A Watermarking Technique for User Authentication Based on a Combination of Face Image and Device Identity in a Mobile Ecosystem

Fatimah Al-Jarba and Mohammed Al-Khathami,
fhaljarba@imamu.edu.sa maalkhathami@imamu.edu.sa
Information Systems Department, Imam Mohammad Ibn Saud Islamic University, Riyadh, Saudi Arabia

Abstract

Digital content protection has recently become an important requirement in biometrics-based authentication systems due to the challenges involved in designing a feasible and effective user authentication method. Biometric approaches are more effective than traditional methods, and simultaneously, they cannot be considered entirely reliable. This study develops a reliable and trustworthy method for verifying that the owner of the biometric traits is the actual user and not an impostor. Watermarking-based approaches are developed using a combination of a color face image of the user and a mobile equipment identifier (MEID). Employing watermark techniques that cannot be easily removed or destroyed, a blind image watermarking scheme based on fast discrete curvelet transform (FDCuT) and discrete cosine transform (DCT) is proposed. FDCuT is applied to the color face image to obtain various frequency coefficients of the image curvelet decomposition, and for high frequency curvelet coefficients DCT is applied to obtain various frequency coefficients. Furthermore, mid-band frequency coefficients are modified using two uncorrelated noise sequences with the MEID watermark bits to obtain a watermarked image. An analysis is carried out to verify the performance of the proposed schema using conventional performance metrics. Compared with an existing approach, the proposed approach is better able to protect multimedia data from unauthorized access and will effectively prevent anyone other than the actual user from using the identity or images.

Key words:
Watermark; User authentication; Biometrics; Digital content; IMEI.

1. Introduction

Digital content protection is one of the oldest and most important topics in scientific research on ensuring the security and integrity of biometrics data based on improvements in Internet technologies and the extensive use of biometrics-based verification systems [1], [2]. Biometric authentication is a security approach that authenticates a user's identity through one of their unique characteristics by storing the biometric data. This approach is essential for completing secure mobile payments. Biometric approaches are based on physiological or behavioral characteristics [3]. The physiological biometric authentication approach involves unique characteristics of the human body, e.g., facial recognition—which a popular and widely used method—is a biometric technique that captures users' facial features from an image [4]. Furthermore, biometrics cannot be considered entirely reliable because an attacker can duplicate a fingerprint or steal an image, and once biometric characteristics are stolen, the attacker is able to access the user's account at any time because biometric characteristics are stable and do not change [5]. Consequently, a reliable and trustworthy method must be used to verify that the owner of these biometric traits is the actual user and not an impostor.

A unique international mobile equipment identity (IMEI) or mobile equipment identifier (MEID) can be used to identify the user of the device that has been activated via a subscriber identity module (SIM). The IMEI is a 15-digit code that is unique for every mobile device using a Global System for Mobile Communication system [6], while the MEID is for mobile devices that use the code-division multiple access system. Every mobile device is assigned a globally unique set of numbers that indicate substantial information on the mobile (e.g., place of manufacture) and can be used to track a stolen mobile via its IMEI or MEID on mobile telecommunication networks. Unfortunately, it is possible to modify the IMEI on many devices, and SIM cards can be cloned or hijacked [7], [8]. Thus, using IMEI or MEID alone to authenticate the user in a mobile ecosystem is insufficient.

Therefore, this research aims to identify a new algorithm for user authentication in mobile devices that solves the outlined limitations. The proposed algorithm is based on a combination of a user face image and mobile device identification information using watermark techniques. Growing copyright protection concerns have contributed to increased interest in watermarking and its becoming an important field [9], [10]. A digital watermark refers to a secret code embedded in digital data (audio, video, or image) that cannot be easily removed or destroyed and can later be decoded or extracted to ascertain ownership claims [11]. It

Manuscript received September 5, 2021
Manuscript revised September 20, 2021
https://doi.org/10.22937/IJCSNS.2021.21.9.40

protects multimedia data from unauthorized access and keeps anyone other than the actual owner from using the identity or images. Therefore, different watermarking methods have been studied for many purposes, such as broadcast monitoring, copy control, content authentication, and copyright protection. A watermarking technique can be used to validate the authenticity of images and to protect the images during digital transmission processes [1], [12]–[15].

1.1 Digital Watermarking Methods

Digital watermarking methods are considered information hiding method. The key features and requirements for a watermarking algorithm are robustness, imperceptibility, security, capacity, and low complexity. Robustness refers to the ability to detect the watermark after signal processing modifications and measures the efficacy with which it survive unintentional attacks. Imperceptibility is considered the most significant requirement for a watermarking system, and it implies that the watermarked image should look similar to the original image. Capacity defines the number of bits embedded in the image, and security means that the algorithm should be sufficiently secure against unauthorized users. Finally, low complexity refers to the economics of using watermark embedders and detectors, including the speed of embedding and detection, and the number of embedders and detectors [14], [16]–[18].However, the digital image watermarking field is still plagued by problems regarding security and protection against various attacks. Furthermore, there is the challenge of achieving a balance between the robustness and imperceptibility features as increasing one decreases the other (e.g., imperceptibility could be achieved, while robustness is simultaneously reduced, and vice versa) [16], [9]. These challenges highlight the need to work with different methods to improve these four fields [19].

Watermarking techniques are designed to protect digital data and can be classified into two domains: spatial domain methods that operate at the pixel level [20], [21], and transform domain methods that depend on a mathematical tool [11]. Spatial domain methods embed the watermark by changing pixel values that are low complexity, simple, and less time consuming. In other words, spatial domain methods are susceptible to attacks. On the other hand, transform domain schemes modify coefficients to embed and hide watermark signals after frequency transformation of the image, and it has good robustness in comparison with spatial domain methods [22], [10]. Examples of transform domain schemes include discrete Fourier transform (DFT), discrete wavelet transform (DWT), discrete cosine transform (DCT), and singular value decomposition (SVD) [2]. However, transform domain methods may degrade image quality significantly by embedding a high-capacity watermark in the domain of frequency [15], [19], [23].

Digital watermarking can be done using hybrid domains, which involves combining different transform domain methods, e.g., tacking the host image and then applying two or more transform domain methods to the image. Hybrid domains are considered more robust and have acceptable levels of imperceptibility. However, hybrid domains cannot resist combined attacks, and based on this limitation, the existing hybrid methods still need to be improved [24]. Consequently, this study aims to address this via a proposed robust and secure hybrid watermarking technique for mobile ecosystem protection that protects multimedia data from unauthorized access and prevents anyone other than the actual owner from using the identity or images. Hence, the proposed algorithm provides stronger protection against different watermarking attacks.

1.1.1 Watermarking Attacks

Over the past few years, different watermarking schemes have been proposed that aim to improve and promote accuracy and robustness and to protect the watermark from different types of attacks [1]. The level of security required by different applications can change based on the level of sophistication of expected adversaries. Table 1 presents the categories of adversaries and the unauthorized actions in each attack category. Furthermore, specific requirements should be considered in the watermark to resist the attacks. For unauthorized removal, the watermark should be robust and irremovable, while for unauthorized detection, it should be an imperceptible watermark. For unauthorized embedding, the watermark should be fragile or semi-fragile to detect any modification [25].

Table 1: Adversary Categories

Category	***Meaning***
Unauthorized Embedding	Adversary composing and embedding an original message
Unauthorized Detection	Adversary trying to decode what a watermark says
Unauthorized Removal	Adversary trying to recover the original message

In addition, previous attacks can be successfully addressed, either directly or indirectly. An attack that cannot be addressed within the confines of watermarking is a system-level attack, which includes scrambling attacks in which samples of a work are scrambled before presenting it to a watermark detector and then subsequently descrambled. Pathological distortions include synchronization attacks, such as shearing, horizontal reflection, and column or line removal in images. Linear filtering and noise removal attacks, which attempt to remove a watermark, are also pathological distortions. Copy attacks are a form of unauthorized embedding in which the attacker copies a watermark from one image to another. Finally, there is sensitivity analysis and gradient descent attacks, which are used for unauthorized removal of a watermark [14]. This research improves and promotes the accuracy and robustness of the proposed scheme, and the algorithm is tested under 12 attacks, including: JPEG compression with Q = (90, 70, 40), Gaussian noise (σ = 0.001, 0.01), salt and pepper noise (σ = 0.1, 0.02), speckle noise (σ = 0.0004), median filter (3 × 3), low-pass filter (3 × 3), scaling (512 → 256 → 512), and histogram equalization.

1.2 Related Research

Digital image watermarking is dependent on embedding a host image with information. Subsequently, the watermarked image can be transmitted and then extracted at the receiver. A previous study by Hemida et al.[26] proposed a restorable fragile watermarking scheme based on DCT. The authentication watermarks are based on a secret key, which is used to identify any modification made to the authenticated image with 4 × 4 blocks, while a variable-capacity recovery watermark of a 2 × 2 block is generated by encoding the significant DCT coefficients to enhance the quality of the watermarked image. The algorithm was tested against various attacks, including general tampering, content-only attack, collage attack, and a hybrid attack. The scheme was found to have good invisibility and superior recovery quality and is less expensive. However, there is a need_to work on improving recovery quality using advanced image processing methods.
Vaidya and Mouli [27] proposed a robust semi-blind watermarking scheme for color images based on multiple decompositions, including DWT, contourlet transform (CT), Schur decomposition, and SVD. In the semi-blind extraction process, the watermark can be extracted without using the original host image, i.e., it is does not require the original information. The performance of the scheme was measured per its imperceptibility and robustness using the following metrics: peak signal-to-noise ratio (PSNR), structural similarity (SSIM) index, and the normalized correlation coefficient (NCC). Furthermore, scheme was tested against 12 attacks and compared with related color image watermarking methods. The scheme was found to have superior imperceptibility, security, and robustness.
Face recognition is the most common biometric feature that is easy to use and enjoys a high level of user acceptance. Due to the continuous development of the technology, a combination of biometric systems and security schemes is inevitable [3]. A study by Isa et al.[28] provide an effective combination of a face recognition system and a watermarking system in order to enhance the security of face recognition systems: a principal component analysis (PCA) and DCT combination. To ensure the authenticity of the data used in the face recognition system, they use logo and timestamp watermarks. Furthermore, this combination does not affect the performance of the individual systems; it is robust and cannot be easily removed by an attacker. In addition, Agarwal et al. [29] studied a wavelet based on four blind invisible watermarking methods with a face image as the watermark. The first two watermarking methods are implemented via DWT, while the other two are based on the redundant discrete wavelet transform (RDWT). To improve the performance of the watermarking methods, the transform includes weighted binary coding. To measure the quality of the watermarks, they used PSNR and NCC, and the watermarking methods were tested using different attacks: cropping, Gaussian filtering, Gaussian noise, salt and pepper noise, rotation, JPEG compression, and resizing. they found that DWT coupled with weighted binary coding has the best performance among the RDWT-based watermarking methods.
Another study by Laur et al. [30] proposed a robust grayscale watermarking algorithm based on face detection. To create a robust and imperceptible watermarked image, they used: DWT, which decomposes the image into a set of frequency subbands; SVD, to find singular values of a matrix; chirp z-transform (CZT), which is a generalization of DFT; and lower–upper (LU) decomposition, which splits the matrix into a lower and upper triangular matrix to select a more accurate watermark location. CZT is applied to the low-frequency subband and LU decomposition is applied to the output. PSNR was used to evaluate the image quality yielded by the method, and the different experiments performed on the algorithm show that the method has good imperceptibility and robustness features, such as flipping, cropping, and JPEG compression.
Furthermore, to increase the reliability of the method, a multimodal biometric method has been used. Rzouga Haddada and Essoukri Ben Amara [31] proposed an authentication framework based on radio frequency identification (RFID), which is a technology that uses radio waves to identify and track tags on an object. The method provides a secure solution that depends on multimodal biometric watermarking approaches, including face and fingerprint characteristics and RFID technology that prevents illegitimate access in the event of RFID card theft. This study focused on an aspect of security where there is only a small space for data storage, and the researchers did not test the method against attacks, which constitutes a

limitation. Another study based on a multimodal biometric watermarking system by Singh et al. was conducted [32]. However, it is based on facial and iris features embedded independently into the subbands of the RDWT. The reason for adopting this approach is that the size of the RDWT subbands will remain the same size as the cover image, rather than other types, such as DWT, which decrease significantly after every decomposition. The algorithm is based on two watermarks: a grayscale watermark based on iris features and a binary watermark based on facial features. After experimenting with the algorithm, the authors found that multimodal biometrics promote accuracy and increased robustness against different attacks. In another study by Kant and Chaudhary [33] using iris and face biometric traits, the watermarked image was generated by instill the iris image onto the face image and storing the new image in a database, rather than saving the original templates in the database. DWT-based watermarking methodology was used to protect the hidden iris data and the cover facial image from unauthorized users, and circular Hough transform (CHT) was used to identify the pupil and iris boundary. Finally, the proposed approach shows that hiding the iris image in the face image provides privacy, security, and superior recognition accuracy.

In addition, secure authentication for identifying or authenticating a user is fast becoming an important feature. To provide greater security, Abawajy et al. [34] propose a secure biometric authentication scheme that facilitates sending text data securely over a network using digital watermarking and steganography techniques to hide data within messages. To provide secret data transmission and cryptography techniques that encode data into an unreadable form to achieve a robust system. First, to reduce bandwidth usage, the cover image is compressed using JPEG compression. Second, the text is encrypted using an improved Rivest–Shamir–Adleman (RSA) algorithm. Finally, the encrypted text and watermark image bits are embedded into the compressed cover image using DCT. The limitation of this method is that after measuring the time required between encryption and decryption for the improved and original RSA, they found that the encryption time for the improved RSA is less than that of the original RSA, which confirms the need to improve the decryption time. Furthermore, the compression algorithm needs to be improved.

A study by Singh et al.[35] propose a new DWT-based spread-spectrum watermarking algorithm for medical images to embed different text watermarks (e.g., patient records and doctors' signatures) that require great robustness. For increased security, the text watermark is encrypted using the American Standard Code for Information Interchange (ASCII) representation, using medical images as the cover image, and using the Haar wavelet transform for the dyadic subband decomposition performed on the medical cover image. The performance of the watermarking algorithm was evaluated based on its robustness and imperceptibility using PSNR, and it was tested against different attacks, including JPEG compression, median filtering, and salt and pepper. There are only a few differences in the medical image quality of the watermarked image. Regarding limitations, the researchers could have improved the correlation and security of the watermarking algorithm by using other extended pseudo-noise (PN) sequences, such as random sequence and the Gold sequence.

In reviewing the literature, it was observed that most of the existing watermarking schemes are designed using DCT, DWT, and SVD. In the study by Hemida et al. [26], there is a need to work on improving the recovery quality using advanced image processing methods, and to improve the correlation and security of the watermarking algorithm. Some existing watermarking schemes (e.g., the study by Rzouga Haddada and Essoukri Ben Amara [31]) are skipping testing their proposed methods against attacks. Furthermore, some studies need to perform imperceptibility and robustness tests, while other studies are challenged by an inability to achieve a suitable trade-off between imperceptibility and robustness. Thus, to achieve a good digital watermarking method, several requirements need to be met to overcome the aforementioned watermarking limitation, e.g., robustness and invisibility.

In this study, a blind watermarking scheme is proposed that uses fast discrete curvelet transform (FDCuT) and DCT techniques. The scheme has been tested against 12 attacks, and its performance is evaluated using PSNR, SSIM, and NCC metrics, which measure the imperceptibility and robustness of the scheme. To implement this scheme, FDCuT is first applied to the red channel of a face image to obtain its various frequency subbands (i.e., low, middle, and high), taking the high frequency subbands and converting the subband coefficients into non-overlapping blocks. Block-wise DCT is then applied to these blocks to obtain hybrid DCT coefficients. The middle frequency hybrid (MFH) DCT coefficients are modified using two uncorrelated noise sequences and watermark bits to obtain a watermarked image. The rest of this paper is organized as follows: Section 2 presents the preliminaries, explaining FDCuT and DCT. Section 3 presents an elaboration on the specific implementation process of the proposed watermarking algorithm. Section 4 presents the results of the experiment and performance evaluation. The conclusions are presented in Section 5.

2. Preliminaries

In this section, the proposed watermarking scheme based on FDCuT-DCT hybrid domain is elaborated in detail.

2.1 Fast Discrete Curvelet Transform (FDCuT)

FDCuT is an improved and redesigned method of discrete time curvelet transform (DTCuT) that is applied to an image to obtain various frequency subbands. While the curvelet transform algorithm is complex and possesses high redundancy, the FDCuT was designed with a new mathematical architecture that is simple and possesses high speed and small redundancy. FDCuT is categorized into two types: unequal spaced fast Fourier transform (USFFT), and frequency wrapping, which is chosen by many researchers [36]. Furthermore, frequency wrapping has an equal sample rate, is easy to implement, requires less computational time, and is easy to understand compared to the USFFT technique. When frequency wrapping is applied to an image, the image is split into three different frequency subbands, as shown in Figure 1: low frequency (LF), middle frequency (MF), and high frequency (HF) [37].

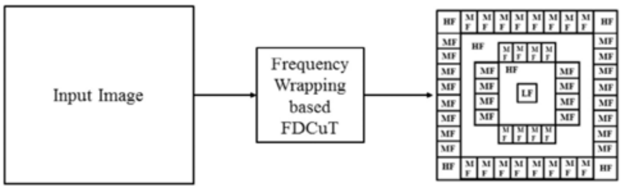


Fig. 1 Curvelet Decomposition of FDCuT

2.2 Discrete Cosine Transform (DCT)

DCT is a popular frequency domain watermarking technique that involves embedding a watermark n long into the n largest (in terms of magnitude) DCT coefficients. DCT will separate a cover image into different frequency bands: low frequency (LF), middle frequency (MF), and high frequency (HF) [15], as illustrated in Figure 2, and the features of these frequencies differ from a watermarking perspective [38]. Subsequently, several DCT bands are selected and modified to hold the watermark bits. DCT and inverse DCT can be calculated using Equation (1) and (2) [37].

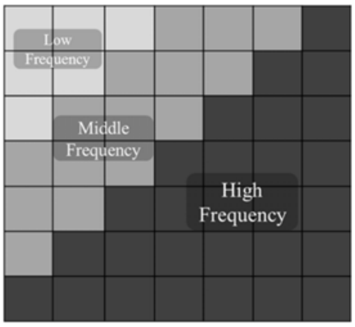


Fig. 2 DCT Frequency Bands

$$F\ (u,v) = a(u).\, a(v) \sum_{X=1}^{M-1} \sum_{Y=1}^{N-1} f(x,y)\ \times\ \cos\left[\frac{(2x+1)\mathcal{U}\pi}{2M}\right] \cos\left[\frac{(2y+1)\upsilon\pi}{2N}\right] \tag{1}$$

$$f(x,y) = \sum_{X=0}^{M-1} \sum_{Y=0}^{N-1} a(u).\ a(\upsilon).\, F(u,\upsilon)\ \times\ \cos\left[\frac{(2x+1)\mathcal{U}\pi}{2M}\right] \cos\left[\frac{(2y+1)\upsilon\pi}{2N}\right] \tag{2}$$

where $a(\mathcal{U}) = \sqrt{1/M}$ for $\mathcal{U} = 0$; $a(\mathcal{U}) = \sqrt{2/M}$ for $\mathcal{U} = 1,2,3 \ldots M-1$;
$a(\upsilon) = \sqrt{1/N}$ for $\upsilon = 0$; and $a(\upsilon) = \sqrt{2/N}$ for $\upsilon = 1,2,3 \ldots N-1$.

3. Proposed Algorithm

This section presents the details of the watermarking strategy, including the sequence of the watermark embedding and extraction processes.

3.1 Embedding the Watermark

In this scheme, a watermark bit is embedded into hybrid coefficients for the red channel of a color face image using random noise sequences that are Gaussian in nature. The process of watermark embedding is as follows:

Step 1. Take the monochromic watermark image and calculate its size; and the watermark converts into a bit vector.

Step 2. Take the color face image as the host image and choose the red channel of this image for watermark embedding. The reason for choosing the red channel is that the channel contains less facial information.

Step 3. Apply first-level forward FDCuT to the red channel of the face image to obtain its various frequency subbands (i.e., low, middle, and high). Here, frequency wrapping based curvelet transform is used.

Step 4. The HF subbands with less facial information are selected for a further process of watermark embedding. Then, convert the subband coefficients into non-overlapping blocks.

Step 5. Apply block-wise DCT to these blocks to obtain hybrid DCT coefficients, i.e., low, middle, and high). The MFH DCT coefficients are selected for a further embedding process.

Step 6. Generate two noise sequences that are uncorrelated in nature using a noise generator. The size of these sequences is equal to the size of the MFH DCT coefficients.

Step 7. Each watermark bit embeds into MFH DCT coefficients using the following conditions:

- If the value of the watermark bit is zero, then

$$modified\_MFH\_DCTblock = MFH\_DCTblock + k * Noise\_Sequence\_0 \quad (3)$$

where *modified_MFH_DCTblock* corresponds to the modified coefficients, *DCT block* are the original coefficients, *k* is the gain factor, and *Noise_Sequence_0* is the noise sequence for watermark bit 0.

- If the value of the watermark bit is one, then

$$modified\_MFH\_DCTblock = MFH\_DCTblock + k * Noise\_Sequence\_1 \quad (4)$$

where *modified_MFH_DCTblock* corresponds to the modified coefficients, *DCTblock* are the original coefficients, *k* is the gain factor, and *Noise_Sequence_1* is the noise sequence for watermark bit 1.

- This process is repeated for all the MFH DCT coefficients of each block of the red channel of the color face image.

Step 8. Apply inverse block-wise DCT to the modified MFH DCT coefficients, keeping other original DCT coefficients as is, to obtain a modified HF curvelet subband of the red channel of the color face image.

Step 9. Apply first-level inverse FDCuT to the modified HF curvelet subband with other original curvelet coefficients to obtain a modified red channel of the color face image.

Step 10. Finally, combine the modified red channel with the green channel and blue channel to obtain the watermarked color face image.

3.2 Extracting the Watermark

In this scheme, a watermark bit is extracted blindly using the correlation between the red channel of the watermarked color face image and noise sequences. The process for watermark extraction is outlined as:

Step 1. Take the watermarked color face image and select the red channel of this image for further processing.

Step 2. Apply first-level forward FDCuT to the red channel of the watermarked color face image to obtain its frequency subbands (i.e., low, middle, and high). Then, the HF curvelet subband converts into non-overlapping blocks.

Step 3. Apply block-wise DCT to the non-overlapping blocks of the HF curvelet subband to obtain hybrid frequency DCT coefficients (i.e., low, middle, and high).

Step 4. Take the two noise sequences generated during the watermark embedding process.

Step 5. Extract the watermark bit from the modified MFH DCT coefficients of the watermarked color face image using the following equations.

$$S1 = corr2(modified\_MFH\_DCTblock, Noise\_Sequence\_1) \quad (5)$$

$$S2 = corr2(modified\_MFH\_DCTblock, Noise\_Sequence\_0) \quad (6)$$

Step 6. If S1 > S2, then the value of the watermark bit is set as 1. Otherwise, the value of the watermark bit is set as 0.

Step 7. Apply reshaping to the extracted watermark bit vectors to obtain the extracted monochromic watermark image.

4. Performance Measurement and Evaluation

In this section, the performance of the proposed watermarking algorithm is tested and analyzed, and the watermarking system is evaluated. Dataset detail, which is the standard test for images in this field, metrics indexes in order to test imperceptibility and robustness.

4.1 Dataset

A subset of a color image of 640 × 370 pixels was used as a dataset, which was provided by three standard face databases. The first is an Indian face database provided by V. Jain and A. Mukherjee in February 2002 at the IIT Kanpur campus, which contains a set of different face images divided into two main directories: females and males. This study takes 50 images from the Indian face database for use as authentic face images. Next, 160 images were taken from a Faculdade de Engenharia Industrial (FEI) face database containing a set of face images taken by the Artificial Intelligence Laboratory of FEI in Sao Bernardo do Campo, Sao Paulo, Brazil, between June 2005 to March 2006. Of the 160 images, 110 are used as authentic face images and 50 as fake face images. Lastly, a Slovenia face database (CVL) containing a set of face images taken by a faculty of computer and information science department. One hundred and ten images are taken from the CVL face database for use as fake face images.

In addition, to conduct a large number of experiments evaluating the performance of the watermark algorithm in various scenarios, four 24-bit color images 512 × 512 in size were chosen from the common standard databases: the USC-SIPI and CVG-UGR [39], [40] image databases. These four images are shown in Figure 3(a) to 3(d), and two 24-bit color watermark images of size 32 × 32 are shown in

Figure 4. We have implemented a variety of simulations, including 12 attacks on the watermarked images, making a comparison of the proposed algorithm and the algorithms in previous studies [41]–[43] using three conventional performance metrics.

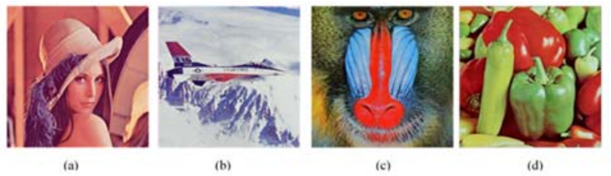


Fig. 3 (a) Lena, (b) F16, (c) Baboon, (d) Peppers.

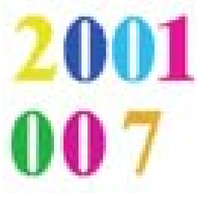


Fig. 4 Watermarked image.

4.2 Metrics

In this study, three conventional performance metrics are used for evaluating watermarking imperceptibility and robustness: PSNR, SSIM, and NCC. PSNR and SSIM are used to evaluate imperceptibility, and high values indicate good imperceptibility. NCC is used to test the robustness of a digital watermark, and a low BER or a high NCC are indicative of strong robustness [15], [44].

First, PSNR is used to measure the similarity between the original host image and the watermarked image and to analyze the visual quality of the watermarked images, with high PSNR values indicating that the degree of similarity between the original image and the watermarked image is high, which indicates high invisibility and high image quality. PSNR is expressed in Equation (8) [15], [44].

$$PSNR_j = 101g \frac{M \times N \times max\{[H(x,y,j)]^2\}}{\sum_{x=1}^{M}\sum_{y=1}^{N}[H(x,y,j)-H^*(x,y,j)]^2} \quad (7)$$

where j = 1,2,3 denote R, G, and B channels respectively; $H(x,y,j)$ and $H^*(x,y,j)$ are the pixel values of the original image and the watermarked image in the j-th channel at coordinates (x,y); and M and N are the size of the image row and column, respectively.

Then, in the color image, the equation is

$$PSNR = \sum_{j=1}^{3} PSNR_j \quad (8)$$

where $PSNR_j$ is the $PSNR$ corresponding to the j-th channel in the color image.

Second, SSIM measures the similarity between two images based on the visual characteristics of the human eye and assesses images by comparing brightness, contrast, and structure. Values are between [0,1], and the maximum value of 1 indicates that the two images are identical. SSIM is expressed in Equation (9) [15], [44].

$$SSIM(H,H^*) = l(H,H^*)c(H,H^*)s(H,H^*) \quad (9)$$

where SSIM comprises the following three equations

$$l(H,H^*) = \frac{2\,\mu_H\mu_{H^*}+C_1}{\mu_H^2+\mu_{H^*}^2+C_1} \quad (10)$$

Equation (6) is a function of the luminance comparison obtained by calculating the means μ_H and μ_{H^*} of the images H and H^*.

$$c(H,H^*) = \frac{2\,\sigma_H\sigma_{H^*}+C_2}{\sigma_H^2+\sigma_{H^*}^2+C_2} \quad (11)$$

Equation (7) is a function of contrast comparison obtained by calculating the standard deviations σ_H and σ_{H^*} of images H and H^*.

$$s(H,H^*) = \frac{\sigma_{HH^*}+C_3}{\sigma_H\sigma_{H^*}+C_3} \quad (12)$$

Equation (8) is a function of structure comparison obtained by calculating the covariance σ_{HH^*} berween H and H^*. C_1, C_2, and C_3 in the three equations are constants used to avoid having zero in the denominators.

Third, the NCC is used to describe the similarity and difference between the extracted watermark and the original watermark. Values are between [0,1], and a value closer to 1 indicates a high similarity between the two images and superior robustness of the digital watermark. NCC is expressed in Equation (13) [15], [44].

$$NC = \frac{\sum_{j=1}^{3}\sum_{x=1}^{m}\sum_{y=1}^{n}(W(x,y,j)\times W^*(x,y,j))}{\sqrt{\sum_{j=1}^{3}\sum_{x=1}^{m}\sum_{y=1}^{n}[W(x,y,j)]^2}\sqrt{\sum_{j=1}^{3}\sum_{x=1}^{m}\sum_{y=1}^{n}[W^*(x,y,j)]^2}} \quad (13)$$

where m and n are the row and column sizes of the watermarked image; $W(x,y,j)$ and $W^*(x,y,j)$ represent the pixels of the original watermarked image and the extracted watermarked image, respectively, at coordinates (x,y) in the j-th channels.

4.3 Imperceptibility: Measurement and Analysis

Imperceptibility is one of the basic characteristics for evaluating the performance of digital watermarks. It measures the distortion between host content and watermarked content within the human auditory and visual range. Higher PSNR and SSIM values indicate good imperceptibility between the original and the watermarked image. This study evaluates the proposed scheme by embedding the color watermark images (Figure 4) into the four standard cover images—Lena, F16, Baboon, and Peppers, shown in Figure 3(a) to 3(d)—to test the invisibility of the proposed algorithm. The performance of the watermark embedding process depends on the gain factor *k*, which varies (k = 2, 5, 10, 12), and two uncorrelated noise sequences. Using different gain factor (*k*) values, it is clearly evident from the results of the extracted watermark images (Table 2 to Table 5) that a small gain factor value affects the quality of the extracted watermark image and decreases the correlation values. On the other hand, when the value of the gain factor increases, the correlation values also increase. The quality measure of PSNR, SSIM, and NCC with different gain factor *k* values are presented in Table 6.

Table 2: Quality Test with a Gain Factor of 2

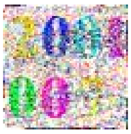
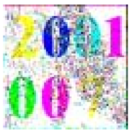
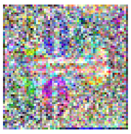
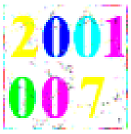
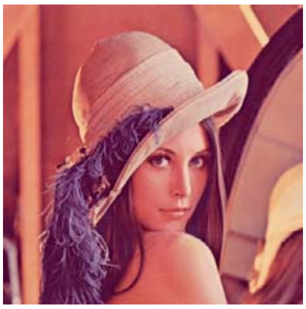
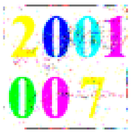
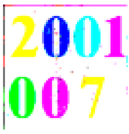
Watermarked Image (after embedding watermark)	***Recovered Watermark***
	
	
	
	

Table 3: Quality Test with a Gain Factor of 5

Watermarked Image (after embedding watermark)	***Recovered Watermark***
	
	

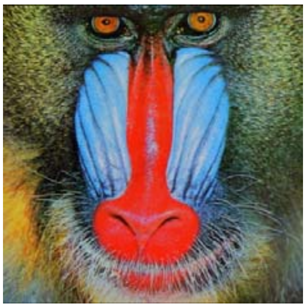
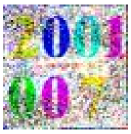
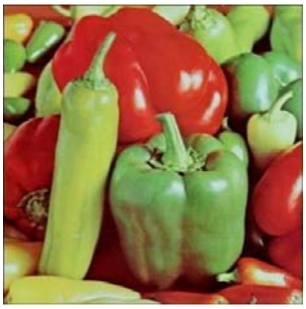
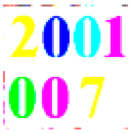
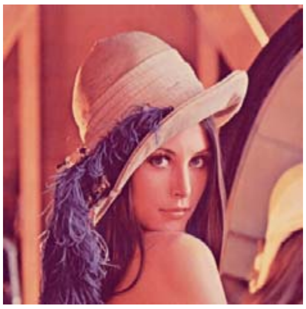
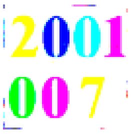
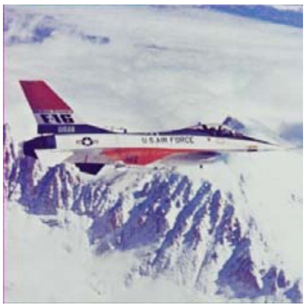
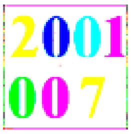
	
	

Table 4: Quality Test with a Gain Factor of 10

Watermarked Image (after embedding watermark)	***Recovered Watermark***
	
	

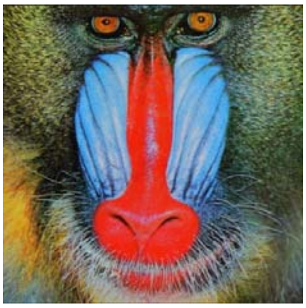
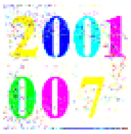
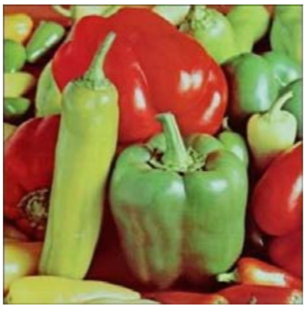
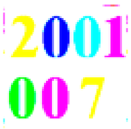
	
	

Table 5: Quality Test with a Gain Factor of 12

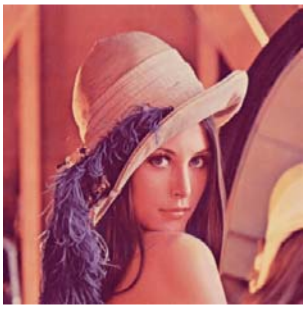
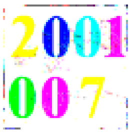
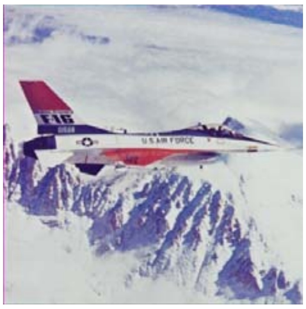
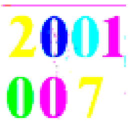
Watermarked Image (after embedding watermark)	***Recovered Watermark***
	
	

Table 6: Quality Measure Values of the Proposed Scheme

Cover Image	*K = 2*			*K = 5*		
	PSNR (dB)	*NC*	*SSIM*	*PSNR (dB)*	*NC*	*SSIM*
Lena	46.0897	0.5961	0.9983	44.1092	0.8679	0.9979
F16	48.0411	0.7176	0.9981	44.1477	0.8843	0.9978
Baboon	39.9008	0.2709	0.9986	39.7048	0.6736	0.9983
Peppers	57.1393	0.8796	0.9979	47.5025	0.9079	0.9978
Cover Image	*K = 10*			*K = 12*		
	PSNR (dB)	*NC*	*SSIM*	*PSNR (dB)*	*NC*	*SSIM*
Lena	36.2042	0.9224	0.9978	36.8914	0.8832	0.9978
F16	38.2196	0.8696	0.9978	36.9693	0.9121	0.9978
Baboon	37.0000	0.8813	0.9976	32.0195	0.8737	0.9979
Peppers	39.8717	0.9187	0.9978	42.3082	0.9014	0.9978

To further verify the effectiveness of the proposed algorithm, a comparison of the proposed algorithm and the algorithms of previous studies [41]–[43] was done to measure watermark invisibility using the cover images Lena, F16, and Peppers. Table 7 presents the experimental results, and it can be seen the average PSNR and SSIM values for the Cheema et al. algorithm [42] are higher than those for the other two studies. This high degree of watermark invisibility indicates that Cheema et al. were unable to achieve a good trade-off between watermark invisibility and robustness. Furthermore, the average PSNR values for the Liu et al. [41] and Su et al. [43] algorithms are approximately 35.6096 dB and 37.842 dB, respectively, and for SSIM, they are approximately 0.9362 and 0.9329, respectively. In contrast, the average values for the proposed method are approximately 39.0900 dB (PSNR) and 0.9714 (SSIM). The proposed method provides better imperceptibility compared to existing schemes, i.e., the watermarked image of the proposed scheme is more similar to the original image per the visual characteristics of the human eye.

Table 7: Comparison of PSNR and SSIM Values of the Proposed Scheme with Existing Schemes [41]–[43].

Cover Image	*Liu et al. Scheme (2019) [41]*		*Su et al. Scheme (2019) [43]*		*Cheema et al. Scheme (2020) [42]*		*Proposed Scheme*	
	PSNR (dB)	*SSIM*	*PSNR (dB)*	*SSIM*	*PSNR (dB)*	*SSIM*	*PSNR (dB)*	*SSIM*
Lena	36.1046	0.9214	37.9574	0.9409	45.0325	0.9992	39.0897	0.9683
F16	36.0268	0.9172	37.7578	0.9305	45.5635	0.9990	40.0411	0.9681
Peppers	34.6974	0.9701	37.8108	0.9274	45.5578	0.9983	38.1393	0.9779
Average	35.6096	0.9362	37.842	0.9329	45.3846	0.9988	39.0900	0.9714

4.4 Robustness: Measurement and Analysis

In this subsection, the NCC values between the original watermark and the extracted watermark are computed to show the robustness of the proposed watermarking method against various kinds of image attacks. Table 8 presents the results generated using a gain factor of 10 for the Lena color cover image and testing it against different attacks, including JPEG compression with Q = (90, 70, 40), Gaussian noise (σ = 0.001, 0.01), salt and pepper noise (σ = 0.1, 0.02), speckle noise (σ = 0.0004), median filter (3 × 3), low-pass filter (3 × 3), scaling (512→256→512), and histogram equalization. Furthermore, after testing the algorithm against different attacks, it is evident in Table 9 that the NCC of the proposed scheme is better than that of the existing schemes [41]–[43] for most of the attacks.

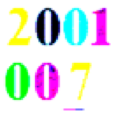
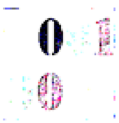
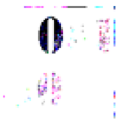
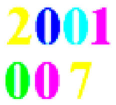
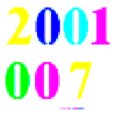
JPEG compression compresses any image, resulting in a perceptible loss in image quality. Thus, for strong robustness, we should ensure that JPEG compression has a smaller effect on the information in the image. JPEG compression based on 10 quality factors is applied to the watermarked Lens images, and the results in Table 9 show that the proposed scheme performs better in resisting JPEG compression and rescaling attacks than the algorithms of existing schemes [41]–[43]. The different noises (i.e., Gaussian noise, salt and pepper noise, and speckle noise) that reduce the visual quality of images were applied at different variance values. The results presented in Table 9 show that the proposed scheme performs better than the existing schemes under these attacks. Under Gaussian noise, with σ = 0.001 and σ = 0.01, the proposed algorithm performs better than the algorithms of Liu et al. [41] and Su et al. [43], with NCC values of 0.9632 and 0.9716, respectively. The NCC value for salt and pepper noise with σ = 0.1 in the Cheema et al. study [42] is 0.9711, while for the proposed algorithm, it is 0.9876. For salt and pepper noise with σ = 0.02, the proposed algorithm scores better than the Liu et al. [41] and Su et al. [43] algorithms with an NCC value of 0.9983. The results show that the proposed scheme performs better than the existing schemes [41]–[43] under different noise attacks.

Different filter attacks, including the median filter and low-pass filter were applied. In the previous studies [41]–[43], the median filter, with a (3 × 3) window size, had NCC values of 0.9078, 0.8413, and 0.8788, while our proposed algorithm has an NCC value of 0.9195, which demonstrates that the proposed algorithm can resist the median filtering attack efficiently. Finally, histogram equalization attacks were also applied to the watermarked images as a robustness test, and the results show that the proposed scheme performs better than the existing Cheema et al. scheme [42] under this attack.

4.5 Comparison of the Proposed Scheme with Existing Schemes

A comparison of various features between the proposed scheme and the existing schemes [41]–[43] is summarized in Table 10. The proposed scheme is applied in the FDCuT-DCT domain, while the Liu et al. scheme [41] is performed in the Schur decomposition domain, the Su et al. scheme [43] in the DFT domain, and the Cheema et al. scheme [42] in the finite ridgelet transform, DWT, and SVD domains. The existing schemes [41]–[43] use encryption for color watermark images, while encryption is not used for this purpose in the proposed scheme. The maximum PSNR value for the proposed scheme is 40.0411 dB, while in the Liu et al. scheme [41], it is 36.1046 dB; for the Su et al. scheme [43], it is 37.9574 dB; and for the Cheema et al. scheme [42], it is 45.5635 dB. The maximum SSIM value for the proposed scheme is 0.9779, while for the Liu et al. scheme [41], it is 0.9701; for the Su et al. scheme [43], it is 0.9409; and for the Cheema et al. scheme [42], it is 0.9992. The maximum NCC value for the proposed scheme is 0.9985, while for the Liu et al. scheme [41], it is 0.9942; for the Su et al. scheme [43], it is 0.9958; and for the Cheema et al. scheme [42], it is 0.9990. Finally, based on a comparison with existing approaches, we found that our approach is better, with a higher level of imperceptibility and stronger robustness.

Table 8: Watermarked Images and Extracted Watermarks under Various Watermarking Attacks for the Proposed Scheme

Attacks	***Watermarked Image (after embedding watermark)***	***Recovered Watermark***	***NCC***
JPEG (Q = 90)			0.9983
JPEG (Q = 70)			0.9975
JPEG (Q = 40)			0.9971
Gaussian Noise (σ = 0.001)			0.9632
Gaussian Noise (σ = 0.01)			0.9716

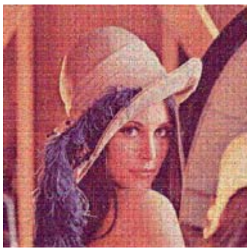
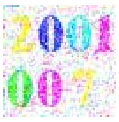
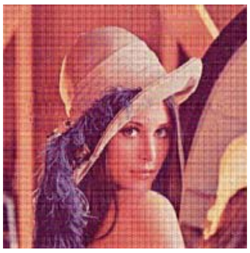
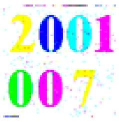
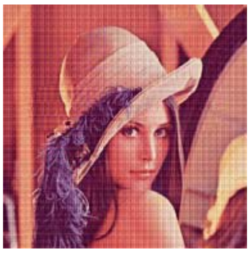
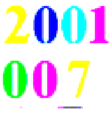
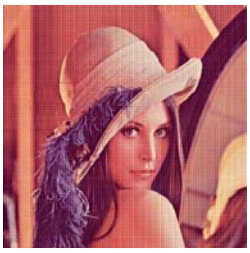
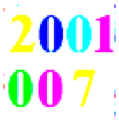
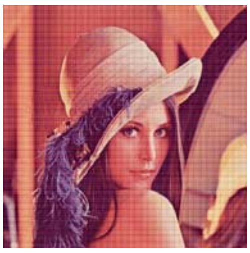
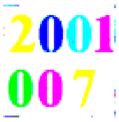
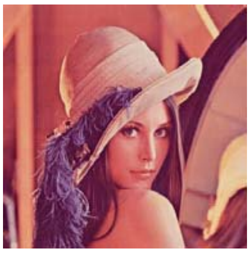
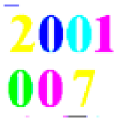
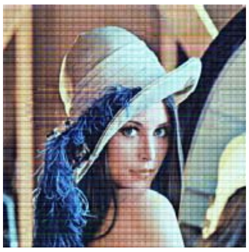
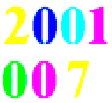
Salt & Pepper Noise ($\sigma = 0.1$)			09876
Salt & Pepper Noise ($\sigma = 0.02$)			0.9983
Speckle Noise ($\sigma = 0.0004$)			0.9185
Median Filter (3 × 3)			0.9195
Low-Pass Filter (3 × 3)			0.9152
Scaling (512→256→512)			0.9158
Histogram Equalization			0.9985

Table 9: Comparison of NCC Values for the Proposed Scheme with those of Existing Schemes [41]–[43].

Attacks	*Liu et al. Scheme (2019) [41]*	*Su et al. Scheme (2019) [43]*	*Cheema et al. Scheme (2020) [42]*	*Proposed Scheme*
JPEG (Q = 90)	Not Reported	Not Reported	0.9975	0.9983
JPEG (Q = 70)	0.9911	Not Reported	Not Reported	0.9975
JPEG (Q = 40)	Not Reported	0.9958	Not Reported	0.9971
Gaussian Noise (0.001)	0.7459	0.9521	Not Reported	0.9632
Gaussian Noise (0.01)	Not Reported	Not Reported	0.9621	0.9716
Salt & Pepper Noise (0.1)	Not Reported	Not Reported	0.9711	09876
Salt & Pepper Noise (0.02)	0.9942	0.9958	Not Reported	0.9983
Median Filter (3 × 3)	0.9078	0.8413	0.8788	0.9195
Histogram Equalization	Not Reported	Not Reported	0.9990	0.9985

Table 10: Comparison of Various Features of Proposed Scheme against Existing Schemes [41]–[43].

Features	*Liu et al. Scheme (2019) [41]*	*Su et al. Scheme (2019) [43]*	*Cheema et al. Scheme (2020) [42]*	*Proposed Scheme*
Embedding Domain	Schur Decomposition	Discrete Fourier Transform	Finite Ridgelet Transform + Discrete Wavelet Transform + Singular Value Decomposition	Discrete Fast Curvelet Transform and Discrete Cosine Transform
Encryption used for Color Watermark Image	Affine transformation	Arnold Transform	Arnold Transform	Not used

Maximum PSNR (dB)	36.1046	37.9574	45.5635	40.0411
Maximum SSIM	0.9701	0.9409	0.9992	0.9779
Maximum NC	0.9942	0.9958	0.9990	0.9985

5. Conclusion

This study develops a reliable and trustworthy hybrid watermarking technique for user authentication in mobile ecosystems that protects multimedia data from unauthorized access and prevents the use of the identity or images by anyone other than the actual owner. It is based on a combination of a face image and the device identity in a mobile ecosystem and uses a watermarking-based approach that cannot be easily removed or destroyed. Consequently, we propose a new blind color face image watermarking technique based on fast discrete curvelet transform (FDCuT), discrete cosine transform (DCT), and two uncorrelated noise sequences. The algorithm was tested under 12 various attacks and compared with similar approaches based on three conventional metrics: PSNR, SSIM, and NCC. It was found that the proposed scheme performs better than existing schemes in terms of imperceptibility and robustness. In the near future, we will work on promoting the implementation of the proposed algorithm in practical applications.

References

[1] M. W. Hatoum, J.-F. Couchot, R. Couturier, and R. Darazi, “Using Deep learning for image watermarking attack,” *Signal Process. Image Commun.*, p. 116019, 2020.

[2] A. Rahman, “Optimum information embedding in digital watermarking,” *J. Intell. Fuzzy Syst.*, vol. 37, no. 1, pp. 553–564, 2019.

[3] S. Parusheva, “A comparative study on the application of biometric technologies for authentication in online banking,” vol. 39, no. 4, p. 12, 2015.

[4] P. Temdee and R. Prasad, *Context-aware communication and computing: Applications for smart environment*. Springer, 2018.

[5] R. Jiang, S. Al-Maadeed, A. Bouridane, D. Crookes, and A. Beghdadi, *Biometric Security and Privacy*. Springer, 2017.

[6] D. C. Wyld, J. Zizka, and D. Nagamalai, Eds., *Advances in Computer Science, Engineering & Applications*, vol. 166. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012.

[7] “What is IMEI Number? - IMEI.info.” https://www.imei.info/faq-what-is-IMEI/ (accessed Nov. 16, 2020).

[8] “What is MEID? - IMEI.info.” https://www.imei.info/faq-what-is-MEID/ (accessed Nov. 16, 2020).

[9] Q. Wei, H. Wang, and G. Zhang, “A Robust Image Watermarking Approach Using Cycle Variational Autoencoder,” *Secur. Commun. Netw.*, vol. 2020, 2020.

[10] X. Zhang, Q. Su, Z. Yuan, and D. Liu, “An efficient blind color image watermarking algorithm in spatial domain combining discrete Fourier transform,” *Optik*, vol. 219, p. 165272, 2020.

[11] J. Abraham and V. Paul, “An imperceptible spatial domain color image watermarking scheme,” *J. King Saud Univ.-Comput. Inf. Sci.*, vol. 31, no. 1, pp. 125–133, 2019.

[12] H.-Y. Shum and M. Liao, *Advances in Multimedia Information Processing-Pcm 2001: Second IEEE Pacific Rim Conference on Multimedia, Beijing, China, October 24-26, 2001, Proceedings*, vol. 2. Springer Science & Business Media, 2001.

[13] M. Begum and M. S. Uddin, “Analysis of Digital Image Watermarking Techniques through Hybrid Methods,” *Adv. Multimed.*, vol. 2020, 2020.

[14] I. Cox, M. Miller, J. Bloom, J. Fridrich, and T. Kalker, *Digital watermarking and steganography*. Morgan kaufmann, 2007.

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

[16] M. Abdullatif, A. M. Zeki, J. Chebil, and T. S. Gunawan, “Properties of digital image watermarking,” in *2013 IEEE 9th International Colloquium on Signal Processing and its Applications*, Kuala Lumpur, Mar. 2013, pp. 235–240, doi: 10.1109/CSPA.2013.6530048.

[17] X. Zhao and A. T. Ho, “An introduction to robust transform based image watermarking techniques,” in *Intelligent multimedia analysis for security applications*, Springer, 2010, pp. 337–364.

[18] S. Ramakrishnan, *Cryptographic and Information Security Approaches for Images and Videos*. CRC Press, 2018.

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

[20] N. Nikolaidis and I. Pitas, “Robust image watermarking in the spatial domain,” *Signal Process.*, vol. 66, no. 3, pp. 385–403, 1998.

[21] Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, “Reversible data hiding,” *IEEE Trans. Circuits Syst. Video Technol.*, vol. 16, no. 3, pp. 354–362, 2006.

[22] W.-H. Chang and L.-W. Chang, “Semi-fragile watermarking for image authentication, localization, and recovery using Tchebichef moments,” in *2010 10th International Symposium on Communications and Information Technologies*, 2010, pp. 749–754.

[23] D. Singh and S. K. Singh, “DWT-SVD and DCT based robust and blind watermarking scheme for copyright

protection," *Multimed. Tools Appl.*, vol. 76, no. 11, pp. 13001–13024, 2017.

[24] M. Begum and M. S. Uddin, "Analysis of Digital Image Watermarking Techniques through Hybrid Methods," *Adv. Multimed.*, vol. 2020, 2020.

[25] C. De Vleeschouwer, J.-F. Delaigle, and B. Macq, "Invisibility and application functionalities in perceptual watermarking an overview," *Proc. IEEE*, vol. 90, no. 1, pp. 64–77, 2002.

[26] O. Hemida, Y. Huo, H. He, and F. Chen, "A restorable fragile watermarking scheme with superior localization for both natural and text images," *Multimed. Tools Appl.*, vol. 78, no. 9, pp. 12373–12403, 2019.

[27] P. Vaidya and C. M. PVSSR, "A robust semi-blind watermarking for color images based on multiple decompositions," *Multimed. Tools Appl.*, vol. 76, no. 24, pp. 25623–25656, 2017.

[28] M. R. M. Isa, S. Aljareh, and Z. Yusoff, "A watermarking technique to improve the security level in face recognition systems," *Multimed. Tools Appl.*, vol. 76, no. 22, pp. 23805–23833, 2017.

[29] H. Agarwal, B. Raman, and I. Venkat, "Blind reliable invisible watermarking method in wavelet domain for face image watermark," *Multimed. Tools Appl.*, vol. 74, no. 17, pp. 6897–6935, 2015.

[30] L. Laur, M. Daneshmand, M. Agoyi, and G. Anbarjafari, "Robust grayscale watermarking technique based on face detection," in *2015 23nd Signal Processing and Communications Applications Conference (SIU)*, May 2015, pp. 471–475, doi: 10.1109/SIU.2015.7129861.

[31] L. Rzouga Haddada and N. Essoukri Ben Amara, "Double watermarking-based biometric access control for radio frequency identification card," *Int. J. RF Microw. Comput.-Aided Eng.*, vol. 29, no. 11, p. e21905, 2019.

[32] P. Singh, B. Raman, and P. P. Roy, "A multimodal biometric watermarking system for digital images in redundant discrete wavelet transform," *Multimed. Tools Appl.*, vol. 76, no. 3, pp. 3871–3897, 2017.

[33] C. Kant and S. Chaudhary, "A Watermarking Based Approach for Protection of Templates in Multimodal Biometric System," *Procedia Comput. Sci.*, vol. 167, pp. 932–941, 2020, doi: 10.1016/j.procs.2020.03.392.

[34] J. H. Abawajy, S. Mukherjea, S. M. Thampi, and A. Ruiz-Martínez, *Security in Computing and Communications: Third International Symposium, SSCC 2015, Kochi, India, August 10-13, 2015. Proceedings*, vol. 536. Springer, 2015.

[35] A. Singh, M. Dave, and A. Mohan, "Multilevel Encrypted Text Watermarking on Medical Images Using Spread-Spectrum in DWT Domain," *Wirel. Pers. Commun.*, vol. 83, no. 3, pp. 2133–2150, Aug. 2015, doi: 10.1007/s11277-015-2505-0.

[36] E. Candes, L. Demanet, D. Donoho, and L. Ying, "Fast discrete curvelet transforms," *Multiscale Model. Simul.*, vol. 5, no. 3, pp. 861–899, 2006.

[37] R. Thanki, S. Borra, V. Dwivedi, and K. Borisagar, "An efficient medical image watermarking scheme based on FDCuT–DCT," *Eng. Sci. Technol. Int. J.*, vol. 20, no. 4, pp. 1366–1379, 2017.

[38] W. Huai-bin, Y. Hong-liang, W. Chun-dong, and W. Shao-ming, "A new watermarking algorithm based on DCT and DWT fusion," in *2010 International Conference on Electrical and Control Engineering*, 2010, pp. 2614–2617.

[39] "CVG - UGR - Image database." https://ccia.ugr.es/cvg/dbimagenes/c512.php (accessed Mar. 11, 2021).

[40] "SIPI Image Database." http://sipi.usc.edu/database/ (accessed Mar. 11, 2021).

[41] D. Liu, Z. Yuan, and Q. Su, "A blind color image watermarking scheme with variable steps based on Schur decomposition," *Multimed. Tools Appl.*, pp. 1–23, 2019.

[42] A. M. Cheema, S. M. Adnan, and Z. Mehmood, "A Novel Optimized Semi-Blind Scheme for Color Image Watermarking," *IEEE Access*, vol. 8, pp. 169525–169547, 2020.

[43] Q. Su *et al.*, "New rapid and robust color image watermarking technique in spatial domain," *IEEE Access*, vol. 7, pp. 30398–30409, 2019.

[44] X. Zhang, Q. Su, Z. Yuan, and D. Liu, "An efficient blind color image watermarking algorithm in spatial domain combining discrete Fourier transform," *Optik*, vol. 219, p. 165272, 2020.