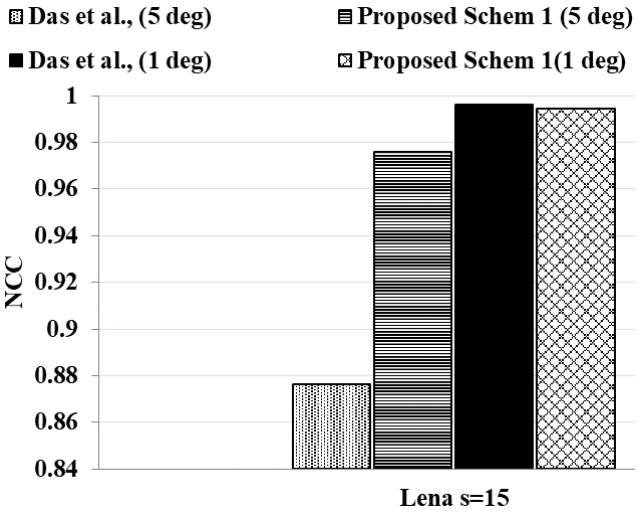


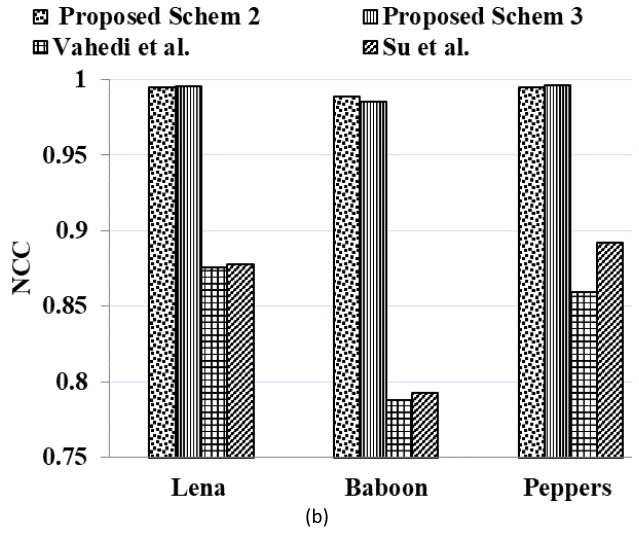
FIGURE 17. Comparison of BER for Lena image against the value of S and angle of rotation for proposed schemes: (a) 1 degree and 5 degrees and (b) 30 degrees and 44 degrees.

images by a large factor may lead to extraction of the non-recognizable watermark as JPEG compression truncates the high-frequency coefficients. Hence, the robustness of any watermarking system should also be examined for JPEG compression attack as well.

The performance of proposed schemes has been tested for JPEG compression at different quality levels (Q) and proposed schemes (1 and 2) are the better choice for such attack. Figure 20a and 20b show the performance of our schemes for JPEG compression at different quality levels for $S = 15$ and $S = 20$. The figures clearly show that proposed schemes are highly robust to JPEG compression as the $BER = 0$ and $NCC = 1$ up to the quality level of 50.



(a)



(b)

FIGURE 18. Comparison of NCC for rotation attack at $S = 15$: (a) between proposed scheme 1 and Das *et al.* [56] for 1 and 5 degrees and (b) between proposed scheme 2, proposed scheme 3, Vahedi *et al.* [52] and Su *et al.* [55] for 1 degree.

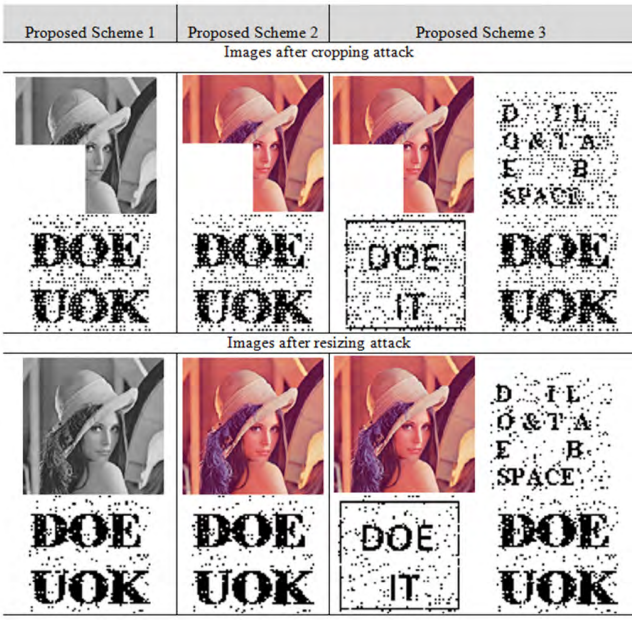


FIGURE 19. Cropped and resized watermarked images and their respective extracted logos.

TABLE 6. NCC comparison for resizing attack.

Image	Algorithm	Resizing Factor		
		0.8	1.2	1.6
Lena	Scheme 1	0.9979	1	1
	Scheme 2	0.9986	1	1
	Scheme 3	0.9958	0.9997	1
	[52]	0.9478	0.9388	0.9046
	[55]	0.9945	0.9965	0.9970
Baboon	Scheme 1	0.9414	0.9972	0.9969
	Scheme 2	0.9593	0.9986	0.9986
	Scheme 3	0.9374	0.9958	0.9964
	[52]	0.8608	0.8586	0.8144
	[55]	0.9444	0.9854	0.9840
Peppers	Scheme 1	0.9959	1	1
	Scheme 2	0.9938	0.9986	0.9986
	Scheme 3	0.9901	0.9972	0.9970
	[52]	0.9599	0.9633	0.8933
	[55]	0.9821	0.9865	0.9870

The results of our scheme 1 were compared with [56] and [62] in terms of BER. Figure 20c shows BER comparison of proposed scheme with [56], which implies that proposed scheme outperforms the scheme under comparison up to compression ratio 16.5. Further, it is worth mentioning here that BER of [62] for the quality level of 60 to 90 are respectively as 1% and 2.8%, while BER of the proposed scheme is zero for JPEG 60 to JPEG 90, which clearly state the superiority of the proposed scheme. Figure 20d shows the comparison of BER for various images against different values of S at the quality level of 40. It is evident that the robustness of our schemes for JPEG compression increases significantly as the value of S increases just by 5. Further, the NCC results of our scheme 2 were compared with [52] and [55] for the quality level of 60 and 90. The comparison results are reported in Table 7 for images like Lena, Baboon, and Peppers. The Table 7 shows that our schemes are more robust to compression attack than the schemes under comparison. Since mid-frequency coefficients are modified in our technique by an optimal value which leads to a high degree robustness toward the JPEG compression. In [52], the watermark is embedded in all the components (i.e., LL3, LH3, HL3, HH3) of 3-level DWT, which contains high-frequency coefficients. These coefficients are affected by a large factor when experiencing JPEG compression, hence low robustness. In [55] DC coefficient of a block of luminance component is

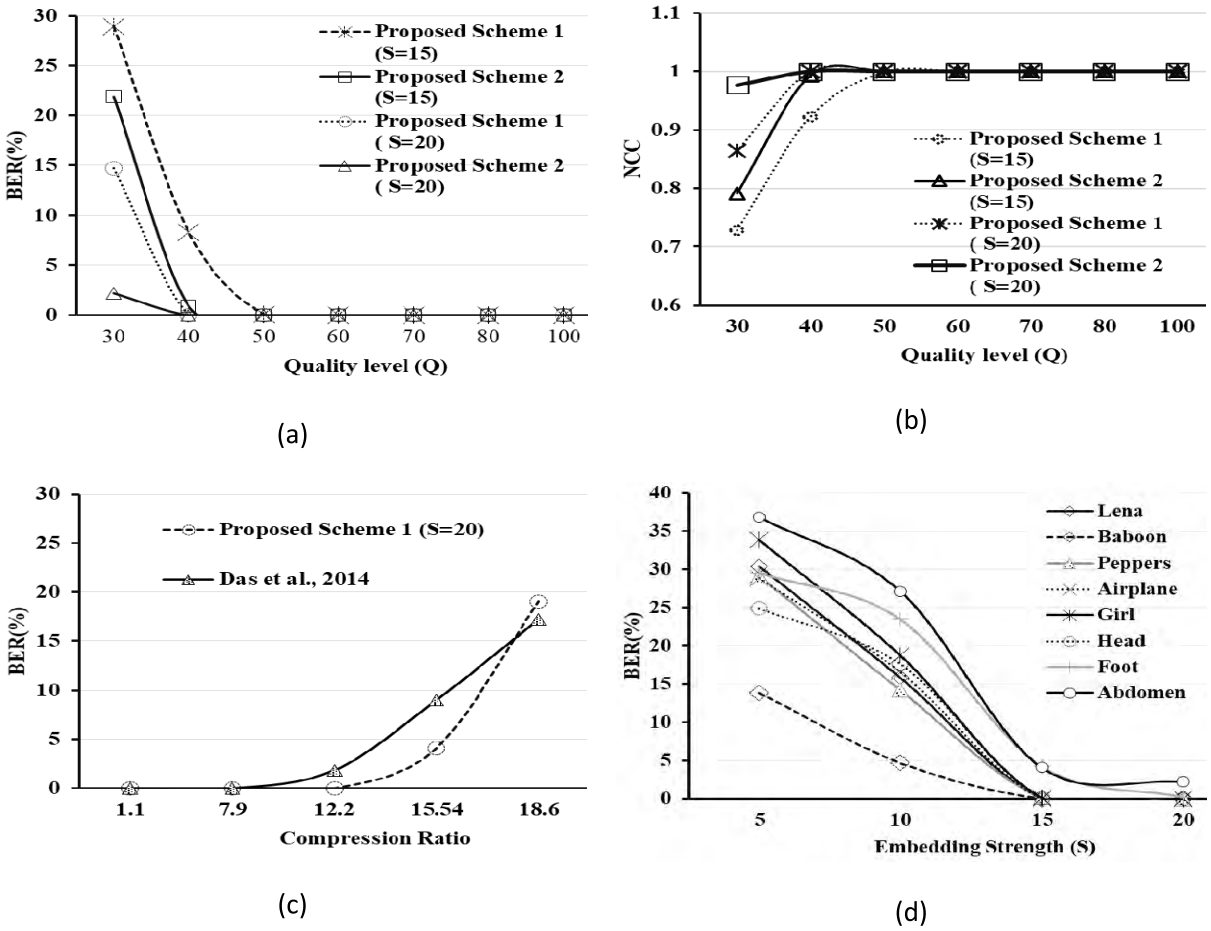


FIGURE 20. Performance of the proposed schemes against JPEG compression: (a) comparison of BER for Lena image at different quality level, (b) comparison of NCC for Lena image at different quality level, (c) comparison of BER for Lena Image against compression ratio and (d) comparison of BER for various images against different embedding strength (S).

TABLE 7. NCC comparison for JPEG compression at Q = 60 and Q = 90.

Algorithm	JPEG 60			JPEG 90		
	Lena	Baboon	Peppers	Lena	Baboon	Peppers
Scheme 2 (S=15)	1	1	0.9969	1	1	0.9986
Scheme 2 (S=20)	1	1	0.9986	1	1	0.9993
[52]	0.926	0.952	0.9248	0.9843	0.9891	0.9799
[55]	0.971	0.968	0.9642	0.9985	0.9980	0.9885

modified by a parameter whose value depends on the DC coefficient and the quantization step. The chosen quantization step does not make it resilient to higher compression levels.

D. ROBUSTNESS ANALYSIS AGAINST NOISE AND FILTERING ATTACKS

The watermarked images were subjected to salt and pepper noise of noise density 0.01 and with Gaussian noise of mean zero and variance 0.001. The results obtained are shown in Figure 21, which shows that the proposed schemes are robust to such distortions as recognizable watermarks have been extracted from the distorted Lena images. The robustness of the system was also tested for image filterings, such as 3×3 median filtering and low-pass filtering attacks. In the results shown in Figure 21, it is evident that our schemes are resilient to filtering attacks as well. Further, it was shown that the proposed schemes are also robust to histogram equalization and sharpening attack. The results are presented in Figure 21. Figure 22a shows BER comparison of the proposed scheme 1 for various test images for different values of S when attacked with the Gaussian noise of variance 0.001. While as Figure 22b shows NCC comparison of proposed scheme 2 for different variances of Gaussian noise. The results obtained for the proposed schemes have been compared with [52], [55], and [52], and the comparison results have been presented in Figure 23.

It is obvious from Figure 23 that our schemes outperform the schemes taken for comparison. This is due to the fact that, compared to the other techniques, the guard band of 2S in our technique plays a significant role during watermark extraction from the attacked images. This is because of the fact that during extraction the embedding strength S is kept

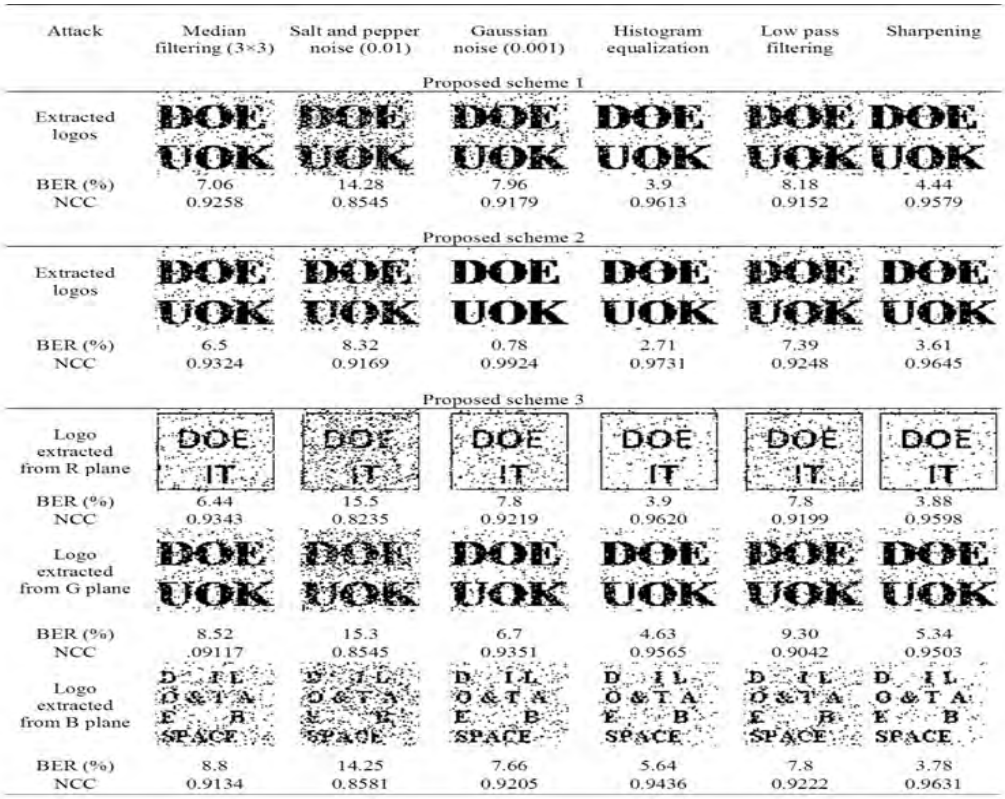


FIGURE 21. Subjective and objective analysis of the watermarks extracted from attacked Lena image.

as zero with this intention that each watermark information carrying difference zone (i.e., Zone 1,2,4,5) is to be extended from both sides by an amount of S. This zone extension enhances the robustness because, if the watermarked image is distorted, the difference between the coefficients (that have been used for embedding purpose) may be altered. This alteration must be large enough so that the difference could cross the boundary of the desired zone and then it would lead to a wrong bit extraction.

Further, it is worth mentioning here that the robustness of the proposed schemes has also been compared with some start of art deep learning techniques [64] and [65]. The comparison result is shown in Figure 24 which validates that the proposed schemes outperforms those under comparison.

E. ROBUSTNESS ANALYSIS FOR COMBINED ATTACKS

The performance of our techniques was also checked for simultaneous attacks wherein two or three different processing operations are applied to the marked image simultaneously. The following combination of two or three attacks was applied on watermarked images, and the results are presented in Figure 25 and Figure 26.

1. Watermarked Lena image has been attacked by salt and pepper noise of noise density 0.01, and then the distorted image is filtered by using 3×3 median filtering.
2. Watermarked Lena image has been firstly attacked by salt and pepper noise (density = 0.01), and then the attacked image is distorted by Gaussian noise (variance = 0.001).
3. Watermarked Lena image has been first distorted with Gaussian noise (variance = 0.001), and then it is compressed by using JPEG at the quality level of 70.
4. Watermarked Lena image has been compressed by using JPEG at the quality level of 70, and then 25% of the compressed image is cropped at top left corner.
5. Watermarked Lena image has been compressed by using JPEG at quality level of 70, and then the compressed image is resized to its 0.5 times.
6. Watermarked Lena image has been first rotated by 10 degrees, and then the rotated image has been resized to its 0.5 times.
7. Firstly, salt and pepper noise is applied to the watermarked image, secondly median filtering is performed, and finally, the filtered image is sharpened.
8. Histogram equalization is performed on the watermarked image, then this image is rotated by 10 degrees and finally, rotated image is cropped 25 % at top left corner.
9. Watermarked Lena image is first rotated by 10 degrees, then the rotated image is cropped 25 % at top left corner and finally the cropped image has been compressed by JPEG 70.
10. Histogram equalization is performed on the watermarked image, then the image is cropped 25 % at

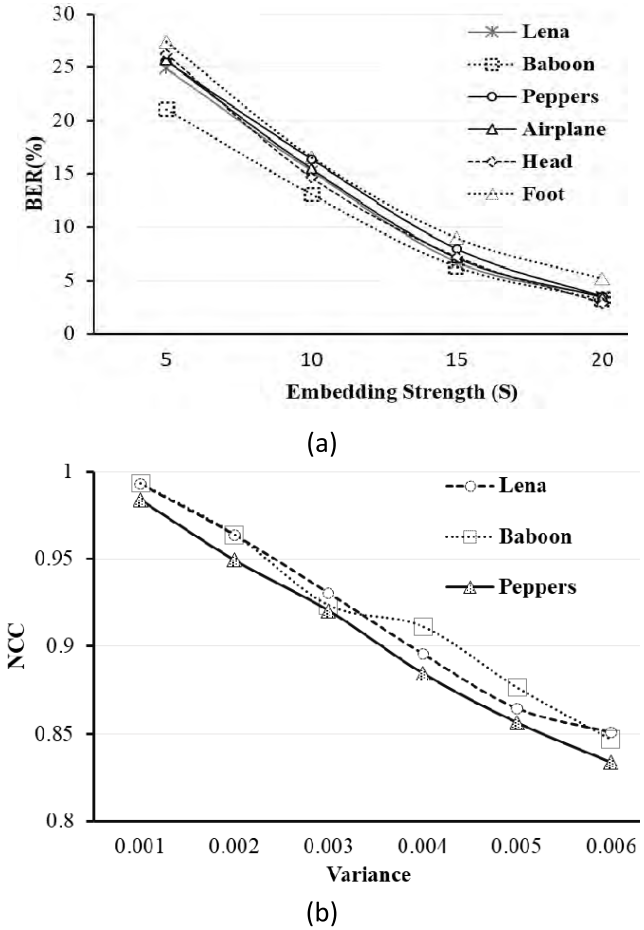


FIGURE 22. Performance of proposed schemes against Gaussian noise (a) BER comparison for proposed scheme 1 at variance = 0.001 and (b) NCC comparison for proposed scheme 2 at $S = 15$ against different variance.

top left corner, and finally, the image is resized to its 0.5 times.

After ten various combined attacks as discussed above we were able to retrieve recognizable watermarks as shown in Figure 25 and Figure 26. Hence the proposed schemes are robust to hybrid attacks.

VI. SECURITY ANALYSIS

According to the well-known Kirchhoff's principle [71], it is assumed that the technique of watermark embedding is known to the adversary. The only thing that an adversary needs to know is the encryption key used for watermark encryption. So, the selection of the key is an important factor that will decide the degree of security of an enciphered system. We carried the security analysis for the proposed scheme, and the results are presented below.

A. KEY SPACE ANALYSIS

In our proposed scheme we are using six different sub-keys for the selection of different parameters as discussed in section 3. These six sub-keys are used to form master key, 53 bits in length. This implies that the maximum possible number of keys is equal to 2^53. If we assume that computation power available with an adversary is such

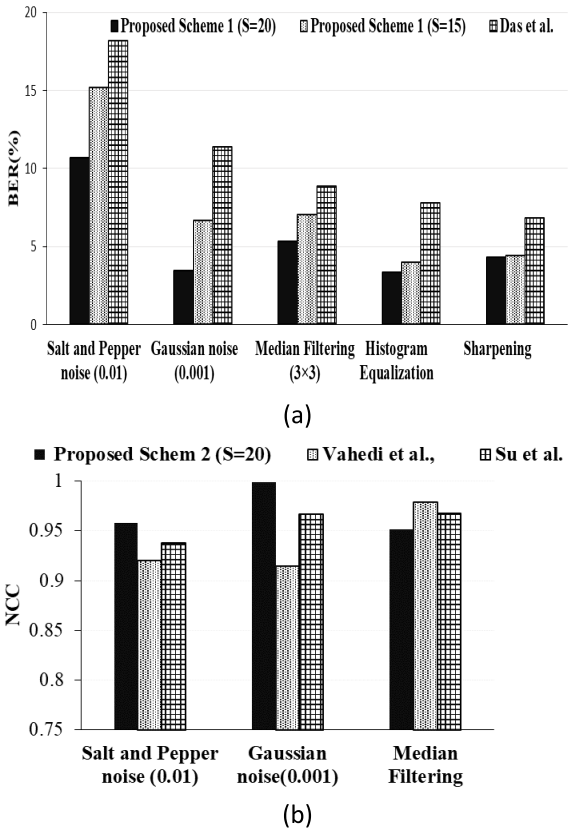


FIGURE 23. Performance comparison for Lena image (a) BER comparison at $S = 15$ and $S = 20$ and (b) NCC comparison at $S = 20$.

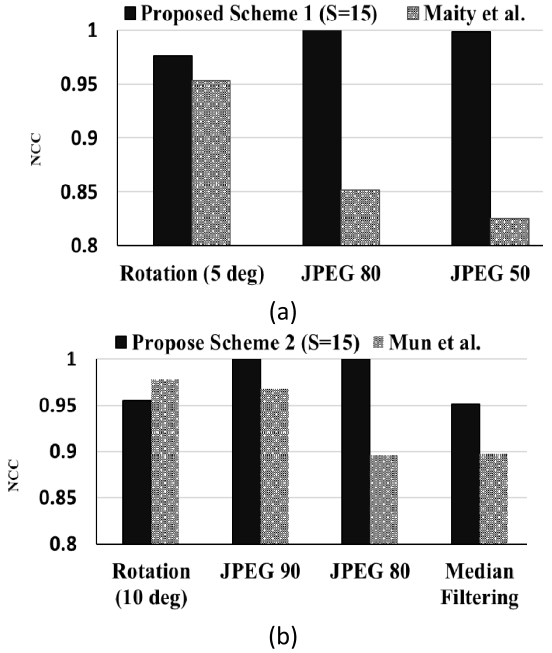


FIGURE 24. Performance comparison for Lena image (a) BER comparison at S = 15 and S = 20 and (b) NCC comparison at S = 20.

FIGURE 25. Performance of proposed schemes against the combination of two attacks on watermarked Lena.

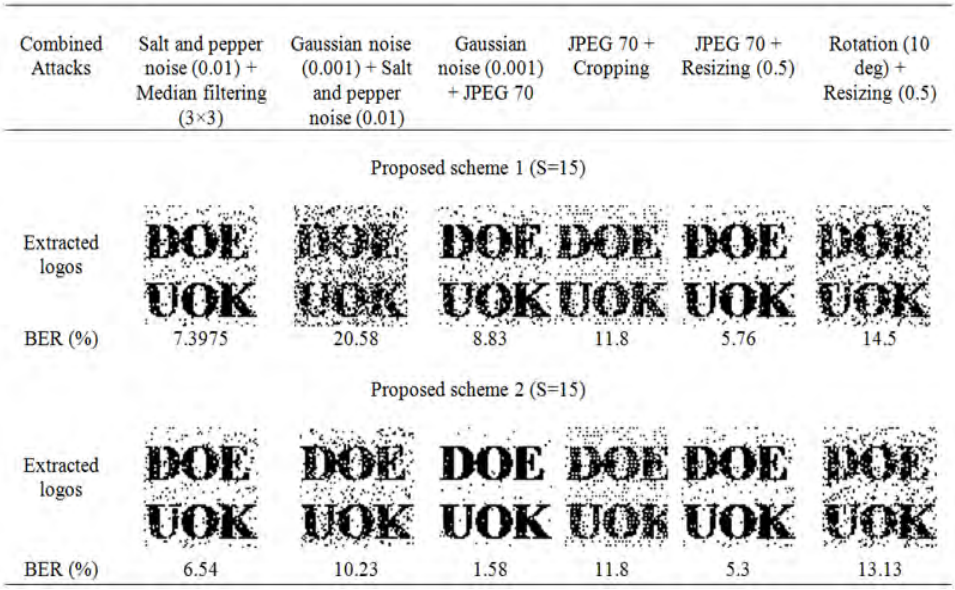


FIGURE 26. Performance of proposed schemes against the combination of three attacks on watermarked Lena image.

that it could generate one million keys per second, then it will take 289 years for it to break the proposed system. In addition to this, it is worth mentioning here that during the calculation of each and every key, involvement of human visual system is necessary as one has to get a well meaningful watermark. Hence, we can conclude from the argument that our scheme can resist any brute force attack.

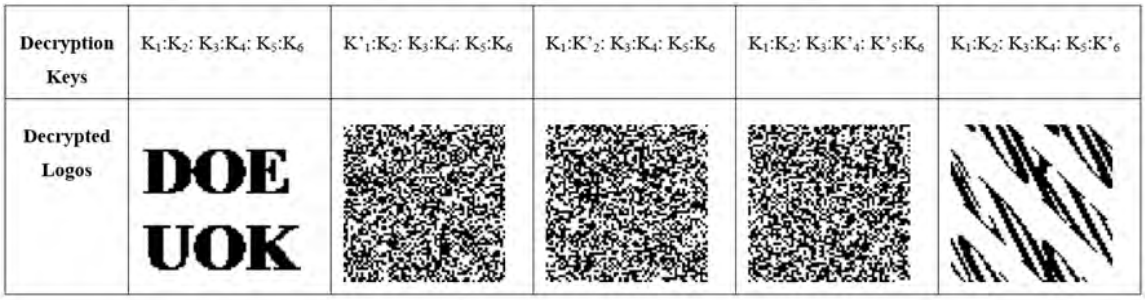


FIGURE 27. Decrypted logos corresponding to a given key.

B. KEY SENSITIVITY ANALYSIS

As far as key sensitivity is concerned, if a single bit of a key is changed, then decryption of an enciphered data must not be possible. In other words, we can say that if an adversary tries to decrypt an encrypted message with a key that differs from original key just by one bit, a wrong message must be extracted by the adversary. The key sensitivity of our encryption model is confirmed by modifying the LSBs of different keys one at a time. In our scheme the master key 'K' comprises six keys $K_1 = 255$, $K_2 = 7$, $K_3 = 405504$, $K_4 = 110$, $K_5 = 90$, $K_6 = 32$, and is given as

$$K = K_1 : K_2 : K_3 : K_4 : K_5 : K_6$$

The key sensitivity analysis has been performed by modifying keys K_1, K_2, K_4, K_5, K_6 whose new values are respectively given as $K'_1 = 254$; $K'_2 = 8$; $K'_4 = 111$; $K'_5 = 91$; $K'_6 = 31$. The resulting decrypted logos corresponding to each modified key are presented in Figure 27. From the figure, it is apparent that the key sensitivity of our encryption model is very high as an unrecognizable logo is extracted after decrypting it with a key that is different from original key just by one bit.

VII. FUTURE WORK

In future, the proposed algorithm will be tested for real time applications by implementing it on Field Programmable Gate Array (FPGA) platform.

VIII. CONCLUSION

A secure and blind watermarking scheme in the DCT domain was proposed in this paper. Arnold transform and chaotic encryption were utilized to add double layer security to the watermark. The proposed embedding technique is based on the difference between the coefficients of adjacent blocks. A watermark bit is embedded by modulating the difference between two preselected mid-frequency coefficients; one from reference block and other from its succeeding block. Depending upon the value of watermark bit to be embedded the difference between two coefficients of the selected blocks is made to lie in a predefined range to facilitate proper extraction. The performance of various variants of our scheme was tested for many image processing operations such as rotation, cropping, filtering, Gaussian noise, etc. The experimental results reveal that besides being resilient to singular attacks, our scheme is highly resilient to combined attacks as well. The comparison results depict that proposed scheme outperforms many state-of-art schemes in terms of imperceptibility, robustness, and payload. Further, the double layer of security of the embedded watermark ensures that the scheme is highly secure in nature. Given the merits of the proposed scheme, we conclude that it is well suited for the application of copyright protection and ownership verification. The scheme could be used to solve various medical image integrity and electronic patient record (EPR), security issues in contemporary telemedicine and e-healthcare setups.

REFERENCES

[1] H. Tao, L. Chongmin, J. M, Zain, and A. N. Abdalla, "Robust image watermarking theories and techniques: A review," *J. Appl. Res. Technol.*, vol. 12, no. 1, pp. 122–138, Feb. 2014.

[2] S. Voloshynovskiy, S. Pereira, T. Pun, J. J. Eggers, and J. K. Su, "Attacks on digital watermarks: Classification, estimation based attacks, and benchmarks," *IEEE Commun. Mag.*, vol. 39, no. 8, pp. 118–126, Aug. 2001.

[3] H. Nyeem, W. Boles, and C. Boyd, "Digital image watermarking: Its formal model, fundamental properties and possible attacks," *EURASIP J. Adv. Signal Process.*, vol. 2014, p. 135, Dec. 2014.

[4] N. Zivic, "Watermarking for Image Authentication," in *Robust Image Authentication Presence Noise*, 1st ed. Cham, Switzerland: Springer, 2015, pp. 43–47. [Online]. Available: http://www.springer.com/in/book/9783319131559

[5] S. A. Parah, F. Ahad, J. A. Sheikh, and G. M. Bhat, "Hiding clinical information in medical images: A new high capacity and reversible data hiding technique," *J. Biomed. Inf.*, vol. 66, pp. 214–230, Feb. 2017, doi: http://doi.org/10.1016/j.jbi.2017.01.006.

[6] S. A. Parah, F. Ahad, J. A. Sheikh, and G. M. Bhat, "A new reversible and high capacity data hiding technique for E-healthcare applications," *Multimed Tools Appl.*, vol. 76, no. 3, pp. 3943–3975, Feb. 2017.

[7] S. A. Parah, J. A. Sheikh, J. A. Akhoon, N. A. Loan, and G. M. Bhat, "Information hiding in edges: A high capacity information hiding technique using hybrid edge detection," *Multimed Tools Appl.*, vol. 77, no. 1, pp. 185–207, 2018, doi: 10.1007/s11042-016-4253-x.

[8] S. A. Parah, F. Ahad, J. A. Sheikh, N. A. Loan, and G. M. Bhat, "Information hiding in medical images: A robust medical image watermarking system for E-healthcare," *Multimed Tools Appl.*, vol. 76, no. 8, pp. 10599–10633, Apr. 2017.

[9] R. Eswaraiah and E. S. Reddy, "Robust medical image watermarking technique for accurate detection of tampers inside region of interest and recovering original region of interest," *IET Image Process.*, vol. 9, no. 8, pp. 615–625, 2015.

[10] M. Benyoussef, S. Mabtoul, M. E. Marraki, and D. Aboutajdine, "Robust ROI watermarking scheme based on visual cryptography: Application on mammograms," *J. Inf. Process. Syst.*, vol. 11, no. 4, pp. 495–508, Dec. 2015.

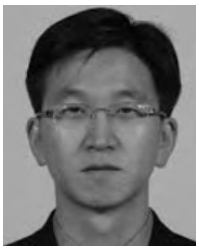
[11] L. Gao, T. Gao, G. Sheng, and S. Zhang, "Robust medical image watermarking scheme with rotation correction," in *Intelligent Data analysis and its Applications*. Cham, Switzerland: Springer, 2015, pp. 283–292.
[12] K. Muhammad, J. Ahmad, S. Rho, and S. W. Baik, "Image steganography for authenticity of visual contents in social networks," *Multimedia Tools Appl.*, vol. 76, no. 18, pp. 18985–19004, 2017. [Online]. Available: https://doi.org/10.1007/s11042-017-4420-8
[13] A. Kanso and M. Ghebleh, "An efficient and robust image encryption scheme for medical applications," *Commun. Nonlinear Sci. Numer. Simulat.*, vol. 24, nos. 1–3, pp. 98–116, Jul. 2015.
[14] K. Muhammad, M. Sajjad, I. Mehmood, S. Rho, and S. W. Baik, "A novel magic LSB substitution method (M-LSB-SM) using multi-level encryption and achromatic component of an image," *Multimedia Tools Appl.*, vol. 75, no. 22, pp. 14867–14893, 2016.
[15] M. M. Abd-Eldayem, "A proposed security technique based on watermarking and encryption for digital imaging and communications in medicine," *Egyptian Informat. J.*, vol. 14, no. 1, pp. 1–13, Mar. 2013.
[16] J. B. Lima, F. Madeiro, and F. J. R. Sales, "Encryption of medical images based on the cosine number transform," *Signal Process., Image Commun.*, vol. 35, pp. 1–8, Jul. 2015.
[17] B. Li, J. He, J. Huang, and Y. Q. Shi, "A survey on image steganography and steganalysis," *J. Inf. Hiding Multimedia Signal Process.*, vol. 2, no. 2, pp. 142–172, 2011.
[18] W. Luo, F. Huang, and J. Huang, "Edge adaptive image steganography based on LSB matching revisited," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 2, pp. 201–214, Jun. 2010.
[19] K. Muhammad, J. Ahmad, N. U. Rehman, Z. Jan, and M. Sajjad, "CISSKA-LSB: Color image steganography using stego key-directed adaptive LSB substitution method," *Multimedia Tools Appl.*, vol. 76, no. 6, pp. 8597–8626, 2017.
[20] K. Muhammad, M. Sajjad, I. Mehmood, S. Rho, and S. W. Baik, "Image steganography using uncorrelated color space and its application for security of visual contents in online social networks," *Future Generat. Comput. Syst.*, vol. 2, Nov. 2016. [Online]. Available: https://doi.org/10.1016/j.future.2016.11.029
[21] S. Das and M. K. Kundu, "Effective management of medical information through ROI-lossless fragile image watermarking technique," *Comput. Methods Programs Biomed.*, vol. 111, no. 3, pp. 662–675, 2013.
[22] D. Bouslimi, G. Coatrieux, M. Cozic, and C. Roux, "A joint encryption/watermarking system for verifying the reliability of medical images," *IEEE Trans. Inf. Technol. Biomed.*, vol. 16, no. 5, pp. 891–899, Sep. 2012.
[23] I. Cox, M. Miller, J. Bloom, J. Fridrich, and T. Kalker, *Digital Watermarking and Steganography*, 2nd ed. San Francisco, CA, USA: Morgan Kaufmann, 2007.
[24] C. I. Podilchuk and E. J. Delp, "Digital watermarking: Algorithms and applications," *IEEE Signal Process. Mag.*, vol. 18, no. 4, pp. 33–46, Jul. 2001.
[25] S. A. Parah, J. A. Sheikh, and G. M. Bhat, "On the realization of a secure, high capacity data embedding technique using joint top-down and down-top embedding approach," *Comput. Sci. Eng.*, vol. 49, pp. 10141–10146, Aug. 2012.
[26] C. C. Chang, P. Y. Lin, and J. S. Yeh, "Preserving robustness and removability for digital watermarks using subsampling and difference correlation," *Inf. Sci.*, vol. 179, no. 13, pp. 2283–2293, Jun. 2009.
[27] S. Bravo-Solorio and A. K. Nandi, "Secure fragile watermarking method for image authentication with improved tampering localisation and self-recovery capabilities," *Signal Process.*, vol. 91, no. 4, pp. 728–739, Apr. 2011.
[28] X. Wu, "Reversible semi-fragile watermarking based on histogram shifting of integer wavelet coefficients," in *Proc. DEST*, Cairns, Australia, 2007, pp. 501–505.
[29] Z. Ni, Y. Q. Shi, N. Ansari, W. Su, Q. Sun, and X. Lin, "Robust lossless image data hiding designed for semi-fragile image authentication," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 18, no. 4, pp. 497–509, Apr. 2008.
[30] C.-C. Lai and C.-C. Tsai, "Digital image watermarking using discrete wavelet transform and singular value decomposition," *IEEE Trans. Instrum. Meas.*, vol. 59, no. 11, pp. 3060–3063, Nov. 2010.
[31] C. I. Podilchuk and W. Zeng, "Image-adaptive watermarking using visual models," *IEEE J. Sel. Areas Commun.*, vol. 16, no. 4, pp. 525–539, May 1998.
[32] A. Benoraira, K. B. Mahammed, and N. Boucenna, "Blind image watermarking technique based on differential embedding in DWT and DCT domains," *EURASIP J. Adv. Signal Process.*, p. 55, Dec. 2015, doi: 10.1186/s13634-015-0239-5.
[33] N. Mohananthini and G. Yamuna, "Comparison of multiple watermarking techniques using genetic algorithms," *J. Electr. Syst. Inf. Technol.*, vol. 3, no. 1, pp. 68–80, May 2016.
[34] C.-T. Hsu and J.-L. Wu, "Hidden digital watermarks in images," *IEEE Trans. Image Process.*, vol. 8, no. 1, pp. 58–68, Jan. 1999.
[35] Y. K. Lin, "A data hiding scheme based upon DCT coefficient modification," *Comput. Standards Int.*, vol. 36, no. 56, pp. 855–862, 2014.
[36] K. Muhammad, J. Ahmad, H. Farman, Z. Jan, M. Sajjad, and S. W. Baik, "A secure method for color image steganography using gray-level modification and multi-level encryption," *Trans. Internet Inf. Syst.*, vol. 9, no. 5, pp. 1938–1962, 2015.
[37] K. Muhammad, M. Sajjad, and S. W. Baik, "Dual-level security based cyclic18 steganographic method and its application for secure transmission of keyframes during wireless capsule endoscopy," *J. Med. Syst.*, vol. 40, no. 5, p. 114, 2016.
[38] Y. Wang, K.-W. Wong, X. Liao, T. Xiang, and G. Chen, "A chaos-based image encryption algorithm with variable control parameters," *Chaos, Solitons Fractals*, vol. 41, no. 4, pp. 1773–1783, 2009.
[39] Y. Wang, K.-W. Wong, X. Liao, and G. Chen, "A new chaos-based fast image encryption algorithm," *Appl. Soft Comput.*, vol. 11, no. 1, pp. 514–522, 2011.
[40] V. Patidar, N. K. Pareek, G. Purohit, and K. K. Sud, "A robust and secure chaotic standard map based pseudorandom permutation-substitution scheme for image encryption," *Opt. Commun.*, vol. 284, no. 19, pp. 4331–4339, 2011.
[41] J. Fridrich, "Image encryption based on chaotic maps," in *Proc. ICSMC*, Orlando, FL, USA, 1997, pp. 1105–1110.
[42] S. Hakak, A. Kamsin, O. Tayan, M. Y. I. Idris, A. Gani, and S. Zerdoumi, "Preserving content integrity of digital holy quran: Survey and open challenges," *Access IEEE*, vol. 5, pp. 7305–7325, 2017.
[43] J. Won, S.-H. Seo, and E. Bertino, "Certificateless cryptographic protocols for efficient drone-based smart city applications," *IEEE Access*, vol. 5, pp. 3721–3749, 2017.
[44] L. Zhang and A. Li, "Robust watermarking scheme based on singular value of decomposition in DWT domain," in *Proc. APCIP*, Shenzhen, China, Jul. 2009, pp. 19–22.
[45] A. G. Bors and I. Pitas, "Image watermarking using DCT domain constraints," in *Proc. ICIP*, Lausanne, Switzerland, 1996, pp. 231–234.
[46] M. Jiansheng, L. Sukang, and T. Xiaomei, "A digital watermarking algorithm based on DCT and DWT," in *Proc. WISA*, Nanchang, China, 2009, pp. 104–107.
[47] T. Zong, Y. G. Xiang, S. Guo, and Y. Rong, "Rank-based image watermarking method with high embedding capacity and robustness," *IEEE Access*, vol. 4, pp. 1689–1699, 2016.
[48] F. Battisti, M. Carli, A. Neri, and K. Egiaziarian, "A generalized fibonacci LSB data hiding technique," in *Proc. IEEE 3rd Int. Conf. Comput. Devices Commun. (CODEC)*, Dec. 2006, pp. 1–4.
[49] S. Dey, A. Abraham, and S. Sanyal, "An LSB data hiding technique using natural number decomposition," in *Proc. IIHMSP*, Kaohsiung, Taiwan, 2007, pp. 473–476.
[50] M. Elbadri, R. Peterkin, V. Groza, D. Ionescu, and A. El Saddik, "Hardware support of JPEG," in *Proc. CCECE* Saskatoon, SK, Canada, May 2005, pp. 812–815.
[51] G. K. Wallace, "The JPEG still picture compression standard," *IEEE Trans. Consum. Electron.*, vol. 38, no. 1, pp. 18–34, Feb. 1992.
[52] E. Vahedi, R. A. Zoroofi, and M. Shiva, "Toward a new wavelet-based watermarking approach for color images using bio-inspired optimization principles," *Digit. Signal Process.*, vol. 22, no. 1, pp. 153–162, Jan. 2012.
[53] I. Prathap, V. Natarajan, and R. Anitha, "Hybrid robust watermarking for color images," *Comput. Electr. Eng.*, vol. 40, no. 3, pp. 920–930, 2014.
[54] S. Golabi, M. S. Helfroush, H. Danyali, and M. Owjimehr, "Robust watermarking against geometric attacks using partial calculation of radial moments and interval phase modulation," *Inf. Sci.*, vol. 269, pp. 94–105, Jun. 2014.
[55] Q. Su, Y. Niu, Q. Wang, and G. Sheng, "A blind color image watermarking based on DC component in the spatial domain," *Optik-Int. J. Light Electron Opt.*, vol. 124, no. 23, pp. 6255–6260, Dec. 2013.
[56] C. Das, S. Panigrahi, V. K. Sharma, and K. K. Mahapatra, "A novel blind robust image watermarking in DCT domain using inter-block coefficient correlation," *Int. J. Electron. Commun.*, vol. 68, no. 3, pp. 244–253, Mar. 2014.
[57] 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.

[58] J.-X. Chen, Z.-L. Zhu, C. Fu, L.-B. Zhang, and Y. Zhang, "An image encryption scheme using nonlinear inter-pixel computing and swapping based permutation approach," *Commun. Nonlinear Sci. Numer Simul.*, vol. 23, nos. 1–3, pp. 294–310, Jun. 2015.
[59] C. Dong, L. Jingbing, M. Haung, and Y. Bai, "The medical image watermarking algorithm with encryption by DCT and logistic," in *Proc. WISA*, Haikou, China, 2012, pp. 119–124.
[60] S. D. Lin, S.-C. Shie, and J. Y. Guo, "Improving the robustness of DCT-based image watermarking against JPEG compression," *Comput. Standards Interfaces*, vol. 32, pp. 54–60, Jan. 2010.
[61] S. D. Lin and C.-F. Chen, "A robust DCT-based watermarking for copyright protection," *IEEE Trans. Consum. Electron.*, vol. 46, no. 3, pp. 415–421, Aug. 2000.
[62] J. Guo, P. Zheng, and J. Huang, "Secure watermarking scheme against watermark attacks in the encrypted domain," *J. Vis. Commun. Image Represent.*, vol. 30, pp. 125–135, Jul. 2015.
[63] A. Ferdowsi and W. Saad. (Nov. 2017). "Deep learning-based dynamic watermarking for secure signal authentication in the Internet of Things." [Online]. Available: https://arxiv.org/abs/1711.01306
[64] S. P. Maity, S. Maity, J. Sil, and C. Delpha, "Perceptually adaptive MC-SS image watermarking using GA-NN hybridization in fading gain," *Eng. Appl. Artif. Intell.*, vol. 31, pp. 3–14, May 2014.
[65] S.-M. Mun, S.-H. Nam, H.-U. Jang, D. Kim, and H.-K. Lee. (Apr. 2017). "A robust blind watermarking using convolutional neural network." [Online]. Available: https://arxiv.org/abs/1704.03248
[66] A. Daneshgar and B. Khadem, "A self-synchronized chaotic image encryption scheme," *Signal Process., Image Commun.*, vol. 36, pp. 106–114, Aug. 2015.
[67] V. I. Arnold and A. Avez, *Ergodic Problems of Classical Mechanics*. (Advanced Book Classics). New York, NY, USA: Benjamin, 1968.
[68] M. Li, T. Liang, and Y. He, *Arnold Transform Based Image Scrambling Method*. Paris, France: Atlantis Press, 2013, pp. 1309–1316.
[69] L. Wu and J. Zhang, "Arnold transformation algorithm and anti-arnold transformation algorithm," in *Proc. ICISE*, Nanjing, China, 2009, pp. 1164–1167.
[70] W. Lingling, Z. Jianwei, and G. Qi, "Arnold transformation and its inverse transformation," *J. Micro Comput.*, vol. 14, pp. 1164–1167, 2009.
[71] G. Ye and K.-W. Wong, "An efficient chaotic image encryption algorithm based on a generalized Arnold map," *Nonlinear Dyn.*, vol. 69, no. 4, pp. 2079–2087, Sep. 2012.
[72] Z. Wang and A. C. Bovik, "A universal image quality index," *IEEE Signal Process. Lett.*, vol. 9, no. 3, pp. 81–84, Mar. 2002.
[73] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, "Image quality assessment: From error visibility to structural similarity," *IEEE Trans. Image Process.*, vol. 13, no. 4, pp. 600–612, Apr. 2004.
[74] S. A. Parah, J. A. Sheikh, U. I. Assad, and G. M. Bhat, "Hiding in encrypted images: A three tier security data hiding technique," *Multidim. Syst. Sign. Process.*, vol. 28, no. 2, pp. 549–572, Apr. 2017.
[75] Masilamani, "An efficient visually meaningful image encryption using Arnold transform," in *Proc. TechSym*, Kharagpur, India, 2016, pp. 266–271.
[76] N. A. M. Abbas, "Image encryption based on Independent Component Analysis and Arnold's Cat Map," *Egyptian Informat. J.*, vol. 17, pp. 139–146, Mar. 2016.

NAZIR A. LOAN is currently pursuing the Ph.D. degree with the Department of Electronics and IT, University of Kashmir. He is currently focusing on the development of robust watermarking algorithms for multimedia applications. He is an INSPIRE fellow of the Department of Science and Technology, Government of India.

NASIR N. HURRAH is currently pursuing the Ph.D. degree with the Department of Electronics and IT, University of Kashmir, under Visvesvaraya Ph.D. Scheme for Electronics and IT, sponsored by the Ministry of Electronics and Information Technology Government of India. He is currently focusing on the development of robust image watermarking techniques for copyright protection and authentication.

SHABIR A. PARAH received the M.Sc. and M.Phil. degrees and the Ph.D. degree in electronics from the University of Kashmir, Srinagar, in 2004, 2010, and 2013, respectively, in the field of signal processing and data hiding. He is currently an Assistant Professor with the Department of Electronics and IT, University of Kashmir. He has authored or co-authored over 100 papers in the journals and conferences of international repute. His fields of interest are signal processing, secure communication, and digital watermarking and steganography.



JONG WEON LEE was born in Seoul, South Korea, in 1966. He received the B.S. degree in electrical engineering from Ohio University in 1989, the M.S. degree in electrical and computer engineering from the University of Wisconsin–Madison in 1991, and the Ph.D. degree from the University of Southern California in 2002. He is currently a Professor with the Department of Software, Sejong University. His research interests include augmented reality, human–computer interaction, and serious game.

JAVAID A. SHEIKH received the M.Sc., M.Phil., and Ph.D. degrees in electronics from the University of Kashmir, Srinagar, in 2004, 2008, and 2012, respectively, in the field of communications and signal processing. He is currently an Assistant Professor with the Department of Electronics and IT, University of Kashmir. He has authored or co-authored over 60 research papers in international and national journals and conference proceedings. His fields of interest are wireless communications, design and development of efficient multi-in multi-out orthogonal frequency division multiplexing-based wireless communication techniques, spread spectrum modulation, digital signal processing, and electromagnetics.

G. MOHIUDDIN BHAT received the M.Sc. degree in electronics from the University of Kashmir, Srinagar, India, in 1987, the M.Tech. degree in electronics and the Ph.D. degree in electronics engineering from Aligarh Muslim University, Aligarh, India, in 1993 and 1997, respectively. He served as an Assistant Professor and an Associate Professor with the Department of Electronics and Instrumentation Technology, University of Kashmir. He is currently serving as a Professor in electronics engineering and as the Director of the Institute of Technology Zakoora. He has guided many research degrees leading to the award of M.Phil. and Ph.D. His major field of research is signal processing techniques and secure message communication. His present research interests include secure message communication, neural networks, and signal processing techniques for communication.