Hindawi
Advances in Multimedia
Volume 2020, Article ID 7912690, 12 pages
https://doi.org/10.1155/2020/7912690

*Research Article*

# Analysis of Digital Image Watermarking Techniques through Hybrid Methods

**Mahbuba Begum** [1] **and Mohammad Shorif Uddin** [2]

[1]*Mawlana Bhashani Science and Technology University, Tangail 1902, Bangladesh*
[2]*Jahangirnagar University, Dhaka 1342, Bangladesh*

Correspondence should be addressed to Mahbuba Begum; mahbuba327@yahoo.com

Received 22 February 2020; Revised 21 June 2020; Accepted 21 July 2020; Published 6 August 2020

Academic Editor: Patrick Seeling



Digital image watermarking is an attractive research area since it protects the multimedia data from unauthorized access. For designing an efficient and robust digital image watermarking system, the trade-off among imperceptibility, robustness, capacity, and security must be maintained. Various studies regarding this concern have been performed to ensure these requirements by hybridizing different domains, such as spatial and transform domains. In this paper, we have presented an analytical study of the existing hybrid digital image watermarking methods. At first, we have given a standard framework for designing a hybrid method that ensures the basic design requirements of watermarking for various applications. After a brief literature review, we compared and analyzed the complexity of several existing hybrid methods in a tabular form. The limitations and applications of these methods are also highlighted. Finally, we summarized the challenges of the existing methods and concluded the study by giving future research directions.

## 1. Introduction

Multimedia technology is improving day by day. Therefore, it is easy to modify, duplicate, reproduce, and distribute the digital image during communications via local networks and throughout the Internet with low cost and immediate delivery without quality degradation. Image security and privacy are a significant concern for the multimedia revolution. Digital image watermarking is a significant advancement of technology in recent years for identifying ownership information of copyright holders and providing multimedia security. This technology embeds the watermark data into a multimedia product (such as text, image, audio, and video) and later extracts or detects it from the watermarked product to assert the product [1]. Thus, the host data are protected by inserting the watermark data that cannot be removed or replaced by an eavesdropper. This technology ensures content authentication, integrity verification, and tamper resistance and produces highly protected images. The cover (or host) image quality and beauty are maintained by an invisible watermarking. In recent years, various methods have been proposed based on either spatial or transform domain or both. The spatial domain method embeds the watermark by modifying the pixel values in the host image. However, in the transform domain, the coefficients of transforms are modified. These transformations include discrete cosine transform (DCT), discrete Fourier transform (DFT), or discrete wavelet transform (DWT) [2]. The hybrid method combines any two or three transformations by maintaining a trade-off among imperceptibility, robustness, capacity, and security. However, in recent years, the transform domain algorithms have gained attention for their improved performance and almost replaced the spatial domain algorithms. Broadcast monitoring, ownership identification, fingerprinting, content authentication, integrity verification, and telemedicine security are important and the latest potential applications of digital image watermarking.

The contributions of this research are

(i) We present the current trends of hybrid methods

(ii) We identify the limitations of the state-of-the-art hybrid methods of digital image watermarking

(iii) We point out the challenges that must be addressed by future researchers

In this research, the existing hybrid domain-based digital image watermarking methods are reviewed in Section 2. The framework of the hybrid method is revised in Section 3. Section 4 contains the design requirements and classification of hybrid methods. After that, the paper makes comparative studies of these hybrid methods in a tabular form. Then, the paper lists some challenges and open research issues that must be addressed by future researchers. Finally, the last section concludes the study.

## 2. Literature Review

In recent years, many hybrid digital image watermarking methods have been developed for hiding data to take into account increasing robustness, capacity, and security by maintaining the visual quality of the watermarked image. The paper [3] proposed a discrete wavelet transform- (DWT-) and discrete cosine transform- (DCT-) based digital image watermarking technique for copyright protection. Here, the watermark image is encrypted using the Arnold transform. The system computes the block-based DCT of DWT LL subband, which provides better visual quality of the image to the human eye. Here, the watermark is embedded into the midfrequency DCT coefficient of the host image. The system is also robust against various attacks and performs better than a single DCT-based method. Another paper [4] combines DWT and singular value decomposition (SVD) for significant improvement of robustness and imperceptibility. Here, two-level (2L) DWT is applied to the host image, and then the watermark is embedded to the singular values of the 2L DWT subband (HL/LH). Hemdan et al. [5] proposed a hybrid watermarking technique based on DWT-SVD. Here, the wavelet fusion algorithm is used for embedding the watermark by using DWT and SVD. Their system is robust and provides better imperceptibility along with improving capacity. The lifting wavelet transform (LWT) and DCT are combined in a study [6], where the LWT is first applied to the host image. Then, the watermark is embedded in the DCT of the selected LWT subband. Here, the original host image is decomposed by using LWT. This paper does not require the original host image for extracting the watermark. Jane et al. [7] proposed a hybrid nonblind watermarking method that combines DWT and SVD for embedding data into the host image. Here, the host image is decomposed into four subbands (HH, HL, LH, and LL), and then SVD is applied to the LL subband. The diagonal singular value coefficients are modified with the watermark image. The experimental result shows significant improvement in peak signal-to-noise ratio (PSNR) values of the watermarked image. Their proposed method is robust against JPEG compression, Gaussian noise, scaling, filtering, cropping, and rotation. Another paper is proposed to protect medical data for telemedicine applications [8]. For transferring medical data over the network by maintaining robustness and security, this paper uses a hybrid method that combines DWT and DCT. Here, the medical host image is divided into two parts: nonregion of interest (NROI) and region of interest (ROI). Multiple watermark images are embedded into the ROI part, and the text watermark is embedded into the NROI part. Here, the Rivest–Shamir–Adleman (RSA) algorithm is applied to the text watermark before embedding for enhancing security. This hybrid method preserves the host image visual quality without any degradation after embedding the watermark. Another hybrid method is proposed based on DCT-DWT and autothresholding. The DCT is applied to the host image prior to DWT. The algorithm uses the best threshold value for choosing the best embedding region and ensures better imperceptibility and high robustness against scaling, cropping, rotation, noising, and compression attacks [9]. Another hybrid method is presented [10] that combines the DWT and DCT domains by maintaining robustness and imperceptibility. In this paper, DWT-DCT coefficients are selected for embedding the watermark based on the human visual system. Here, quantization index modulation (QIM) is applied to the DWT-DCT coefficients of the host image for improving the performance in terms of imperceptibility and robustness.

For color image watermarking, another method is proposed based on the SVD and DCT Walsh hybrid transform [11]. This method uses low-frequency coefficients for embedding the watermark rather than middle-frequency transform coefficients of DCT. The experimental result shows significant robustness of this method against noise addition, histogram equalization, compression, and cropping attack. For securing medical images, another method combines DWT, DCT, and SVD for improving the robustness of the system [12]. Here, an invisible watermark image is embedded into the medical image. The third-level (3L) DWT is applied to the medical host image. Here, the high-frequency subbands of DWT coefficients of the medical host image are used. Then, DCT and SVD transformations are applied to the host image. The system ensures better imperceptibility and improved robustness against noise addition (Gaussian and salt-and-pepper noise), Wiener filter, average filter, and median filter. The LWT, DCT, and SVD are combined in another scheme [13] that uses edge detection for selecting the best region for embedding the watermark. The particle swarm optimization (PSO) algorithm has been used to maintain the trade-off between robustness and imperceptibility. The experimental result shows that the system is robust against various attacks and also preserves the host image quality. A frequency domain-based hybrid DCT-SVD-based method is presented in the paper [14] for ensuring more capacity. This robust watermarking technique uses the Arnold transform for texturizing the watermark logo. At first, two-dimensional (2D) DCT is applied to the host image, and then SVD of the watermark logo is taken. Different weights are selected according to the decreased singular values for minimizing the distortion of the host image. For protecting copyright information, two transform domain methods like discrete Fourier transform (DFT) and DCT are combined [15]. At first, DFT is applied

to the host image. The imperceptibility is achieved by using the DFT magnitude. Then, DCT is applied to this DFT magnitude of the host image that improves the robustness of the system. The watermark is encrypted by using the Arnold transform before embedding, and the watermark is embedded into the middle-band DCT coefficients of the host image. The method shows that there is no visual difference between the host image and the watermarked image. The system shows improved robustness against different kinds of attacks. In another study [16], at first different levels of DWT are applied to the host image, and then DCT is applied to it. Then, spread transform QIM is used for implementing the watermark embedding. The method shows significant improvement in terms of robustness and imperceptibility over the existing methods. A combination of DCT- and DWT-based robust color image watermarking method is proposed in another study [17]. At first, the RGB host image is divided into three components (red, blue, and green), and then DCT and DWT are applied to that image. Arnold transform encrypts the grayscale watermark image. The encrypted watermark is divided into equal smaller parts, and the DCT coefficient of each part is computed. After then, each DCT coefficient of the watermark part is embedded into the DWT subbands of the color host image. The experiment shows that the watermarked image is robust against resizing, noise adding, rotation, filtering, and JPEG compression attacks. Also, the system shows better imperceptibility compared to other methods. A combination of blind and nonblind watermarking technique is proposed where inner and outer watermarking techniques are used, respectively [18]. Here, a binary watermark image is embedded into the inner host image by using DWT with the help of the inner scheme. Then, the resultant inner watermarked image is embedded into the outer host image by using DWT and SVD. The watermark extraction is done in a reverse manner. This proposed system is robust against Gaussian noise, salt-and-pepper noise, Poisson noise, speckle noise, rotation, and JPEG compression. Apart from the idea of combining spatial and transform domain algorithms, current trends are integrating them with various machine learning and artificial neural network algorithms for improving the performance. These algorithms are used to find out the most effective embedding function. In 2020, an image watermark is proposed based on matrix factorization with Q learning which is a reinforcement learning model [19]. Here, Q learning is used to find out the appropriate host blocks for embedding by using the trial and error method. It has a better result for imperceptibility and robustness than random embedding. But, the performance against various attacks is not shown here. Another article is proposed that uses the support vector machine with a genetic algorithm [20]. Here, significant regions are selected by the fuzzy entropy, and then prominent low-frequency regions are calculated from these significant regions by the support vector regression model which increases robustness in a significant way than traditional methods. The watermark scaling factor (strength) is calculated here by the genetic algorithm—an optimization algorithm. Optimization algorithms, such as the genetic algorithm, particular swarm optimization, ant colony optimization, and firefly algorithm, are commonly used for finding the right embedding function or the right block for embedding [21–23]. The neural network is now becoming more popular than other machine learning algorithms. A spiking neural network (SNN) with DWT is proposed which has less time complexity, and the extraction problem is treated as an optimization problem that is solved by SNN [24]. Many works are done based on a neural network which then integrated with contourlet transform, Kurtosis coefficients, and YCbCr spaces besides the known frequency domains like DCT or DWT [24–26].

## 3. Framework of Hybrid Methods of Digital Image Watermarking

Digital watermarking technology is the way of altering multimedia data by adding information into the host media to protect its copyright information [27]. First, the system takes the host image and embeds the watermark image to it with the help of the embedding algorithm and the key. Then, the system gets the watermarked image and sends it over the communication channel. Finally, the system extracts the watermark image by using the watermark extraction algorithm and the key. Figure 1 shows the above procedure.

Digital watermarking can be done by either spatial or transform or hybrid domains. Spatial domain techniques do not provide high robustness against attacks or any manipulation [28]. For this concerned issue, transform domain techniques have gained attention for multimedia security [29]. However, due to the limited payload capacity of transform domain methods, hybrid domain methods are preferred in recent years [30]. In hybrid domain methods, two or more than two image transformations are used for watermarking. These hybrid domain methods are the extended versions of transform domain methods [31]. These methods provide more imperceptibility and high robustness to multimedia data and mainly used for multimedia security and copyright protection.

The hybrid digital image watermarking method takes the host image and applies two or more transform domain methods (DCT, DFT, DWT, and SVD) to it. This process is called hybridization. The watermark image is encrypted by any lightweight encryption method, and then the encrypted watermark image is divided into $n$-blocks. After then, the encrypted block-based watermark image is embedded into the host image. Here, $n$-places of the host image are selected randomly for embedding $n$-blocks of the encrypted watermark. Then, the inverse transformation is applied, and the watermarked image is finally obtained. The watermark extraction is done in a reverse manner. Figure 2 shows the framework of the watermark embedding for hybrid methods.

## 4. Design Requirements and Classification of Hybrid Image Watermarking

The digital image watermarking technique embeds data into an image in such a manner so that the data cannot be easily removed or destroyed. For effective watermarking, there

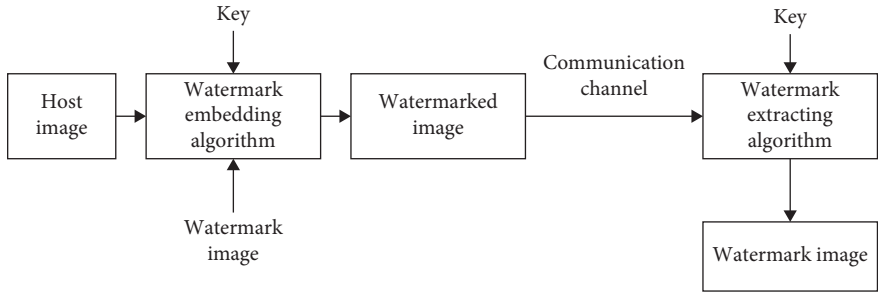


Figure 1: Watermark embedding and extraction.

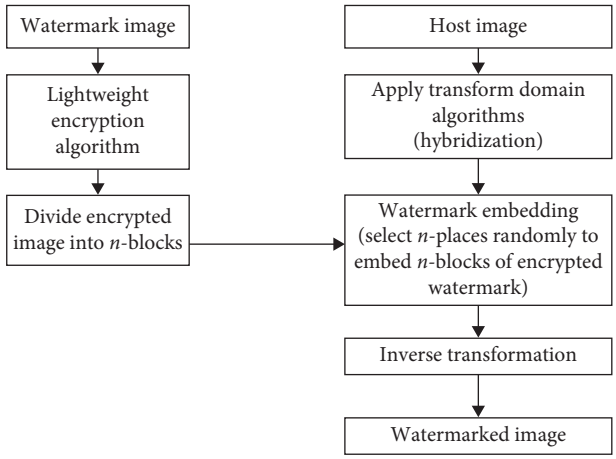


Figure 2: Framework of hybrid methods of digital image watermark embedding.

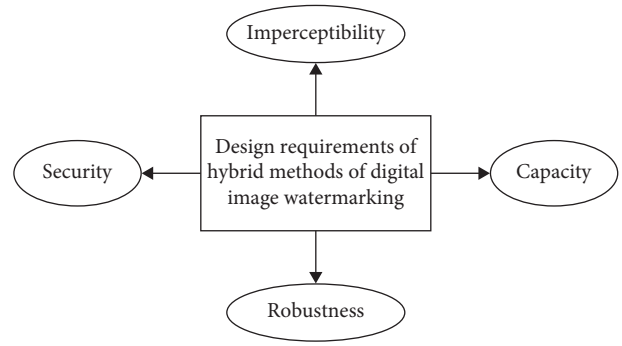


Figure 3: Basic requirements of hybrid digital image watermarking.

exist some design requirements. Moreover, hybrid watermarking can be done by combining various transform domain methods. This section discusses design requirements and the classification of hybrid digital image watermarking methods.

*4.1. Design Requirements of Hybrid Digital Image Watermarking.* Due to the Internet and multimedia, it is easy to duplicate, transmit, and distribute the digital image when it is transmitted over the Internet or the personal network. Therefore, to prevent unauthorized access, digital image watermarking adds information to the host media. Therefore, the system should be efficient. Some requirements must be satisfied for designing efficient hybrid digital image watermarking methods. Among other requirements, the four basic requirements are imperceptibility, robustness, capacity, and security. These requirements are depicted in Figure 3.

Imperceptibility is one of the important requirements of hybrid digital image watermarking methods that evaluates the performance of the watermarking system. It means there is no visual difference between the host image and the watermarked image. They are perceptually indistinguishable to human eyes even after degradation in brightness or contrast [27, 32]. Robustness is the requirement where the watermark image can still be detected after the watermarked image has been affected by some common image processing operations. These operations include scanning, printing, scaling, translation, spatial filtering, rotation, color mapping, and lossy compression [27]. Robustness can be categorized into robust, fragile, and semifragile. Payload capacity evaluates the amount of embedded information to the host image based on the host image size. But, inserting more watermark bits to the host image is a difficult task that depends on practical applications [33]. Security is an important design requirement for fingerprinting, copyright protection, data authentication, and digital content tracking. Security is confirmed by encrypting the watermark image with various encryption methods. These include the Arnold transform, chaos-based method, DCT, and logistic map-based methods. These methods ensure the security and confidentiality of the watermark image [34].

*4.2. Classification of Hybrid Methods of Digital Image Watermarking.* Based on the working domain, the digital image watermarking can be classified as spatial, transform, or hybrid domains. The spatial domain methods include the least significant bit (LSB), intermediate significant bit (ISB), or patchwork algorithm. On the other hand, transform or frequency domain methods include DCT, DFT, DWT, and SVD. The hybrid domain method combines two or more transform domain algorithms. These include DCT and DFT, DCT and DWT, DCT and SVD, DFT and DWT, DFT and SVD, DWT and SVD, and a combination of DCT, DFT, and DWT and others. The classification of digital image watermarking is shown in Figure 4.

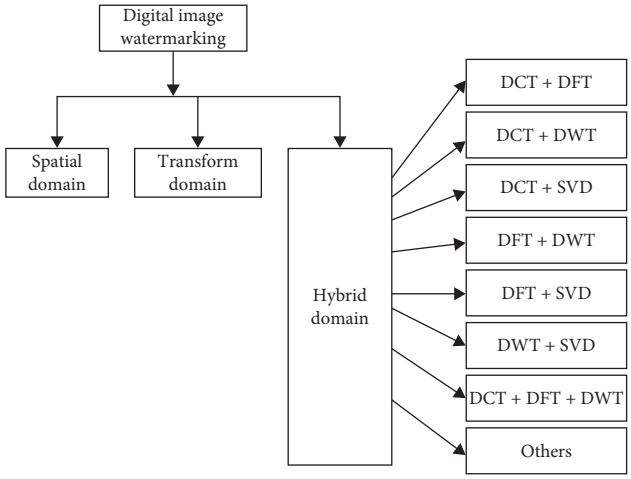


Figure 4: Classification of digital image watermarking.

## 5. Comparative Study of Hybrid Digital Image Watermarking Methods

Some performance metrics determine the overall performance of the watermarking system. Hence, this section discusses the performance evaluating metrics. Then, it highlights the experimental results of state-of-the-art hybrid methods in Tables 1 and 2. Then, the complexity analysis of these hybrid methods is shown in Tables 3 and 4. The limitations and associated applications are highlighted in Table 5.

*5.1. Performance Evaluating Metrics.* Quality recognizes an image-based object, and this quality is measured by some performance evaluating metrics that can be treated as benchmark tools for evaluating performance. These include peak signal-to-noise ratio (PSNR), mean squared error (MSE), bit error rate (BER), mean absolute error (MAE), normalized correlation (NC), Euclidean distance (ED), structural similarity index (SSIM), feature similarity indexing method (FSIM), image fidelity (IF), and correlation quality (CQ). The more the PSNR, the more quality image is obtained. For an effective system, it is better to have $\text{PSNR} > 30\,\text{dB}$, $\text{NC} = 1.0$, and $\text{SSIM} = 1$.

*5.2. Experimental Results of Various Schemes.* In recent years, various hybrid methods have been developed for improving robustness, imperceptibility, and security, along with enhanced embedding capacity. However, this section keeps an eye on the summary of the state-of-the-art hybrid methods in Tables 1 and 2. Table 1 includes schemes, used techniques for imperceptibility, robustness, security requirements, size, type, and color of the cover image and the watermark image, and also embedding capacity. Table 2 includes schemes, test image, and imperceptibility measured in PSNR (dB) without any deformation of the watermarked image.

*5.3. Complexity Analysis of Hybrid Digital Image Watermarking Methods.* The watermarked image goes through a communication channel and is attacked by common signal processing operations or attacks. This section analyzes the complexity of various hybrid methods with the help of Tables 3 and 4. Table 3 consists of the schemes and test images and evaluates the PSNR, SSIM, BER, MAE, and NC values under type 1 attacks that include histogram equalization (HE), Gaussian noise (GN), salt-and-pepper noise (SPN), low-pass Gaussian filtering (LPGF), JPEG compression, JPEG 2000, cropping, and rotation. Table 4 consists of the schemes and test images and evaluates the PSNR, SSIM, and NC values under type 2 attacks that include sharpening, blurring, average filter (AF), median filter (MF), resizing/scaling, Poisson noise (PN), Gaussian white noise (GWN), and speckle noise (SN). Here, QF = quality factor, CR = compression ratio, $\mu$ = mean, and var = variance.

*5.4. Limitations and Applications of Various Hybrid Digital Image Watermarking Methods.* From the above summary, it is concluded that the hybrid domain digital image watermarking methods are more robust and provide better imperceptibility with high security. However, they have some limitations. They cannot resist combined attacks like HE + GN, HE + SPN, GN + JPEG compression, SPN + JPEG compression, and LPGF + SPN. These hybrid methods can be applied for multimedia security, telemedicine security, digital image security, and copyright protection. Figure 5 highlights the associated applications of hybrid digital image watermarking methods.

The limitations and applications of various state-of-the-art hybrid digital image watermarking methods are summarized in Table 5.

## 6. Challenges of Hybrid Methods of Digital Image Watermarking

The existing hybrid digital image watermarking methods are not so much robust against rotation, sharpening, blurring, average filtering (AF), Poisson noise (PN), speckle noise (SN), and print/scan attacks. Also, they are not much robust against combined attacks, like HE + GN, HE + SPN, GN + JPEG compression, SPN + JPEG compression, and LPGF + SPN. These techniques increase higher computational complexity (time and space). Also, they cannot achieve high performance with a trade-off between imperceptibility, robustness, security, and capacity. Moreover, security is a big challenge for this technology. However, the recent induction of the Internet of Things (IoT) and blockchain-based authentication provide better security. IoT devices use lightweight encryption algorithms for enhancing security, whereas a computer uses sophisticated encryption algorithms. Besides, IoT needs limited storage and requires less computing complexity [35]. On the other side, a blockchain-based authentication is a decentralized approach. A blockchain contains digital information blocks that are linked together and secured by cryptography. This blockchain technology stores the signature of the host image on the blockchain. Therefore, the host image cannot be modified by an attacker. For locating the tampered region and authenticity of the host image, the signature can be

Table 1: Summary of the state-of-the-art hybrid methods.

| Schemes | For imperceptibility | For robustness | For security | Cover image size, type, and color | Watermark image size, type, and color | Capacity (bits) |
|---|---|---|---|---|---|---|
| DWT-DCT [3] | DWT + DCT | DWT + DCT | Arnold transform | 512 × 512, Lena image, greyscale | 32 × 32, greyscale | — |
| DWT-SVD [4] | DWT + SVD | DWT + SVD | Encryption algorithm | 512 × 512, Lena image, greyscale | 256 × 256, greyscale | — |
| DWT-SVD [5] | DWT-SVD and wavelet fusion algorithm | DWT-SVD and wavelet fusion algorithm | — | 256 × 256, Cameraman image, greyscale | Primary watermark 256 × 256, logo image and secondary watermark 256 × 256, Lena image (both greyscale) | — |
| LWT-DCT [6] | LWT + DCT | LWT + DCT | — | 256 × 256, Lena image, color image | 64 × 64, Mandrill, greyscale | — |
| DWT-SVD [7] | SVD | DWT | — | 512 × 512, Goldhill image, grayscale image | 256 × 256, logo image, binary image | — |
| DWT-DCT [8] | DWT + DCT | DWT + DCT | RSA algorithm | 512 × 512, medical image, greyscale image | Health center logo and EPR data, greyscale | — |
| DCT-DWT [9] | DCT-DWT and autothresholding | DCT-DWT and autothresholding | — | 512 × 512, Peppers, RGB colored image | 27 × 100, text image, white background, and plotted black numbers | 2700 bits |
| DWT-DCT [10] | DWT-DCT and QIM | DWT-DCT and QIM | Arnold transform | 512 × 512, natural image, greyscale images | 64 × 64, logo, image, binary image | 1/64 bit per pixel |
| SVD-DCT [11] | SVD and DCT Walsh hybrid transform | SVD and DCT Walsh hybrid transform | — | 256 × 256 × 3 bytes, natural image, color bitmap images | 128 × 128 × 3 bytes, natural image, color bitmap images | — |
| DWT-DCT-SVD [12] | DWT-DCT and SVD | DWT-DCT and SVD | — | 512 × 512, abdominal, greyscale | 512 × 512, girl face, greyscale | — |
| LWT-DCT-SVD [13] | LWT-DCT-SVD and PSO algorithm | LWT-DCT-SVD and PSO algorithm | — | 512 × 512, natural image, greyscale image | 32 × 32, logo, binary image | — |
| DCT-SVD [14] | DCT + SVD | DCT + SVD | Arnold transform | 512 × 512, natural image, greyscale image | 64 × 64, Lena (logo image), greyscale image | 262144 |
| DFT-DCT [15] | Magnitudes of DFT coefficients | DCT to the magnitudes of DFT coefficients | Arnold transform | 512 × 512, natural and textured image, greyscale | 19 × 52 and 64 × 64, binary logo, greyscale | 988 (for Lena image) |
| DWT-DCT [16] | DWT-DCT and OMP reconstruction | DWT-DCT and OMP reconstruction | — | 256 × 256, Lena, greyscale | 32 × 32, logo image, binary | — |
| DCT-DWT [17] | DCT + DWT | DCT + DWT | Arnold transform | 1024 × 1024 × 3, natural image, RGB | 96 × 96, natural image, greyscale | — |
| DWT-SVD [18] | DWT + SVD | DWT + SVD | — | 512 × 512 (for both inner and outer image), natural image, color | 50 × 20, text image, binary image | — |

Table 2: Evaluation performance of the watermarked image.

| Schemes | Test image | Imperceptibility measured in PSNR (dB) (without any deformation of watermarked image) |
|---|---|---|
| DWT-DCT [3] | Lena | 37.7160 |
| DWT-SVD [4] | Lena | 109.84 |
| DWT-SVD [5] | Cameraman | 64.3155 |
| LWT-DCT [6] | Lena | 46.7629 |
| DWT-DCT [8] | MRI-brain | 52.743550 (for gain factor, $k = 0.02$) |
| DCT-DWT [9] | Peppers | 42.74 |
| DWT-DCT-SVD [12] | Abdominal | 57.80 ((for gain factor, $k = 0.1$) |
| LWT-DCT-SVD [13] | Lena | 46.5085 |
| DCT-SVD [14] | Barbara | 62.74 |
| DFT-DCT [15] | Mandrill and D9 | 61.28 (for Mandrill), 58.97 (for D9 image) |
| DCT-DWT [17] | Baboon | >35 |

Table 3: PSNR, SSIM, BER, MAE, and NC values under type 1 attacks.

| Schemes | Test image | Histogram equalization | Gaussian noise | Salt-and-pepper noise | LPGF | JPEG compression (QF) | JPEG 2000 (CR) | Cropping (%) | Rotation (°) |
|---|---|---|---|---|---|---|---|---|---|
| DWT-DCT [3] | Lena | — | — | — | — | SSIM = 0.9839 (QF = 50%) | — | SSIM = 0.9495 (25%) | — |
| DWT-SVD [4] | Lena | NC = 1.0 | NC = 1.0 (for scaling factor = 0.99) | NC = 1.0 (for scaling factor = 0.99) | — | NC = 0.7593 | — | — | — |
| DWT-SVD [5] | Cameraman | — | PSNR = 20.4017 (for scaling factor = 0.01) | — | — | — | — | PSNR = 7.8166 | — |
| DWT-SVD [7] | Goldhill | PSNR = 17.545 (for scaling factor, $\mu = 5$) | PSNR = 30.000 (for scaling factor, $\mu = 5$) | PSNR = 12.364 (for scaling factor, $\mu = 5$) | PSNR = 29.794 (for scaling factor, $\mu = 5$) | PSNR = 8.356 (for scaling factor, $\mu = 5$) | — | PSNR = 13.047 (for scaling factor, $\mu = 5$) | PSNR = 11.430 (up to 200) (for scaling factor, $\mu = 5$) |
| DWT-DCT [8] | MRI-brain | NC = 0.7498 | NC = 0.9487 (for $\mu = 0$, var = 0.00001) | NC = 0.9850 (for noise level = 0.001) | NC = 0.7779 | NC = 1.0000 (for QF = 65) | — | NC = 0.6963 | NC = 0.6981 (for 0.01°) |
| DCT-DWT [9] | Peppers | | NC = 0.9739 | NC = 0.9413 (for noise level = 10%) | — | NC = 0.9926 (for QF = 100) | — | NC = 0.9594 (for 154 × 154) | NC = 0.9886 (for 75°) |
| DWT-DCT [10] | Lena | — | BER = 5.67 (for var = 0.001) | BER = 14.44 (for intensity = 1%) | BER = 0.04 (for 3 × 3) | BER = 0.02 (for QF = 80) | BER = 0.01 (for CR = 2) | BER = 11.99 (25%) | BER = 13.94 (for 45°) |
| SVD-DCT [11] | Face | MAE = 25.449 | MAE = 0.068 | — | — | MAE = 1.346 (for QF = 100) | — | MAE = 11.462 (cropping 32 × 32 at corners) | — |
| DWT-DCT-SVD [12] | Abdominal | — | NC = 0.9999 at scaling factor 0.8 (for $\mu = 0$, var = 0.01) | NC = 0.9999 at scaling factor 0.8 (for density = 0.01) | — | — | — | — | — |
| LWT-DCT-SVD [13] | Lena | PSNR = 45.01206 | PSNR = 43.96941 (for $\mu = 0$, var = 0.001) | PSNR = 44.05564 (for density = 0.02) | PSNR = 44.88039 (for 3 × 3) | PSNR = 43.86933 (for QF = 70%) | — | PSNR = 44.97377 (for 25%) | PSNR = 44.82333 (for 5°) |
| DCT-SVD [14] | Barbara | — | — | — | — | — | — | NC = 0.9952 | NC = 0.9952 |
| DFT-DCT [15] | D9 | SSIM = 0.9995, NC = 1.0 | SSIM = 0.9928, NC = 0.9947 (for $\mu = 0$, var = 0.0005) | SSIM = 0.9997, NC = 1.0, (for $\mu = 0$, var = 0.0001) | SSIM = 0.9996, NC = 0.9984 (for $\sigma = 0.6$, 9 × 9) | SSIM = 0.9997, NC = 1.0 (for QF = 90) | SSIM = 0.9002, NC = 0.9003 (for CR = 10) | SSIM = 1.0, NC = 1.0, (50%) | — |
| DWT-DCT [16] | Lena | — | BER = 0.0869 (for 0.0008) | BER = 0.0615 (for 0.005) | BER = 0.0869 (for 3 × 3, 0.9) | BER = 0.1660 (for QF = 20) | — | — | — |
| DCT-DWT [17] | Baboon | — | NC = 0.9982 (for scaling factor = 80) | NC = 0.9530 (for scaling factor = 80) | — | NC = 0.9994 (for scaling factor = 80) | — | — | NC = 0.8669 (for scaling factor = 80) |
| DWT-SVD [18] | Pepper | — | NC = 0.9438 | NC = 0.9139 | — | NC = 1.0000 | — | — | NC = 1.0000 (up to 90°) |

Table 4: PSNR, SSIM, and NC values under type 2 attacks.

| Schemes | Test image | Sharpening | Blurring | Average filter (AF) | Median filter (MF) | Resizing/scaling | Poisson noise (PN) | Gaussian white noise (GWN) | Speckle noise (SN) |
|---|---|---|---|---|---|---|---|---|---|
| DWT-DCT [3] | Lena | — | — | — | SSIM = 0.9777 | SSIM = 0.9798 | — | SSIM = 0.9558 ($\mu = 0$, var = 0.01) | — |
| DWT-SVD [4] | Lena | — | — | — | — | — | — | — | NC = 1.0 (for scaling factor = 0.8) |
| DWT-SVD [5] | Cameraman | — | — | PSNR = 20.6928 | — | — | — | — | — |
| DWT-SVD [7] | Goldhill | — | — | — | — | — | — | PSNR = 30.000 (for scaling factor, $\mu = 5$) | — |
| DWT-DCT [10] | Lena | — | — | — | BER = 4.45 (for $3 \times 3$) | BER = 1.09 (scaling 25%) | — | — | — |
| DWT-DCT-SVD [12] | Abdominal | — | — | NC = 0.9940 (for $5 \times 5$) | NC = 0.9995 (for $3 \times 3$) | — | — | — | NC = 0.9996 (for density = 0.08) |
| LWT-DCT-SVD [13] | Lena | PSNR = 45.00733 | — | PSNR = 43.74854 (for $3 \times 3$) | PSNR = 44.06895 (for $3 \times 3$) | PSNR = 44.43792 (for 512 to 256 to 512) | PSNR = 44.23103 | — | PSNR = 43.78754 (for $\mu = 0$, var = 0.04 |
| DCT-SVD [14] | Barbara | — | — | — | NC = 0.8812 | — | — | — | — |
| DCT-DWT [17] | Baboon | NC = 0.9292 (for scaling factor = 80) | NC = 0.9663 (for scaling factor 80) | NC = 0.9715 (for scaling factor 80) | NC = 0.9988 (for scaling factor 80) | NC = 0.9589 (for scaling factor 80) | NC = 0.9589 (for scaling factor 80) | NC = 0.9982 (for scaling factor 80) | NC = 0.8770 (for scaling factor 80) |
| DWT-SVD [18] | Pepper | — | — | — | — | — | NC = 1.0000 | — | NC = 0.9346 |

Table 5: Limitations and applications of various hybrid methods.

| Schemes | Limitations | Applications |
|---|---|---|
| DWT-DCT [3] | Less robust against HE, SPN, LPGF, JPEG 2000, rotation, sharpening, blurring, AF, PN, SN, print/scan attack, and combined attacks | Copyright protection |
| DWT-SVD [4] | Less robust against LPGF, JPEG 2000, cropping, rotation, sharpening, blurring, AF, MF, resizing, PN, GWN, print/scan attack, and combined attacks | — |
| DWT-SVD [5] | Less secured, not robust against HE, SPN, LPGF, JPEG compression, JPEG 2000, rotation, sharpening, blurring, resizing, PN, GWN, SN, print/scan attack, and combined attacks | — |
| DWT-SVD [7] | Not robust against JPEG 2000, sharpening, blurring, resizing, PN, SN, print/scan attack, and combined attacks | Copyright protection and multimedia security |
| DWT-DCT [8] | Not robust against sharpening, blurring, AF, MF, resizing, PN, GWN, SN, print/scan attack, and combined attacks | Telemedicine security |
| DCT-DWT [9] | Not robust against sharpening, blurring, AF, MF, PN, GWN, SN, print/scan attack, and combined attacks | Digital images security |
| DWT-DCT [10] | Not robust against AF, PN, GWN, SN, print/scan attack, combined attacks, and desynchronization attacks | — |
| SVD-DCT [11] | Not robust against SPN, LPGF, JPEG 2000, rotation, sharpening, blurring, AF, GWN, PN, SN, print/scan attack, and combined attacks | Copyright protection |
| DWT-DCT-SVD [12] | Not robust against HE, LPGF, JPEG compression, JPEG 2000, rotation, cropping, sharpening, blurring, resizing, PN, GWN, print/scan attack, and combined attacks | Medical image security |
| LWT-DCT-SVD [13] | Less robust against JPEG 2000, print/scan attack, desynchronization attacks, and combined attacks | Multimedia security |
| DCT-SVD [14] | Less robust against GN, LPGF, histogram equalization, JPEG compression, JPEG 2000, sharpening, blurring, resizing, PN, GWN, desynchronization attacks, and combined attacks | Medical science and defense applications |
| DFT-DCT and Arnold transform [15] | Less robust against rotation, sharpening, blurring, AF, MF, wiener filter, print/scan attack, resizing, PN, GWN, SN, desynchronization, and combined attacks | Copyright protection |
| DWT-DCT [16] | Less robust against HE, JPEG 2000, rotation, sharpening, blurring, AF, MF, Wiener filter, print/scan attack, resizing, PN, GWN, SN, desynchronization, and combined attacks | Multimedia security and copyright protection |
| DCT-DWT [17] | Not robust against HE, LPGF, JPEG 2000, cropping, Wiener filter, print/scan attack, desynchronization, and combined attacks | Copyright protection |
| DWT-SVD [18] | Not robust against HE, LPGF, JPEG 2000, cropping, sharpening, blurring, AF, MF, resizing, GWN, Wiener filter, print/scan attack, desynchronization, and combined attacks | Copyright protection |

recovered from the blockchain. In this case, this blockchain technology protects the signature of the host image by 100% against any manipulation [36]. We have highlighted some of these techniques below.

For checking the authenticity of pharmaceutical products in the IoT environment, a method is proposed that uses the NFC or near-field communication [37]. The method ensures session key security by using the ROR (real-or-random) model which is effective from computation and communication cost perspectives. A content-based image retrieval (CBIR) method is proposed without accessing cloud-server information [38]. Here, images are represented by extracting feature vectors. The secure k-nearest neighbor (kNN) algorithm protects the feature vector. For ensuring the security of existing devices, a blockchain-based secured mutual authentication (termed as BSeIn) method is proposed that ensures privacy and security [39]. A lightweight blockchain-based RFID authentication protocol, LBRAPS, is designed for supply chains in the 5G mobile environment. The method is secured against various attacks [40]. In addition, a new authentication method related to cloud-assisted cyber-physical system (CPS) is designed in reference [41]. Here, the external user can access the cloud server information. Cloud server data can communicate securely by the authentication scheme between a cloud server and a smart meter. The method ensures the security of the system. Recently, Wazid et al. [42] proposed a LAM-CIoT (lightweight authentication mechanism in a cloud-based IoT environment) mechanism where the authorized users can access the IoT data remotely. The method uses cryptographic hash functions and bitwise XOR operations and has shown better security experimentally.

*6.1. Open Research Issues (Long-Term Vision).* Current trends of image authentication are based on the frequency or transform domain, whereas some are based on the spatial domain. But, now research trends are integrated with artificial intelligence. So, some new open research issues are growing. They are given as follows:

(i) *Voice to Authentication.* It is the ultimate desire to have image authentication along with the voice. Technology needs to integrate the watermark (text)

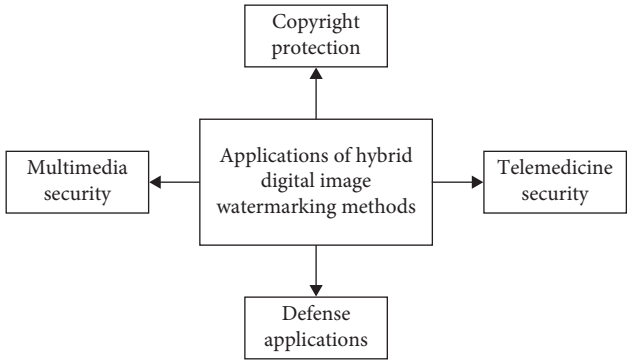


Figure 5: Applications of hybrid digital image watermarking methods.

from the direct voice. At first, voice to text conversion will be done and then the text will be inserted to the cover image. It will be more secured than traditional authentication for the extra step voice to text as it finds applications in natural language processing.

(ii) *Biometric Authentication*. An effective invisible biometric authentication system is very much demanding in today's digital world, as it has huge applications in the medical field, e-commerce, and banking system.

(iii) *Social Authentication*. At present, fake accounts can be seen on social media which harms society. Various crimes, fake news, and rumors are spreading on an increasing scale through these fake profiles. So, to stop these unwanted profile activities special research focus is needed.

(iv) *Image Authentication with Cloud Outsourcing*. This research will lead to the privacy-preserving image authentication system. Image authentication is a costly operation when we consider a big image database. So, image databases should be encrypted before sending it to the cloud. Blockchain technology can be integrated here for better security. It is a challenging issue to find out the original watermark from the encrypted cover image on the receiver side and an open problem for future researchers.

## 7. Conclusions and Future Directions

Images are an important part of multimedia data. Image authentication is a challenging task due to Internet traffic. Because of the interactive communication of multimedia data and wide-spread use of IoT technology, information can be duplicated easily. Along with image data security, it is essential to ensure the imperceptibility, robustness, and enhanced data embedding capacity. Hybrid digital image watermarking is a significant field for ensuring these issues. However, our investigation has found that the existing hybrid methods need to be improved to ensure these issues. Moreover, we have pointed out that the recent induction of the Internet of Things (IoT) and blockchain-based authentication provide better security. Therefore, to get improved robustness and high image data security along with better imperceptibility and embedding capacity, future researchers must combine machine learning and artificial neural network algorithms in the hybrid transform domain.

## Data Availability

There are no data available.

## Conflicts of Interest

The authors declare no conflicts of interest.

## Authors' Contributions

M.B. studied and drafted the whole paper; M.S.U. initiated the concept, supervised the study, and fine-tuned the manuscript.

## References

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

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

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

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

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

[6] A. Tun and Y. Thein, "Digital image watermarking scheme based on LWT and DCT," *International Journal of Engineering and Technology*, vol. 5, pp. 272–277, 2013.

[7] O. Jane, E. Elbaşi, and H. G. İlk, "Hybrid non-blind watermarking based on DWT and SVD," *Journal of Applied Research and Technology*, vol. 12, no. 4, pp. 750–761, 2014.

[8] A. Sharma, A. K. Singh, and S. P. Ghrera, "Secure hybrid robust watermarking technique for medical images," *Procedia Computer Science*, vol. 70, pp. 778–784, 2015.

[9] N. A. A. S. Al-maweri, W. A. W. Adnan, A. Rahman Ramli, K. Samsudin, and S. M. S. Ahmad, "A hybrid digital image watermarking algorithm based on DCT-DWT and auto-thresholding," *Security and Communications Networks*, vol. 8, no. 18, pp. 4373–4395, 2015.

[10] H.-T. Hu and L.-Y. Hsu, "Collective blind image watermarking in DWT-DCT domain with adaptive embedding strength governed by quality metrics," *Multimedia Tools and Applications*, vol. 76, no. 5, pp. 6575–6594, 2017.

[11] S. Natu, P. Natu, and T. Sarode, "Improved robust digital image watermarking with SVD and hybrid transform," in

*Proceedings of the International Conference on Intelligent Communication and Computational Techniques (ICCT)*, pp. 177–181, Jaipur, India, December 2017.

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

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

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

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

[16] Y. Zhang, Y. Li, and Y. Sun, "Digital watermarking based on Joint DWT–DCT and OMP reconstruction," *Circuits, Systems, and Signal Processing*, vol. 38, pp. 5135–5148, 2019.

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

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

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

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

[21] G. Dubey, C. Agarwal, S. Kumar, and H. P. Singh, "Image watermarking scheme using cuckoo search algorithm," *Advances in Data and Information Sciences, Lecture Notes in Networks and Systems*, vol. 94, pp. 667–675, Springer, Singapore, 2020.

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

[23] Y.-H. Chen, H.-C. Huang, C.-H. Lai, and T.-Y. Chang, "An image watermarking approach based on artificial fish swarm algorithm," in *Proceedings of Analysis of watermarking framework for color image through*, pp. 46–50, Kyoto, Japan, March 2020.

[24] M. F. Kazemi, M. A. Pourmina, and A. H. Mazinan, "Analysis of watermarking framework for color image through a neural network-based approach," *Complex & Intelligent Systems*, vol. 6, no. 1, pp. 213–220, 2020.

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

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

[27] M. L. Miller, I. J. Cox, J. A. Bloom, J. Fridrich, and T. Kalker, *Digital Watermarking and Steganography*, Morgan Kaufmann Publishers, Burlington, VT, USA, 2008.

[28] G. C. Langelaar, I. Setyawan, and R. L. Lagendijk, "Watermarking digital image and video data. A state-of-the-art overview," *IEEE Signal Processing Magazine*, vol. 17, no. 5, pp. 20–46, 2000.

[29] R. M. Thanki and A. M. Kothari, "Digital watermarking: technical art of hiding a message," *Intelligent Analysis of Multimedia Information*, pp. 426–460, IGI Global, Hershey, PA, USA, 2016.

[30] F. N. Thakkar and V. K. Srivastava, "A fast watermarking algorithm with enhanced security using compressive sensing and principal components and its performance analysis against a set of standard attacks," *Multimedia Tools and Applications*, vol. 76, no. 14, pp. 15191–15219, 2017.

[31] K. Ashish, *Design, implementation and performance analysis of digital watermarking for video*, Ph.D Thesis, JJT University, Jhunjhunu, India, 2013.

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

[33] H. Tao, L. Chongmin, J. Mohamad Zain, and A. N. Abdalla, "Robust image watermarking theories and techniques: a review," *Journal of Applied Research and Technology*, vol. 12, no. 1, pp. 122–138, 2014.

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

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

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

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

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

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

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

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

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